Abstract Algebra

Basics, Polynomials, Galois Theory

Categorial and Commutative Algebra

by Andreas Hermann

June 22, 2005 (383 pages)

If you have read this text I would like to invite you to contribute to it. Comments, corrections and suggestions are very much appreciated, at

bernhard.der.grosse@gmx.de, or visit my homepage at

www.mathematik.uni-tuebingen.de/ab/algebra/index.html

This book is dedicated to the entire mathematical society. To all those who contribute to mathematics and keep it alive by teaching it.

Contents

	0.1	About this Book				
	0.2	Notation and Symbols				
	0.3	Mathematicians at a Glance				
1	Gro	ups and Rings 17				
	1.1	Defining Groups				
	1.2	Defining Rings $\ldots \ldots 22$				
	1.3	Examples $\ldots \ldots 26$				
	1.4	First Concepts				
	1.5	Ideals				
	1.6	Homomorphisms $\ldots \ldots 54$				
	1.7	Products				
2	Commutative Rings 67					
	2.1	Maximal Ideals				
	2.2	Prime Ideals				
	2.3	$Radical \ Ideals \ . \ . \ . \ . \ . \ . \ . \ . \ . \ $				
	2.4	Noetherian Rings				
	2.5	Unique Factorisation Domains				
	2.6	Principal Ideal Domains				
	2.7	Lasker-Noether Decomposition				
	2.8	Finite Rings				
	2.9	Localisation				
	2.10	Local Rings				
	2.11	Dedekind Domains				
3	Mod	lules 146				
	3.1	Defining Modules				
	3.2	First Concepts				
	3.3	Free Modules				
	3.4	Homomorphisms				
	3.5	Rank of Modules \hdots				
	3.6	Length of Modules $\ldots \ldots 179$				
	3.7	Localisation of Modules $\hfill \ldots \hfill \hfill \ldots \hfill \hfill \ldots \hfill \ldots$				

4	\mathbf{Lin}	ear Algebra 181
	4.1	Matices
	4.2	Elementary Matrices
	4.3	Linear Equations
	4.4	Determinants
	4.5	Rank of Matrices
	4.6	Canonical Forms
5	Str	ucture Theorems 187
	5.1	Asociated Primes
	5.2	Primary Decomposition
	5.3	The Theorem of Prüfer
6	Pol	ynomial Rings 191
	6.1	Monomial Orders
	6.2	Graded Algebras
	6.3	Defining Polynomials
	6.4	The Standard Cases
	6.5	Roots of Polynomials
	6.6	Derivation of Polynomials
	6.7	Algebraic Properties
	6.8	Gröbner Bases
	6.9	Algorithms
7	Pol	ynomials in One Variable 209
	7.1	Interpolation
	7.2	Irreducibility Tests
	7.3	Symmetric Polynomials
	7.4	The Resultant
	7.5	The Discriminant $\ldots \ldots 214$
	7.6	Polynomials of Low Degree
	7.7	Polynomials of High Degree
	7.8	Fundamental Theorem of Algebra
8	Gro	oup Theory 218
9	Mu	ltilinear Algebra 219
	9.1	Multilinear Maps
	9.2	Duality Theory
	9.3	Tensor Product of Modules
	9.4	Tensor Product of Algebras
	9.5	Tensor Product of Maps
	9.6	Differentials

10 Categorial Algebra	225				
10.1 Sets and Classes	. 225				
10.2 Categories and Functors	. 226				
10.3 Examples	. 227				
10.4 Products	. 228				
10.5 Abelian Categories	. 229				
10.6 Homology \ldots	230				
11 Ring Extensions	231				
12 Galois Theory	232				
13 Graded Rings 233					
14 Valuations 23					
15 Proofs - Fundamentals	236				
16 Proofs - Rings and Modules	2 46				
17 Proofs - Commutative Algebra	300				

0.1 About this Book

The Aim of this Book

Mathematics knows two directions - analysis and algebra - and any mathematical discipline can be weighted how analytical (resp. algebraical) it is. Analysis is characterized by having a notion of convergence that allows to approximate solutions (and reach them in the limit). Algebra is characterized by having no convergence and hence allowing finite computations only. This book now is meant to be a thorough introduction into algebra.

Likewise every textbook on mathematics is drawn between two pairs of extremes: (easy understandability versus great generality) and (completeness versus having a clear line of thought). Among these contrary poles we usually chose (generality over understandability) and (completeness over a clear red line). Nevertheless we try to reach understandability by being very precise and accurate and including many remarks and examples.

At last some personal philosophy: a perfect proof is like a flawless gem unbreakably hard, spotlessly clear, flawlessly cut and beautifully displayed. In this book we are trying to collect such gemstones. And we are proud to claim, that we are honest about where a proof is due and present complete proofs of almost every claim contained herein (which makes this textbook *very* different from most others).

This Book is Written for

many differen kinds of mathematicans: primarily is meant to be a source of reference for intermediate to advanced students, who have already had a first contact with algebra and now closely examine some topic for their seminars, lectures or own thesis. But because of its great generality and completeness it is also suited as an encyclopedia for professors who prepare their lectures and researchers who need to estimate how far a certain method carries. Frankly this book is not perfectly suited to be a monograph for novices to mathematics. So if you are one we think you can greatly profit from this book, but you will propably have to consult additional monographs (at a more introductory level) to help you understand this text.

Prerequisites

We take for granted, that the reader is familiar with the basic notions of naive logic (statements, implication, proof by contradiction, usage of quantifiers, ...) and naive set theory (Cantor's notion of a set, functions, parially ordered sets, equivalence relations, Zorn's Lemma, ...). We will present a short introduction to classes and the NBG axioms when it comes to category theory. Further we require some basic knowledge of integers (including proofs by induction) and how to express them in decimal numbers. We will sometimes use the field of real numbers, as they are most propably wellknown to the reader, but they are not required to understand this text. Aside from these prerequesites we will start from scratch.

TOPICS COVERED

We start by introducing groups and rings, immediatly specializing on rings. Of general ring theory we will introduce the basic notions only, e.g. the isomorphism theorems. Then we will turn our attention to commutative rings, which will be the first major topic of this book: we closely study maximal ideals, prime ideals, intersections of such (radical ideals) and the relations to localisation. Further we will study rings with chain conditions (noetherian and artinian rings) including the Lasker-Noether theorem. This will lead to standard topics like the fundamental theorem of arithmetic. And we conclude commutative ring theory by studying discrete valuation rings and Dedekind domains.

Then we will turn our attention to modules, including rank, dimension and length. We will see that modules are a natural and powerful generalisation of ideals and large parts of ring theory generalize to this setting, e.g. localisation and primary decomposition. Module theory naturally leads to linear algebra, i.e. the theory of matrix representations of a homomorphism of modules. Applying the structure theorems of modules (the theorem of Prüfer to be precise) we will treat canonical form theory (e.g. Jordan normal form).

Next we will study polynomials from top down: that is we introduce general polynomial rings (also known as group algebras) and graded algebras. Only then we will regard the more classical problems of polynomials in one variable and their solvability. Finally we will regard polynomials in several variables again. Using Gröbner bases it is possible to solve abstract algebraic questions by purely computational means.

Then we will return to group theory: most textbooks begin with this topic, but we chose not to. Even though group theory seems to be elementary and fundamental this is notquite true. In fact it heavily relies on arguments like divisibility and prime decomposition in the integers, topics that are native to ring theory. And commutative groups are best treated from the point of view of module theory. Never the less you might as well skip the previous sections and start with group theory right away. We will present the standard topics: the isomorphism theorems, group actions (including the formula of Burnside), the theorems of Sylow and lastly the p-q-theorem. However we are aiming directly for the representation theory of finite groups.

The first part is concluded by presenting a thorough introduction to what is called multi-linear algebra. We will study dual pairings, tensor products of modules (and algebras) over a commutative base ring, derivations and the module of differentials. Thus we have gathered a whole buch of seperate theories - and it is time for a second structurisation (the first structurisation being algebra itself). We will introduce categories, functors, equivalency of categories, (co-)products and so on. Categories are merely a manner of speaking nothing that can be done with category theory could not have been achieved without. Yet the language of categories presents a unifying concept for all the different branches of mathematics, extending far beyond algebra. So we will first recollect which part of the theory we have established is what in the categories as a unifying concept of all those seperate theories.

We will then aim for some more specialized topics: At first we will study ring extensions and the dimension theory of commutative rings. A special case are field extensions including the beautiful topic of Galois theory. Afterwards we turn our attention to filtrations, completions, zeta-functions and the Hilbert-Samuel polynomial. Finally we will venture deeper into number theory: studying valuations theory up to the theorem of Riemann-Roche for number fields.

TOPICS NOT COVERED

There are many instances where, dropping a finiteness condition, one has to introduce some topology in order to pursue the theory further. Examples are: linear algebra on infinite dimensional vector-spaces, representation theory of infinite groups and Galois theory of infinite field extensions. Another natural extension would be to introduce the Zariski toplogy on the spectrum of a ring, which would lead to the theory of schemes directly. The scope of this text is purely algebraic and hence we will stop at the point where toplogoy sets in (and give hints for further readings only).

The Two Parts

Mathematics has a peculiarity to it: there are problems (and answers) that are easy to understand but hard to prove. The most famous example is Fermat's Last Theorem - the statement (for any $n \ge 3$ there are no nontrivial integers $(a, b, c) \in \mathbb{Z}^3$ that satisfy the equation $a^n + b^n = c^n$) can be understood by anyone. Yet the proof is extremely hard to provide. Of course this theorem has no value of its own (it is the proof that contains deep insights into the structure of mathematics), but this is no general rule. E.g. the theorem of Wedderburn (every finite skew-field is a field) is easy and useful, but its proof will be perfomed using a beautiful trick-computation (requiring the more advanced method of cyclotomic polynomials).

Thus we have chosen an uncostomary approach: we have seperated the truth (i.e. definitions, examples and theorems) from their proofs. This enables us to present the truth in a stringent way, that allows the reader to get a feel for the mathematical objects displayed. Most of the proofs could have been given right away, but in several cases the proof of a statement can only be done after we have developped the theory further. Thus the sequel of theorems may (and will) be different from the order in which they are proved. Hence the two parts.

OUR BEST ADVICE

It is a well-known fact, that some proofs are just computational and only contain little (or even no) insight into the structure of mathematics. Others are brilliant, outstanding insights that are of no lesser importance than the theorem itself. Thus we have already included remarks of how the proof works in the first part of this book. And our best advice is to read a section entirely to get a feel for the objects involved - only then have a look at the proofs that have been recommended. Ignore the other proofs, unless you have to know about them, for some reason. At several occasions this text contains the symbols (\diamondsuit) and (\blacksquare). These are meant to guide the reader in the following way:

- (◊) As we have assorted the topics covered thematically (paying little attention to the sequel of proofs) it might happen that a certain example or theorem is beyond the scope of the theory presented so far. In this case the reader is asked to read over it lightly (or even skip it entirely) and come back to it later (when he has gained some more experience).
- (■) On some very rare occasions we will append a theorem without giving a proof (if the proof is beyond the scope of this text). Such an instance will be marked by the *black box* symbol. In this case we will always give a complete reference of the most readable proof the author is aware of. And this symbol will be hereditarily, that is once we use a theorem that has not been proved any other proof relying on the unproved statement will also be branded by the black box symbol.

0.2 Notation and Symbols

Conventions

We now wish to include a set of the frequently used symbols, conventions and notations. In particular we clarify the several domains of numbers.

- First of all we employ the nice convention (introduced by Halmos) to write *iff* as an abbreviation for *if and only if*.
- We denote the set of natural numbers i.e. the positive integers including zero by $\mathbb{N} := \{0, 1, 2, 3, ...\}$. Further for any two integers $a, b \in \mathbb{Z}$ we denote the interval of integer numbers ranging from a to b by $a \dots b := \{k \in \mathbb{Z} \mid a \le k \le b\}$.
- We will denote the set of integers by Z = N ∪ (-N), and the rationals by Q = { a/b | a, b ∈ Z, b ≠ 0 }. Whereas Z will be taken for granted, Q will be introduced as quotient field of Z.
- The reals will be denoted by \mathbb{R} and we will present an example of how they can be defined (without proving their properties however). The complex numbers will be denoted by $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ and we will present several ways of constructing them.
- (\diamond) We will sometimes use the *Kronecker-Symbol* $\delta(a, b)$ (in the literature this is also denoted by $\delta_{a,b}$), which is defined to be

$$\delta(a,b) = \delta_{a,b} := \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

In most cases a and $b \in \mathbb{Z}$ will be integers and $0, 1 \in \mathbb{Z}$ will be integers, too. But in general we are given some ring $(R, +, \cdot)$ and $a, b \in R$. Then the elements 0 and $1 \in R$ on the right hand side are taken to be the zero-element 0 and unit-element 1 of R again.

- We will write $A \subseteq X$ to indicate that A is a subset of X and $A \subset X$ will denote strict inclusion (i.e. $A \subseteq X$ and there is some $x \in X$ with $x \notin A$). For any set X we denote its power set (i.e. the set of all its subsets) by $\mathcal{P}(X) := \{A \mid A \subseteq X\}$. And for a subset $A \subseteq X$ we denote the complement of A in X by $\mathbf{C}A := X \setminus A$.
- Listing several elements $x_1, \ldots, x_n \in X$ of some set X, we do not require these x_i to be pairwise distict (e.g. $x_1 = x_2$ might well happen). Yet if we only give explicit names x_i to the elements of some previously given subset $A = \{x_1, \ldots, x_n\} \subseteq X$ we already consider the x_i to be pairwise distinct (that is $x_i = x_j$ implies i = j). Note that if the x_i (not the set $\{x_1, \ldots, x_n\}$) is given then $\{x_1, \ldots, x_n\}$ may hence contain fewer than n elements!

• Given an arbitrary set of sets \mathcal{A} one defines the grand union $\bigcup \mathcal{A}$ and the grand intersection $\bigcap \mathcal{A}$ to be the set consisting of all elements a that are contained in one (resp. all) of the sets $A \in \mathcal{A}$, formally

$$\bigcup \mathcal{A} := \{ a \mid \exists A \in \mathcal{A} : a \in A \}$$
$$\bigcap \mathcal{A} := \{ a \mid \forall A \in \mathcal{A} : a \in A \}$$

Note that $\bigcap \mathcal{A}$ only is a well-defined set, if $\mathcal{A} \neq \emptyset$ is non-empty. A wellknown special case of this is the following: consider any two sets A and B and let $\mathcal{A} := \{A, B\}$. Then $A \cup B = \bigcup \mathcal{A}$ and $A \cap B = \bigcap \mathcal{A}$. This notion is just a generalisation of the ordinary union and intersection to arbitrary collections of sets \mathcal{A} .

• If X and Y are any sets then we will denote the set of all functions from X to Y by $\mathcal{F}(X,Y) = Y^X = \{f \mid f : X \to Y\}$. And for any such function $f : X \to Y : x \to f(x)$ we will denote its **graph** by (note that from the set-theoretical point of view f is its graph)

$$\Gamma(f) := \{ (x, f(x)) \mid x \in X \} \subseteq X \times Y$$

• Once we have defined functions, it is easy to define arbitrary carthesian products. That is let $I \neq \emptyset$ be any non-empty set and for any $i \in I$ let X_i be another set. Let us denote the union of all the X_i by X, that is

$$X := \bigcup_{i \in I} X_i = \{ x \mid \exists i \in I : x \in X_i \}$$

Then the carthesian product of the X_i consists of all the functions $x: I \to X$ such that for any $i \in I$ we have $x_i := x(i) \in X_i$. Note that thereby it is customary to write (x_i) in place of x. Formally

$$\prod_{i \in I} X_i := \{ x : I \to X : i \mapsto x_i \mid \forall i \in I : x_i \in X_i \}$$

- Let $X \neq \emptyset$ be a nonempty set, then a subset of the form $R \subseteq X \times X$ said to be a **relation** on X. And in this case it is customary to write xRy instead of $(x, y) \in R$. This notation will be used primarily for partial orders and equivalence relations (see below).
- Consider any nonempty set $X \neq \emptyset$ again. Then a relation \sim on X is said to be an **equivalence relation** on X, iff it is *reflexive*, *symmetric* and *transitive*. Formally that is for any x, y and $z \in X$ we get

$$\begin{array}{rcl} x = y & \Longrightarrow & x \sim y \\ x \sim y & \Longrightarrow & y \sim x \\ x \sim y, \; y \sim z & \Longrightarrow & x \sim z \end{array}$$

And in this case we define the equivalence class [x] of x to be the set of all $y \in X$ being equivalent to x, that is $[x] := \{ y \in X \mid x \sim y \}$. And the set of all equivalence classes is denoted by $X/\sim := \{ [x] \mid x \in X \}$. Example: if $f : X \to Y$ is any function then we obtain an equivalence relation \sim on X by letting $x \sim y :\iff f(x) = f(y)$. And the equivalence class of $x \in X$ is just the fiber $[x] = f^{-1}(f(x))$.

• Consider a nonempty set $X \neq \emptyset$ once more. Then a family of subsets $\mathcal{P} \subseteq \mathcal{P}(X)$ is said to be a **partition** of X, iff for any $P, Q \in \mathcal{P}$ we obtain the statements

$$\begin{array}{rcl} X & = & \bigcup \mathcal{P} \\ P & \neq & \emptyset \\ P \neq Q \implies & P \cap Q = \emptyset \end{array}$$

Example: if \sim is an equivalence relation on X, then X/\sim is a partition of X. Conversely if \mathcal{P} is a partition of X, then we obtain an equivalence relation \sim on X by letting $x \sim y \iff \exists P \in \mathcal{P} : x \in P$ and $y \in P$. Hence there is a one-to-one correspondence between the equivalence relations on X and the partitions of X given by $\sim \mapsto X/\sim$.

• Consider any nonempty set $I \neq \emptyset$, then a relation \leq on I is said to be a **parial order** on I, iff it is *reflexive*, *transitive* and *anti-symmetric*. Formally that is for any i, j and $k \in I$ we get

$$\begin{array}{ccc} i=j & \Longrightarrow & i\leq j \\ i\leq j, \; j\leq k & \Longrightarrow & i\leq k \\ i\leq j, \; j\leq i & \Longrightarrow & i=j \end{array}$$

And \leq is said to be a **total** or **linear order** iff for any $i, j \in I$ we also get $i \leq j$ or $j \leq i$ (that is any two elements contained in I can be compared). Example: for any set X the inclusion relation \subseteq is a partial (but not linear) order on $\mathcal{P}(X)$. If now \leq is a linear order on I, then we define the *minimum* and *maximum* of $i, j \in I$ to be

$$i \wedge j := \begin{cases} i & \text{if } i \leq j \\ j & \text{if } j \leq i \end{cases} \qquad i \lor j := \begin{cases} j & \text{if } i \leq j \\ i & \text{if } j \leq i \end{cases}$$

• Now consider a partial order \leq on the set X and a subset $A \subseteq X$. Then we define the set A_* of *minimal* respectively the set A^* of *maximal* elements of A to be the following

$$\begin{array}{rcl} A_{*} & := & \left\{ \left. a_{*} \in A \mid \forall \, a \in A : a \leq a_{*} \right. \Longrightarrow \right. a = a_{*} \right. \right\} \\ A^{*} & := & \left\{ \left. a^{*} \in A \mid \forall \, a \in A : a^{*} \leq a \right. \Longrightarrow \right. a = a^{*} \right. \right\} \end{array}$$

And an element $a_* \in A_*$ is said to be a *minimal* element of A. Likewise $a^* \in A^*$ is said to be a *maximal* element of A. Note that in general it may happen that A has several minimal (or maximal) elements or even none at all (e.g. $\mathbb{N}_* = \{0\}$ and $\mathbb{N}^* = \emptyset$). For a linear order minimal (and maximal) elements are unique however.

• Finally \leq is said to be a **well-ordering** on the set X, iff \leq is a linear order on X such that any non-empty subset $A \subseteq X$ has a (already unique) minimal element. Formally that is

$$\forall \emptyset \neq A \subseteq X \ \exists a_* \in A \quad \text{such that} \quad \forall a \in A : a_* \leq a$$

• Let X be any set, then the **cardinality** of X is defined to be the *class* of all sets that correspond bijectively to X. Formally that is

$$|X| := \{Y \mid \exists \omega : X \to Y \text{ bijective}\}$$

Note that most textbooks on set theory define the cardinality to be a certain representant of our |X| here. However the exact definition is of no importance to us, what matters is comparing cardinalities: we define the following relation \leq between cardinals:

$$\begin{split} |X| &\leq |Y| &: \Longleftrightarrow \quad \exists \iota : X \to Y \text{ injective} \\ & \Longleftrightarrow \quad \exists \pi : Y \to X \text{ surjective} \\ |X| &= |Y| &: \Longleftrightarrow \quad \exists \omega : X \to Y \text{ bijective} \\ & \Leftrightarrow \quad |X| \leq |Y| \text{ and } |Y| \leq |X| \end{split}$$

Note that the first equivalency can be proved (as a standard excercise) using equivalency relations and a choice function (axiom of choice). The second equivalency is a rather non-trivial statement called the equivalency theorem of Bernstein. However these equivalencies grant that \leq has the properties of a partial order, i.e. reflexivity, transitivity and anti-symmetry.

(◊) We will introduce and use several different notions of substructures and isomorphy. In order to avoid eventual misconceptions, we emphasise the kinds of structures regarded by applying subscripts to the symbols ≤ and ≤ of substructures and ≈ of isomorphy. E.g. we will write R ≤_r S to indicate, that R is a subring of S, a ≤_i R to indicate that a is an ideal of R and R ≈_r S to indicate that R and S are isomorphic as rings. Note that the latter is different from R ≈_m S (R and S are isomorphic as modules). And this did make sense, since R ≤_r S and hence R and S can be regarded as R-modules. We will use the same subscripts for generated algebraic substructures, i.e. (•)_r for rings, (•)_i for ideals and (•)_m for modules.

Notation

A, B, C	matrices, algebras and monoids
D, E, F	fields
G, H	groups and monoids
I, J, K	index sets
L, M, N	modules
P, Q	subsets and substructures
R, S, T	rings (all kinds of)
U, V, W	vectorspaces, multiplicatively closed sets
X, Y, Z	arbitary sets
a. b. c	elements of rings
d. e	degree of polynomials, dimension
e	neutral element of a (group or) monoid
f. a. h	functions, polynomials and elements of algebras
i. j. k. l	integers and indices
m, n	natural numbers
p. q	residue classes
r, s	elements of further rings
s, t, u	polynomial variables
u, v, w	elements of vectorspaces
x,y,z	elements of groups and modules
α , β , γ	multi-indices
ι, κ	(canonical) monomorphisms
λ, μ	eigenvalues
ρ, σ	(canonical) epimorphisms
ρ, σ, τ	permutations
φ, ψ	homomorphisms
Φ, Ψ	isomorphisms
Ω	(fixed) finite set
αβς	ideals
u, v, v	other ideals
D. J	prime ideals
r, t	other prime ideals
m. n	maximal ideals
f. a. b	fraction ideals
1, 3, 7	

0.3 Mathematicians at a Glance

In the following we wish to give a short list of several mathematicians who's names are attributed to some particular definition or theorem in honor of their outstanding contributions (to the field of algebra). Naturally this list is far from being exhaustive, and if any person has been omitted this is solely due to the author's uninformedness. Likewise it is impossible to boil down an entire life to a few short sentences without crippling the biography. Nevertheless the author is convinced that it would be even more ignorant to make no difference between words like *noetherian* and *factorial*. This is the reason why we chose not to say nothing about these avatars of mathematics.

- ??? Abel
- ??? Akizuki
- Emil Artin
- ??? Bernstein
- ??? Bézout
- ??? Brauer
- Nicolas Bourbaki (???)
- ??? Cauchy
- ??? Cayley
- ??? Cohen
- ??? Dedekind
- ??? Euklid
- Evariste Galois
- ??? Fermat
- Carl Friedrich Gauss
- ??? Gröbner
- David Hilbert
- ??? Hopf
- ??? Jacobi
- ??? Jacobson

- ??? Kaplansky
- ??? Kronecker
- ??? Krull
- ??? Lagrange
- ??? Lasker
- ??? Legendre
- ??? Leibnitz
- ??? Nagata
- ??? Nakayama
- Johann von Neumann
- Isaak Newton
- Emmy Noether
- ??? Ostrowski
- ??? Prüfer
- ??? Pythagoras
- ??? Riemann
- ??? Schur
- ??? Serre
- Bernd Sturmfels
- ??? Sylvester
- ??? Weber
- ??? Wedderburn
- ??? Weierstrass
- André Weil
- ??? Yoneda
- ??? Zariski
- ??? Zorn

Part I The Truth

Chapter 1

Groups and Rings

1.1 Defining Groups

The most familiar (and hence easiest to understand) objects of algebra are rings. And of these the easiest example are the integers \mathbb{Z} . On these there are two operations - an addition + and a multiplication \cdot . Both of these operations have familiar properties (associativity for example). So we first study objects with a single operation \circ only - monoids and groups - as these are a unifying concept for both addition and multiplication. However our aim solely lies in preparing the concepts of rings and modules, so the reader is asked to venture lightly over problems within this section until he has reached the later sections of this chapter.

(1.1) Definition:

Let $G \neq \emptyset$ be any non-empty set and \circ a *binary operation* on G, i.e. \circ is a mapping of the form $\circ : G \times G \to G : (x, y) \mapsto xy$. Then the ordered pair (G, \circ) is said to be a **monoid** iff it satisfies the following properties

- (A) $\forall x, y, z \in G : x(yz) = (xy)z$
- (N) $\exists e \in G \ \forall x \in G : xe = x = ex$

Note that this element $e \in G$ whose existence is required in (N) then already is uniquely determined (see below). It is said to be the **neutral element** of G. And therefore we may define: a monoid (G, \circ) is said to be a **group** iff any element $x \in G$ has an **inverse element** $y \in G$, that is iff

(I) $\forall x \in G \exists y \in G : xy = e = yx$

Note that in this case the inverse element y of x is uniquely determined (see below) and we hence write $x^{-1} := y$. Finally a monoid (or group) (G, \circ) is said to be **commutative** iff it satisfies the property

(C) $\forall x, y \in G : xy = yx$

(1.2) Remark:

• We have to append some remarks here: first of all we have employed a function $\circ: G \times G \to G$. The image $\circ(x, y)$ of the pair $(x, y) \in G \times G$ has been written in an unfamiliar way however

$$xy := \circ(x, y)$$

If you have never seen this notation before it may be somewhat startling, in this case we would like to reassure you, that this actually is nothing new - just have a look at the examples further below. Yet this notation has the advantage of restricting itself to the essential. If we had stuck to the classical notation such terms would be by far more obfuscated. E.g. let us rewrite property (A) in classical terms

$$\circ (x, \circ(y, z)) = \circ (\circ (x, y), z)$$

- It is easy to see that the neutral element e of a monoid (G, ◦) is uniquely determined: suppose that another element f ∈ G would satisfy ∀x ∈ G : xf = x = fx, then we would have ef = e by letting x = e. But as e is a neutral element we have ef = f by (N) applied with x = f. And hence e = f are equal, i.e. e is uniquely determined. Hence in the following we will reserve the letter e for the neutral element of the monoid regarded without specifically mentioning it. In case we apply several monoids at once, we will name the respective neutral elements explicitly.
- Property (A) is a very important one and hence it has a name of its own: **associativity**. A pair (G, \circ) that satisfies (A) only also is called a **groupoid**. We will rarely employ these objects however.
- Suppose (G, \circ) is a monoid with the (uniquely determined) neutral element $e \in G$. And suppose $x \in G$ is some element of G, that has an inverse element. Then this inverse is uniquely determined: suppose both y and $z \in G$ satisfy xy = e = yx and xz = e = zx. Then the asociativity yields y = z, as we may compute

$$y = ye = y(xz) = (yx)z = ez = z$$

• Another important consequence of the associativity is the following: consider finitely many elements $x_1, \ldots, x_n \in G$ (where (G, \circ) is a groupoid at least). Then any application of parentheses to the product $x_1x_2\ldots x_n$ produces the same element of G. As an example consider

$$x_1(x_2(x_3x_4)) = x_1((x_2x_3)x_4) = (x_1(x_2x_3))x_4 = ((x_1x_2)x_3)x_4$$

In every step of these equalities we have only used the associativity law (A). The remarkable fact is that any product of any n elements (here n = 4) only depends on the order of the elements, not on the bracketing. Hence it is costumary to omit the bracketing altogether, i.e. we define

$$x_1 x_2 \dots x_n := ((x_1 x_2) \dots) x_n \in G$$

And any other assingment of pairs (without changing the order) to the elements x_i would yield the same element as $x_1x_2...x_n$. A formal version of this statement and its proof are given in part II of this book. The proof clearly will be done by induction on $n \ge 3$, the foundation of the induction precisely is the associativity.

• Suppose (G, \circ) is any groupoid, $x \in G$ is an element and $1 \leq k \in \mathbb{N}$, then we abbreviate the k-times product of x by x^k , i.e. we let

$$x^k := xx \dots x \quad (k - \text{times})$$

If (G, \circ) even is a monoid (with neutral element e) it is customary to define $x^0 := e$. Thus in this case $x^k \in G$ is defined for all $k \in \mathbb{N}$. Now suppose that x even is invertible (e.g. if (G, \circ) is a group), then we may even define $x^k \in G$ for any $k \in \mathbb{Z}$. Suppose $1 \leq k \in \mathbb{N}$, then

$$x^{-k} := \left(x^{-1}\right)^k$$

• In a commutative groupoid (G, \circ) we may even change the order in which the elements $x_1, \ldots, x_n \in G$ are multiplied. I.e. if we are biven a bijective map $\sigma : 1 \ldots n \longleftrightarrow 1 \ldots$ on the indices $1 \ldots n$ then we get

$$x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)} = x_1x_2\ldots x_n$$

The reason behind this is the following: any permutation σ can be decomposed into a series of transpositions (this is intuitively clear: we can generate any order of *n* objects by repeatedly interchanging two of these objects). And any transposition can be realized by interchanging adjacent objects only. But any transposition of adjacent elements is allowed by property (C). A formal proof of this reasoning will be presented in part II again.

(1.3) Example:

- The most familiar example of a (commutative) monoid are the natural numbers under addition: $(\mathbb{N}, +)$. Here the neutral element is given to be e = 0. However $1 \in \mathbb{N}$ has no inverse element (as for any $a \in \mathbb{N}$ we have a + 1 > 0) and hence $(\mathbb{N}, +)$ is no group.
- The integers however are a (commutative) group $(\mathbb{Z}, +)$ under addition. The neutral element is zero again e = 0 and the inverse element of $a \in \mathbb{Z}$ is -a. Thus \mathbb{N} is contained in a group $\mathbb{N} \subseteq \mathbb{Z}$.
- Next we regard the non-zero rationals $\mathbb{Q}^* := \{a/b \mid 0 \neq a, b \in \mathbb{Z}\}$. These form a group under multiplication (\mathbb{Q}^*, \cdot) . The neutral element is given to be 1 = 1/1 and the inverse of $a/b \in \mathbb{Q}^*$ is b/a.
- Consider any non-empty set $X \neq \emptyset$. Then the set of bijective mappings $S_X := \{ \sigma : X \to X \mid \sigma \text{ bijective} \}$ on X becomes a group under the composition of maps (S_X, \circ) . The neutral element is the identity map $e = \mathbb{1}_X$ and the inverse of $\sigma \in S_X$ is the inverse function σ^{-1} .
- (\diamond) A special case of the above is $\operatorname{gl}_n E := \{ A \in \operatorname{mat}_n E \mid \det E \neq 0 \}$ the set of invertible $(n \times n)$ -matrices over a field $(E, +, \cdot)$. This is a group $(\operatorname{gl}_n E, \cdot)$ under the multiplication of matrices.

(1.4) Remark:

Consider a finite groupoid (G, \circ) , that is the set $G = \{x_1, \ldots, x_n\}$ is finite. Then the composition \circ can be given by a table of the following form

0	x_1	x_2	 x_n
x_1	$x_1 x_1$	$x_1 x_2$	 x_1x_n
x_2	$x_{2}x_{1}$	$x_2 x_2$	 $x_2 x_n$
÷	:	÷	÷
x_n	$x_n x_1$	$x_n x_2$	 $x_n x_n$

Such a table is also known as the **Cayley diagram** of G. As an example consider a set with 4 elements $K := \{e, x, y, z\}$, then the following diagram determines a group structure \circ on K ((K, \circ) is called the *Klein* 4-group).

(1.5) **Proposition:** (viz. 237)

Let (G, \circ) be any group (with neutral element e), $x, y \in G$ be any two elements of G and $k, l \in \mathbb{Z}$. Then we obtain the following identities

$$e^{-1} = e \\ (x^{-1})^{-1} = x \\ (xy)^{-1} = y^{-1}x^{-1} \\ x^{k}x^{l} = x^{k+l} \\ (x^{k})^{l} = x^{kl}$$

In particular the inversion $i: G \longleftrightarrow G: x \mapsto x^{-1}$ of elements is a selfinverse, bijective mapping $i = i^{-1}$ on the group G. If now xy = yx do commute then for any $k \in \mathbb{Z}$ we also obtain

$$xy = yx \implies (xy)^k = x^k y^k$$

(1.6) **Proposition:** (viz. 239)

Let (G, \circ) be a group with neutral element $e \in G$, then a subset $P \subseteq G$ is said to be a **subgroup** of G (written as $P \leq_{g} G$) iff it satisfies

$$e \in P$$

$$x, y \in P \implies xy \in P$$

$$x \in P \implies x^{-1} \in P$$

In other words $P \subseteq G$ is a subgroup of G iff it is a group (P, \circ) under the operation \circ inherited from G. And in this case we obtain an equivalence relation on G by letting (for any $x, y \in G$)

$$x \sim y \quad :\iff \quad y^{-1}x \in P$$

And for any $x \in G$ the equivalence class of x is thereby given to be the **coset** $xP := [x] = \{xp \mid p \in P\}$. We thereby define the **index** [G : P] of P in G to be the following cardinal number

$$\begin{array}{rcl} G/P & \coloneqq & G/\sim \\ [G:P] & \coloneqq & \left| G/P \right| \end{array}$$

And thereby we finally obtain the following identity of cardinals which is called the *Theorem of Lagrange* (and which means $G \longleftrightarrow (G/P) \times P$)

$$|G| = [G:P]|P|$$

1.2 Defining Rings

In the previous section we have introduced an atomic component - groups (and their generalisations monoids and groupoids). We have also introduced some notation, that we employ whenever we are dealing with these objects. We will glue two groupoids over the same set R together - that is we consider a set equipped with two binary relations + and \cdot that are compatible in some way (by distributivity). Note that we again write a + b instead of +(a, b) and likewise $a \cdot b$ (or ab only) for $\cdot(a, b)$. These objects will be called rings and we will dedicate the entire first part of this book to the study of what structures rings may have.

(1.7) Definition:

Let $R \neq \emptyset$ be any non-empty set and consider two binary operations + called **addition** and \cdot called **multiplication** on R

$$\begin{array}{rrrr} + & : & R \times R \to R & : & (a,b) \mapsto a+b \\ & \cdot & : & R \times R \to R & : & (a,b) \mapsto a \cdot b \end{array}$$

Then the ordered tripel $(R, +, \cdot)$ is said to be **ringoid** iff it satisfies both of the following properties (A) and (D)

(A) (R, +) is a commutative group, that is the addition is *associative* and *commutative*, admits a neutral element (called *zero-element*, denoted by 0) and every element of R has an additive inverse. Formally

$$\begin{array}{rcl} \forall \, a,b,c\in R & : & a+(b+c) \,=\, (a+b)+c\\ \forall \, a,b\in R & : & a+b \,=\, b+a\\ \exists \, 0\in R \, \forall \, a\in R & : & a+0 \,=\, a\\ \forall \, a\in R \, \exists \, n\in R & : & a+n \,=\, 0 \end{array}$$

Note that the **zero-element** 0 thereby is already uniquely determined and hence the fourth property makes sense. Further, if we are given $a \in R$, then the element $n \in R$ with a + n = 0 is uniquely determined, and we call it the **negative** of a, denoted by -a := n.

(D) The addition and multiplication on R respect the following distributivity laws, i.e. $\forall a, b, c \in R$ we have the properies

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

$$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$$

(1.8) Definition:

In the following let $(R, +, \cdot)$ be a ringoid, then we consider a couple of additional properties (S), (R) and (C), that R may or may not have

(C) The multiplication \cdot on R is *commutative*, that is we have the property

$$\forall a, b, c \in R : a \cdot b = b \cdot a$$

(S) The multiplication \cdot on R is associative, that is we have the property

 $\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(R) The multiplication \cdot on R admits a neutral element 1, that is we have

$$\exists 1 \in R \ \forall a \in R : 1 \cdot a = a = a \cdot 1$$

Note that the neutral element 1 of R in this case already is uniquely determined - it will be called the **unit-element** of R.

(F) Let us assume properties (S) and (R), then we define property (F): every non-zero element R has an *inverse element*, that is

$$\forall 0 \neq a \in R \; \exists i \in R \; : \; a \cdot i \; = \; 1 \; = i \cdot a$$

Note that 1 is given by (R) and due to (S) the element $i \in R$ is uniquely determined by a. We call i the **inverse** of a, denoted by $a^{-1} := i$.

Using these properties we define the following notions: let $(R, +, \cdot)$ be a ringoid, then $(R, +, \cdot)$ is even said to be **commutative** resp. called a **semi-ring**, **ring**, **skew-field** of even **field**, iff

commutative	$:\iff$	(C)
semi-ring	$:\iff$	(S)
ring	$:\iff$	(S) and (R)
commutative ring	$:\iff$	(S), (R) and (C)
skew-field	$:\iff$	(S), (R), (F) and $0 \neq 1$
field	$:\iff$	(S), (R), (C), (F) and $0 \neq 1$

NOTA in the mathematical literature the word *ring* may have many different meanings, depending of what topic a given text pursues. While some authors do not assume rings to have a unit (or even not be associative) others assume them to always be commutative. Hence it also is customary to speak of a *non-unital ring* in case of a semi-ring and of a *unital ring* in case of a ring.

(1.9) Remark:

Let $(R, +, \cdot)$ be a ringoid, then we simplify our notation somewhat by introducing the following conventions

- The zero-element of any ringoid R is denoted by 0. If we deal with several ringoids simultaneously then we will write 0_R to emphasise, which ringoid the zero-element belongs to.
- Analogously the unit element of any ring R is denoted by 1 and by 1_R if we wish to stress the ring R. For some specific rings we will use a different symbol than 1, e.g. 1 or $\mathbb{1}$.
- In order to save some parentheses we agree that the multiplication \cdot is of higher priority than the addition +, e.g. ab + c abbreviates $(a \cdot b) + c$.
- The additive inverse is sometimes used just like a binary operation, i.e. a b stands shortly for a + (-b).
- We have introduced the multiplicative inverse a^{-1} of a and we use the convention that the inversion is of higher priority, than the multiplication itself, i.e. ab^{-1} stands shortly for $a \cdot (b^{-1})$.
- If a₁,..., a_n ∈ R are finitely many elements of R, then we denote the sum and product of these to be the following

$$\sum_{i=1}^{n} a_i := \left((a_1 + a_2) + \dots \right) + a_n$$
$$\prod_{i=1}^{n} a_i := \left((a_1 \cdot a_2) \cdot \dots \right) \cdot a_n$$

• For some integer $k \in \mathbb{Z}$ we now introduce the following abbreviations

$$ka := \begin{cases} \sum_{i=1}^{k} a & \text{for } k > 0 \\ 0 & \text{for } k = 0 \\ \sum_{i=1}^{-k} (-a) & \text{for } k < 0 \end{cases}$$
$$a^{k} := \begin{cases} \prod_{i=1}^{k} a & \text{for } k > 0 \\ 1 & \text{for } k = 0 \\ \prod_{i=1}^{-k} (a^{-1}) & \text{for } k < 0 \end{cases}$$

For the definition of a^k we, of course, required R to be a ring in the case k = 0 and even that a is *invertible* (refer to the next section for this notion) in the case k < 0.

(1.10) Remark:

• Consider any ringoid $(R, +, \cdot)$, then the addition + on R is associative by definition. Hence the result of the sum $a_1 + \cdots + a_n \in R$ does not depend on the way we applied parentheses to it (cf. (1.2)). Therefore we may equally well omit the bracketing in the summation, writing

$$a_1 + \dots + a_n := \sum_{i=1}^n a_i$$

The same is true for the multiplication \cdot in a semi-ring $(R, +, \cdot)$. So by the same reasoning we omit the brackets in products, writing

$$a_1 \dots a_n := \prod_{i=1}^n a_i$$

• Yet by definition the addition + of a ringoid $(R, +, \cdot)$ also is commutative. Thus the sum $a_1 + \cdots + a_n \in R$ does not even depend on the ordering of the a_i (refer to (1.2) again). Now take any finite set Ω and regard a mapping $a : \Omega \to R$. Then we may even define the sum over the unordered set Ω . To do this fix any bijection of the form $\sigma : 1 \dots n \longleftrightarrow \Omega$ (in particular $n := \#\Omega$). Then we may define

$$\sum_{i \in \Omega} a(i) := \begin{cases} 0 & \text{if } \Omega = \emptyset \\ \sum_{i=1}^{n} a(\sigma(i)) & \text{if } \Omega \neq \emptyset \end{cases}$$

The same is true for the multiplication \cdot in a commutative semi-ring $(R, +, \cdot)$. So given $a : \Omega \to R$ and σ as above we define (note that the case $\Omega = \emptyset$ even requires R to be a commutative ring)

$$\prod_{i \in \Omega} a(i) := \begin{cases} 1 & \text{if } \Omega = \emptyset \\ \prod_{i=1}^{n} a(\sigma(i)) & \text{if } \Omega \neq \emptyset \end{cases}$$

• If I is infinite but the set $\Omega := \{i \in I \mid a(i) \neq 0\}$ is finite still we write an infinite sum over all $i \in I$, that actually is defined by a finite sum

$$\sum_{i \in I} a(i) \quad := \quad \sum_{i \in \Omega} a(i)$$

If R is a commutative ring and analogously $\Omega := \{ i \in I \mid a(i) \neq 1 \}$ is finite then the same is true for the infinite product

$$\prod_{i \in I} a(i) := \prod_{i \in \Omega} a(i)$$

1.3 Examples

(1.11) Example:

- The most well-known example of a commutative ring are the integers $(\mathbb{Z}, +, \cdot)$. And they are a most beautiful ring indeed e.g. \mathbb{Z} does not contain zero-divisors (that is ab = 0 implies a = 0 or b = 0). And we only wish to remark here that \mathbb{Z} is an UFD (that is any $a \in \mathbb{Z}$ admits a unique primary decomposition) this will be the formulated and proved as the fundamental theorem of arithmetic.
- Now regard the set 2Z := { 2a | a ∈ Z } of even integers. It is easy to see, that the sum and product of even numbers again is even. Hence (2Z, +, ·) is a (commutative) semi-ring under the operations inherited from Z. Yet it does not contain a unit element 1 and hence does not qualify to be a ring.
- Next we will regard a somewhat strange ring, the so called *zero-ring* Z. As a set it is defined to be $Z := \{0\}$ (with $0 \in \mathbb{Z}$ if you wish). As it solely contains one point 0 it is clear how the binary operations have to be defined 0 + 0 := 0 and $0 \cdot 0 := 0$. It is esy to check that $(Z, +, \cdot)$ thereby becomes a commutative ring in which 1 = 0. We will soon see that Z even is the only ring in which 1 = 0 holds true. In this sense this ring is a bit pathological.
- Now consider an arbitrary (commutative) ring $(R, +, \cdot)$ and a nonempty set $I \neq \emptyset$. Then the set R^I of functions from I to R can be turned into another (commutative) ring $(R^I, +, \cdot)$ under the *pointwise* operations of functions

$$\begin{array}{rcl} R^I & := & \{ f \mid f : I \to R \, \} \\ \\ f + g \; : \; I \to R \; : \; i \mapsto f(i) + g(i) \\ \\ f \cdot g \; : \; I \to R \; : \; i \mapsto f(i) \cdot g(i) \end{array}$$

- Let X be any set and denote its power set by $\mathcal{P}(X) := \{A \mid A \subseteq X\}$. And for any subsets $A, B \subseteq X$ we define the symmetric difference as $A \Delta B := (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) \subseteq X$. Thereby $(\mathcal{P}(X), \Delta, \cap)$ becomes a commutative ring with zero-element \emptyset and unit element X. And if $A \subseteq X$ is any subset, then the additive inverse of A is just -A = A again.
- The next ring we study are the rationals $(\mathbb{Q}, +, \cdot)$. It is well-known that \mathbb{Q} even is a field if $a/b \neq 0$ then $a \neq 0$ and hence $(a/b)^{-1} = (b/a)$ is invertible. We will even present a construction of \mathbb{Q} from \mathbb{Z} in a separate example in this section.

(◊) Another well-known field are the reals (ℝ, +, ·). They may be introduced axiomatically (as a positively ordered field satisfying the supremum-axiom), but we would like to sketch an algebraic construction of ℝ. Let us denote the sets of Cauchy-sequencies and zero-sequencies over the rationals Q respectively

$$\begin{aligned} \mathcal{C} &:= \left\{ \left(q_n \right) \subseteq \mathbb{Q} \; \middle| \; \begin{array}{l} \forall k \in \mathbb{N} \; \exists \, n(k) \in \mathbb{N} \\ \forall \, m, n \geq n(k) \; : \; |q_n - q_m| < 1/k \end{array} \right\} \\ \\ \mathfrak{z} &:= \; \left\{ \left(q_n \right) \subseteq \mathbb{Q} \; \middle| \; \begin{array}{l} \forall k \in \mathbb{N} \; \exists \, n(k) \in \mathbb{N} \\ \forall \, n \geq n(k) \; : \; |q_n| < 1/k \end{array} \right\} \end{aligned}$$

Then \mathcal{C} becomes a commutative ring under the pointwise operations of mappings, that is $(p_n) + (q_n) := (p_n + q_n)$ and $(p_n)(q_n) := (p_n q_n)$. And $\mathfrak{z} \leq_i \mathcal{C}$ is a maximal ideal of \mathcal{C} (cf. to section 2.1). Now the reals can be introduced as the quotient (cf. to section 1.5) of \mathcal{C} modulo \mathfrak{z}

$$\mathbb{R} := \frac{\mathcal{C}}{\delta}$$

As \mathfrak{z} has been maximal \mathbb{R} becomes a field. Thereby \mathbb{Q} can be embedded into \mathbb{R} , as $\mathbb{Q} \hookrightarrow \mathbb{R} : q \mapsto (q)$. And we obtain a positive order on \mathbb{R} by letting $(p_n) + \mathfrak{z} \leq (q_n) + \mathfrak{z} \iff \exists m \in \mathbb{N} \ \forall n \geq m : p_n \leq q_n$. Note that this *completion* of \mathbb{Q} (that is Cauchy-sequencies modulo zero-sequencies) can be generalized to arbitrary metric spaces. Its effect is that the resulting space becomes *complete* (that is Cauchy sequencies are already convergent). In our case this also guarantees the supremum-axiom. Hence this construction truly realizes the reals.

Most of the previous examples have been quite large (considering the number of elements involved). We would now like to present an example of a finite field consisting of precisely four elements F = {0, 1, a, b}. As F is finite, we may give the addition and multiplication in tables

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0
	0	1	a	b
	0	1	$\frac{a}{0}$	$\frac{b}{0}$
$\begin{array}{c} \cdot \\ \hline 0 \\ 1 \end{array}$	0 0 0	1 0 1	$\begin{array}{c} a \\ 0 \\ a \end{array}$	b 0 b
$\begin{array}{c} \cdot \\ \hline 0 \\ 1 \\ a \end{array}$	0 0 0 0	$\begin{array}{c}1\\0\\1\\a\end{array}$	$egin{array}{c} a \\ 0 \\ a \\ b \end{array}$	$b \\ 0 \\ b \\ 1$

(1.12) Example:

Having introduced \mathbb{Z} , \mathbb{Q} and the reals \mathbb{R} we would like to turn our attention to another important case - the *residue rings* of \mathbb{Z} . First note, that the integers \mathbb{Z} allow a division with remainder (cf. to section 2.6). That is if we let $2 \leq n \in \mathbb{N}$ and $a \in \mathbb{Z}$ then there are uniquely determined numbers $q \in \mathbb{Z}$ and $r \in 0 \dots (n-1)$ such that

$$a = qn + r$$

Thereby r is called the *remainder* of a in the integer division of a times n. Formally one denotes (which is common in programming languages)

$$a \operatorname{div} n := q$$
$$a \operatorname{mod} n := r$$

And by virtue of this operation "mod" we may now define the residue ring $(\mathbb{Z}_n, +, \cdot)$ of \mathbb{Z} modulo n. First let $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ as a set. And if $a, b \in \mathbb{Z}_n$, then we define the operations

$$a+b := (a+b) \mod n$$

 $a \cdot b := (a \cdot b) \mod n$

Thereby $(\mathbb{Z}_n, +, \cdot)$ will in fact be a commutative ring. And \mathbb{Z}_n will be a field if and only if n is a prime number. We will soon give a more natrual construction of \mathbb{Z}_n as the quotient $\mathbb{Z}/n\mathbb{Z}$, as this will be far better suited to derive the properties of this ring.

(1.13) Example:

Let $(R, +, \cdot)$ be an *integral domain*, that is $R \neq 0$ is a non-zero commutative ring such that for any two elements $a, b \in R$ we have the implication

$$ab = 0 \implies a = 0 \text{ or } b = 0$$

Then we take to the set $X := R \times (R \setminus \{0\})$ and obtain an equivalence relation \sim on X by letting (where (a, u) and $(b, v) \in X$)

$$(a, u) \sim (b, v) \quad :\iff \quad av = bu$$

If now $(a, u) \in X$ then we denote its equivalence class by a/u, and let us denote the quotient set of X modulo ~ by Q. Formally that is

$$\begin{aligned} \frac{a}{u} &:= \left\{ \left(b, v \right) \in X \mid av = bu \right\} \\ Q &:= \left\{ \left. \frac{a}{u} \right| a, b \in R, \ b \neq 0 \right\} \end{aligned}$$

Thereby Q becomes a commutative ring (with zero-element 0/1 and unit element 1/1) under the following (well-defined) addition and multiplication

$$\begin{array}{rcl} \displaystyle \frac{a}{u} + \frac{a}{u} & := & \displaystyle \frac{av + bu}{uv} \\ \displaystyle \frac{a}{u} \cdot \frac{a}{u} & := & \displaystyle \frac{ab}{uv} \end{array}$$

In fact $(Q, +, \cdot)$ even is a field, called the *quotient field* of R. This is due to the fact that the inverse of $a/u \neq 0/1$ is given to be $(a/u)^{-1} = u/a$. This construction will be vastly generalized in section 2.9. Note that this is precisely the way to obtain the rationals $\mathbb{Q} := Q$ by starting with $R = \mathbb{Z}$.

(1.14) Example:

Consider an arbitrary ring $(R, +, \cdot)$ and $1 \leq n \in \mathbb{N}$, then an $(n \times n)$ -matrix over R is a mapping of the form $A : (1 \dots n) \times (1 \dots n) \to R$. And we denote the set of all such by $\operatorname{mat}_n R := \{A \mid A : (1 \dots n) \times (1 \dots n) \to R\}$. Usually a matrix is written as an array of the following form (where $a_{i,j} := A(i, j)$)

$$A = (a_{i,j}) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$$

And using this notation we may turn $\operatorname{mat}_n R$ into a (non-commutative even if R is commutative) ring by defining the addition and multiplication

$$\begin{pmatrix} a_{i,j} \end{pmatrix} + \begin{pmatrix} b_{i,j} \end{pmatrix} := \begin{pmatrix} a_{i,j} + b_{i,j} \end{pmatrix}$$
$$\begin{pmatrix} a_{i,j} \end{pmatrix} \cdot \begin{pmatrix} b_{i,j} \end{pmatrix} := \begin{pmatrix} \sum_{s=1}^{n} a_{i,s} b_{s,j} \end{pmatrix}$$

It is immediately clear from the construction, that the zero-element, resp. the unit-element are given by the *zero-matrix* and *unit-matirx* respectively

$$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$
$$1 = \begin{pmatrix} 1 & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

(1.15) Example:

Let now $(R, +, \cdot)$ be any commutative ring, the we define the (commutative) ring of *formal power series* over R, as the following set

$$R\llbracket t \rrbracket := \{ f \mid f : \mathbb{N} \to R \}$$

And if $f \in R[t]$ then we will write f[k] instead of f(k), that is $f : k \mapsto f[k]$. Further we denote f as (note that this is purely notational and no true sum)

$$\sum_{k=0}^{\infty} f[k] t^k := f$$

And thereby we may define the sum and product of two formal power series $f, g \in R[t]$, by pointwise summation $f+g: k \mapsto f[k]+g[k]$ and an involution product $f \cdot g: k \mapsto f[0]g[k] + f[1]g[k-1] + \cdots + f[k]g[0]$. In terms of the above notation that is

$$\begin{aligned} f+g &:= \sum_{k=0}^{\infty} \left(f[k] + g[k] \right) t^k \\ f \cdot g &:= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} f[i]g[j] \right) t^k \end{aligned}$$

An elementary computation (cf. section 6.3) shows that $(R[t]], +, \cdot)$ truly becomes a commutative ring. The zero-element of this ring is given by $0: k \mapsto 0$ and the unit element is $1 = t^0: k \mapsto \delta(k, 0)$. The element $t: k \mapsto \delta(k, 1)$ plays another central role. An easy computation shows that for any $n \in \mathbb{N}$ we get $t^n: k \mapsto \delta(k, n)$. If now $0 \neq f \in R[t]$ is a non-zero formal power series we define the *degree* of f to be

$$\deg(f) := \sup\{k \in \mathbb{N} \mid f[k] \neq 0\} \in \mathbb{N} \cup \{\infty\}$$

That is $\deg(f) < \infty$ just states that the set $\{k \in \mathbb{N} \mid f[k] \neq 0\}$ is a finite subset of \mathbb{N} . And thereby we define the *polynomial ring* over R to be

$$R[t] := \{ f \in R[t] \mid \deg(f) < \infty \}$$

By definition $R[t] \subseteq R[t]$ is a subset, but one easily verifies, that R[t] even is another commutative ring under the addition and multiplication inherited from R[t]. Further note that every polynomial $f \in R[t]$ now truly is a finite sum of the form

$$f = \sum_{k=0}^{\infty} f[k] t^k$$

(1.16) Example: (\diamondsuit)

The next example is primarily concerned with ideals, not with rings, and should hence be postponed until you want to study an example of these. Now fix any (commutative) base ring $(R, +, \cdot)$ and a non-empty index set $I \neq \emptyset$. We have already introduced the ring $S := R^I = \mathcal{F}(I, R)$ of functions from I to R under the pointwise operations. For any subset $A \subseteq I$ we now obtain an ideal of S by letting

$$\mathfrak{v}(A) := \{ f \in S \mid \forall a \in A : f(a) = 0 \}$$

And for any two subsets $A, B \subseteq I$ it is easy to prove the following identities

$$\mathfrak{v}(A)\,\mathfrak{v}(B) = \mathfrak{v}(A) \cap \mathfrak{v}(B) = \mathfrak{v}(A \cup B)$$
$$\mathfrak{v}(A) + \mathfrak{v}(B) = \mathfrak{v}(A \cap B)$$

Clearly (if I contains at least two distinct points) S contains zero-divisors. And if I is infinite then S is no noetherian ring (we obtain a strictly ascending chain of ideals by letting $\mathfrak{a}_k := \mathfrak{V}(I \setminus \{a_1, \ldots, a_k\})$ for a sequence of points $a_i \in I$). In this sense S is a *really bad* ring. On the other hand this ring can easily be dealt with. Hence we recommend looking at this ring when searching for counterexamples in general ring theory. Finally if $A \subseteq I$ is a *finite* set then the radical of the ideal $\mathfrak{V}(A)$ can also be given explicitly

$$\sqrt{\mathfrak{V}(A)} = \{ f \in S \mid \forall a \in A : f(a) \in \operatorname{Nil} R \}$$

PROB in the first equality $\mathfrak{V}(A) \cap \mathfrak{V}(B) = \mathfrak{V}(A \cup B)$ is clear and the containment $\mathfrak{V}(A)\mathfrak{V}(B) \subseteq \mathfrak{V}(A) \cap \mathfrak{V}(B)$ is generally true. Thus suppose $h \in \mathfrak{V}(A \cup B)$

$$f(a) := \begin{cases} 0 & \text{if } a \in A \\ 1 & \text{if } a \notin A \end{cases} \text{ and } g(a) := \begin{cases} 0 & \text{if } a \in B \\ h(a) & \text{if } a \notin B \end{cases}$$

then $f \in \mathfrak{P}(A)$ and $g \in \mathfrak{V}(B)$ are clear and also h = fg. Thus we have proved $\mathfrak{V}(A \cup B) \subseteq \mathfrak{V}(A) \cap \mathfrak{V}(B)$ and thereby finished the first set of identities. In the second equality $\mathfrak{V}(A) + \mathfrak{V}(B) \subseteq \mathfrak{V}(A \cap B)$ is clear. And if we are conversely given any $h \in \mathfrak{V}(A \cap B)$ then let us define

$$f(a) := \begin{cases} 0 & \text{if } a \in A \\ h(a) & \text{if } a \notin A \end{cases} \text{ and } g(a) := \begin{cases} h(a) & \text{if } a \in A \setminus B \\ 0 & \text{if } a \notin A \setminus B \end{cases}$$

thereby it is clear that $f \in \mathfrak{V}(A)$ and $g \in \mathfrak{V}(B)$ and an easy distinction of cases truly yields h = f + g. Now consider some $f \in S$ with $f^k \in \mathfrak{V}(A)$. That is for any $a \in A$ we get $f(a)^k = f^k(a) = 0$. In other words $f(a) \in \text{NIL } R$ for any $a \in A$. Conversely suppose that A is finite and that for any $a \in A$ we get $f(a) \in \text{NIL } R$. That is for any $a \in A$ there is some $k(a) \in \mathbb{N}$ such that $f^{k(a)}(a) = 0$. By taking $k := \max\{k(a) \mid a \in A\}$, we find $f^k \in \mathfrak{V}(A)$.

(1.17) Example:

The complex numbers $(\mathbb{C}, +, \cdot)$ also form a field (that even has a lot of properties that make it better-behaved than the reals). We want to present three ways of introducing \mathbb{C} now (note that all are isomorphic):

(1) First of all define $\mathbb{C} := \mathbb{R}^2$ to be the real plane. For any two complex numbers z = (a, b) and w = (c, d) we define the operations

$$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} a+c \\ b+d \end{pmatrix}$$
$$\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} ad-bc \\ ac+bd \end{pmatrix}$$

The advantage of this construction is, that it is purely elementary. The disadvantage is that one has to check that $(\mathbb{C}, +, \cdot)$ truly becomes a field under these operations (which we leave as an excercise). We only present the inverse of $(0,0) \neq z = (a,b) \in \mathbb{C}$. Define the *complex conjugate* of z to be $\overline{z} := (a,-b)$ and let $\nu(z) := z\overline{z} = a^2 + b^2 \in \mathbb{R}$, then $z^{-1} = (a\nu(z)^{-1}, -b\nu(z)^{-1})$. Let us now denote 1 = (1,0) and $i = (0,1) \in \mathbb{C}$, then it is clear, that 1 is the unit element of \mathbb{C} and that $i^2 = -1$. Further any $z = (a,b) \in \mathbb{C}$ can be written uniquely, as z = a1 + bi. It is costumary to write z = a + ib for this however.

(2) (\diamond) The next construction will imitate the one in (1) - yet it realizes (a, b) as a real (2×2) -matrix. This has the advantage, that addition and multiplication are well-known for matrices

$$\mathbb{C} := \left\{ \left(\begin{array}{cc} a & b \\ -b & a \end{array} \right) \ \middle| \ a, b \in \mathbb{R} \right\}$$

It is straighforward to see that \mathbb{C} thereby becomes a field under the addition and multiplication of matrices, that coincides with the one introduced in (1) (check this, it's cute). Note that thereby the determinant plays the role of $\nu(z) = \det(z)$ and the transposition of matrices is the complex conjugation $\overline{z} = z^*$.

(3) (\diamond) The third method implements the idea that *i* is introduced in such a way as to $i^2 = -1$. We simply force a solution of $t^2 + 1 = 0$ into \mathbb{C}

$$\mathbb{C} := \mathbb{R}[t]/(t^2+1)\mathbb{R}[t]$$

Comparing this construction with the one in (1) we have to identify (a, b) with $a + bt + (t^2 + 1)\mathbb{R}[t]$. In particular $i = t + (t^2 + 1)\mathbb{R}[t]$. Then it again is easy to see, that addition and multiplication coincide under this identification. The advantage of this construction is that it focusses on the idea of finding a solution to $t^2 + 1 = 0$ (namely *i*), that \mathbb{C} immediately is a field (as $t^2 + 1$ is prime, $\mathbb{R}[t]$ is a PID and hence $(t^2 + 1)\mathbb{R}[t]$ is maximal). The disadvantage is that it already requires the algebraic machinery, which remains to be introduced here.

(1.18) Example: (\diamondsuit)

Now fix any square-free $0 \neq d \in \mathbb{Z}$ (*d* being sqare-free means that there is no prime number $p \in \mathbb{Z}$ such that p^2 divides *d*). Then we define the following subset of the (reals or) complex numbers

$$\mathbb{Z}[\sqrt{d}] := \left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \right\}$$

Note that $\mathbb{Z}[\sqrt{d}]$ is contained in the reals if and only if 0 < d, and in the case of d < 0 we have $\sqrt{d} = i\sqrt{-d} \in \mathbb{C}$. In any case $\mathbb{Z}[\sqrt{d}]$ becomes a commutative ring under the addition and multiplication inherited from \mathbb{C}

$$(a+b\sqrt{d}) + (e+f\sqrt{d}) = (a+e) + (b+f)\sqrt{d}$$
$$(a+b\sqrt{d}) \cdot (e+f\sqrt{d}) = (ae+dbf) + (af+be)\sqrt{d}$$

It will be most interesting to see how the algebraic porperties of these rings vary with d. E.g. for $d \in \{-2, -1, 2, 3\} \mathbb{Z}[\sqrt{d}]$ will be an Euclidean domain under the Euclidean function $\nu(a + b\sqrt{d}) := |a^2 - db^2|$. Yet $\mathbb{Z}[\sqrt{d}]$ will not even be an UFD for d < -3.

(1.19) Example:

We have just introduced the complex numbers as a two-dimensional space \mathbb{R} over the reals. The next (and last sensibly possible, cf. to the theorem of Frobenius) step in the hirarchy leads us to the *quaternions* \mathbb{H} . These are defined to be a four-dimensional, space $\mathbb{H} := \mathbb{R}^4$ over the reals. And analogous to the above we specifically denote four elements

$$1 := (1, 0, 0, 0)$$

$$i := (0, 1, 0, 0)$$

$$j := (0, 0, 1, 0)$$

$$k := (0, 0, 0, 1)$$

That is any element $z = (a, b, c, d) \in \mathbb{H}$ can be written uniquely, in the form z = a + ib + jc + kd. The addition of elements of \mathbb{H} is pointwise and the multiplication is then given by linear expansion of the following multiplication table for these basis elements

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

For z = a + ib + jc + kd and $w = p + iq + jr + ks \in \mathbb{H}$ these operations are

$$z + w = (a + p) + i(b + q) + j(c + r) + k(d + s)$$

$$zw = (ap - bq - cr - ds) + i(aq + bp + cs - dr)$$

$$+ j(ar - bs + cp + dq) + k(as + br - cq + dp)$$

Note that we may again define $\overline{z} := a - ib - jc - kd$ and thereby obtain $\nu(z) = z\overline{z} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$ such that any non-zero $0 \neq z \in \mathbb{H}$ has an inverse $z^{-1} = \nu(z)^{-1}\overline{z} = (a\nu(z)^{-1}, -b\nu(z)^{-1}, -c\nu(z)^{-1}, -d\nu(z)^{-1})$. Yet \mathbb{H} clearly is not commutative, as ij = k = -ji. Thus the quaternions form a skew-field, but not a field. Using the complex numbers \mathbb{C} we may also realize the quaternions as (2×2) -matrices over \mathbb{C} . Given $a + ib + jc + kd \in \mathbb{H}$ we pick up the complex numbers z = a + ib and $w = c + id \in \mathbb{C}$ and identify a + ib + jc + kd with a (2×2) -matrix of the following form

$$\mathbb{H} \cong_{\mathbf{r}} \left\{ \left(\begin{array}{cc} z & w \\ -\overline{w} & \overline{z} \end{array} \right) \ \middle| \quad z, w \in \mathbb{C} \right\}$$

(1.20) Example: (\diamondsuit)

Let $(R, +, \cdot)$ be an arbitrary ring, we will later employ the **opposite ring** $(R, +, \cdot)^{\text{op}}$ of R. This is defined to be R as a set, under the same addition + but with a multiplication that reverses the order of elements. Formally

$$(R, +, \cdot)^{\operatorname{op}} := (R, +, \circ) \text{ where } a \circ b := b \cdot a$$

Note that thereby $(R, +, \cdot)^{\text{op}}$ is a ring again with the same properties as $(R, +, \cdot)$ before. And if $(R, +, \cdot)$ has been commutative, then the opposite ring of R is just R itself (even as a set), i.e. $(R, +, \cdot)^{\text{op}} = (R, +, \cdot)$.

1.4 First Concepts

Some Combinatoric

In the following proposition we want to establish some basic computational rules, that are valid in arbitrary rings. But in order to do this we first have to recall some elementary facts from combinatorics: First consider a set containing $1 \leq k \in \mathbb{N}$ elements. If we want to put a linear order to this set, we have to choose some first element. To do this there are k possibilities. We commence by choosing the second element - now having (k-1) possibilities, and so on. Thus we end up with a number of linear orders on this set that equals k! the faculty of k, that is defined to be

$$k! := \# \{ \sigma : 1 \dots k \to 1 \dots k \mid \sigma \text{ bijective} \}$$
$$= k \cdot (k-1) \cdots 2 \cdot 1$$

If k = 0 we specifically define 0! := 1. Next we consider a set containing $n \in \mathbb{N}$ elements. If we want to select a subset I of precisely $k \in 0 \dots n$ elements we have to start by choosing a first element (n possibilities). In the next step we may only choose from (n-1) elements and so on. But as a subset does not depend on the order of its elements we still have to divide this by k! - the number of linear orders on I. Altogether we end up with

$$\begin{pmatrix} n \\ k \end{pmatrix} := \# \{ I \subseteq 1 \dots n \mid \#I = k \}$$

$$= \frac{n}{k} \cdot \frac{n-1}{k-1} \cdots \frac{n-k+1}{1}$$

$$= \frac{n!}{k! (n-k)!}$$

Note that this definition also works out in the case n = 0 and k = 0 (in which the *binomial coefficient* (n k) equals one. That is we get (n 0) = 1 = (n n). Furthermore the binomial coefficients satisfy a famous recursion formula

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Finally consider some multi-index $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k$. Then it will be useful to introduce the following notations (where $n := |\alpha|$)

$$\begin{aligned} |\alpha| &:= \alpha_1 + \dots + \alpha_k \\ \alpha! &:= (\alpha_1!) \cdots (\alpha_k!) \\ \binom{n}{\alpha} &:= \frac{n!}{\alpha!} \end{aligned}$$

(1.21) Proposition: (viz. 246)

Let (R, +, ·) be any semi-ring and a, b ∈ R be arbitrary elements of R.
 Then the following statements hold true

$$0 = -0$$

 $a0 = 0 = 0a$
 $(-a)b = -(ab) = a(-b)$
 $(-a)(-b) = ab$

• If now $a_1, \ldots, a_m \in R$ and $b_1, \ldots, n_n \in R$ are finitely many arbitrary elements of R, then we also obtain the general rule of distributivity

$$\left(\sum_{i=1}^{m} a_i\right) \left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$$

And if $J(1), \ldots, J(n)$ are finite index sets (where $1 \leq n \in \mathbb{N}$) and $a(i, j) \in R$ for any $i \in 1 \ldots n, j \in J(i)$ then we let $J := J(1) \times \cdots \times J(n)$ (and $j = (j_1, \ldots, j_n) \in J$) and thereby obtain

$$\prod_{i=1}^{n} \sum_{j_i \in J(i)} a(i, j_i) = \sum_{j \in J} \prod_{i=1}^{n} a(i, j_i)$$

• Now suppose $(R, +, \cdot)$ is a ring, $n \in \mathbb{N}$ and $a, b \in R$ are elements, that mutually commute (that is ab = ba), then we get the *binomial rule*

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

And if $(R, +, \cdot)$ even is a commutative ring $a_1, \ldots, a_k \in R$ are finitely many elements and $n \in \mathbb{N}$ then we even get the *polynomial rule*

$$(a_1 + \dots + a_k)^n = \sum_{|\alpha|=n} {n \choose \alpha} a^{\alpha}$$

where the above sum runs over all multi-indices $\alpha \in \mathbb{N}^k$ that satisfy $|\alpha| = \alpha_1 + \cdots + \alpha_k = n$. And a^{α} abbreviates $a^{\alpha} := (a_1)^{\alpha_1} \cdots (a_k)^{\alpha_k}$.

(1.22) Remark:

Thus there are many computational rules that hold true for arbitrary rings. However there also are some exceptions to integer (or even real) arithmetic. E.g. we are *not* allowed to deduce a = 0 or b = 0 from ab = 0. As a counterexample regard $a = 2 + 6\mathbb{Z}$ and $b = 3 + 6\mathbb{Z}$ in \mathbb{Z}_6 . A special case of this is the following: we may *not* deduce a = 0 from a = -a. As a counterexample regard $a = 1 + 2\mathbb{Z}$ in \mathbb{Z}_2 .
(1.23) Remark:

An exceptional role pays the **zero-ring** $R = \{0\}$, it clearly is a commutative ring (under the trivial operations) that would even satisfy condition (F). But it is the only ring in which 0 = 1. More formally we've got the equalency

$$R = \{0\} \iff 0 = 1$$

[as \implies is clear and in the converse direction regard a = 1a = 0a = 0]. This equality 0 = 1 will lead to some peculiarities however. This is precisely why we required $0 \neq 1$ for skew-fields and fields. And several theorems will require R to be not the zero-ring, which we will abbreviate by $R \neq 0$.

(1.24) Definition: (viz. 250)

Let $(R, +, \cdot)$ be any semi-ring and $b \in R$ be any element of R. Then we define the set ZDR of **zero-divisors**, the set NZDR of **non-zero-divisors**, the **nil-radical** NIL R and the **annulator** ANN (R, b) of b to be

$$\begin{aligned} \text{ZD} R &:= \left\{ a \in R \mid \exists 0 \neq b \in R : ab = 0 \right\} \\ \text{NZD} R &:= \left\{ a \in R \mid \forall b \in R : ab = 0 \implies b = 0 \right\} \\ \text{NIL} R &:= \left\{ a \in R \mid \exists k \in \mathbb{N} : a^k = 0 \right\} \\ \text{ANN} (R, b) &:= \left\{ a \in R \mid ab = 0 \right\} \end{aligned}$$

An element $a \in \text{NIL } R$ contained in the nil-radical is also said to be *nilpotent*. If now R even is a ring we define the set R^* of **units** (or *invertible* elements) and the set R^{\bullet} of *relevant* elements of R to be

$$\begin{array}{rcl} R^* & := & \left\{ \, a \in R \mid \exists \, b \in R : ab = 1 = ba \, \right\} \\ R^\bullet & := & R \setminus \left(\, \left\{ \, 0 \, \right\} \cup R^* \right) \end{array}$$

And $(R, +, \cdot)$ is said to be **integral**, iff it does not contain any non-zero zero-divisors, that is iff it satisfies one of the following equivalent statements

- (a) $ZDR = \{0\}$
- (b) for any a, b and $c \in R$ such that $a \neq 0$ we get $ab = ac \implies b = c$
- (b') for any a, b and $c \in R$ such that $a \neq 0$ we get $ba = ca \implies b = c$
- (c) for any $a, b \in R$ such that $a \neq 0$ we get $ab = a \implies b = 1$
- (c') for any $a, b \in R$ such that $a \neq 0$ we get $ba = a \implies b = 1$

Now $(R, +, \cdot)$ is said to be an **integral domain**, iff it is a commutative ring that also is integral. I.e. a commutative ring with $\text{ZD } R = \{0\}$.

(1.25) Remark:

• Consider any semi-ring $(R, +, \cdot)$, two elements $a, b \in R$ and a non-zerodivisor $n \in NZD R$. Then we obtain the equivalence

 $a = b \iff na = nb$

PROB " \implies " is clear, and if na = nb then n(a - b) = 0 which implies a - b = 0 (and hence a = b), since n is a non-zero-divisor.

• Let $(R, +, \cdot)$ be a ring, $a \in R$ be any element and $n \in NZDR$ be a non-zerodivisor. Then we obtain the implication

$$na = 1 \implies an = 1$$

PROB since n(an) = (na)n = n and hence n(an - 1) = 0. But as n is a non-zerodivisor this implies an - 1 = 0 and hence an = 1.

• Consider a commutative ring $(R, +, \cdot)$ and $a_1, \ldots, a_n \in R$ finitely many elements. Now let $u := a_1 \ldots a_n \in R$, then we obtain the implication

$$u \in R^* \implies a_1, \dots, a_n \in R^*$$

PROB choose any $j \in 1 \dots n$ and let $\hat{a}_j := \prod_{i \neq i} a_i$, then by construction we get $1 = u^{-1}(a_1 \dots a_n) = (u^{-1}\hat{a}_j)a_j$. And hence we see $a_j \in R^*$.

• If $(R, +, \cdot)$ is a skew-field, then R already is integral (i.e. $\text{ZD} R = \{0\}$) and allows division: that is for any $a, b \in R$ with $a \neq 0$ we get

$$\exists ! u, v \in R : ua = b \text{ and } av = b$$

PROB consider $a \neq 0$, since R is a skew-field there is some $i \in R$ such that ai = 1 = ia. Now suppose ab = 0, then b = (ia)b = i(ab) = 0 and hence $a \in NZD R$. This proves $ZD R = \{0\}$. Now consider $a, b \in R$ with $a \neq 0$. Again choose $i \in R$ such that ai = 1 = ia and let u := bi and v := ib. Then ua = (bi)a = b(ia) = b and av = a(ib) = (ai)b = b. Now suppose $u', v' \in R$ with ua = b = u'a and av = b = av'. Then a(v - v') = 0 but as $a \neq 0$ we have seen that this implies v - v' = 0 and hence v = v'. Likewise (u - u')a = 0 but as $u \neq 0$ this can only be, if u - u' = 0 and hence u = u'.

The sets of zero-divisors ZD R and of relevant elements R^{\bullet} rarely carry any noteworthy algebraic structure. Yet the units R^* form a group, the non-zerodivisors NZD R are multiplicatively closed, the nil-radical NIL R is an (even perfect) ideal of R and the annulator ANN (R, b) of some element $b \in R$ is a submodule. Though we have not introduced these structures yet, we would like to present a formal proposition (and proof) of these facts already.

(1.26) Proposition: (viz. 249) (\diamondsuit)

(i) Let $(R, +, \cdot)$ be any semi-ring, then R is the disjoint union of its zerodivisors and non-zero divisors, formally that is

NZD
$$R = R \setminus ZD R$$

(ii) In any non-zero $(R \neq 0)$ ring $(R, +, \cdot)$ the nilradical is contained in the set of zero-divisors. And the zero-divisors are likewise contained in non-units of R. That is we've got the inclusions

$$\operatorname{NIL} R \subseteq \operatorname{ZD} R \subseteq R \setminus R^*$$

(iii) Let $(R, +, \cdot)$ be any semi-ring, then the set NZD $R \subseteq R$ of non-zerodivisors of R is multiplicatively closed, that is we get

$$1 \in \operatorname{NZD} R$$
$$a, b \in \operatorname{NZD} R \implies ab \in \operatorname{NZD} R$$

- (iv) Consider any ring $(R, +, \cdot)$, then (R^*, \cdot) is a group (where \cdot denotes the multiplication of R), called the *multiplicative group* of R.
- (v) If $(R, +, \cdot)$ is any ring then R is a skew-field if and only if the multiplicative group of R consists precisely of the non-zero elements

$$R$$
 skew-field $\iff R^* = R \setminus \{0\}$

(vi) If $(R, +, \cdot)$ is a commutative ring, then the nil-radical is an ideal of R

NIL
$$R \leq_{i} R$$

(vii) Let $(R, +, \cdot)$ be any ring and $b \in R$ an element of R. Then the annulator ANN (R, b) is a left-ideal (i.e. submodule) of R

ANN
$$(R, b) \leq_{\mathrm{m}} R$$

(viii) Let $(R, +, \cdot)$ be a commutative ring and $u \in R^*$ be a unit of R. Then $u + \text{NIL } R \subseteq R^*$. To be precise, if $a \in R$ with $a^n = 0$ then we get

$$(u+a)^{-1} = \sum_{k=0}^{n-1} (-1)^k a^k u^{-k-1}$$

(1.27) Example:

We present a somewhat advanced example that builds upon some results from linear algebra. Let us regard the ring $R := \text{mat}_2 \mathbb{Z}$ of (2×2) -matrices over the integers. We will need the notions of *determinant* and *trace*

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc \in \mathbb{Z}$$
$$\operatorname{tr} \begin{pmatrix} a & b \\ c & d \end{pmatrix} := a + d \in \mathbb{Z}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sharp} := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Then we can explicitly determine which matrices are *invertible* (that is units), which are zero-divisors and which are nilpotent. We find

$$R^* = \{ A \in R \mid \det A = \pm 1 \}$$

ZD $R = \{ A \in R \mid \det A = 0 \}$
NIL $R = \{ A \in R \mid \det A = \operatorname{tr} A = 0 \}$

PROB (\diamondsuit) first note that an easy computation yields $AA^{\sharp} = (\det A)\mathbb{1} = A^{\sharp}A$. Hence if A is invertible, then $A^{-1} = (\det A)^{-1}A^{\sharp}$. Thus A is invertible if and only if det A is a unit (in \mathbb{Z}), but as the units of \mathbb{Z} are given to be $\mathbb{Z}^* = \{\pm 1\}$ this already is the first identity. For the second identity we begin with det A = 0. Then $AA^{\sharp} = (\det A)\mathbb{1} = 0$ and hence A is a zerodivisor. Conversely suppose that $A \in \mathbb{ZD}R$ is a zero-divisor, then AB = 0for some $B \neq 0$ and hence $(\det A)B = A^{\sharp}AB = 0$. But as B is non-zero this implies det A = 0. Finally if det A = 0 then an easy computation shows $A^2 = (\operatorname{tr} A)A$, thus if also $\operatorname{tr} A = 0$ then $A^2 = 0$ and hence $A \in \operatorname{NIL} R$. And if conversely $A \in \operatorname{NIL} R \subseteq \operatorname{ZD} R$, then det A = 0 and hence (by induction on n) $A^n = (\operatorname{tr} A)^{n-1}A$. As A is nilpotent there is some $1 \leq n \in \mathbb{N}$ such that $0 = A^n = (\operatorname{tr} A)^{n-1}A$ and hence $\operatorname{tr} A \in \operatorname{NIL} \mathbb{Z} = \{0\}$.

1.5 Ideals

(1.28) Definition:

- Let $(R, +, \cdot)$ be a semi-ring and $P \subseteq R$ a subset. Then P is said to be a **sub-semi-ring** of R (abbreviated by $P \leq_{s} R$), iff
 - $(1) \ 0 \ \in \ P$
 - (2) $a, b \in P \implies a+b \in P$
 - $(3) \ a \in P \implies -a \in P$
 - $(4) \ a, b \in P \implies ab \in P$
- And if $(R, +, \cdot)$ is a ring having the unit element 1, then a subset $P \subseteq R$ is called a **sub-ring** of R (abbreviated by $P \leq_{\mathbf{r}} R$), iff
 - (S) $P \leq_{\mathrm{s}} R$
 - $(5) 1 \in R$
- Finally if (R, +, ·) even is a (skew)field, then a subset P ⊆ R is said to be a sub-(skew)field of R (abbreviated P ≤_f R), iff
 - (R) $P \leq_{\rm r} R$
 - (6) $0 \neq a \in P \implies a^{-1} \in P$
- Let $(R, +, \cdot)$ be a semi-ring again, then a subset $\mathfrak{a} \subseteq R$ is said to be a **left-ideal** (or **submodule**) of R (abbreviated by $\mathfrak{a} \leq_{\mathrm{m}} R$), iff
 - (1) $0 \in \mathfrak{a}$
 - (2) $a, b \in \mathfrak{a} \implies a+b \in \mathfrak{a}$
 - $(3) \ a \in \mathfrak{a} \implies -a \in \mathfrak{a}$
 - (4) $a \in \mathfrak{a}, b \in R \implies ba \in \mathfrak{a}$

And $\mathfrak{a} \subseteq R$ is said to be an **ideal** of R (abbreviated by $\mathfrak{a} \leq_i R$), iff

- (M) $\mathfrak{a} \leq_{\mathrm{m}} R$ (5) $a \in \mathfrak{a}, b \in R \implies ab \in \mathfrak{a}$
- We will sometimes use the set of all subrings (of a ring R), the set of all sub(skew)fields (of a (skew)field R), resp. the set of all (left-)ideals (of a semi-ring R) these will be denoted, by

$$subr R := \{ P \subseteq R \mid P \leq_{r} R \}$$
$$subf R := \{ P \subseteq R \mid P \leq_{f} R \}$$
$$subm R := \{ \mathfrak{a} \subseteq R \mid \mathfrak{a} \leq_{m} R \}$$
$$ideal R := \{ \mathfrak{a} \subseteq R \mid \mathfrak{a} \leq_{i} R \}$$

(1.29) Remark:

• Consider any semi-ring $(R, +, \cdot)$ and a sub-semi-ring $P \leq_{s} R$ of R. Then we would like to emphasise, that the notion of a sub-semi-ring was defined in such a way that the addition + and multiplication \cdot of R induces the like operations on P

$$+\Big|_{P} : P \times P \to P : (a,b) \mapsto a + b$$
$$\cdot\Big|_{P} : P \times P \to P : (a,b) \mapsto ab$$

And thereby $(P, +|_P, \cdot|_P)$ becomes a semi-ring again (clearly all the properties of such are inherited from R). And in complete analogy we find that subrings of rings are rings again and sub(skew)fields of (skew)fields are (skew)fields again, under the induced operations.

NOTA as $+|_{P}$ and $\cdot|_{P}$ are just restrictions (to $P \times P$) of the respective functions + and \cdot on R, we will not distinguish between $+|_{P}$ and +respectively between $\cdot|_{P}$ and \cdot . That is we will speak of the semiring $(P, +, \cdot)$, where + and \cdot here are understood to be the restricted operations $+|_{P}$ and $\cdot|_{P}$ respectively.

- Beware: it is possible, that a sub-semi-ring $P \leq_{s} R$ is a ring $(P, +, \cdot)$ under the induced operations, but *no* subring of R. E.g. consider $R := \mathbb{Z} \times \mathbb{Z}$ under the pointwise operations and $P := \mathbb{Z} \times \{0\} \subseteq R$. Then $P \leq_{s} R$ is a sub-semi-ring. But it is no subring, as the unit element $(1,1) \in R$ of R is *not* contained $(1,1) \notin P$ in P. Nevertheless P has a unit-element, namely $(1,0) \in P$ and hence is a ring.
- If $(R, +, \cdot)$ is a *ring*, then property (3) of left-ideals is redundant, it already follows from property (4) by letting b := -1.
- Let $(R, +, \cdot)$ be a semi-ring, then trivially any left-ideal \mathfrak{a} of R already is a sub-semi-ring. Formally put for any subset $\mathfrak{a} \subseteq R$ we get

$$\mathfrak{a} \leq_{\mathrm{m}} R \implies \mathfrak{a} \leq_{\mathrm{s}} R$$

• Consider a commutative semi-ring $(R, +, \cdot)$, then the property (4) of left-ideals already implies property (5) of ideals, due to commutativity. That is in a *commutative* semi-ring R we find the following equivalence for any subset $\mathfrak{a} \subseteq R$

$$\mathfrak{a} \leq_{\mathrm{m}} R \iff \mathfrak{a} \trianglelefteq_{\mathrm{i}} R$$

• Now let $(R, +, \cdot)$ be any ring and let $\mathfrak{a} \leq_{\mathrm{m}} R$ be a left-ideal of R. Then we clearly obtain the following equivalence

$$\mathfrak{a}=R\quad\Longleftrightarrow\quad 1\in\mathfrak{a}$$

PROB " \implies is clear, as $1 \in R$ and if conversely $1 \in \mathfrak{a}$ then due to property (4) we have $a = a1 \in \mathfrak{a}$ for any $a \in R$. Hence $R \subseteq \mathfrak{a} \subseteq R$.

• Consider any semi-ring $(R, +, \cdot)$ and some element $a \in R$. Then we obtain a left-ideal Ra in R (called the **principal ideal** of a), by letting

$$Ra := \{ ba \mid b \in R \} \leq_{\mathrm{m}} R$$

PROB clearly $0 = 0a \in Ra$ and if ba and $ca \in R$, then we see that $ba + ca = (b + c)a \in Ra$ and $-(ba) = (-b)a \in Ra$. Finally we have $c(ba) = (cb)a \in Ra$ for any $c \in R$.

• In a commutative semi-ring $(R, +, \cdot)$ (where $a \in R$ again) we clearly get Ra = aR, where the latter is defined to be

$$aR := \{ab \mid b \in R\} \leq_i R$$

And as R is commutative Ra = aR already is an ideal of R. And it is customary to regard aR instead of Ra in this case. We will later see (cf. section 2.6), that \mathbb{Z} is a PID - that is every ideal of \mathbb{Z} is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$. Formally that is

$$\operatorname{ideal} \mathbb{Z} = \{ a \mathbb{Z} \mid a \in \mathbb{Z} \}$$

• In any semi-ring $(R, +, \cdot)$ we have the *trivial* ideals $\{0\}$ and $R \leq_i R$. If R is a skew-field, then these even are the the only ideals of R.

$$R \text{ skew-field} \implies \text{ subm } R = \{\{0\}, R\}$$

PROB let $\mathfrak{a} \leq_{\mathrm{m}} R$ be any left-ideal of R, if there is some $0 \neq a \in \mathfrak{a}$ then $a^{-1} \in R$ and hence $1 = a^{-1}a \in \mathfrak{a}$. And from this we get $\mathfrak{a} = R$.

• Now consider some non-zero $(R \neq 0)$ commutative ring $(R, +, \cdot)$. Then we even get: R is a field if and only if the only ideals of R are the trivial ones. That is equivalent are

$$R$$
 field \iff ideal $R = \{\{0\}, R\}$

PROB " \implies " has already been shown above, for " \Leftarrow " regard any $0 \neq a \in R$, then $aR \leq_i R$ is an ideal of R. But as $aR \neq \{0\}$ this only leaves aR = R and hence there is some $i \in R$ such that ai = 1, which means $i = a^{-1}$. Altogether R is a field.

• We could have introduced a dual notion of a left-ideal - a so-called *right-ideal*. This is a subset $\mathfrak{a} \subseteq R$ such that the properties (1), (2), (3) and (5) of (left-)ideals hold true. That is we have replaced (4) by (5). However this would lead to a completely analogous theory. Also refer to section 3.1 for a little more comments on this.

(1.30) Lemma: (viz. 250)

For the moment being let \star abbreviate any one of the words *semi-ring*, *ring*, *skew-field* or *field* and let $(R, +, \cdot)$ be a \star . Further consider an arbitrary family (where $i \in I \neq \emptyset$) $P_i \subseteq R$ of sub- \star s of R. Then the intersection P_i is a sub- \star of R again

$$\bigcap_{i \in I} P_i \subseteq R \quad \text{is a sub-} \star$$

Likewise let us abbreviate by \star the word *left-ideal* or the word *ideal*. Now suppose $(R, +, \cdot)$ is a semi-ring and consider an arbitrary family (where $i \in I \neq \emptyset$) $\mathfrak{a}_i \subseteq R$ of \star s of R. Then the intersection of the \mathfrak{a}_i is a \star of R again

$$\bigcap_{i\in I} \mathfrak{a}_i \subseteq R \text{ is a } \star$$

The proof of this lemma is an easy, straightforward verification of the properties of a (sub-)* in all the seperate cases. But though this is most easy it has far-reaching consequences. Whenever we are given a subset $X \subseteq R$ we may consider the smallest \star of R containing X. Just take the intersection over all \star s containing X (this is possible since at least R is a \star with $X \subseteq R$). The following definition formalizes this idea. And it is not much of a surprise, that this smallest \star then can be described explicitly by taking all the elements of X and performing all the operations allowed for a \star .

(1.31) Definition:

Let now $(R, +, \cdot)$ be a semi-ring and consider an arbitrary subset $X \subseteq R$ of R. Then the above lemma allows us to introduce the sub-semi-ring, left-ideal, resp. ideal **generated** by X to be the intersection of all such containing X

$$\langle X \rangle_{\mathrm{s}} := \bigcap \{ P \subseteq R \mid X \subseteq P \leq_{\mathrm{s}} R \} \langle X \rangle_{\mathrm{m}} := \bigcap \{ \mathfrak{a} \subseteq R \mid X \subseteq \mathfrak{a} \leq_{\mathrm{m}} R \} \langle X \rangle_{\mathrm{i}} := \bigcap \{ \mathfrak{a} \subseteq R \mid X \subseteq \mathfrak{a} \leq_{\mathrm{i}} R \}$$

Likewise if R even is a ring (or (skew)field) we may define the subring (or sub-(skew)field respectively) to be the intersection of all such containing X

$$\langle X \rangle_{\mathbf{r}} := \bigcap \{ P \subseteq R \mid X \subseteq P \leq_{\mathbf{r}} R \} \langle X \rangle_{\mathbf{f}} := \bigcap \{ P \subseteq R \mid X \subseteq P \leq_{\mathbf{f}} R \}$$

NOTA in case that there may be any doubt concerning the semi-ring X is contained in (e.g. $X \subseteq R \subseteq S$) we emphasise the semi-ring R used in this construction by writing $\langle X \subseteq R \rangle_i$ or $\langle X \rangle_i \leq_i R$ or even $R \langle X \rangle_i$.

(1.32) Remark:

In case $X = \emptyset$ it is clear that $\{0\}$ is an ideal containing X. And as 0 is contained in any other ideal (even sub-semiring) of R we find

$$\langle \emptyset \rangle_{s} = \langle \emptyset \rangle_{m} = \langle \emptyset \rangle_{i} = \{ 0 \}$$

The case of the subring resp. sub(skew)field generated by \emptyset usually is less trivial however. Let us regard the case $R = \mathbb{Q}$ for example. As any subring has to contain 1 and allow sums and negatives, we find that $\mathbb{Z} = \langle \emptyset \rangle_{\mathrm{r}} \subseteq \mathbb{Q}$. And as a subfield even allows to take inverses we find $\mathbb{Q} = \langle \emptyset \rangle_{\mathrm{f}} \subseteq \mathbb{Q}$. However in \mathbb{C} we also get $\mathbb{Q} = \langle \emptyset \rangle_{\mathrm{f}} \subseteq \mathbb{C}$ only. Hence the intersection of all subrings resp. all sub(skew)fields deserves a special name, it is called the **prime-ring** resp. **prime(skew)field** of R

$$\langle \emptyset \rangle_{\mathbf{r}} = \bigcap \{ P \subseteq R \mid P \leq_{\mathbf{r}} R \} \langle \emptyset \rangle_{\mathbf{f}} = \bigcap \{ P \subseteq R \mid P \leq_{\mathbf{f}} R \}$$

(1.33) Proposition: (viz. 252)

Consider a ring $(R, +, \cdot)$ and a nonempty subset $\emptyset \neq X \subseteq R$. Then we can give an explicit description of the (left)-ideal generated by X

$$\langle X \rangle_{\mathbf{m}} = \left\{ \sum_{i=1}^{n} a_{i} x_{i} \mid 1 \leq n \in \mathbb{N}, x_{i} \in X, a_{i} \in R \right\}$$
$$\langle X \rangle_{\mathbf{i}} = \left\{ \sum_{i=1}^{n} a_{i} x_{i} b_{i} \mid 1 \leq n \in \mathbb{N}, x_{i} \in X, a_{i}, b_{i} \in R \right\}$$

Suppose R is any semi-ring and denote $\pm X := \{x \mid x \in X\} \cup \{-x \mid x \in X\}$ then we can also give an explicit description of the sub-semiring of R generated by X (and if R is a ring also of the subring of R generated by X)

$$\langle X \rangle_{s} = \left\{ \sum_{i=1}^{m} \prod_{j=1}^{n} x_{i,j} \mid 1 \le m, n \in \mathbb{N}, x_{i,j} \in \pm X \right\}$$
$$\langle X \rangle_{r} = \langle X \cup \{1\} \rangle_{s}$$

Finally suppose that R even is a field, referring to the generated subring we can also give an explicit description of the subfield of R generated by X

$$\langle X \rangle_{\mathbf{f}} = \left\{ ab^{-1} \mid a, b \in \langle X \rangle_{\mathbf{r}}, \ b \neq 0 \right\}$$

Ideals have been introduced into the theory of rings, as computations with ordinary elements of rings may have very strange results. Thus instead of looking at $a \in R$ one may turn to $aR \leq_i R$ (in a commutative ring). It turns out that it is possible to define the sum and product of ideals, as well and that this even has nicer properties that the ordinary sum and product of elements. Hence the name - aR is an *ideal* element of R. Nowadays ideals have become an indespensible tool in ring theory, as they turn out to be kernels of ring-homomorphisms.

(1.34) Proposition: (viz. 253)

Consider any semi-ring $(R, +, \cdot)$ and arbitrary ideals $\mathfrak{a}, \mathfrak{b}$ and $\mathfrak{c} \leq_{\mathrm{i}} R$. Then these induce further ideals of R by letting

$$\begin{split} \mathfrak{a} \cap \mathfrak{b} &:= \left\{ \left. a \in R \mid a \in \mathfrak{a} \text{ and } a \in \mathfrak{b} \right\} \\ \mathfrak{a} + \mathfrak{b} &:= \left\{ \left. a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b} \right\} \\ \mathfrak{a} \mathfrak{b} &:= \left\{ \left. \sum_{i=1}^{n} a_{i} b_{i} \right| \right| 1 \le n \in \mathbb{N}, a_{i} \in \mathfrak{a}, b_{i} \in \mathfrak{b} \right\} \end{aligned}$$

Note however that $\mathfrak{a} \cup \mathfrak{b}$ need not be an ideal of R. And thereby we have the following chains of inclusions of ideals of R

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a}+\mathfrak{b}$$

(1.35) **Proposition:** (viz. 254)

Let $(R, +, \cdot)$ be any semi-ring, then the compositions \cap , + and \cdot of ideals are associative, that is if $\mathfrak{a}, \mathfrak{b}$ and $\mathfrak{c} \leq_i R$ are ideals of R, then we get

$$(\mathfrak{a} \cap \mathfrak{b}) \cap \mathfrak{c} = \mathfrak{a} \cap (\mathfrak{b} \cap \mathfrak{c})$$
$$(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$$
$$(\mathfrak{a} \mathfrak{b}) \mathfrak{c} = \mathfrak{a} (\mathfrak{b} \mathfrak{c})$$

Further \cap and + are commutative, and if R is commutative then so is the multiplication \cdot of ideals, formally again (with \mathfrak{a} and $\mathfrak{b} \leq_{i} R$)

$$\begin{array}{rcl} \mathfrak{a} \cap \mathfrak{b} &=& \mathfrak{b} \cap \mathfrak{a} \\ \mathfrak{a} + \mathfrak{b} &=& \mathfrak{b} + \mathfrak{a} \\ \mathfrak{a} \mathfrak{b} &=& \mathfrak{b} \mathfrak{a} \end{array}$$

Recall that the last equality need not hold true, unless R is commutative! The addition + and multiplication \cdot of ideals even satisfies the distributivity laws, that is for any ideals $\mathfrak{a}, \mathfrak{b}$ and $\mathfrak{c} \leq_{i} R$ we get

(1.36) Remark:

It is clear that for any ideal $\mathfrak{a} \leq_i R$ we get $\mathfrak{a} \cap R = \mathfrak{a}$. Thus (ideal R, \cap) is a commutative monoid with neutral element R. Likewise we get $\mathfrak{a} + 0 = \mathfrak{a}$ for any ideal $\mathfrak{a} \leq_i R$ and hence (ideal R, +) is a commutative monoid with neutral element 0. Finally $\mathfrak{a}R = \mathfrak{a} = R\mathfrak{a}$ for any ideal $\mathfrak{a} \leq_i R$ and hence (ideal R, \cdot) is a monoid with neutral element R, as well. And if R is commutative, so is (ideal R, \cdot). In this sense it is understood that $\mathfrak{a}^0 := R$ and $\mathfrak{a}^i := \mathfrak{a} \dots \mathfrak{a}$ (*i*-times) for $1 \leq i \in \mathbb{N}$.

(1.37) Proposition: (viz. 254)

Now consider a ring $(R, +, \cdot)$ and two arbitrary subsets X and $Y \subseteq R$. Let $\mathfrak{a} = \langle X \rangle_i$ and $\mathfrak{b} = \langle Y \rangle_i$ be the ideals generated by these. Then the sum $\mathfrak{a} + \mathfrak{b}$ is generated by the union $X \cup Y$, formally that is

$$\mathfrak{a} + \mathfrak{b} = \langle X \cup Y \rangle_{\mathbf{i}}$$

And if R is commutative, then the product \mathfrak{ab} is generated by the pointwise product $XY := \{xy \mid x \in X, y \in Y\}$ of these sets, formally again

$$\mathfrak{ab} = \langle XY \rangle_{\mathbf{i}}$$

(1.38) Remark: (viz. 255)

(i) Due to (1.37) it oftenly makes sense to regard sums $\mathfrak{a} + \mathfrak{b}$ or products $\mathfrak{a}\mathfrak{b}$ of ideals. And in (1.43) we will also the notion $\mathfrak{b}/\mathfrak{a}$ of a quotient of ideals. Thus one might also be led to think that there should be something like a *difference* of ideals. A good candidate would be the following: consider the ideals $\mathfrak{a} \subseteq \mathfrak{b} \leq_{i} R$ in some semi-ring $(R, +, \cdot)$. Then we might take $\langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{i}$ to be the difference of \mathfrak{b} minus \mathfrak{a} . Yet this yields nothing new, since

$$\mathfrak{a} \subset \mathfrak{b} \quad \Longrightarrow \quad \mathfrak{b} = \langle \mathfrak{b} \setminus \mathfrak{a}
angle_{\mathrm{i}}$$

(ii) Let $(R, +, \cdot)$ be a ring again and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \leq_i R$ be a finite family of ideals of R. Then using (1.37) and induction on n it is clear that

$$\sum_{i=1}^{n} \mathfrak{a}_{i} := \left\{ \left. \sum_{i=1}^{n} a_{i} \right| a_{i} \in \mathfrak{a}_{i} \right\} = \left\langle \bigcup_{i=1}^{n} \mathfrak{a}_{i} \right\rangle_{\mathrm{i}}$$

This property inspires us to define the sum of an arbitrary family $(i \in I)$ of ideals $\mathfrak{a}_i \leq_i R$ of R. As it is not clear what we should substitute for the finite sum of elements we instead define

$$\sum_{i\in I}\mathfrak{a}_i := \langle \bigcup_{i\in I}\mathfrak{a}_i \rangle_{\mathrm{i}}$$

(iii) And thereby it turns out that the *infinite* sum consists of arbitarily large but finite sums over elements of the \mathfrak{a}_i , formally that is

$$\sum_{i \in I} \mathfrak{a}_{i} = \left\{ \sum_{i \in I} a_{i} \mid a_{i} \in \mathfrak{a}_{i}, \# \{ i \in I \mid a_{i} \neq 0 \} < \infty \right\}$$
$$= \left\{ \sum_{i \in \Omega} a_{i} \mid a_{i} \in \mathfrak{a}_{i}, \Omega \subseteq I, \#\Omega < \infty \right\}$$
$$= \left\{ \sum_{k=1}^{n} a_{k} \mid n \in \mathbb{N}, i(k) \in I, a_{k} \in \mathfrak{a}_{i(k)} \right\}$$

(iv) Let now $\mathfrak{b} \leq_{\mathbf{i}} R$ be another ideal of R, then the distributivity rule of (1.35) generalizes to the case of infinite sums, that is

$$\left(\sum_{i\in I}\mathfrak{a}_i\right)\mathfrak{b} = \sum_{i\in I}(\mathfrak{a}_i\mathfrak{b})$$

(1.39) Proposition: (viz. 256)

Let $(R, +, \cdot)$ be a commutative ring and consider the ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{a}_1, \ldots, \mathfrak{a}_k$ and $\mathfrak{b}, \ldots, \mathfrak{b}_k \leq_i R$ of R (where $1 \leq k \in \mathbb{N}$). Then we obtain the statements

- (i) \mathfrak{a} and \mathfrak{b} are said to be **coprime** iff they satisfy one of the following three equivalent conditions
 - (a) $\mathfrak{a} + \mathfrak{b} = R$
 - (b) $(1 + \mathfrak{a}) \cap \mathfrak{b} \neq \emptyset$
 - (c) $\exists a \in \mathfrak{a}, \exists b \in \mathfrak{b}$ such that a + b = 1
- (ii) Suppose that \mathfrak{a} and \mathfrak{b} are coprime and consider any $i, j \in \mathbb{N}$, then the powers \mathfrak{a}^i and \mathfrak{b}^j are coprime as well, formally that is

$$\mathfrak{a} + \mathfrak{b} = R \implies \mathfrak{a}^i + \mathfrak{b}^j = R$$

(iii) Suppose that \mathfrak{a} and \mathfrak{b}_i (for any $i \in 1...k$) are coprime, then \mathfrak{a} and $\mathfrak{b}_1...\mathfrak{b}_k$ are coprime as well, formally this is

$$\left(\forall i \in 1 \dots k : \mathfrak{a} + \mathfrak{b}_i = R\right) \implies \mathfrak{a} + (\mathfrak{b}_1 \dots \mathfrak{b}_k) = R$$

(iv) Suppose that the \mathfrak{a}_i are pairwise coprime, then the product of the \mathfrak{a}_i equals their intersection, formally that is

$$\left(\forall i \neq j \in 1 \dots k : \mathfrak{a}_i + \mathfrak{a}_j = R\right) \implies \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_k = \mathfrak{a}_1 \dots \mathfrak{a}_k$$

(1.40) Definition: (viz. 257)

Let $(R, +, \cdot)$ be any semi-ring and $\mathfrak{a} \leq_{\mathrm{m}} R$ be a left-ideal of R, then \mathfrak{a} induces an equivalence relation \sim on R by virtue of

$$a \sim b \quad :\iff \quad a - b \in \mathfrak{q}$$

where $a, b \in R$. And the equivalence classes under this relation are called **cosets** of \mathfrak{a} , and for any $b \in R$ this is given to be

$$b + \mathfrak{a} := [b] = \{b + a \mid a \in \mathfrak{a}\}$$

Finally we denote the quotient set of R modulo \mathfrak{a} (meaning the relation \sim)

$$R/\mathfrak{a} := R/\mathfrak{a} = \{a + \mathfrak{a} \mid a \in R\}$$

If $\mathfrak{a} \leq_i R$ even is an ideal (e.g. when R is commutative) then R/\mathfrak{a} can even be turned into a semi-ring $(R/\mathfrak{a}, +, \cdot)$ again under the following operations

$$\begin{array}{rcl} (a+\mathfrak{a})+(b+\mathfrak{a}) &:= & (a+b)+\mathfrak{a} \\ (a+\mathfrak{a})\cdot(b+\mathfrak{a}) &:= & (a\cdot b)+\mathfrak{a} \end{array}$$

Thereby $(R/\mathfrak{a}, +, \cdot)$ is also called the **quotient ring** or **residue ring** of R modulo \mathfrak{a} . Clearly, if R is commutative, then so is R/\mathfrak{a} . And if R is a ring, so is R/\mathfrak{a} , where the unit element is given to be the coset $1 + \mathfrak{a}$.

(1.41) Remark:

It is common that beginners in the field of algebra encounter problems with this notion. But on the other hand the construction of taking to the quotient ring is one of the two most important tools of algebra (the other being localizing). Hence we would like to append a few remarks:

We have defined R/\mathfrak{a} to be the quotient set of R under the equivalence relation $a - b \in \mathfrak{a}$. And the equivalence classes have been the cosets $b + \mathfrak{a}$. Hence two cosets are equal if and only if their representants are equivalent and formally for any $a, b \in R$ this is

$$a + \mathfrak{a} = b + \mathfrak{a} \iff a - b \in \mathfrak{a}$$

And if $\mathfrak{a} \leq_i R$ is an ideal of R we even were able to turn this quotient set R/\mathfrak{a} into a ring again, under the operations above. Now don't be confused, we sometimes also employ the pointwise sum $A + B := \{a + b \mid a \in A, b \in B\}$ and product $A \cdot B := \{ab \mid a \in A, b \in B\}$ of two subsets $A, B \subseteq R$. But this a completely different story - the operations on cosets $b + \mathfrak{a}$ have been *defined* by referring to the representants b.

(1.42) Remark:

Intuitively speaking the residue ring R/\mathfrak{a} is the ring R where all the information contained in \mathfrak{a} has been erased. Thus R/\mathfrak{a} only retains the information that has been stored in R but not in \mathfrak{a} . Hence it is no wonder that R/\mathfrak{a} is "smaller" than $R(|R/\mathfrak{a}| \leq |R|)$ to be precise). However R/\mathfrak{a} is not a subring of R! Let us study some special cases to enlighten things:

- In the case $\mathfrak{a} = R$ the residue ring R/R contains precisely one element, namely 0 + R. Hence $R/R = \{0 + R\}$ is the zero-ring. This matches the intuition all information has been forgotten, what remains carries the trivial structure only.
- The other extreme case is $\mathfrak{a} = \{0\}$. In this case \mathfrak{a} induces the trivial relation $a \sim b \iff a = b$. Hence the residue class of a is just $a + \{0\} = \{a\}$. Therefore we have a natural identification

$$R \longleftrightarrow \frac{R}{\{0\}} : a \mapsto \{a\}$$

Again this matches the intuition: $\{0\}$ contains no information hence $R/\{0\}$ retains all the information of R. In fact we have just rewritten any $a \in R$ as $\{a\} \in R/\{0\}$.

• Now consider any commutative ring $(R, +, \cdot)$ and build the polynomial ring R[t] upon it. Then the ideal $\mathfrak{a} = tR[t]$ allows us to regain R from R[t]. Formally there is a natural identification

$$R \longleftrightarrow \frac{R[t]}{tR[t]} : a \mapsto at^0 + tR[t]$$

Hence one should think that tR[t] contains the information we have added by going to the polynomial ring R[t]. Forgetting it we return to R. Further it is nice to note that the same is true for the formal power series R[t] instead of R[t]. The same amount of information that has been added is lost.

PROB it is clear that $R \to R[t] : a \mapsto at^0$ is injective and for $a \neq b \in R$ we even get $at^0 - bt^0 = (a - b)t^0 \notin tR[t]$. This means that even $a \mapsto at^0 + tR[t]$ is injective. And if we are given an arbitrary polynomial $f = a_n t^n + \cdots + a_1 t + a_0 t^0$ then $f + tR[t] = a_0 t^0 + tR[t]$ which also is the surjectivity. Note that this all is immediate from the first isomorphism theorem: $R[t] \to R : f \mapsto f[0]$ has kernel tR[t] and image R.

• Likewise we obtain a natural identification (that is an isomorphism) between the ring \mathbb{Z}_n and the residue ring $\mathbb{Z}/n\mathbb{Z}$ via

$$\mathbb{Z}_n \longleftrightarrow \mathbb{Z}/_{n\mathbb{Z}} : k \mapsto k + n\mathbb{Z}$$

This example teaches that the properties of the residue ring (here $\mathbb{Z}/n\mathbb{Z}$) may well differ from those of the ring (here \mathbb{Z}). E.g. \mathbb{Z} is an integral domain, whereas $\mathbb{Z}/4\mathbb{Z}$ is not $((2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 0 + 4\mathbb{Z})$. On the other hand $\mathbb{Z}/2\mathbb{Z}$ is a field, whereas \mathbb{Z} is not.

PROB we will prove that the above correspondence truly is bijective: suppose $0 \le k < l < n$ then $l - k \in n\mathbb{Z}$ would mean $n \mid l - k$, but as l - k < l < n this can only be if k = l. This proves the injectivity, for the surjectivity we are given $a \in \mathbb{Z}$ arbitarily. Then we write a = k + hn for some $0 \le k < n$ and $h \in \mathbb{Z}$, then $k + n\mathbb{Z} = a + n\mathbb{Z}$.

(1.43) Lemma: (viz. 259) Correspondence Theorem

Consider any semi-ring $(R, +, \cdot)$ and an ideal $\mathfrak{a} \leq_{i} R$, then we obtain a 1-to-1 correspondence between the ideals of the residue ring R/\mathfrak{a} and the ideals of R containing \mathfrak{a} by virtue of (where $\mathfrak{b}/\mathfrak{a} := \{b + \mathfrak{a} \mid b \in \mathfrak{b}\})$

$$\begin{array}{rcl} \operatorname{ideal} {R / \mathfrak{a}} & \longleftrightarrow & \left\{ \mathfrak{b} \trianglelefteq_{i} R \mid \mathfrak{a} \subseteq \mathfrak{b} \right\} \\ \mathfrak{u} & \mapsto & \left\{ b \in R \mid b + \mathfrak{a} \in \mathfrak{u} \right\} \\ \mathfrak{b / \mathfrak{a}} & \longleftrightarrow & \mathfrak{b} \end{array}$$

And this correspondence even is compatible with intersections, sums and products. That is if consider any two ideals \mathfrak{b} and $\mathfrak{c} \leq_i R$ with $\mathfrak{a} \subseteq \mathfrak{b} \cap \mathfrak{c}$

$${}^{\mathfrak{b}}/\mathfrak{a} \cap {}^{\mathfrak{c}}/\mathfrak{a} = {}^{\mathfrak{b}} \cap {}^{\mathfrak{c}}/\mathfrak{a}$$
$${}^{\mathfrak{b}}/\mathfrak{a} + {}^{\mathfrak{c}}/\mathfrak{a} = {}^{\mathfrak{b}} + {}^{\mathfrak{c}}/\mathfrak{a}$$
$${}^{\mathfrak{b}}/\mathfrak{a} {}^{\mathfrak{c}}/\mathfrak{a} = {}^{\mathfrak{b}} {}^{\mathfrak{c}}/\mathfrak{a}$$

Finally the correspondence also is compatible with the generation of ideals. That is consider an arbitrary subset $X \subseteq R$ and denote its set of residue classes by $X/\mathfrak{a} := \{ x + \mathfrak{a} \mid x \in X \}$. Then we obtain the identity

$$\langle X \rangle_{\mathbf{i}} + \mathfrak{a}/_{\mathfrak{a}} = \langle X/_{\mathfrak{a}} \rangle_{\mathbf{i}}$$

(1.44) Remark:

Let $(R, +, \cdot)$ be a semi-ring and $\mathfrak{a}, \mathfrak{b} \leq_{i} R$ be two ideals, such that $\mathfrak{a} \subseteq \mathfrak{b}$. As above let us denote the ideal of R/\mathfrak{a} induced by \mathfrak{b} by

$$\mathfrak{b}/\mathfrak{a} := \{ b + \mathfrak{a} \mid b \in \mathfrak{b} \} \ \leq_{\mathrm{i}} \ R/\mathfrak{a}$$

Then it is easy to see that for any $x \in R$ we even get the following equivalence

$$x \in \mathfrak{b} \quad \Longleftrightarrow \quad x + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$$

PROB if $x \in \mathfrak{b}$ then $x + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ by definition. And if conversely $x + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ then there is some $b \in \mathfrak{b}$ such that $x + \mathfrak{a} = b + \mathfrak{a}$. That is $x - b \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $x + \mathfrak{b} = b + \mathfrak{b} = 0 + \mathfrak{b}$ again. But the latter already means $x \in \mathfrak{b}$.

(1.45) Remark:

We will soon introduce the notion of a homomorphism, an example of such a thing is the following map that sends $b \in R$ to its equivalence class $b + \mathfrak{a}$

$$\varrho : R \twoheadrightarrow R /_{\mathfrak{a}} : b \mapsto b + \mathfrak{a}$$

It is clear that this mapping is surjective. And it also is clear that for any ideal $\mathfrak{b} \leq_{i} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$ the image of \mathfrak{b} under ϱ is given to be

$$\varrho(\mathfrak{b}) = \left\{ b + \mathfrak{a} \mid b \in \mathfrak{b} \right\} = \left. \frac{\mathfrak{b}}{\mathfrak{a}} \right\}$$

Hence the above correspondence of ideals is just given by ρ acting on ideals (i.e. on certain subsets of R). That is $\mathfrak{b} \mapsto \rho(\mathfrak{b})$ and $\mathfrak{u} \mapsto \rho^{-1}(\mathfrak{u})$.

(1.46) Remark: (\diamondsuit)

Let now $(R, +, \cdot)$ be a commutative ring, then the above correspondence of ideals interlocks maximal ideals, prime ideals and radical ideals:

$$\begin{array}{cccc} \operatorname{ideal} R / \mathfrak{a} & \longleftrightarrow & \left\{ \mathfrak{b} \in \operatorname{ideal} R \mid \mathfrak{a} \subseteq \mathfrak{b} \right\} \\ \cup & \cup \\ \operatorname{srad} R / \mathfrak{a} & \longleftrightarrow & \left\{ \mathfrak{b} \in \operatorname{srad} R \mid \mathfrak{a} \subseteq \mathfrak{b} \right\} \\ \cup & \cup \\ \operatorname{spec} R / \mathfrak{a} & \longleftrightarrow & \left\{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \right\} \\ \cup & \cup \\ \operatorname{smax} R / \mathfrak{a} & \longleftrightarrow & \left\{ \mathfrak{m} \in \operatorname{smax} R \mid \mathfrak{a} \subseteq \mathfrak{m} \right\} \end{array}$$

That is the ideal $\mathfrak{b} \leq_{i} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$ is radical if and only if the corresponding ideal $\mathfrak{b}/\mathfrak{a} \leq_{i} R/\mathfrak{a}$ is radical, too. Likewise $\mathfrak{a} \subseteq \mathfrak{b} \leq_{i} R$ is prime (maximal) iff $\mathfrak{b}/\mathfrak{a} \leq_{i} R/\mathfrak{a}$ is prime (maximal). In fact we even have the following equality of radical ideals for any $\mathfrak{b} \leq_{i} R$ with $\mathfrak{a} \subseteq \mathfrak{b}$

$$\sqrt{\mathfrak{b}/\mathfrak{a}} = \sqrt{\mathfrak{b}}/\mathfrak{a}$$

(1.47) Example: (\diamondsuit)

Consider the ring $(\mathbb{Z}, +, \cdot)$, as \mathbb{Z} is an Euclidean domain all its ideals are of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$ (confer to section 2.6 for a proof). We now fix some ideal $\mathfrak{a} := a\mathbb{Z}$, then $a\mathbb{Z} \subseteq b\mathbb{Z}$ is equivalent, to the fact that b divides a (see section 2.5 for details). Hence by the correspondence theorem the ideals of $\mathbb{Z}_a = \mathbb{Z}/a\mathbb{Z}$ are precisely given to be

$$\operatorname{ideal}^{\mathbb{Z}} /_{a\mathbb{Z}} = \left\{ \begin{array}{c} b\mathbb{Z} /_{a\mathbb{Z}} \\ b \mid a \end{array} \right\}$$

1.6 Homomorphisms

(1.48) Definition:

Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be arbitrary semi-rings, a mapping $\varphi : R \to S$ is said to be a **homomorphism of semi-rings** (or shortly *semi-ring-homomorphism*) iff for any $a, b \in R$ it satisfies the following two properties

- (1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
- (2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

And if R and S even are rings having the unit elements 1_R and 1_S respectively, then φ is said to be a **homomorphism of rings** (or shortly ring-homomorphism iff for any $a, b \in R$ it even satisfies the properties

- (1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
- (2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$$(3) \varphi(1_R) = 1_S$$

And we denote the set of all semi-ring-homomorphisms respectively of all ring-homomorphisms from R to S (that is a subset of $\mathcal{F}(R, S)$) by

shom
$$(R, S) := \{ \varphi : R \to S \mid (1) \text{ and } (2) \}$$

rhom $(R, S) := \{ \varphi : R \to S \mid (1), (2) \text{ and } (3) \}$

And if $\varphi : R \to S$ is a homomorphism of semi-rings, then we define its **image** im $\varphi \subseteq S$ and **kernel** kn $\varphi \subseteq R$ to be the following subsets

$$\begin{split} &\operatorname{im}\left(\varphi\right) \; := \; \varphi(R) \; = \; \left\{ \left. \varphi(a) \right| a \in R \right\} \\ &\operatorname{kn}\left(\varphi\right) \; := \; \varphi^{-1}(0_S) \; = \; \left\{ \left. a \in R \right| \varphi(a) = 0 \right\} \end{split}$$

(1.49) Remark:

In the literature it is customary to only write hom(R, S) instead of what we denoted by shom(R, S) or rhom(R, S). And precisely which of these two sets is meant is determined by the context only, not by the notation. In this book we try to increase clarity by adding the letter "s" or "r". From a systematical point of view it might be appealing to write $hom_s(R, S)$ for shom(R, S) (and likewise $hom_r(R, S)$ for rhom(R, S)), as we have already used these indices with substructures. Yet we will require the position of the index later on (when it comes to modules and algebras). Hence we chose to place precisely this index in front of "hom" instead.

(1.50) Example:

• The easiest example of a homomorphism of semi-rings is the so-called *zero-homomorphism* which we denote by 0 and which is given to be

$$0 : R \to S : a \mapsto 0_S$$

• Let $(S, +, \cdot)$ be any semi-ring and $R \leq_{s} S$ be a sub-semi-ring of S. Then the inclusion $R \subseteq S$ gives rise the the *inclusion homomorphism*

$$\iota \; : \; R \, \hookrightarrow \, S \; : \; a \mapsto a$$

Clearly this is a homomorphism of semi-rings. And if S even is a ring and $R \leq_{\rm r} S$ is a subring of S, then ι is a homomorphism of rings. In the special case R = S we call $1 := \iota$ the *identity map* of R.

• Now let $(R, +, \cdot)$ be any (semi-)ring and consider some ideal $\mathfrak{a} \leq_{i} R$. Then we have already introduced the quotient (semi-)ring R/\mathfrak{a} in (??). And this gives rise to the following homomorphism of (semi-) rings (which is called *canonical epimorphism*)

$$\varrho : R \twoheadrightarrow R /_{\mathfrak{a}} : b \mapsto b + \mathfrak{a}$$

Note that the definition of the addition and multiplication on R/\mathfrak{a} are precisely the properties of ϱ being a homomorphism. And also by definition the kernel of this map precisely is $\operatorname{kn}(\varrho) = \mathfrak{a}$. Of course ϱ is surjective and hence its image is the entire ring $\operatorname{im}(\varrho) = R/\mathfrak{a}$.

• Consider any (semi-)ring $(R, +, \cdot)$ again and let $\mathfrak{a}, \mathfrak{b} \leq_i R$ be two ideals of R such that $\mathfrak{a} \subseteq \mathfrak{b}$. Then we obtain a well-defined, surjective homomorphism of (semi-)rings by (further note that the kernel of this map is given to be the quotient ideal $\mathfrak{b}/\mathfrak{a}$)

$$R/\mathfrak{a} \twoheadrightarrow R/\mathfrak{b} : a + \mathfrak{a} \mapsto a + \mathfrak{b}$$

PROB if $a + \mathfrak{a} = b + \mathfrak{a}$ then $a - b \in \mathfrak{a} \subseteq \mathfrak{b}$ whence we get $a + \mathfrak{b} = b + \mathfrak{b}$ again. This already is the well-definedness and the surjectivity and homorphism properties are clear. Further $b + \mathfrak{b} = 0 + \mathfrak{b}$ iff $b \in \mathfrak{a}$ which again is equivalent, to $b + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$. And this also is kn $(\bullet) = \mathfrak{b}/\mathfrak{a}$.

• Finally we would like to present an example of a homomorphism π of semi-rings, that is *no* homomorphism of rings. The easiest way to achieve this is by regarding the ring $R = \mathbb{Z}^2$. Then we may take

$$\pi : \mathbb{Z}^2 \to \mathbb{Z}^2 : (a,b) \mapsto (a,0)$$

(1.51) **Proposition:** (viz. 265)

(i) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be semi-rings and $\varphi : R \to S$ be a homomorphism of semi-rings again. Then φ already satisfies (for any $a \in R$)

$$\varphi(0_R) = 0_S$$

 $\varphi(-a) = -\varphi(a)$

(ii) And if $(R, +, \cdot)$ and $(S, +, \cdot)$ are rings, $u \in R^*$ is an invertible element of R and $\varphi : R \to S$ is a homomorphism of rings, then $\varphi(u) \in S^*$ is an invertible element of S, too with inverse

$$\varphi(u^{-1}) = \varphi(u)^{-1}$$

(iii) Let $(R, +, \cdot)$, $(S, +, \cdot)$ and $(T, +, \cdot)$ be (semi-)rings, $\varphi : R \to S$ and $\psi : S \to T$ be homomorphisms of (semi-)rings. Then the composition ψ after φ is a homomorphism of (semi-)rings again

$$\psi \varphi : R \to S : a \mapsto \psi(\varphi(a))$$

- (iv) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be (semi-)rings and $\Phi : R \to S$ be a bijective homomorphism of (semi-)rings. Then the inverse map $\Phi^{-1} : S \to R$ is a homomorphism of (semi-)rings, too.
- (v) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be (semi-)rings and $\varphi : R \to S$ be a homomorphism of (semi-)rings, then the image of φ is a sub-(semi-)ring of S and its kernel is an ideal of R

$$\lim \left(\varphi\right) \leq_{\mathrm{s}} S \\ \operatorname{kn}\left(\varphi\right) \leq_{\mathrm{i}} R$$

(vi) More generally let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two (semi-)rings containing the sub-(semi-)rings $P \leq_{\rm s} R$ and $Q \leq_{\rm s} S$ respectively. If now $\varphi: R \to S$ is a homomorphism of (semi-)rings, then $\varphi(P)$ and $\varphi^{-1}(Q)$ are sub-(semi-)rings again

$$\begin{array}{ll} \varphi(P) & \leq_{\mathrm{s}} & S \\ \varphi^{-1}(Q) & \leq_{\mathrm{s}} & R \end{array}$$

(vii) Analogously let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two semi-rings containing the (left-)ideals $\mathfrak{a} \leq_{\mathrm{m}} R$ and $\mathfrak{b} \leq_{\mathrm{m}} S$ respectively. If now $\varphi : R \to S$ is a homomorphism of semi-rings then $\varphi^{-1}(\mathfrak{b})$ is a (left-)ideal of R again. And if φ even is surjective, then $\varphi(\mathfrak{a})$ is a (left-)ideal of R

$$\varphi^{-1}(\mathfrak{b}) \leq_{\mathrm{m}} R$$

 $\varphi \text{ surjective } \Longrightarrow \varphi(\mathfrak{a}) \leq_{\mathrm{m}} R$

(viii) Let $(R, +, \cdot)$ be a ring again and $(S, +, \cdot)$ even be a skew field. Then any non-zero homomorphism of semi-rings from R to S already is a homomorphism of rings (i.e. satisfies property (3)). Formally

S skew-field \implies shom $(R, S) = \text{rhom}(R, S) \cup \{0\}$

(ix) Now let $(R, +, \cdot)$ be a skew-field and $(S, +, \cdot)$ be an arbitrary semi-ring, then any nonzero homomorphism $\varphi : R \to S$ of semi-rings is injective

R skew-field $\implies \varphi$ injective or $\varphi = 0$

(1.52) Definition:

Consider any two (semi-)rings $(R, +, \cdot)$ and $(S, +, \cdot)$ and a homomorphism φ : $R \to S$ of (semi-)rings. Then φ is said to be a **mono-**, **epi-** or **isomorphism** of (semi-)rings, iff it is injective, surjective or bijective respectively. And a homomorphism of the form $\varphi : R \to R$ is said to be an **endomorphism** of R. And φ is said to be an **automorphism** of R iff it is a bijective endomorphism of R. Altogether we have defined the notions

φ is called	iff φ is
$\operatorname{monomorphism}$	injective
epimorphism	surjective
isomorphism	bijective
endomorphism	R = S
automorphism	R = S and bijective

And if $(R, +, \cdot)$ is any ring, then we denote the set of all ring automorphisms on R by (note that this is a group under the composition of mappings)

 $\operatorname{raut}(R) := \{ \Phi : R \to R \mid \Phi \text{ bijective homomorphism of rings} \}$

In the case that $\Phi: R \to S$ is an isomorphism of semi-rings we will abbreviate this by writing $\Phi: R \cong_{s} S$. And if $\Phi: R \to S$ even is an isomorphism of rings we write $\Phi: R \cong_{r} S$. And thereby R and S are said to be **isomorphic** if there is an isomorphism Φ between them. And in this case we wite

$$\begin{array}{rcl} R \cong_{\mathrm{s}} S & :\Longleftrightarrow & \exists \, \Phi \, : \, \Phi : R \cong_{\mathrm{s}} S \\ R \cong_{\mathrm{r}} S & :\Longleftrightarrow & \exists \, \Phi \, : \, \Phi : R \cong_{\mathrm{r}} S \end{array}$$

(1.53) Proposition: (viz. 267)

(i) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be semi-rings and $\varphi : R \to S$ be a homomorphism of semi-rings. Then φ is injective, resp. surjective iff

$$\varphi \text{ injective } \iff \operatorname{kn}(\varphi) = \{0\}$$

$$\varphi \text{ surjective } \iff \operatorname{in}(\varphi) = S$$

- (ii) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be (semi-)rings and $\Phi : R \to S$ be a homomorphism of (semi-)rings, then the following statements are equivalent (and in this case we already get $\alpha = \beta = \Psi = \Phi^{-1}$)
 - (a) Φ is bijective
 - (b) there is some homomorphism $\Psi : S \to R$ of (semi-)rings such that $\Psi \Phi = \mathbb{1}_R$ and $\Phi \Psi = \mathbb{1}_S$
 - (c) there are homomorphisms $\alpha : S \to R$ and $\beta : S \to R$ of (semi-) rings such that $\alpha \Phi = \mathbb{1}_R$ and $\Phi \beta = \mathbb{1}_S$
- (iii) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two semi-rings and $\Phi : R \cong_{s} S$ be an isomorphism between them. Then R is a ring if and only if S is a ring. And in this case $\Phi : R \cong_{r} S$ already is an isomorphism of rings.
- (iv) The relation $\cong_{\rm r}$ has the properties of an equivalence relation on the class of all rings (and the same is true for $\cong_{\rm s}$ on the class of all semirings). To be precise, for all rings $(R, +, \cdot)$, $(S, +, \cdot)$ and $(T, +, \cdot)$ we obtain the following statements

$$\begin{split} \mathbbm{1}_R : R \ \cong_{\mathrm{r}} R \\ \Phi : R \ \cong_{\mathrm{r}} S \ \Longrightarrow \ \Phi^{-1} : S \ \cong_{\mathrm{r}} R \\ \Phi : R \ \cong_{\mathrm{r}} S \ \text{and} \ \Psi : S \ \cong_{\mathrm{r}} T \ \Longrightarrow \ \Psi \Phi : R \ \cong_{\mathrm{r}} T \end{split}$$

(1.54) Remark:

Intuitively speaking two (semi-)rings $(R, +, \cdot)$ and $(S, +, \cdot)$ are isomorphic if and only if they carry precisely the same structure. A bit lax that is the elements may differ by the names they are given but nothing more. Therefore any algebraic property satisfied by R also holds true for S and vice versa. We give a few examples of this fact below, but this is really true for *any* algebraic property. Thus from an algebraic point of view, isomorphic (semi-)rings are just two copies the same thing (just like two 1 Euro coins). And the difference between equality and isomorphy is just a settheoretical one. We verify this intuitive view by presenting a few examples - let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two semi-rings that are isomorphic under $\Phi : R \cong_{s} S$. Then we get

- In the above proposition we have already shown R is a ring if and only if S is a ring. And in this case already Φ is an isomorphism of rings.
- *R* is commutative if and only if *S* is commutative. PROB suppose that *R* is commutative and consider any two elements $x, y \in S$. Then let $a := \Phi^{-1}(x)$ and $b := \Phi^{-1}(y) \in R$ and compute $xy = \Phi(a)\Phi(b) = \Phi(ab) = \Phi(ba) = \Phi(b)\Phi(a) = yx$. Hence *S* is commutative, too. And the converse implication follows with Φ instead of Φ^{-1} .

- *R* is an integral domain if and only if *S* is an integral domain. PROB suppose that *S* is an integral domain and consider any two elements $a, b \in R$. If we had ab = 0 then $0 = \Phi(0) = \Phi(ab) = \Phi(a)\Phi(b)$. But as *S* is an integral domain this means $\Phi(a) = 0$ or $\Phi(b) = 0$. And as Φ is injective this implies a = 0 or b = 0. Hence *R* is an integral domain, too. And the converse implication follows with Φ^{-1} instead of Φ .
- R is a skew-field if and only if S is a skew-field. In fact for any two rings R and S we even get the stronger correspondence

$$\Phi(R^*) = S^*$$

PROB if $a \in R^*$ is a unit of R then $\Phi(a^{-1}) = \Phi(a)^{-1}$ and hence $\Phi(a) \in S^*$ is a unit, too. And if conversely $x \in S^*$ is a unit of S, then let $a := \Phi^{-1}(x)$ and $b := \Phi^{-1}(x^{-1})$. Thereby $ab = \Phi^{-1}(x)\Phi^{-1}(x^{-1}) = \Phi^{-1}(xx^{-1}) = \Phi(1_S) = 1_R$ and likewise $ba = 1_R$. Hence we have $a^{-1} = b$ such that $a \in R^*$ and $x \in \Phi(R^*)$ is the image of a unit of R.

(1.55) Remark: (\diamondsuit)

In book 2 we will introduce the notion of a category (in our case this would be the collection of all semi-rings or of all rings respectively). And in any category there is the notion of *monomorphisms*, *epimorphisms* and *isomorphisms*. That is let $(R, +, \cdot)$ and $(S, +, \cdot)$ be two (semi-)rings. Then $\varphi: R \to S$ will be called a **monomorphism** in the category of (semi-)rings, iff it is a homorphism of (semi-)rings, such that for any (semi-)ring $(Q, +, \cdot)$ and any two homomorphisms $\alpha, \beta: Q \to R$ of (semi-)rings we would have the implication

$$\varphi \alpha = \varphi \beta \implies \alpha = \beta$$

Likewise $\varphi : R \to S$ will be called a **epimorphism** in the category of (semi-)rings, iff it is a homorphism of (semi-)rings, such that for any (semi-)ring $(T, +, \cdot)$ and any two homomorphisms $\alpha, \beta : S \to T$ of (semi-)rings we would have the implication

$$\alpha \varphi = \beta \varphi \implies \alpha = \beta$$

Finally $\Phi: R \to S$ is said to be an **isomorphism** in the category of (semi-) rings, iff it is a homomorphism of (semi-)rings and there is another homomorphism $\Psi: S \to R$ of (semi-)rings that is inverse to Φ , formally

$$\exists \Psi: S \to R : \Psi \Phi = \mathbb{1}_R \text{ and } \Phi \Psi = \mathbb{1}_S$$

It is immediately clear that an injective homomorphism of (semi-)rings thereby is a monomorphism in the categorial sense. And likewise a surjective homomorphism of (semi-rings) is an epimorphism in the categorial sense. The converse implications need not be true however. Yet we will see in the subsequent proposition that the two notions of isomorphy are equivalent.

(1.56) Theorem: (viz. 267) Isomorphism Theorems

(i) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two rings, $\mathfrak{a} \leq_i R$ be an ideal of R and $\varphi : R \to S$ be a homomorphism of rings. If now $\mathfrak{a} \subseteq \operatorname{kn}(\varphi)$ then we obtain a well-defined homomorphism of rings by virtue of

$$\widetilde{\varphi} : R/_{\mathfrak{a}} \to S : b + \mathfrak{a} \mapsto \varphi(a)$$

Note if R and S are semi-rings and φ is a homomorphism of such, then $\tilde{\varphi}$ still is a well-defined homomorphism of semi-rings.

(ii) First Isomorphism Theorem

Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two rings and $\varphi : R \to S$ be a homomorphism of rings. Then the kernel of φ is an ideal kn $(\varphi) \leq_{\mathrm{i}} R$ of R and the its image im $(\varphi) \leq_{\mathrm{r}} S$ is a subring of S. And finally we obtain the following isomorphy of rings

$$\frac{R}{\ln (\varphi)} \cong_{\mathbf{r}} \operatorname{im}(\varphi) : a + \ln (\varphi) \mapsto \varphi(a)$$

Note if R and S are semi-rings and φ is a homomorphism of such, then we still get kn $(\varphi) \leq_{i} R$, im $(\varphi) \leq_{s} S$ and $R/\mathfrak{a} \cong_{s} \operatorname{im}(\varphi)$.

(iii) Second Isomorphism Theorem

Let $(S, +, \cdot)$ be a ring, $R \leq_{\mathbf{r}} S$ be a subring of S and $\mathfrak{b} \leq_{\mathbf{i}} S$ be an ideal of S. Then $\mathfrak{b} \cap R \leq_{\mathbf{i}} R$ is an ideal of R, the set $\mathfrak{b} + R :=$ $\{b+a \mid b \in \mathfrak{b}, a \in R\} \leq_{\mathbf{r}} S$ is a subring of S and $\mathfrak{b} \leq_{\mathbf{i}} \mathfrak{b} + R$ is an ideal of $\mathfrak{b} + R$. And thereby we obtain the following isomorphy of rings

$$R/\mathfrak{b}\cap R \cong_{\mathrm{r}} \mathfrak{b}+R/\mathfrak{b} : a+\mathfrak{b}\cap R\mapsto a+\mathfrak{b}$$

Note if S is a semi-ring and $R \leq_{s} S$ is a sub-semi-ring of S, then still $\mathfrak{b}+R \leq_{s} S, \mathfrak{b} \leq_{i} \mathfrak{b}+R$ and we retain the isomorphy $R/\mathfrak{b}\cap R \cong_{s} \mathfrak{b}+R/\mathfrak{b}$.

(iv) Third Isomorphism Theorem

Let $(R, +, \cdot)$ be any ring containing the ideals $\mathfrak{a} \subseteq \mathfrak{b} \leq_{i} R$, then $\mathfrak{b}/\mathfrak{a} := \{ b + \mathfrak{a} \mid b \in \mathfrak{b} \} \leq_{i} R/\mathfrak{a}$ is an ideal of the quotient ring R/\mathfrak{a} and we obtain the following isomorphy of rings

$$R/\mathfrak{a}_{\mathfrak{f}} \cong_{\mathrm{r}} R/\mathfrak{b} : (a+\mathfrak{a}) + \mathfrak{b}/\mathfrak{a} \mapsto a + \mathfrak{b}$$

Note if R is a semi-ring then everythis remains the same, except that the above isomorphy is an isomorphy of semi-rings (and not of rings).

1.7 Products

(1.57) Definition:

Let $\emptyset \neq I$ be an arbitrary set and for any $i \in I$ let $(R, +, \cdot)$ be a semi-ring. Then we define the (exterior) **direct product** of the R_i to be just the carthesian product of the sets R_i

$$\prod_{i \in I} R_i := \left\{ a : I \to \bigcup_{i \in I} R_i \ \middle| \ \forall i \in I : a(i) \in R_i \right\}$$

Let us abbreviate this set by ΠR for a moment. Then we may turn this set into a semi-ring $(\Pi R, +, \cdot)$ by defining the following addition + and multiplication \cdot for elements a and $b \in \Pi R$

$$a+b : I \to \bigcup_{i \in I} R_i : i \mapsto a(i) + b(i)$$
$$a \cdot b : I \to \bigcup_{i \in I} R_i : i \mapsto a(i) \cdot b(i)$$

Note that thereby the addition a(i) + b(i) and multiplication a(i)b(i) are those of R_i . Further note that it is customary to write (a_i) instead of $a \in \Pi R$, where the $a_i \in R_i$ are given to be $a_i := a(i)$. And using this notation the above definitions of + and \cdot in ΠR take the more elegant form

$$(a_i) + (b_i) := (a_i + b_i)$$

 $(a_i) \cdot (b_i) := (a_i \cdot b_i)$

For any $i \in I$ let us now denote the zero-element of the semi-ring R_i by 0_i . Then we define the (exterior) **direct sum** of the R_i to be the subset of those $a = (a_i) \in \Pi R$ for which only finitely many a_i are non-zero. Formally

$$\bigoplus_{i \in I} R_i := \left\{ a \in \prod_{i \in I} R_i \mid \#\{i \in I \mid a(i) \neq 0_i\} < \infty \right\}$$

Let us denote this set by ΣR for the moment, then $\Sigma R \leq_{s} \Pi R$ is a subsemi-ring. In particular we will always understand ΠR and ΣR as semi-rings under these compositions, without explicitly mentioning it.

(1.58) Example:

• Propably the most important case is where only two (semi-)rings $(R, +, \cdot)$ and $(S, +, \cdot)$ are involved. In this case the direct product and direct sum coincide, to be the carthesian product

$$R \oplus S = R \times S = \{ (a, b) \mid a \in R, b \in S \}$$

And if we write out the operations on $R \oplus S$ explicitly (recall that these were defined to be the pointwise operations) these simply read as (where $a, r \in R$ and $b, s \in S$)

$$(a,b) + (r,s) = (a+r,b+s)$$

 $(a,b)(r,s) = (ar,bs)$

Thereby it is clear that the zero-element of $R \oplus S$ is given to be 0 = (0,0). And if both R and S are rings then the unit element of $R \oplus S$ is given to be 1 = (1,1). It also is clear that $R \oplus S$ is commutative iff both R and S are such. The remarks below just generalize these observations and give hints how this can be proved.

• Another familiar case is the following: consider a (semi-)ring $(R, +, \cdot)$ and any non-empty index set $I \neq \emptyset$. In the examples of section 1.3 we have already studied the (semi-)ring

$$R^{I} := \prod_{i \in I} R = \{ f \mid f : I \to R \}$$

In the previous example as well as in this definition here we have taken the pointwise operations. That is for two elements $f, g: I \to R$ we have defined the operations

$$f + g : I \to R = i \mapsto f(i) + g(i)$$

$$fg : I \to R = i \mapsto f(i) \cdot g(i)$$

And it is clear that the zero-element is given to be the constant function $0: I \to R: i \mapsto 0$. And if R is a ring then we also have a unit element given to be the constant function $1: I \to R: i \mapsto 1$.

• We continue with the example above. Instead of the direct product we may also take to the direct sum of R over I. That is we may regard

$$R^{\oplus I} := \bigoplus_{i \in I} R = \{ f : I \to R \mid \# \operatorname{supp}(f) < \infty \}$$

where $\operatorname{supp}(f) := \{i \in I \mid f(i) \neq 0\}$. It is clear $R^{\oplus I} \subseteq R^I$ truly is a subset of the direct product. But be careful, as in in any non-zero ring $R \neq 0$ we have $1 \neq 0$ we find that for infinite index sets I the unit element $1: I \to R: i \mapsto 1$ is *not* contained in $R^{\oplus I}$. That is $R^{\oplus I}$ need not be a ring, even if R is such.

(1.59) Remark:

As above let $\emptyset \neq I$ be an arbitrary index set and for any $i \in I$ let $(R_i, +, \cdot)$ be a (semi-)ring having the zero element 0_i (and unit element 1_i if any). Then let us denote the direct product of the R_i by ΠR and the direct sum of the R_i by ΣR . Then we would like to remark the following

• It is clear that $(\Pi R, +, \cdot)$ truly becomes a (semi-)ring under the operations above. And if we denote the zero-element of any R_i by 0_i then the zero-element of ΠR is given to be $0 = (0_i)$.

PROB one easily checks all the porperties required for a semi-ring. As an example we prove the associativity of the addition: let $a = (a_i)$, $b = (b_i)$ and $c = (c_i) \in \Pi R$, then $((a + b) + c)_i = (a + b)_i + c_i =$ $(a_i + b_i) + c_i = a_i + (b_i + c_i) = a_i + (b + c)_i = (a + (b + c))_i$.

• Clearly ΠR is commutative if and only if R_i is commutative for any $i \in I$. And ΠR is a ring if and only if R_i is a ring for any $i \in I$. In the latter case let us denote the unit element of R_i by 1_i . Then the unit element of ΠR is given to be $1 = (1_i)$.

PROB if any R_i is commutative, then for any $a = (a_i), b = (b_i) \in \Pi R$ we get $(ab)_i = a_i b_i = b_i a_i = (ba)_i$ which is the commutativity of ΠR . And if ΠR is commutative, then any R_i is commutative, by the same argument. If any R_i is a ring then for any $a = (a_i) \in \Pi R$ we get $(1a)_i = 1_i a_i = a_i$ and $(a1)_i = a_i 1_i = a_i$. And if ΠR is a ring, then any R_i is a ring, by the same argument.

• By definition $\Sigma R \subseteq \Pi R$ is a subset. But ΣR even is a sub-semi-ring $\Sigma R \leq_{\rm s} \Pi R$ of ΠR . Yet ΣR need *not* be a subring of ΠR (even if any R_i is a ring), as (1_i) need not be contained in ΣR .

PROB consider any $a = (a_i)$ and $b = (b_i) \in \Sigma R$ and let us denote the set $S(a) := \{i \in I \mid a_i \neq 0_i\}$. E.g. we get $S(0) = \emptyset$ and hence $0 \in \Sigma R$. Further it is clear that $S(a + b) \subseteq S(a) \cup S(b)$, S(-a) = S(a) and $S(ab) \subseteq S(a) \cap S(b)$. In particular all these sets are finite again and hence a + b, -a and $ab \in \Sigma R$, which had to be shown.

• Note that we get $\Sigma R = \Pi R$ if and only if I is a finite set. And in the case of finitely many semi-rings R_1, \ldots, R_n we also use the slightly lax notation (note that thereby $R_1 \times \cdots \times R_n = R_1 \oplus \cdots \oplus R_n$)

$$R_1 \times \cdots \times R_n := \prod_{i=1}^n R_i$$

 $R_1 \oplus \cdots \oplus R_n := \bigoplus_{i=1}^n R_i$

• It is clear that the product of (semi-)rings is associative and commutative up to isomorphy. That is if we consider the (semi-)rings $(R, +, \cdot), (S, +, \cdot)$ and $(T, +, \cdot)$, then we obtain the following isomorphies of (semi-)rings

$$R \oplus S \cong_{\mathrm{s}} S \oplus R : (a,b) \mapsto (b,a)$$
$$(R \oplus S) \oplus T \cong_{\mathrm{s}} R \oplus (S \oplus T) : ((a,b),c) \mapsto (a,(b,c))$$

PROB it is immediately clear that the above mappings are homomorphisms of (semi-)rings by definition of the operations on the product. And likewise it is clear (this is an elementary property of carthesian products) that these mappings also are bijective.

- Note that ΠR usually does *not* inherit any nice properties from the R_i (except being commutative or a ring). E.g. \mathbb{Z} is an integral domain, but $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ contains the zero-divisors (1,0) and (0,1).
- For any $j \in I$ let us denote the canonical projection from ΠR (or ΣR respectively) by π_j . Likewise let ι_j denote the canonical injection of R_j into ΠR (or ΣR respectively). That is we let

$$\pi_j : \Sigma R \twoheadrightarrow R_j : (a_i) \mapsto a_j$$
$$\iota_j : R_j \hookrightarrow \Sigma R : a_j \mapsto \left(i \mapsto \begin{cases} a_j & \text{if } i = j \\ 0_i & \text{if } i \neq j \end{cases} \right)$$

Then it is clear that π_i and ι_j are homomorphisms of semi-rings satisfying $\pi_j \iota_j = \mathbb{1}_j$. In particular π_j is surjective and ι_j is injective. And we will oftenly interpret R_j as a sub-semi-ring of ΠR (or ΣR respectively) by using the isomorphism $\iota_j : R_j \cong_{\rm s} \operatorname{in}(\iota_j)$.

(1.60) Proposition: (viz. 269) (\diamond) Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any commutative rings and consider the ideals $\mathfrak{a} \leq_{i} R$ and $\mathfrak{b} \leq_{i} R$. Then we obtain an ideal $\mathfrak{a} \oplus \mathfrak{b}$ of $R \oplus S$ by letting

$$\mathfrak{a} \oplus \mathfrak{b} := \{ (a, b) \mid a \in \mathfrak{a}, b \in \mathfrak{b} \}$$

Conversely let us denote the canonical projections of $R \oplus S$ to R and S respectively by $\varrho: R \oplus S \twoheadrightarrow R: (a, b) \mapsto a$ and $\sigma: R \oplus S \twoheadrightarrow S: (a, b) \mapsto b$. If now $\mathfrak{l} \leq_{\mathbf{i}} R \oplus S$ is an ideal then we get the identity

$$\mathfrak{u} = \varrho(\mathfrak{u}) \oplus \sigma(\mathfrak{u})$$

And thereby we obtain an explicit description of all ideals (respectively of all radical, prime or maximal) ideals of $R \oplus S$, to be the following

$$\begin{aligned} &\text{ideal } R \oplus S &= \left\{ \mathfrak{a} \oplus \mathfrak{b} \mid, \mathfrak{a} \in \text{ideal } R, \ \mathfrak{b} \in \text{ideal } S \right\} \\ &\text{srad } R \oplus S &= \left\{ \mathfrak{a} \oplus \mathfrak{b} \mid, \mathfrak{a} \in \text{srad } R, \ \mathfrak{b} \in \text{srad } S \right\} \\ &\text{spec } R \oplus S &= \left\{ \mathfrak{p} \oplus S \mid \mathfrak{p} \in \text{spec } R \right\} \cup \left\{ R \oplus \mathfrak{q} \mid \mathfrak{q} \in \text{spec } S \right\} \\ &\text{smax } R \oplus S &= \left\{ \mathfrak{m} \oplus S \mid \mathfrak{m} \in \text{smax } R \right\} \cup \left\{ R \oplus \mathfrak{n} \mid \mathfrak{n} \in \text{smax } S \right\} \end{aligned}$$

(1.61) Theorem: (viz. 271)

(i) Consider any commutative ring (R, +, ·) and two elements e, f ∈ R. Further let us denote the respective principal ideals by a := eR and b := fR. If now e and f satisfy e + f = 1 and ef = 0 then we get a + b = R and a ∩ b = {0}, formally that is

$$e + f = 1, \ ef = 0 \implies \mathfrak{a} + \mathfrak{b} = R, \ \mathfrak{a} \cap \mathfrak{b} = \{0\}$$

(ii) Now let $(R, +, \cdot)$ be any (not necessarily commutative) ring and \mathfrak{a} , $\mathfrak{b} \leq_{i} R$ be two ideals of R satisfying $\mathfrak{a} + \mathfrak{b} = R$ and $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. Then we obtain the following isomorphy of rings

$$R \cong_{\mathbf{r}} {R / \mathfrak{g} \oplus {R / \mathfrak{g}}} : x \mapsto (x + \mathfrak{a}, x + \mathfrak{b})$$

(iii) Chinese Remainder Theorem

Let $(R, +, \cdot)$ be any commutative ring and consider finitely many ideals $\mathfrak{a}_i \leq_i R$ (where $i \in 1 \dots n$) of R, that are pairwise coprime. That is for any $i \neq j \in 1 \dots n$ we assume

$$\mathfrak{a}_i + \mathfrak{a}_j = R$$

Let us now denote the intersection of all the \mathfrak{a}_i by $\mathfrak{a} := \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. Then we obtain the following isomorphy of rings

$$R/\mathfrak{a} \cong_{\mathrm{r}} \bigoplus_{i=1}^{n} R/\mathfrak{a}_{i} : x + \mathfrak{a} \mapsto (x + \mathfrak{a}_{1}, \dots, x + \mathfrak{a}_{n})$$

(1.62) Remark:

• Combining (i) and (ii) we immediately see that, whenever we are given two elements $e, f \in R$ in a commutative ring R, such that e + f = 1 and ef = 0, then this induces a decomposition of R into two rings

$$R \cong_{\mathbf{r}} \frac{R}{eR} \oplus \frac{R}{fR} : x \mapsto (x + eR, x + fR)$$

• Clearly (ii) is just a special case of the chinese remainder theorem (iii). Never the less we gave a seperate fomulation (and proof) of the statement to be easily accessible. In fact (ii) talks about decomposing R into smaller rings, whereas (iii) talks about solving equations:

• Suppose we are given the elements $a_i \in R$ (where $i \in 1...n$). Then the surjectivity of the isomorphism in (iii) guarantees that there is a solution $x \in R$ to the following system of congruencies

$$\begin{array}{rcl} x + \mathfrak{a}_1 &=& a_1 + \mathfrak{a}_1 \\ &\vdots \\ x + \mathfrak{a}_n &=& a_n + \mathfrak{a}_n \end{array}$$

Now let x be any solution of this system, then due to the isomorphy in (iii) we also find that the set of all solutions is given to be $x + \mathfrak{a}$.

• (\diamondsuit) Let us consider an example of the above in the integers $R := \mathbb{Z}$. Let $\mathfrak{a}_1 := 8\mathbb{Z}$ and $\mathfrak{a}_2 := 15\mathbb{Z}$. As 8 and 15 are relatively prime we truly find $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathbb{Z}$. And also $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 = 120\mathbb{Z}$, since the least common multiple of 8 and 15 is 120. It is elementary to verify the following two systems of congruencies

$$105 + 8\mathbb{Z} = 1 + 8\mathbb{Z}$$

$$105 + 15\mathbb{Z} = 0 + 15\mathbb{Z}$$

$$16 + 8\mathbb{Z} = 0 + 8\mathbb{Z}$$

$$16 + 15\mathbb{Z} = 1 + 15\mathbb{Z}$$

Hence if we are given any $a_1, a_2 \in \mathbb{Z}$ then we let $x := 105a_1 + 16a_2 \in \mathbb{Z}$ to solve the general system of congruencies

$$\begin{array}{rcl} x + 8\mathbb{Z} &=& a_1 + 8\mathbb{Z} \\ x + 15\mathbb{Z} &=& a_2 + 15\mathbb{Z} \end{array}$$

Chapter 2

Commutative Rings

2.1 Maximal Ideals

(2.1) Remark:

• Let us first recall the definition of a **partial order** on some nonempty set $X \neq \emptyset$. This is a relation \leq on X [formally that is a subset of the form $\leq \subseteq X \times X$] such that for any x, y and $z \in X$ we get

$$\begin{array}{rcl} x=y & \Longrightarrow & x\leq y \\ x\leq y, \; y\leq z & \Longrightarrow & x\leq z \\ x\leq y, \; y\leq x & \Longrightarrow & x=y \end{array}$$

[where we already wrote $x \leq y$ for the formal statement $(x, y) \in \leq$]. And in this case we also call (X, \leq) a *partially odered set*. And in this case it is also customary to use the notation (for any $x, y \in X$)

$$x < y \quad :\iff \quad x \leq y \text{ and } x \neq y$$

• And \leq is said to be a **linear order** on X (respectively (X, \leq) is called a *linearly ordered set*), iff \leq is a partial order such that any two elements of X are *comparable*, formally

$$\forall x, y \in X : x \le y \text{ or } y \le y$$

And in this case we may define the maximum $x \lor y$ and minimum of any two elements $x, y \in X$ to me the following element of X

$$x \wedge y := \begin{cases} x & \text{if } x \leq y \\ y & \text{if } y \leq x \end{cases} \qquad x \vee y := \begin{cases} y & \text{if } x \leq y \\ x & \text{if } y \leq x \end{cases}$$

• Example: if S is any set (even $S = \emptyset$ is allowed), then we may take the power set $X := \mathcal{P}(X) = \{A \mid A \subseteq S\}$ of X. Then the *inclusion relation* \subseteq which is defined by (for any two $A, B \in X$)

$$A \subseteq B :\iff (\forall x : x \in A \implies x \in B)$$

is a partial order on S. However the inclusion \subseteq almost never is a total order. E.g. regard $S := \{0,1\}$. Then the elements $\{0\}$ and $\{1\} \in X$ of X are not comparable. In what follows we will usually consider a set $X \subseteq$ ideal $R \subseteq \mathcal{P}(R)$ of ideals of a commutative ring R under the inclusion relation \subseteq .

• Now let (X, \leq) be a partially ordered set and $A \subseteq X$ be a subset. Then we define the sets A_* of *minimal* and A^* of *maximal* elements of A to be the following

$$\begin{array}{rcl} A_* & := & \left\{ \left. a_* \in A \mid \forall \, a \in A : a \leq a_* \right. \Longrightarrow \, a = a_* \right. \right\} \\ A^* & := & \left\{ \left. a^* \in A \mid \forall \, a \in A : a^* \leq a \right. \Longrightarrow \, a = a^* \right. \right\} \end{array}$$

And an element $a_* \in A_*$ is said to be a *minimal* element of A. Likewise $a^* \in A^*$ is said to be a *maximal* element of A. Note that in general it may happen that A has several minimal (or maximal) elements or even none at all. Example: $\mathbb{N}_* = \{0\}$ and $\mathbb{N}^* = \emptyset$ under the usual order \leq on \mathbb{N} .

• If (X, \leq) is a linearly ordered set and $A \subseteq X$ is a subset, then maximal and minimal elements of A are uniquely determined. Formally that is

$$a, b \in A^* \implies a = b$$

$$a, b \in A_* \implies a = b$$

PROB as \leq is a total order, we may assume $a \leq b$ without loss of generality. If $a, b \in A^*$, then $b \in A, a \leq b$ and $a \in A^*$ implies a = b. Likewise if $a, b \in A_*$ then $a \in A, a \leq b$ and $a \in A_*$ implies a = b.

• Let again (X, \leq) be a linearly ordered set and $A = \{a_1, \ldots, a_n\} \subseteq X$ be a finite subset of X. Then there is a (uniquely) determined minimal element A_* (resp. maximal element a^*) of A. And this is given to be

$$A^* = \{a^*\} \text{ where } a^* = \left((a_1 \lor a_2)\dots\right) \lor a_n$$
$$A_* = \{a_*\} \text{ where } a_* = \left((a_1 \land a_2)\dots\right) \land a_n$$

PROB by induction on n: if n = 1 then $a_* = a_1$ is trivial and if n = 2then a_* is minimal by construction. Thus for $n \ge 3$ we let $H := \{a_1, \ldots, a_{n-1}\} \subseteq A$. By induction hypothesis we have $H_* = \{h_*\}$ for $h^* = ((a_1 \land a_2) \ldots) \land a_{n-1}$. Now let $a_* := h_* \land a_n$ then $a_* \le h_* \le a_i$ for i < n and $a_* \le a_n$ by construction. Hence we have $a_* \le a_i$ for any $i \in 1 \ldots n$, which means $a_* \in A_*$. And the uniqueness has already been shown above. This also proves the like statement for A^* by taking to the inverse ordering $b \ge a :\iff a \le b$.

• Once again let (X, \leq) be any partially ordered set and $A \subseteq X$ be a subset of X. Then it is clear that \leq induces another partial order \leq_A on A by restricting

$$\leq_A := (\leq) \cap (A \times A)$$

And we will write \leq for \leq_A again, that is we write (A, \leq) instead of the more correct form (A, \leq_A) . Now a subset $C \subseteq X$ is said to be a **chain** in X iff (C, \leq) is linearly ordered. Equivalently that is iff any two elements of C are comparable, formally

$$\forall x, y \in C : x \le y \text{ or } y \le x$$

• Lemma of Zorn

Let (X, \leq) be a partially ordered set (in particular $X \neq \emptyset$). Further suppose that any chain C of X has an upper bound u in X, formally

$$\forall C \subseteq X : C \text{ chain } \implies \exists u \in X \ \forall c \in C : c \leq u$$

Then X already contains a (not necessarily) unique maximal element

$$\exists x^* \in X \ \forall x \in X : x^* \leq x \implies x = x^*$$

NOTA though it may come as a surprise the lemma of Zorn surely is the single most powerful tool in mathematics! We will see its imact on several occasions: e.g. the existence of maximal ideals or the existence of bases (in vector-spaces). However we do ask the reader to refer to the literature (on set-theory) for a proof. In fact the lemma of Zorn is just one of the equivalent reformulations of the axiom of choice. Hence you may also regard the lemma of Zorn as a set-theoretic axiom.

- In most cases we will use a quite simple form of the lemma of Zorn: consider an arbitrary collection of sets \mathcal{Z} . Now verify that
 - (1) $\mathcal{Z} \neq \emptyset$ is non-empty
 - (2) if $\mathcal{C} \subseteq \mathcal{Z}$ is a chain in \mathcal{Z} (that is $\mathcal{C} \neq \emptyset$ and for any $A, B \in \mathcal{C}$ we get $A \subseteq B$ or $B \subseteq A$) then we get $\bigcup \mathcal{C} \in \mathcal{Z}$ again

Then (by the lemma of Zorn) \mathcal{Z} already contains a (not necessarily unique) \subseteq -maximal element $Z \in \mathcal{Z}^*$. That is for any $A \in \mathcal{Z}$ we get

$$Z \subseteq A \implies A = Z$$

PROB regard \mathcal{Z} as a partially ordered set (\mathcal{Z}, \subseteq) under the inclusion relation (this is allowed, due to (1)). If now $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then by (2) we get $U := \bigcup \mathcal{C} \in \mathcal{Z}$. And clearly we have $C \subseteq U$ for any $C \in \mathcal{C}$. Thus U is an upper bound of \mathcal{C} and hence we may apply the lemma of Zorn to (\mathcal{Z}, \subseteq) , to find a maximal element $Z \in \mathcal{Z}^*$.

- Of course the lamma of Zorn can also be applied to findminimal elements. In analogy the the above we obtain the following special case: consider an arbitrary collection of sets Z. Now verify that
 - (1) $\mathcal{Z} \neq \emptyset$ is non-empty
 - (2) if $\mathcal{C} \subseteq \mathcal{Z}$ is a chain in \mathcal{Z} (that is $\mathcal{C} \neq \emptyset$ and for any $A, B \in \mathcal{C}$ we get $A \subseteq B$ or $B \subseteq A$) then we get $\bigcap \mathcal{C} \in \mathcal{Z}$ again

Then (by the lemma of Zorn) \mathcal{Z} already contains a (not necessarily unique) \subseteq -minimal element $Z \in \mathcal{Z}_*$. That is for any $A \in \mathcal{Z}$ we get

$$A \subseteq Z \implies A = Z$$

PROB let us define the partial order $B \leq A :\iff A \subseteq B$ on \mathcal{Z} . If now $\mathcal{C} \subseteq \mathcal{Z}$ is a chain, then by (2) we get $U := \bigcap \mathcal{C} \in \mathcal{Z}$. And clearly $U \subseteq C$ (which translates into $C \leq U$) for any $C \in \mathcal{C}$. Thus U is an upper bound of \mathcal{C} and hence we may apply the lemma of Zorn to find a \leq -maximal element Z. But being \leq -maximal trivially translates into being \subseteq -minimal again.

(2.2) Definition:

Let $(R, +, \cdot)$ be a commutative ring and $\emptyset \neq \mathcal{A} \subseteq$ ideal R be a non-empty family of ideals of R. Then we recall the definiton of maximal $\mathfrak{a}^* \in \mathcal{A}^*$ and minimal $\mathfrak{a}_* \in \mathcal{A}_*$ elements (concerning the order " \subseteq ") of \mathcal{A} :

$$\begin{array}{rcl} \mathcal{A}^* & := & \{\,\mathfrak{a}^* \in \mathcal{A} \mid \forall \,\mathfrak{a} \in \mathcal{A} : \mathfrak{a}^* \subseteq \,\mathfrak{a} \implies \mathfrak{a} = \mathfrak{a}^* \,\} \\ \mathcal{A}_* & := & \{\,\mathfrak{a}_* \in \mathcal{A} \mid \forall \,\mathfrak{a} \in \mathcal{A} : \mathfrak{a} \subseteq \,\mathfrak{a}_* \implies \mathfrak{a} = \mathfrak{a}_* \,\} \end{array}$$

(2.3) Definition:

Let $(R, +, \cdot)$ be a commutative ring, then \mathfrak{m} is said to be a **maximal ideal** of R, iff the following three statements hold true

- (1) $\mathfrak{m} \leq_{\mathbf{i}} R$ is an ideal
- (2) $\mathfrak{m} \neq R$ is proper
- (3) \mathfrak{m} is a maximal element of ideal $R \setminus \{R\}$. That is for any ideal $\mathfrak{a} \leq_i R$

$$\mathfrak{m} \subseteq \mathfrak{a} \implies \mathfrak{a} = \mathfrak{m} \text{ or } \mathfrak{a} = R$$

The set $\operatorname{smax} R$ of all maximal ideals is called **maximal spectrum** of R and the intersection of all maximal ideals is called **Jacobson radical** of R

smax
$$R := \{ \mathfrak{m} \subseteq R \mid (1), (2) \text{ and } (3) \}$$

JAC $R := \bigcap \operatorname{smax} R$

NOTA in the light of this definition the maximal spectrum is nothing but the maximal elements of the set of non-full ideals: smax $R = (\text{ideal } R \setminus \{R\})^*$.

(2.4) Lemma: (viz. 287)

(i) Let $(R, +, \cdot)$ be a commutative ring and $\emptyset \neq \mathcal{A} \subseteq$ ideal R be a chain of ideals (that is for any $\mathfrak{a}, \mathfrak{b} \in \mathcal{A}$ we have $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$). Then the union of all the $\mathfrak{a} \in \mathcal{A}$ is an ideal of R, formally

$$\emptyset \neq \mathcal{A} \subseteq \operatorname{ideal} R$$
 chain $\Longrightarrow \bigcup \mathcal{A} \trianglelefteq_{\mathrm{i}} R$ ideal

(ii) Let $R \neq \mathfrak{a} \leq_i R$ be a non-full ideal in the commutative ring $(R, +, \cdot)$, then there is a maximal ideal of R containing \mathfrak{a} , formally

$$R \neq \mathfrak{a} \leq_{\mathrm{i}} R \implies \exists \mathfrak{m} \in \operatorname{smax} R : \mathfrak{a} \subseteq \mathfrak{m}$$

(iii) In a commutative ring $(R, +, \cdot)$ the group of units R^* of R is precisely the complement of the union of all maximal ideals of R, formally

$$R^* = R \setminus \bigcup \operatorname{smax} R$$

(iv) The zero-ring is the one and only ring without maximal ideals, formally

$$R = 0 \iff \operatorname{smax} R = \emptyset$$

(2.5) **Proposition:** (viz. 288)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{m} \leq_i R$ be an ideal of R. Then the following four statements are equivalent

- (a) \mathfrak{m} is a maximal ideal
- (b) the quotient ring R/\mathfrak{m} is a field
- (c) the quotient ring R/\mathfrak{m} is simple i.e. it only contains the trivial ideals

$$\overline{\mathfrak{a}} \leq_{\mathrm{i}} R/\mathfrak{m} \implies \overline{\mathfrak{a}} = \{0 + \mathfrak{m}\} \text{ or } \overline{\mathfrak{a}} = R/\mathfrak{m}$$

(d) \mathfrak{m} is coprime to any principal ideal that is not already contained in \mathfrak{m} , formally that is: for any $a \in R$ we get the implication

$$a \notin \mathfrak{m} \implies \mathfrak{m} + aR = R$$

(2.6) **Proposition:** (viz. 288)

Let $(R, +, \cdot)$ be any commutative ring, then we can reformulate the jacobson radical of R: for any $j \in R$ the following two statements are equivalent

- (a) $j \in \operatorname{JAC} R$
- (b) $\forall a \in R \text{ we get } 1 aj \in R^*$

And if $\mathfrak{a} \leq_{i} R$ is an ideal of R, then \mathfrak{a} is contained in the jacobson radical iff $1 + \mathfrak{a}$ is a subgroup of the multiplicative group. That is equivalent are

- (a) $\mathfrak{a} \subseteq \operatorname{JAC} R$
- (b) $1 + \mathfrak{a} \subseteq R^*$
- (c) $1 + \mathfrak{a} \leq_{\mathrm{g}} R^*$

(2.7) Proposition: (viz. 290)

Let $(R, +, \cdot)$ be a commutative ring and let $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\} \subseteq \operatorname{smax} R$ be finitely many maximal ideals of R. Then we obtain the following statements

$$\forall i \neq j \in 1 \dots n : \mathfrak{m}_i + \mathfrak{m}_j = R$$
$$\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_k = \mathfrak{m}_1 \dots \mathfrak{m}_k$$
$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \mathfrak{m}_2 \supset \dots \supset \mathfrak{m}_1 \mathfrak{m}_2 \dots \mathfrak{m}_k$$
2.2 Prime Ideals

(2.8) Definition:

Let $(R, +, \cdot)$ be a commutative ring, then \mathfrak{P} is said to be a **prime ideal** of R, iff the following three statements hold true

- (1) $\mathfrak{p} \leq_{\mathbf{i}} R$ is an ideal
- (2) $\mathfrak{p} \neq R$ is proper
- (3) $\forall a, b \in R$ we get $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

And the set spec R of all prime ideals of R is called **spectrum** of R, formally

spec
$$R := \{ \mathfrak{p} \subseteq R \mid (1), (2) \text{ and } (3) \}$$

An ideal $\mathfrak{p}_* \leq_{\mathrm{i}} R$ is said to be a **minimal prime ideal** of R, iff it is a minimal element of spec R. That is $\mathfrak{p}_* \in \operatorname{spec} R$ and for any prime ideal $\mathfrak{p} \in \operatorname{spec} R$ we get the implication $\mathfrak{p}_* \subseteq \mathfrak{p} \Longrightarrow \mathfrak{p}_* = \mathfrak{p}$. Let us finally denote the set of all minimal prime ideals of R by

$$\operatorname{smin} R := \left(\operatorname{spec} R\right)_*$$

(2.9) Proposition: (viz. 289)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{P} \leq_{i} R$ be an ideal of R. Then the following four statements are equivalent

- (a) \mathfrak{p} is a prime ideal
- (b) the quotient ring R/\mathfrak{p} is a non-zero $(R/\mathfrak{p} \neq 0)$ integral domain
- (c) the complement $U := R \setminus \mathfrak{p}$ is multiplicatively closed, this is to say that
 - (1) $1 \in U$
 - $(2) \ u, v \in U \implies uv \in U$
- (d) $\mathfrak{p} \neq R$ is non-full and for any two ideals $\mathfrak{a}, \mathfrak{b} \leq_i R$ we get the implication

$$\mathfrak{ab} \subseteq \mathfrak{p} \implies \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p}$$

(2.10) Remark:

At this point we can reap an important harvest of the theory: maximal ideals are prime. Using the machinery of algebra this can be seen in a most beautiful way: if \mathfrak{m} is a maximal ideal, then R/\mathfrak{m} is a field by (2.5). But fields are (by definition non-zero) integral domains. Hence \mathfrak{m} already is prime by (2.9). Of course it is also possible to give a direct proof - an example of such will be presented for (2.19).

(2.11) Proposition: (viz. 290)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{P} \leq_i R$ be a prime ideal of R, then

(i) If $a_1, \ldots, a_k \in R$ are finitely many elements then by induction it is clear that we obtain the following implication

$$a_1 \dots a_k \in \mathfrak{p} \implies \exists i \in 1 \dots k : a_i \in \mathfrak{p}$$

(ii) Likewiese let $\mathfrak{a}_1, \ldots, \mathfrak{a}_k \leq_i R$ be finitely many ideals of R, then by induction we also find the following implication

$$igcap_{i=1}^k \mathfrak{a}_i \subseteq \mathfrak{p} \implies \exists i \in 1 \dots k : \mathfrak{a}_i \subseteq \mathfrak{p}$$

(iii) prime avoidance

Consider some ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_n \leq_{\mathrm{i}} R$ where $2 \leq n \in \mathbb{N}$ such that $\mathfrak{b}_3, \ldots, \mathfrak{b}_n \in \operatorname{spec} R$ are prime. If now $\mathfrak{a} \leq_{\mathrm{i}} R$ is another ideal, then we obtain the following implication

$$\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{b}_i \implies \exists i \in 1 \dots n : \mathfrak{a} \subseteq \mathfrak{b}_i$$

(2.12) Example:

In a less formalistic way the prime avoidance lemma can be put like this: if an ideal \mathfrak{a} is contained in the union of finitely many ideals \mathfrak{b}_i of which at most two are non-prime, then it already is contained in one of these. In spite of the odd assumption the statement is rather sharp. In fact it may happen that \mathfrak{a} is contained in the union of three strictly smaller ideals (which of course are all non-prime in this case). Let us give an example of this: fix the field $E := \mathbb{Z}_2$ and the ideal $\mathfrak{o} := \langle s, t \rangle_i^2 = \langle s^2, st, t^2 \rangle_i \leq_i E[s, t]$. Then the ring in consideration is

$$R := E[s,t]/\mathfrak{g}$$

Note that any residue class of $f \in E[s, t]$ can be represented in the form $f + \mathfrak{o} = f[0, 0] + f[1, 0]s + f[0, 1]t + \mathfrak{o}$. That is R contains precisely 6 elements, namely $a + bs + ct + \mathfrak{o}$ where a, b and $c \in E = \mathbb{Z}_2$. Now take the following ideal

$$\mathfrak{a} := \frac{\langle s + \mathfrak{o}, t + \mathfrak{o} \rangle_{i}}{\mathfrak{o}}$$

= { f + \tilde{o} | f \in E[s, t], f[0, 0] = 0 }
= { 0 + \tilde{o}, s + \tilde{o}, t + \tilde{o}, s + t + \tilde{o} }

On the other hand let us also take the following ideals $\mathfrak{b}_1 := (s + \mathfrak{o})R$, $\mathfrak{b}_2 := (t + \mathfrak{o})R$ and $\mathfrak{b}_2 := (s + t + \mathfrak{o})R$. Now an easy computation (e.g. for \mathfrak{b}_1 we get $(s + \mathfrak{o})(a + bs + ct + \mathfrak{o}) = as + \mathfrak{o}$) yields

$$\begin{aligned}
\mathfrak{b}_1 &:= \{0 + \mathfrak{o}, s + \mathfrak{o}\} \\
\mathfrak{b}_2 &:= \{0 + \mathfrak{o}, t + \mathfrak{o}\} \\
\mathfrak{b}_3 &:= \{0 + \mathfrak{o}, s + t + \mathfrak{o}\}
\end{aligned}$$

And hence it is immediately clear that any $\mathfrak{b}_i \subset \mathfrak{a}$ is a strict subset, but the union of these ideals precisely is the ideal \mathfrak{a} again

$$\mathfrak{a} = \mathfrak{b}_1 \cup \mathfrak{b}_2 \cup \mathfrak{b}_3$$

(2.13) Lemma: (viz. 291)

Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two commutative rings and denote their prime spectra by $X := \operatorname{spec}(R)$ and $Y := \operatorname{spec}(S)$ respectively. Now consider some ring-homomorphism $\varphi : R \to S$. Then φ induces a well-defined map on the spectra of S and R, by virtue of

$$\operatorname{spec}(\varphi) : Y \to X : \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$$

For any element $a \in R$ let us denote $X_a := \{ \mathfrak{p} \in X \mid a \notin \mathfrak{p} \}$ and for any ideal $\mathfrak{a} \trianglelefteq_i R$ let us denote $\mathbb{V}(\mathfrak{a}) := \{ \mathfrak{p} \in X \mid \mathfrak{a} \subseteq \mathfrak{p} \}$. If now $a \in R, \mathfrak{a} \trianglelefteq_i R$ and $\mathfrak{b} \trianglelefteq_i S$, then spec (φ) satisfies the following properties

$$(\operatorname{spec} \varphi)^{-1}(X_a) = Y_{\varphi(a)}$$
$$(\operatorname{spec} \varphi) (\mathbb{V}(\mathfrak{b})) \subseteq \mathbb{V} (\varphi^{-1}(\mathfrak{b}))$$
$$(\operatorname{spec} \varphi)^{-1} (\mathbb{V}(\mathfrak{a})) = \mathbb{V} (\langle \varphi(\mathfrak{a}) \rangle_{i})$$

(2.14) Proposition: (viz. 292)

(i) Let $(R, +, \cdot)$ be a commutative ring and $\mathcal{P} \subseteq \operatorname{spec} R$ be a chain of prime ideals of R (that is for any $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}$ we have $\mathfrak{p} \subseteq \mathfrak{q}$ or $\mathfrak{q} \subseteq \mathfrak{p}$). Then the intersection of all the $\mathfrak{p} \in \mathcal{P}$ is a prime ideal of R, formally

$$\emptyset \neq \mathcal{P} \subseteq \operatorname{spec} R$$
 chain $\Longrightarrow \bigcap \mathcal{P} \in \operatorname{spec} R$ prime

(ii) Let $\emptyset \neq \mathcal{P} \subseteq \operatorname{spec} R$ be a non-empty set of prime ideals of the commutative ring $(R, +, \cdot)$. And assume that \mathcal{P} is closed under \subseteq , i.e.

$$\forall \, \mathfrak{p} \in \operatorname{spec} R \ \forall \, \mathfrak{q} \in \mathcal{P} \ : \ \mathfrak{p} \subseteq \, \mathfrak{q} \implies \, \mathfrak{p} \in \mathcal{P}$$

Then \mathcal{P} already contains a minimal element, formally that is $\mathcal{P}_* \neq \emptyset$.

(iii) Let $(R, +, \cdot)$ be a commutative ring and consider an arbitrary ideal $\mathfrak{a} \leq_{i} R$ and a prime ideal $\mathfrak{q} \leq_{i} R$. We now give a short list of possible *conditions* we may impose and the respective *assumptions* that have to be supposed for \mathfrak{a} and \mathfrak{q} in this case

assumption	$\operatorname{condition}(\mathfrak{p})$
$R \neq 0$	none
nothing	$\mathfrak{p}\subseteq\mathfrak{q}$
$\mathfrak{a} \neq R$	$\mathfrak{a}\subseteq\mathfrak{p}$
$\mathfrak{a} \subseteq \mathfrak{q}$	$\mathfrak{a}\subseteq\mathfrak{p}\subseteq\mathfrak{q}$

Then there is a prime ideal \mathfrak{p} of R that is minimal among all prime ideals satisfying the condition imposed. Formally that is

 $\emptyset \neq \{ \mathfrak{p} \in \operatorname{spec} R \mid \operatorname{condition}(\mathfrak{p}) \}_*$

(iv) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_i R$ be any ideal and $\mathfrak{q} \leq_i R$ a prime ideal with $\mathfrak{a} \subseteq \mathfrak{q}$. Then there is a prime ideal \mathfrak{p}_* minimal over \mathfrak{a} that is contained in \mathfrak{q} . Formally that is

$$\exists \mathfrak{p}_* \in \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\}_* \quad \text{with} \quad \mathfrak{a} \subseteq \mathfrak{p}_* \subseteq \mathfrak{q}$$

(v) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_{i} R$ be an ideal of R and $U \subseteq R$ be a multiplicatively closed set (that is $1 \in U$ and $u, v \in U$ implies $uv \in U$). If now $\mathfrak{a} \cap U = \emptyset$ then the set of all ideals $\mathfrak{b} \leq_{i} R$ satisfying $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U$ contains maximal elements. And any such is maximal element is a prime ideal, formally

$$\emptyset \neq \left\{ \mathfrak{b} \trianglelefteq_{\mathbf{i}} R \mid \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U \right\}^* \subseteq \operatorname{spec} R$$

(2.15) Corollary: (viz. 364)

(i) Let $(R, +, \cdot)$ be a non-zero $R \neq 0$, commutative ring, then the set of zero-divisors of R is the union of a certain set of prime ideals of R

$$\operatorname{ZD} R = \bigcup \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \subseteq \operatorname{ZD} R \}$$

(ii) In a commutative ring $(R, +, \cdot)$ the minimal prime ideals are already contained in the zero-divisors of R, formally that is

$$\mathfrak{p} \in \operatorname{smin} R \implies \mathfrak{p} \subseteq \operatorname{ZD} R$$

2.3 Radical Ideals

(2.16) Definition:

Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_i R$ be an ideal of R and $b \in R$ be an element. Then we define the **radical** $\sqrt{\mathfrak{a}}$ and **fraction** $\mathfrak{a} : b$ of \mathfrak{a} to be

$$\sqrt{\mathfrak{a}} := \left\{ a \in R \mid \exists k \in \mathbb{N} : a^k \in \mathfrak{a} \right\}$$
$$\mathfrak{a} : b := \left\{ a \in R \mid ab \in \mathfrak{a} \right\}$$

Now \mathfrak{a} is said to be a **radical ideal** (sometimes this is also called *perfect ideal* in the literature), iff \mathfrak{a} equals its radical, that is iff we have

- (1) $\mathfrak{a} \leq_{\mathrm{i}} R$
- (2) $\mathfrak{a} = \sqrt{\mathfrak{a}}$

And thereby we define the **radical spectrum** stad R of R to be the set of all radical ideals of R, formally that is

$$\operatorname{srad} R := \left\{ \mathfrak{a} \trianglelefteq_{\mathrm{i}} R \mid \mathfrak{a} = \sqrt{\mathfrak{a}} \right\}$$

(2.17) Proposition: (viz. 293)

Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_i R$ be an ideal of R and $b \in R$ be an element. Then we obtain the following statements

(i) The fraction $\mathfrak{a}: b$ is an ideal of R again containing \mathfrak{a} , formally that is

$$\mathfrak{a} \subseteq \mathfrak{a}: b \trianglelefteq_{\mathbf{i}} R$$

(ii) The radical $\sqrt{\mathfrak{a}}$ even is a radical ideal of R containing \mathfrak{a} , formally again

$$\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \in \operatorname{srad} R$$

(iii) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a}, \mathfrak{b} \leq_{i} R$ ideals and $b \in R$, then

$$\begin{array}{ll} \mathfrak{a} \subseteq \mathfrak{b} & \Longrightarrow & \mathfrak{a} : b \subseteq \mathfrak{b} : b \\ \mathfrak{a} \subseteq \mathfrak{b} & \Longrightarrow & \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}} \end{array}$$

(iv) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_i R$ an ideal and $b \in R$, then

$$\mathfrak{a}: b = R \iff b \in \mathfrak{a}$$

Thus if $\mathfrak{P} \trianglelefteq_i R$ even is a prime ideal then we have precisely two cases

(v) The intersection of a collection $\mathcal{A} \neq \emptyset$ of radical ideals is a radical ideal

$$\emptyset \neq \mathcal{A} \subseteq \operatorname{srad} R \implies \bigcap \mathcal{A} \in \operatorname{srad} R$$

(vi) Let again $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a}_i \leq_i R$ be an arbitrary family of ideals $(i \in I)$ and $b \in R$. Then we find the equality

$$\bigcap_{i\in I}(\mathfrak{a}_i:b) \ = \ \left(\bigcap_{i\in I}\mathfrak{a}_i\right):b$$

(2.18) Proposition: (viz. 295)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_i R$ be an ideal of R. Then the following four statements are equivalent

- (a) $\sqrt{\mathfrak{a}} \subseteq \mathfrak{a}$
- (b) $\mathfrak{a} = \sqrt{\mathfrak{a}}$ is a radical ideal
- (c) $\forall a \in R$ we get $\exists k \in \mathbb{N} : a^k \in \mathfrak{a} \implies a \in \mathfrak{a}$
- (d) the quotient ring R/\mathfrak{a} is *reduced*, i.e. it contains no non-zero nilpotents

$$\operatorname{NIL}^{R}/_{\mathfrak{a}} = \{0 + \mathfrak{a}\}$$

(2.19) Corollary: (viz. 295)

Let $(R, +, \cdot)$ be a commutaive ring and \mathfrak{m} , \mathfrak{p} and $\mathfrak{a} \leq_{i} R$ be ideals of R respectively. Then we have gained the following table of equivalencies

where a ring S is said to be *reduced*, iff $s^k = 0$ (for some $k \in \subseteq \mathbb{N}$) implies s = 0. And subsuming the properties of the respective quotient rings we thereby find the inclusions

$$\operatorname{smax} R \subseteq \operatorname{spec} R \subseteq \operatorname{srad} R$$

(2.20) Proposition: (viz. 295)

(i) The radical of \mathfrak{a} is the intersection of all prime ideals containing \mathfrak{a} , i.e.

$$\sqrt{\mathfrak{a}} = \bigcap \left\{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \right\}$$
$$= \bigcap \left\{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \right\}_{*}$$

(ii) In particular the nil-radical is just the intersection of all prime ideals

$$\operatorname{NIL} R = \sqrt{0} = \bigcap \operatorname{spec} R = \bigcap \operatorname{smin} R$$

(iii) In a commutative ring $(R, +, \cdot)$ the map $\mathfrak{a} \mapsto \sqrt{\mathfrak{a}}$ is a projection (i.e. idempotent). That is for any ideal $\mathfrak{a} \leq_{\mathbf{i}} R$ we find

$$\sqrt{\sqrt{a}} = \sqrt{a}$$

(iv) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_{i} R$ be an arbitrary and $\mathfrak{p} \leq_{i} R$ be a prime ideal. If now $k \in \mathbb{N}$, then we get the implication

$$\mathfrak{a}^k \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}} \implies \mathfrak{p} = \sqrt{\mathfrak{a}}$$

(v) Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a}, \mathfrak{b} \leq_{i} R$ be ideals, then we get

$$\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a}\cap\mathfrak{b}} = \sqrt{\mathfrak{a}}\cap\sqrt{\mathfrak{b}}$$

(vi) And thereby - if $(R, +, \cdot)$ is a commutative ring, $1 \le k \in \mathbb{N}$ and $\mathfrak{a} \leq_i R$ is an ideal, then we obtain the equality

$$\sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}}$$

(vii) Let $\mathfrak{a} \leq_{\mathbf{i}} R$ be a finitely generated ideal in the commutative ring $(R, +, \cdot)$. And let $\mathfrak{b} \leq_{\mathbf{i}} R$ be another ideal of R. Then we get

$$\mathfrak{a} \subseteq \sqrt{\mathfrak{b}} \hspace{0.1 cm} \Longrightarrow \hspace{0.1 cm} \exists \, k \in \mathbb{N} \hspace{0.1 cm} : \hspace{0.1 cm} \mathfrak{a}^k \subseteq \mathfrak{b}$$

(viii) Let again $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a}_i \leq_i R$ be an arbitrary family of ideals $(i \in I)$, then we obtain the following inclusions

$$\sum_{i \in I} \sqrt{\mathfrak{a}} \subseteq \sqrt{\sum_{i \in I} \mathfrak{a}_i}$$
$$\sqrt{\bigcap_{i \in I} \mathfrak{a}_i} \subseteq \bigcap_{i \in I} \sqrt{\mathfrak{a}_i}$$

(2.21) Remark:

Due to (2.17.(iii)) the intersection of prime ideals yields a radical ideal. And in (2.19) we have just seen that maximal and prime ideals already are radical. Now recall that the *jacobson-radical* JAC *R* has been defined to be the intersection of all maximal ideals. And we have just seen in (2.20.(ii))above that the *nil-radical* is the intersection of all (minimal) prime ideals. This means that both are radical ideals (and hence the name)

$$JAC R = \bigcap \operatorname{smax} R \in \operatorname{srad} R$$
$$NIL R = \bigcap \operatorname{spec} R \in \operatorname{srad} R$$

(2.22) Example:

Note however that taking sums and radicals of (even finitely many) ideals does *not* commute. That is there is *no* analogous statement to (2.20.(vi)) concerning sums $\mathfrak{a} + \mathfrak{b}$. As an example consider R := E[s, t], the polynomial ring in two variables, where $(E, +, \cdot)$ is an arbitrary field. Now pick up

$$\mathfrak{p} := (s^2 - t)R$$
 and $\mathfrak{q} := tR$

It is clear that \mathfrak{p} and \mathfrak{q} are prime ideals (as the quotient is isomorphic to the integral domain E[s] under the isomorphisms induced by $f(s,t) \mapsto f(s,s^2)$ and $f(s,t) \mapsto f(s,0)$ respectively). However the sum $\mathfrak{p} + \mathfrak{q}$ of both not even is a radical ideal, in fact we get

$$\mathfrak{p} + \mathfrak{q} = s^2 R + tR \subset sR + tR = \sqrt{\mathfrak{p} + \mathfrak{q}}$$

PROB We first prove $\mathfrak{a} + \mathfrak{q} = s^2 R + tR$ - thus consider any $h = (s^2 - t)f + tg \in \mathfrak{p} + \mathfrak{q}$, then h can be rewritten as $h = s^2 f + t(g - f) \in s^2 R + tR$. But conversely $t \in \mathfrak{q} \subseteq \mathfrak{p} + \mathfrak{q}$ and $s^2 = (s^2 - t) + t \in \mathfrak{p} + \mathfrak{q}$. In particular s is contained in the radical of $\mathfrak{p} + \mathfrak{q}$ and hence $\mathfrak{p} + \mathfrak{q} \subseteq sR + tR \subseteq \sqrt{\mathfrak{p} + \mathfrak{q}}$. As sR + tR is prime (even maximal) this implies the equality of the radical ideal. So finally we wish to prove $s \notin \mathfrak{p} + \mathfrak{q}$ (and in particular $\mathfrak{p} + \mathfrak{q}$ is no radical ideal. Thus suppose $s = s^2 f + tg$ for some polynomials $f, g \in R$. Then (as s is prime and does not divide t) s divides g. To be precise we get g = sh for $h = (1 - st)/t \in R$. And hence we get $s = s^2 f + sth$. Eliminating s we find 1 = sf + th, an equation that cannot hold true (as 1 is of degree 0 and sf + th of degree at least 1). Thus we got $s^2 \notin s^2 R + tR$.

(2.23) Example: (viz. 298)

Be aware that radicals may be very large when compared with their original ideals. E.g. it may happen that $\mathfrak{a} = aR$ is a principal ideal, but $\sqrt{\mathfrak{a}}$ is *not* finitely generated. In fact in the chapter of proofs we give an example where there even is no $n \in \mathbb{N}$ such that $(\sqrt{\mathfrak{a}})^n \subseteq \mathfrak{a}$, as well.

(2.24) Remark:

Combining (2.17.(iii)) and (viii) in the above proposition it is clear that for an arbitrary collection of ideals $\mathfrak{a}_i \leq_i R$ (where $i \in I$) in a commutative ring $(R, +, \cdot)$ we obtain the following equalities

$$\sqrt{\sum_{i \in I} \sqrt{\mathfrak{a}}} = \sqrt{\sum_{i \in I} \mathfrak{a}_i}$$
$$\sqrt{\bigcap_{i \in I} \sqrt{\mathfrak{a}_i}} = \sqrt{\bigcap_{i \in I} \mathfrak{a}_i}$$

(2.25) Example:

The inclusions in (2.20.(viii)) need *not* be equalities! As an example let us consider the ring of integers $R = \mathbb{Z}$. And let us take $I = \mathbb{N}$ and $\mathfrak{a}_i = p^i \mathbb{Z}$ for some prime number $p \in \mathbb{Z}$. As any non-zero element of \mathbb{Z} is divisible by finite powers p^i only the intersection of the \mathfrak{a}_i is $\{0\}$. On the other hand $\sqrt{\mathfrak{a}_i} = p\mathbb{Z}$ due to (2.20.(vii)) and since $p\mathbb{Z}$ is a prime (and hence radical) ideal of \mathbb{Z} . Thereby we found the counterexample

$$\sqrt{\bigcap_{i \in \mathbb{N}}} \mathfrak{a}_i = \sqrt{0} = 0 \subset p\mathbb{Z} = \bigcap_{i \in \mathbb{N}} p\mathbb{Z} = \bigcap_{i \in \mathbb{N}} \sqrt{\mathfrak{a}_i}$$

(2.26) Proposition: (viz. 298)

Let now $\varphi : R \to S$ be a ring-homomorphism between the commutative rings $(R, +, \cdot)$ and $(S, +, \cdot)$. And consider the ideals $\mathfrak{a} \leq_{i} R$ and $\mathfrak{b} \leq_{i} S$. Then let us denote the transferred ideals of \mathfrak{a} and \mathfrak{b}

$$\begin{split} \mathfrak{b} \cap R &:= \varphi^{-1}(\mathfrak{b}) & \trianglelefteq_{\mathbf{i}} R \\ \mathfrak{a} S &:= \langle \varphi(\mathfrak{a}) \rangle_{\mathbf{i}} & \trianglelefteq_{\mathbf{i}} S \end{split}$$

Note that in case that φ is surjective (but not generally), we get $\mathfrak{a}S = \varphi(\mathfrak{a})$. Using these notions we obtain the following statements

(i)

$$\sqrt{\mathfrak{b} \cap R} = \sqrt{\mathfrak{b}} \cap R$$

(ii)

$$\sqrt{\mathfrak{a}S} = \sqrt{\sqrt{\mathfrak{a}S}}$$

(iii) Now let us abbreviate by \star any of the words maximal ideal, prime ideal or radical ideal. Then we find the equivalence

$$\mathfrak{b} \text{ is a } \star \iff \mathfrak{b} \cap R \text{ is a } \star$$

And if $\varphi: R \twoheadrightarrow S$ even is surjective then we get another equivalence

$$\mathfrak{a} + \operatorname{kn}(\varphi)$$
 is a $\star \iff \mathfrak{a}S$ is a \star

2.4 Noetherian Rings

In this section we will introduce and study noetherian and artinian rings. Both types of rings are defined by a chain condition on ideals - ascending in the case of noetherian and descending in the case of artinian rings. So one might expect a completely dual theory for these two objects. Yet this is not the case! In fact it turns out that the artinian property is much stronger: any artinian ring already is noetherian, but the converse is false. An while examples of noetherian rings are abundant, there are few artinian rings. On the other hand both kinds of rings have several similar properties: e.g. both are very well-behaved under taking quotients or localisations.

Throughout the course of this book we will see that noetherian rings have lots of beautiful properties. E.g. they allow the Lasker-Noether decomopsition of ideals. However in non-noetherian rings peculiar things may happen. Together with the easy properties of inheritance this makes noetherian rings one of the predominant objects of commutative algebra and algebraic geometry. Artinian rings are of lesser importance, yet they arise naturally in number theory and the theory of algebraic curves.

(2.27) Definition: (viz. 300)

Let $(R, +, \cdot)$ be a commutative ring, then R is said to be **noetherian** iff it satisfies one of the following four equivalent conditions

(a) R satisfies the ascending chain condition (ACC) of ideals - that is any family of ideals $\mathfrak{a}_k \leq_{i} R$ of R (where $k \in \mathbb{N}$) such that

 $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \subseteq \ldots$

becomes eventually constant - that is there is some $s \in \mathbb{N}$ such that

 $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_s = \mathfrak{a}_{s+1} = \ldots$

- (b) Every nonempty family of ideals contains a maximal element, formally that is: for any $\emptyset \neq \mathcal{A} \subseteq$ ideal R there is some $\mathfrak{a}^* \in \mathcal{A}^*$.
- (c) Every ideal of R is finitely generated, formally that is: for any ideal $\mathfrak{a} \leq_{i} R$ there are some $a_1, \ldots, a_k \in R$ such that we get

$$\mathfrak{a} = \langle a_1, \dots, a_k \rangle_{\mathbf{i}} = a_1 R + \dots + a_k R$$

(d) Every prime ideal of R is finitely generated, formally that is: for any prime ideal $\mathfrak{p} \in \operatorname{spec} R$ there are some $a_1, \ldots, a_k \in R$ such that

$$\mathfrak{p} = \langle a_1, \dots, a_k \rangle_{\mathbf{i}} = a_1 R + \dots + a_k R$$

We will now define artinian rings (by property (a) from a strictly logical point of view). And again we will find an even longer list of equivalent statements. The similarity in the definition gives strong reason to study these objects simultaneously. But as oftenly only one half of the equivalencies can be proved straightforwardly while the other half requires heavy-duty machinery that is not yet available. For a novice reader it might hence be wise to concentrate noetherian rings only. These will be the important objects later on. Artinian rings not only are far less common but they also are severely more difficult to handle.

(2.28) Definition: (viz. ??)

Let $(R, +, \cdot)$ be a commutative ring, then R is said to be **artinian** iff it satisfies one of the following six equivalent conditions

(a) R satisfies the descending chain condition (DCC) of ideals - that is any family of ideals $\mathfrak{a}_k \leq_{i} R$ of R (where $k \in \mathbb{N}$) such that

 $\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_k \supseteq \mathfrak{a}_{k+1} \supseteq \ldots$

becomes eventually constant - that is there is some $s \in \mathbb{N}$ such that

 $\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_s = \mathfrak{a}_{s+1} = \ldots$

- (b) Every nonempty family of ideals contains a minimal element, formally that is: for any $\emptyset \neq \mathcal{A} \subseteq$ ideal R there is some $\mathfrak{a}_* \in \mathcal{A}_*$.
- (c) *R* is of finite length as an *R*-module that is there is an upper bound on the maximal length of a strictly ascending chain of ideals, formally

$$\ell(R) := \sup \left\{ k \in \mathbb{N} \mid \begin{array}{l} \exists \, \mathfrak{a}_0, \mathfrak{a}_1, \dots, \mathfrak{a}_k \, \leq_i R : \\ \mathfrak{a}_0 \, \subset \, \mathfrak{a}_1 \, \subset \, \dots \, \subset \, \mathfrak{a}_k \end{array} \right\} \, < \, \infty$$

(d) R is a noetherian ring and any prime ideal already is maximal, formally

$$\operatorname{smax} R = \operatorname{spec} R$$

(e) R is a noetherian ring and even any minimal prime ideal already is a maximal ideal, formally again

$$\operatorname{smax} R = \operatorname{smin} R$$

(f) R is a noetherian ring whise jacobson radical equals its nil-radical (i.e. JAC R = NIL R) and that is semi-local (i.e. $\# \text{smax } R < \infty$).

(2.29) Example:

- Any field E is an artinian (and noetherian) ring, as it only contains the trivial ideals 0 and E. In particular the chain of ideals with strict inclusions is $0 \subset E$, and this is finite.
- Any finite ring such as \mathbb{Z}_n is artinian (and noetherian), as it only contains finitely many ideals (and in particular any chain of ideals has to be eventually constant).
- We will study principal ideal domains (PIDs) in section 2.6. These are integral domains R in which every ideal $\mathfrak{a} \leq_i R$ is generated by some element $a \in R$ (that is $\mathfrak{a} = aR$). In particular any ideal is finitely generated and hence any PID is noetherian.
- The integers \mathbb{Z} form an easy example of a noetherian ring (as they are a PID). But they are not artinian, e.g. they contain the infinitely decreasing chain of ideals $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \ldots \supset 2^k\mathbb{Z} \supset \ldots$
- We will soon see (a special case of the Hilbert basis theorem) that the polynomial ring $R = E[t_1, \ldots, t_n]$ in finitely many variables over a field E is a noetherian ring. And again this is no artinian ring, as it contains the infinitely decreasing chain of ideals $R \supset t_1 R \supset t_1^2 R \supset \ldots$
- Of course there are examples of non-noetherian rings, too. E.g. let E be a field and consider $R := E[t_i \mid 1 \leq i \in \mathbb{N}]$ the polynomial ring in (countably) infinitely many indeterminates. Then R is an integral domain but it is not noetherian. Just let $\mathfrak{p}_k := \langle t_1, t_2, \ldots, t_k \rangle_i$ be the ideal generated by the first k indeterminates. Then we obtain an infinitely ascending chain of (prime) ideals $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_k \subset \ldots$
- Non-noetherian rings may well lie inside of noetherian rings. As an example regard the ring $R = E[t_i \mid 1 \leq i \in \mathbb{N}]$ again. As R is an integral domain R is contained in its quotient field F. But as F is a field it in particular is noetherian.
- (◊) We would finally like to present an example from complex analysis: let \$\mathcal{O}\$:= { f : C → C | f holomorphic } be the ring of entire functions (note that this is isomorphic to the ring C{z} of globally convergent power series). Now let \$\mathbf{a}_k\$:= { f ∈ \$\mathcal{O}\$ | \$\forall k ≤ n ∈ \$\mathbb{N}\$: f(n) = 0 }. Clearly the \$\mathbf{a}_k\$ \$\leq i\$ \$\mathcal{O}\$ are ideals of \$\mathcal{O}\$ they even form a strictly ascending chain of ideals (this is a special case of the Weierstrass product theorem). Again \$\mathcal{O}\$ is an integral domain (by the identity theorem of holomorphic functions).

(2.30) Proposition: (viz. 302)

Let $(R, +, \cdot)$ be a commutative ring and fix \star as an abbreviation for either of the words *noetherian* or *artinian*. Then the following statements hold true:

- (i) If $\mathfrak{a} \leq_i R$ is an ideal and R is \star , then the quotient R/\mathfrak{a} also is a \star ring.
- (ii) Let $(S, +, \cdot)$ be any ring and let $\varphi : R \twoheadrightarrow S$ be a surjective ring-homomorphism. If now R is a \star ring, then S is a \star ring, too.
- (iii) Suppose R and S are commutative rings. Then the direct sum $R \oplus S$ is a \star ring if and only if both R and S are \star rings.

(2.31) Remark:

We are about to formulate Hilbert's basis theorem. Yet in order to do this we first staighten out a few thigs for the reader who is not familiar with the notion of an *R*-algebra. Consider a commutative ring $(S, +, \cdot)$ and a subring $R \leq_{\rm r} S$ of it. Further let $E \subseteq S$ be any subset, then we introduce the *R*-subring of *S* generated by *E* to be the following

$$R[E] := \left\{ \sum_{i=1}^{m} a_i \prod_{j=1}^{n} e_{i,j} \mid m, n \in \mathbb{N}, a_i \in R, e_{i,j} \in E \right\}$$

NOTA that $0 \in R[X]$ as m = 0 and $1 \in R[E]$ as n = 0 are allowed. And thereby R[E] is a subring of S, containing R. In fact R[E] is precisely the R-subalgebra of S generated by E in the sense of section 3.2. And for those who already know the notion of polynomials in several variables this can also be put in the following form

$$R[E] = \{ f(e_1, \dots, e_n) \mid 1 \le n \in \mathbb{N}, \ f \in R[t_1, \dots, t_n], \ e_i \in E \}$$

In particular if E is a finite set - say $E = \{e_1, \ldots, e_k\}$ - we also write $R[e_1, \ldots, e_k] := R[E]$. And this is just the image of the polynomial ring $R[t_1, \ldots, t_n]$ under the evaluation homomorphism $t_i \mapsto e_i$.

(2.32) Theorem: (viz. 304) Hilbert Basis Theorem

Let $(S, +, \cdot)$ be a commutative ring and consider a subring $R \leq_{\mathrm{r}} S$. Further suppose that S is *finitely generated* (as an R-algebra) over R, that is there are finitely many $e_1, \ldots, e_n \in S$ such that $S = R[e_1, \ldots, e_n]$. If now R is a noetherian ring, then S is a noetherian ring, too

$$R$$
 noetherian $\implies S = R[e_1, \dots, e_n]$ noetherian

(2.33) Remark:

The major work in proving Hilbert's Basis Theorem lies in regarding the polynomial ring S = R[t]. The rest is just induction and (2.30.(iii)). And for this we chose a constructive proof. That is given a non-zero ideal $0 \neq \mathfrak{u} \leq_i S$ we want to find a finite set of generators of \mathfrak{u} . To do this let

$$\mathfrak{a}_k := \{ \operatorname{lc}(f) \mid f \in \mathfrak{u}, \operatorname{deg}(f) = k \} \cup \{ 0 \}$$

As \mathfrak{a}_k is an ideal of R it is finitely generated, say $\mathfrak{a}_k = \langle a_{k,1}, \ldots, a_{k,n(k)} \rangle_i$ where $a_{k,i} = f_{k,i}$ for some $f_{k,i} \in \mathfrak{u}$ with $\deg(f_{k,i} = k \text{ and } a_{k,i} = \operatorname{lc}(f_{k,i})$. Further the \mathfrak{a}_k form an ascending chain and hence there is some $s \in \mathbb{N}$ such that $\mathfrak{a}_s = \mathfrak{a}_{s+1} = \mathfrak{a}_{s+2} = \ldots$. Then a trick argument shows

$$\mathfrak{u} = \langle f_{k,1} \mid k \in 0 \dots s, \ i \in 1 \dots n(k) \rangle_{\mathbf{i}}$$

(2.34) Definition:

Let $(R, +, \cdot)$ be any commutative ring and \mathfrak{q}_{\circ} , $\mathfrak{q} \leq_{i} R$ be a prime ideals of R. Then we say that \mathfrak{q}_{\circ} lies directly under \mathfrak{q} if \mathfrak{q}_{\circ} is maximal among the prime ideals contained in \mathfrak{q} . And we abbreviate this by writing $\mathfrak{q}_{\circ} \subset_{*} \mathfrak{q}$. Formally that is

$$\begin{split} \mathfrak{q}_{\circ} \ \subset_{*} \ \mathfrak{q} & :\iff \quad \mathfrak{q}_{\circ} \in \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \subset \mathfrak{q} \}^{*} \\ & \iff \quad (1) \ \mathfrak{q}_{\circ} \in \operatorname{spec} R \text{ with } \mathfrak{q}_{\circ} \subset \mathfrak{q} \\ & (2) \ \forall \ \mathfrak{p} \in \operatorname{spec} R : \ \mathfrak{q}_{\circ} \subseteq \mathfrak{p} \subseteq \mathfrak{q} \implies \mathfrak{q}_{\circ} = \mathfrak{p} \text{ or } \mathfrak{p} = \mathfrak{q} \end{split}$$

(2.35) Proposition: (viz. 306)

Let $(R, +, \cdot)$ be a noetherian ring, then we obtain following three statements

(i) Any non-empty set of prime ideals of R contains maximal and minimal elements. That is for any $\emptyset \neq \mathfrak{p} \subseteq \operatorname{spec} R$ we get

$$\mathcal{P}_* \neq \emptyset$$
 and $\mathcal{P}^* \neq \emptyset$

(ii) In particular for any two prime ideals $\mathfrak{p}, \mathfrak{q} \leq_i R$ with $\mathfrak{p} \subset \mathfrak{q}$ there is a prime ideal \mathfrak{q}_{\circ} lying directly under \mathfrak{q} . Formally that is

$$\exists \ \mathfrak{q}_{\circ} \in \operatorname{spec} R \ : \ \mathfrak{p} \subseteq \mathfrak{q}_{\circ} \subset_{*} \mathfrak{q}$$

(iii) Let $\mathfrak{a} \leq_{i} R$ be any ideal except $\mathfrak{a} \neq R$, then there only are finitely many prime ideals lying minimally over \mathfrak{a} . Formally that is

$$1 \leq \# \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \}_* < \infty$$

(2.36) **Proposition:** (viz. ??)

Let $(R, +, \cdot)$ be an artinian ring, then we obtain following seven statements

(i) An artinian integral domain already is a field, that is the equivalence

R artinian, integral domain $\iff R$ field

(ii) Any artinian ring already is a noetherian ring, that is the implication

$$R \operatorname{artinian} \implies R \operatorname{noetherian}$$

(iii) Maximal, prime and minimal prime ideals of R all coincide, formally

 $\operatorname{smax} R = \operatorname{spec} R = \operatorname{smin} R$

(iv) R is a semilocal ring, that is it only has finitely many maximal ideals

 $\#\operatorname{smax} R < \infty$

(v) The jacobson radical and nil-radical coincide and are nilpotent, that is

JAC R = NIL R and $\exists n \in \mathbb{N} : (JAC R)^n = 0$

(vi) The reduction R/NIL R is isomorphic to the (finite) direct sum of its residue fields - to be precise we get

$$\mathbb{R}/_{\operatorname{NIL} R} \cong_{\mathrm{r}} \bigoplus_{\mathfrak{m} \in \operatorname{smax} R} \mathbb{R}/\mathfrak{m}$$

(vii) R can be decomposed into a finite number of local artinian rings. That is there are local, artinian rings L_i (where $i \in 1 \dots r := \# \operatorname{smax} R$) with

$$R \cong_{\mathbf{r}} L_1 \oplus \cdots \oplus L_r$$

(2.37) Corollary: (viz. 306)

Let $(R, +, \cdot)$ be any commutative ring, then R is the union of a net of noetherian subrings. That is there is a family (R_i) (where $i \in I$) of subrings such that the following statements hold true

- (1) $R_i \leq_{\mathbf{r}} R$ is a subring for any $i \in I$
- (2) R_i is a noetherian ring for any $i \in I$
- (3) $R = \bigcup_{i \in I} R_i$
- (4) $\forall i, j \in I \exists k \in I \text{ such that } R_i \cup R_j \subseteq R_k$

2.5 Unique Factorisation Domains

The reader most propably is aware of the fact, that any integer $n \in \mathbb{Z}$ (apart from 0) admits a decomposition into primes. In this and the next section we will study what kinds of rings qualify to have this property. We will see that neotherian integral domains come close, but do not suffice. And we will see that PIDs will allow primary decomposition. That is the truth lies somewhere in between but cannot be pinned down precisely.

According to the good, old traditions of mathematics we're in for a definition: a ring will simply said to be *factorial*, iff it allows primary decomposition (a mathematical heretic might object: "If you can't prove it, define it!"). Then PIDs are factorial. And the lemma of Gauss is one of the few answers in which cases the factorial property is preserved.

So we have to start with a lengthy series of (luckily very easy) definitions. But once we have assembled the language needed for primary decomposition we will be rewarded with several theorems of great beauty - the fundamental theorem of arithmetic at their center.

(2.38) Definition: (viz. 307)

Let $(R, +, \cdot)$ be a commutative ring and $a, b \in R$ be two elements of R. Then we say that a **divides** b (written as $a \mid b$) iff one of the following three equivalent properties is satisfied

- (a) $b \in aR$
- (b) $bR \subseteq aR$
- (c) $\exists h \in R : b = ah$

And we define the **order** of a in b to be the highest number $k \in \mathbb{N}$ such that a^k still divides b (respectively ∞ if a^k divides b for any $k \in \mathbb{N}$)

$$\langle a:b\rangle := \sup\{k \in \mathbb{N} \mid b \in a^k R\} \in \mathbb{N} \cup \{0\}$$

Now let R even be an integral domain. Then we say that a and b are **associated** (written as $a \approx b$) iff one of the following three equivalent properties is satisfied

- (a) aR = bR
- (b) $a \mid b$ and $b \mid a$
- (c) $\exists \alpha \in R^* : b = \alpha a$

(2.39) Proposition: (viz. 308)

- (i) Let $(R, +, \cdot)$ be any commutative ring then for any a, b and $c \in R$ the relation of divisibility has the following properies
 - $1 \mid b$ $a \mid 0$ $a \mid ab$ $0 \mid b \iff b = 0$ $a \mid 1 \iff a \in R^*$ $a \mid b \implies ac \mid bc$
- (ii) If a, b and $u \in R$ such that $u \in NZD R$ is a non-zero divisor of R, then we even find the following equivalence

$$a \mid b \iff au \mid bu$$

(iii) Divisibility is a reflexive, transitive relation that is antisymmetric up to associativity. Formally that is for any a, b and $c \in R$

			$a \mid a$	
a	\boldsymbol{b} and \boldsymbol{b}	$\mid c$	\Longrightarrow	$a \mid c$
$a \mid$	\boldsymbol{b} and \boldsymbol{b}	a	\implies	$a \approx b$

(iv) Let $(R, +, \cdot)$ be an integral domain, then associateness \approx is an equivalence relation on R. And for any $a \in R^*$ its equivalence class [a] under \approx is given to be aR^* . Formally that is

$$[a] = aR^* := \{ \alpha a \mid \alpha \in R^* \}$$

(2.40) Remark:

If $(R, +, \cdot)$ is an integral domain and $a, b \in R$ such that $a \neq 0$ and $a \mid b$ then the *divisor* $h \in R$ satisfying b = ah is uniquely determined. As we sometimes wish to refer to the divisor, it deserves a name of its own. Hence if R is an integral domain, $a, b \in R$ with $a \neq 0$ and $a \mid b$ we let

$$\frac{a}{b} := h$$
 such that $b = ah$

PROB we have to show the uniqueness: thus suppose b = ag and b = ah then a(g - h) = 0. And as $a \neq 0$ and R is an integral domain this yields g - h = 0 and hence g = h.

(2.41) Example:

Let $(R, +, \cdot)$ be an commutative ring and $a, b \in R$. Let us denote the ideal generated by a and b by $\mathfrak{a} := aR+bR$. Now consider any polynomial $f \in R[t]$, $1 \leq k \in \mathbb{N}$ and let $d := \deg(f)$. Then a straightforward computation yields

$$f(a)a^{k} - f(b)b^{k} = (a-b)\left(\sum_{i=0}^{d} f[i]\sum_{j=0}^{k-1+i} a^{j}b^{k-j}\right)$$

A special case of this is the third binomial rule $a^2 - b^2 = (a-b)(a+b)$ which is obtained by leting f(t) := t. Thus this cumbersome double sum on the right is the divisor of $f(a)a^k - f(b)b^k$ times a - b. And in the case of an integral domain (and $a \neq b$) this even is uniquely determined. And from the explict representation of the divisor one also finds

$$\frac{f(a)a^k - f(b)b^k}{a - b} = \sum_{i=0}^d f[i] \sum_{j=0}^{k-1+i} a^j b^{k-j} \in \mathbf{a}^{k-1}$$

(2.42) Remark:

Let $(R, +, \cdot)$ be a commutative ring, recall that we have defined the set of **relevant** elements of R to be the non-zero, non-units of R

$$R^{\bullet} := R \setminus (R^* \cup \{0\})$$

• R^{\bullet} is empty if and only if R = 0 or R is a field, that is equivalent are

$$R^{\bullet} = \emptyset \iff R = 0 \text{ or } R \text{ field}$$

PROB if R = 0 then trivially $R^{\bullet} = \emptyset$. Conversely $R^{\bullet} = \emptyset$ if and only if $R^* = R \setminus \{0\}$. And this is just the definition of R being a field.

• The complement of R^{\bullet} is multiplicatively closed (recall that this can be put as: $1 \notin R^{\bullet}$ and $a, b \notin R^{\bullet} \implies ab \notin R^{\bullet}$)

 $R \setminus R^{\bullet} = R^* \cup \{0\}$ is multiplicatively closed

PROB first of all we have $1 \in R^* \cup \{0\} = R \setminus R^{\bullet}$ (we ther R = 0 or not). Now consider $a, b \in R \setminus R^{\bullet}$. If a = 0 or b = 0 then ab = 0 and hence $ab \in R \setminus R^{\bullet}$. Else if $a, b \neq 0$ then $a, b \in R^*$ and hence $ab \in R^*$, too.

• If R is an integral domain, then R^{\bullet} is closed under multiplication, i.e.

$$R$$
 integral domain $\implies (a, b \in R^{\bullet} \implies ab \in R^{\bullet})$

PROB if $a, b \in \mathbb{R}^{\bullet}$ then $a, b \neq 0$ and hence $ab \neq 0$, as R is an integral domain. Also we get $a, b \notin \mathbb{R}^{*}$ and likewise this implies $ab \notin \mathbb{R}^{*}$ (else we had $a^{-1} = b(ab)^{-1}$ for example). Together this means $ab \in \mathbb{R}^{\bullet}$.

(2.43) Definition:

Let $(R, +, \cdot)$ be a commutative ring and $p \in R$ be an elements of R. Then p is said to be **irreducible** if p is a relevant element of R but cannot be further factored into relevant elements. Formally iff

- (1) $p \in R^{\bullet}$
- (2) $\forall a, b \in R : p = ab \implies a \in R^* \text{ or } b \in R^*$

Likewise $p \in R$ is said to be a **prime** element of R, iff it is a relevant element of R such that it divides (at least) one of the factors in every product it divides. Formally again, iff

(1) $p \in R^{\bullet}$

(2) $\forall a, b \in R : p \mid ab \implies p \mid a \text{ or } p \mid b$

(2.44) Definition:

Let $(R, +, \cdot)$ be a commutative ring and $a \in R$ and let \star abbreviate either the word *prime* or the word *irreducible*. Then a tupel $(\alpha, p_1, \ldots, p_k)$ (with $k \in \mathbb{N}$ and k = 0 allowed!) is said to be a \star **decomposition** of a, iff

- (1) $\alpha \in R^*$
- (2) $a = \alpha p_1 \dots p_k$
- (3) $\forall i \in 1 \dots n : p_i \in R \text{ is } \star$

If $(\alpha, p_1, \ldots, p_k)$ at least satisfies (1) and (3) then let us agree to call it a \star series. Now two \star series $(\alpha, p_1, \ldots, p_k)$ and $(\beta, q_1, \ldots, q_l)$ are said to be essentially equal (written as $(\alpha, p_1, \ldots, p_k) \approx (\beta, q_1, \ldots, q_l)$), iff k = l, both decompose the same element and the p_i and q_i are pairwise associated. Formally that is $(\alpha, p_1, \ldots, p_k) \approx (\beta, q_1, \ldots, q_l)$: \iff (1), (2) and (3) where

- (1) k = l
- (2) $\alpha p_1 \dots p_k = \beta q_1 \dots q_l$
- (3) $\exists \sigma \in S_k : \forall i \in 1 \dots k : p_i \approx q_{\sigma(i)}$

(2.45) Example: (\diamondsuit)

Let $(R, +, \cdot)$ be an integral domain and $a \in R$, then the linear polynomial $p(t) := t - a \in R[t]$ is prime. Note that this need not be true unless R is an integral domain. E.g. for $R = \mathbb{Z}_6$ we have

$$t-1 = (2t+1)(3t-1)$$
 but $t-1/2t+1, t-1/3t-1$

PROB consider $f, g \in R[t]$ such that $p \mid fg$. that is there is some $h \in R[t]$ such that (t-a)h = fg. In particular f(a)g(a) = (fg)(a) = (a-a)h(a) = 0. As R is an integral domain this means f(a) = 0 or g(a) = 0. And from this again we get $p = t - a \mid f$ or $p = t - a \mid g$.

(2.46) Definition:

• Let $(R, +, \cdot)$ be a commutative ring again and $\emptyset \neq A \subseteq R$ be a nonempty subset of R. Then we say that $m \in R$ is a **common multiple** of A, iff every $a \in A$ divides m, formally

$$A \mid m :\iff \forall a \in A : a \mid m$$

- And thereby *m* is said to be a **least common multiple** of *A*, iff *m* is a common multiple that divides any other common multiple
 - (1) $A \mid m$
 - $(2) \ \forall n \in R : A \mid n \implies m \mid n$

And we denote the set of least common multiples of A by lcm(A) i.e.

$$lcm(A) := \{ m \in R \mid (1) \text{ and } (2) \}$$

• Analogous to the above we say that an element $d \in R$ is a **common** divisor of A, iff d divides every $a \in A$, formally again

$$d \mid A :\iff \forall a \in A : d \mid a$$

- And thereby d is said to be a greatest common divisor of A, iff d is a common divisor that is divided by any other common divisor
 - (1) $d \mid A$ (2) $\forall c \in R : c \mid A \implies c \mid d$

And we denote the set of greatest common divisors of A by gcd(A) i.e.

$$gcd(A) := \{ d \in R \mid (1) \text{ and } (2) \}$$

• Finally A is said to **relatively prime**, iff 1 is a greatest common divisor of A. And by (2.39) this can also be formulated, as

$$\begin{array}{rcl} A \mbox{ relatively prime} & :\Longleftrightarrow & 1 \in \gcd(A) \\ & \Leftrightarrow & \forall c \in R \ : \ c \ \mid A \implies c \in R^* \end{array}$$

By abuse of notation a finite family of elements $a_1, \ldots, a_k \in R$ is said to be *relatively prime*, iff the set $\{a_1, \ldots, a_k\}$ is relatively prime.

(2.47) Proposition: (viz. 308)

(i) Let $(R, +, \cdot)$ be a commutative ring, $p \in R$ be a prime element and $a_1, \ldots, a_k \in R$ be arbitrary elements of R. Then we obtain

$$p \mid \prod_{i=1}^{k} a_i \implies \exists i \in 1 \dots k : p \mid a_i$$

(ii) Let $(R, +, \cdot)$ be a commutative ring and $p \in R$. Then p is a prime element iff $p \neq 0$ and the principal ideal $pR \leq_i R$ is a prime ideal

 $p \in R$ prime $\iff p \neq 0$ and $pR \leq_{i} R$ prime

 (iii) Let (R, +, ·) be a commutative ring, p ∈ R and α ∈ R* a unit of R. Let us again abbreviate the word prime or irreducible by ★, then

 $p \text{ is } \star \iff \alpha p \text{ is } \star$

(iv) Let $(R, +, \cdot)$ be an integral domain $0 \neq a \in R$ and $b \in R^{\bullet}$ be a non-zero non-unit. Then we obtain the following strict inclusion of ideals

 $(ab)R \subset aR$

(v) Let $(R, +, \cdot)$ be an integral domain. Then any prime element of R already is irreducible. That is for any $p \in R$ we get

 $p \text{ is prime} \implies p \text{ is irreducible}$

(vi) Let $(R, +, \cdot)$ be an integral domain. Then the set D of all $d \in R$ that allow a prime decomposition is saturated and multiplicatively closed. That is $D := \{\alpha p_1 \dots p_k \mid \alpha \in R^*, k \in \mathbb{N}, p_i \in R \text{ prime}\}$ satisfies

$$\begin{array}{rcl} 1 & \in & D \\ c, d \in D & \Longleftrightarrow & cd \in D \end{array}$$

(vii) Let $(R, +, \cdot)$ be an integral domain, $p_1, \ldots, p_k, q_1, \ldots, q_l \in R$ be a finite collection of prime elements of R (where $k, l \in \mathbb{N}$ with k = 0 and l = 0 allowed) and $\alpha, \beta \in R^*$ be two units of R. Then we obtain

$$\alpha p_1 \dots p_k = \beta q_1 \dots q_l \implies k = l \text{ and } \exists \sigma \in S_k \text{ such that} \\ \forall i \in 1 \dots k : p_i \approx q_{\sigma(i)}$$

(viii) Let $(R, +, \cdot)$ be an integral domain and $\emptyset \neq A \subseteq R$ be a non-empty subset of R. Further let $d, m \in R$ be two elements of R, then

$$m \in \operatorname{lcm}(A) \iff \operatorname{lcm}(A) = mR^*$$
$$d \in \operatorname{gcd}(A) \iff \operatorname{gcd}(A) = dR^*$$

(2.48) Theorem: (viz. 311)

Let $(R, +, \cdot)$ be a noetherian integral domain and fix some elements a, b and $p \in R$ where p is prime. Then we obtain the following statements

(i) If $a \in \mathbb{R}^{\bullet}$ then the order in which a divides b is finite, formally that is

$$\langle a:b\rangle \in \mathbb{N}$$

(ii) The order of a prime element $p \in R$ turns multiplications into additions

$$\langle p:ab \rangle = \langle p:a \rangle + \langle p:b \rangle$$

(iii) Any $a \neq 0$ admits an irreducible decomposition. That is there are some $\alpha \in R^*$ and finitely many irreducibles $p_1, \ldots, p_k \in R$ such that

$$a = \alpha p_1 \dots p_k$$

(iv) If $0 \neq \mathfrak{p} \leq_{i} R$ is any prime ideal of R then \mathfrak{p} is generated by finitaly many irreducibles. That is there are $p_1, \ldots, p_k \in R$ irreducible with

$$\mathfrak{p} = \langle p_1, \ldots, p_k \rangle_{\mathbf{i}}$$

(v) Let $P \subseteq R^{\bullet}$ be a set of parwise non-associate non-zero non-units of R. That is we assume that for any $p, q \in P$ we get $p \approx q \implies p = q$. Then for any $a \neq 0$ the number of $p \in P$ that divide a is finite, i.e.

$$\# \{ p \in P \mid a \in pR \} < \infty$$

(vi) Let $b \in R^{\bullet}$ be a non-zero, non-unit of R. Further consider a finite collection $q_1, \ldots, q_k \in R$ of prime elements of R that are pairwise non-associate. That is for any $i, j \in 1 \ldots k$ we assume

$$q_i \approx q_j \implies i = j$$

If now $p \in R$ is any prime element of R then we obtain the statements

$$a := \prod_{i=1}^{k} q_i^{\langle q_i:b\rangle} \mid b$$
$$p \mid b \implies p \mid \frac{b}{a} \quad \text{xor} \quad \exists i \in 1 \dots k : p \approx q_i$$

(2.49) Definition: (viz. 314)

We call $(R, +, \cdot)$ an **unique factorisation domain** (which we will always abbreviate by **UFD**), iff R is an integral domain that further satisfies one of the following equivalent properties

(a) Every non-zero element admits a decomposition into prime elements. That is for any $0 \neq a \in R$ we get the following statement

$$\exists (\alpha, \mathbf{p}) = (\alpha, p_1, \dots, p_k)$$
 prime decomposition of a

- (b) Every non-zero element admits an essentially unique decomposition into irreducible elements. That is for any $0 \neq a \in R$ we have
 - (1) $\exists (\alpha, \mathbf{p}) = (\alpha, p_1, \dots, p_k)$ irreducible decomposition of a
 - (2) $(\alpha, \mathbf{p}), (\beta, \mathbf{q})$ irreducible decompositions of $a \implies (\alpha, \mathbf{p}) \approx (\beta, \mathbf{q})$
- (c) Every non-zero element admits a decomposition into irreducible elements and every irreducible element is prime. Formally that is
 - (1) $\forall 0 \neq a \in R \ \exists (\alpha, \mathbf{p})$ irreducible decomposition of a
 - (2) $\forall p \in R : p \text{ prime} \iff p \text{ irreducible}$
- (d) The principal ideals of R satisfy the ascending chain condition and every irreducibe element is prime, Formally that is
 - (1) for any family of elements $a_k \in R$ (where $k \in \mathbb{N}$) of R such that $a_0R \subseteq a_1R \subseteq \ldots \subseteq a_kR \subseteq a_{k+1}R \subseteq \ldots$ there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $a_{s+i}R = a_sR$.
 - (2) $\forall p \in R : p$ prime $\iff p$ irreducible
- (e) Any non-zero prime ideal of R contains a prime element of R, formally

$$\forall 0 \neq \mathfrak{p} \in \operatorname{spec} R \ \exists p \in P \text{ prime } : p \in \mathfrak{p}$$

(f) (\diamond) Let $D := \{\alpha p_1 \dots p_k \mid \alpha \in R^*, k \in \mathbb{N}, p_i \in R \text{ prime}\}$ denote the set of all $d \in R$ that allow a prime decomposition again. Then either R = 0 is the zero ring or the quotient field of R is precisely the localisation of R in D, formally

QUOT
$$R = D^{-1}R$$

(2.50) Remark:

- The zero-ring R = 0 trivially is an UFD. As it does not contain a single non-zero element such that condition (a) of UFDs is void (hence true).
- Property (b) guarantees that in an UFD $(R, +, \cdot)$ any nonzero element $0 \neq a \in R$ admits an irreducible (equivalently prime) decomposition $a = \alpha p_1 \dots p_k$, that even is essentially unique. And this uniqueness determines the number k of irreducible factors. Hence we may define the **length** of a to be precisely this number

 $\ell(a) := k$ where $(\alpha, p_1, \dots, p_k)$ prime decomposition of a

- Any field $(E, +, \cdot)$ is an UFD, as we allowed k = 0 for a prime decomposition $(\alpha, p_1, \ldots, p_k)$. To be precise if $0 \neq a \in E$ then $a \in E^*$ already is a unit and hence (a) is a prime decomposition of a.
- In the next section we will prove that any PID (i.e. an integral domain in which every ideal can be generated by a single element) is an UFD.
- If $(R, +, \cdot)$ is a noetherian integral domain in which any irreducible element is prime, then R is an UFD. This is clear from property (d).
- If $(R, +, \cdot)$ is an UFD then so is the polynomial ring R[t] (this is the one of the lemmas of Gauss that will be proved in (??)).
- (\diamond) If $(R, +, \cdot)$ is an UFD and $U \subseteq R$ is multiplicatively closed, then $U^{-1}R$ is an UFD too. In fact, if $p \in R$ is a prime element then p/1 either is a unit or a prime in $U^{-1}R$. This will be proved in (2.109).
- (\diamond) A subring $\mathcal{O} \leq_{\mathbf{r}} \mathbb{C}$ of the complex numbers is said to be an *algebraic number ring*, iff any $a \in \mathcal{O}$ satisfies an integral equation over \mathbb{Z} (that is there is a normed polynomial $f \in \mathbb{Z}[t]$ such that f(a) = 0). We will see that any algebraic number ring \mathcal{O} is a Dedekind domain. And it is also true, that \mathcal{O} is an UFD if and only if it is a PID.
- This list of UFDs is almost exhaustive. At the end of this section we will append a list of counter examples such that the reader may convince himself that the above equivalencies cannot be generalized.

(2.51) Remark:

It is oftenly useful not to regard all the prime (analogously irreducible) elements of R but to restrict to a representant set modulo associateness. That is a subset $\mathbb{P} \subseteq R$ such that we obtain a bijection of the form

$$\mathbb{P} \longleftrightarrow \{ p \in R \mid p \text{ prime} \}_{\sim} : p \mapsto pR^*$$

PROB this is possible since \approx is an equivalence relation on R of which the equivalence classes are precisely aR^* by (2.39). In particular \approx also is on equivalence relation on the subset P of prime elements of R. And by (2.47) we know that for any $p \in P$ we have $[p] = \{q \in P \mid p \approx q\} = pR^*$ again. Hence we may choose \mathbb{P} as a representing system of P/\approx by virtue of the axiom of choice.

(2.52) Example:

• The units of the integers \mathbb{Z} are given to be $\mathbb{Z}^* = \{-1, +1\}$. That is associateness identifies all elements having the same absolute value, $a\mathbb{Z}^* = \{-a, a\}$. And thereby we can choose a representing system of \mathbb{Z} modulo \approx simply by choosing all *positive* elements $a \ge 0$. Thus we find a representing system of the prime elements of \mathbb{Z} by

$$\mathbb{P} := \{ p \in \mathbb{Z} \mid p \text{ prime, } 0 \le p \}$$

• (\diamond) Now let $(E, +, \cdot)$ be any field and consider the polynomial E[t]. Then we will see that the units of E[t] are given to be $E[t]^* = E^* = \{at^0 \mid 0 \neq a \in E\}$. Thus associateness identifies all polynomials having the same coefficients up to a common factor. That is we get $fE[t]^* = \{af \mid 0 \neq a \in E\}$. Thus by requiring a polynomial f to be normed (i.e. $f[\deg(f)] = 1$) we eliminate this ambiguity. Therefore we find a representing system of the prime elements of E[t] by

$$\mathbb{P} := \{ p \in E[t] \mid p \text{ prime, normed} \}$$

(2.53) Theorem: (viz. 315)

Let $(R, +, \cdot)$ be an UFD, $p \in R$ be a prime element and $0 \neq a, b \in R$ be any two non-zero elements. Then the following statements hold true

(i) Suppose $(\alpha, p_1, \ldots, p_k)$ is a prime decomposition of a. Then for any prime $p \in R$ the order of p in a can be expressed as

$$\langle p:a\rangle = \#\{i \in 1\dots k \mid p \approx p_i\} \in \mathbb{N}$$

(ii) The order of a prime element $p \in R$ turns multiplications into additions

$$\langle p:ab \rangle = \langle p:a \rangle + \langle p:b \rangle$$

(iii) a divides b if and only if for any prime p the order of p in a does not exceed the order of p in b. Formally that is the equivalence

 $a \mid b \iff \forall p \in R \text{ prime} : \langle p : a \rangle \leq \langle p : b \rangle$

(iv) Let \mathbb{P} be a representing system of the prime elements modulo associateness. Then for any $0 \neq a \in R$ we obtain a unique representation

$$\exists ! \ \alpha \in R^* \ \exists ! \ n = (n(p)) \in \bigoplus_{p \in \mathbb{P}} \mathbb{N} \ : \ a = \alpha \prod_{p \in \mathbb{P}} p^{n(p)}$$

and thereby we even have $n(p) = \langle p : a \rangle$ such that the sum of all n(p) is precisely the length of a (and in particular finite). Formally that is

$$\ell(a) = \sum_{p \in \mathbb{P}} n(p) < \infty$$

NOTA that $n \in \bigoplus_p \mathbb{N}$, that is $n : \mathbb{P} \to \mathbb{N}$ is a map such that the number of $p \in \mathbb{P}$ with $n(p) \neq 0$ is finite. And hence the product over all $p^{n(p)}$ (where $p \in \mathbb{P}$) well-defined using the notations of section 1.2.

(v) Let \mathbb{P} be a representing system of the prime elements modulo associateness again. And consider a non-empty subset $\emptyset \neq A \subseteq R$ such that $0 \notin A$. Then A has a greatest common divisor, namely

$$\prod_{p \in \mathbb{P}} p^{m(p)} \in \gcd(A) \quad \text{where} \quad m(p) := \min\{ \langle p : a \rangle \mid a \in A \}$$

Likewise if $A = \{a_1, \ldots, a_n\} \subseteq R$ is a non-empty, finite $(1 \leq n \in \mathbb{N})$ subset with $0 \notin A$ then A has a least common multiple, namely

$$\prod_{p \in \mathbb{P}} p^{n(p)} \in \operatorname{lcm}(A) \quad \text{where} \quad n(p) := \max\{ \langle p : a \rangle \mid a \in A \}$$

(vi) Let $A := \{a, b\}$ and $d \in gcd(A)$ be a greatest common divisor, $m \in lcm(A)$ a least common multiple of a and b. Then we obtain

$$ab \approx dm$$

(vii) If $0 \neq a, b, c \in R$ are any three non-zero elements of R, then the least common multiple and greatest common divisor of these can be evaluated recursively. That is if $d \in \gcd\{a, b\}$ and $m \in \operatorname{lcm}\{a, b\}$ then

$$gcd \{ a, b, c \} = gcd \{ d, c \}$$
$$lcm \{ a, b, c \} = gcd \{ m, c \}$$

(2.54) Proposition: (viz. 318) (\diamondsuit)

Any UFD R is normal. Thereby a commutative ring $(R, +, \cdot)$ is said to be **normal** (or **integrally closed**), iff R is an integral domain that is integrally closed in its quotient field. That is R is normal, iff

- (1) R is an integral domain
- (2) for any $a, b \in R$ with $a \neq 0$ get: if there is some normed polynomial $f \in R[t]$ such that $f(b/a) = 0 \in \text{QUOT } R$, then we already had $a \mid b$.

(2.55) Example: (viz. 318)

- (i) UFDs need not be noetherian! As an example regard a field $(E, +, \cdot)$, then the polynomial ring in countably many variables $E[t_i \mid i \in \mathbb{N}]$ is an UFD by the lemma of Gauss (??)). But it is not noetherian (by the examples in section 2.4).
- (ii) Noetherian integral domains need not be UFDs! As an example we would like to present the following algebraic number ring

$$\mathbb{Z}[\sqrt{-3}] := \left\{ a + ib\sqrt{3} \mid a, b \in \mathbb{Z} \right\} \subseteq \mathbb{C}$$

It is quite easy to see that in this ring $2 \in \mathbb{Z}[\sqrt{-3}]$ is an irreducible element, that is not prime. Hence $\mathbb{Z}[\sqrt{-3}]$ cannot be an UFD. Never the less it is an integral domain (being a subring of \mathbb{C}) and noetherian (by Hilbert's basis theorem (2.32), as it is generated by $\sqrt{-3}$ over \mathbb{Z}).

(iii) Residue rings (even integral domains) of UFDs need not be UFDs! As an example let us start with the polynomial ring $\mathbb{R}[s, t]$ in two variables over the reals. Then $\mathbb{R}[s, t]$ is an UFD by the lemma of Gauss (??). Now consider the residue ring

$$R := \frac{\mathbb{R}[s,t]}{\mathfrak{p}}$$
 where $\mathfrak{p} := (s^2 + t^2 - 1)R[s,t]$

Then $p(s,t) = s^2 + t^2 - 1 \in \mathbb{R}[s,t]$ is an irreducible (hence prime) polynomial, such that \mathfrak{p} is a prime ideal. Yet we are able to prove that R is no UFD (in fact we will prove that there is an irreducible, non-prime element in a certain localisation of R).

2.6 Principal Ideal Domains

(2.56) Definition:

Let $(R, +, \cdot)$ be an integral domain and ν be a mapping of the following form

 $\nu : R \setminus \{0\} \to \mathbb{N} \cup \{-\infty\}$

Then the ordered pair (R, ν) is said to be an **Euclidean domain**, iff R allows *division with remainder* - that is for any $a, b \in R$ with $a \neq 0$ there are $q, r \in R$ such that we get

(1) b = qa + r

(2)
$$\nu(r) < \nu(a) \text{ or } r = 0$$

(2.57) Remark:

• We will employ a notational trick to eliminate the distinction of the case r = 0 in the definition above. To do this we pick up a symbol $-\infty$ and set $-\infty < n$ for any $n \in \mathbb{N}$. Then ν will be extended to

$$\nu : R \to \mathbb{N} \cup \{-\infty\} : a \mapsto \begin{cases} \nu(a) & \text{if } a \neq 0\\ -\infty & \text{if } a = 0 \end{cases}$$

Thereby the property to allow division with remainder simply reads as: for any $a, b \in R$ with $a \neq 0$ there are $q, r \in R$ such that we get

- (1) b = qa + r
- (2) $\nu(r) < \nu(a)$
- If (R, ν) is an euclidean domain and $a \in R$ satisfies $\nu(a) = 0$, then $a \in R^*$ already is a unit of R. The converse need not be true however. That is we have the incluison (but not necessarily equality)

$$\{a \in R \mid \nu(a) = 0\} \subseteq R^*$$

PROB using division with remainder we may find $q, r \in R$ such that 1 = qa + r and $\nu(r) < \nu(a) = 0$. But this can only be if $\nu(r) = -\infty$ and hence r = 0. But this means 1 = qa again and hence $a \in R^*$.

(2.58) Example: (viz. 321)

(i) If $(E, +, \cdot)$ is a field, then (E, ν) is an Euclidean domain under any function $\nu : E \setminus \{0\} \to \mathbb{N}$. Because for any $0 \neq a \in E$ and $b \in E$ we may let $q := ba^{-1}$ and r := 0.

(ii) The ring Z of integers is an Euclidean domain (Z, α) under the (slightly modified) absolute value α as an Euclidean function

$$\alpha \ : \ \mathbb{Z} \to \mathbb{N} \cup \{ -\infty \} \ : \ k \mapsto \begin{cases} a & \text{if } a > 0 \\ -a & \text{if } a < 0 \\ -\infty & \text{if } a = 0 \end{cases}$$

In fact consider $1 \leq a \in \mathbb{Z}$ and any $b \in \mathbb{Z}$ then for q := b div a and $r := b \mod a$ (see below for a definition) we have b = aq + r and $0 \leq r < a$ (in particular $\alpha(r) < \alpha(a)$). And in case a < 0 we can choose q and r similarly to have division with remainder.

$$b \operatorname{div} a := \max\{q \in \mathbb{Z} \mid aq \le b\}$$
$$b \operatorname{mod} a := b - (b \operatorname{div} a) \cdot a$$

(iii) If $(E, +, \cdot)$ is a field then the polynomial ring E[t] (in one variable) is an Euclidean domain $(E[t], \deg)$ under the *degree*

$$\deg : E[t] \setminus \{0\} : f \mapsto \max\{k \in \mathbb{N} \mid f[k] \neq 0\}$$

This is true because of the division algorithm for polynomials - see (??). Note that the division algorithm can be applied as any non-zero polynomial can be normed, since E is a field. Hence R[t] will not be a Euclidean ring, unless R is a field. Also, though the division algorithm for polynomials can be generalized to Buchberger's algorithm it is *untrue* that the polynomial ring $E[t_1, \ldots, t_n]$ is an Euclidean domain (for $n \geq 2$) under some Euclidean function ν .

(iv) Consider any $d \in \mathbb{Z}$ such that $\sqrt{d} \notin \mathbb{Q}$ (refer to (??) for this). Then we consider the subring of \mathbb{C} generated by \sqrt{d} , that is we regard

$$\mathbb{Z}[\sqrt{d}] \hspace{2mm} := \hspace{2mm} \left\{ \hspace{2mm} a + b \sqrt{d} \mid a, b \in \mathbb{Z} \hspace{2mm} \right\} \hspace{2mm} \subseteq \hspace{2mm} \mathbb{C}$$

Then the representation $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is unique (that is for any a, b, f and $g \in \mathbb{Z}$ we get $a + b\sqrt{d} = f + g\sqrt{d} \iff (a, b) = (f, g)$). And thereby we obtain a well-defined ring-automorphism on $\mathbb{Z}[\sqrt{d}]$ by virtue of $x = a + b\sqrt{d} \mapsto \overline{x} := a - b\sqrt{d}$. Now define

$$\nu : \mathbb{Z}[\sqrt{d}] \setminus \{0\} \to \mathbb{N} : x = a + b\sqrt{d} \mapsto |x\overline{x}| = |a^2 - db^2|$$

Then ν is multiplicative, that is $\nu(xy) = \nu(x)\nu(y)$ for any $x, y \in \mathbb{Z}[\sqrt{d}]$. And it is quite easy to see that the units of $\mathbb{Z}[\sqrt{d}]$ are given to be

$$\mathbb{Z}[\sqrt{d}]^* = \left\{ x \in \mathbb{Z}[\sqrt{d}] \mid \nu(x) = 1 \right\}$$

We will also prove that for $d \leq -3$ the ring $\mathbb{Z}[\sqrt{d}]$ will not be an UFD, as 2 is an irreducible element, that is not prime. Yet for $d \in \{-2, -1, 2, 3\}$, we find that $(\mathbb{Z}[\sqrt{d}], \nu)$ even is an Euclidean domain.

(2.59) Proposition: (viz. 323)

Let (R, ν) be an Euclidean domain and $0 \neq a, b \in R$ be two non-zero elements. Then a and b have a greatest common divisor $g \in R$ that can be computed by the following (so called *Euclidean*) algorithm

```
 \begin{array}{lll} \text{input} & 0 \neq a, \, b \in R \\ \text{initialisation} & \text{if } \nu(a) \leq \nu(b) \\ & \text{then } (f := a, \, g := b) \\ & \text{else } (f := b, \, g := a) \\ \text{algorithm} & \text{while } f \neq 0 \text{ do begin} \\ & \text{choose } q, \, r \in R \text{ with} \\ & (g = qf + r \text{ and } \nu(r) < \nu(f)) \\ & g := f, \, f := r \\ & \text{end} \\ \text{output} & g \\ \end{array}
```

That is given $0 \neq a, b \in R$ we start the above algorithm that returns $g \in R$ and for this g we get $g \in \gcd\{a, b\}$. If now g denotes the greatest common divisor $g \in \gcd\{a, b\}$ of a and b, then there are r and $s \in R$ such that g = ra + sb. And these r and s can be computed (along with g) using the following refinement of the *Euclidean algorithm*

```
0 \neq a, b \in R
input
                  if \nu(a) \leq \nu(b)
initialisation
                   then (f_1 := b, f_2 := a)
                   else (f_1 := a, f_2 := b)
algorithm
                   k := 1
                   repeat
                       k := k + 1
                       choose q_k, f_{k+1} \in R with
                       (f_{k-1} = q_k f_k + f_{k+1} \text{ and }
                       \nu(f_{k+1}) < \nu(f_k))
                   until f_{k+1} = 0
                   n := k, g := f_n
                   r_2 := 1, s_2 := 0
                   r_3 := -q_2, s_3 := 1
                   for k := 3 to n - 1 do begin
                       r_{k+1} := r_{k-1} - q_k r_k
                       s_{k+1} := s_{k-1} - q_k s_k
                   end
                   if \nu(a) \leq \nu(b)
                   then (r := r_n, s := s_n)
                   else (r := s_n, s := r_n)
                   g, r \text{ and } s
output
```

(2.60) Example:

As an application we want to compute the greatest common divisor of a = 84and b = 1330 in Z. That is we initialize the algorithm with $f_1 := b = 1330$ and $f_2 := a = 84$. Then we find $1330 = 15 \cdot 84 + 70$ (at k = 2), which is $q_2 = 15$ and $f_3 = 70$. Thus in the next step (now k = 3) we observe $84 = 1 \cdot 70 + 14$, that is we may choose $q_3 := 1$ and $f_4 := 14$. Now (at counter k = 4) we have $70 = 5 \cdot 14 + 0$ which means $q_4 = 5$ and $f_5 = 0$. Thus for n := k = 4 we have finally arrived at $f_{k+1} = 0$ terminating the first part of the algorithm. It returns $g = f_n = 14$ the greatest common divisor of a = 84 and b = 1330. The following table summarizes the computations

k	f_{k-1}	f_k	f_{k+1}	q_k
2	1330	84	70	15
3	84	70	14	1
4	70	14	0	5

Now in the second part of the algorithm we initialize $r_2 := 1$, $s_2 := 0$, $r_3 := -q_2 = -15$ and $s_3 := 1$. Then we compute $r_4 := r_2 - q_3 r_3 = 16$ and $s_4 := s_2 - q_3 s_3 = -1$. As n = 4 this already is $r = r_4 = 16$ and $s = s_4 = -1$. And in fact $r_4 + b_5 = 14 = g$. Again we summarize these computations in

(2.61) Proposition: (viz. 325)

Consider an integral domain $(R, +, \cdot)$ and $n \in \mathbb{N}$, then we recursively define

$$R_0 := R^* = \{ a \in R \mid \exists b \in R : ab = 1 \}$$

$$R_{n+1} := \{ 0 \neq a \in R \mid \forall b \in R \exists r \in R_n \cup \{ 0 \} : a \mid b - r \}$$

(i) The sets R_n form an ascending chain of subsets of R, i.e. for any $n \in \mathbb{N}$

 $R_0 \subseteq R_1 \subseteq \ldots \subseteq R_n \subseteq R_{n-1} \subseteq \ldots$

(ii) If $R(,\nu)$ is an Euclidean domain that for any $n \in \mathbb{N}$ the set of $a \in R$ with $a \neq 0$ and $\nu(a) \leq n$ is contained in R_n , formally that is

$$\{a \in R \mid \nu(a) \le n\} \subseteq R_n \cup \{0\}$$

(iii) Conversely if the R_n cover R, that is $R \setminus \{0\} = \bigcup_n R_n$, then (R, μ) becomes an Euclidean domain under the following Euclidean function

$$\mu : R \setminus \{0\} : a \mapsto \min\{n \in \mathbb{N} \mid a \in R_n\}$$

And thereby we obtain the following statements for any $a, b \in R, b \neq 0$

$$\mu(a) \leq \mu(ab)$$
$$\mu(b) = \mu(ab) \iff a \in R^*$$

(iv) In particular we obtain the equivalency of the following two statements

$$R \setminus \{0\} = \bigcup_{n \in \mathbb{N}} R_n \iff \exists \nu : (R, \nu)$$
 Euclidean domain

(v) If $R(,\nu)$ is an Euclidean domain, then (R,μ) is an Euclidean domain, too and for any $a \in R$ we get $\mu(a) \leq \nu(a)$. That is μ is the minimal Euclidean function on R.

(2.62) Definition:

Let $(R, +, \cdot)$ be any commutative ring, then an ideal $\mathfrak{a} \leq_i R$ is said to be **principal**, iff it can be generated by a single element, i.e. $\mathfrak{a} = aR$ for some $a \in R$. And R is said to be a **principal ring** iff every ideal of R is principal, that is iff

$$\forall \mathfrak{a} \leq_{\mathrm{i}} R \exists a \in R : \mathfrak{a} = aR$$

Finally R is said to be a b**principal ideal domain** (which we will always abbreviate by **PID**), iff it is an integral domain that also is principal, i.e.

- (1) R is an integral domain
- (2) R is a principal ring

(2.63) Remark:

- Clearly the trivial ideals $\mathfrak{a} = 0$ and $\mathfrak{a} + R$ are always principal, as they can be generated by the elements 0 = 0R and R = 1R respectively.
- If R is a principal ring and $\mathfrak{a} \leq_{i} R$ is any ideal, then the quotient ring R/\mathfrak{a} is principal, too. PROB due to the correspondence theorem (1.43) any ideal $\mathfrak{u} \leq_{i} R/\mathfrak{a}$ is of the form $\mathfrak{u} = \mathfrak{b}/\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq \mathfrak{b} \leq_{i} R$. Thus there is some $b \in R$ with $\mathfrak{b} = bR$. Now let $u := b + \mathfrak{a}$, then clearly $\mathfrak{u} = \{bh + \mathfrak{a} \mid h \in R\} = u(R/\mathfrak{a})$ is a principal ideal, too.
- Let R_1, \ldots, R_n be principal rings, then the direct sum $R_1 \oplus \cdots \oplus R_n$ is a principal ring, too. PROB by (1.60) the ideals of the direct sum are of the form $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ for some ideals $\mathfrak{a}_i \leq i_i R_i$. Thus by assumption there are some $a_i \in R_i$ such that $\mathfrak{a}_i = a_i R_i$. And thereby it is clear, that $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n = (a_1, \ldots, a_n)R_1 \oplus \cdots \oplus R_n$ is principal again.

(2.64) Lemma: (viz. 326)

(i) If $(R, +, \cdot)$ is a non-zero PID then all non-zero prime ideals of R already are maxmial (in a fancier notation kdim $R \leq 1$), formally that is

spec $R = \operatorname{smax} R \cup \{0\}$

- (ii) If $(R, +, \cdot)$ is a PID then R already is a noetherian ring and an UFD. That is any $0 \neq a \in R$ admits an (essentially uniqe) decomposition $a = \alpha p_1 \dots p_k$ into prime elements p_i - viz. (2.49).
- (iii) If (R, ν) is an Euclidean domain then R already is a PID. In fact if $0 \neq \mathfrak{a} \leq_{i} R$ is a non-zero ideal then $\mathfrak{a} = aR$ for any $a \in \mathfrak{a}$ satisfying

 $\nu(a) = \min\{\nu(b) \mid 0 \neq b \in \mathfrak{a}\}$

(iv) If $(R, +, \cdot)$ is an integral domain such that any prime ideal is principal, then R already is a PID. Put formally that is the equivalency

$$R \text{ PID} \iff \forall \mathfrak{p} \in \operatorname{spec} R \exists p \in R : \mathfrak{p} = pR$$

(2.65) Remark:

- In (2.58.(i)) we have seen that any field E is an Euclidean domain (under any ν). Hence any field is a PID due to (iii) above. But this is also clear from the fact that the only ideals of a field E are 0 and E itself. And these are principal due to 0 = 0E and E = 1E. Also (i) is trivially satisfied: the one and only prime ideal of a field is 0.
- The items (i) and (ii) in the above lemma are very useful and will yield a multitude of corollaries (e.g. the lemma of Kronecker that will give birth to field theory in book II). And (iii) provides one of the reasons why we have introduced Euclidean domains: combining (iii) and (ii) we see that any Euclidean domain is an UFD. And this yields an elegant way of proving that a certain integral domain R is an UFD. Just establish an Euclidean function ν on R and voilà R is an UFD.
- Due to example (2.58.(ii)) we know that (\mathbb{Z}, α) is an Euclidean domain. By (iii) above this means that \mathbb{Z} is a PID and (ii) then implies that \mathbb{Z} is an UFD. By definition of UFDs this means that \mathbb{Z} allows essentially unique prime decomposition. This now is a classical result that is known as the *Fundamental Theorem of Arithmetic*. We have proved an even stronger version, namely

 (R, ν) Euclidean domain \implies R is an UFD

• In the subsequent proposition we will discuss how far a PID deviates from being an Euclidean domain (though this is of little practical value). To do this we will introduce the notion of a Dedekind-Hasse norm. We will then see that an Euclidean function can be easily turned into a Dedekind-Hasse norm and that R is a PID if and only if it admits a Dedekind-Hasse norm. This of course is another way of proving that any Euclidean domain is a PID.

(2.66) Proposition: (viz. 327)

- (i) If $(R, +, \cdot)$ is a PID then R admits a multiplicative Dedekind-Hasse norm. That is there is a function $\delta : R \to \mathbb{N}$ satisfying the following three properties for any $a, b \in R$
 - (1) $\delta(ab) = \delta(a)\delta(b)$
 - (2) $\delta(a) = 0 \iff a = 0$
 - (3) if $a, b \neq 0$ then $b \in aR$ or $\exists r \in aR + bR$ such that $\delta(r) < \delta(a)$

NOTA to be precise we may define $\delta(0) := 0$ and for any $0 \neq a \in R$ we let $\delta(a) := 2^k$ for $k := \ell(a)$ the length of any decomposition of $a = \alpha p_1 \dots p_k$ into prime elements.

(ii) If $(R, +, \cdot)$ is an integral domain and δ is a Dedekind-Hasse norm on R (that is $\delta : R \to \mathbb{N}$ is a function satisfying (2) and (3) in (i)), then R already is a PID. In fact if $0 \neq \mathfrak{a} \leq_{\mathbf{i}} R$ is a non-zero ideal then we get $\mathfrak{a} = aR$ for any $0 \neq a \in \mathfrak{a}$ satisfying

$$\delta(a) = \min\{\,\delta(b) \mid 0 \neq b \in \mathfrak{a}\,\}$$

(iii) If (R, ν) is an Euclidean domain then we obtain a Dedekind-Hasse norm on R (that is $\delta : R \to \mathbb{N}$ satisfies (2) and (3) in (i)) by letting

$$\delta \ : \ R \to \mathbb{N} \ : \ a \mapsto \left\{ \begin{array}{cc} 0 & \text{if } a = 0 \\ \nu(a) + 1 & \text{if } a \neq 0 \end{array} \right.$$

(2.67) Lemma: (viz. 328) of Bezout

Let $(R, +, \cdot)$ be an integral domain and $\emptyset \neq A \subseteq R$ be a non-empty subset of R. Then we obtain the following statements

(i) The intersection of the ideals aR (where $a \in A$) is a principal ideal if and only if A admits a least common multiple. More precisely for any $m \in R$ we obtain the following equivalency

$$\bigcap_{a \in A} aR = mR \quad \Longleftrightarrow \quad m \in \operatorname{lcm}(A)$$

(ii) If the sum of the ideals aR (where $a \in A$) is a principal ideal then A admits a greatest common divisor. More precisely for any $d \in R$ we obtain the following equivalency

$$\sum_{a \in A} aR = dR \implies d \in \gcd(A)$$

NOTA the converse implication is *untrue* in general. E.g. regard the polynomial ring $R = \mathbb{Z}[t]$, then $1 \in \operatorname{gcd}(2, t)$ but the ideal 2R + tR is not principal. The converse is true in PIDs however:

(iii) If R even is a PID then the sum of the ideals aR (where $a \in A$) is the principal ideal generated by the greatest common divisor of A. More precisely for any $d \in R$ we obtain the following equivalency

$$\sum_{a \in A} aR = dR \quad \Longleftrightarrow \quad d \in \gcd(A)$$

In particular in a PID a greatest common divisor $d \in \text{gcd}(A)$ can be written as a linear combination of the elements $a \in A$

$$\exists (b_a) \in R^{\oplus A} : d = \sum_{a \in A} ab_a$$

NOTA in an Euclidean ring (R, ν) (supposed that A is finite) the Euclidean algorithm (2.59) provides an effective method to (recursively, using (2.53.(viii))) compute these elements b_a .

(iv) Let R be a PID again and consider finitely many non-zero elements $0 \neq a_1, \ldots, a_n \in R$ such that the a_i are pairwise relatively prime (that is $i \neq j \in 1 \ldots n \implies 1 \in \text{gcd}(a_i, a_j)$). If now $b \in R$ then there are $b_1, \ldots, b_n \in R$ such that we obtain the following equality (in the quotient field QUOT R of R)

$$\frac{b}{a_1\dots a_n} = \frac{b_1}{a_1} + \dots + \frac{b_n}{a_n}$$

In an UFD R any collection $\emptyset \neq A \subseteq R$ of elements of R has a greatest common divisor d, due to (2.53.(v)). And we have just seen that in a PID the greatest common divisor d, that can even be written as a linear combination $d = \sum_{a} ab_{a}$. In an Euclidean domain d and the b_{a} can even be computed algorithmically, using the Euclidean algorithm. We now ask for the converse, that is: if any finite collection of elements of R has a greatest common divisor, that is a linear combination is R a PID already? The answer will be *yes* for noetherian rings, but *no* in general.

(2.68) Definition: (viz. 329)

Let $(R, +, \cdot)$ be an integral domain, then R is said do be a **Bezout domain** iff it satisfies one of the following three equivalent properties

(a) Any two elements $a, b \in R$ admit a greatest common divisor, that can be written as a linear combination of a and b. Formally that is

$$\forall a, b \in R \; \exists r, s \in R \; : \; ra + sb \in \gcd\{a, b\}$$

(b) For any $a, b \in R$ the ideal aR + bR is principal, that is there is some $d \in R$ such that we get dR = aR + bR. Formally again that is

$$\forall a, b \in R \; \exists d \in R \; : \; dR = aR + bR$$

(c) Any finitely generated ideal $\mathfrak{a} \leq_{i} R$ of R is principal, formally that is

 $\forall \mathfrak{a} \leq_{\mathrm{i}} R : \mathfrak{a} \text{ finitely generated} \implies \mathfrak{a} \text{ principal}$

(2.69) Corollary: (viz. 329)

Let $(R, +, \cdot)$ be any ring ring, then the following statements are equivalent

- (a) R is a PID
- (b) R is an UFD and Bezout domain
- (c) R is a noetherian ring and Bezout domain

(2.70) Example:

(i) Let $R := \mathbb{Z} + t\mathbb{Q}[t] := \{f \in \mathbb{Q}[t] \mid f(0) \in \mathbb{Z}\} \subseteq \mathbb{Q}[t]$ be the subring of polynomials over \mathbb{Q} with constant term in \mathbb{Z} . Then R is an integral domain [as it is a subring of $\mathbb{Q}[t]$] having the units $R^* = \{-1, 1\}$ only [as fg = 1 implies f(0)g(0) = 1 and $\deg(f) = 0 = \deg(g)$]. However Rneither is noetherian, nor an UFD, as it contains the following infinitely ascending chain of principal ideals

$$tR \ \subset \ \frac{1}{2}tR \ \subset \ \ldots \ \subset \ \frac{1}{2^n}tR \ \subset \ \frac{1}{2^{n+1}}tR \ \subset \ \ldots$$
[the inclusion is strict, as 2 is not a unit of R]. (Also the ideal $t\mathbb{Q}[t] \leq_i R$ is not finitely generated, as else there would be some $a \in \mathbb{Z}$ such that $at\mathbb{Q}[t] \subseteq t\mathbb{Z}[t]$, which is absurd). Yet it can be proved that R is a Bezout domain (see [Dummit, Foote, 9.3, exercise 5] for hints on this).

(ii) We want to present another example of a Bezout domain. Fix any field $(E, +, \cdot)$ and let $S := E[t_k | k \in \mathbb{N}]$ be the polynomial ring in countably many variables. Then we define the following ideal

$$\mathfrak{u} := \langle t_k - t_{k+1}^2 \mid k \in \mathbb{N} \rangle_{\mathbf{i}} \quad \trianglelefteq_{\mathbf{i}} \quad S$$

Then $R := S/\mathfrak{u}$ is a Bezout domain (refer to [Dummit, Foote, 9.2, exercise 12] for hints). However it is no noetherian ring (in particular no PID), as the following ideal \mathfrak{a} of R is *not* finitely generated

$$\mathfrak{a} := \langle t_k + \mathfrak{u} \mid k \in \mathbb{N} \rangle_{\mathbf{i}} \quad \trianglelefteq_{\mathbf{i}} \quad R$$

(iii) (\diamondsuit) Let us denote denote the integral closure of \mathbb{Z} in \mathbb{C} by \mathcal{O} . That is if we denote the set of normed polynomials over \mathbb{Z} by $\mathbb{Z}[t]_1$ (that is $\mathbb{Z}[t]_1 := \{t^n + a_1t^{n-1} + \cdots + a_n \in \mathbb{Z}[t] \mid n \in \mathbb{N}, a_i \in \mathbb{Z}\}$), then

$$\mathcal{O} := \{ z \in \mathbb{C} \mid \exists f \in \mathbb{Z}[t]_1 : f(z) = 0 \}$$

It will be proved in book II that \mathcal{O} is a subring of \mathbb{C} (and in particular an integral domain, as \mathbb{C} is a field). In fact \mathcal{O} is a Bezout domain that satisfies spec $\mathcal{O} = \operatorname{smax} \mathcal{O} \cup \{0\}$ (see [Dummit, Foote, chapter 16.3, exercise 23] for hints how to prove this). However \mathcal{O} neither is noetherian, nor an UFD, as it contains the following infinitely ascending chain of principal ideals

$$2\mathcal{O} \subset \sqrt{2}\mathcal{O} \subset \ldots \subset 2^{1/2^n}\mathcal{O} \subset 2^{1/2^{n+1}}\mathcal{O} \subset \ldots$$

(iv) Consider $\omega := (1 + i\sqrt{19})/2 \in \mathbb{C}$ and consider the following subring $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Then we obtain a Dedekind-Hasse norm on $\mathbb{Z}[\omega]$ by letting

$$\delta : \mathbb{Z}[\omega] \to \mathbb{N} : a + b\omega \mapsto a^2 + ab + 5b^2$$

(this is proved in [Dummit, Foote, page 282]). In particular $\mathbb{Z}[\omega]$ is a PID by virtue of (2.66.(ii)). However $\mathbb{Z}[\omega]$ is *not* an Euclidean domain (under any function ν whatshowever). The latter statement is proved in [Dummit, Foote, page 277].

(2.71) Remark:

By now we have studied a quite respectable list of different kinds of commutative rings from integral domains and fields over noetherian rings to Bezout domains. Thereby we have found several inclusions, that we wish to summarize in the diagram below

> integral domains \cup UFDs Bezout domains noetherian rings \cup PIDs \cup \cup Euclidean domains artinitan rings \cup fields

Note however that every single inclusion in this diagram is strict. E.g. there are integral domains that are not Bezout domains and there are PIDs that are not Euclidean domains. The following table presents examples of rings R that satisfy one property, but not the next stronger one

R	is	is not
$\mathbb{Z}[\sqrt{-3}]$	noetherian integral domain	UFD
$\mathbb{Z} + t\mathbb{Q}[t]$	Bezout domain	noetherian, UFD
$\mathbb{Q}[s,t]$	noetherian UFD	Bezout domain
$\mathbb{Z}[(1+\sqrt{-19})/2]$	PID	Euclidean domain
\mathbb{Z}	Euclidean domain	field, artinian ring

2.7 Lasker-Noether Decomposition

(2.72) Definition: (viz. 330)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_{i} R$ be a proper (i.e. $\mathfrak{a} \neq R$) ideal of R, then \mathfrak{a} is said to be a **primary** ideal of R, iff it satisfies one of the following equivalencies

(a) The radical of \mathfrak{a} contains the set of zero-divisors of R/\mathfrak{a} (as *R*-module)

$$\operatorname{ZD}_R R / \mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$$

(b) In the ring R/\mathfrak{a} the nil-radical is contained in the set of zero-divisors

$$\operatorname{ZD}^{R}/\mathfrak{a} \subseteq \operatorname{NIL}^{R}/\mathfrak{a}$$

(c) The set of zero-divisors of R/\mathfrak{a} (as a ring) equals the nil-radical of R/\mathfrak{a}

$$\operatorname{ZD}^R/\mathfrak{a} = \operatorname{NIL}^R/\mathfrak{a}$$

(d) For any two elements $a, b \in R$ of R we obtain the following implication

$$ab \in \mathfrak{a}, \ b \notin \mathfrak{a} \implies a \in \sqrt{\mathfrak{a}}$$

(e) For any two elements $a, b \in R$ of R we obtain the following implication

$$ab \in \mathfrak{a}, \ b \notin \sqrt{\mathfrak{a}} \implies a \in \mathfrak{a}$$

And if \mathfrak{a} is a primary ideal, then it is customary to say that \mathfrak{a} is **associated** to (the prime ideal) $\sqrt{\mathfrak{a}}$. Finally the set of all primary ideals of R is said to be the **primary spectrum** of R and we will abbreviate it by writing

$$\operatorname{spri} R := \{ \mathfrak{a} \leq_{\mathrm{i}} R \mid \mathfrak{a} \neq R, (\mathrm{a}) \}$$

And if $\mathfrak{p} \in \operatorname{spec} R$ is a prime ideal of R, then we denote the set of all primary ideals of R associated to \mathfrak{p} , by

$$\operatorname{spri}_{\mathfrak{p}} R := \left\{ \mathfrak{a} \in \operatorname{spri} R \mid \sqrt{\mathfrak{a}} = \mathfrak{p} \right\}$$

NOTA clearly associateness is an equivalency relation on spri R. That is for any primary ideals \mathfrak{a} and $\mathfrak{b} \leq_i R$ we let $\mathfrak{a} \approx \mathfrak{b} :\iff \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$ and thereby \approx is an equivalency relation on spri R. Further if $\mathfrak{p} = \sqrt{\mathfrak{a}}$, then $\operatorname{spri}_{\mathfrak{p}} R$ is precisely the equivalency class of \mathfrak{a} under \approx .

(2.73) Remark:

In the deninition above there already occured the notion of zero-divisors of a module (which will be introduced in 3.2). Thus we shortly wish to present what this means in the context here. Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_i R$ be an ideal. Then the set of zero-divisors of R/\mathfrak{a} as an R-module will be defined to be

$$\operatorname{ZD}_{R} \overset{R}{/}_{\mathfrak{a}} := \left\{ a \in R \mid \exists 0 \neq b + \mathfrak{a} \in \overset{R}{/}_{\mathfrak{a}} : a(b + \mathfrak{a}) = 0 \right\}$$
$$= \left\{ a \in R \mid \exists 0 \neq b + \mathfrak{a} \in \overset{R}{/}_{\mathfrak{a}} : (a + \mathfrak{a})(b + \mathfrak{a}) = 0 \right\}$$

because of $a(b + \mathfrak{a}) := ab + \mathfrak{a} = (a + \mathfrak{a})(b + \mathfrak{a})$ (this is just the definition of the scalar multiplication of R/\mathfrak{a} as an *R*-module). Now have a look at the set of zero-divisors of R/\mathfrak{a}

$$\operatorname{ZD}^{R}/_{\mathfrak{a}} = \left\{ a + \mathfrak{a} \in R/_{\mathfrak{a}} \mid \exists 0 \neq b + \mathfrak{a} \in R/_{\mathfrak{a}} : (a + \mathfrak{a})(b + \mathfrak{a}) = 0 \right\}$$

We find that the condition in both of these sets conincides. And it also is clear that \mathfrak{a} is contained in $\mathbb{ZD}_R R/\mathfrak{a}$ (unless $\mathfrak{a} = R$) [as in this case we have $ab \in \mathfrak{a}$ for $b = 1 \in R$]. Thus we find

$$\operatorname{ZD}^R/\mathfrak{a} = (\operatorname{ZD}_R R/\mathfrak{a})/\mathfrak{a}$$

(2.74) Proposition: (viz. 331)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_i R$ be an ideal. Then we obtain the following statements

(i) Any prime ideal of R already is primary, that is we obtain the inclusion

$$\operatorname{spec} R \subseteq \operatorname{spri} R$$

(ii) If \mathfrak{a} is a primary ideal of R, then the radical $\sqrt{\mathfrak{a}}$ is a prime ideal of R. In fact it is the uniquely determined smallest prime ideal containing \mathfrak{a} , that is we obtain the following implications

$$\mathfrak{a} \in \operatorname{spri} R \implies \sqrt{\mathfrak{a}} \in \operatorname{spec} R$$
$$\mathfrak{a} \in \operatorname{spri} R \implies \left\{ \sqrt{\mathfrak{a}} \right\} = \left\{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \right\}_{*}$$

(iii) If $\mathfrak{m} := \sqrt{\mathfrak{a}}$ is a maximal ideal of R, then \mathfrak{a} is a primary ideal of R associated to \mathfrak{m} , that is we obtain the following implication

$$\sqrt{\mathfrak{a}} \in \operatorname{smax} R \implies \mathfrak{a} \in \operatorname{spri} R$$

(iv) Suppose that $\mathfrak{m} \in \operatorname{smax} R$ is a maximal ideal of R, such that there is some $k \in \mathbb{N}$ such that $\mathfrak{m}^k \subseteq \mathfrak{a} \subseteq \mathfrak{m}$. Then \mathfrak{a} is a primary ideal of R associated to \mathfrak{m} . That is we obtain the following implication

 $\mathfrak{m}^k \subseteq \mathfrak{a} \subseteq \mathfrak{m} \implies \mathfrak{a} \in \operatorname{spri}_{\mathfrak{m}} R$

(v) If $\mathfrak{a}_1, \ldots, \mathfrak{a}_k \leq_i R$ are finitely many primary ideals of R, all associated to the same pirme ideal $\mathfrak{p} = \sqrt{\mathfrak{a}_i}$. Then their intersection is a primary ideal associated to \mathfrak{p} , too

$$\mathfrak{a}_1,\ldots,\mathfrak{a}_k\in\operatorname{spri}_{\mathfrak{p}}R \implies \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_k\in\operatorname{spri}_{\mathfrak{p}}R$$

(vi) If $\mathfrak{a} \leq_{i} R$ is a primary ideal and $u \in R \setminus \mathfrak{a}$, then $\mathfrak{a} : u \leq_{i} R$ is another primary ideal, associated to the same prime ideal, that is

$$\mathfrak{a} \in \operatorname{spri}_{\mathfrak{p}} R, \ u \notin \mathfrak{a} \implies \mathfrak{a} : u \in \operatorname{spri}_{\mathfrak{p}} R$$

(vii) Consider a homomorphism $\varphi : R \to S$ between the commutative rings $(R, +, \cdot)$ and $(S, +, \cdot)$. If now $\mathfrak{b} \leq_{\mathbf{i}} S$ is a primary ideal of S, then $\mathfrak{a} := \varphi^{-1}(\mathfrak{b})$ is a primary ideal of R. And if $\mathfrak{q} := \sqrt{\mathfrak{b}}$ denotes the ideal \mathfrak{b} is associated to, then \mathfrak{a} is associated to $\varphi^{-1}(\mathfrak{q})$. Formally that is

$$\mathfrak{b} \in \operatorname{spri}_{\mathfrak{q}} S \implies \varphi^{-1}(\mathfrak{b}) \in \operatorname{spri}_{\varphi^{-1}(\mathfrak{q})} R$$

(viii) (\diamond) Let $U \subseteq R$ be a multiplicatively closed set, $\mathfrak{p} \leq_{\mathbf{i}} R$ be a prime ideal of R with $\mathfrak{p} \cap U = \emptyset$ and denote by $\mathfrak{q} := U^{-1}\mathfrak{p} \leq_{\mathbf{i}} U^{-1}R$ the corresponding prime ideal of $U^{-1}R$. Then we obtain a one-to-one correspondence, by

$$\operatorname{spri}_{\mathfrak{p}} R \quad \longleftrightarrow \quad \operatorname{spri}_{\mathfrak{q}} U^{-1} R$$
$$\mathfrak{a} \quad \mapsto \quad U^{-1} \mathfrak{a}$$
$$\mathfrak{b} \cap R \quad \longleftrightarrow \quad \mathfrak{b}$$

(2.75) Example: (viz. 332)

- (i) Let $(R, +, \cdot)$ be an integral domain and $p \in R$ be a prime element of R. Then for any $1 \leq n \in \mathbb{N}$ the ideal $\mathfrak{a} := p^n R$ is primary and associated, to the prime ideal $\sqrt{\mathfrak{a}} = pR$.
- (ii) In a PID $(R, +, \cdot)$ the primary ideals are precisely the ideals 0 and $p^n R$ for some $p \in R$ prime. Formally that is the identity

$$\operatorname{spri} R = \{ p^n R \mid 1 \le n \in \mathbb{N}, p \in R \text{ prime} \} \cup \{ 0 \}$$

- (iii) Primary ideals do *not* need to be powers of prime ideals. As an example let $(E, +, \cdot)$ be any field and consider R := E[s, t]. Then the ideal $\mathfrak{a} := \langle s, t^2 \rangle_i$ is primary and associated to the maximal ideal $\mathfrak{m} := \langle s, t \rangle_i$. In fact we get $\mathfrak{m}^2 \subset \mathfrak{a} \subset \mathfrak{m}$ and hence there is *no* prime ideal $\mathfrak{p} \leq_i R$ such that $\mathfrak{a} = \mathfrak{p}^k$ for some $k \in \mathbb{N}$.
- (iv) Powers of prime ideals do *not* need to be primary ideals. As an example let $(E, +, \cdot)$ be any field again and consider $R := E[s, t, u]/\mathfrak{u}$ where $\mathfrak{u} := \langle u^2 - st \rangle_i$. Let us denote $a := s + \mathfrak{u}, b := t + \mathfrak{u}$ and $c := u + \mathfrak{u}$. Then we obtain a prime ideal $\mathfrak{p} \leq_i R$ by letting $\mathfrak{p} := \langle b, c \rangle_i$. However we will see that $\mathfrak{a} := \mathfrak{p}^2$ is no primary ideal.

(2.76) Definition:

Let $(R, +, \cdot)$ be a commutative ring, then \mathfrak{p} is said to be an **irreducible** ideal of R, iff it satisfies the following three properties

- (1) $\mathfrak{p} \leq_{\mathbf{i}} R$ is an ideal
- (2) $\mathfrak{p} \neq R$ is proper
- (3) \mathfrak{p} is not the intersection of finitely many larger ideals. That is for any two ideals $\mathfrak{a}, \mathfrak{b} \leq_i R$ we obtain the implication

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b} \implies \mathfrak{p} = \mathfrak{a} \text{ or } \mathfrak{p} = \mathfrak{b}$$

(2.77) Theorem: (viz. 334)

(i) Let $(R, +, \cdot)$ be a commutative ring, then any prime ideal of R already is irreducible. That is for any ideal $\mathfrak{p} \leq_i R$ we get the implication

 \mathfrak{p} prime $\implies \mathfrak{p}$ irreducible

(ii) Let $(R, +, \cdot)$ be a noetherian ring, then any irreducible ideal of R already is primary. That is for any ideal $\mathfrak{p} \leq_i R$ we get the implication

 \mathfrak{p} irreducible $\implies \mathfrak{p}$ primary

- (iii) Let $(R, +, \cdot)$ be a noetherian ring, then any proper ideal $\mathfrak{a} \leq_{\mathrm{i}} R, \mathfrak{a} \neq R$ admits an irreducible decomposition $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$. That is there are ideals $\mathfrak{p}_i \leq_{\mathrm{i}} R$ (where $i \in 1 \ldots k$ and $1 \leq k \in \mathbb{N}$) such that
 - (1) $\forall i \in 1...k : \mathfrak{p}_i$ is an irreducible ideal
 - (2) $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$

(2.78) Definition:

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_i R$ be an ideal of R. Then a tupel $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ is said to be a **primary decomposition** of \mathfrak{a} , iff we have

(1) $\forall i \in 1 \dots k : \mathfrak{a}_i \in \operatorname{spri} R$ is a primary ideal of R

(2)
$$\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$$

And $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ is said to be **minimal** (or **irredundant**) iff we further get

- (3) $\forall j \in 1 \dots k : \mathfrak{a} \neq \bigcap_{i \neq j} \mathfrak{a}_i$
- (4) $\forall i \neq j \in 1 \dots k : \sqrt{\mathfrak{a}_i} \neq \sqrt{\mathfrak{a}_j}$

Finally if $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ is a minimal primary decomposition of \mathfrak{a} , then let us denote $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$. Then we define the set of *associated prime ideals* and *isolated* and *embedded components* of $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ to be the following

$$\begin{aligned} \operatorname{ass}(\mathfrak{a}_{1},\ldots,\mathfrak{a}_{k}) &:= \{\mathfrak{p}_{1},\ldots,\mathfrak{p}_{k}\} \\ \operatorname{iso}(\mathfrak{a}_{1},\ldots,\mathfrak{a}_{k}) &:= \{\mathfrak{a}_{i} \mid i \in 1 \ldots k, \ \mathfrak{p}_{i} \in \operatorname{ass}(\mathfrak{a}_{1},\ldots,\mathfrak{a}_{k})_{*}\} \\ &= \left\{\mathfrak{a}_{i} \mid i \in 1 \ldots k, \ \forall j \in 1 \ldots k : \mathfrak{p}_{j} \subseteq \mathfrak{p}_{i} \implies j = i\right\} \\ \operatorname{emb}(\mathfrak{a}_{1},\ldots,\mathfrak{a}_{k}) &:= \left\{\mathfrak{a}_{1},\ldots,\mathfrak{a}_{k}\right\} \setminus \operatorname{iso}(\mathfrak{a}_{1},\ldots,\mathfrak{a}_{k}) \end{aligned}$$

NOTA that is the isolated components belong to the minimal associated prime ideals. And a \mathfrak{a}_i is said to be an embedded component if it is not an isolated component, that is if its prime ideal \mathfrak{p}_i is not minimal. These notions have a geometric interpretation, whence the odd names come from.

(2.79) Example:

Let $(R, +, \cdot)$ be an UFD and $a \in R$ with $0 \neq a \notin R^*$. Then we pich up a primary decomposition of a, that is $a = p_1^{n_1} \dots p_k^{n_k}$ where $1 \leq k \in \mathbb{N}$ and for any $i, j \in 1 \dots k$ we have $p_i \in R$ is prime, $1 \leq n_i \in \mathbb{N}$ and $p_i R = p_j R$ implies i = j. Then we obtain a minimal primary decomposition of $\mathfrak{a} = aR$

 $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k)$ where $\mathfrak{a}_i := p_i^{n_i} R$

And for this primary decomposition we find $\mathfrak{p}_i = \sqrt{\mathfrak{a}_i} = p_i R$ and furthermore

$$\operatorname{ass}(\mathfrak{a}_1, \dots, \mathfrak{a}_k) := \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \\ \operatorname{iso}(\mathfrak{a}_1, \dots, \mathfrak{a}_k) := \{\mathfrak{a}_1, \dots, \mathfrak{a}_k\}$$

(2.80) Proposition: (viz. 335)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_i R$ be an ideal of R. If \mathfrak{a} admits any primary decomposition, then it already admits a minimal primary decomposition. More precisely let $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ be a primary decomposition of \mathfrak{a} . Then we select a subset $I \subseteq 1 \ldots k$ such that

$$#I = \min \left\{ #J \middle| J \subseteq 1 \dots k, \ \mathfrak{a} = \bigcap_{j \in J} \mathfrak{a}_j \right\}$$

Now define an equivalency relation on I by letting $i \approx j :\iff \sqrt{\mathfrak{a}_i} = \sqrt{\mathfrak{a}_j}$. And denote the quotient set by $A := I/\approx$. Then we have found a minimal primary decomposition (\mathfrak{a}_α) (where $\alpha \in A$) of \mathfrak{a} by letting

$$\mathfrak{a}_{lpha} := igcap_{i\inlpha} \mathfrak{a}_i$$

(2.81) Proposition: (viz. 336)

Let $(R, +, \cdot)$ be a commutative ring, $\mathfrak{a} \leq_{i} R$ be a proper $\mathfrak{a} \neq R$ ideal and consider $(\mathfrak{a}_{1}, \ldots, \mathfrak{a}_{k})$ a minimal primary decomposition of \mathfrak{a} . Let us further denote $\mathfrak{p}_{i} := \sqrt{\mathfrak{a}_{i}}$, then we obtain the following statements

(i) Clearly the number of associated prime ideals of the decomposition equals the number of primeary ideals of the decomposition. Formally

$$\#$$
ass $(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) = k$

(ii) For any $u \in R$ we obtain the following identity (where by convention the intersection over the empty set is defined to be the ring R itself)

$$\sqrt{\mathfrak{a}: u} = \bigcap \{ \mathfrak{p}_i \mid i \in 1 \dots k, \ u \notin \mathfrak{a}_i \}$$

(iii) (\diamondsuit) If \mathfrak{p}_i is minimal among $\operatorname{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ then we can recunstruct \mathfrak{a}_i from \mathfrak{a} and \mathfrak{p}_i . To be precise for any $i \in 1 \ldots k$ we get

$$\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)_* \implies \mathfrak{a}: (R \setminus \mathfrak{p}_i) = \mathfrak{a}_i$$

(iv) Let us introduce $\operatorname{ass}(\mathfrak{a}) := \operatorname{spec} R \cap \{\sqrt{\mathfrak{a} : u} \mid u \in R\}$ the set of *prime ideals associated* to \mathfrak{a} . Then we obtain the following identity

$$\operatorname{ass}(\mathfrak{a}) = \operatorname{ass}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$$

(v) (\diamond) Let us introduce iso(\mathfrak{a}) := { \mathfrak{a} : $(R \setminus \mathfrak{p}) \mid \mathfrak{p} \in \operatorname{ass}(\mathfrak{a})_*$ } the set of *isolated components* of \mathfrak{a} . then we obtain the following identity

$$\operatorname{iso}(\mathfrak{a}) = \operatorname{iso}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$$

(2.82) Remark: (\diamondsuit)

Let $(R, +, \cdot)$ be a commutative ring. In section 5.1 we will introduce the notion of a prime ideal *associated* to an *R*-module *M*. Thus if $\mathfrak{a} \leq_i R$ is an ideal, then it makes sense to the regard the prime ideals associated to \mathfrak{a} as an *R*-module. And by definition this is just

$$\operatorname{ass}_{R}(\mathfrak{a}) = \operatorname{spec} R \cap \{\operatorname{ANN}(b) \mid b \in \mathfrak{a} \}$$

= spec $R \cap \{0 : b \mid b \in \mathfrak{a} \}$

(where the equality is due to ANN (b) = 0 : b for any $b \in R$). Thus we find that $\operatorname{ass}_R(\mathfrak{a})$ has *absolutely nothing* to do with the set $\operatorname{ass}(\mathfrak{a})$ that has been defined in the proposition above

$$\operatorname{ass}(\mathfrak{a}) = \operatorname{spec} R \cap \left\{ \sqrt{\mathfrak{a} : u} \mid u \in R \right\}$$

However it will turn out that the set $ass(\mathfrak{a})$ is closely related to the set of associated prime ideals of the *R*-module R/\mathfrak{a} . By definition this is

$$\operatorname{ass}_{R} \begin{pmatrix} R/\mathfrak{a} \end{pmatrix} = \operatorname{spec} R \cap \left\{ \operatorname{ANN} (x) \mid x \in R/\mathfrak{a} \right\} \\ = \operatorname{spec} R \cap \left\{ \operatorname{ANN} (b + \mathfrak{a}) \mid b \in R \right\} \\ = \operatorname{spec} R \cap \left\{ \mathfrak{a} : b \mid b \in R \right\}$$

(the latter equality is due to ANN $(b + \mathfrak{a}) = \mathfrak{a} : b$ for any $b \in R$ again). Thus the difference between this set and $\operatorname{ass}(\mathfrak{a})$ lies in the fact that $\operatorname{ass}(\mathfrak{a})$ allows the taking of radicals. Hence it is easy to see that $\operatorname{ass}_R(R/\mathfrak{a}) \subseteq \operatorname{ass}(\mathfrak{a})$. In section 5.1 we will prove that for noetherian rings R we even have

$$\operatorname{ass}_R\left(\frac{R}{\mathfrak{a}}\right) = \operatorname{ass}(\mathfrak{a})$$

(2.83) Corollary: (viz. 337) Lasker-Noether

Let $(R, +, \cdot)$ be a noetherian ring, then any proper ideal $\mathfrak{a} \leq_{i} R$, $\mathfrak{a} \neq R$ admits a minimal primary decomposition. And in this decomposition the associated prime ideals and the isolated components are uniquely determined by \mathfrak{a} . Formally that is

- (1) There are ideals $\mathfrak{a}_i \leq_i R$ (where $i \in 1 \dots k$ and $1 \leq k \in \mathbb{N}$) such that $(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$ is a minimal primary decomposition of \mathfrak{a} .
- (2) If $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ and $(\mathfrak{b}_1, \ldots, \mathfrak{b}_l)$ are any two minimal primary decompositions of \mathfrak{a} then we obtain the following three identities

$$k = l$$

$$\operatorname{ass}(\mathfrak{a}_1, \dots, \mathfrak{a}_k) = \operatorname{ass}(\mathfrak{b}_1, \dots, \mathfrak{b}_l)$$

$$\operatorname{iso}(\mathfrak{a}_1, \dots, \mathfrak{a}_k) = \operatorname{iso}(\mathfrak{b}_1, \dots, \mathfrak{b}_l)$$

(3) In particular if $\mathfrak{a} = \sqrt{\mathfrak{a}}$ is a radical ideal, then the minimal primary decomposition $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$ of \mathfrak{a} is uniquely determined (up to ordering) and consists precisely of the prime ideals minimal over \mathfrak{a} , formally

$$\{\mathfrak{p}_1,\ldots,\mathfrak{p}_k\} = \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\}_*$$

(2.84) Example:

Fix any field $(E, +, \cdot)$ and let R := E[s, t] be the polynomial ring over E in s and t (note that R is noetherian due to Hilbert's basis theorem). Now consider the ideal $\mathfrak{a} := \langle s^2, st \rangle_i$. Then we obtain two distinct primary decompositions $(\mathfrak{a}_1, \mathfrak{a}_2)$ and $(\mathfrak{b}_1, \mathfrak{b}_2)$ of \mathfrak{a} by letting

$$\begin{array}{cccc} \mathfrak{a}_{i} & \mathfrak{b}_{i} & \mathfrak{p}_{i} \\ i = 1 & \langle s \rangle_{\mathbf{i}} & \langle s \rangle_{\mathbf{i}} & \langle s \rangle_{\mathbf{i}} \\ i = 2 & \langle s^{2}, st, t^{2} \rangle_{\mathbf{i}} & \langle s^{2}, t \rangle_{\mathbf{i}} & \langle s, t \rangle_{\mathbf{i}} \end{array}$$

where $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i} = \sqrt{\mathfrak{b}_i}$. It is no coincidence that both primary decompositions have 2 elements and that the radicals \mathfrak{p}_i are equal. Further $\mathfrak{p}_1 \subset \mathfrak{p}_2$, that is $\mathfrak{a}_1 = \mathfrak{b}_1$ are isolated components of \mathfrak{a} and $\mathfrak{a}_2 \neq \mathfrak{b}_2$ are embedded components (of the decompositions). In fact this example demonstrates that the embedded components may be different.

$$\operatorname{ass}(\mathfrak{a}) = \{ sR, sR + tR \}$$

$$\operatorname{iso}(\mathfrak{a}) = \{ sR \}$$

(2.85) Corollary: (viz. 338)

Let $(R, +, \cdot)$ be a noetherian ring and \mathfrak{a} be a proper ideal of R, that is $R \neq \mathfrak{a} \leq_{i} R$. If now $\mathfrak{q} \leq_{i} R$ is any prime ideal of R then we obtain

(i) \mathfrak{a} is contained in \mathfrak{q} iff \mathfrak{q} contains an associated prime ideal of \mathfrak{a} iff \mathfrak{q} contains an isolated component of \mathfrak{a} . Formally that is

$$\mathfrak{a} \subseteq \mathfrak{q} \iff \exists \mathfrak{p} \in \operatorname{ass}(\mathfrak{a}) : \mathfrak{p} \subseteq \mathfrak{q} \\ \iff \exists \mathfrak{l} \in \operatorname{iso}(\mathfrak{a}) : \mathfrak{l} \subseteq \mathfrak{q}$$

(ii) The set of primes lying minimally over \mathfrak{a} is precisely the set of primes belonging to the isolated components of \mathfrak{a} . Formally again

$$\{\mathfrak{q} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{q}\}_* = \operatorname{ass}(\mathfrak{a})_*$$

(iii) And thereby the radical of \mathfrak{a} is precisely the intersection of all (minimal) associated prime ideals of \mathfrak{a} . Put formally that is

$$\sqrt{\mathfrak{a}} = \bigcap \operatorname{ass}(\mathfrak{a}) = \bigcap \operatorname{ass}(\mathfrak{a})_*$$

2.8 Finite Rings

(2.86) Definition: (viz. 339)

Let $(R, +, \cdot)$ be any ring, denote its zero element by 0_R and its unit element by 1_R . For any $1 \le k \in \mathbb{N}$ let us denote $k_R := k 1_R = 1_R + \cdots + 1_R$ (k-times). Then there exists a uniquely determined homomorphism of rings ζ from \mathbb{Z} to R, and this is given to be

$$\zeta \ : \ \mathbb{Z} \to R \ : \ k \mapsto \begin{cases} k_R & \text{if } k > 0 \\ 0_R & \text{if } k = 0 \\ -(-k)_R & \text{if } k < 0 \end{cases}$$

The image of ζ in R is said to be the **prime ring** of R and denoted by PRR R. In fact it precisely is the intersection of all subrings of R. Formally

$$\operatorname{PRR} R := \operatorname{im}(\zeta) = \bigcap \{ P \mid P \leq_{\mathrm{r}} R \}$$

And the kernel of ζ is an ideal in \mathbb{Z} . Hence (as \mathbb{Z} is a PID) there is a uniquely determined $n \in \mathbb{N}$ such that $\operatorname{kn}(\zeta) = n\mathbb{Z}$. This number n is said to be the **characteristic** of R, denoted by

CHAR
$$R := n$$
 where $\operatorname{kn}(\zeta) = n\mathbb{Z}$

That is if R has characteristic zero n = 0, then we get $k_R = 0 \implies k = 0$. And if R has non-zero characteristic $n \neq 0$, then n is precisely the smallest number such that $n_R = 0$. Formally that is

CHAR
$$R = \min\{1 \le k \in \mathbb{N} \mid k_R = 0\}$$

(2.87) Remark:

If $(F, +, \cdot)$ even is a field, we may also introduce the **prime field** of F (denoted by PRF F) to be this intersection of all subfields of F. Formally

$$\operatorname{PRF} F := \bigcap \{ E \mid E \leq_{\mathrm{f}} F \}$$

And if is easy to see that PRF F is precisely the quotient field of the prime ring PRR F. Formally that is the following identity

$$\operatorname{PRF} F = \left\{ ab^{-1} \mid a, b \in \operatorname{PRR} F, \ b \neq 0 \right\}$$

PROB as $E \leq_{\mathrm{f}} F$ implies $E \leq_{\mathrm{r}} F$ (by definition) we have PRR $F \subseteq$ PRF F. Let us now denote the quotioent field of PRR F by $Q \subseteq F$. As PRF F is a field and PRR \subseteq PRF F it is clear that $Q \subseteq$ PRF F. On the other hand $Q \leq_{\mathrm{f}} F$ is a subfield and hence we have PRF $F \subseteq Q$ by construction. Together this means PRF F = Q as claimed. (2.88) **Proposition:** (viz. 340)

Let $(R, +, \cdot)$ be any ring, then the characteristic of R satisfies the properties

(i) If $R \neq 0$ is a non-zero integral domain, then the characteristic of R is prime or zero. Formally that is the following implication

 $R \neq 0$ integral domain \implies CHAR R = 0 or prime

(ii) R has characteristic zero if and only if the prime ring of R is isomorphic to \mathbb{Z} . More precisely we find the following equivalencies

CHAR R = 0 \iff $\forall k \in \mathbb{N} : k_R = 0 \implies k = 0$ \iff $\mathbb{Z} \cong_{\mathbf{r}} \operatorname{PRR} R : k \mapsto \zeta(k)$

(iii) R has non-zero characteristic if and only if the prime ring of R is isomorphic to \mathbb{Z}_n (where $n = \operatorname{CHAR} R$). More precisely for any $n \in \mathbb{N}$ we find the equivalency of the following statements

CHAR
$$R = n \neq 0 \iff n = \min\{1 \le k \in \mathbb{N} \mid k_R = 0\}$$

 $\iff n \neq 0 \text{ and } \mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRR} R : k + n\mathbb{Z} \mapsto \zeta(k)$

(iv) Now suppose that R is a field, then the prime field of R is given to be

 $\begin{aligned} & \operatorname{Char} R = 0 & \Longleftrightarrow & \mathbb{Q} \cong_{\mathrm{r}} \operatorname{PRF} R \\ & \operatorname{Char} R = n \neq 0 & \Longleftrightarrow & \mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRF} R \end{aligned}$

(v) Let $(R, +, \cdot)$ be a finite ring (that is $\#R < \infty$), then the characteristic of R is non-zero and divides the number of elements of R, formally

$$0 \neq \text{CHAR } R \mid \#R$$

(2.89) Proposition: (viz. 342)

(i) Let $(R, +, \cdot)$ be a finite (that is $\#R < \infty$), commutative ring. Then the non-zero divisors of R already are invertible, that is

$$R^* = R \setminus ZD R$$

(ii) Let $(S, +, \cdot)$ be an integral domain and consider a prime element $p \in S$. Let further $1 \leq n \in \mathbb{N}$ and denote the quotient ring $R := S/p^n S$. Then the set of zero-divisors of R is precisely the ideal generated by the residue class of p. Formally that is

$$\operatorname{ZD} R = (p + p^n S) R$$

(iii) Now let $(S, +, \cdot)$ be a PID, consider a prime element $p \in S$ and let $R := S/p^n S$ again. Then we obtain the following statements

NIL
$$R = \operatorname{ZD} R = R \setminus R^* = (p + p^n S) R$$

spec $R = \operatorname{smax} R = \{\operatorname{NIL} R\}$

(iv) Let $(R, +, \cdot)$ be any noetherian (in particular commutative) ring and fix any $1 \le m \in \mathbb{N}$. Then there only are finitely many prime ideals \mathfrak{p} of R such that R/\mathfrak{p} has at most m elements. Formally

$$\#\left\{\mathfrak{p}\in\operatorname{spec} R\;\middle|\; \#^R/\mathfrak{p}\leq m\right\} < \infty$$

(2.90) Remark: (\diamondsuit)

As in (iii) let $(S, +, \cdot)$ be a PID, $p \in S$ be a prime element and define $R := S/p^n S$ again. Then we have seen, that NIL $R = R \setminus R^*$ and we will soon call a ring with such a property a local ring. To be precise: R is a *local ring* with maximal ideal NIL R. Further - in a fancier language - the property spec $R = \operatorname{smax} R$ can be reformulated as "R is a *zero-dimensional* ring". We will not introduce the concept of the Krull dimension of a commutative ring until book 2, however.

(2.91) Theorem: (viz. 345) of Wedderburn

Let $(F, +, \cdot)$ be a ring with finitely many elements only (formally $\#F < \infty$), then the following three statements are equivalent

- (a) F is a field
- (b) F is a skew-field
- (c) F is an integral domain

2.9 Localisation

Localisation is one of the most powerful and fundamental tools in commutative algebra - and luckily one of the most simple ones. The general idea of localisation is to start with a commutative ring $(R, +, \cdot)$, to designate a sufficient subset $U \subseteq R$ and to enlarge R to the ring $U^{-1}R$ in which the elements of $u \in U \subseteq R \subseteq U^{-1}R$ now are units. And it will turn out, that in doing this the ideal structure of $U^{-1}R$ will be *easier* than that of R. And conversely we can restore information of R by regarding sufficiently many localisations of R (this will be the *local-global-principle*). These two properties gives the method of localizing its punch. In fact commutative algebra has been most successful with problems that allowed localisation. So let us finally begin with the fundamental definitions:

(2.92) Definition:

Let $(R, +, \cdot)$ be any commutative ring, then a subset $U \subseteq R$ is said to be **multiplicatively closed** iff it satisfies the following two properties

$$\begin{array}{rccc} 1 & \in & U \\ u, v \in U & \Longrightarrow & uv \in U \end{array}$$

And $U \subseteq R$ is said to be a **saturated** mutilplicative system, iff we even get

$$1 \quad \in \quad U$$
$$u, v \in U \implies uv \in U$$
$$uv \in U \implies u \in U$$

(2.93) Proposition: (viz. 347)

- (i) In a commutative ring $(R, +, \cdot)$ the set R^* of units and the set NZD R of non-zero-divisors of R both are saturated multiplicatively closed sets.
- (ii) If $U \subseteq R$ is a saturated, multiplicatively closed set, then $R^* \subseteq U$, as for any $u \in R^*$ we get $uu^{-1} = 1 \in U$ and hence $u \in U$.
- (iii) If $U, V \subseteq R$ are multiplicatively closed sets in the commutative ring R, then $UV := \{ uv \mid u \in U, v \in V \}$ is multiplicatively closed, too.
- (iv) If $\mathfrak{a} \leq_i R$ is an ideal, then $1 + \mathfrak{a} \subseteq R$ is a multiplicatively closed subset.
- (v) Let $\varphi : R \to S$ be a ring-homomorphism between the commutative rings R and S and consider $U \subseteq R$ and $V \subseteq V$. Then we get

U	mult. closed	\implies	$\varphi(U)$	mult. closed
V	mult. closed	\implies	$\varphi^{-1}(V)$	mult. closed
V	saturated	\implies	$\varphi^{-1}(V)$	saturated

- (vi) If $\mathcal{U} \subseteq \mathcal{P}(R)$ is a chain (under \subseteq) of multiplicatively closed subsets of R, then the union $\bigcup \mathcal{U} \subseteq R$ is a multiplicatively closed set again.
- (vii) If $\mathcal{U} \subseteq \mathcal{P}(R)$ is a nonempty $(\mathcal{U} \neq \emptyset)$ family of (saturated) multiplicatively closed subsets of R, then the intersection $\bigcap \mathcal{U} \subseteq R$ is a (saturated) multiplicatively closed set, too. NOTA this allows to define the *multiplicative closure* of a subset A of

NOTA this allows to define the *multiplicative closure* of a subset A of R to be $\bigcap \{ U \subseteq R \mid A \subseteq U, U \text{ multiplicatively closed } \}$. Likewise we may define the *saturated multiplicative closure* of A to be the intersetion of all saturated multiplicatively closed subsets containing A.

- (viii) Consider any $u \in R$, then the set $U := \{ u^k \mid k \in \mathbb{N} \}$ clearly is a multiplicatively closed set. In fact it is the smallest multiplicatively closed set containing u. That is U is the multiplicative closure of $\{ u \}$.
 - (ix) Let $U \subseteq R$ be a multiplicatively closed subset of R, then the saturated multiplicative closure \overline{U} of U can be given explicitly to be the set

$$\overline{U} = \{ a \in R \mid \exists b \in R, \exists u, v \in U : uab = uv \}$$

(2.94) Proposition: (viz. 348)

Let $(R, +, \cdot)$ be any commutative ring and $U \subseteq R$ be a subset. Then U is saturated multiplicatively closed, iff it is the complement of a union of prime ideals of R. Formally that is the equivalence of

- (a) $\exists \mathcal{P} \subseteq \operatorname{spec} R$ such that $U = R \setminus \bigcup \mathcal{P}$
- (b) $U \subseteq R$ is a saturated multiplicatively closed subset

(2.95) Definition: (viz. 348)

Let $(R, +, \cdot)$ be any commutative ring and $U \subseteq R$ be a multiplicatively closed subset of R. Then we obtain an equivalence relation \sim on the set $U \times R$ by virtue of (with $a, b \in R$ and $u, v \in U$)

$$(u,a) \sim (v,b) \quad :\iff \quad \exists w \in U \; : \; vwa = uwb$$

And we denote the quotient of $U \times R$ modulo \sim by $U^{-1}R$ and the equivalence class of (u, a) is denoted by a/u, formally this is

$$\begin{array}{ll} \displaystyle\frac{a}{u} &:= & \left\{ \left. (v,b) \in U \times R \right. \right| \left. (u,a) \sim (v,b) \right. \right\} \\ \displaystyle U^{-1}R &:= & \displaystyle\frac{U \times R}{\sim} \end{array}$$

Now $U^{-1}R$ is a commutative ring under the following algebraic operations

$$\frac{a}{u} + \frac{b}{v} := \frac{av + bu}{uv}$$
$$\frac{a}{u} \cdot \frac{b}{v} := \frac{ab}{uv}$$

It is clear that under these operations the zero-element of $U^{-1}R$ is given to be 0/1 and the unit element of $U^{-1}R$ is given to be 1/1. And we obtain a canonical ring homomorphism from R to $U^{-1}R$ by letting

$$\kappa \; : \; R \to U^{-1}R \; : \; a \mapsto \frac{a}{1}$$

In general this canonical homomorphism need not be and embedding (i.e. injective). Yet we do obtain the following equivalencies

$$\begin{array}{lll} \kappa \text{ injective } & \Longleftrightarrow & U \subseteq \text{ NZD } R \\ \kappa \text{ bijective } & \Longleftrightarrow & U \subseteq R^* \end{array}$$

(2.96) Remark:

• Though the equivalence relation \sim in the above definition might look a little artificial at first sight nothing here is mythical or mere chance. To see this let us first consider the case of an integral domain $(R, +, \cdot)$. Then we may divide by w and hence we get

$$\frac{a}{u} = \frac{b}{v} \iff va = ub$$

and this is just what we expect, if we multiply the left-hand equation by uv. To allow a common factor w is just the right way to deal with zero divisors in R. For convenience we repeat the defining property of the quotient a/u for general commutative rings $(R, +, \cdot)$

$$\frac{a}{u} = \frac{b}{v} \quad \Longleftrightarrow \quad \exists w \in U \ : \ vwa = uwb$$

• And from this equivalence it is immediately clear that fractions a/u in $U^{-1}R$ can be reduced by common facors v of U. That is for any elements $a \in R$ and $u, v \in U$ we have the equality

$$\frac{av}{uv} = \frac{a}{u}$$

And this allows to express sums by going to a common denominator. That is consider $a_1, \ldots, a_n \in R$ and $u_1, \ldots, u_n \in U$. Then we denote $u := u_1 \ldots u_n \in U$ and $\hat{u}_i := u/u_i \in U$ (e.g. $\hat{u}_1 = u_2 \ldots u_n$). Then we have just remarked that $a_i/u_i = (a_i\hat{u}_i)/u$ and thereby

$$\frac{a_1}{u_1} + \dots + \frac{a_n}{u_n} = \frac{a_1\widehat{u}_1 + \dots + a_n\widehat{u}_n}{u}$$

• This equivalence also yields that 1/1 = 0/1 holds true in $U^{-1}R$ if and only if the multiplicatively closed set contains zero $0 \in U$. But as 0/1is the zero-element and 1/1 is the unit element of $U^{-1}R$ we thereby found another equivalence

$$U^{-1}R = 0 \quad \Longleftrightarrow \quad 0 \in U$$

• As we have intended, localizing turns the elements $u \in U$ into units. More precisely if $U \subseteq R$ is multiplicatively closed, then we obtain

$$(U^{-1}R)^* \supseteq \left\{ \frac{au}{v} \mid a \in R^*, u, v \in U \right\}$$

Yet the equality need not hold true! As an example consider $R = \mathbb{Z}$ and $U = \{ 6^k \mid k \in \mathbb{N} \} = \{ 1, 6, 36, ... \}$. Then 2/1 is invertible, with inverse $(2/1)^{-1} = 3/6$, yet 2 is not of the form $R^*U = \{ \pm 6^k \mid k \in \mathbb{N} \}$. PROB consider any au/v such that $a \in R^*$ and $u, v \in U$, then we get $(au/v)(a^{-1}v/u) = (aa^{-1}uv)/(uv) = (uv)/(uv) = 1/1$ and hence au/vis a unit, with inverse $(au/v)^{-1} = a^{-1}v/u$.

• If $U \subseteq R$ even is a saturated multiplicatively closed subset, then we even obtain a complete description of the units of $U^{-1}R$ to be

$$\left(U^{-1}R\right)^* = \left\{ \frac{u}{v} \mid u, v \in U \right\}$$

PROB clearly u/v is a unit of $U^{-1}R$, since $(u/v)^{-1} = v/u$. Conversely if b/v is a unit of $U^{-1}R$ there is some $a/u \in U^{-1}R$ such that ab/uv = (a/u)(b/v) = 1/1. That is there is some $w \in U$ such that abw = uvw. Hence $b(aw) = uvw \in U$ and as U is saturated this implies $b \in U$.

• Let $(R, +, \cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed set, such that $U^{-1}R$ is finitely generated as an *R*-module. That is we suppose there are $b_1, \ldots, b_n \in R$ and $v_1, \ldots, v_n \in U$ such that

$$U^{-1}R = \left\{ \left. \frac{a_1b_1}{v_1} + \dots + \frac{a_nb_n}{v_n} \right| a_1, \dots, a_n \in R \right\}$$

Then the canonical mapping $\kappa : R \to U^{-1}R : b \mapsto b/1$ is surjective. PROB consider any $a/u \in U^{-1}R$ and denote $v := v_1 \dots v_n \in U$ and $\hat{v}_i := v/v_i \in V$ (e.g. $\hat{v}_1 = v_2 \dots v_n$). As $uv \in V$ and $U^{-1}R$ is generated by the b_i/v_1 there are $a_1, \dots, a_n \in R$ such that

$$\frac{a}{uv} = \frac{a_1b_1}{v_1} + \dots + \frac{a_nb_n}{v_n} = \frac{a_1b_1\widehat{v}_1 + \dots + a_nb_n\widehat{v}_n}{v}$$

That is there is some $w \in U$ such that vwa = uvwb where we let $b := a_1b_1\hat{v}_1 + \cdots + a_nb_n\hat{v}_n \in R$. That is we have found (vw)1a = (vw)ub, thus by definition we have $\kappa(b) = b/1 = a/u$. And as a/u has been arbitrary this is the surjectivity of κ .

(2.97) Example:

Let now $(R, +, \cdot)$ be any commutative ring. Then we present three examples that are of utmost importance. Hence the reader is asked to regard these examples as definitions of the objects R_u , QUOT R and $R_{\mathfrak{p}}$.

If R is an integral domain and U ⊆ R is a multiplicatively closed set, then the construction of U⁻¹R can be simplified somewhat. First let B := (R \ {0}) × R, then we obtain an equivalency relation on B by letting (a, u) ~ (b, v) :⇔ av = bu. Let us denote the equivalency class of (a, u) by a/u := [(a, u)]. Then we have regained the quotient field, that has already been introduced in section 1.3

Quot
$$R = \left\{ \left. \frac{a}{b} \right| a, b \in R, \ b \neq 0 \right\}$$

Note that this is precisely the construction that is used to obtain \mathbb{Q} from \mathbb{Z} . If now $U \subseteq R$ is an arbitrary multiplicatively closed set satisfying $0 \notin U$, then the localisation of R in U is canonically isomorphic to the following subring of the quotient field:

$$U^{-1}R \cong_{\mathbf{r}} \left\{ \frac{a}{b} \in \text{QUOT} R \mid a \in R, u \in U \right\} : \frac{a}{u} \mapsto \frac{a}{u}$$

PROB we will first prove the well-deinedness and injectivity: by definition a/u = b/v in $U^{-1}R$ is equivalent to w(av - bu) = 0 for some $w \in U$. But as $0 \notin U$ we get $w \neq 0$ and hence av = bu, as R is an integral domain. This again is just a/u = b/v in QUOT R. The surjectivity of the map is obvious and it clearly is a homomorphism, as the algebraic operations are literally the same.

• Let us generalize the previous construction a little: it is clear that the set U := NZD R of non-zero divisors of R is a saturated multiplicatively closed set. Thus we may define the **total ring of fractions** of a commutative ring R to be the localisation in this set

QUOT
$$R := (\operatorname{NZD} R)^{-1} R$$

Note that in case of an integral domain we have NZD $R = R \setminus \{0\}$ and hence we obtain precisely the same ring as before. Further note that by the very nature of U = NZD R the canonical homomorphism κ is injective. That is we can always regard R as a subring in QUOT R

$$R \hookrightarrow \text{QUOT } R : a \mapsto a/1 \text{ is injective}$$

And as NZD R is saturated we can give the units of QUOT R explicitly

$$(\operatorname{QUOT} R)^* = \left\{ \frac{u}{v} \mid u, v \in \operatorname{NZD} R \right\}$$

In particular we find that QUOT R is a field if and only if NZD $R = R \setminus \{0\}$ and this is precisely the property of R being an integral domain. That is we obtain the equivalence

R integral domain \iff QUOT R field

• Consider some field $(F, +, \cdot)$ and a subring $R \leq_{\mathrm{r}} F$. In particular $R \neq 0$ is a non-zero integral domain and hence QUOT R is a field. Let us now denote the subfield of F generated by R by E, explicitly

$$E := \{ ab^{-1} \mid a, b \in R \}$$

Then is is straightforward to check that the algebraic operations on the quotient field QUOT R coincide with those of the field E. That is we obtain a well-defined isomorphism of rings

QUOT
$$R \cong_{\mathbf{r}} E : \frac{a}{b} \mapsto ab^{-1}$$

• Consider any $u \in R$, then clearly $U := \{1, u, u^2, u^3, ...\}$ is multiplicatively closed. Hence we obtain a commutative ring by

$$R_u := \left\{ u^k \mid k \in \mathbb{N} \right\}^{-1} R$$

in which u = u/1 is invertible (with inverse 1/u). By the remarks above it is clear that $R_u = 0$ is zero if and only if u is a nilpotent of R. And $R \hookrightarrow R_u$ is embedded under κ if and only if u is a non-zero divisor of R, respectively isomorphic if u is a unit. Altogether

$$R_u = 0 \iff u \in \text{NIL } R$$

$$\kappa : R \hookrightarrow R_u \iff u \in \text{NZD } R$$

$$\kappa : R \cong_{\mathbf{r}} R_u \iff u \in R^*$$

• In (2.9) and (in a more general version) in (2.94) we have seen, that the complement $R \setminus \mathfrak{p}$ of a prime ideal $\mathfrak{p} \leq_i R$ is multiplicatively closed. Thus for prime ideals \mathfrak{p} we may always define the localisation

ŀ

$$R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} R$$

And by going to complements it is clear that R is embedded into $R_{\mathfrak{p}}$ under κ , iff \mathfrak{p} is contained in the set of zero divisors of R

 $\kappa: R \, \hookrightarrow \, R_{\mathfrak{p}} \quad \Longleftrightarrow \quad \mathfrak{p} \, \subseteq \, \mathrm{ZD} \, R$

In any case - as $R \setminus \mathfrak{p}$ is saturated multiplicatively closed subset we can explicitly describe the group of units of $R_{\mathfrak{p}}$ to be the following

$$(R_{\mathfrak{p}})^* = \left\{ \frac{u}{v} \mid u, v \notin \mathfrak{p} \right\}$$

• If $(R, +, \cdot)$ is an integral domain and $\mathfrak{P} \leq_{\mathbf{i}} R$ is a prime ideal of R then we get an easy alternative description of the localised ring $R_{\mathfrak{P}}$: let E := QUOT R be the quotient field of R, then we denote:

$$E_{\mathfrak{p}} := \left\{ \frac{a}{b} \in E \mid b \notin \mathfrak{p} \right\}$$

And thereby we obtain a canonical isomorphy from the localised ring $R_{\mathfrak{p}}$ to $E_{\mathfrak{p}}$ by virtue of $a/b \mapsto a/b$. (One might hence be tempted to say $R_{\mathfrak{p}} = E_{\mathfrak{p}}$, but - from a set-theoretical point of view - this is not quite true, as the equivalency class $a/b \in R_{\mathfrak{p}}$ only is a subset of $a/b \in E_{\mathfrak{p}}$)

$$R_{\mathfrak{p}} \cong_{\mathrm{r}} E_{\mathfrak{p}} : \frac{a}{b} \mapsto \frac{a}{b}$$

Note that under this isomorphy the maximal ideal $\mathfrak{M}_{\mathfrak{p}}$ of $R_{\mathfrak{p}}$ induced by \mathfrak{p} (that is $\mathfrak{M}_{\mathfrak{p}} := \mathfrak{p}R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$) corresponds to

$$\mathfrak{m}_{\mathfrak{p}} \quad \longleftrightarrow \quad \left\{ \left. \frac{a}{b} \in E \right| \ a \in \mathfrak{p}, \ b \notin \mathfrak{p} \right\}$$

(2.98) Lemma: (viz. 350) Local-Global-Principle

Let $(R, +, \cdot)$ be any commutative ring and $a, b \in R$, then equivalent are

$$a = b \quad \Longleftrightarrow \quad \forall \, \mathfrak{p} \in \operatorname{spec} R \; : \; \frac{a}{1} = \frac{b}{1} \in R_{\mathfrak{p}}$$
$$\iff \quad \forall \, \mathfrak{m} \in \operatorname{smax} R \; : \; \frac{a}{1} = \frac{b}{1} \in R_{\mathfrak{m}}$$

Further if R is an integral domain and F := QUOT R is its quotient field, then we can embed R into E, as $R = \{a/1 \in F \mid a \in R\}$. Likewise if $\mathfrak{p} \leq_i R$ is a prime ideal then we embed the localisation into F as well, as $R_{\mathfrak{p}} := \{a/u \in F \mid a \in R, u \notin \mathfrak{p}\}$. And thereby we obtain the following identities (as subsets of F)

$$R = \bigcap_{\mathfrak{p} \in \operatorname{spec} R} R\mathfrak{p} = \bigcap_{\mathfrak{m} \in \operatorname{smax} R} R\mathfrak{m}$$

(2.99) Proposition: (viz. 351) Universal Property

Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings, $U \subseteq R$ be a multiplicatively closed subset and $\varphi : R \to S$ be a homomorphism of rings, such that $\varphi(U) \subseteq S^*$. Then there is a uniquely determined homomorphism of rings $\overline{\varphi} : U^{-1}R \to S$ such that $\overline{\varphi}\kappa = \varphi$. And this is given to be

$$\overline{\varphi} : U^{-1}R \to S : \frac{a}{u} \mapsto \varphi(a)\varphi(u)^{-1}$$

(2.100) Remark:

Let $(R, +, \cdot)$ be a commutative ring and $U, V \subseteq R$ be multiplicatively closed sets, such that $U \subseteq V$. Further consider the canonical homomorphism $\kappa : R \to V^{-1}R : a \mapsto a/1$. Then it is clear that $\kappa(U) \subseteq (V^{-1}R)^*$, as the inverse of u/1 is given to be 1/u. Thus by the above proposition we obtain an induced homomorphism

$$\overline{\kappa} : U^{-1}R \to V^{-1}R : \frac{a}{u} \mapsto \frac{a}{u}$$

Thereby $\overline{\kappa}(a/u) = 0/1$ iff there is some $v \in V$ such that va = 0. And this is precisely the same property for $\kappa(a) = 0/1$. Hence the kernel of $\overline{\kappa}$ is just

$$\operatorname{kn}(\overline{\kappa}) = U^{-1}(\operatorname{kn}(\kappa)) = \left\{ \frac{a}{u} \mid a \in \operatorname{kn}(\kappa), u \in U \right\}$$

(2.101) Definition: (viz. 351)

Let $(R, +, \cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and denote the canonical homomorphism, by $\kappa : R \to U^{-1}R : a \mapsto a/1$ again. If now $\mathfrak{a} \leq_{\mathbf{i}} R$ and $\mathfrak{u} \leq_{\mathbf{i}} U^{-1}R$ are ideals then we define the transferred ideals $\mathfrak{u} \cap R \leq_{\mathbf{i}} R$ and $U^{-1}\mathfrak{a} \leq_{\mathbf{i}} U^{-1}R$ to be the following

$$\begin{split} \mathfrak{u} \cap R &:= \kappa^{-1}(\mathfrak{u}) = \left\{ a \in R \mid \frac{a}{1} \in \mathfrak{u} \right\} \\ U^{-1}\mathfrak{a} &:= \langle \kappa(\mathfrak{a}) \rangle_{\mathbf{i}} = \left\{ \frac{a}{u} \mid a \in \mathfrak{a}, u \in U \right\} \end{split}$$

(2.102) Example:

Let $(R, +, \cdot)$ be any commutative ring, $a \in R$ and $U \subseteq R$ be multiplicatively closed. Then an easy, straightforward computation shows

$$U^{-1}(aR) = \frac{a}{1}U^{-1}R$$

(2.103) Definition: (viz. 352)

Let $(R, +, \cdot)$ be a commutative ring, $U \subseteq R$ be a multiplicatively closed set and $\mathfrak{a} \leq_{i} R$ be an ideal of R. Then we obtain another ideal $\mathfrak{a} : U \leq_{i} R$ by

$$\mathfrak{a}: U := \{ b \in R \mid \exists v \in U : vb \in \mathfrak{a} \}$$

And clearly $\mathfrak{a}: U \leq_{i} R$ thereby is an ideal of R containing $\mathfrak{a} \subseteq \mathfrak{a}: U$ and using the notation of (2.101) we finally obtain the equality

$$(U^{-1}\mathfrak{a}) \cap R = \mathfrak{a} : U$$

(2.104) Proposition: (viz. 352)

Let $(R, +, \cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed subset. Further let $\mathfrak{a}, \mathfrak{b} \leq_{\mathbf{i}} R$ be any two ideals of R, then we obtain

$$U^{-1}(\mathfrak{a} \cap \mathfrak{b}) = (U^{-1}\mathfrak{a}) \cap (U^{-1}\mathfrak{b})$$
$$U^{-1}(\mathfrak{a} + \mathfrak{b}) = (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$$
$$U^{-1}(\mathfrak{a}\mathfrak{b}) = (U^{-1}\mathfrak{a}) (U^{-1}\mathfrak{b})$$
$$U^{-1}\sqrt{\mathfrak{a}} = \sqrt{U^{-1}\mathfrak{a}}$$

$$\begin{aligned} & (\mathfrak{a}:U):U &= \mathfrak{a}:U \\ & (\mathfrak{a}\cap\mathfrak{b}):U &= (\mathfrak{a}:U)\cap(\mathfrak{b}:U) \\ & \sqrt{\mathfrak{a}}:U &= \sqrt{\mathfrak{a}:U} \end{aligned}$$

Conversely consider any two ideals $\mathfrak{u}, \mathfrak{w} \leq_{i} U^{-1}R$ and abbreviate $\mathfrak{a} := \mathfrak{u} \cap R$ and $\mathfrak{b} := \mathfrak{w} \cap R \leq_{i} R$. Then we likewise get the identities

$$\begin{array}{rcl} (\mathfrak{u} \cap \mathfrak{w}) \cap R &=& \mathfrak{a} \cap \mathfrak{b} \\ (\mathfrak{u} + \mathfrak{w}) \cap R &=& (\mathfrak{a} + \mathfrak{b}) : U \\ (\mathfrak{u} \mathfrak{w}) \cap R &=& (\mathfrak{a} \mathfrak{b}) : U \\ \sqrt{\mathfrak{u}} \cap R &=& \sqrt{\mathfrak{a}} \end{array}$$

(2.105) Example:

The equality $(\mathfrak{a} + \mathfrak{b}) : U = (\mathfrak{a} : U) + (\mathfrak{b} : U)$ need not hold true. As an example consider $R = \mathbb{Z}, U := \{1, 2, 4, 8, ...\}, \mathfrak{a} = 9\mathbb{Z}$ and $\mathfrak{b} = 15\mathbb{Z}$. Then it is clear that $\mathfrak{a} : U = \mathfrak{a}$ and $\mathfrak{b} : U = \mathfrak{b}$ such that $(\mathfrak{a} : U) + (\mathfrak{b} : U) = 3\mathbb{Z}$ (as 3 is the greatest common divisor of 9 and 15). Yet $13 \cdot 2 = 26 = 9 + 15 \in \mathfrak{a} + \mathfrak{b}$. Thus $13 \in (\mathfrak{a} + \mathfrak{b}) : U$ even though $13 \notin 3\mathbb{Z} = (\mathfrak{a} : U) + (\mathfrak{b} : U)$.

(2.106) Definition: (viz. 354)

Let $(R, +, \cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed set in R. Then we define the following sets of ideals in R

$$U^{-1} \text{ideal } R := \{ \mathfrak{a} \in \text{ideal } R \mid \mathfrak{a} = \mathfrak{a} : U \}$$

$$= \{ \mathfrak{a} \in \text{ideal } R \mid u \in U, ua \in \mathfrak{a} \implies a \in \mathfrak{a} \}$$

$$U^{-1} \text{srad } R := \operatorname{srad} R \cap (U^{-1} \text{ideal } R)$$

$$U^{-1} \text{spec } R := \operatorname{spec} R \cap (U^{-1} \text{ideal } R)$$

$$= \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \cap U = \emptyset \}$$

$$U^{-1} \text{smax } R := \operatorname{smax} R \cap (U^{-1} \text{ideal } R)$$

$$= \{ \mathfrak{m} \in \operatorname{smax} R \mid \mathfrak{m} \cap U = \emptyset \}$$

(2.107) Proposition: (viz. 354)

Let $(R, +, \cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed set in R. Then we obtain an order-preserving one-to-one correspondence between the ideals of the localisation $U^{-1}R$ and U^{-1} ideal R, formally

$$\begin{aligned} \operatorname{ideal} \left(U^{-1} R \right) & \longleftrightarrow \quad \left(U^{-1} \operatorname{ideal} R \right) \\ \mathfrak{u} & \mapsto \quad \mathfrak{u} \cap R \\ U^{-1} \mathfrak{a} & \longleftrightarrow \quad \mathfrak{a} \end{aligned}$$

• This correspondence is order-preserving, that is for any two ideals \mathfrak{a} , $\mathfrak{b} \in U^{-1}$ ideal R and \mathfrak{u} , $\mathfrak{w} \in$ ideal $U^{-1}R$ respectively, we get

$$\mathfrak{a} \subseteq \mathfrak{b} \implies U^{-1}\mathfrak{a} \subseteq U^{-1}\mathfrak{b} \\ \mathfrak{u} \subseteq \mathfrak{w} \implies \mathfrak{u} \cap R \subseteq \mathfrak{w} \cap R$$

• And this correspondence correlates maximal, prime and radical ideals of $U^{-1}R$ with U^{-1} smax R, U^{-1} spec R respectively with U^{-1} srad R

$$\begin{aligned} \operatorname{ideal} (U^{-1}R) &\longleftrightarrow & (U^{-1}\operatorname{ideal} R) \\ & \cup & & \cup \\ \operatorname{srad} (U^{-1}R) &\longleftrightarrow & U^{-1}(\operatorname{srad} R) \\ & \cup & & \cup \\ \operatorname{spec} (U^{-1}R) &\longleftrightarrow & U^{-1}(\operatorname{spec} R) \\ & \cup & & \cup \\ \operatorname{smax} (U^{-1}R) &\longleftrightarrow & U^{-1}(\operatorname{smax} R) \end{aligned}$$

(2.108) Example:

- Thus the ideal structure of $U^{-1}R$ is simpler than that of R itself. The most drastic example is the following \mathbb{Z} has a multitude of ideals (namely all $a\mathbb{Z}$ where $a \in \mathbb{N}$, which are countably many). Yet $\mathbb{Q} =$ QUOT \mathbb{Z} if a field and hence only has the trivial ideals 0 and \mathbb{Q} itself.
- Let now $(R, +, \cdot)$ be any commutative ring and choose any $u \in R$, then the spectrum of R_u corresponds (under the mapping $\mathfrak{u} \mapsto \mathfrak{u} \cap R$ of the proposition above) to the following subset of the spectrum of R

$$\operatorname{spec} R_u \iff \{ \mathfrak{p} \in \operatorname{spec} R \mid u \notin \mathfrak{p} \}$$

PROB this is clear as for prime ideals \mathfrak{P} of R we have the equivalence $u \in \mathfrak{P} \iff \{u, u^2, u^3, \ldots\} \subseteq \mathfrak{P} \iff \mathfrak{P} \cap \{u, u^2, u^3, \ldots\} \neq \emptyset$ such that the claim is immediate from (2.107).

• Let $\mathfrak{q} \in \operatorname{spec} R$ be a fixed prime ideal of R, then (for any other prime ideal \mathfrak{p} of R) clearly $\mathfrak{p} \cap (R \setminus \mathfrak{q}) = \emptyset$ is equivalent to $\mathfrak{p} \subseteq \mathfrak{q}$. Using this in the above proposition (2.107) we find the correspondence

spec $R_{\mathfrak{q}} \longleftrightarrow \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \subseteq \mathfrak{q}\}$

Thus localizing in \mathfrak{q} simply preserves the prime ideals below \mathfrak{q} and deletes all the prime ideals beyond \mathfrak{q} . Note that this is just the opposite of the quotient R/\mathfrak{q} - here all the ideals below \mathfrak{q} are cut off. That is let $\mathcal{P} := \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \subseteq \mathfrak{q} \text{ or } \mathfrak{q} \subseteq \mathfrak{p} \}$ be the set of all prime ideals of R comparable with \mathfrak{q} . Then the situation is the following



(2.109) Corollary: (viz. 358)

Let $(R, +, \cdot)$ be a commutative ring and $U \subseteq R$ be a multiplicatively closed subset with $0 \notin U$. Further let us abbreviate by \star any one of the words *integral domain, noetherian ring, artinian ring, UFD, PID, DKD* or *normal ring.* Then we get the following implication

$$R \text{ is a } \star \implies U^{-1}R \text{ is a } \star$$

(2.110) Corollary: (viz. 361)

Let $(R, +, \cdot)$ be an integral domain and denote its quotient field by E := QUOT R. Then the following three statements are equivalent

- (a) R is normal
- (b) $\forall \mathfrak{p} \in \operatorname{spec} R : R_{\mathfrak{p}} \text{ is normal}$
- (c) $\forall \mathfrak{m} \in \operatorname{smax} R : R_{\mathfrak{m}} \text{ is normal}$

(2.111) Proposition: (viz. 355)

Let $(R, +, \cdot)$ be any commutative ring, then we present a couple of useful isomorphies concerning localisations: fix a multiplicatively closed set $U \subseteq R$ and some point $u \in R$ then we obtain

(i) The localisation of the polynomial ring R[t] is isomorphic to the polynomial ring over the localized ring, formally that is

$$\begin{array}{rcl} U^{-1}\big(R[t]\big) &\cong_{\mathbf{r}} & (U^{-1}R)[t] \\ \\ \frac{f}{u} &\mapsto & \displaystyle\sum_{\alpha=0}^{\infty} \frac{f[\alpha]}{u} t^{\alpha} \end{array}$$

(ii) The localized ring R_u is just a quotient of some polynomial ring of R

$$R_u \cong_{\mathbf{r}} \frac{R[t]}{(ut-1)R[t]}$$

$$\frac{a}{u^k} \mapsto at^k + (ut-1)R[t]$$

$$f(1/u) \iff f + (ut-1)R[t]$$

(iii) Let $(R, +, \cdot)$ be an integral domain and $0 \notin U \subseteq R$ be a multiplicatively closed subset of R not containing 0. Then the quotient fields of R and $U^{-1}R$ are isomorphic under

QUOT
$$R \cong_{\mathbf{r}} \operatorname{QUOT} U^{-1}R : \frac{a}{b} \mapsto \frac{a/1}{b/1}$$

(iv) Let $(R, +, \cdot)$ be an integral domain and $0 \neq a, b \in R$ be two non-zero elements of R and let $n \in \mathbb{N}$. Then we obtain the following isomorphy

$$\left(R_a\right)_{b/a^n} \cong_{\mathbf{r}} R_{ab} : \frac{x/a^i}{(b/a^n)^j} \mapsto \frac{xa^{(n+1)j}b^i}{(ab)^{i+j}}$$

(v) Consider $U \subseteq R$ multiplicatively closed and $\mathfrak{a} \leq_{i} R$ any ideal of R such that $U \cap \mathfrak{a} = \emptyset$. Now denote $U/\mathfrak{a} := \{ u + \mathfrak{a} \mid u \in U \}$, then we obtain the following isomorphy

$$\frac{U^{-1}R}{U^{-1}\mathfrak{a}} \cong_{\mathbf{r}} \left(\frac{U}{\mathfrak{a}}\right)^{-1} \left(\frac{R}{\mathfrak{a}}\right)$$
$$\frac{b}{v} + U^{-1}\mathfrak{a} \mapsto \frac{b+\mathfrak{a}}{v+\mathfrak{a}}$$

(vi) In particular: let $p \leq_i R$ be a prime ideal and $\mathfrak{a} \leq_i R$ be any ideal of R such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then we denote $\mathfrak{a}_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}\mathfrak{a}$ and thereby obtain the following isomorphy

$$R_{\mathfrak{p}/\mathfrak{a}_{\mathfrak{p}}} \cong_{\mathrm{r}} (R/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}} : \frac{b}{u} + \mathfrak{a}_{\mathfrak{p}} \mapsto \frac{b + \mathfrak{a}}{u + \mathfrak{a}}$$

(vii) Let $\mathfrak{p} \leq_{\mathbf{i}} R$ be a prime ideal of R and denote $\overline{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$. If now $a \notin \mathfrak{p}$ is *not* contained in \mathfrak{p} then we obtain the isomorphy

$$R_{\mathfrak{p}} \cong_{\mathbf{r}} (R_a)_{\overline{\mathfrak{p}}} : \frac{a}{u} \mapsto \frac{r/1}{u/1}$$

. .

2.10 Local Rings

(2.112) Definition: (viz. 364)

Let $(R, +, \cdot)$ be any commutative ring, then R is said to be a **local ring**, iff it satisfies one of the following two equivalent properties

- (a) R has precisely one maximal ideal (i.e. $\# \operatorname{smax} R = 1$)
- (b) the set of non-units is an ideal in R (i.e. $R \setminus R^* \leq_i R$)

NOTA and in this case the uniquely determined maximal ideal of R is precisely the set $R \setminus R^* = \{a \in R \mid aR \neq R\}$ of non-units of R.

(2.113) Proposition: (viz. 365)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{m} \leq_i R$ be a proper ideal of R (that is $\mathfrak{m} \neq R$). Then the following four statements are equivalent

- (a) R is a local ring with maximal ideal \mathfrak{m}
- (b) $\forall \mathfrak{a} \leq_{\mathrm{i}} R : \mathfrak{a} \neq R \implies \mathfrak{a} \subseteq \mathfrak{m}$
- (c) $R \setminus \mathfrak{m} = R^*$
- (d) $R \setminus \mathfrak{m} \subseteq R^*$

(2.114) Example:

- If (F,+, ·) is a field, then F \ {0} = F*, in particular F already is a local ring having the maximal ideal {0}.
- Let $(E, +, \cdot)$ be a field and consider the ring of formal power series $R := E[\![t]\!]$ over E. Then $E[\![t]\!]$ is a local ring having the maximal ideal

$$\mathfrak{m} := t E[t] = \{ f \in E[t] \mid f[0] = 0 \}$$

To prove this it suffices to check $R \setminus \mathfrak{m} \subseteq R^*$ (due to the above proposition (2.113)). But in fact if $f \in E[t]$ is any power series with $f[0] \neq 0$ then an elementary computation shows that we can iteratively compute the inverse of f, by

$$f^{-1}[0] = \frac{1}{f[0]}$$

$$f^{-1}[k] = \frac{-1}{f[0]} \sum_{j=0}^{k-1} f[k-j] f^{-1}[j]$$

• Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{P} \leq_{\mathbf{i}} R$ be any prime ideal of R. Then in (2.115) below we will prove that the localised ring $R_{\mathfrak{P}}$ is a local ring having the maximal ideal

$$\mathfrak{m}_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} \mathfrak{p} = \{ p/u \mid p \in \mathfrak{p}, u \notin \mathfrak{p} \}$$

• Let $(S, +, \cdot)$ be a PID, $1 \le n \in \mathbb{N}$ and $p \in S$ be a prime element of S. Then we have proved in (2.89.(iii)) that $R := S/p^n S$ is a local ring having the maximal ideal

NIL
$$R = \operatorname{ZD} R = R \setminus R^* = (p + p^n S) R$$

(2.115) Proposition: (viz. 365)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{P} \leq_i R$ be a prime ideal. Then $R_{\mathfrak{P}}$ is a local ring (i.e. a ring with precisely one maximal ideal). Thereby the maximal ideal of $R_{\mathfrak{P}}$ is given to be

$$\mathfrak{m}_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} \mathfrak{p} = \{ p/u \mid p \in \mathfrak{p}, u \notin \mathfrak{p} \}$$

And the residue field of $R_{\mathfrak{p}}$ is isomorphic to the quotient field of R/\mathfrak{p} via

$$R_{\mathfrak{p}/\mathfrak{m}_{\mathfrak{p}}} \cong_{\mathrm{f}} \operatorname{QUOT} R/\mathfrak{p} : \frac{a}{u} + \mathfrak{m}_{\mathfrak{p}} \mapsto \frac{a+\mathfrak{p}}{u+\mathfrak{p}}$$

(2.116) Proposition: (viz. 383) (\diamondsuit)

Let $(R, +, \cdot)$ be a local, noetherian ring with maximal ideal \mathfrak{m} and denote the *residue field* of R by $E := R/\mathfrak{m}$. We now regard \mathfrak{m} as an R-module, then $\mathfrak{m}/\mathfrak{m}^2$ becomes an E-vector space under the following scalar multiplication:

$$(a+\mathfrak{m})(m+\mathfrak{m}^2) \ := \ (am)+\mathfrak{m}^2$$

And if we now denote by $\operatorname{rank}_R(\mathfrak{m})$ the minimal number $k \in \mathbb{N}$ such that there are elements $m_1, \ldots, m_k \in \mathfrak{m}$ with $\mathfrak{m} = Rm_1 + \cdots + Rm_k$, then we get

$$\dim_E\left(\mathfrak{m}/\mathfrak{m}^2\right) = \operatorname{rank}_R(\mathfrak{m})$$

(2.117) Definition:

Let $(R, +, \cdot)$ be any non-zero (i.e. $R \neq 0$), commutative ring, then a mapping $\nu : R \to \mathbb{N} \cup \{\infty\}$ is called a **valuation** (and the ordered pair (R, ν) a **valued ring**) if for any $a, b \in R$ we obtain the following properties

- (1) $\nu(a) = \infty \iff a = 0$
- (2) $\nu(ab) = \nu(a) + \nu(b)$
- (3) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$

And a valuation ν is said to be **normed** iff it further satisfies the property

(N) $\exists a \in S : \nu(a) = 1$

(2.118) Proposition: (viz. 365)

- (i) Let (R, ν) be a valued ring (in particular $R \neq 0$), then R and its valuation ν already satisfy the following additional properties
 - (U) $\alpha \in R^* \implies \nu(\alpha) = 0$
 - (I) R is an integral domain
 - (P) $[\nu] := \{a \in R \mid \nu(a) \ge 1\} \in \operatorname{spec} R$
- (ii) If $(R, +, \cdot)$ is a non-zero integral domain then R always carries the **trivial valuation** $\tau : R \to \mathbb{N} \cup \{\infty\}$ defined by $\tau(a) := 0$ iff $a \neq 0$ and $\tau(a) := \infty$ iff a = 0. Note that this valuation is *not* normed.
- (iii) Let $(R, +, \cdot)$ be a noetherian integral domain and consider any $p \in R$ prime. Then we obtain a normed valuation $\nu = \nu_p$ on R by

$$\nu \ : \ R \to \mathbb{N} \cup \{\infty\} \ : \ a \mapsto a[p]$$

where $a[p] \ := \ \sup\{k \in \mathbb{N} \mid p^k \mid a\}$

In particular we have $\nu(p) = 1$ and $[\nu] = pR$. And for any $a, b \in R$ this valuation satisfies a fifth property, namely we get

$$\nu(a) \neq \nu(b) \implies \nu(a+b) = \min\{\nu(a), \nu(b)\}$$

(iv) Let $(R, +, \cdot)$ be a PID then we obtain a one-to-one correspondence between the maximal spectrum of R and the normed valuations on R:

$$\begin{array}{rcl} \operatorname{smax} R & \longleftrightarrow & \left\{ \nu : R \to \mathbb{N} \cup \left\{ \infty \right\} \mid (1), (2), (3), (N) \right\} \\ \mathfrak{m} & \mapsto & \nu_p \text{ where } \mathfrak{m} = pR \\ [\nu] & \longleftrightarrow & \nu \end{array}$$

(2.119) Definition:

Let $(R, +, \cdot)$ be a commutative ring, then we call $\nu : R \to \mathbb{N} \cup \{\infty\}$ a **discrete valuation** on R (and the ordered pair (R, ν) is said to be a **discrete valuation ring**), iff ν satisfies all of the following properties $(\forall a, b \in R)$

- (1) $\nu(a) = \infty \iff a = 0$
- (2) $\nu(ab) = \nu(a) + \nu(b)$
- (3) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$
- (4) $\nu(a) \le \nu(b) \implies a \mid b$
- (N) $\exists m \in R : \nu(m) = 1$

(2.120) Proposition: (viz. 367)

Let (R, ν) be a discrete valuation ring, then R and its valuation ν already satisfy all of the following additional properties

- (i) (R, ν) is a valued ring, in particular R is a non-zero integral domain.
- (ii) R is a local ring with maximal ideal $[\nu] = \{a \in R \mid \nu(a) \ge 1\}.$
- (iii) (R,ε) is an Euclidean domain under $\varepsilon : R \setminus \{0\} \mapsto \mathbb{N} : a \mapsto \nu(a)$.
- (iv) Fix any $m \in R$ with $\nu(m) = 1$, then for any $0 \neq a \in R$ there is a uniquely determined unit $\alpha \in R^*$ such that $a = \alpha m^k$ for $k = \nu(a)$.
- (v) According to (iii) and (iv) the set of ideal of R is precisely the following

ideal
$$R = \left\{ m^k R \mid k \in \mathbb{N} \right\} \cup \{ 0 \}$$

- (vi) Let $(F, +, \cdot)$ be an arbitrary field and $\nu : F \to \mathbb{Z} \cup \{\infty\}$ be a function satisfying the following four properties (for any $x, y \in F$)
 - (1) $\nu(x) = \infty \iff x = 0$ (2) $\nu(xy) = \nu(x) + \nu(y)$ (3) $\nu(x+y) \ge \min\{\nu(x), \nu(y)\}$ (N) $\exists m \in F : \nu(m) = 1$

In this case ν is said to be a *discrete valuation* and further we obtain a subring R of F by letting $R := \{a \in F \mid \nu(a) \ge 0\} \le_{\mathrm{r}} F$. Also $\nu : R \to \mathbb{N} \cup \{\infty\}$ is a discrete valuation on R. Finally F is the quotient field of R, that is we get

$$F = \{ ab^{-1} \mid a, b \in F, b \neq 0 \}$$

(2.121) Example:

• We regard $F = \mathbb{Q}$ and any prime number $p \in \mathbb{Z}$. Then we obtain a discrete valuation $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by (where $a, b \in \mathbb{Z}, b \neq 0$)

$$\nu_p\left(\frac{a}{b}\right) := [a]_p - [b]_p$$
$$[a]_p := \sup\{k \in \mathbb{N} \mid p^k \mid a\}$$

Thereby ν_p is said to be the *p*-adic valuation of \mathbb{Q} . And if we denote $\mathfrak{p} := p\mathbb{Z}$, then the discrete valuation ring determined by ν_p is just $\mathbb{Z}_{\mathfrak{p}}$.

- More generally the above construction works out for any PID R: let F be the quotient field of R and $p \in R$ be any prime element. Then we may repeat the definition of ν_p literally (except for $a, b \in R$) and thereby obtain a discrete valuation $\nu_p : F \to \mathbb{Z} \cup \{\infty\}$. And the discrete valuation ring determined by ν_p is $R_{\mathfrak{p}}$ (where $\mathfrak{p} := pR$) again.
- The prototype of a discrete valuation ring is the ring of formal power series E[t] over a field E. And in this case we obtain a discrete valuation ν (note that $\nu = tE[t]$), by

$$\nu : E\llbracket t \rrbracket \to \mathbb{Z} \cup \{\infty\} : f \mapsto \sup\{k \in \mathbb{N} \mid t^k \mid f\}$$

(2.122) Theorem: (viz. 368)

A commutative ring $(R, +, \cdot)$ is said to be a **discrete valuation ring** (abbreviated by DVR), iff it satisfies one of the following equivalent properties

- (a) R admits a discrete valuation $\nu : R \to \mathbb{N} \cup \{\infty\}$
- (b) R is an integral domain and there is some element $0 \neq m \in R$ satisfying

$$R \setminus mR = R^*$$
 and $\bigcap_{k \in \mathbb{N}} m^k R = 0$

- (c) R is a PID and local ring but no field.
- (d) R is an UFD but no field and any two prime elements of R are associates (i.e. if $p, q \in R$ are irreducible, then we get pR = qR).
- (e) R is a noetherian integral domain and local ring, whose maximal ideal \mathfrak{m} is a non-zero principal ideal (i.e. $\mathfrak{m} = mR$ for some $0 \neq m \in R$).
- (f) R is a noetherian, normal and local ring with non-zero maximal ideal $\mathfrak{M} \neq 0$ and the only prime ideals of R are 0 and \mathfrak{M} (i.e. spec $R = \{0, \mathfrak{M}\}$).

(2.123) Definition:

A commutative ring $(R, +, \cdot)$ is said to be a **valuation ring**, iff it is a nonzero integral domain in which the *divides* relation is a total order. Formally that is, iff R satisfies the following three properties

- (1) $R \neq 0$
- (2) R is an integral domain
- (3) $\forall a, b \in R$ we get $a \mid b$ or $b \mid a$

(2.124) Remark:

The last property (3) in the definition above might seem a little artificial. We hence wish to explain where it comes from: as R is an integral domain we may regard its quotient field E := QUOT R. Then property (3) can be reformulated, as

$$\forall x \in E \setminus \{0\} : x \in R \text{ or } x^{-1} \in R$$

Thus if we are given a valuation (in the sense of fields) $\nu : E \to \mathbb{Z} \cup \{0\}$ on E, we may regard the subring $R := \{a \in E \mid \nu(a) \geq 0\}$. And it is clear that R satisfies the property $x \in R$ or $x^{-1} \in R$ for any $0 \neq x \in E$. Thus every ν is assigned a valuation ring R in E. Therefore valuation rings appear naturally whenever we regard valuations on fields.

(2.125) Proposition: (viz. 370)

- (i) If $(R, +, \cdot)$ is a valuation ring, then R already is a local ring and Bezout domain (that is any finitely generated ideal already is principal).
- (ii) If $(R, +, \cdot)$ is a valuation ring, then we get the following equivalencies
 - (a) R is noetherian
 - (b) R is a PID
 - (c) R is a DVR or field

2.11 Dedekind Domains

(2.126) Definition:

Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by F := QUOT R. Then a subset $\mathfrak{f} \subseteq F$ is called a **fraction ideal** of R (which we abbreviate by writing $\mathfrak{f} \leq_{\mathfrak{f}} R$) iff it satisfies

- (1) $f \leq_{\mathrm{m}} F$ is an *R*-submodule of *F*
- (2) $\exists 0 \neq r \in R$ such that $r \mathbf{f} \subseteq R$

(2.127) Remark:

- In particular any ideal $\mathfrak{a} \leq_{i} R$ is a fraction ideal $\mathfrak{a} \leq_{f} R$ (PROB just let r = 1). By abuse of nomenclature ordinary ideals of R are hence also said to be the *integral ideals* of F.
- Conversely for any fraction ideal $\mathfrak{f} \leq_{\mathfrak{f}} R$ we see that $\mathfrak{f} \cap R \leq_{\mathfrak{i}} R$ is an ideal of R. PROB because $0 \in \mathfrak{f} \cap R$ and if $f, g \in \mathfrak{f}$ and $a \in R$ then clearly $f + g \in \mathfrak{f} \cap R$ and $af \in \mathfrak{f} \cap R$ as both, \mathfrak{f} and R are R-modules.
- And clearly for any $x \in F$ the generated module $\mathfrak{f} := xR$ is a fraction ideal $\mathfrak{f} \leq_{\mathfrak{f}} R$ of R PROB because if x = r/s then $s\mathfrak{f} = rR \subseteq R$.
- If R itself is a field, then F = R and the only possible fraction ideals of R are 0 and R (PROB if $0 \neq x \in \mathfrak{f} \leq_{\mathfrak{f}} R$ then x has an inverse in R and hence $1 = x^{-1}x \in \mathfrak{f}$. Thus for any $a \in R$ we have $a = a1 \in \mathfrak{f}$).

(2.128) Proposition: (viz. 371)

Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by F := QUOT R. As in the case of integral ideals, if f and $g \leq_{\text{f}} R$ are fraction ideals of R, then the sum $\mathfrak{f} + \mathfrak{g}$, intersection $\mathfrak{f} \cap \mathfrak{g}$ and product $\mathfrak{f} \mathfrak{g}$ of finitely many fraction ideals is a fraction ideal again. And if $\mathfrak{g} \neq 0$ we may also define the quotient $\mathfrak{f} : \mathfrak{g}$ of two fraction ideals. I.e. if f and $g \leq_{\text{f}} R$ are fraction ideals of R then we obtain further fraction ideals of R by letting

$$\begin{split} \mathfrak{f} + \mathfrak{g} &:= \left\{ x + y \mid x \in \mathfrak{f}, y \in \mathfrak{g} \right\} \\ \mathfrak{f} \cap \mathfrak{g} &:= \left\{ x \mid x \in \mathfrak{f} \text{ and } x \in \mathfrak{g} \right\} \\ \mathfrak{f} : \mathfrak{g} &:= \left\{ x \in F \mid x \mathfrak{g} \subseteq \mathfrak{f} \right\} \end{split}$$

$$\begin{split} \mathfrak{f} \mathfrak{g} &:= \left\{ \sum_{i=1}^{n} f_{i} g_{i} \mid n \in \mathbb{N}, f_{i} \in \mathfrak{f}, g_{i} \in \mathfrak{g} \right\} \end{split}$$

(2.129) Remark:

• Let now $0 \neq \mathfrak{f}$ and $\mathfrak{g} \leq_{\mathfrak{f}} R$ be two non-zero fraction ideals of the integral domain $(R, +, \cdot)$ and let F = QUOT R. Then the product \mathfrak{fg} and quotient $\mathfrak{f} : \mathfrak{g} \neq 0$ are non-zero, too. Formally that is

$$\mathbf{f}, \mathbf{g} \neq 0 \implies \mathbf{f} \mathbf{g} \neq 0 \text{ and } \mathbf{f} : \mathbf{g} \neq 0$$

PROB as \mathfrak{f} and $\mathfrak{g} \neq 0$ we may choose some $0 \neq f \in \mathfrak{f}$ and $0 \neq g \in \mathfrak{g}$. Then $fg \in \mathfrak{f}\mathfrak{g}$ and $fg \neq 0$, as F is an integral domain (yielding $\mathfrak{f}\mathfrak{g} \neq 0$). Now let $s\mathfrak{g} \subseteq R$ for some $s \neq 0$. Then $(sf)\mathfrak{g} = f(s\mathfrak{g}) \subseteq fR \subseteq \mathfrak{f}$ and hence $sf \in \mathfrak{f} : \mathfrak{g}$. But as $sf \neq 0$ this means $\mathfrak{f} : \mathfrak{g} \neq 0$.

• For any fraction ideal $\oint \trianglelefteq_f R$ we always get the following two inclusions

$$\mathbf{f}(R:\mathbf{f}) \subseteq R \subseteq \mathbf{f}:\mathbf{f}$$

PROB $\mathbf{f}(R:\mathbf{f})$ contains elements of the form $x_1y_1 + \cdots + x_ny_n$ where $x_i \in R:\mathbf{f}$ and $y_i \in \mathbf{f}$. But by definition of $R:\mathbf{f}$ this means $x_iy_i \in R$ and hence $x_1y_1 + \cdots + x_ny_n \in R$. And $R \subseteq \mathbf{f}:\mathbf{f}$ is clear, as $\mathbf{f} \leq_{\mathrm{m}} F$.

• First note that the multiplication \mathfrak{fg} of fraction ideals is both commutative and associative. Further it is clear that for any fraction ideal $\mathfrak{f} \leq_{\mathfrak{f}} R$ we get $R\mathfrak{f} = \mathfrak{f}$. That is the set of fraction ideals of R is a commutative monoid under the multiplication (defined in (2.128)) with neutral element R. This naturally leads to the definition of an *invertible* fraction ideal. Of course the non-zero fraction ideals als form a monoid and this is called the *class monoid* of R, denoted by

$$\mathcal{C}(R) := \left\{ \mathbf{f} \leq_{\mathbf{f}} R \mid \mathbf{f} \neq 0 \right\}$$

(2.130) Definition: (viz. 371)

Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by F := QUOT R. Then a fraction ideal $\oint \trianglelefteq_f R$ of R is said to be **invertible**, iff it satisfies one of the following two equivalent conditions

- (a) $\exists \mathfrak{g} \leq_{\mathbf{f}} R : \mathfrak{f}\mathfrak{g} = R$
- (b) f(R:f) = R

Note that in this case the fraction ideal \mathfrak{g} with $\mathfrak{f}\mathfrak{g}$ is uniquely determined, to be $\mathfrak{g} = R : \mathfrak{f}$. And it is called the **inverse** of \mathfrak{f} , written as

$$\mathbf{f}^{-1} := \mathbf{g} = R:\mathbf{f}$$

(2.131) Proposition: (viz. 372)

Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by F := QUOT R. If now $0 \neq \mathfrak{a} \leq_i R$ is a non-zero ideal of R, then the following statements are equivalent

- (a) \mathfrak{a} is invertible (as a fraction ideal of R), i.e. there is some fraction ideal $\mathfrak{g} \trianglelefteq_{\mathfrak{f}} R$ of R such that $\mathfrak{ag} = R$.
- (b) There are some $a_1, \ldots, a_n \in \mathfrak{a}$ and $x_1, \ldots, x_n \in F$ such that for any $i \in 1 \ldots n$ we get $x_i \mathfrak{a} \subseteq R$ and $a_1 x_1 + \cdots + a_n x_n = 1$.
- (c) \mathfrak{a} is a projective *R*-module, i.e. there is a free *R*-module *M* and a submodule $P \leq_{\mathrm{m}} M$ such that $\mathfrak{a} \oplus P = M$.

(2.132) Corollary: (viz. 373)

Let $(R, +, \cdot)$ be a local ring, that also is an integral domain. If now $0 \neq \mathfrak{a} \leq_i R$ is a non-zero ideal of R then the following statements are equivalent

- (a) \mathfrak{a} is a principal ideal (i.e. $\mathfrak{a} = aR$ for some $a \in R$)
- (b) \mathfrak{a} is invertible (as a fraction ideal $\mathfrak{a} \leq_{\mathrm{f}} R$)

(2.133) Remark:

• If aR is any non-zero $(a \neq 0)$ principal ideal in an integral domain $(R, +, \cdot)$, then $aR \leq_{\mathrm{f}} R$ is an invertible fraction ideal of R. This is clear as its inverse obviously given by

$$\left(aR\right)^{-1} = \frac{1}{a}R$$

• Now consider an (integral) ideal $\mathfrak{a} \leq_i R$ and elements $a_1, \ldots, a_n \in \mathfrak{a}$ and $x_1, \ldots, x_n \in R : \mathfrak{a} \subseteq F$ such that $a_1x_1 + \cdots + a_nx_n = 1$. Then \mathfrak{a} is already generated by the a_i , formally that is

$$\mathfrak{a} = \langle a_1, \ldots, a_n \rangle_{\mathbf{i}}$$

PROB the inclusion " \supseteq " is clear, as $a_i \in \mathfrak{a}$. For the converse inclusion we consider any $a \in \mathfrak{a}$. As $x_i \in R : \mathfrak{a}$ we in particlar have $x_i \mathfrak{a} \subseteq R$. And because of $a_1x_1 + \cdots + a_nx_n = 1$ we are able to write a in the form $a = (x_1a)a_1 + \cdots + (x_na)a_n \in \langle a_1, \ldots, a_n \rangle_i$.

• We have seen in the proposition above, that an (integral) ideal $\mathfrak{a} \leq_{i} R$ is invertible if and only if there are $a_1, \ldots, a_n \in \mathfrak{a}$ and $x_1, \ldots, x_n \in F$ such that for any $i \in 1 \ldots n$ we get

$$x_i \mathfrak{a} \in R$$
 and $a_1 x_1 + \ldots a_n x_n = 1$

NOTA as we have just seen this already implies, that the a_i generate \mathfrak{a} . Hence any invertible ideal already is finitely generated!

• Now consider some multiplicatively closed subset $0 \notin U \subseteq R$. Then $F = \text{QUOT } R = \text{QUOT } U^{-1}R$ are canonically isomorphic, by (2.111.(iii)). If now \mathfrak{f} and $\mathfrak{g} \leq_{\mathfrak{f}} R$ are any two fraction ideals of R then it is easy to see that $U^{-1}\mathfrak{f} := \{a/ub \mid a/b \in \mathfrak{f}, u \in U\} \leq_{\mathfrak{f}} U^{-1}R$ is a fraction ideal of $U^{-1}R$ and a straightforward computation shows

$$\left(U^{-1}\mathbf{f}\right)\left(U^{-1}\mathbf{g}\right) = U^{-1}(\mathbf{f}\mathbf{g})$$

In particular if $\mathfrak{f} \leq_{\mathfrak{f}} R$ is invertible (over R) then $U^{-1}\mathfrak{f}$ is invertible (over $U^{-1}R$) and vice versa. Formally that is the equivalence

$$\oint \trianglelefteq_{\mathbf{f}} R$$
 invertible $\iff U^{-1} \oint \trianglelefteq_{\mathbf{f}} U^{-1} R$ invertible

PROB $(U^{-1}\mathfrak{f})(U^{-1}\mathfrak{g})$ is generated by elements of the form (a/ub)(c/vd)where $a/b \in \mathfrak{f}$, $c/d \in \mathfrak{g}$ and $u, v \in U$. Now $uv \in U$ and (a/ub)(c/vd) = (ac)/(uvbd) such that this is contained in $U^{-1}(\mathfrak{f}\mathfrak{g})$ again. This proves " \subseteq " conversely let $a/b \in \mathfrak{f}$, $c/d \in \mathfrak{g}$ and $u \in U$. Then $U^{-1}(\mathfrak{f}\mathfrak{g})$ is generated by elements of the form (ac)/(ubd). And as (ac)/(ubd) = (a/ub)(c/d) this is also contained in $(U^{-1}\mathfrak{f})(U^{-1}\mathfrak{g})$. This proves the converse inclusion " \supseteq " and hence the equality. And from this equality it is clear that $(U^{-1}\mathfrak{f})^{-1} = U^{-1}(\mathfrak{f}^{-1})$ for invertible fraction ideals (and hence the equivalence).

(2.134) Definition: (viz. 373)

Let $(R, +, \cdot)$ be an integral domain and let us denote its quotient field by F := QUOT R. Then R is said to be a **Dedekind domain** (shortly DKD) iff it satisfies one of the following equivalent statements

- (a) every non-zero fraction ideal $0 \neq \mathfrak{f} \leq_{\mathfrak{f}} R$ is invertible (i.e. there is some fraction ideal $\mathfrak{g} \leq_{\mathfrak{f}} R$ such that $\mathfrak{f}\mathfrak{g} = R$).
- (b) every non-zero (integral) ideal $0 \neq \mathfrak{a} \leq_{i} R$ is invertible, (i.e. there is some fraction ideal $\mathfrak{g} \leq_{f} R$ such that $\mathfrak{ag} = R$).
- (c) every ideal $\mathfrak{a} \leq_{i} R$ with $\mathfrak{a} \notin \{0, R\}$ allows a decomposition into finitely many prime ideals, i.e. $\exists \mathfrak{p}_{1}, \ldots, \mathfrak{p}_{n} \in \operatorname{spec} R$ such that $\mathfrak{a} = \mathfrak{p}_{1} \ldots \mathfrak{p}_{n}$.
- (d) R is a notherian, normal ring in which every non-zero prime ideal already is maximal, that is spec $R = \operatorname{smax} R \cup \{0\}$.
- (e) R is noetherian and for any non-zero prime ideal $0 \neq \mathfrak{p} \in \operatorname{spec} R$ the localisation $R_{\mathfrak{p}}$ is a discrete valuation ring (i.e. a local PID).

(2.135) Example:

In particular any PID $(R, +, \cdot)$ is a Dedekind domain - it is noetherian, as any ideal even has only one generator, it is normal (as it is an UFD by the fundamental theorem of arithmetic) and non-zero prime ideals are maximal (which can be seen using generators of the ideals).

(2.136) Theorem: (viz. 380)

Let $(R, +, \cdot)$ be a Dedekind domain and $0 \neq \mathfrak{a} \leq_i R$ be a non-zero ideal of R. Then R already satisfies an extensive list of further properties, namely

(i) Any ideal $0 \neq \mathfrak{a} \leq_{i} R$ admits a decomposition into finitely many (up to permutations) uniquely determined prime ideals, formally

 $\exists ! \mathfrak{p}_1, \dots, \mathfrak{p}_n \in \operatorname{spec} R \setminus \{ 0 \}$ such that $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n$

- (ii) For any ideal $0 \neq \mathfrak{a} \leq_i R$ the quotient ring R/\mathfrak{a} is a principal ring (i.e. a ring in which any ideal is generated by a single element).
- (iii) Any ideal of R can be generated by two elements already, we even get:

$$\forall 0 \neq a \in \mathfrak{a} \ \exists b \in \mathfrak{a}$$
 such that $\mathfrak{a} = aR + bR$

- (iv) If R also is semilocal (i.e. R only has finitely many maximal ideals) then R already is a PID (i.e. every ideal is a principal ideal).
- (v) If $\mathfrak{m} \leq_{\mathbf{i}} R$ is a maximal ideal of R and $1 \leq k \in \mathbb{N}$ then we obtain the following isomorphy of rings (where as usual $R_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}R$ and $\mathfrak{m}^{k}R_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}\mathfrak{m}^{k} \leq_{\mathbf{i}} R_{\mathfrak{m}}$ denote the localisation of R resp. \mathfrak{m}^{k})

$${}^{R}/\mathfrak{m}^{k} \cong_{\mathrm{r}} {}^{R}\mathfrak{m}/\mathfrak{m}^{k}R_{\mathfrak{m}} : a + \mathfrak{m}^{k} \mapsto \frac{a}{1} + \mathfrak{m}^{k}R_{\mathfrak{m}}$$

(2.137) Definition: (viz. 378)

Let $(R, +, \cdot)$ be a Dedekind domain, $\mathfrak{m} \in \operatorname{smax} R$ be a maximal ideal and $0 \neq \mathfrak{a} \leq_{\mathrm{i}} R$ be a non-zero ideal of R. Then we define the **valuation** $\nu_{\mathfrak{m}}$ induced by \mathfrak{m} on the set of ideals of R, by

$$\nu_{\mathfrak{m}} : \operatorname{ideal} R \to \mathbb{N}$$

: $\mathfrak{a} \mapsto \max\{k \in \mathbb{N} \mid \mathfrak{a} \subseteq \mathfrak{m}^k\}$
: $0 \mapsto 0$

And for any $a \in R$ we denote $\nu_{\mathfrak{m}}(a) := \nu_{\mathfrak{m}}(aR) \in \mathbb{N}$. Let now $\mathfrak{a}, \mathfrak{b} \leq_{\mathrm{i}} R$ be arbitrary ideals of R. The we say that \mathfrak{b} divides \mathfrak{a} , written as $\mathfrak{b} \mid \mathfrak{a}$, iff it satisfies one of the following equivalent properties:

$$\begin{array}{cccc} \mathfrak{b} & | & \mathfrak{a} & :\Longleftrightarrow & \exists \mathfrak{c} \leq_{\mathrm{i}} R : \mathfrak{a} = \mathfrak{b} \mathfrak{c} \\ & \Leftrightarrow & \mathfrak{a} \subseteq \mathfrak{b} \\ & \Leftrightarrow & \forall \mathfrak{m} \in \operatorname{smax} R : \nu_{\mathfrak{m}}(\mathfrak{b}) \leq \nu_{\mathfrak{m}}(\mathfrak{a}) \end{array}$$
(2.138) Proposition: (viz. 378)

Let $(R, +, \cdot)$ be a Dedekind domain with quotient field F := QUOT R. And let $\mathfrak{M} \leq_i R$ be any maximal (i.e. non-zero prime) ideal of R. Then we obtain the following statements:

(i) Consider $\mathcal{M} = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\} \subseteq \operatorname{smax} R$ a finite collection of maximal ideals and $k(1), \dots, k(n) \in \mathbb{N}$. Then for any $\mathfrak{m} \in \operatorname{smax} R$ we obtain

$$\nu_{\mathfrak{m}}\left(\mathfrak{m}_{1}^{k(1)}\ldots\mathfrak{m}_{n}^{k(n)}\right) = \begin{cases} k(i) & \text{if } \mathfrak{m} = \mathfrak{m}_{i} \\ 0 & \text{if } \mathfrak{m} \notin \mathcal{M} \end{cases}$$

(ii) Consider any two non-zero ideals $0 \neq \mathfrak{a}, \mathfrak{b} \leq_{i} R$ then the multiplicity function $\nu_{\mathfrak{m}}$ acts additively under multiplication of ideals, that is

$$\nu_{\mathfrak{m}}(\mathfrak{a}\mathfrak{b}) = \nu_{\mathfrak{m}}(\mathfrak{a}) + \nu_{\mathfrak{m}}(\mathfrak{b})$$

(iii) Let $0 \neq \mathfrak{a}, \mathfrak{b} \leq_{i} R$ be any two non-zero ideals of R and decompose $\mathfrak{a} = \mathfrak{m}_{1}^{k(1)} \dots \mathfrak{m}_{n}^{k(n)}$ and $\mathfrak{b} = \mathfrak{m}_{1}^{l(1)} \dots \mathfrak{m}_{n}^{l(n)}$ with pairwise distinct maximal ideals $\mathfrak{m}_{i} \in \operatorname{smax} R$ and $k(i), l(i) \in \mathbb{N}$ (note that this can always be established, as k(i) = 0 and l(i) = 0 is allowed). Then we get

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{m}_1^{m(1)} \dots \mathfrak{m}_n^{m(n)} \text{ where } m(i) := \min\{k(i), l(i)\}$$

(iv) Consider any non-zero ideal $0 \neq \mathfrak{a} \leq_i R$, as before we decompose \mathfrak{a} into $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ (with pairwise distinct $\mathfrak{m}_i \in \operatorname{smax} R$ and $1 \operatorname{leqk}(i) \in \mathbb{N}$). Then we obtain *chinese remainder theorem*:

$$R_{\mathfrak{a}} \cong_{\mathrm{r}} \bigoplus_{i=1}^{n} R_{\mathfrak{m}_{i}^{k(i)}} : b + \mathfrak{a} \mapsto \left(b + \mathfrak{m}_{i}^{k(i)}\right)$$

(v) Let $\mathfrak{a} \leq_{i} R$ be any ideal in R, then there is some ideal $\mathfrak{b} \leq_{i} R$ such that $\mathfrak{a} + \mathfrak{b} = R$ are coprime and $\mathfrak{a}\mathfrak{b}$ is principal (i.e. $\exists a \in R : \mathfrak{a}\mathfrak{b} = aR$).

Chapter 3

Modules

3.1 Defining Modules

(3.1) Definition:

Let $(R, +, \cdot)$ be a ring, then the triple $(M, +, \diamond)$ is said to be an *R*-module, iff $M \neq \emptyset$ is a non-empty set and + resp. \diamond are binary operations of the form $+: M \times M \to M: (x, y) \mapsto x + y$ and $\diamond: R \times M \to M: (a, x) \mapsto a \diamond x = ax$ that satisfy the following properties

(G) (M, +) is a commutative group, that is the addition is *associative* and *commutative*, admits a neutral element (called *zero-element*, denoted by 0) and every element of M has an additive inverse. Formally

$$\begin{array}{rcl} \forall x,y,z\in M & : & x+(y+z) = & (x+y)+z \\ & \forall x,y\in M & : & x+y = & y+x \\ \exists \, 0\in M\,\forall x\in M & : & x+0 = & x \\ \forall x\in M\,\exists \overline{x}\in M & : & x+\overline{x} = & 0 \end{array}$$

(M) The addition + and scalar multiplication \diamond on M satisfy the following compatibility conditions regarding the operations of R

 $\begin{array}{rcl} \forall \, a \in R \, \forall \, x, y \in M & : & a \diamond (x+y) \, = \, (a \diamond x) + (a \diamond y) \\ \forall \, a, b \in R \, \forall \, x \in M & : & (a+b) \diamond x \, = \, (a \diamond x) + (b \diamond x) \\ \forall \, a, b \in R \, \forall \, x \in M & : & (a \cdot b) \diamond x \, = \, a \diamond (b \diamond x) \\ & \forall \, x \in M & : & 1 \diamond x \, = \, x \end{array}$

(3.2) Remark:

• The notations in the definition above deserve some special attention. First note that - as always with binary operations - we wrote x + y instead of +(x, y). Likewise $a \diamond x$ instead of $\diamond(a, x)$ and of course a + b instead of +(a, b), $a \cdot b$ instead of $\cdot(a, b)$ (as we already did with rings).

- Recall that for a ring $(R, +, \cdot)$ the operation + has been called *addition* and \cdot has been called *multiplication* of R. In analogy, if $(M, +, \diamond)$ is an R-module, then + is said to be the *addition* of M and \diamond is called the *scalar multiplication* of M.
- Next note that we have used two different binary operations +, namely +: $R \times R \to R$ of $(R, +, \cdot)$ and +: $M \times M \to M$ of $(M, +, \diamond)$. At first it may be misleading to denote two different functions by the same symbol, but you will soon become used to it and appreciate the simplicity of this notation. It will not lead to ambiguities, as the neighbouring elements (a and b for a + b, resp. x and y for x + y) determine which of the two functions is to be applied. As an excercise it might be useful to rewrite the defining properties (M) using $+_R$ for + in R and $+_M$ for + in M. As an example let us reformulate the first two properties in this way

$$\forall a \in R \ \forall x, y \in M \quad a \diamond (x +_M y) = (a \diamond x) +_M (a \diamond y)$$

$$\forall a, b \in R \ \forall x \in M \quad (a +_B b) \diamond x = (a \diamond x) +_M (b \diamond x)$$

• Note that the properties (G) of R-modules truly express that (M, +) is a commutative group. In particular we employ the usual notational conventions for groups. E.g. we may omit the bracketing in sums due to the associativity of the addition + of M

$$x + y + z := (x + y) + z$$

 $\sum_{i=1}^{n} x_i := ((x_1 + x_2) + \dots) + x_r$

And as always the *neutral element* $0 \in M$ is uniquely determined again (if 0 and 0' are neutral elements, then 0' = 0 + 0' = 0' + 0 = 0). Likewise given $x \in M$ there is a uniquely determined $\overline{x} \in M$ such that $x + \overline{x} = 0$ and this is said to be the *negative* element of x, denoted by $-x := \overline{x}$ (if p and q are negative elements of x then p = p + 0 =p + (x + q) = q + (x + p) = q + 0 = q).

• Let $(R, +, \cdot)$ be any ring (with unit element 1) and M be an R-module, then we wish to note some immediate consequences of the axioms above. Let $x \in M$ and recall that -x denotes the negative of x, then

$$\begin{array}{rcl} 0\diamond x & = & 0 \\ (-1)\diamond x & = & -x \end{array}$$

PROB as 0 = 0 + 0 in R we get $0 \diamond x = (0 + 0) \diamond x = (0 \diamond x) + (0 \diamond x)$ from (M). And subtracting $0 \diamond x$ once from this equality we find $0 = 0 \diamond x$. This may now be used to see $0 = 0 \diamond x = (1 + (-1)) \diamond x = (1 \diamond x) + ((-1) \diamond x)$. Subtracting $x = 1 \diamond x$ we find $-x = (-1) \diamond x$.

- We have already simplified the notations for modules rigorously. However it is still useful to introduce some further conventions. Recall that for rings $(R, +, \cdot)$ we wrote ab instead of $a \cdot b$. And we wrote a - b instead of a + (-b) and ab + c instead of $(a \cdot b) + c$. The same is true for the addition in the module M: we will write x - y instead of x + (-y). Likewise we write ax instead of $a \diamond x$ and declare that the scalar multiplication \diamond is of higher priority that the addition +. That is we write ax + y instead of $(a \diamond x) + y$. Note that it is unambiguously to write abx instead of $(a \cdot b) \diamond x = a \diamond (b \diamond x)$, as this equality has been one of the axioms for *R*-modules. Thus we may also omit the brackets in mixed terms with multiplication and scalar multiplication.
- In contrast to rings (where we faithfully wrote $(R, +, \cdot)$ on every first occurance of the ring) we will omit the operatins + and \diamond when referring to the *R*-module $(M, +, \diamond)$. That is we will say: let *M* be an *R*-module and think of $(M, +, \diamond)$ instead.
- What we defined here is also called a left *R*-module, this is to say that in the scalar multiplication ◇: *R* × *M* → *M* the ring *R* acts from the left. One might be tempted to regard right *R*-modules as well, i.e. structures (*M*, +, △) in which the ring *R* acts from the right △: *M* × *R* → *M*: (*x*, *a*) ↦ *x* △ *a* that satisfy the analogous properites (*x* + *y*) △ *a* = (*x* △ *a*) + (*y* △ *a*), *x* △ (*a* + *b*) = (*x* △ *a*) + (*x* △ *b*), *x* △ (*a* · *b*) = (*x* △ *a*) △ *b* and *x* △ 1 = *x*. However this would only yield an entirely analogous theory: Recall the construction of the *opposite* ring (*R*, +, ·)^{op} in section 1.3. If (*M*, +, ◇) is a (left) *R*-module, then we obtain a right *R*^{op}-module (*M*, +, ◇)^{op} by taking *M* as a set and + as an addition again, but using a scalar multiplication that reverses the order of elements. That is we obtain a right *R*^{op}-module by

$$(M, +, \diamond)^{\operatorname{op}} := (M, +, \bigtriangleup) \quad \text{where} \quad x \bigtriangleup a := a \diamond x$$

• The theory of R-modules is particularly simple in the case that R is a field. As this case historically has been studied first there is some special nomenclature: suppose that V is an F-module, where $(F, +, \cdot)$ is a field. Then we will use the following notions

set theory	linear algebra
$(F, +, \cdot)$	base field
$(V, +, \diamond)$	vector space
elements of ${\cal F}$	scalars
elements of ${\cal V}$	vectors

(3.3) Example:

• Consider any commutative group (G, +), then G becomes a Z-module under the following scalar multiplication $\diamond : \mathbb{Z} \times G \to G$

$$k \diamond x := \begin{cases} \sum_{i=1}^{k} x & \text{for } k > 0 \\ 0 & \text{for } k = 0 \\ \sum_{i=1}^{-k} (-x) & \text{for } k < 0 \end{cases}$$

• Let $(R, +, \cdot)$ be any ring and $\mathfrak{a} \leq_{\mathrm{m}} R$ be a left-ideal of R (note that in particular $\mathfrak{a} = R$ is allowed). Then \mathfrak{a} is an R module under the operations inherited from R, that is

$$\begin{array}{rcl} + \ : \ \mathfrak{a} \times \mathfrak{a} \to \mathfrak{a} & : & (x,y) \mapsto x+y \\ \diamond \ : \ R \times \mathfrak{a} \to \mathfrak{a} & : & (a,x) \mapsto ax \end{array}$$

That is: although we started with quite a lot of axioms for R-modules, examples are abundant - the theory of modules encompasses the theory of rings! And the proofs are full of examples how module theory can be put to good use in ring theory (e.g. the lemma of Nakayama).

• Consider any (i.e. not necessarily commutative) ring $(S, +, \cdot)$ and suppose $R \leq_{\mathbf{r}} S$ is a subring of S. If now M is an S-module, then M becomes an R-module under the operations inherited from S

$$\begin{array}{rrrr} + & : & M \times M \to M & : & (x,y) \mapsto x+y \\ \diamond & : & R \times M \to M & : & (a,x) \mapsto ax \end{array}$$

• Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be any two (not necessarily commutative) rings and consider a ring-homomorphism $\varphi : R \to S$. If now M is an S-module, then M also becomes an R-module under the operations

$$\begin{array}{rcl} + & : & M \times M \to M & : & (x,y) \mapsto x+y \\ \diamond & : & R \times M \to M & : & (a,x) \mapsto \varphi(a)x \end{array}$$

• Consider an arbitrary (i.e. not necessarily commutative) ring $(R, +, \cdot)$. If now $1 \leq n \in \mathbb{N}$ then \mathbb{R}^n becomes a well defined \mathbb{R} -module under the pointwise operations $+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ and $\diamond : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n) a \diamond (x_1, \dots, x_n) := (a \cdot x_1, \dots, a \cdot x_n)$$

Note that the operations + and \cdot on the right hand side are those of the ring R, whereas the operations + and \diamond are thereby defined on the module R^n . Further note that in the case n = 1 we get $R^n = R$ and the addition + on R^1 by definition coincides with the addition + on R. This is the precisely reason why we did not need to distinguish between $+_R$ and $+_M$ - in case of doubt it doesn't matter.

(3.4) Definition:

Let $(R, +, \cdot)$ be a ring, then the quadrupel $(A, +, \cdot, \diamond)$ is said to be an *R*-semi-algebra, iff $A \neq \emptyset$ is a non-empty set and $+, \cdot$ resp. \diamond are binary opertations of the form $+: A \times A \to A, \cdot : A \times A \to A$ and $\diamond : R \times A \to A$ that satisfy the following properties

(R) (A, +, ·) is a semi-ring, that is the addition + is associative and commutative, admits a neutral element (called zero-element, denoted by 0), every element of A has an additive inverse, the multiplication · is associative and satisfies the distributivity laws. Formally

$$\begin{array}{rcl} \forall f,g,h\in A & : & f+(g+h) = (f+g)+h \\ & \forall f,g\in A & : & f+g = g+f \\ \exists 0\in A \,\forall f\in A & : & f+0 = f \\ \forall f\in A \,\exists \overline{f}\in A & : & f+\overline{f} = 0 \\ & \forall f,g,h\in A & : & f\cdot(g\cdot h) = (f\cdot g)\cdot h \\ & \forall f,g,h\in A & : & f\cdot(g+h) = (f\cdot g)+(f\cdot h) \\ & \forall f,g,h\in A & : & (f+g)\cdot h = (f\cdot h)+(g\cdot h) \end{array}$$

(M) $(A, +, \diamond)$ is an *R*-module, that is the *addition* + and *scalar multiplication* \diamond of *A* satisfy the following compatibility conditions

$$\begin{array}{rcl} \forall \, a \in R \; \forall \, f, g \in A & : & a \diamond (f+g) \, = \, (a \diamond f) + (a \diamond g) \\ \forall \, a, b \in R \; \forall \, f \in A & : & (a+b) \diamond f \, = \, (a \diamond f) + (b \diamond f) \\ \forall \, a, b \in R \; \forall \, f \in A & : & (a \cdot b) \diamond f \, = \, a \diamond (b \diamond f) \\ & \forall \, f \in A \quad : & 1 \diamond f \, = \, f \end{array}$$

(A) The multiplication \cdot and scalar multiplication \diamond of A are compatible in the following sense (note that this is some kind of associativity)

$$\forall a \in R \ \forall f, g \in A : (a \diamond f) \cdot g = a \diamond (f \cdot g) = f \cdot (a \diamond g)$$

If now $(A, +, \cdot, \diamond)$ is an *R*-algebra, then we transfer most of the notions of ring theory to the case of algebras, by referring to the semi-ring $(A, +, \cdot)$. To be precise introduce the following notions

$(A, +, \cdot, \diamond)$ is called		$(A, +, \cdot)$ is
R-algebra	$:\iff$	ring
commutative	$:\iff$	commutative
integral	$:\iff$	integral domain
division	$:\iff$	skew-field
noetherian	$:\iff$	commutative, noetherian ring
artinian	$:\iff$	commutarive, artinian ring
local	$:\iff$	commutative, local ring
semi-local	$: \iff$	commutative, semi-local ring

(3.5) Remark:

- By definition any *R*-semi-algebra (A, +, ·, ◊) has a (uniquely determined) neutral element of addition, denoted by 0 (that is f + 0 = f for any f ∈ A). To be an *R*-algebra by definition means that the multiplication also admits a neutral element. That is there is some 1 ∈ A such that for any f ∈ A we get f · 1 = f = 1 · f. And due to the associativity of · this unit element 1 is uniquely determined again.
- If (A, +, ·, ◇) is an R-algebra, then by definition (A, +, ·) is a semi-ring and (A, +, ◇) is an R-module. In particular A inherits all the properties of these objects and we also pick up all notational conventions introduced for these objects. That is we write 0 for the zero-element and 1 for the unit element (supposed A is an R-algebra). Likewise we write -f for the additive inverse of f (that is f + (-f) = 0 and f⁻¹ for the multiplicative inverse of f (that is f · f⁻¹ = 1 = f⁻¹ · f), supposed such an element exists. In case you are not familiar with these conventions we recommend having a look at section 1.2.
- If A is a commutative R-semialgebra, then condition (A) boils down to $(a \diamond f) \cdot g = a \diamond (f \cdot g)$ for any $a \in R$ and $f, g \in A$. Because if this property is satisfied then we already get $(a \diamond f) \cdot g = f \cdot (a \diamond g)$ from the commutativity $f \cdot (a \diamond g) = (a \diamond g) \cdot f = a \diamond (g \cdot f) = a \diamond (f \cdot g) = (a \diamond f) \cdot g$.
- If A is an R-algebra, i.e. an R-semialgebra containing a unit element 1, then due to property (A) the scalar multiplication \diamond can be expressed in terms of the ordinary multiplication of A with elements of the form $a \diamond 1$. To be precise, let $a \in R$ and $f \in A$, then we clearly obtain

$$(a \diamond 1) \cdot f = a \diamond f$$

- Note that property (A) in the definition of *R*-semi-algebras enables us to not only omit the multiplicative symbol

 and scalar multiplication
 but also the bracketing. Whenever we have a term of the form *afg* then we may use either bracketing (*af*)*g* = *a*(*fg*) due to (A).
- (\diamondsuit) Let $(R, +, \cdot)$ be a commutative ring and A be an R-semi-algebra, then we can embed A into an R-algebra A' canonically: as a set we take $A' := R \times A$ and define the following operations on A'

$$\begin{array}{rcl} (a,f) + (b,g) &:= & (a+b,f+g) \\ (a,f) \cdot (b,g) &:= & (ab,fg+ag+bf) \\ & a \diamond (b,g) &:= & (ab,af) \end{array}$$

Then $(A', +, \cdot, \diamond)$ truly becomes an *R*-algebra (the verification of this is left to the interested reader) with zero element (0, 0) and unit element (1, 0). And of course we get a canonical embedding (i.e. an injective homomorphism of *R*-algebras), by virtue of

$$A \hookrightarrow A' : f \mapsto (0, f)$$

(3.6) Example:

Let (R, +, ·) be a commutative ring then, R becomes an R-module (even an R-algebra) canonically under its addition + as an addition of vectors and its multiplication · as both, its multiplication and scalar-multiplication. I.e. if we let A := R, then R becomes an R-algebra (A, +, ·, ◊), under the operations

$$\begin{array}{rrrr} + \ : \ A \times A \to A & : & (f,g) \mapsto f+g \\ & \cdot \ : \ A \times A \to A & : & (f,g) \mapsto fg \\ & \diamond \ : \ R \times A \to A & : & (a,f) \mapsto af \end{array}$$

In the following - whenever we say that we regard some ring $(R, +, \cdot)$ as an *R*-module - we will refer to this construction. And in this case any subset $\mathfrak{a} \subseteq R$ is an ideal of *R* if and only if it is an *R*-submodule of *R* (where *R* is regarded as an *R*-module, as we just did)

 $\mathfrak{a} \leq_{\mathrm{i}} R \iff \mathfrak{a} \leq_{\mathrm{m}} R$

• Let $(A, +, \cdot)$ be a commutative ring again and $I \neq \emptyset$ be any non-empty set, then we take $A := \mathcal{F}(I, R)$ to be the set of functions from I to R. Note that this includes the case $A = R^n$ by taking $I := 1 \dots n$. Then A becomes an R-algebra $(A, +, \cdot, \diamond)$, under the pointwise operations

$$\begin{array}{rcl} + & : & A \times A \to A & : & (f,g) \mapsto (i \mapsto f(i) + g(i)) \\ & \cdot & : & A \times A \to A & : & (f,g) \mapsto (i \mapsto f(i) \cdot g(i)) \\ & \diamond & : & R \times A \to A & : & (a,f) \mapsto (i \mapsto af(i)) \end{array}$$

• Likewise let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_{\mathrm{i}} R$ be an ideal of R. Then we may consider the quotient ring $A := R/\mathfrak{a}$ as an R-algebra $(A, +, \cdot, \diamond)$, under the following operations

$$\begin{array}{rcl} + & : & A \times A \to A & : & (b + \mathfrak{a}, c + \mathfrak{a}) \mapsto (b + c) + \mathfrak{a} \\ & \cdot & : & A \times A \to A & : & (b + \mathfrak{a}, c + \mathfrak{a}) \mapsto (bc) + \mathfrak{a} \\ & \diamond & : & R \times A \to A & : & (a, b + \mathfrak{a}) \mapsto (ab) + \mathfrak{a} \end{array}$$

• This is a special case of the following general concept: consider any two commutative rings $(R, +, \cdot)$ and $(S, +, \cdot)$ and regard an arbitrary ring-homomorphism $\varphi : R \to S$. Then S can be considered to be an R-algebra under its own addition + and its own multiplication \cdot as multiplication and scalar multiplication with the imported elements $\varphi(a)$. That is A := S becomes an R-algebra under the operations

$$\begin{array}{rrrr} + \ : \ A \times A \to A & : & (f,g) \mapsto f+g \\ & \cdot \ : \ A \times A \to A & : & (f,g) \mapsto fg \\ & \diamond \ : \ R \times A \to A & : & (a,f) \mapsto \varphi(a)f \end{array}$$

• The most general case of the above is the following: let $(R, +, \cdot)$ be any (that is non-commutative) ring. Then R still is an R-module under the above operations. But R no longer is an R-algebra. Likewise consider a second ring $(S, +, \cdot)$ and a ring-homomorphism $\varphi : R \to S$. Then S is an R-module under the above operations.

$$\begin{array}{rcl} + & : & S \times S \to S & : & (x,y) \mapsto x+y \\ \diamond & : & R \times S \to S & : & (a,x) \mapsto \varphi(a)y \end{array}$$

Again S, need not be an R-algebra, in general. However S becomes an R-algebra (under its own multiplication), if the image of R under φ is contained in the center of S, that is if

$$\varphi(R) \subseteq \operatorname{cen}(S) := \{ x \in S \mid \forall y \in S : xy = yx \}$$

• An example of the above situation will be the ring of $n \times n$ matrices over a commutative ring $(R, +, \cdot)$. Recall the construction of matrices given in section 1.3 (for more details confer to section 4.1) and let $S := \operatorname{mat}_n R$. Then we obtain a homomorphism of rings by letting

$$\varphi \ : \ R \to S \ : \ a \mapsto \left(\begin{array}{cc} a & & 0 \\ & \ddots & \\ 0 & & a \end{array} \right)$$

And as R is commutative it is clear, that $\varphi(R) \subseteq \operatorname{cen}(S)$ (in fact it even is true that $\varphi(R) = \operatorname{cen}(S)$) and hence S becomes a well-defined R-algebra (under the usual multiplication and addition of matrices).

(3.7) Definition:

Let $(R, +, \cdot)$ be a ring and M be an R-module, then a subset $P \subseteq M$ is said to be an R-submodule of M, iff it satisfies the following properties

- (1) $0 \in P$
- (2) $x, y \in P \implies x + y \in P$
- (3) $a \in R, x \in P \implies ax \in P$

And in this case we will write $P \leq_{\mathrm{m}} M$. Likewise if A is a R-semi-algebra and $P \subseteq A$ is a subset, then P is said to be an R-sub-semi-algebra, iff it is both, a submodule and sub-semi-ring of A, formally iff it satisfies

- (M) $P \leq_{\mathrm{m}} A$
- $(4) \ f, g \in P \implies fg \in P$

And in this case we will write $P \leq_b A$. If A even is an R-algebra (with unit element 1), then a subset $P \subseteq A$ is said to be an *R***-subalgebra**, iff it is both, a submodule and subring of A, formally iff it satisfies

- (B) $P \leq_{\mathrm{b}} A$
- (5) $1 \in P$

And in this case we will write $P \leq_a A$. Let now A be an R-semi-algebra again. Then a subset $\mathfrak{a} \subseteq A$ is said to be an R-algebra-ideal of A. iff it is both, an ideal and a submodule of A, formally iff it satisfies

- (M) $\mathfrak{a} \leq_{\mathrm{m}} A$
 - (I) $f \in \mathfrak{a}, g \in A \implies fg \in \mathfrak{a}$ and $gf \in \mathfrak{a}$

And in this case we write $\mathfrak{a} \leq_{a} A$. Having defined all these notions the set of all submodules of an *R*-module *M* is denoted by subm *M*. Likewise subb *A* denotes the set of all *R*-sub-semialgebras, aideal *A* denotes the set of all algebra-ideals of a semi-algebra *A*. And finally the set of all *R*-subalgebras of an *R*-algebra *A* id denoted by suba *A*. Formally we define

 $\begin{aligned} \operatorname{subm} M &:= \{ P \subseteq M \mid P \leq_{\mathrm{m}} M \} \\ \operatorname{subb} A &:= \{ P \subseteq A \mid P \leq_{\mathrm{b}} A \} \\ \operatorname{suba} A &:= \{ P \subseteq A \mid P \leq_{\mathrm{a}} A \} \\ \operatorname{aideal} A &:= \{ \mathfrak{q} \subseteq A \mid P \leq_{\mathrm{b}} A \} \end{aligned}$

(3.8) Remark:

- If $P \leq_{\mathrm{m}} M$ is a submodule (of the *R*-module *M*, where $(R, +, \cdot)$ is an arbitrary ring), then $P \leq_{\mathrm{g}} M$ already is a *subgroup* of (M, +), too. That is $0 \in P$ and for any $x, y \in P$ we get $-x \in P$ and $x + y \in P$. Thereby $-x \in P$ follows from (3) by regarding a := -1, as in this case we get $-x = (-1) \diamond x \in P$.
- Likewise if A is an R-algebra (over an arbitrary ring $(R, +, \cdot)$), then we only need to check properties (1), (2), (4) and (5), as (3) already follows from (4). Given $f \in R$ and $a \in A$ we get $af = (a1_A) \diamond f \in P$.
- Let A be an R-semi-algebra over the ring $(R, +, \cdot)$, then any sub-semialgebra of A already is a sub-semi-ring of A, formally

$$P \leq_{\mathrm{b}} A \implies P \leq_{\mathrm{s}} A$$

PROB properties (1), (2) and (4) of sub-semi-algebras and sub-semirings coincide. It only remains to check property (3) of sub-semi-rings: consider any $f \in P$, then $-f = (-1)f \in P$ by (3) of sub-semi-algebras.

• Let A be an R-semi-algebra over the ring $(R, +, \cdot)$, then \mathfrak{a} is an algebra ideal of A iff it is an ideal and R-sub-semialgebra of A, formally

$$\mathfrak{a} \trianglelefteq_{\mathbf{a}} A \iff \mathfrak{a} \leqq_{\mathbf{b}} A \text{ and } \mathfrak{a} \trianglelefteq_{\mathbf{i}} A$$

PROB the implication \Leftarrow is clear: (M) of algebra-ideals is identical to (M) of sub-semi-algebras and (I) of algebra ideals just combines (4) and (5) of ideals. Concersely we first check property (4) of sub-semialgebras: if $f, g \in \mathfrak{a}$, then in particular $g \in A$ and hence $fg \in \mathfrak{a}$ by (4) of algebra-ideals. Now properties (1) and (2) of ideals are contained in (M) of algebra ideals ((4) and (5) are (I) again). Thus it only remains to check property (3) of ideals. But if $f \in \mathfrak{a}$ then, as before $-f = (-1)f \in \mathfrak{a}$ by property (3) of algebra-ideals.

• If A even is an R-algebra over the ring $(R, +, \cdot)$, then there is no difference between ideals and algebra-ideals of A, formally

$$\mathfrak{a} \trianglelefteq_{\mathrm{a}} A \iff \mathfrak{a} \trianglelefteq_{\mathrm{i}} A$$

PROB we have already seen $\mathfrak{a} \leq_a A \implies \mathfrak{a} \leq_i A$ above. Further we have already argued that it only remains to check property (3) of algebra-ideals: thus consider any $a \in R$ and $f \in \mathfrak{a}$, then $a1 \in A$ (where $1 \in A$, as A is an R-algebra) and hence $af = (a1)f \in \mathfrak{a}$ by (I).

(3.9) **Proposition:** (viz. 251)

Fix any ring $(R, +, \cdot)$ and for the moment being let \star appreviate any one of the words *R*-module, *R*-semi-algebra, *R*-algebra and let *M* be a \star . Further consider an arbitrary family (where $i \in I \neq \emptyset$) $P_i \subseteq M$ of sub- \star s of *M*. Then the intersection of the P_i is a sub- \star again

$$\bigcap_{i \in I} P_i \subseteq M \text{ is a sub-}\star$$

Likewise let A be an R-semi-algebra and let $\mathfrak{a}_i \leq_{\mathrm{a}} A$ be an arbitrary (that is $i \in I \neq \emptyset$ again) family of R-algebra-ideals of A, then the intersection of the \mathfrak{a}_i is an R-algebra-ideal of A again

$$\bigcap_{i \in I} \mathfrak{a}_i \quad \trianglelefteq_{\mathbf{a}} \quad A \quad \text{is an } R\text{-algebra-ideal}$$

(3.10) Definition:

Fix any ring $(R, +, \cdot)$ again, let \star appreviate any one of the words *R*-module, *R*-semi-algebra, *R*-algebra again and let *M* be a \star . If now $X \subseteq M$ is an arbitrary subset then we define the \star generated by *X* to be the intersection of all sub- \star s containing *X*

NOTA in case there is any doubt concerning the module X is contained in, (e.g. $X \subseteq M \subseteq N$) we emphasise the *R*-module *M* used in this construction by writing $\langle X \subseteq M \rangle_{\rm m}$ or $\langle X \rangle_{\rm m} \leq_{\rm m} M$ or even $M \langle X \rangle_{\rm m}$. Let us finally define the **linear hull** $\ln(X)$ resp. $\ln_R(X)$ of X to be the following subset of *M*. If $X = \emptyset$, then we let $\ln(\emptyset) := \{0\}$ and if $X \neq \emptyset$ then

$$\ln(X) = \left\{ \sum_{i=1}^{n} a_i x_i \mid 1 \le n \in \mathbb{N}, a_i \in R, x_i \in X \right\}$$

(3.11) Proposition: (viz. 253)

Fix any ring $(R, +, \cdot)$ and consider an *R*-module *M* containing the non-empty subset $\emptyset \neq X \subseteq M$. Then the submodule generated by *X* is precisely the linear hull of *X* in *M*, formally

$$\langle X \rangle_{\mathrm{m}} = \left\{ \sum_{i=1}^{n} a_i x_i \mid 1 \le n \in \mathbb{N}, a_i \in R, x_i \in X \right\}$$

And if A is an R-semi-algebra, $\emptyset \neq X \subseteq A$, then we can also describe the R-sub-semi-algebra generated by X explicitly. Namely we get

$$\langle X \rangle_{\mathrm{b}} = \left\{ \sum_{i=1}^{n} a_i \prod_{j=1}^{m} f_{i,j} \mid 1 \le m, n \in \mathbb{N}, a_i \in R, x_{i,j} \in X \right\}$$

Finally if A is an R-algebra, then the sub-algebra generated by X becomes

$$\langle X \rangle_{\mathbf{a}} = \langle X \cup \{1\} \rangle_{\mathbf{b}}$$

(3.12) Remark:

Let $(R, +, \cdot)$ be any ring and M an R-module. Further consider any R-submodules $P_1, \ldots, P_n \leq_m M$ of M, then we define the **sum** of these

$$P_1 + \dots + P_n := \{ x_1 + \dots + x_n \mid x_i \in P_i \}$$

And in the light of the above proposition (3.11) this is just the *R*-submodule of *M* generated by the P_i , i.e. $P_1 + \cdots + P_n = \langle P_1 \cup \cdots \cup P_n \rangle_m \leq_m M$. Thus if we are given an arbitrary collection of *R*-submodules $P_i \leq_m M$, where $i \in I$ is any index set, then we generalize the finite case directly by defining the **sum** of the P_i to be

$$\sum_{i \in I} P_i := \langle \bigcup_{i \in I} P_i \rangle_{\mathrm{m}}$$

Thus by definition the sum is an *R*-submodule of *M* again. And by (3.11) it consists of *finite* sums of elements $x_1 + \cdots + x_n$ where $x_k \in P_{i(k)}$ for some $i(k) \in I$. Thus if we denote the collection of finite subsets of *I* by $\mathcal{I} := \{ \Omega \subseteq I \mid \#\Omega < \infty \}$ then we obtain the explicit description

$$\sum_{i \in I} P_i = \left\{ \sum_{i \in \Omega} x_i \mid \Omega \in \mathcal{I}, \ x_i \in P_i \right\}$$

3.2 First Concepts

In this section we will introduce three seperate concepts, that are all of fundamental importance. First we will introduce quotient modules - we has already studied quotient rings in (1.40), now we will generalize this concept to modules. Secondly we will turn our attention to torsion and annihilation. This is an important concept when it comes to analyzing the structure of a module, but will not occur in linear algebra. And thirdly we will introduce direct sums and products - the major tool for composing and decomposing modules over a common base ring.

(3.13) Definition: (viz. 258)

Let $(R, +, \cdot)$ be an arbitrary ring, consider an *R*-module *M* an *R*-submodule $P \leq_{\mathrm{m}} M$ of *M*, then *P* induces an equivalence relation on *M*, by

$$x \sim y \quad :\iff \quad y - x \in P$$

where $x, y \in M$. The equivalency classes under this relation are called **cosets** of P and for any $x \in M$ this is given to be

$$x + P := [x] = \{x + p \mid p \in P\}$$

Finally we denote the quotient set of M modulo P (meaning the relation \sim)

$$M/P := M/\sim = \{x + P \mid x \in M\}$$

And thereby M/P can be turned into an R-module $(M/P, +, \diamond)$ again under

$$(x+P) + (y+P) := (x+y) + P$$

 $a \diamond (x+P) := (ax) + P$

Thereby $(M/P, +, \diamond)$ is also called the **quotient module** or **residue mod**ule of M modulo P. Now consider an R-semi-algebra A and an R-algebraideal $\mathfrak{a} \leq_{\mathfrak{a}} A$. Then A/\mathfrak{a} (in the sense above) not only is an R-module, but even becomes an R-semi-algebra $(A/\mathfrak{a}, +, \cdot, \diamond)$, under the multiplication

$$(f + \mathfrak{a})(g + \mathfrak{a}) := (fg) + \mathfrak{a}$$

Thereby $(A/\mathfrak{a}, +, \cdot, \diamond)$ is also called the **quotient algebra** or **residue algebra** of A modulo \mathfrak{a} . And if A even is an R-algebra, then $(A/\mathfrak{a}, +, \cdot, \diamond)$ is an R-algebra again, its unit element being given to be $1 + \mathfrak{a}$.

(3.14) Proposition: (viz. 261) Correspondence Theorem

Let $(R, +, \cdot)$ be an arbitrary ring, M be an R-module and $L \leq_{\mathrm{m}} M$ be any R-submodule of M. Then we obtain the following correspondence

(i) Consider some R-submodule $P \leq_{\mathrm{m}} M$ such that $L \subseteq P$, then we obtain an R-submodule P/L of the quotient module M/L by virtue of

$$P/_L := \{ p+L \mid p \in P \} \leq_{\mathrm{m}} M/_L$$

and thereby for any element $x \in M$ we obtain the following equivalency

$$x + L \in P/L \iff x \in P$$

(ii) Now the *R*-submodules of M/L correspond to the *R*-submodules of M containing L and this correspondence can be explicitly given to be

$$\begin{array}{rcl} \operatorname{subm} M/_L & \longleftrightarrow & \{ P \in \operatorname{subm} M \mid L \subseteq P \} \\ U & \mapsto & \{ x \in M \mid x + L \in U \} \\ P/_L & \longleftrightarrow & P \end{array}$$

(iii) Consider an arbitrary family $P_i \leq_{\mathrm{m}} M$ (where $i \in I$) of *R*-submodules of *M* such that for any $i \in I$ we get $L \subseteq P_i$. Then the intersection commutes with taking to quotients, that is we obtain

$$\bigcap_{i \in I} \left(\frac{P_i}{L} \right) = \left(\bigcap_{i \in I} \frac{P_i}{L} \right) / L$$

(iv) As in (iii) consider any $P_i \leq_{\mathrm{m}} M$ where $i \in I$ and $L \subseteq P_i$, then the summation also commutes with taking to quotients, that is

$$\sum_{i \in I} \left(\frac{P_i}{L} \right) = \left(\sum_{i \in I} \frac{P_i}{L} \right) / L$$

(v) More generally consider any family of sumbodules $P_i \leq_{\mathrm{m}} M$ (where $i \in I$) such that $L \subseteq \sum_i P_i$, then we obtain the following identity

$$\sum_{i \in I} \left(\frac{P_i + L}{L} \right) = \left(\sum_{i \in I} \frac{P_i}{L} \right) / L$$

(vi) Finally for any subset $X \subseteq M$ let us denote $X/L := \{x + L \mid x \in X\}$ that is $X/L \subseteq M/L$, then we obtain the following identity

$$\langle X/L \rangle_{\rm m} = \langle X \rangle_{\rm m} + L/L$$

(3.15) Definition:

Let $(R, +, \cdot)$ be any ring and M be an R-module. Further consider an element $x \in M$ and an arbitrary subset $X \subseteq M$, then we introduce

(i) We define the **annihilator** of x resp. of X to be the following subsets

$$ANN_R(x) := \{ a \in R \mid ax = 0 \}$$

$$ANN_R(X) := \{ a \in R \mid \forall x \in X : ax = 0 \}$$

$$= \bigcap_{x \in X} ANN_R(x)$$

It is easy to see that any annihilator $ANN_R(x)$ is a left-ideal in R, thus we denote the set of all left-ideals of R occuring as annihilators by

annihil
$$M := \{ \operatorname{ANN}_R(x) \mid 0 \neq x \in M \}$$

(ii) For $X \subseteq \{0\}$ we let $\text{ZD}_R(X) := \{0\}$ and if there is some $x \in X$ with $x \neq 0$ then we define the set of **zero-divisors** of X to be

$$ZD_R(X) := \{ a \in R \mid \exists 0 \neq x \in X : ax = 0 \}$$
$$= \bigcup_{0 \neq x \in X} ANN_R(x)$$

(iii) The complement of the zero-divisors is called the set of **non-zerodivisors** of X, written as $NZD_R(X) := R \setminus ZD_R(X)$. And if there is some $x \in X$ with $x \neq 0$ then this is given to be

$$\operatorname{NZD}_R(X) = \{ a \in R \mid \forall 0 \neq x \in X : ax \neq 0 \}$$

(iv) We thereby define the **torsion submodule** of M to be the collection of elements of M that have an non-trivial annihilator, formally that is

TOR
$$M := \{ x \in M \mid \exists 0 \neq a \in R : ax = 0 \}$$

= $\{ x \in M \mid \operatorname{ANN}_R(x) \neq 0 \}$

Now M is said to be a **torsion module** iff TOR M = M and M is said to be **faithful** or **torsion free** iff $\text{TOR } M = \{0\}$.

(3.16) Proposition: (viz. 263)

Let $(R, +, \cdot)$ be any ring, M be an R-module and $X \subseteq M$ be an arbitrary subset of M. Then we obtain the following statements

(i) The annihilator of an arbitrary set X is a left-ideal of R, the aniihilator of an R-module M even is an ideal of R, formally that is

$$ANN_R(X) \leq_{\mathrm{m}} R$$
$$ANN_R(M) \leq_{\mathrm{i}} R$$

(ii) (\diamond) Let $x \in M$ be any element of the *R*-module *M* and recall that the *R*-submodule of *M* generated by $\{x\}$ is given to be $Rx = \{ax \mid a \in R\}$. Then we obtain the following isomorphy of *R*-modules

$$R_{ANN_R(x)} \cong_{\mathrm{m}} Rx : b + ANN_R(x) \mapsto bx$$

(iii) Let $R \neq 0$ be a non-zero integral domain, then the torsion submodule TOR M truly is an R-submodule of M, formally that is

TOR
$$M \leq_{\mathrm{m}} M$$

and the quotient module of M modulo TOR M is torsion-free, formally

$$\operatorname{TOR}\left(\frac{M}{\operatorname{TOR}M}\right) = \{0\}$$

- (iv) If $R \neq 0$ is not the zero-ring, then the following statements are equivalent (recall that in this case M was said to be *torsion free*)
 - (a) TOR $M = \{0\}$
 - (b) $\operatorname{ZD}_R(M) \subseteq \{0\}$
 - (c) $\forall a \in R, \forall x \in M$ we get $ax = 0 \implies a = 0$ or x = 0
- (v) Suppose R is a commutative ring, then the annihilator of X equals the annihilator of the R-submodule generated by X, formally that is

$$\operatorname{ANN}_R(X) = \operatorname{ANN}_R(\langle X \rangle_m)$$

Consequently if $\{x_i \mid i \in I\} \subseteq M$ is a set of generators of the *R*-module $M = lh\{x_i \mid i \in I\}$ then the annihilator of *M* is given to be

$$\operatorname{ANN}_R(M) = \bigcap_{i \in I} \operatorname{ANN}_R(x_i)$$

(vi) Let $(S, +, \cdot)$ be a skew-field and M be an S-module, if now $x \in M$ is any element of M, then the annihilator of x is given to be

$$\operatorname{ANN}_{S}(x) = \begin{cases} S & \text{if } x = 0\\ 0 & \text{if } x \neq 0 \end{cases}$$

In particular M is torsion free and if $x \neq 0$ then $S \cong_{\mathrm{m}} Sx : a \mapsto ax$.

(vii) Let $(R, +, \cdot)$ be a commutative ring, then maximal, proper annihilator ideals of (the *R*-module) *M* are prime ideals of *R*, formally that is

$$\left(\operatorname{annihil} M \setminus \{R\}\right)^* \subseteq \operatorname{spec} R$$

(3.17) Proposition: (viz. 264) Modular Rule

Let $(R, +, \cdot)$ be an arbitrary ring, M be an R module and P, Q and $U \leq_{\mathrm{m}} M$ be R-submodules of M such that $P \subseteq Q$. Then we obtain

$$(Q \cap U) + P = Q \cap (P + U)$$
$$P \cap U = Q \cap U, P + U = Q + U \implies P = Q$$

(3.18) Definition: (viz. 272)

• Let $(R, +, \cdot)$ be any ring, $I \neq \emptyset$ be an arbitrary index set and for any $i \in I$ let M_i (more explicitly $(M_i, +, \diamond)$) be an *R*-module. Then we regard the Carthesian product of the M_i

$$M := \prod_{i \in I} M_i$$

This can be turned into another *R*-module - called the (exterior) **di**rect product of the M_i - by installing the following (pointwise) algebraic operatons (where $x = (x_i), y = (y_i) \in M$ and *i* runs in $i \in I$)

$$+ : M \times M \to M : (x, y) \mapsto (x_i + y_i)$$

$$\diamond : R \times M \to M : (a, x) \mapsto (ax_i)$$

Note that $x_i + y_i$ is the addition of vectors in M_i and ax_i is the scalar multiplication in M_i and hence these operations are well-defined. It is easy to see that M thereby inherits the properties of an R-module.

We have just introduced the direct product M of the M_i as an R-module. Let us now define a certain R-submodule of M, called the (exterior) direct sum of the M_i. To do this let us first denote the support of x = (x_i) ∈ M to be supp(x) := { i ∈ I | x_i ≠ 0 ∈ M_i } ⊆ I, i.e. the set of indices i with non-vanishing x_i. Then we let

$$\bigoplus_{i \in I} M_i := \left\{ x \in \prod_{i \in I} M_i \; \middle| \; \# \operatorname{supp}(x) < \infty \right\}$$

That is $\bigoplus_i M_i$ consists of all the $x = (x_i) \in \prod_i M_i$ that contain finitely many non-zero coefficients $x_i \neq 0$ only. In particular the direct sum coincides with the direct product if and only if I is finite

$$\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i \iff \#I < \infty$$

And $\bigoplus_i M_i$ becomes an *R*-module again under the same algerbaic operations that we have introduced for the direct product $\prod_i M_i$. Formally that is: the direct sum is an *R*-submodule of the direct product

$$\bigoplus_{i \in I} M_i \leq_{\mathrm{m}} \prod_{i \in I} M_i$$

• (\diamond) Let now N be another R-module and for any $i \in I$ consider an R-module homomorphism $\varphi_i : M_i \to N$. Then we obtain a well-defined R-module-homomorphism from the direct sum to N by virtue of

$$\bigoplus_{i \in I} \varphi_i : \bigoplus_{i \in I} M_i \to N : (x_i) \mapsto \sum_{i \in I} \varphi_i(x_i)$$

This is well-defined, as only finitely many $x_i \in M_i$ are non-zero (as (x_i) is contained in the direct sum of the M_i) and hence the sum only contains finitely many non-zero summands. And the properties of an R-module-homomorphism are trivially inherited from the φ_i .

• Now consider any *R*-module *M* and for any $i \in I$ an *R*-submodule $P_i \leq_{\mathrm{m}} M$. And for any $j \in I$ let us denote by \widehat{P}_j the *R*-submodule generated by all P_i except P_j , formally that is

$$\widehat{P}_j := \sum_{i \neq j} P_i = \langle \bigcup_{i \in I \setminus \{j\}} P_i \rangle_{\mathrm{m}}$$

Then M is said to be the **(inner) direct sum** of the P_i iff the P_i satisfy one of the following two equivalent statements concerning M:

(a) The P_i build up M but for any index $j \in I$ the intersection of P_j and its complement \widehat{P}_j is trivial, formally that is

$$M = \sum_{i \in I} P_i$$
 and $\forall j \in I : P_j \cap \widehat{P}_j = 0$

(b) Any $x \in M$ has a uniquely determined representation as a (finite) sum of elements of the P_i , formally that is

$$\forall x \in M \exists ! (x_i) \in \bigoplus_{i \in I} P_i : x = \sum_{i \in I} x_i$$

And in case that M is the inner direct sum of the P_i we will write (beware the similarity to the exterior direct sum above)

$$M = \bigoplus_{i \in I} P_i$$

• Let M be any R-module and $P \leq_{\mathrm{m}} M$ and R-submodule again. Then P is said to be **complemented** or a **direct summand** of M, iff there is another submodule \widehat{P} of M, such that M is the inner direct sum of P and \widehat{P} . Formally that is: $\exists \widehat{P} \leq_{\mathrm{m}} M$ such that

(1)
$$M = P + \hat{P}$$

(2)
$$P \cap \widehat{P} = 0$$

(3.19) Remark: (viz. 273)

Recall that in Carthesian products (and the direct product has been defined as such) for any $j \in I$ there is a *canonical projection* π_j of the product $\prod_i M_i$ onto M_j . Thereby the projection π_j is defined, to be

$$\pi_j : \prod_{i \in I} M_i \to M_j : (x_i) \mapsto x_j$$

But in contrast to arbitrary Carthesisan products we also find (for any $j \in I$) a canonical embedding ι_j into the direct sum (and product), by letting

$$\iota_j : M_j \to \bigoplus_{i \in I} M_i : x_j \mapsto (\delta_{i,j} x_j)$$

where $\delta_{i,j}x_j := x_j$ for i = j and $\delta_{i,j}x_j := 0 \in M_i$ for $i \neq j$. Then it is clear that $\pi_j \iota_j = 1$ is the identity on M_j and in particular π_j is surjective and ι_j is injective. Further these maps are tightly interwoven with the structure of the direct product and sum respectively. To be precise, consider any $x = (x_i) \in \prod_i M_i$ then we get

$$x = \left(\pi_i(x)\right)$$

On the other hand for any $x = (x_i) \in \bigoplus_i M_i$ we obtain another identity (note that the sum thereby is well-defined, as only finitely many x_i are non-zero, such that in truth the sum is a finite only)

$$x = \sum_{i \in I} \iota_i(x_i)$$

 (\diamondsuit) By definition of the operations on the direct product/sum it is also clear that both projection and embedding are homomorphisms of *R*-modules.

(3.20) Example:

Consider any ring $(R, +, \cdot)$, the *R*-module $M := R^2$ and the submodules $P_1 := R(1,0) = \{ (a,0) \mid a \in R \}$ and $P_2 := R(0,1) = \{ (0,b) \mid b \in R \}$. Then clearly M is the inner direct sum of P_1 and P_2

$$M = P_1 \oplus P_2$$

To check wether M can be decomposed as a direct sum of some P_i it does not suffice to verify, that the intersection of the P_i is pairwise trivial. In the example above let $P_3 := R(1,1) = \{(a,a) \mid a \in R\}$. Then it is clear that $M = P_1 + P_2 + P_3$ and $P_i \cap P_j = 0$ for any $i \neq j \in 1...3$, but M is not the inner direct sum of P_1 , P_2 and P_3 . In fact $x = (1,1) \in M$ has a non-unique representation as $x = (1,0)+(0,1) \in P_1+P_2$ and $x = (1,1) \in P_3$.

(3.21) Remark:

There is a reason why we didn't bother to strictly seperate exterior and inner direct products. The reason simply is: there is not much of a difference, any inner direct product already is an exterior direct product (up to isomorphy) and any exterior direct product can be reformulated as an interior direct product. We will give a precise formulation of this fact in the proposition below. Thus the distinction between inner and exterior is a purely set-theoretic one, it doesn't affect the algebra. This is why we do not bother that our formalism doesn't really distinguish between the interior and exterior direct sums - the difference is no structural one. (In general group theory there *will be* a difference).

(3.22) Proposition: (viz. 274)

(i) (\diamond) Let $(R, +, \cdot)$ be any ring, M be an R-module and $P_i \leq_{\mathrm{m}} M$ be an arbitrary $(i \in I)$ collection of R-submodules of M. If now M is the inner direct sum $M = \bigoplus_i P_i$ of the P_i , then M is already isomorphic (as an R-module) to the exterior direct sum of the P_i under

$$\bigoplus_{i \in I} P_i \cong_{\mathbf{m}} M : (x_i) \mapsto \sum_{i \in I} x_i$$

(ii) Let $(R, +, \cdot)$ be any ring and M_i an arbitrary $(i \in I)$ collection of Rmodules. Now let $P_i := \iota_i(M_i) \leq_{\mathrm{m}} \bigoplus_i M_i$, then the exterior direct sum of the M_i is just the interior direct sum of the P_i put formally

$$\bigoplus_{i \in I} M_i = \bigoplus_{i \in I} P_i$$

(3.23) Proposition: (viz. 274) (\diamondsuit)

Let $(R, +, \cdot)$ be an arbitrary ring and let I and J be arbitrary index sets. For any $i \in I$ resp. $j \in J$ let M_i and N_j be R-modules. Then we obtain the following isomorphy of R-modules

$$\operatorname{mhom}\left(\bigoplus_{i\in I} M_i, \prod_{j\in J} N_j\right) \cong_{\mathrm{m}} \prod_{(i,j)\in I\times J} \operatorname{mhom}(M_i, N_j)$$

We can even give the above isomorphism explicitly: let us denote the direct sum of the M_i by $M := \bigoplus_i M_i$ and the direct product of the N_j by $N := \prod_j N_j$. Further denote the canonical embedding $\iota_i : M_i \to M$ and the canonical projection $\pi_j : N \to N_j$. Then the isomorphy explicitly reads as

$$\begin{array}{ll} \mathrm{mhom}(M,N) & \cong_{\mathrm{m}} & \prod_{(i,j)\in I\times J} \mathrm{mhom}(M_{i},N_{j}) \\ \varphi & \mapsto & \left(\pi_{j}\varphi\pi_{i}\right) \\ \left(\bigoplus_{i\in I}\varphi_{i,j}\right) & \longleftrightarrow & \left(\varphi_{i,j}\right) \end{array}$$

Let us explain this comact notation a bit: for any $(I \times J)$ -tupel of homomorphisms $\varphi_{i,j} : M_i \to N_j$ the corresponding homomorphism $\varphi := (\bigoplus_i \varphi_{i,j})$ is explicitly given to be the following: $\varphi : M \to N : (x_i) \to (\sum_i \varphi_{i,j}(x_i))$.

(3.24) Remark:

Suppose we even have $(\varphi_{i,j}) \in \prod_i \bigoplus_j \operatorname{mhom}(M_i, N_j)$, that is for any $i \in I$ the set $\{j \in J \mid \varphi_{i,j} \neq 0\}$ is finite. Then the induced map φ even lies in $(\bigoplus_i \varphi_{i,j}) \in \operatorname{mhom}(\bigoplus_i M_i, \bigoplus_j N_j)$. The converse need not be true however, as an example regard $I = 0, J = \mathbb{N}, M = R^{\oplus \mathbb{N}}$ and $N_j = R$. As a homomorphism φ we choose the identity $\varphi = \mathbb{1} : R^{\oplus \mathbb{N}} \to R^{\oplus \mathbb{N}}$. Then φ induces the tuple $\mathbb{1} \mapsto (\pi_j)$, which has no finite support.

3.3 Free Modules

The primary task of any algebraic theory is to classify the objects involved. The same is true for module theory: what types of modules do exist? Surprisingly the answer will strongly depend on the module's base ring. A first complete answer can be given in the case that the base ring is a skew-field S, then all modules over S are of the form $S^{\oplus I}$ for some index set I. (We will later also find complete answers in case the base ring is a PID or DKD. But this is how far the theory carries).

In order to achieve this result we will have to define the notion of a *basis* of a module. Modules with basis will be said to be *free*. And free modules are all of the form $R^{\oplus I}$, where R is the base ring and I is the (cardinality of) the basis. This is the easy part, it remains to show that any module over a skew-field has a basis. It is customary to approach this problem directly. However we will try a more abstract approach: first we will introduce the general notion of a *dependence relation*. Then we will prove that any dependence relation admits a basis and lastly we will prove that linear dependence (over a skew-field) is a dependence relation.

This approach features two advantages: first it neatly seperates settheoretic and algebraic concepts, which yields a beautiful clarity and pinpoints precisely where the skew-field is involved. And secondly we will be able to put this theory to good use when it comes to algebraic dependence and transcendence bases. So let us begin with some preparational set-theory: dependence relations.

(3.25) Definition:

Let M be an arbitrary set, in the following we will regard relations \vdash of the following form $\vdash \subseteq \mathcal{P}(M) \times M$. And for any such relation, elements $x \in M$ and subsets $S, T \subseteq M$ we will use the following notations

$$S \vdash x \quad :\iff \quad (S, x) \in \vdash$$

$$S \vdash x \quad :\iff \quad \neg(S \vdash x)$$

$$\langle S \rangle \quad := \quad \{ x \in M \mid S \vdash x \}$$

$$\operatorname{sub}(M) \quad := \quad \{ \langle S \rangle \mid S \subseteq M \}$$

$$T \vdash S \quad :\iff \quad S \subseteq \langle T \rangle$$

$$\iff \quad \forall x \in S : T \vdash x$$

Now \vdash is said to be a **dependence relation** on M, iff it is of the form $\vdash \subseteq \mathcal{P}(M) \times M$ and for any elements $x \in M$ and subsets $S, T \subseteq M$ it satisfies the following four properties:

(D1) any element x of S already depends on S, formally this can be put as

$$x \in S \implies S \vdash x$$

(D2) if x depends on S and S depends on T, then x already depends on T

$$T \vdash S, S \vdash x \implies T \vdash x$$

(D3) if x depends on S, then it already depends on a finite subset S_x of S

$$S \vdash x \implies \exists S_x \subseteq S : \#S_x < \infty \text{ and } S_x \vdash x$$

(D4) if x depends on S but not on $S \setminus \{s\}$ (for some $s \in S$), then we can interchange the dependencies of x and s, formally again

$$S \vdash x, \ s \in S, \ S \setminus \{s\} \not \vdash x \implies \left((S \setminus \{s\}) \cup \{x\} \right) \vdash s$$

And in case that \vdash is a dependence realtion on M we further introduce the following notions: a subset $S \subseteq M$ is said to be **independent** (or more precisely \vdash independent), iff it satisfies

$$\forall s \in S : S \setminus \{s\} \not\vdash s$$

Clearly S is said to be **dependent** (or more precisely \vdash dependent), iff it is not independent (that is $S \setminus \{s\} \vdash s$ for some $s \in S$). And a subset $B \subseteq M$ is said to be a **basis** (or more precisely a \vdash basis) iff it is independent and generates M. Formally B is a basis, iff it satisfies

(B1) B is independent

(B2) $\langle B \rangle = M$

(3.26) Lemma: (viz. 280)

Let M be an arbitrary set, $S, T \subseteq M$ be arbitrary subsets and \vdash be a dependence relation on M. Then we obtain all of the following statements

(i) The generation of subsets under \vdash preserves the inclusion of sets, i.e.

$$S \subseteq T \implies \langle S \rangle \subseteq \langle T \rangle$$

(ii) Recall that we denoted $\operatorname{sub}(M)$ to be the set of all $\langle T \rangle$ for some subset $T \subseteq M$. Then for any subset $S \subseteq M$ we obtain the identities

$$\langle \langle S \rangle \rangle = \langle S \rangle = \bigcap \{ P \in \operatorname{sub}(M) \mid S \subseteq P \}$$

- (iii) For any subset $S \subseteq M$ the following three statements are equivalent
 - (a) S is \vdash dependent
 - (b) $\forall T \subseteq M : S \subseteq T \implies T$ is \vdash dependent
 - (c) $\exists S_0 \subseteq S$ such that $\#S_0 < \infty$ and S_0 is \vdash dependent
- (iv) For any subset $T \subseteq M$ the following three statements are equivalent
 - (a) T is \vdash independent
 - (b) $\forall S \subseteq M : S \subseteq T \implies S$ is \vdash independent
 - (c) $\forall T_0 \subseteq T$ we get $\#T_0 < \infty \implies T_0$ is \vdash independent
- (v) For any $S \subseteq M$ and $x \in M$ the following statements are equivalent
 - (a) $S \cup \{x\}$ is \vdash independent and $x \notin S$
 - (b) S is \vdash independent and $S \not\vdash x$
- (vi) Let $S_i \subseteq M$ be a chain (where $i \in I$ of \vdash idependent subsets of M, then the union of the S_i is \vdash independent again. Formally that is

$$\begin{array}{ll} \forall i \in I & : \quad S_i \text{ is } \vdash \text{independent} \\ \forall i, j \in I & : \quad S_i \subseteq S_j \text{ or } S_j \subseteq S_i \end{array} \right\} \implies \bigcup_{i \in I} S_i \text{ is } \vdash \text{independent}$$

- (vii) Let $S \subseteq M$ be an \vdash independent subset and $T \subseteq M$ be a generating subset $M = \langle T \rangle$. If now $S \subseteq T$, then there is some $B \subseteq X$ such that
 - (1) $S \subseteq B \subseteq T$ and
 - (2) B is a \vdash basis of M
- (viii) Let $B \subseteq M$ be a \vdash basis of $X, b \in B$ and $x \in M$ be arbitary. Then we denote by $B' := (B \setminus \{b\}) \cup \{x\}$ the set B with b replaced by x. If now $B' \vdash b$, then B' is a \vdash basis of M, as well.

- (ix) A subset $B \subseteq M$ is a \vdash basis of M if and only if it is a minimal \vdash generating subset of M. And this again is equivalent to being a maximal \vdash independent subset. Formally that is the equivalency of
 - (a) B is a \vdash basis of M
 - (b) B generates M (that is $M = \langle B \rangle$) and for any $S \subseteq M$ we obtain

 $S \subset B \implies M \neq \langle S \rangle$

(c) B is \vdash independent and for any $S \subseteq M$ we obtain the implication

 $B \subset S \implies S \text{ is not } \vdash \text{independent}$

(x) All \vdash bases of M have the same number of elements, formally that is

 $A, B \subseteq M \vdash \text{bases of } M \implies |A| = |B|$

- (xi) If $S \subseteq M$ is \vdash independent and $B \subseteq M$ is an \vdash basis of M, then S contains no more elements than B, that is $|S| \leq |B|$.
- (xii) Consider a \vdash independent subset $S \subseteq M$ and a \vdash basis $B \subseteq M$ of M. Further assume that $\#B < \infty$ is finite, then the following two statements are equivalent
 - (a) |S| = |B|
 - (b) S is an \vdash basis of M

NOTA that in the proof of this lemma we did not always require all the properties of a dependence relation. Namely (i), (ii), (iii), (iv), the implication (a) \implies (b) in (v), (vi) and the equivalence (a) \iff (b) in (ix) require the relation \vdash to satisfy properties (D1), (D2) and (D3) only.

(3.27) Remark:

In item (vi) we may chose $S = \emptyset$, as this always is \vdash independent respectively T = M, as always $M = \langle M \rangle$. These special choices yield the so called basis selection respectively basis completion theorems (the converse implications follow immediately from (i) and (ii) repsectively). And as these are used frequently let us append them here. Thus suppose M is an arbitrary set and \vdash is a dependence relation on M again. Then we get

- Basis Selection Theorem: a subset $T \subseteq M$ contains a \vdash basis of M if and only if it generates M, that is equivalent are
 - (a) $\langle T \rangle = M$
 - (b) $\exists B \subseteq T : B$ is a \vdash basis of M

- Basis Completion Theorem: a subset $S \subseteq M$ can be extended to a \vdash basis of M if and only if S is \vdash independent, that is equivalent are
 - (a) S is \vdash independent
 - (b) $\exists B \subseteq M : S \subseteq B$ and B is a \vdash basis of M

(3.28) Definition:

Let $(R, +, \cdot)$ be an arbitrary ring an M be R-module. Further consider an arbitrary subset $X \subseteq M$. Then we introduce the following notions

(i) A subset $X \subseteq M$ is said to generate M as an R-module (or simply to R-generate M), iff the R-module generated by X is M. Formally that is iff (where we also recalled proposition (3.11))

$$M = \langle X \rangle_{\mathbf{m}} = \left\{ \sum_{i=1}^{n} a_i x_i \mid 1 \le n \in \mathbb{N}, a_i \in R, x_i \in X \right\}$$

Now X is said to be a **minimal** R-generating set, iff X R-generates M but any proper subset of X does not R-generate M, formally iff

$$\forall W \subseteq M : W \subset X \Longrightarrow \langle W \rangle_{\mathrm{m}} \neq M$$

(ii) We thereby define the **rank** - denoted by rank(M) - to be the minimal cardinality of an *R*-generating subset X of M. Formally that is

 $\operatorname{rank}(M) := \min\{ |X| \mid X \subseteq M, \langle X \rangle_{\mathrm{m}} = M \}$

NOTA that this is well defined, as the cardinal numbers are welloredered. That is any non-empty set of cardinal numbers has a minimal element. And the defining set above is non-empty, as $M \subseteq M$ and $M = \langle M \rangle_{\rm m}$. In particular we have rank $(M) \leq |M|$.

- (iii) M is said to be **finitely generated**, iff it is R-generated by some finite subset $X \subseteq M$. That is iff it satisfies one of the equivalent conditions
 - (a) $\operatorname{rank}(M) < \infty$
 - (b) $\exists X \subseteq M : \#X < \infty$ and $M = \langle X \rangle_{\mathrm{m}}$
- (iv) Let us now introduce a relation of the form $\vdash \subseteq \mathcal{P}(M) \times M$ called the relation of *R*-linear dependence. For any subset $X \subseteq M$ and any element $x \in M$ let us define

$$X \vdash x \quad :\iff \quad \begin{array}{l} \exists n \in \mathbb{N}, \exists x_1, \dots, x_n \in X, \exists a_1, \dots, a_n \in R \\ \text{such that } x = a_1 x_1 + \dots + a_n x_n \end{array}$$

NOTA that we allowed n = 0 in this definition. And by convention the empty sum is set to be 0. Thus we get $X \vdash 0$ for any subset $X \subseteq M$. In fact we even get $\emptyset \vdash x \iff x = 0$ for any $x \in M$. (v) A subset $X \subseteq M$ is said to be *R*-linearly dependent iff for any $1 \leq n \in \mathbb{N}$, any $x_1, \ldots, x_n \subseteq X$ and any $a_1, \ldots, a_n \in R$ we get

$$\begin{array}{l} a_1 x_1 + \dots + a_n x_n = 0 \\ \forall i, j \in 1 \dots n : x_i = x_j \implies i = j \end{array} \right\} \implies a_1 = \dots = a_n = 0$$

If this is not the case (i.e. there are some $a_1, \ldots, a_n \in R \setminus \{0\}$ and pairwise distinct $x_1, \ldots, x_n \in X$ such that $a_1x_1 + \cdots + a_nx_n = 0$), then X is said to be *R*-linearly dependent. Finally X is said to be a **maximal** *R*-linearly independent set, iff X is *R*-linearly dependent, but any proper superset of X is *R*-linearly dependent. Formally

$$\forall Y \subseteq M : X \subset Y \implies Y \text{ is } R\text{-linearly dependent}$$

(vi) A subset $B \subseteq M$ is said to be a *R*-basis of *M*, iff it is *R*-linearly independent (that is (iv)) and *R*-generates *M* (that is (i)). And *M* is said to be **free**, iff it has a basis. That is

$$M$$
 free $\iff \exists B \subseteq M : B$ is a R -basis

- (vii) Finally an ordered tupel $(x_i) \subseteq M$ (where $i \in I$) is said to be an **ordered** *R*-basis of *M*, iff it satisfies the following two properties
 - (1) $\{x_i \mid i \in I\}$ is a *R*-basis of *M*
 - (2) $\forall i, j \in I : x_i = x_j \implies i = j$

(3.29) Example:

• A very special case in the above definitions is the zero-module $\{0\}$. It is a free module, as $\emptyset \subseteq \{0\}$ is an *R*-basis. And thereby for an arbitrary *R*-module *M* we obtain

$$\operatorname{rank}(M) = 0 \iff M = \{0\}$$

PROB trivially \emptyset is *R*-linearly independent and \emptyset also generates $\{0\}$, as $\{0\}$ is the one and only submodule of $\{0\}$. Together \emptyset is an *R*-basis of $\{0\}$ and in particular rank $\{0\} = 0$. Conversely if rank M = 0, then by definition $M = \langle \emptyset \rangle_m = \{0\}$.

• Consider an integral domain $(R, +, \cdot)$ and an *R*-submodule (that is an ideal) $\mathfrak{a} \leq_{\mathrm{m}} R$. Then \mathfrak{a} is a free *R*-module, if and only if it is principal

$$\mathfrak{a}$$
 free $\iff \exists a \in R : \mathfrak{a} = aR$

PROB first suppose $\mathfrak{a} = aR$ is principal. If a = 0, then $\mathfrak{a} = 0$, which is a free *R*-module, with basis \emptyset . And if $a \neq 0$, then $\{a\}$ is an *R*basis of \mathfrak{a} . It generates \mathfrak{a} , as $\langle \{a\} \rangle_{\mathrm{m}} = aR = \mathfrak{a}$ and it is *R*-linearly independent, as $ba = 0 \implies b = 0$ (as $a \neq 0$ and *R* is an integral domain). Conversely suppose \mathfrak{a} is free, with basis $B \subseteq \mathfrak{a}$. If $B = \emptyset$, then $\mathfrak{a} = \langle \emptyset \rangle_{\mathrm{m}} = 0$, which is principal $\mathfrak{a} = 0 = R0$. And if we had $\#B \ge 2$, then we could choose some $b_1, b_2 \in B$. But this would yield $b_2b_1 + (-b_1)b_2 = 0$ (as *R* is commutative) and hence *B* would not be *R*-linearly independent. Thus it only remains #B = 1, say $B = \{a\}$ and hence $\mathfrak{a} = \langle B \rangle_{\mathrm{m}} = aR$ is principal.

• The standard example of a free module is the following: let $(R, +, \cdot)$ be an arbitrary ring and $I \neq \emptyset$ be any non-empty set. Then we let

$$R^{\oplus I} := \bigoplus_{i \in I} R = \{ (x_i) \in R^I \mid \# \{ i \in I \mid x_i \neq 0 \} < \infty \}$$

Recall that this is an *R*-module under the component-wise operations $(x_i) + (y_i) := (x_i + y_i)$ and $a(x_i) := (ax_i)$ - where a, a_i and $y_i \in R$. For any $j \in I$ let us now denote the *j*-th Euclidean vector

$$e_j := (\delta_{i,j}) \in R^{\oplus I}$$

That is the *i*-th component of e_j is 1 if and only if i = j and 0 otherwise. Then $R^{\oplus I}$ is a free *R*-module having the **Euclidean basis**

$$E = \{ e_j \mid j \in I \}$$

PROB we have to prove that E is an R-linearly independent set, that also R-generates $R^{\oplus I}$. Thus suppose we are given any $x = (x_i) \in R^{\oplus I}$. Let us denote $\Omega := \{i \in I \mid x_i \neq 0\}$, then Ω is finite, by definition of $R^{\oplus I}$. And hence we get $x = \sum_{i \in \Omega} x_i e_i \in \langle E \rangle_{\mathrm{m}}$. Therefore Egenerates $R^{\oplus I}$ as an R-module. For the R-linear independence we have $\sum_{i \in \Omega} a_i e_i = 0$ for sume finite subset $\Omega \subseteq I$ and some $a_i \in R$. We now compare the coefficients of 0 and $\sum_{i \in \Omega} a_i e_i$. Hereby for any $i \in \Omega$ the *i*-th coefficient of $0 \in R^{\oplus I}$ is $0 \in R$. And the *i*-th coefficient of $\sum_{i \in \Omega} a_i e_i$ is a_i . That is $a_i = 0$ for any $i \in \Omega$ and this means that Eis R-linearly independent.

(3.30) Proposition: (viz. 284)

Let $(R, +, \cdot)$ be an arbitrary ring and M be an R-module. Let us denote the relation of R-linear dependence by \vdash again (refer to (3.28.(iv))). Then the following statements hold true

- (i) The relation \vdash satisfies the properties (D1), (D2) and (D3) of a dependence relation (refer to (3.25) for the explicit definitions).
- (ii) If $X \subseteq M$ is any subset and we denote $\langle X \rangle := \{ y \in M \mid X \vdash y \}$ again, then we obtain the following identities

$$\langle X \rangle = \langle X \rangle_{\mathrm{m}} = \mathrm{lh}_R(X)$$

- (iii) For any subset $X \subseteq M$ the following three statements are equivalent
 - (a) X is \vdash dependent
 - (b) $\forall Y \subseteq M : X \subseteq Y \implies Y$ is \vdash dependent
 - (c) $\exists X_0 \subseteq X$ such that $\#X_0 < \infty$ and X_0 is \vdash dependent
- (iv) For any subset $Y \subseteq M$ the following three statements are equivalent
 - (a) Y is \vdash independent
 - (b) $\forall X \subseteq M : X \subseteq Y \implies X$ is \vdash independent
 - (c) $\forall Y_0 \subseteq Y$ we get $\#Y_0 < \infty \implies Y_0$ is \vdash independent
- (v) A subset $B \subseteq M$ is a \vdash basis of M if and only if it is a minimal \vdash generating subset of M. Formally that is the equivalency of
 - (a) B is a \vdash basis of M
 - (b) $M = \langle B \rangle$ and $S \subset B \implies M \neq \langle S \rangle$
- (vi) A subset $B \subseteq M$ is an *R*-basis of *M* if and only if any $x \in M$ has a unique representation as an *R*-linear combination over *B*. Formally that is the equivalency of
 - (a) B is an R-basis of M
 - (b) for any element $x \in M$ there is a uniquely determined tupel $(x_b) \in R^{\oplus B}$ such that x can be represented in the form

$$x = \sum_{b \in B} x_b b$$

NOTA that the sum occuring in (b) is well-defined, as only finitely many of the x_b are non-zero. Further note that in fact the existence of such a representation is equivalent to $M = \langle B \rangle_{\rm m}$ and the uniqueness of the representation is equivalent to the *R*-linear independence of *B*.

(3.31) Proposition: (viz. 286)

Let $(S, +, \cdot)$ be a skew-field and M be an S-module. Let us denote the relation of S-linear dependence by \vdash again (refer to (3.28.(iv))). Then we obtain the following statements in addition to (3.30)

(i) \vdash is a dependence relation (in the sense of (3.25)), that even satisfies the following property (for any $X \subseteq M$ and any $x, y \in M$)

$$x \in X, \ X \vdash y, \ y \neq 0 \implies ((X \setminus \{x\}) \cup \{y\}) \vdash x$$

- (ii) Let $X \subseteq M$ be an arbitrary subset, then the following two statements are equivalent (for arbitrary rings we only get (b) \implies (a))
 - (a) X is \vdash independent
 - (b) X is S-linearly independent
- (iii) For any $X \subseteq M$ and $y \in M$ the following statements are equivalent
 - (a) $X \cup \{y\}$ is S-linearly independent and $y \notin X$
 - (b) X is S-linearly independent and $X \not\vdash y$
- (iv) For any subset $B \subseteq M$ all of the following statements are equivalent
 - (a) B is a \vdash basis of M
 - (b) B is an S-basis of M
 - (c) B is a minimal S-generating subset of M, that is B generates M (i.e. $M = lh_S(B)$) and for any $X \subseteq M$ we obtain

$$X \subset B \implies M \neq \ln_S(X)$$

(d) B is a maximal S-linearly independent subset, that is B is S-linearly independent and for any $X \subseteq M$ we obtain

 $B \subset X \implies X$ is not S-linearly independent

(e) for any element $x \in M$ there is a uniquely determined tupel $(x_b) \in S^{\oplus B}$ such that x can be represented in the form

$$x = \sum_{b \in B} x_b b$$

- (v) Let $X \subseteq M$ be a S-linearly independent subset and $Y \subseteq M$ be a generating subset $M = lh_S(Y)$. If now $X \subseteq Y$, then there is some $B \subseteq M$ such that
 - (1) $X \subseteq B \subseteq Y$ and
 - (2) B is an S-basis of M
- (vi) All S-bases of M have the same number of elements, formally that is

 $A, B \subseteq M$ S-bases of $M \implies |A| = |B|$

Thus by (v) M has an S-basis (it is a free module) and by (vi) all S-bases of M share the same cardinality. Hence we may define the **dimension** of M over S to be the cardinality of any S-basis of M. That is we let

$$\dim_S(M) := |B|$$
 where B is an S-base of M

(vii) A set of S-linearly elements contains at most $\dim_S(M)$ many elements

 $X \subseteq M$ S-linearly independent $\implies |X| \leq \dim_S(M)$

- (viii) Suppose M is finite-dimensional (i.e. $\dim_S(M) < \infty$) and consider an S-linearly independent subset $X \subseteq M$. Then the following two statements are equivalent
 - (a) $|X| = \dim_S(M)$
 - (b) X is an S-basis of M

3.4 Homomorphisms

def: homomorphisms, lem: isomorphism theorems, (short) exact sequences, split exact

(3.32) Lemma: (viz. ??)

Let $(R, +, \cdot)$ be a commutative ring then the following statements are true

(i) If $R \neq 0$ is non-zero and $1 \leq m, n \in \mathbb{N}$ are numbers then R^m is isomorphic (as an *R*-module) to R^n iff *m* and *n* are equal

 $R^m \cong_{\mathrm{m}} R^n \iff m = n$

(ii) Let $\mathfrak{a}, \mathfrak{b} \leq_{i} R$ be two ideals in R, if now R/\mathfrak{a} and R/\mathfrak{b} are isomorphic as R-algebras, then \mathfrak{a} and \mathfrak{b} are isomorphic as R-modules

$${R\!/}_{\mathfrak{a}} \cong_{\mathrm{a}} {R\!/}_{\mathfrak{b}} \implies \mathfrak{a} \cong_{\mathrm{m}} \mathfrak{b}$$

(3.33) Remark:

- The statement of (i) need not be true for non-commutative rings R. As an example fix any ring R, number $k \in \mathbb{N}$ and let $S := \operatorname{end}(()R^k)$ be the ring of R-module endomorphisms of R^k . Then for any $m, n \in \mathbb{N}$ we get $S^m \cong_{\mathrm{m}} S^n$ as an S-module.
- A ring R with the property of (i) is also called to have IBN (invariant basis number). Thus (i) may be expressed as *commutative rings have IBN*. Of course there is a multitude of non-commutative rings that have IBN as well. An important example is: if $\varphi : R \rightarrow S$ is a ring-epimorphism and S has IBN then R has IBN, as well. For more comments on this, please refer to the first chapter of [Lam].
- Likewise the converse of (ii) is false in general e.g. regard S := R[s, t]. If we now define the ideals $\mathfrak{a} := tS$ and $\mathfrak{b} := stS$ then \mathfrak{a} and \mathfrak{b} clearly are isomorphic as *R*-modules, but we find

$$\begin{array}{ll} S/_{\mathfrak{g}} & \cong_{\mathbf{a}} & R[s] \\ S/_{\mathfrak{f}} & \cong_{\mathbf{a}} & R[s] \oplus tR[t] \end{array}$$

3.5 Rank of Modules

3.6 Length of Modules

3.7 Localisation of Modules
Chapter 4

Linear Algebra

4.1 Matices

4.2 Elementary Matrices

4.3 Linear Equations

4.4 Determinants

4.5 Rank of Matrices

4.6 Canonical Forms

Chapter 5

Structure Theorems

5.1 Asociated Primes

Skripten von Dimitrios und Benjamin Matsumura Kapitel 6 (in Teil 2)

Bourbaki (commutative algebra) IV.1, IV.2

Eisenbud 3.1, 32., 3.3, Aufgaben 3.1, 3.2, 3.3

Dummit, Foote: Kapitel 15.1: Aufgaben 29, 30, 31, 32, 33, 34 und 35 Kapitel 15.4: Aufgaben 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 und 40 Kapitel 15.5: Aufgaben 25, 26, 28, 29 (bemerke $\operatorname{ass}_R \subseteq \operatorname{ass}(\mathfrak{a})$ geht viel einfacher direkt). und 30

5.2 Primary Decomposition

5.3 The Theorem of Prüfer

Chapter 6

Polynomial Rings

6.1 Monomial Orders

We have already introduced the polynomial ring R[t] in one variable (over a commutative ring R) as an example in section 1.3. And we have also used this concept in the chapter on linear algebra (e.g. the characteristic polynomial of a linear mapping). In this chapter we will now introduce a powerful generalisation of this ring - the polynomial ring (also called group ring) R[A]. Thereby R is a commutative ring once more and A will be any commutative monoid. On the other hand polynomial rings are natural examples of graded algebras. So it may be advantegeous to first study graded algebras as a general concept. This will be done in the subsequent section.

There are a multitude of special cases of this concept which we will regard in this chapter, as well. The most important special case will be the polynomial ring $R[t_1, \ldots, t_n]$ in (finitely many) variables. The polynomials $f \in R[t_1, \ldots, t_n]$ are the working horses of ring theory, as they describe all the compositions (of additions and multiplications) that can be performed in a ring. This makes the study of the polynomial ring a task of vast importance and likewise gives the theory its punch.

The polynomial ring R[t] is included into this general theory as the polynomial ring R[A] where A is chosen to be the the natural numbers $A = \mathbb{N}$. Yet the algabraic structure of \mathbb{N} is not the sole important property for R[t]. The natural order \leq on \mathbb{N} is of no lesser importance. Therefore we will first study moniods A that carry an adequate order, as well.

So first recall the definitition of a *linear order* (also called *total order*). If you are not familiar with this notion take a look at the introduction (section 0.2) or (re)read the beginning of section 2.1 for even more comments. So let uns now introduce the basic concepts of ordered monoids:

(6.1) Definition:

Let (A, +) be a commutative monoid and denote its neutral element by 0. Then we introduce the following notions concerning A

• A is said to be **integral** iff for any $\alpha, \beta, \gamma \in A$ we get the implication

 $\alpha + \gamma \; = \; \beta + \gamma \quad \Longrightarrow \quad \alpha \; = \; \beta$

• Further we A is said to be **solution-finite** iff for any fixed $\gamma \in A$ the equation $\alpha + \beta = \gamma$ has finitely many solutions only, formally that is

$$\forall \gamma \in A : \# \left\{ (\alpha, \beta) \in A^2 \mid \alpha + \beta = \gamma \right\} < \infty$$

(6.2) Definition:

- (i) The triple $(A, +, \leq)$ is said to be a **positively ordered monoid**, iff it satisfies both of the following two properties
 - (1) (A, +) is a commutative monoid (with neutral element 0)
 - (2) \leq is a positive, linear order on A. That is \leq is a linear order such that for any elements α, α' and $\beta \in A$ we get the implication

$$\alpha \le \alpha' \implies \alpha + \beta \le \alpha' + \beta$$

- (ii) The triple $(A, +, \leq)$ is said to be a strictly positively ordered monoid, iff it satisfies both of the following two properties
 - (1) (A, +) is a commutative monoid (with neutral element 0)
 - (2) \leq is a strictly positive, linear order on A. That is \leq is a linear order such that for any elements α, α' and $\beta \in A$ we get

$$\alpha < \alpha' \implies \alpha + \beta < \alpha' + \beta$$

Note that thereby we used the convention $a < b :\iff a \leq b$ and $a \neq b$. Thus it is clear that a strictly positively ordered monoid already is a positively ordered monoid (if $\alpha = \alpha'$, then $\alpha + \beta = \alpha' + \beta$ is clear).

- (iii) Finally $(A, +, \leq)$ is said to be an **monomially ordered monoid** and \leq is said to be a **monomial order** on (A, +) iff we get
 - (1) $(A, +, \leq)$ is a positively ordered monoid
 - (2) \leq is a well-ordering on A, that is iff any nonempty subset M of A has a minimal element, formally this can be written as

$$\forall \emptyset \neq M \subseteq A \ \exists \mu_* \in M \text{ such that } \forall \mu \in M \text{ we get } \mu_* \leq \mu$$

(6.3) Remark:

If now $(A, +, \leq)$ is a positively ordered monoid, we extend A to \overline{A} by formally picking up a new element $-\infty$ (i.e. we introduce a new symbol to A)

$$\overline{A} := A \cup \{-\infty\}$$

We then extend the composition + and order \leq of A to \overline{A} defining the following operations and relations for any $\alpha \in A$

$$(-\infty) \neq \alpha$$

$$(-\infty) \leq \alpha$$

$$(-\infty) + \alpha := -\infty$$

$$\alpha + (-\infty) := -\infty$$

NOTA clearly $(\overline{A}, +)$ thereby is a commutative monoid again and if \leq has been a positive or monomial order on \overline{A} then the extended order on $\overline{\overline{A}}$ is a positive resp. monimial order again.

(6.4) Example:

The standard example of a monoid that we will use later is \mathbb{N}^n under the pointwise addition as the composition. However we will already discuss a slight generalisation of this monoid here. Let $I \neq \emptyset$ be any nonempty index set and let us define the set

$$\mathbb{N}^{\oplus I} := \left\{ \alpha \in \mathbb{N}^{I} \mid \# \left\{ i \in I \mid \alpha_{i} \neq 0 \right\} < \infty \right\}$$

If I is finite, say $I = 1 \dots n$, then it is clear, that $\mathbb{N}^{\oplus(1\dots n)} = \mathbb{N}^n$. We now turn this set into a commutative monoid by defining the composition + to be the pointwise addition, i.e. for any $\alpha = (\alpha_i)$ and $\beta = (\beta_i)$ we let

$$(\alpha_i) + (\beta_i) := (\alpha_i + \beta_i)$$

And it is clear that this composition turns $\mathbb{N}^{\oplus I}$ into a commutative monoid, that is integral and solution-finite (for any $\gamma \in \mathbb{N}^{\oplus I}$ the set of solutions (α, β) of $\alpha + \beta = \gamma$ is determined given to be $\{ (\alpha, \gamma - \alpha) \mid \alpha_i \leq \gamma_i \}$, which is finite, as $\gamma \in \mathbb{N}^{\oplus I}$). For any $i \in I$ we now define

$$\delta_i : I \to \mathbb{N} : j \mapsto \delta_{i,j}$$

where $\delta_{i,j}$ denotes the Kronecker symbol (e.g. refer to the notation and symbol list). From the construction it is clear, that any $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$ is a (uniquely determined) *finite* sum of these δ_i since

$$(\alpha_i) = \sum_{i \in I} \alpha_i \, \delta_i$$

This sum in truth is finite as only finitely many coefficients α_i are non-zero and we can omit those $i \in I$ with $\alpha_i = 0$ from the sum. This enables us to introduce some notation here that will be put to good use later on. • Let us first define the **absolute value** and **norm** of $\alpha = (\alpha_i) \in \mathbb{N}^{\oplus I}$

$$\begin{aligned} |\alpha| &:= \sum_{i \in I} \alpha_i \\ \|\alpha\| &:= \max\{\alpha_i \mid i \in I\} \end{aligned}$$

• For a fixed weight $\omega \in \mathbb{N}^I$ we introduce the **weighted sum** of α (note that this is well-defined, as $\alpha \in \mathbb{N}^{\oplus I}$ only has finitely many non-zero entries and hence the sum is finite only)

$$|\alpha|_{\omega} := \sum_{i \in I} \omega_i \alpha_i$$

• Another oftenly useful notation (for any $\alpha \in \mathbb{N}^{\oplus I}$ and any $k \in \mathbb{N}$ with $\|\alpha\| \le k$) are the **faculty** and **binomial coefficients**

$$\begin{array}{rcl} \alpha! & := & \prod_{i \in I} \alpha_i! \\ \binom{k}{\alpha} & := & \prod_{i \in I} \binom{k}{\alpha_i} \end{array}$$

• And if $x = (x_i) \in \mathbb{R}^I$ is an *n*-tupel of elements of a commutative ring $(\mathbb{R}, +, \cdot)$ we finally introduce the notations (note that these are well-defined again, as $\alpha \in \mathbb{N}^{\oplus I}$ has only finitely many $\alpha_i \neq 0$)

$$\begin{array}{rcl} \alpha x & := & \sum_{i \in I} \, \alpha_i \, x_i \\ x^{\alpha} & := & \prod_{i \in I} \, x_i^{\alpha_i} \end{array}$$

(6.5) **Proposition:** (viz. 242)

(i) Let $A \neq \emptyset$ be a non-empty set and $\leq \subseteq A \times A$ be a linear order on A. Then any finite, non-empty subset $\emptyset \neq M \subseteq A$ has uniquely determined minimal and a maximal elements. I.e. for any $\emptyset \neq M \subseteq A$ with $\#M < \infty$ we get

$$\exists ! \ \mu_* \in M : \ \forall \ \mu \in M : \ \mu_* \leq \mu$$
$$\exists ! \ \mu^* \in M : \ \forall \ \mu \in M : \ \mu \leq \mu^*$$

(ii) Let $A \neq \emptyset$ be a non-empty set and $\leq \subseteq A \times A$ be a well-ordering on A. Then any non-empty subset $\emptyset \neq M \subseteq A$ has a uniquely determined minimal element. I.e. for any $\emptyset \neq M \subseteq A$ we get

$$\exists ! \ \mu_* \in M : \forall \ \mu \in M : \mu_* \le \mu$$

NOTA we will refer to these minimal and maximal elements of M by writing min $M := \mu_*$ and max $M := \mu^*$ respectively.

- (iii) Let (A, +) be a commutative monoid and let $\leq \subseteq A \times A$ be a linear order on A. Then the following three statements are equivalent
 - (a) A is integral and \leq is a positive order on A
 - (b) $(A, +, \leq)$ is a strictly positively ordered monoid
 - (c) for any $\alpha, \beta, \gamma \in A$ we get $\alpha < \beta \iff \alpha + \gamma < \beta + \gamma$
- (iv) Let $(A, +, \leq)$ be a positively ordered monoid, such that (A, +) is integral. Let further $M, N \subseteq A$ be any two subsets and $\mu_* \in M$ respectively $\nu_* \in N$ be minimal elements of M and N, i.e.

 $\forall \mu \in M : \mu_* \leq \mu \quad \text{and} \quad \forall \nu \in N : \nu_* \leq \nu$

Then for any elements $\mu \in M$ and $\nu \in N$ we obtain the implication

$$\mu + \nu = \mu_* + \nu_* \implies \mu = \mu_* \text{ and } \nu = \nu_*$$

(6.6) Example: (viz. 243)

Let now (I, \leq) be a well-ordered set (i.e. $I \neq \emptyset$ is a non-empty set and \leq is a linear well-orderering on I) and fix any weight $\omega \in \mathbb{N}^{I}$. Then we introduce two different linear orders on the commutative monoid $(\mathbb{N}^{\oplus I}, +)$. Of these the ω -graded lexicographic order will be the standard order we will employ in later sections. Thus consider $\alpha = (\alpha_i)$ and $\beta = (\beta_i) \in \mathbb{N}^{\oplus I}$ and define

• Lexicographic Order

$$\alpha \leq_{\text{lex}} \beta :\iff (\alpha = \beta) \text{ or } (*)$$

$$(*) := \exists k \in I \text{ such that } \alpha_k < \beta_k \text{ and } \forall i < k : \alpha_i = \beta_i$$

It will be proved below, that the lexicographic order \leq_{lex} is positive, i.e. the triple $(\mathbb{N}^{\oplus I}, +, \leq_{\text{lex}})$ is a positively ordered monoid. In the case of $I = 1 \dots n$ we will see that \leq_{lex} even is a well-ordering, i.e. the triple $(\mathbb{N}^n, +, \leq_{\text{lex}})$ is a monomially ordered monoid.

• ω -Graded Lexicographic Order

$$\alpha \leq_{\omega} \beta \quad :\iff \quad (|\alpha|_{\omega} < |\beta|_{\omega}) \text{ or } (|\alpha|_{\omega} = |\beta|_{\omega} \text{ and } \alpha \leq_{\text{lex}} \beta)$$

Analogously to the above the ω -graded lexicographic order \leq_{ω} is positive, i.e. the triple $(\mathbb{N}^{\oplus I}, +, \leq_{\omega})$ is a positively ordered monoid. And in the case $I = 1 \dots n$ it even is a well-ordering, i.e. the triple $(\mathbb{N}^n, +, \leq_{\omega})$ is a monomially ordered monoid once more.

(6.7) Remark: (■)

We wish to append two further linear orders on $(\mathbb{N}^{\oplus I}, +)$. However we will not require these any further and hence abstain from proving any details about them. The interested reader is asked to refer to [Cox, Little, O'Shaea; Using Algebraic Geometry; ???] for more comments on these.

• Reverse Graded Lexicographic Order

 $\alpha \leq_{\text{rgl}} \beta \quad :\iff \quad (\alpha = \beta) \text{ or } (|\alpha| < |\beta|) \text{ or } (|\alpha| = |\beta| \text{ and } (2))$ (2) := $\exists k \in I$ such that $\alpha_k > \beta_k$ and $\forall i < k : \alpha_i = \beta_i$

Just like \leq_{ω} the reverse graded lexicographic order \leq_{rgl} is positive and in the case of $I = 1 \dots n$ it even is a well-ordering again.

• Bayer-Stillman Order

For the fourt order we will require $I = 1 \dots n$ already. Then we fix any $m \in 1 \dots n$ and obtain another monomial order on \mathbb{N}^n

$$\alpha \leq_{\mathrm{bs}(m)} \beta \quad :\iff \quad (3) \text{ or } ((4) \text{ and } \alpha \leq_{\mathrm{gl}} \beta)$$

$$(3) \quad := \quad \alpha_1 + \dots + \alpha_m < \beta_1 + \dots + \beta_m$$

$$(4) \quad := \quad \alpha_1 + \dots + \alpha_m = \beta_1 + \dots + \beta_m$$

6.2 Graded Algebras

(6.8) Definition:

Let (D, +) be a commutative monoid and $(R, +, \cdot)$ be a commutative ring. Then the ordered pair (A, \deg) is said to be a *D*-graded *R*-(semi)algebra, iff it satisfies all of the following properties

- (1) A is a commutative R-(semi)algebra
- (2) deg : hom $(A) \to D$ is a function from some subset hom $(A) \subseteq A$ to D, where we require $0 \notin \text{hom}(A)$. Thereby an element $h \in A$ is said to be **homogeneous**, iff $h \in \text{hom}(A) \cup \{0\}$.
- (3) for any $d \in D$ let us denote $A_d := \deg^{-1}(d) \cup \{0\} \subseteq A$. Then we require that $A_d \leq_{\mathrm{m}} A$ is an *R*-submodule of *A*. And we assume that *A* has a decomposition as an inner direct sum of submodules

$$A = \bigoplus_{d \in D} A_d$$

(4) given any two $c, d \in D$ we require that the product gh of homogeneous elements g of degree c and h of degree d is a homogeneous element of degree c+d. That is letting $A_cA_d := \{gh \mid g \in A_c, h \in A_d\}$ we assume

$$A_c A_d \subseteq A_{c+d}$$

(6.9) Remark:

• By property (2) A_d is a submodule of A, that is the sum g + h of two homogeneous elements of degree d again is a homogeneous element of degree d. And likewise the scalar multiple ah is a homogeneous element of degree d as well. Thus for any $g, h \in \text{hom}(A)$ with deg(g) = deg(h)and any $a \in R$ such that $ag + h \neq 0$ we get

$$\deg(ag+h) = \deg(g) = \deg(h)$$

• Property (4) asserts that the product of homogeneous elements is homogeneous again, in particular $hom(A) \cup \{0\}$ is closed under multiplication. And thereby the degree even is additive, that is for any two homogeneous elements $g, h \in hom(A)$ we get

$$gh \neq 0 \implies \deg(gh) = \deg(g) + \deg(h)$$

• According to (3) any element $f \in A$ has a unique decomposition in terms of homogeneous elements. To be precise, given any $f \in A$, there is a uniquely determined sequence of elements (f_d) (where $d \in D$) such that $f_d \in A_d$ (that is $f_d = 0$ or $\deg(f_d) = d$) the set $\{ d \in D \mid f_d \neq 0 \}$ is finite and

$$f = \sum_{d \in D} f_d$$

Thereby f_d is called the **homogeneous component** of degree d of f. And writing $f = \sum_d f_d$ we will oftenly speak of the decomposition of f into homogeneous components.

• It is insatisfactory to always distinguish the cases h = 0 when considering a homogeneous element $h \in \text{hom}(A) \cup 0 \subseteq A$. Hence we will add a symbol $-\infty$ to D as outlined in (6.3). Then the degree can be extended canonically to all homogeneous elements

$$\deg : \hom(A) \cup \{0\} \to D \cup \{-\infty\} : h \mapsto \begin{cases} \deg(h) & \text{if } h \neq 0 \\ -\infty & \text{if } h = 0 \end{cases}$$

If A is an integral domain this this turns "deg" into a homorphism of semigroups, from $hom(A) \cup \{0\}$ (under the multiplication of A) to D. That is for any $g, h \in hom(A) \cup \{0\}$ we now get

$$\deg(gh) = \deg(g) + \deg(h)$$

• In the literature it is customary to call the decomposition $A = \bigoplus_d A_d$ itself a *D*-graded *R*-algebra, supposed $A_cA_d \subseteq A_{c+d}$. But this clearly is equivalent to the definition we gave here. Just let

$$\hom(A) := \bigcup_{d \in D} A_d \setminus \{0\}$$

Then we obtain a well-defined function deg : $\hom(A) \to D$ by letting deg(h) := d where $d \in D$ is (uniquely) determined by $h \in A_d$. And thereby it is clear that (A, deg) becomes a *D*-graded *R*-algebra, with deg⁻¹ $(d) = A_d \setminus \{0\}$ again.

(6.10) Example:

If $(R, +, \cdot)$ is any commutative ring and (D, +) is any commutative monoid (with neutral element 0). Then there is a trivial construction turning R into a D-graded R-algebra. Just let $hom(R) := R \setminus 0$ and define the degree by deg : $hom(R) \to D : h \mapsto 0$. That is $R_0 = R$, whereas $R_d = 0$ for any $d \neq 0$. Thus examples of graded algebras abound, but of course this construction won't produce any new insight.

(6.11) Remark:

Given some commutative ring $(A, +, \cdot)$ (and a commutative monoid (D, +)) there are two canonical ways how to regard A as an R-algebra

- (1) We could fix R := A, in this case the submodules $A_d \leq_{\mathrm{m}} A$ occuring in property (3) would be ideals $A_d \leq_{\mathrm{i}} A$. So this would yield the quite peculiar property $A_c A_d \subseteq A_{c+d} \cap A_d = \{0\}$ (if $c + d \neq d$).
- (2) Secondly we could fix $R := \mathbb{Z}$, in this case the submodules $A_d \leq_{\mathrm{m}} A$ occuring in property (3) would only have to be subgroups $A_d \leq_{\mathrm{g}} A$. Thus there no longer is a reference to the algebra structure of A. Hence we will also speak of a *D*-graded ring in this case.

(6.12) Example: Rees Algebra (\diamondsuit)

Let $(R, +, \cdot)$ be a commutative ring and $\mathfrak{a} \leq_i R$ be an ideal of R. Note that for any $n \in \mathbb{N}$ the quotient $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ becomes an R/\mathfrak{a} -module under the following, well-defined scalar multiplication $(a + \mathfrak{a})(f + \mathfrak{a}^{n+1}) := af + \mathfrak{a}^{n+1}$. Let us now take to the exterior direct sum of these R/\mathfrak{a} -modules

$$R(\mathfrak{a}) := \bigoplus_{n \in \mathbb{N}} \mathfrak{a}^n / \mathfrak{a}^{n+1}$$

Then $R(\mathfrak{a})$ can be turned into an R/\mathfrak{a} -algebra (the so called *Rees algebra* of R in \mathfrak{a}), by defining the following multiplication

$$(f_n + \mathfrak{a}^{n+1})(g_n + \mathfrak{a}^{n+1}) := \left(\sum_{i+j=n} f_i g_j + \mathfrak{a}^{n+1}\right)$$

Let us denote $R(\mathfrak{a})_n := \mathfrak{a}^n/\mathfrak{a}^{n+1}$ where we consider $R(\mathfrak{a})_n$ as a subset $R(\mathfrak{a})_n \subseteq R(\mathfrak{a})$ canonically (as in (3.19)). Further we define the homogeneous elements of $R(\mathfrak{a})$ to be hom $(R(\mathfrak{a})) := \bigcup_n R(\mathfrak{a})_n \setminus \{0\}$. Then $(R(\mathfrak{a}), \deg)$ becomes an N-graded R/\mathfrak{a} -algebra under the graduation

deg : hom
$$(R(\mathfrak{a})) \to \mathbb{N}$$
 : $f_n + \mathfrak{a}^{n+1} \mapsto n$

(6.13) Definition:

Let (D, +) be a commutative monoid, $(R, +, \cdot)$ be a commutative ring and (A, \deg) be a *D*-graded *R*-algebra. Then a subset $\mathfrak{a} \subseteq A$ is said to be a **graded ideal** of (A, \deg) , iff $\mathfrak{a} \leq_i A$ is an ideal and \mathfrak{a} is decomposed as an inner direct sum of *R*-submodules

$$\mathfrak{a} = \bigoplus_{d \in D} \mathfrak{a} \cap A_d$$

Now suppose (E, +) is another commutative monoid and $(B \deg)$ is an *E*-graded *R*-algebra. Then the ordered pair (φ, ε) is said to be a **homorphism** of **graded algebras** from (A, \deg) to (B, \deg) (or shortly a *graded homorphism*) iff it satisfies

- (1) $\varphi: A \to B$ is a homorphism of *R*-algebras
- (2) $\varepsilon: D \to E$ is a homorphism of monoids
- (3) $\forall h \in \text{hom}(A)$ we get $\deg(\varphi(h)) = \varepsilon(\deg(h))$

(6.14) Remark:

• If (A, \deg) is a *D*-graded *R*-algebra and $\mathfrak{a} \leq_i A$ is a graded ideal of (A, \deg) , then (P, \deg) clearly becomes a *D*-graded *R*-semi-algebra under the graduation inherited from (A, \deg)

$$\begin{array}{rcl} \hom(\mathfrak{a}) & := & \hom(A) \cap \mathfrak{a} \\ \deg & := & \deg\big|_{\hom(\mathfrak{a})} \end{array}$$

If both (A < deg) and (B, deg) are D-graded R-algebras, then a homorphism φ : A → B of R-algebras is said to be graded iff (φ, 1) is a homorphism of graded algebras, that is iff for any h ∈ hom(A) we get

$$\deg(\varphi(h)) = \deg(h)$$

(6.15) Proposition: (viz. 276)

Let (D, +) be a commutative monoid (with neutral element 0), $(R, +, \cdot)$ be a commutative ring and (A, \deg) be a *D*-graded *R*-algebra. Then the following statements are true

- (i) If D is an integral monoid, then $1 \in A_0$
- (ii) If (B, \deg) is another *D*-graded *R*-algebra and $\varphi : A \to B$ is a graded homorphism, then the kernel of φ is a graded ideal in *A*

$$\operatorname{kn}\left(\varphi\right) = \bigoplus_{d \in D} \operatorname{kn}\left(\varphi\right) \cap A_d$$

(iii) If $\mathfrak{a} \leq_i A$ is a graded ideal of (A, \deg) , then the quotient A/\mathfrak{a} becomed a *D*-graded *R*-algebra again under the induced graduation

$$\hom\left(\frac{A}{\mathfrak{a}}\right) := \{h + \mathfrak{a} \mid h \in \hom(A) \setminus \mathfrak{a}\}$$

where $\deg(h + \mathfrak{a}) := \deg(h)$. And thereby the set of homogeneous elements of degree $d \in D$ is precisely given to be the following

$$\left(\frac{A}{\mathfrak{a}}\right)_d = \frac{A_d + \mathfrak{a}}{\mathfrak{a}}$$

(6.16) Definition:

Let $(R, +, \cdot)$ be a commutative ring, $(D, +, \leq)$ be a positively ordered monoid and (A, \deg) be a *D*-graded *R*-algebra. If now $f \in A$ with $f \neq 0$ has the homogeneous decomposition $f = \sum_d f_d$ (where $f_d \in A_d$) then we define

$$deg(f) := \max\{d \in D \mid f_d \neq 0\}$$

ord(f) := min{ $d \in D \mid f_d \neq 0$ }

Note that this is well-defined, as only finitely many f_d are non-zero and \leq is a linear order on D. Thus we have defined two functions on A

deg :
$$A \setminus \{0\} \to D$$

ord : $A \setminus \{0\} \to D$

(6.17) Proposition: (viz. 278)

Let $(R, +, \cdot)$ be a commutative ring, $(D, +, \leq)$ be a positively ordered monoid and (A, \deg) be a D-graded R-algebra. Then we obtain

(i) The newly introduced function deg : $A \setminus \{0\} \to D$ is an extension of the degree original function deg : hom $(A) \to D$. Formally that is

$$h \in A_d, h \neq 0 \implies \deg(h) = d$$

(ii) It is clear that the *order* and *degree* of some homogeneous element $h \in \text{hom}(A)$ will agree. But even the converse is true, that is for any non-zero element $f \in \backslash \{0\}$ we get the equivalency

$$f \in \hom(A) \iff \operatorname{ord}(f) = \deg(f)$$

(iii) For any elements $f, g \in A$ such that $fg \neq 0$ we obtain the estimates

$$\begin{array}{rcl} \operatorname{ord}(f) & \leq & \operatorname{deg}(f) \\ \operatorname{deg}(fg) & \leq & \operatorname{deg}(f) + \operatorname{deg}(g) \\ \operatorname{ord}(fg) & \geq & \operatorname{ord}(f) + \operatorname{ord}(g) \end{array}$$

(iv) And if $(D, +, \leq)$ is a strictly positively ordered monoid and A is an integral domain, then for any $f, g \in A \setminus \{0\}$ we even get the equalities

$$deg(fg) = deg(f) + deg(g)$$

ord(fg) = ord(f) + ord(g)

(v) Thus if $(D, +, \leq)$ is a strictly positively ordered monoid and $A \neq 0$ is a non-zero integral domain again, then the invertible elements of A already are homogeneous

$$A^* \subseteq \hom(A)$$

6.3 Defining Polynomials

6.4 The Standard Cases

6.5 Roots of Polynomials

6.6 Derivation of Polynomials

6.7 Algebraic Properties

6.8 Gröbner Bases

6.9 Algorithms

Chapter 7

Polynomials in One Variable

7.1 Interpolation

7.2 Irreducibility Tests

7.3 Symmetric Polynomials

7.4 The Resultant

7.5 The Discriminant

7.6 Polynomials of Low Degree

7.7 Polynomials of High Degree
7.8 Fundamental Theorem of Algebra

Group Theory

groups, group actions, permutations, sylow theorems, $p\hbox{-}q$ theorem, ordered groups, representation theory

Multilinear Algebra

9.1 Multilinear Maps

9.2 Duality Theory

9.3 Tensor Product of Modules

9.4 Tensor Product of Algebras

9.5 Tensor Product of Maps

9.6 Differentials

Matsumura - commutative ring theory - chapter $9\,$

Categorial Algebra

10.1 Sets and Classes

App: Cantor's definition of sets, App: Russel's antinomy, Rem: formalisation - the language \mathcal{L}_{set} , Def: axiomatisation of set theory (ZFC) and consequences (the foundation axiom, the axiom of choice), Lem: AC \iff Zorn \iff well ordering theorem, Def: Peano's axioms, App: construction of \mathbb{N} , Def: axioms of the arithmetic, Def: construction \mathbb{Z} , Q and R, App: Heuristical definition of classes (2-nd level sets), Exp: the universe of sets, Rem: formalisation - the language \mathcal{L}_{class} , Def: axioms of classes (NBG)

10.2 Categories and Functors

definition of categories,(full) subcategories, small categories, ordinary categories, monomorphisms, epimorphisms, isomorphisms, definition of functors Rem: covariant, contravariant via opposite category, composition of functors, isofunctors, representable functors, Yoneda's lemma, natural equivalence, equivalence of categories

10.3 Examples

categories: Set, Top, Ring, Dom, Mod(R), Loc, C_S, C[•], Bun(•), opposite category, functor category, functors: •/ \mathfrak{a} , U^{-1} •, hom, spec

10.4 Products

definition of (co) products, examples: $\times, \oplus, \otimes,$ fibered product, injective and projective objects, definition of (co) limits

10.5 Abelian Categories

additive categories and their properties, additive functors, examples, kernel, cokernel and their properties, examples, canonical decomposition of morphisms, definition of abelian categories, left/right-exactness, examples: \bullet/\mathfrak{a} , $U^{-1}\bullet$, hom

10.6 Homology

chain (co)
complexes, (co)
homology modules, (co)
homology morphisms, examples $% \left(\left(x,y\right) \right) =\left(x,y\right) \right) =\left(x,y\right) +\left(x,y\right) +\left($

Ring Extensions

basics, transfer of ideals, integral extensions, dimension theory, [Eb, exercise 9.6] gibt Beispiel für ∞ -dimensionalen noetherschen Ring

Galois Theory

Graded Rings

Chapter 14 Valuations

siehe Bourbaki (commutative algebra) VI, mein Skriptum

Part II The Proofs

Proofs - Fundamentals

In this chapter we will finally present the proofs of all the statements (propositions, lemmas, theorems and corollaries) that have been given in the previous part. Note that the order of proofs is different from the order in which we gave the statements, though we have tried to stick to the order of the statements as tightly as possible. So we begin with proving the statements in section 1.1. In this section however we have promised to fill in a gap first: we still have to present a formal notion of applying brackets to a product:

Formal Bracketing (\diamondsuit)

If we multiply (or sum up) several elements $x_1, \ldots, x_n \in G$ of a groupoid (G, \circ) we've got (n - 1) possibilities, with which two elements we start - even if we keep their ordering. And we have to keep choosing until we finally got one element of G. In this light it is quite clear, what we mean by saying "any way of applying parentheses to the product of the x_i results in the same element". It just says, that the result actually doesn't depend on our choices. However - as we do math - we wish to give a formal way of putting this. To do this first define a couple mappings for $2 \le n \in \mathbb{N}$ and $k \in 2 \ldots (n-2)$

$$b_{(n,1)} : G^n \to G^{n-1} : (x_1, \dots, x_n) \mapsto (x_1 x_2, x_3, \dots, x_n)$$

$$b_{(n,k)} : G^n \to G^{n-1} : (x_1, \dots, x_n) \mapsto (x_1, \dots, x_k x_{k+1}, \dots, x_n)$$

$$b_{(n,n-1)} : G^n \to G^{n-1} : (x_1, \dots, x_n) \mapsto (x_1, \dots, n_{n-2}, x_{n-1} x_n)$$

Now we can determine the sequel of choosing the parentheses simply by selecting an (n-1)-tupel k in the following set

$$D_n := \{ k = (k_1, \dots, k_{n-1}) \mid k_i \in 1 \dots (n-i) \text{ for } i \in 1 \dots (n-1) \}$$

For fixed $k \in D_n$ the bracketing (by k) now simply is the following mapping

$$B_k := b_{(2,k_{n-1})} \circ \cdots \circ b_{(n,k_1)} : G^n \to G$$

Proof of 1.2 (associativity): (\diamondsuit)

We now wish to prove the fact that in a groupoid (G, \circ) the product of the elements x_1, \ldots, x_n is independent of the order in which we applied parentheses to it. Formally this can now be put as: for any $k \in D_n$ we get

$$B_k(x_1,\ldots,x_n) = x_1x_2\ldots x_n$$

We will prove this statement by induction on the number n of elements multiplied. In the cases n = 1 and n = 2 there only is one possibility how to apply parentheses and hence the statement is trivial. The case n = 3 there are two possibilities, which are equal due to the associativity law (A) of (G, \circ) . Thus we assume n > 3 and regard two ways of applying parentheses $k, l \in D_n$, writing them in terms of the last multiplication used

$$a := B_k(x_1, \dots, x_n) = B_p(x_1, \dots, x_i)B_p(x_{i+1}, \dots, x_n)$$

$$b := B_l(x_1, \dots, x_n) = B_q(x_1, \dots, x_j)B_q(x_{j+1}, \dots, x_n)$$

where $i := k_1$, $j := l_1$ and $p := (k_2, \ldots, k_{n-1})$, $q := (l_2, \ldots, l_{n-1})$. We may assume $i \leq j$ and if i = j we are already done because of the induction hypothesis. Thus we have i < j and by the induction hypothesis the parentheses may be rearranged to

$$a = \left((x_1 \dots x_i) \left((x_{i+1} \dots x_j) (x_{j+1} \dots x_n) \right) \right)$$
$$b = \left(\left((x_1 \dots x_i) (x_{i+1} \dots x_j) \right) (x_{j+1} \dots x_n) \right)$$

Now the associativity law again implies a = b and as k and l were arbitrary this implies $a = x_1 x_2 \dots x_n$ for any bracketing k chosen.

Proof of (1.5):

• Let (G, \circ) be any group, then ee = e = ee and hence $e = e^{-1}$ by definition of the inverse element. Likewise if $y = x^{-1}$ then xy = e = yx and hence $x = y^{-1}$. Then we prove $(xy)^{-1} = y^{-1}x^{-1}$ by

$$(xy)(y^{-1}x^{-1}) = x\left(y(y^{-1}x^{-1})\right) = x\left((yy^{-1})x^{-1}\right)$$
$$= x\left(ex^{-1}\right) = xx^{-1} = e$$
$$(y^{-1}x^{-1})(xy) = y^{-1}\left(x^{-1}(xy)\right) = y^{-1}\left((x^{-1}x)y\right)$$
$$= y^{-1}\left(ey\right) = y^{-1}y = e$$

• Next we will prove $(x^k)^{-1} = (x^{-1})^k$ by induction on $k \ge 0$. If k = 0 then the claim is satisfied, as $e^{-1} = e$. Now we conduct the induction step, using what we have just proved:

$$(x^{k+1})^{-1} = (x^k x)^{-1} = x^{-1} (x^k)^{-1} = x^{-1} (x^{-1})^k = (x^{-1})^{k+1}$$

• Now assume that xy = yx do commute. Then it is easy to see that $x^{-1}y^{-1} = y^{-1}x^{-1} = (xy)^{-1}$ do commute as well, just compute

$$y^{-1}x^{-1} = (xy)^{-1} = (yx)^{-1} = x^{-1}y^{-1}$$

And by induction on $k \ge 0$ it also is clear, that $x^k y = yx^k$. Now we will prove $(xy)^k = x^k y^k$ by induction on k. In the case k = 0everything is clear $(xy)^0 = e = ee = x^0 y^0$. Now compute

$$(xy)^{k+1} = (xy)^k (xy) = (x^k y^k) (yx)$$
$$= x^k (y^k (yx)) = x^k (y^{k+1}x)$$
$$= x^k (xy^{k+1}) = x^{k+1} y^{k+1}$$

And for negative k we regard -k where $k \ge 0$, then we easily compute

$$(xy)^{-k} = ((xy)^{-1})^k = (x^{-1}y^{-1})^k$$
$$= (x^{-1})^k (y^{-1})^k = x^{-k}y^{-k}$$

• Note: in the last step of the above we have used $(x^{-1})^k = x^{-k}$. But we still have to prove this equality: as for any $x \in G$ we find that $xx^{-1} = e = x^{-1}x$ do commute we also obtain $x^{-k} = (x^k)^{-1} = (x^{-1})^k$ for any $k \ge 0$, just compute

$$x^{-k}x^{k} = (x^{-1})^{k}x^{k} = (x^{-1}x)^{k} = e^{k} = e$$
$$x^{k}x^{-k} = x^{k}(x^{-1})^{k} = (xx^{-1})^{k} = e^{k} = e$$

• This also allows us to prove $(x^k)^l = x^{kl}$ for any $k, l \in \mathbb{Z}$. We will distinguish four cases - to do this assume $k, l \ge 0$ then

$$\begin{pmatrix} x^k \end{pmatrix}^l = x^k x^k \dots x^k \quad (l - \text{times}) = x^{kl}$$

$$\begin{pmatrix} x^{-k} \end{pmatrix}^l = \left((x^{-1})^k \right)^l = \left(x^{-1} \right)^{kl} = x^{-(kl)} = x^{(-k)l}$$

$$\begin{pmatrix} x^k \end{pmatrix}^{-l} = \left((x^k)^{-1} \right)^l = \left((x^{-1})^k \right)^l = x^{-(kl)} = x^{k(-l)}$$

$$\begin{pmatrix} x^{-k} \end{pmatrix}^{-l} = \left(((x^{-1})^k)^{-1} \right)^l = \left(((x^k)^{-1})^{-1} \right)^l = x^{kl} = x^{(-k)(-l)}$$

• It remains to prove $x^k x^l = x^{k+l}$ for any $k, l \in \mathbb{Z}$. As above we will distinguish four cases, that is we regard $k, l \ge 0$. In this case $x^k x^l = x^{k+l}$ is clear by definition. Further we can compute

$$x^{-k}x^{-l} = (x^{-1})^k (x^{-1})^l = (x^{-1})^{k+l} = x^{-(k+l)} = x^{(-k)+(-l)}$$

For the remaining two cases we first show $x^{-1}x^l = x^{l-1}$. In case $l \ge 0$ this is immediately clear. And in case $l \le 0$ we regard -l with $l \ge 0$

$$x^{-1}x^{-l} = x^{-1}(x^{-1})^{l} = (x^{-1})^{l+1} = x^{-(l+1)} = x^{(-l)-1}$$

We are now able to prove $x^{-k}x^l = x^{(-k)+l}$ by induction on k. The case k = 0 is clear, for the induction step we compute

$$x^{-(k+1)}x^{l} = (x^{-1})^{k}x^{-1}x^{l} = (x^{-1})^{k}x^{-1}x^{l} = x^{-k}x^{l-1} = x^{-(k+1)+l}$$

The fourth case finally is $x^k x^{-l} = x^{k+(-l)}$, but as x^k and x^{-l} commute (use inductions on k and l) this readily follows the above.

Proof of (1.6):

The first statement that needs to be verified is that a subgroup $P \leq_{g} G$ truly invekes an equivalence relation $x \sim y \iff y^{-1}x \in P$. This relation clearly is reflexive: $x \sim x$ due to $x^{-1}x = e \in P$. And it also is transitive because if $x \sim y$ and $y \sim z$ then $y^{-1}x \in P$ and $z^{-1}y \in P$. Thereby $z^{-1}x =$ $z^{-1}(yy^{-1})x = (z^{-1}y)(y^{-1}x) \in P$ too, which again means $x \sim z$. Finally it is symmetric as well: if $x \sim y$ then $y^{-1}x \in P$ and hence $x^{-1}y = (y^{-1}x) \in P$ too, which is $y \sim x$. Next we wish to prove that truly [x] = xP

$$\begin{aligned} [x] &= \{ y \in G \mid y \sim x \} &= \{ y \in G \mid x^{-1}y = p \in P \} \\ &= \{ y \in G \mid \exists p \in P : y = xp \} = \{ xp \mid p \in P \} = xP \end{aligned}$$

So it only remains to prove the theorem of Lagrange. To do this we fix a system \mathbb{P} of representants of G/P. That is we fix a subset $\mathbb{P} \subseteq G$ such that $\mathbb{P} \longleftrightarrow G/P : q \mapsto qP$ (which is possible due to the axiom of choice). Then we obtain a bijection by letting

$$G \longleftrightarrow (G/P) \times P : x \mapsto (xP, q^{-1}x \text{ where } xP = qP)$$

This map is well defined: as $xP \in G/P$ there is a uniquely determined $q \in \mathbb{P}$ such that qP = xP. And for this we get $q \sim x$ which means $q^{-1}x \in P$. And it is injective: if xP = yP = qP then $q^{-1}x = q^{-1}y$ yields x = y (by multiplication with q). Finally it also is surjective: given (qP, p) we let $x := qp \in qP$ and thereby obtain $q \sim x$ and hence $(xP, q^{-1}x) = (qP, p)$.

Proof of 1.2 (commutativity): (\diamondsuit)

We want to prove the fact, that in a commutative groupoid, the order of elements in a product can be rearranged arbitarily. That is given a commutative grupoid (G, \circ) , elements $x_1, \ldots, x_n \in G$ and a permutation $\sigma \in S_n$ we have $x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)} = x_1x_2\ldots x_n$. This is a consequence of some basic propositions of group theory. Yet as we do not pursue group theory in this text, we would like to sketch these methods here:

• Let us define the set $S := \{ \sigma^k \mid k \in \mathbb{N} \} \subseteq S_n$. It can be easily proved (by induction on *n*) that $\#S_n = n!$, in particular *S* is a finite set. Thus there have to be $i \neq j \in \mathbb{N}$ such that $\sigma^i = \sigma^j$. Without loss of generality we may assume i < j, then this implies $\sigma^{j-i} = \mathbb{1}$. And thereby we may define

$$d := \min\{1 \le h \in \mathbb{N} \mid \sigma^h = \mathbb{1}\}$$

NOTA for those who are familiar with group theory: S is the subgroup of S_n generated by σ and d is the order of σ , that is d = #S.

• It is clear that $\sigma^{-1} = \sigma^{d-1} \in S$, as $\sigma\sigma^{d-1} = \sigma^d = 1$ and likewise $\sigma^{d-1}\sigma = 1$. Therefore we obtain an equivalence relation on the set $1 \dots n$ by letting

$$a \sim b : \iff \exists k \in \mathbb{N} : \sigma^k(a) = b$$

The reflexivity is clear, by choosing k = 0 and if $\sigma^k(a) = b$ then $a = (\sigma^k)^{-1}(b) = (\sigma^{-1})^k(b) = \sigma^{k(d-1)}(b)$. And as $k(d-1) \in \mathbb{N}$ this is the symmetry of this relation. The transitivity finally follows from: if $b = \sigma^k(b)$ and $c = \sigma^l(b)$ then $c = \sigma^k \sigma^l(a) = \sigma^{k+l}(a)$. By construction it is clear, that the equivalence class of $a \in 1 \dots n$ is given to be

$$Sa := [a] = \left\{ \sigma^k(a) \mid k \in \mathbb{N} \right\}$$

NOTA for those who are familiar with group theory: we have an action of the group S on $1 \dots n$ by $\sigma a := \sigma(a)$. And the equivalence class Sa is just the orbit of a under S.

- As $Sa \subseteq 1 \dots n$ we see that Sa is a finite set d(a) := #Sa. Thereby $\{a, \sigma(a), \dots, \sigma^{d(a)-1}(a)\} \subseteq Sa$ is as subset with d(a) elements and hence these sets even are equal. In particular we find $\sigma^{d(a)}(a) = a$.
- We now choose a representing system A ⊆ 1...n of 1...n / ~, that is we choose A in such a way that there is a one-to-one correspondence A ↔ (1...n / ~) : a ↦ Sa. And for any a ∈ A we define the following permutation

$$\zeta_a : 1 \dots n \longleftrightarrow 1 \dots n : x \mapsto \begin{cases} \sigma(x) & \text{if } x \in Sa \\ x & \text{if } x \notin Sa \end{cases}$$

If $a \neq b \in S$ then $Sa \cap Sb = \emptyset$ are disjoint and hence we get $\zeta_a \zeta_b = \zeta_b \zeta_a$ do commute. And thereby it is easy to see, that σ is given to be the product (in S_n , i.e. under composition of mappings as an operation)

$$\sigma = \prod_{a \in A} \zeta_a$$

• For any $a, b \in 1 \dots n$ let us now denote the transposition of a and b

$$(a b) : 1 \dots n \longleftrightarrow 1 \dots n : x \mapsto \begin{cases} a & \text{if } x = b \\ b & \text{if } x = a \\ x & \text{if } x \notin \{a, b\} \end{cases}$$

It is clear that $(a \ a) = 1$ and $(a \ b) = (b \ a)$. Thus we may assume a < b without loss of generality. In this case one immediately verifies

$$(a b) = (b b - 1)(b - 1 b - 2) \dots (a + 1 a)$$

• Again it is easy to see, that the cycle $\zeta_a = (a \ \sigma(a) \dots \ \sigma^{d(a)-1}(a))$ can be expressed as the following product of transpositions

$$\zeta_a = \left(a \ \sigma^{d(a)-1}(a)\right) \left(a \ \sigma^{d(a)-2}(a)\right) \dots \left(a \ \sigma(a)\right)$$

• Altogether σ can be expressed as a product of cycles, which can be expressed as a product of transpositions, which can be expressed as a product of adjacent transpositions. That is $\sigma = \tau_1 \dots \tau_r$ where $\tau_i = (a_i \ a_i + 1)$ is an adjacent transposition. By the commutativity rule of G adjacent permutations do not change the product of the elements and hence we finally obtain the claim

$$\prod_{a=1}^{n} x_{a} = \prod_{a=1}^{n} x_{\tau_{r}(a)}$$

$$= \prod_{a=1}^{n} x_{\tau_{r-1}\tau_{r}(a)}$$

$$= \text{ inductively}$$

$$= \prod_{a=1}^{n} x_{\tau_{1}...\tau_{r-1}\tau_{r}(a)}$$

$$= \prod_{a=1}^{n} x_{\sigma(a)}$$

Proof of (6.5):

(i) Recall the definition of the *minimum* and *maximum* of any two elements $\alpha, \beta \in A$ (this is truly well-defined, since \leq is a linear order)

$$\alpha \wedge \beta := \begin{cases} \alpha & \text{if } \alpha \leq \beta \\ \beta & \text{if } \beta \leq \alpha \end{cases} \qquad \alpha \vee \beta := \begin{cases} \beta & \text{if } \alpha \leq \alpha \\ \beta & \text{if } \beta \leq \alpha \end{cases}$$

In the case that $M = \{\mu\}$ contains one element only, we clearly get the minimal and maximal elements $\mu_* = \mu = \mu^*$. If now M is given to be $M = \{\mu_1, \ldots, \mu_n\}$ where $n \ge 2$ then we regard

$$\mu_* := (\dots (\mu_1 \land \mu_2) \dots) \land \mu_n$$

$$\mu^* := (\dots (\mu_1 \lor \mu_2) \dots) \lor \mu_n$$

Then μ_* and μ^* are minimal, resp. maximal elements of M, which can be seen by induction on n: if n = 2 then μ_* is minimal by construction. Thus for $n \ge 3$ we let $H := \{\mu_1, \ldots, \mu_{n-1}\} \subseteq M$. By induction hypothesis we have $H_* = \{\nu_*\}$ for $\nu^* = ((\mu_1 \land \mu_2) \ldots) \land \mu_{n-1}$. Now let $\mu_* := \nu_* \land \mu_n$ then $\mu_* \le \nu_* \le \mu_i$ for i < n and $\mu_* \le \mu_n$ by construction. Hence we have $\mu_* \le \mu_i$ for any $i \in 1 \ldots n$, which means $\mu_* \in M_*$. And the uniqueness is obvious by the anti-symmetry of \le . And this also proves the the claim for the maximal element μ^* , by taking to the inverse order $\alpha \ge \beta :\iff \beta \le \alpha$.

- (ii) The existence of μ_* is precisely the property of a well-ordering. The uniqueness is immediate from the anti-symmetry of \leq again: suppose μ_1 and μ_2 both are minimal elements of M, in particular $\mu_1 \leq \mu_2$ and $\mu_2 \leq \mu_1$. Ant this implies $\mu_1 = \mu_2$, as \leq is a (linear) order on A.
- (iii) In the direction (a) \implies (b) we consider $\alpha < \beta$. By the positivity of \leq this implies $\alpha + \gamma \leq \beta + \gamma$. If the equality $\alpha + \gamma = \beta + \gamma$ would hold true then as A is integral we would find $\alpha = \beta$ in contradiction to the assumption $\alpha < \beta$. In the converse direction (b) \implies (a) we are given $\alpha \leq \beta$. The positivity $\alpha + \gamma \leq \beta + \gamma$ (for any $\gamma \in A$) of \leq is clear in this case. Now asume $\alpha + \gamma = \beta + \gamma$ then we need to show $\alpha = \beta$ to see that A is integral. But as \leq is total we have $\alpha \leq \beta$ or $\beta \leq \alpha$, where we may assume $\alpha \leq \beta$ without loss of generality. If we now had $\alpha \neq \beta$ then $\alpha < \beta$ and hence $\alpha + \gamma < \beta + \gamma$ in contradiction to $\alpha + \gamma = \beta + \gamma$, which rests this case, too. Now (c) \implies (b) is trivial such that there only remains the direction (b) \implies (c). But this is clear assume $\alpha + \gamma < \beta + \gamma$ but $\alpha \geq \beta$, then by the positivity (a) we would get the contradiction: $\alpha + \gamma \geq \beta + \gamma$.
- (iv) Assume $\mu \neq \mu_*$, then by the minimality of μ_* this would yield $\mu_* < \mu$ and hence (by property (b) in point (iv) above)

$$\mu + \nu \ = \ \mu_* + \nu_* \ < \ \mu + \nu_*$$

Thus we see that $\nu \neq \nu_*$ and hence (by the minimality of ν_*) we get $\nu_* < \nu$ again. Using (b) once more this yields a contradiction

$$\mu+\nu \ < \ \mu+\nu_* \ < \ \mu+\nu$$

Thus we have seen $\mu = \mu_*$ but in complete analogy we find that $\nu \neq \nu_*$ leads to another contradiction and hence $\nu = \nu_*$.

Proof of (6.6):

• In the following we will regard arbitrary elements $\alpha = (\alpha_i), \beta = (\beta_i)$ and $\gamma = (\gamma_i) \in A := \mathbb{N}^{\oplus I}$. In a first step we will show that - assuming (I, \leq) is a linearly ordered set - the lexicographic order is a positive partial order on A. The *reflexivity* $\alpha \leq_{\text{lex}} \alpha$ is trivial, however, and for the *transitivity* we are given $\alpha \leq_{\text{lex}} \beta$ and $\beta \leq_{\text{lex}} \gamma$ and need to show $\alpha \leq_{\text{lex}} \gamma$. The case where two (or more) of α, β and γ are equal is trivial and hence the assumption reads as

$$\begin{aligned} \alpha_k < \beta_k & \text{and} & \forall i < k : \alpha_i = \beta_i \\ \beta_l < \gamma_l & \text{and} & \forall i < l : \beta_i = \gamma_i \end{aligned}$$

for some $k, l \in I$. We now let $m := \min\{k, l\}$ then it is easy to see, that $\forall i < m : \alpha_i = \beta_i = \gamma_i$ and $\alpha_m < \gamma_m$ which establishes $\alpha \leq_{\text{lex}} \gamma$. It remains to prove the *anti-symmetry*, i.e. we are given $\alpha \leq_{\text{lex}} \beta$ and $\beta \leq_{\text{lex}} \alpha$ and need to show $\alpha = \beta$. Suppose we had $\alpha \neq \beta$ then again

$$\alpha_k < \beta_k$$
 and $\forall i < k : \alpha_i = \beta_i$
 $\beta_l < \alpha_l$ and $\forall i < l : \beta_i = \alpha_i$

In the case $k \leq l$ this implies $\alpha_k < \beta_k = \alpha_k$ and in the case $l \leq k$ we get $\beta_l < \alpha_l = \beta_l$. In both cases this is a contradiction. Hence \leq_{lex} is a partial order, but the *positivety* is easy. Assume $\alpha \leq_{\text{lex}} \beta$, then we need to show $\alpha + \gamma \leq_{\text{lex}} \beta + \gamma$. If even $\alpha = \beta$, then there is nothing to prove. Hence we may assume, that there is some $k \in I$ such that

$$\alpha_k < \beta_k$$
 and $\forall i < k : \alpha_i = \beta_i$

But then $\alpha + \gamma \leq_{\text{lex}} \beta + \gamma$ is clear, as from this we immeditately get

$$\alpha_k + \gamma_k < \beta_k + \gamma_k$$
 and $\forall i < k : \alpha_i + \gamma_i = \beta_i + \gamma_i$

• In a second step we will show that - assuming (I, \leq) is a well-ordered set - the lexicographic order truly is a positive linear order on A. By the first step it only remains to verify that \leq_{lex} is *total*, i.e. we assume

that $\beta \leq_{\text{lex}} \alpha$ is untrue and need to show $\alpha \leq_{\text{lex}} \beta$. By assumption we now have for any $k \in I$

$$\beta_k \ge \alpha_k \quad \text{or} \quad \exists i < k : \alpha_i \neq \beta_i$$

It is clear that $\alpha \neq \beta$ and as (I, \leq) is well-ordered we may choose

 $k := \min\{l \in I \mid \alpha_l \neq \beta_l\}$

Then $\forall i < k$ we get $\alpha_i = \beta_i$ (as k was chosen minimally) and $\beta_k \ge \alpha_k$ (by assumption). Yet $\beta_k = \alpha_k$ is false by construction which only leaves $\beta_k > \alpha_k$ and hence establishes $\alpha \le_{\text{lex}} \beta$.

• In the third step we assume that I is finite, i.e. $I = 1 \dots n$ without loss of generality. Note that I clearly is well-ordered under its standard ordering and hence it only remains to prove the following assertion: let $\emptyset \neq M \subseteq A$ be a non-empty subset, then there is some $\mu \in M$ such that for any $\alpha \in M$ we get $\mu \leq_{\text{lex}} \alpha$. To do this we define

$$\mu_{1} := \min\{\alpha_{1} \in \mathbb{N} \mid \alpha \in M\}$$

$$\mu_{2} := \min\{\alpha_{2} \in \mathbb{N} \mid \alpha \in M, \alpha_{1} = \mu_{1}\}$$

$$\dots \qquad \dots$$

$$\mu_{n} := \min\{\alpha_{n} \in \mathbb{N} \mid \alpha \in M, \alpha_{1} = \mu_{1}, \dots, \alpha_{n-1} = \mu_{n-1}\}$$

Hereby the set $\{ \alpha_1 \mid \alpha \in M \}$ is non-empty, since $M \neq \emptyset$ was assumed to be non-empty. And $\{ \alpha_2 \mid \alpha \in M, \alpha_1 = \mu_1 \}$ is non-empty, as there was some $\alpha \in M$ with $\alpha_1 = \mu_1$ and so forth. Hence μ is well defined and it is clear that $\mu \in M$, as $\mu = \alpha$ for some $\alpha \in M$. But the property $\mu \leq_{\text{lex}} \alpha$ is then clear from the construction.

• Now we will proof, that - assuming (I, \leq) is a linearly ordered set the ω -graded lexicographic order is a positive partial order as well. It is clear that $\leq \omega$ inherits the porperty of being a partial order from \leq_{lex} so it only remains to verify the positivity: let $\alpha \leq_{\omega} \beta$, then we distinguish two cases. In the case $|\alpha|_{\omega} < |\beta|_{\omega}$ we clearly get

$$|\alpha + \gamma|_{\omega} = |\alpha|_{\omega} + |\gamma|_{\omega} < |\beta|_{\omega} + |\gamma|_{\omega} = |\beta + \gamma|_{\omega}$$

If on the other hand $|\alpha|_{\omega} = |\beta|_{\omega}$ then by assumption $\alpha \leq_{\text{lex}} \beta$ and as we have seen already this implies $\alpha + \gamma \leq_{\text{lex}} \beta + \gamma$. Thus in both cases we have found $\alpha + \gamma \leq_{\omega} \beta + \gamma$.

• We now assume that (I, \leq) even is a well-ordered set and prove that \leq_{ω} is a total order in this case. Hence we need to regard the case that $\beta \leq_{\omega} \alpha$ is untrue. Of course this implies $|\alpha|_{\omega} \leq |\beta|_{\omega}$ and in the case $|\alpha|_{\omega} < |\beta|_{\omega}$ we are done already. Thus we may assume $|\alpha|_{\omega} = |\beta|_{\omega}$, but in this case the assumption reads as: $\neg \beta \leq_{\text{lex}} \alpha$. As we have seen above the lexicographic order is total and hence $\alpha <_{\text{lex}} \beta$ which conversely implies $\alpha <_{\omega} \beta$.

• In the final step we assume that I is finic, i.e. $I = 1 \dots n$ and we need to show that \leq_{ω} is a well-ordering. Thus let $\emptyset \neq M \subseteq A$ be a nonempty subset again, then we have to verify that there is some $\mu \in M$ such that for any $\alpha \in M$ we get $\mu <_{\omega} \alpha$. To do this we define

$$\begin{split} m &:= & \min\{ \, |\alpha|_{\omega} \mid \alpha \in M \, \} \\ \mu &:= & \min\{ \, \alpha \mid \alpha \in M, \ |\alpha|_{\omega} = m \, \} \end{split}$$

where the second minimum is taken under the lexicographic order. As M is non-empty m is well-defined and as \leq_{lex} has been shown to be a well-ordering μ is well-defined, too. But $\mu \in M$ is trivial and $\mu \leq_{\omega} \alpha$ is clear from the construction.

Proofs - Rings and Modules

Proof of (1.21):

- The statement 0 = -0 is clear from 0 + 0 = 0. And a0 = 0 follows from a0 = a(0+0) = a0 + a0. Likewise we get 0a = 0. And from this an easy computation shows (-a)b = -(ab), this computation reads as ab + (-a)b = (a + (-a))b = 0b = 0 (and a(-b) = -(ab) follows analogously). Combining these two we find (-a)(-b) = ab, since ab = -(-ab) = -((-a)b) = (-a)(-b).
- Next we will prove the general rule of distributivity: we start by showing that $(a_1 + \cdots + a_m)b = (a_1b) + \cdots + (a_mb)$ by induction on m. The case m = 1 is clear and in the induction step we simply compute

$$\left(a_{1} + \dots + a_{m} + a_{m+1}\right)b = \left((a_{1} + \dots + a_{m}) + a_{m+1}\right)b$$
$$= \left(\sum_{i=1}^{m} a_{i}\right)b + a_{m+1}b = \left(\sum_{i=1}^{m} a_{i}b\right) + a_{m+1}b = \sum_{i=1}^{m+1} a_{i}b$$

Likewise it is clear, that $a(b_1 + \cdots + b_n) = (ab_1) + \cdots + (ab_n)$. And combining these two equations we find the generale rule

$$\left(\sum_{i=1}^{m} a_i\right) \left(\sum_{j=1}^{n} b_j\right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_i\right) b_j$$
$$= \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_i b_j\right)$$
$$= \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$$

• Using induction on n we will now prove the generalisation of the general law of distributivity. The case n = 1 is trivial (here J = J(1) so there is nothing to prove). Thus consider the induction step by adding J(0) to our list $J(1), \ldots, J(n)$ of index sets. Then clearly

$$\prod_{i=0}^{n} \sum_{j_i \in J(i)} a(i, j_i) = \left(\sum_{j_0 \in J(0)} a(0, j_0) \right) \left(\prod_{i=1}^{n} \sum_{j_i \in J(i)} a(i, j_i) \right)$$

Hence we may use the induction hypothesis in the second term on the right hand side and the general law of distributivity (note that we use $J = J(1) \times \cdots \times J(n)$) again) to obtain

$$\prod_{i=0}^{n} \sum_{j_i \in J(i)} a(i, j_i) = \left(\sum_{j_0 \in J(0)} a(0, j_0) \right) \left(\sum_{j \in J} \prod_{i=1}^{n} a_{i, j_i} \right)$$

$$= \sum_{j_0 \in J(0)} \sum_{j \in J} a(0, j_0) \prod_{i=1}^{n} a(i, j_i)$$

To finish the induction step it suffices to note that the product of $a(0, j_0)$ with $\prod_{i=1}^n a(i, j_i)$ can be rewritten $\prod_{i=0}^n a(i, j_i)$ (due to the associativity of the multiplication). And the two sums over $j(0) \in J(0)$ resp. over $j \in J$ can be composed to a single sum over $(j_0, j) \in J(0) \times J$. Thas is we have obtained the claim

$$\prod_{i=0}^{n} \sum_{j_i \in J(i)} a(i, j_i) = \sum_{(j_0, j) \in J(0) \times J} \prod_{i=0}^{n} a(i, j_i)$$

• Thus we have arrived at the binomial rule, which will be proved by induction on n. In the case n = 0 we have $(a+b)^0 = 1 = 1 \cdot 1 = a^0 b^{0-0}$.

Thus we commence with the induction step

$$\begin{aligned} (a+b)^{n+1} &= (a+b)^n (a+b) \\ &= \left(\sum_{k=0}^n \binom{n}{k} a^k b^{n-k}\right) (a+b) \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{(n+1)-k} \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{(n+1)-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{(n+1)-k} \\ &= \binom{n}{n} a^{n+1} b^0 + \sum_{k=1}^n \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{(n+1)-k} + \binom{n}{0} a^0 b^{n+1} \\ &= \binom{n+1}{0} a^0 b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{(n+1)-k} + \binom{n+1}{n+1} a^{n+1} b^0 \\ &= \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k} \end{aligned}$$

• It remains to verify the polynomial rule, which will be done by induction on k. The case k = 1 is clear again, and the case k = 2 is the ordinary binomial rule. Thus consider the induction step

$$\begin{pmatrix} a_{1} + \dots + a_{k} + a_{k+1} \end{pmatrix}^{n}$$

$$= \left(a_{k+1} + (a_{1} + \dots + a_{k}) \right)^{n}$$

$$= \sum_{\alpha_{k+1}=0}^{n} \binom{n}{\alpha_{k+1}} a_{k+1}^{\alpha_{k+1}} (a_{1} + \dots + a_{k})^{n-\alpha_{k+1}}$$

$$= \sum_{\alpha_{k+1}=0}^{n} \binom{n}{\alpha_{k+1}} a_{k+1}^{\alpha_{k+1}} \left(\sum_{|\alpha|=n-\alpha_{k+1}} \binom{n-\alpha_{k+1}}{\alpha} a^{\alpha} \right)$$

$$= \sum_{\alpha_{k+1}=0}^{n} \sum_{|\alpha|=n-\alpha_{k+1}} \binom{n}{\alpha_{k+1}} \binom{n-\alpha_{k+1}}{\alpha} a^{\alpha} a_{k+1}^{\alpha_{k+1}}$$

$$= \sum_{|(\alpha,\alpha_{k+1})|=n} \binom{n}{(\alpha,\alpha_{k+1})} (a,a_{k+1})^{(\alpha,\alpha_{k+1})}$$

Proof of (1.26):

- The equality of sets NZD $R = R \setminus ZD R$ is immediately clear from the definition: the negation of the formula $\exists b \in R : (b \neq 0) \land (ab = 0)$ is just $\forall b \in R : ab = 0 \implies b = 0$.
- If $a \in \text{NIL } R$ then we choose $k \in \mathbb{N}$ minimal such that $a^k = 0$. Suppose k = 0, then $0 = a^0 = 1$ which would mean that R = 0 has been the zero-ring. Thus we have $k \ge 1$ and may hence define $b := a^{k-1} \ne 0$. Then $ab = a^k = 0$ and hence $a \in \text{ZD } R$, which proves $\text{NIL } R \subseteq \text{ZD } R$. And if ab = 0, then $a \in R^{ast}$ would imply $b = a^{-1}0 = 0$. Thus if $a \in \text{ZD } R$ then $a \notin R^*$ which also proves $\text{ZD } R \subseteq R \setminus R^*$.
- It is clear that $1 \in NZD R$, as 1b = b. Now suppose a and $b \in NZD R$ and consider any $c \in R$. If (ab)c = 0 then (because of the associativity a(bc) = 0 and as $a \in NZD R$ this implies bc = 0. As $b \in NZD R$ this now implies c = 0 which means $ab \in NZD R$.
- It is clear that $1 \in R^*$ just choose b = 1. Now the associativity and existence of a neutral element e = 1 is immediately inherited from (the multiplication) of R. Thus consider $a \in R^*$, by definition there is some $b \in R$ such that ab = 1 = ba. Hence we also have $b \in R^*$ and thereby b is the inverse element of a in R^* .
- " \Leftarrow " first suppose $0 = 1 \in R$ then we would have R = 0 and hence $R \setminus \{0\} = \emptyset$ and $R^* = R \neq \emptyset$, in contradiction to the assumption $R^* = R \setminus \{0\}$. Thus we get $0 \neq 0$. If now $0 \neq a \in R$ then $a \in R^*$ by assumption and hence there is some $b \in R$ such that ab = 1 = ba. But this also is porperty (F) of skew-fields. " \Longrightarrow " if $0 \neq a \in R$ then as R is a skew field there is some $b \in R$ such that ab = 1 = ba. But this already is $a \in R^*$ and hence $R \setminus \{0\} \subseteq R^*$. Conversely consider $a \in R^*$, that is ab = 1 = ba for some $b \in R$. Suppose a = 0, then $1 = ab = 0 \cdot b = 0$ and hence 0 = 1, a contradiction. Thus $a \neq 0$ and this also proves $R^* \subseteq R \setminus \{0\}$.
- Consider a and $b \in \text{NIL } R$ such that $a^k = 0$ and $b^l = 0$. Then we will prove $a + b \in \text{NIL } R$ by demonstrating $(a + b)^{k+l} = 0$, via

$$(a+b)^{k+l} = \sum_{i=0}^{k+l} \binom{k+l}{i} a^i b^{k+l-i}$$

$$= \sum_{i=0}^k \binom{k+l}{i} a^i b^{l+(k-i)} + \sum_{j=1}^l \binom{k+l}{k+j} a^{k+j} b^{l-j}$$

$$= b^l \sum_{i=0}^k \binom{k+l}{i} a^i b^{k-i} + a^k \sum_{j=1}^l \binom{k+l}{k+j} a^j b^{l-j}$$

$$= 0+0 = 0$$

And if $c \in R$ is an arbitrary element, then also $(ca)^k = c^k a^k = c^k 0 = 0$ such that $ca \in \text{NIL } R$. As a has been chosen arbitrarily, this implies $R(\text{NIL } R) \subseteq R$ and hence $\text{NIL } R \leq_i R$ is an ideal.

- Consider x and $y \in ANN(R, b)$. Then it is clear that (x+y)b = xb+yb = 0 + 0 = 0 and hence $x + y \in ANN(R, b)$. And if $a \in R$ is arbitrary then (ax)b = a(bx) = a0 = 0 such that $ax \in ANN(R, b)$. In particular $-x = (-1)x \in ANN(R, b)$ and hence ANN(R, b) is a submodule of R.
- Let $u \in R^*$ and $a \in R$ with $a^n = 0$, then we can verify the formula for the inverse of u + a in straightforward computation (see below). And in particular we found $u + a \in R^*$. But as a has been an arbitrary nilpotent, this has truly been $u + \text{NIL } R \subseteq R^*$.

$$(a+u)\sum_{k=0}^{n-1} (-1)^k a^k u^{-k-1}$$

$$= \sum_{k=0}^{n-1} (-1)^k a^{k+1} u^{-(k+1)} + \sum_{k=0}^{n-1} (-1)^k a^k u^{-k}$$

$$= \sum_{k=1}^n (-1)^{k-1} a^k u^{-k} \sum_{k=0}^{n-1} (-1)^k a^k u^{n-(k-1)}$$

$$= (-1)^{n-1} a^n u^{-n} + (-1)^0 a^0 u^{-0} = 1$$

Proof of (1.24):

We now prove of the equivalencies for integral rings: for (a) \implies (b') we are given a, b and $c \in R$ with $a \neq 0$ and ba = ca. Then we get (c - b)a = 0 which is $c - b \in \text{ZD } R$. By assumption (a) this implies c - b = 0 and hence b = c. Now the implication (b') \implies (c') is trivial, just let c = 1. And for the final step (c') \implies (a) we consider $0 \neq b \in R$ such that ab = 0. Then (a + 1)b = ab + b = b such that by assumption (c') we get a + 1 = 1 and hence a = 0. Thereby we have obtained $\text{ZD } R \subseteq \{0\}$ and the converse inclusion is clear.

Next we consider (a) \implies (b), again we are given a, b and $c \in R$ with $a \neq 0$ and ab = ac. This yields a(c - b) = 0 and as $a \neq 0$ we have $a \notin ZDR$ such that $a \in NZDR$. Hence c - b = 0 which is b = c. The implication (b) \implies (c) is clear again, just let c = 1. And for (c) \implies (a) we consider $0 \neq a \in R$ such that ab = 0. Then a(b+1) = ab + a = a. By assumption (c) this implies b + 1 = 1 and hence b = 0. Therefore $R \setminus \{0\} \subseteq NZDR$ which is $R \setminus \{0\} = NZDR$ and hence $ZDR = \{0\}$.

Proof of (1.30):

- $(\star = \text{semi-ring})$ as any P_i is a sub-semiring we have $0 \in P_i$ and hence $0 \in \bigcap_i P_i$ again. Now consider $a, b \in \bigcap_i P_i$ that is $a, b \in P_i$ for any $i \in I$. As any P_i is a sub-semiring this implies that a + b, ab and $-a \in P_i$ (for any $i \in I$). And thereby a + b, ab and $-a \in \bigcap_i P_i$ again.
- $(\star = \text{ ring})$ in complete analogy we have $1 \in P_i$ (for any $i \in I$, as any P_i has been assumed to be a subring. Hence we also get $1 \in \bigcap_i P_i$.
- $(\star = (\text{skew})\text{field}) \text{ consider } 0 \neq a \in \bigcap_i P_i$. That is $a \in P_i$ for any $i \in I$ and as any P_i is a subfield we get $a^{-1} \in P_i$ such that $a^{-1} \in \bigcap_i P_i$.
- $(\star = (\text{left})\text{ideal})$ consider any $b \in R$ and $a \in \bigcap_i P_i$ that is $a \in P_i$ for any $i \in I$. As P_i is a left-ideal we find $ba_i \in P_i$ again and hence $ba \in \bigcap_i P_i$. In the case of ideals P_i we analogously find $ab \in \bigcap_i P_i$.
- Note that thereby the generation of * is well-defined the set of all *s containing X is nonempty, as R itself is a * (e.g. R is an ideal of R). And by the lemma we have just proved, the intersection is a * again.

Proof of (3.9):

- First suppose M is an R-module and $P_i \leq_{\mathrm{m}} M$ are R-submodules and let $P := \bigcap_i P_i \subseteq M$. In particular we get $0 \in P_i$ for any $i \in I$ and hence $0 \in P$. And if we are given any $x, y \in P$ this means $x, y \in P_i$ for any $i \in I$. And as any $P_i \leq_{\mathrm{m}} M$ is an R-submodule this implies $x + y \in P_i$ which is $x + y \in P$ again, as i has been arbitary. Likewise consider any $a \in R$, then $ax_i \in P_i$ again and hence $ax \in P$. Altogether $P \leq_{\mathrm{m}} M$ is an R-submodule of M.
- Now suppose M is an R-semi-algebra and $P_i \leq_b A$ are R-sub-semialgebras and let $P := \bigcap_i P_i \subseteq M$ again. In particular $P_i \leq_m M$ and, as we have already seen, this implies $P \leq_m M$. Thus consider any $f, g \in P$ that is $f, g \in P_i$ for any $i \in I$. As any P_i is an R-subsemi-algebra we get $fg \in P_i$ again and hence $fg \in P$, as i has been arbitary. Thus P is an R-sub-semi-algebra again.
- Next suppose M is an R-algebra with unit element 1, $P_i \leq_a M$ are R-subalgebras and let $P := \bigcap P_i$ once more. Then we have just seen that $P \leq_b M$ again. But as $P_i \leq_a M$ we have $1 \in P_i$ again. And as this is true for any $i \in I$ this implies $1 \in P$, such that $P \leq_a M$.
- Finally consider the *R*-semialgebra *A* and the *R*-algebra-ideals $\mathfrak{a}_i \trianglelefteq_a A$ and let $\mathfrak{a} := \bigcap_i \mathfrak{a}_i \subseteq A$. As our first claim we have already shown

 $\mathfrak{a} \leq_{\mathrm{m}} A$, thus consider any $f \in \mathfrak{a}$ and any $g \in M$. Then we have $f \in \mathfrak{a}_i$ for any $i \in I$ and as this is an *R*-sub-semialgebra this implies fg and $gf \in \mathfrak{a}_i$ again. And as i is arbitrary this finally is fg and $gf \in \mathfrak{a}$ such that $\mathfrak{a} \leq_{\mathrm{a}} A$, again.

Proof of (1.33):

- Let us denote the set $\mathfrak{a} := \{\sum_i a_i x_i\}$ of which we claim $\mathfrak{a} = \langle X \rangle_{\mathrm{m}}$. First of all it is clear that $X \subseteq \mathfrak{a}$, as $x = 1x \in \mathfrak{a}$ for any $x \in X$. Further it is clear that $\mathfrak{a} \leq_{\mathrm{m}} R$ is a left-ideal of R: choose any $x \in X$, then $0 = 0 \cdot x \in \mathfrak{a}$, and if $b \in R$, $x = a_1 x_1 + \cdots + a_m x_m$ and $y = b_1 y_1 + \cdots + b_n y_n \in \mathfrak{a}$ then $bx = (ba_1)x_1 + \cdots + (ba_m)x_m \in \mathfrak{a}$ and $x + y = a_1 x_1 + \cdots + a_m x_m + b_1 y_1 + \cdots + b_n y_n \in \mathfrak{a}$. Thus by definition of $\langle X \rangle_{\mathrm{m}}$ we get $\langle X \rangle_{\mathrm{m}} \subseteq \mathfrak{a}$. Now suppose $\mathfrak{b} \leq_{\mathrm{m}} R$ is any left-ideal of R containing $X \subseteq \mathfrak{b}$, Then for any $a_i \in R$ and any $x_i \in X \subseteq \mathfrak{b}$ we get $a_i x_i \in \mathfrak{b}$ and hence $\sum_i a_i x_i \in \mathfrak{b}$, too. That is $\mathfrak{a} \subseteq \mathfrak{b}$, and as \mathfrak{b} has been arbitary this means $\mathfrak{a} \subseteq \langle X \rangle_{\mathrm{m}}$, by the definition of $\langle X \rangle_{\mathrm{m}}$.
- Denote the set $P := \{\sum_i \prod_j x_{i,j}\}$ of which we claim $P = \langle X \rangle_s$ again. Trivially we have $X \subseteq P$ and further it is clear that $P \leq_s R$ is a sub-semialgebra of R: choose any $x \in X$, then $0 = 0 \cdot x \in P$, and if $a = \sum_i \prod_j x_{i,j}$ and $b = \sum_k \prod_l y_{k,l}$, then $-a = \sum_i (-x_{i,1}) \prod_{j \geq 2} x_{i,j} \in$ $P, a + b = \sum_i \prod_j x_{i,j} + \sum_k \prod_l y_{k,l} \in P$ and by general distributivity also $ab = \sum_i \sum_j (\prod_j x_{i,j} \prod_l y_{k,l}) \in P$. Thus by definition of $\langle X \rangle_s$ we get $\langle X \rangle_s \subseteq P$. Now suppose $Q \leq_s R$ is any sub-semi-ring of R. Then for any and any $x \in X \subseteq Q$ we also get $-x \in Q$ and hence $\pm X \subseteq Q$. Now consider any $x_{i,j} \in \pm X \subseteq Q$ then $\prod_j x_{i,j} \in Q$ and hence $\prod_j x_{i,j} \in Q$. That is $P \subseteq Q$, and as Q has been arbitary, this means $P \subseteq \langle X \rangle_s$, by definition of $\langle X \rangle_s$.
- By construction $P := \langle X \cup \{1\} \rangle_s$ is a sub-semiring containing 1, in other words a subring. And as $X \subseteq P$ this implies $\langle X \rangle_r \subseteq P$. And as any subring $Q \leq_r R$ contains 1 we get $X \subseteq Q \implies X \cup \{1\} \subseteq$ $Q \implies P \subseteq Q$. This also proves $\langle X \rangle_r \subseteq P$, as Q has been arbitrary.
- Now suppose R is a field, and let $P := \{ab^{-1} \mid a, b \in \langle X \rangle_{\mathbf{r}}, b \neq 0\}$. First of all $0 = 0 \cdot 1^{-1}$ and $1 = 1 \cdot 1^{-1} \in P$. And if ab^{-1} and $cd^{-1} \in P$, then we get $(ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1} \in P$ and $(ab^{-1})(cd^{-1}) = (ab)(cd)^{-1} \in P$. And if $ab^{-1} \neq 0$ then we in particular have $a \neq 0$ and hence $(ab^{-1})^{-1} = ba^{-1} \in P$. Clearly $X \subseteq P$, as even $X \subseteq \langle X \rangle_{\mathbf{r}}$. Altogether P is a field containing X and hence $\langle X \rangle_{\mathbf{f}} \subseteq P$. And if conversely $Q \subseteq R$ is a field containing X, then $\langle X \rangle_{\mathbf{r}} \subseteq Q$. Thus is $a, b \in Q$ with $b \neq 0$ then $b^{-1} \in Q$ and hence $ab^{-1} \in Q$, as Q is a field. But this proves $P \subseteq Q$ and thus $P \subseteq \langle X \rangle_{\mathbf{f}}$.
Proof of (3.11):

- Let us denote the set $P := \{\sum_i a_i x_i\}$ of which we claim $P = \langle X \rangle_{\mathrm{m}}$. First of all it is clear that $X \subseteq P$, as $x = 1x \in P$ for any $x \in X$. Further it is clear that $P \leq_{\mathrm{m}} M$ is a submodule of M: choose any $x \in X$, then $0 = 0 \diamond x \in P$, and if $a \in R$, $x = a_1 x_1 + \dots + a_m x_m$ and $y = b_1 y_1 + \dots + b_n y_n \in P$ then $ax = (aa_1)x_1 + \dots + (aa_m)x_m \in P$ and $x + y = a_1 x_1 + \dots + a_m x_m + b_1 y_1 + \dots + b_n y_n \in P$. Thus by definition of $\langle X \rangle_{\mathrm{m}}$ we get $\langle X \rangle_{\mathrm{m}} \subseteq P$. Now suppose $Q \leq_{\mathrm{m}} M$ is any submodule of M containing $X \subseteq Q$. Then for any $a_i \in R$ and any $x_i \in X \subseteq Q$ we get $a_i x_i \in Q$ and hence $\sum_i a_i x_i \in Q$, too. That is $P \subseteq Q$, and as Q has been arbitary this means $P \subseteq \langle X \rangle_{\mathrm{m}}$, by the definition of $\langle X \rangle_{\mathrm{m}}$.
- Denote the set $P := \{\sum_i a_i \prod_j x_{i,j}\}$ of which we claim $P = \langle X \rangle_{\rm b}$. Again it is clear, that $X \subseteq P$, as $x = 1x \in P$ for any $x \in X$. Further it is clear that $P \leq_{\rm b} A$ is a sub-semialgebra of A: choose any $x \in X$, then $0 = 0 \diamond x \in P$, and if $a \in R$, $f = \sum_i a_i \prod_j x_{i,j}$ and $g = \sum_k b_k \prod_l y_{k,l}$, then $af = \sum_i (aa_i) \prod_j x_{i,j} \in P$, $f + g = \sum_i a_i \prod_j x_{i,j} + \sum_k b_k \prod_l y_{k,l} \in P$ and by general distributivity $fg = \sum_i \sum_j (a_i b_j) (\prod_j x_{i,j} \prod_l y_{k,l}) \in P$. Thus by definition of $\langle X \rangle_{\rm b}$ we get $\langle X \rangle_{\rm b} \subseteq P$. Now suppose $Q \leq_{\rm b} A$ is any sub-semi-algebra of A. Then for any $a_i \in R$ and any $x_{i,j} \in X \subseteq Q$ we get $\prod_j x_{i,j} \in Q$, hence $a_i \prod_j x_{i,j} \in Q$ and finally $\sum_i a_i \prod_j x_{i,j} \in Q$. That is $P \subseteq Q$, and as Q has been arbitary, this means $P \subseteq \langle X \rangle_{\rm b}$, by definition of $\langle X \rangle_{\rm b}$.
- By construction $P := \langle X \cup \{1\} \rangle_{\mathrm{b}}$ is a sub-semi-algeba containing 1, in other words a subalgebra. And as $X \subseteq P$ this implies $\langle X \rangle_{\mathrm{a}} \subseteq P$. And as any subalgebra $Q \leq_{\mathrm{a}} A$ contains 1 we get the implications $X \subseteq Q \implies X \cup \{1\} \subseteq Q \implies P \subseteq Q$. This also proves $\langle X \rangle_{\mathrm{a}} \subseteq P$, as Q has been arbitary.

Proof of (1.34):

We first have to prove, that $\mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$ truly are ideals of R. In the case of $\mathfrak{a} \cap \mathfrak{b}$ this has already been done in (1.30). For $\mathfrak{a} + \mathfrak{b}$ it is clear that $0 = 0 + 0 \in \mathfrak{a} + \mathfrak{b}$. and if a + b and $a' + b' \in \mathfrak{a} + \mathfrak{b}$ then also $(a + b) + (a' + b') = (a + a') + (b + b') \in \mathfrak{a} + \mathfrak{b}$ and $-(a + b) = (-a) + (-b) \in \mathfrak{a} + \mathfrak{b}$. Thus consider any $f \in R$, as \mathfrak{a} and \mathfrak{b} are ideals we have fa, $af \in \mathfrak{a}$ and fb, $bf \in \mathfrak{b}$ again. Hence we get f(a + b) = (fa) + (fb) and $(a + b)f = (af) + (bf) \in \mathfrak{a} + \mathfrak{b}$. Likewise $0 = 0 \cdot 0 \in \mathfrak{a}\mathfrak{b}$. And if $f = \sum_i a_i b_i$ and $g = \sum_j c_j d_j \in \mathfrak{a}\mathfrak{b}$ then it is clear

from the definition that $f + g \in \mathfrak{ab}$. Further $-f = \sum_i (-a_i)b_i \in \mathfrak{ab}$ and for any arbitrary $h \in R$ we also get $hf = \sum_i (ha_i)b_i$ and $fh = \sum_i a_i(b_ih) \in \mathfrak{ab}$ by the same reasoning as for $\mathfrak{a} + \mathfrak{b}$.

Thus it remains to prove the chain of inclusions $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$. Hereby $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$ is clear by taking b = 0 in $a + b \in \mathfrak{a} + \mathfrak{b}$. And $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ is true trivially. Thus it only remains to verify $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. That is we consider $f = \sum_i a_i b_i \in \mathfrak{a}\mathfrak{b}$. Since $a_i \in \mathfrak{a}$ and \mathfrak{a} is an ideal we have $a_i b_i \in \mathfrak{a}$ and hence even $f \in \mathfrak{a}$. Likewise we can verify $f \in \mathfrak{b}$ such that $f \in \mathfrak{a} \cap \mathfrak{b}$ as claimed.

Proof of (1.35):

The associativity of \cap is clear (from the associativity of the locical *and*). The associativity of ideals $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$ is immediate from the associativity of elements (a + b) + c = a + (b + c). The same is true for the commutativity of \cap and +. Next we prove $(\mathfrak{a}\mathfrak{b})\mathfrak{c} \subseteq \mathfrak{a}(\mathfrak{b}\mathfrak{c})$. That is we are given an element of $(\mathfrak{a}\mathfrak{b})\mathfrak{c}$ which is of the form

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{i,j} b_{i,j} \right) c_j = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} (b_{i,j} c_j)$$

For some $a_{i,j} \in \mathfrak{a}$, $b_{i,j} \in \mathfrak{b}$ and $c_j \in \mathfrak{c}$. However from the latter representation it is clear that this element is also contained in $\mathfrak{a}(\mathfrak{b}\mathfrak{c})$, which establishes the inclusion. The converse inclusion can be shown in complete analogy, which proves the associativity $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$. And if R is commutative the commutativity of ideals $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ is immediate from the commutativity of the elements ab = ba. Thus it remains to check the distributivity

$$\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}\mathfrak{b}) + (\mathfrak{a}\mathfrak{c})$$

For the inclusion " \supseteq " we are given elements $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $c_i \in \mathfrak{c}$ (where $i \in 1...m$) such that $\sum_i a_i(b_i + c_i) \in \mathfrak{a}(\mathfrak{b} + \mathfrak{c})$. But it is already obvious that $\sum_i a_i(b_i + c_i) = \sum_i a_i b_i + \sum_i a_i c_i \in (\mathfrak{a}\mathfrak{b}) + (\mathfrak{a}\mathfrak{c})$. And for the converse inclusion " \subseteq " we are given $a_i, a'_j \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $c_j \in \mathfrak{c}$ such that $\sum_i a_i b_i + \sum_j a'_j c_j \in (\mathfrak{a}\mathfrak{b}) + (\mathfrak{a}\mathfrak{c})$. This however can be rewritten into the form $\sum_i a_i b_i + \sum_j a'_j c_j = \sum_i a_i(b_i + 0) + \sum_j a'_j(0 + c_j) \in \mathfrak{a}(\mathfrak{b} + \mathfrak{c})$. In complete analogy it can be shown, that $(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = (\mathfrak{a}\mathfrak{c}) + (\mathfrak{b}\mathfrak{c})$.

Proof of (1.37):

By assumption we have $\mathfrak{a} = \langle X \rangle_i$ and $\mathfrak{b} = \langle Y \rangle_i$, in particular $X \subseteq \mathfrak{a}$ and $Y \subseteq \mathfrak{b}$. Hence we get $X \cup Y \subseteq \mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$ and therefore $\langle X \cup Y \rangle_i \subseteq \mathfrak{a} + \mathfrak{b}$ (as $\mathfrak{a} + \mathfrak{b}$ is an ideal of R). For the converse inclusion we regard $f = \sum_i a_i x_i b_i \in \mathfrak{a}$ and $g = \sum_j c_j y_j d_j$ (note that this representation with $x_i \in X$ and $y_j \in Y$ is allowed, due to (1.33)). And hence we get $f + g = \sum_{i} a_{i}x_{i}b_{i} + \sum_{j} c_{j}y_{j}d_{j} \in \langle X \cup Y \rangle_{i}$. Together we have found $\mathfrak{a} + \mathfrak{b} = \langle X \cup Y \rangle_{i}$. For $\mathfrak{ab} = \langle XY \rangle_{i}$ we have assumed R to be commutative. The one incluion is clear: as $X \subseteq \mathfrak{a}$ and $Y \subseteq \mathfrak{b}$ we trivially have $XY \subseteq \mathfrak{ab}$. And as \mathfrak{ab} is an ideal of R this implies $\langle XY \rangle_{i} \subseteq \mathfrak{ab}$. For the converse inclusion we regard $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ as above. Then $fg = \sum_{i} \sum_{j} a_{i}b_{i}x_{i}y_{j}c_{j}d_{j} \in \langle XY \rangle_{i}$ (due to the commutativity of R) which also establishes $\langle XY \rangle_{i} = \mathfrak{ab}$.

Proof of (1.38):

(i) First of all it is clear that $\mathfrak{b} \setminus \mathfrak{a} \subseteq \mathfrak{b}$. And hence we find $\langle \mathfrak{b} \setminus \mathfrak{a} \rangle_i \subseteq \langle \mathfrak{b} \rangle_i = \mathfrak{b}$ (as \mathfrak{b} is an ideal already). Thus we have proved

$$\langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathrm{i}} \subseteq \mathfrak{k}$$

Now fix any $b \in \mathfrak{b} \setminus \mathfrak{a}$ (this is possible by assumption $\mathfrak{a} \subset \mathfrak{b}$) and consider any $a \in \mathfrak{a}$. Then $a-b \in \mathfrak{b}$ but $a-b \notin \mathfrak{a}$ (else let $\alpha := a-b \in \mathfrak{a}$, then $b = a - \alpha \in \mathfrak{a}$, a contradiction). Thus $a - b \in \mathfrak{b} \setminus \mathfrak{a}$ and hence $a = b + (a-b) \in \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{i}$. As a has been arbitrary this yields $\mathfrak{a} \subseteq \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{i}$ and thereby we have also proved the converse inclusion

$$\mathfrak{b} = \mathfrak{a} \cup (\mathfrak{b} \setminus \mathfrak{a}) \subseteq \mathfrak{a} \cup \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathrm{i}} = \langle \mathfrak{b} \setminus \mathfrak{a} \rangle_{\mathrm{i}}$$

- (ii) By (1.33) the ideal generated by the union of the \mathfrak{a}_i consists of finite sums of elements of the form $a_i x_i b_i$ where $a_i, b_i \in \mathbb{R}$ and $x_i \in \mathfrak{a}_i$. But as \mathfrak{a}_i is an ideal we get $a_i x_i b_i \in \mathfrak{a}_i$ already. And conversely any finite sum of elements $x_i \in \mathfrak{a}_i$ can be realized, by taking $a_i = b_i = 1$.
- (iii) Here we just rewrote the the equality in (ii) in several ways: given a sum $\sum_{i \in I} a_i$ where $a_i \in \mathfrak{a}_i$ and $\Omega := \{i \in I \mid a_i \neq 0\}$ is finite then $\sum_{i \in I} a_i = \sum_{i \in \Omega} a_i$ by definition of arbitrary sums. And likewise this is just $\sum_k a_k$ where $n := \#\Omega$, $\Omega = \{i(1), \ldots, i(n)\}$ and $a_k = a_{i(k)}$.
- (iv) The general distributivity rule can be seen by a straightforward computation using the general rules of distributivity and associativity. First note that by definition and (iii) we have

$$\sum_{i \in I} \mathfrak{a}_i \mathfrak{b} = \left\{ \sum_{i \in \Omega} \left(\sum_{k=1}^{n(i)} a_{i,k} b_{i,k} \right) \middle| a_{i,k} \in \mathfrak{a}_i, \ b_{i,k} \in \mathfrak{b} \right\}$$

Now let $n := \max\{n(i) \mid i \in \Omega\}$ and for any k > n(i) let $a_{i,k} := 0 \in \mathfrak{a}_i$. Then we may rewrite the latter set in the form

$$\sum_{i\in I} \mathfrak{a}_i \mathfrak{b} = \left\{ \sum_{k=1}^n \sum_{i\in\Omega} a_{i,k} b_{i,k} \mid a_{i,k} \in \mathfrak{a}_i, \ b_{i,k} \in \mathfrak{b} \right\}$$

Let us now regart the other set involved. Again we will compute what this set means explicitly - and thereby we will find the same identity as the one wh have just proved

$$\left(\sum_{i\in I}\mathfrak{a}_i\right)\mathfrak{b} = \left\{\sum_{k=1}^n \left(\sum_{i\in\Omega(k)}a_{i,k}\right)b_k \ \middle| \ a_{i,k}\in\mathfrak{a}_i, \ b_k\in\mathfrak{b}\right\}$$

Then (in analogy to the above) we take $\Omega := \Omega(1) \cup \cdots \cup \Omega(n)$, $a_{i,k} := 0$ for $i \notin \Omega(k)$ and $b_{i,k} := b_k$. Then this turns into

$$\left(\sum_{i\in I}\mathfrak{a}_i\right)\mathfrak{b} = \left\{\sum_{k=1}^n\sum_{i\in\Omega}a_{i,k}b_{i,k} \mid a_{i,k}\in\mathfrak{a}_i, \ b_{i,k}\in\mathfrak{b}\right\}$$

Proof of (1.39):

- (i) (a) ⇒ (b): 1 ∈ R = a + b = {a + b | a ∈ a, b ∈ b} is clear. Hence there are a' ∈ a and b ∈ b such that 1 = a' + b. Now let a := -a' ∈ a then 1 = (-a) + b and hence b = 1 + a ∈ (1 + a) ∩ b. (b) ⇒ (c): let b ∈ (1 + a) ∩ b, that is there is some a' ∈ a such that b = 1 + a'. Again we let a := -a' ∈ a, then a + b = 1. (c) ⇒ (a): by the same reasoning as before we find 1 = a + b ∈ a + b. And as a + b is an ideal of R, this implies a + b = R.
- (ii) As \mathfrak{a} and \mathfrak{b} are coprime there are some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that a + b = 1 diue to (i). Using these we compute

$$1 = 1^{i+j} = (a+b)^{i+j} = \sum_{h=0}^{i+j} {i+j \choose h} a^h b^{i+j-h}$$
$$= \sum_{h=0}^{i} {i+j \choose h} a^h b^{i+j-h} + \sum_{h=i+1}^{i+j} a^h b^{i+j-h}$$
$$= b^j \sum_{h=0}^{i} {i+j \choose h} a^h b^{i-h} + a^i \sum_{h=1}^{j} {i+j \choose i+h} a^h b^{j-h}$$
$$\in \mathfrak{h}^j + \mathfrak{a}^i$$

(iii) We will use induction on k. The case k = 1 is trivial and hence we found the induction at k = 2. In this case let us first choose $a_1, a_2 \in \mathfrak{a}$, $b_1 \in \mathfrak{b}_1$ and $b_2 \in \mathfrak{b}_2$ such that $a_1 + b_1 = 1$ and $a_2 + b_2 = 1$. Then

$$b_1b_2 = (1-a_1)(1-a_2) = 1-a_1-a_2+a_1a_2$$

This implies $1 = (a_1 + a_2 - a_1a_2) + b_1b_2 \in \mathfrak{a} + \mathfrak{b}_1\mathfrak{b}_2$ which rests the case k = 2. So we now assume $k \geq 2$ and are given $\mathfrak{a} + \mathfrak{b}_i = R$ for any $i \in 1 \dots k + 1$. By induction hypothesis we in particular get $\mathfrak{a} + \mathfrak{b}_1 \dots \mathfrak{b}_k = R$. And together with $\mathfrak{a} + \mathfrak{b}_{k+1} = R$ and the case k = 2 this yields the induction step $\mathfrak{a} + (\mathfrak{b}_1 \dots \mathfrak{b}_k)\mathfrak{b}_{k+1} = R$.

(iv) We will prove the two inclusions by induction on k seperately. The case k = 1 is trivial, so we will start with k = 2 only. In this case the inclusion $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$ has already been proved. And if $k \ge 2$ then

$$(\mathfrak{a}_1 \dots \mathfrak{a}_k)\mathfrak{a}_{k+1} \subseteq (\mathfrak{a}_1 \dots \mathfrak{a}_k) \cap \mathfrak{a}_{k+1} \subseteq (\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_k) \cap \mathfrak{a}_{k+1}$$

due to the case k = 2 and the induction hypothesis respectively. For the converse inclusion we start with k = 2 again. And as \mathfrak{a}_1 and \mathfrak{a}_2 are coprime we may find $a_1 \in \mathfrak{a}_1$ and $a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. If now $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$ is an arbitrary element then

$$x = x1 = x(a_1 + a_2) = xa_1 + xa_2 = a_1x + a_2x \in \mathfrak{a}_1\mathfrak{a}_2$$

This proves $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1 \mathfrak{a}_2$ and hence we may commence with $k \geq 2$. In this case we are given some $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k \cap \mathfrak{a}_{k+1}$. In particular this is $x \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$ and hence $x \in \mathfrak{a}_1 \dots \mathfrak{a}_k$ by induction hypothesis. Thus we get $x \in (\mathfrak{a}_1 \dots \mathfrak{a}_k) \cap \mathfrak{a}_{k+1}$. But because of (iii) (using $\mathfrak{a} := \mathfrak{a}_{k+1}$ and $\mathfrak{b}_i := \mathfrak{a}_i$) we know that $\mathfrak{a}_1 \dots \mathfrak{a}_k$ and \mathfrak{a}_{k+1} are coprime. Therefore we may apply the case k = 2 again to finally find $x \in (\mathfrak{a}_1 \dots \mathfrak{a}_k)\mathfrak{a}_{k+1}$.

Proof of (1.40):

We first prove that \sim is an equivalence relation: *Reflexivity* $a \sim a$ is clear, as $a - a = 0 \in \mathfrak{a}$. Symmetry if $a \sim b$ then $a - b \in \mathfrak{a}$ and hence $b - a = -(a - b) \in \mathfrak{a}$ which proves $b \sim a$. Transitivity if $a \sim b$ and $b \sim c$ then $a - c = (a - b) + (b - c) \in \mathfrak{a}$ such that $a \sim c$. If now $a \in R$ then

 $\begin{array}{rcl} \left[a\right] &=& \left\{b \in R \mid a \sim b\right\} &=& \left\{b \in R \mid a - b \in \mathfrak{a}\right\} \\ &=& \left\{b \in R \mid \exists h \in \mathfrak{a} : a - b = h\right\} \\ &=& \left\{a + h \mid h \in \mathfrak{a}\right\} &=& a + \mathfrak{a} \end{array}$

Now assume that $\mathfrak{a} \leq_{i} R$ even is an ideal, then we have to prove, that R/\mathfrak{a} is a ring under the operations + and \cdot as we have introduced them. Thus we prove the well-definedness: suppose $a + \mathfrak{a} = a' + \mathfrak{a}$ and $b + \mathfrak{a} = b' + \mathfrak{a}$ then a - a' and $b - b' \in \mathfrak{a}$ and hence $(a + b) - (a' + b') = (a - a') + (b - b') \in \mathfrak{a}$. This means $a + b \sim a' + b'$ and hence $(a + b) + \mathfrak{a} = (a' + b') + \mathfrak{a}$. Analogously

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$$

As \mathfrak{a} is an ideal both (a - a')b and a'(b - b') are contained in \mathfrak{a} and hence also the sum $ab - a'b' \in \mathfrak{a}$. This means $ab \sim a'b'$ and hence $ab + \mathfrak{a} = a'b' + \mathfrak{a}$. Hence these operations are well-defined. And all the properties (associativity, commutativity, distributivity and so forth) are immediate from the respective properties of R. This also shows that $1 + \mathfrak{a}$ is the unit element of R/\mathfrak{a} (supposed 1 is the unit element of R).

Proof of (3.13):

We first prove that ~ truly is an equivalence relation, the reflexivity x ~ x is clear, as x - x = 0 ∈ P. For the symmetry suppose x ~ y, that is y - x ∈ P and hence x - y = -(y - x) = (-1)(y - x) ∈ P. For the transitivity we finally consider x ~ y and y ~ z. That is y - x ∈ P and z - y ∈ P and this yields z - x = (z - y) + (y - x) ∈ P. As in the proof of (1.40) it is clear that [x] = x + P, as

$$[x] = \{ y \in M \mid y - x \in P \} = x + P$$

- Next we will prove the well-definedness of the addition and scalarmultiplication. Thus consider x + P = x' + P and y + P = y' + P, that is $x' - x \in P$ and $y' - y \in P$. As P is an R-submodule we get $(x' + y') - (x + y) = (x' - x) + (y' - y) \in P$ and this again is (x + y) + P = (x' + y') + P. Likewise for any $a \in R$ we get $(ax') - (ax) = a(x' - x) \in P$, which is ax + P = ax' + P.
- Now we immediately see, that M/P is an R-module again. The associativity and commutativity of + are inherited trivially from M. And the same is true for the compatibility properties of \diamond . The neutral element of M/P is given to be 0 + P, as for any $x + P \in M/P$ we get (x+P)+(0+P) = (x+0)+P = x+P. And the inverse of $x+P \in M/P$ is just (-x) + P, as (x+P) + ((-x) + P) = (x + (-x)) + P = 0 + P.
- Finally suppose A is an R-(semi)algebra, then we want to show that A/\mathfrak{a} is an R-(semi)algebra again. As the R-algebraideal \mathfrak{a} is an R-submodule A/\mathfrak{a} already is an R-module, by what we have already shown. Next we have to verify the well-definedness of the multiplication. Thus consider $f + \mathfrak{a} = f' + \mathfrak{a}$ and $g + \mathfrak{a} = g' + \mathfrak{a}$, then $(f'g') (fg) = f'(g'-g) + (f'-f)g \in \mathfrak{a}$, by assumption on \mathfrak{a} . Now it is clear that A/\mathfrak{a} inherits the associativity of the multiplication from A. Likewise the compatibility properties of \cdot , + and \diamond are inherited

trivially. As an example let us regard the identity of

$$\begin{split} & \left(a(f+\mathfrak{a})\right)(g+\mathfrak{a}) &= (af+\mathfrak{a})(g+\mathfrak{a}) = (af)g+\mathfrak{a} = a(fg)+\mathfrak{a} \\ & (f+\mathfrak{a})\left(a(g+\mathfrak{a})\right) &= (f+\mathfrak{a})(ag+\mathfrak{a}) = f(ag)+\mathfrak{a} = a(fg)+\mathfrak{a} \\ & a\left((f+\mathfrak{a})(g+\mathfrak{a})\right) &= a(fg+\mathfrak{a}) = a(fg)+\mathfrak{a} \end{split}$$

Г			
L			
۲	-	-	-

Proof of (1.43):

- We first prove that b/a truly is an ideal of R/a. Thus regard a + a and b + a ∈ b/a, that is a, b ∈ b. Then we clearly get a + b and -a ∈ b such that (a+a) + (b+a) = (a+b)+a ∈ b/a and -(a+a) = (-a)+a ∈ b/a. Further if f + a ∈ R/a (that is f ∈ R) then fb, bf ∈ b, as b is an ideal. And hence (f + a)(b+a) = (fb)+a ∈ b/a, likewise (b+a)(f+a) ∈ b/a.
- Next we prove that $\mathfrak{b} := \{b \in R \mid b + \mathfrak{a} \in \mathfrak{u}\} \leq_{i} R$ is an ideal, supposed $\mathfrak{u} \leq_{i} R/\mathfrak{a}$ is an ideal. Thus consider $a, b \in \mathfrak{b}$ then $(a + b) + \mathfrak{a} = (a + \mathfrak{a}) + (b + \mathfrak{a}) \in \mathfrak{u}$ and $(-a) + \mathfrak{a} = -(a + \mathfrak{a}) \in \mathfrak{u}$ which proves a + band $-a \in \mathfrak{b}$. And if $f \in R$ then $(fb) + \mathfrak{a} = (f + \mathfrak{a})(b + \mathfrak{a}) \in \mathfrak{u}$ which proves $fb \in \mathfrak{b}$ (likewise $bf \in \mathfrak{b}$. Hence \mathfrak{b} is an ideal, and $\mathfrak{a} \subseteq \mathfrak{b}$ is clear, as for any $a \in \mathfrak{a}$ we get $a + \mathfrak{a} = 0 + \mathfrak{a} \in \mathfrak{u}$.
- Thus we have proved that the maps $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ and $\mathfrak{u} \mapsto \mathfrak{b}$ are well defined. We now claim that they even are mutually inverse. For the first composition we start with $\mathfrak{a} \subseteq \mathfrak{b} \leq_i R$. Then

$$\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a} \mapsto \left\{ b \in R \mid b + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a} \right\} = \left\{ b \mid b \in \mathfrak{b} \right\} = \mathfrak{b}$$

For the converse composition we start with an ideal $\mathfrak{U} \leq_i R/\mathfrak{a}$, which is mapped to $\mathfrak{b} := \{b \in R \mid b + \mathfrak{a} \in \mathfrak{U}\}$. Now it is easy to see that

$$\mathfrak{u} \mapsto \mathfrak{b} \mapsto \mathfrak{b}/_{\mathfrak{a}} = \{ b + \mathfrak{a} \mid b + \mathfrak{a} \in \mathfrak{u} \} = \mathfrak{u}$$

• Next we prove that this correspondence respects intersections, sums and products of ideals as claimed. That is \mathfrak{b} and $\mathfrak{c} \leq_{\mathbf{i}} R$ are ideals

with $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{a} \subseteq \mathfrak{c}$. Then

$$\begin{split} & \mathfrak{b}/\mathfrak{c} \cap \mathfrak{c}/\mathfrak{c} &= \left\{ b + \mathfrak{a} \mid b \in \mathfrak{b} \cap \mathfrak{c} \right\} = \mathfrak{b} \cap \mathfrak{c}/\mathfrak{c} \\ & \mathfrak{b}/\mathfrak{c} + \mathfrak{c}/\mathfrak{c} &= \left\{ (b + \mathfrak{a}) + (c + \mathfrak{a}) \mid b \in \mathfrak{b}, c \in \mathfrak{c} \right\} \\ &= \left\{ (b + c) + \mathfrak{a} \mid b \in \mathfrak{b}, c \in \mathfrak{c} \right\} = \mathfrak{b} + \mathfrak{c}/\mathfrak{c} \\ & \mathfrak{b}/\mathfrak{c} \mathfrak{c}/\mathfrak{c} &= \left\{ \sum_{i=1}^{n} (b_i + \mathfrak{a})(c_i + \mathfrak{a}) \mid b_i \in \mathfrak{b}, c_i \in \mathfrak{c} \right\} \\ &= \left\{ \left(\sum_{i=1}^{n} b_i c_i \right) + \mathfrak{a} \mid b_i \in \mathfrak{b}, c_i \in \mathfrak{c} \right\} = \mathfrak{b} \mathfrak{c}/\mathfrak{c} \end{split}$$

• The final statement of the lemma is concerned with the generation of ideals. For the inclusion " \supseteq " we consider any $u \in \langle X/\mathfrak{a} \rangle_i$. That is there are $a_i + \mathfrak{a}$, $b_i + \mathfrak{a} \in R/\mathfrak{a}$ and $x_i + \mathfrak{a} \in X/\mathfrak{a}$ such that

$$u = \sum_{i=1}^{k} (a_i + \mathfrak{a})(x_i + \mathfrak{a})(b_i + \mathfrak{a})$$
$$= \left(\sum_{i=1}^{k} a_i x_i b_i\right) + \mathfrak{a} \in \langle X \rangle_i + \mathfrak{a}/\mathfrak{a}$$

And for the converse inclusion " \subseteq " we are given some $a \in \mathfrak{a}$ and $y \in \langle X \rangle_{i}$. This again means that there are some $a_i, b_i \in R$ and $x_i \in X$ such that $y = \sum_i a_i x_i b_i$. We now undo the above computation

$$(a+y) + \mathfrak{a} = y + \mathfrak{a} = \sum_{i=1}^{k} (a_i + \mathfrak{a})(x_i + \mathfrak{a})(b_i + \mathfrak{a}) \in \langle X/\mathfrak{a} \rangle_{i}$$

• We now prove that this correspondence even interlocks radical ideals. First note that $\mathfrak{b} \leq_i R$ is radical iff $\sqrt{\mathfrak{b}} = \mathfrak{b}$. Now remark that $(b+\mathfrak{a})^k = b^k + \mathfrak{a} \in \mathfrak{b}/\mathfrak{a}$ is (by definition) equivalent to $b^k \in \mathfrak{b}$. Thus we found

$$\sqrt{\mathfrak{b}/\mathfrak{a}} = \sqrt{\mathfrak{b}}/\mathfrak{a}$$

And in particular we see that $\mathfrak{b}/\mathfrak{a}$ is a redical ideal if and only if \mathfrak{b} is a radical ideal. And this has been claimed.

• If $\mathfrak{p} \leq_{i} R/\mathfrak{a}$ is prime then regard any $a, b \in R$. Then $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$ is equivalent, to $ab \in \mathfrak{p}$ which again is equivalent, to $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (as \mathfrak{p} is prime). And again this is equivalent, to $a + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$ or $b + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$. Hence $\mathfrak{p}/\mathfrak{a}$ is prime, too. For the converse implication just pursue the same arguments in inverse order.

• As the correspondence $\mathfrak{b} \longleftrightarrow \mathfrak{b}/\mathfrak{a}$ maintains the inclusion \subseteq of subsets, it is clear that maximal elements mutually correspond to each other. That is $\mathfrak{m}/\mathfrak{a}$ is maximal, if and only if $\mathfrak{m}/\mathfrak{a}$ is maximal.

Proof of (3.14):

- (i) We will first prove the eqivalency $x + L \in P/L \iff x \in P$. The one implication is trivial: if $x \in P$, then $x + L \in P/L$ by definition. Conversely suppose there is some $p \in P$ such that $x+L = p+L \in P/L$. By definition of M/L this means $x - p \in L$, that is $x - p = \ell$ for some $\ell \in L \subseteq P$. And therefore $x = p + \ell \in P$, as $p, \ell \in P$ and $P \leq_{\mathrm{m}} M$. Now we are ready to prove $P/L \leq_{\mathrm{m}} M/L$, clearly $0 = 0 + L \in P/L$, as we have $0 \in P$. Now consider x + L and $y + L \in P/L$, by what we have just seen this means x and $y \in P$. As $P \leq_{\mathrm{m}} M$ this implies $x + y \in P$ and hence $(x + L) + (y + L) = (x + y) + L \in P/L$ again. Finally consider any $a \in R$, as $x \in P$ and $P \leq_{\mathrm{m}} M$ this implies $ax \in P$ and hence also $a(x + L) = (ax) + L \in P/L$. Altogether P/Lis a submodule of M/L.
- (ii) In (i) we have seen that $P \mapsto P/L$ is a well-defined map, so next we will point out that $U \mapsto (U) := \{x \in M \mid x + L \in U\}$ is well-defined, too. That is we have to verify $(U) \leq_{\mathrm{m}} M$ and $L \subseteq (U)$. The containment $L \subseteq (U)$ is clear, if $\ell \in L$ then $\ell + L = 0 + L = 0 \in U$ and hence $\ell \in (U)$. In particular $0 \in (U)$. Next suppose we age given $x, y \in (U)$, that is $x + L, y + L \in U$. Then $(x + y) + L = (x + L) + (y + L) \in U$ as $U \leq_{\mathrm{m}} M/L$ and hence $x + y \in (U)$ again. Likewise for any $a \in R$ we get $(ax) + L = a(x + L) \in U$ and hence $ax \in (U)$, as $x + L \in U$ and $U \leq_{\mathrm{m}} M/L$. Thus both maps given are well-defined. It remains to verify that they are mutually inverse: the one direction is easy, consider any $U \leq_{\mathrm{m}} M/L$, then $U \mapsto (U) \mapsto (U)/L = \{x + L \mid x + L \in U\} =$ U. Conversely consider any $L \subseteq P \leq_{\mathrm{m}} M$, then $P \mapsto P/L \mapsto (P/L)$, yet using (i) we obtain (P/L) = P from the following computation

$$\binom{P}{L} = \left\{ x \in M \mid x + L \in \frac{P}{L} \right\} = \left\{ x \in M \mid x \in P \right\} = P$$

(iii) To prove this claim we just have to iterate the equivalency in (i): $x + L \in (\bigcap_i P_i)/L$ is equivalent to $x \in \bigcap_i P_i$, which again is equivalent to $\forall i \in I : x \in P_i$. Now we use (i) once more to reformulate this into the equivalent statement $\forall i \in I : x + L \in P_i/L$, which obviously translates into $x + L \in \bigcap_i (P_i/L)$ again.

(iv) We want to verify $\sum_i (P_i/L) = (\sum_i P_i)/L$, to do this recall the explicit description of an arbitrary sum of submodules for the $P_i/L \leq_{\rm m} M/L$

$$\sum_{i \in I} \left(\frac{P_i}{L} \right) = \left\{ \sum_{i \in \Omega} (x_i + L) \mid \Omega \subseteq I \text{ finite, } x_i + L \in \frac{P_i}{L} \right\}$$

Next recall the equivalency in (i), this allows us to simply substitute $x_i + L \in P_i/L$ by $x_i \in P_i$. Further - by definition of + in M/L - we can rewrite the sum $\sum_i (x_i + L) = (\sum_i x_i) + L$. Together this yields

$$\sum_{i \in I} \left(\frac{P_i}{L} \right) = \left\{ \left(\sum_{i \in \Omega} x_i \right) + L \mid \Omega \subseteq I \text{ finite, } x_i \in P_i \right\}$$

That is the term on the right hand side is (apart from the +L in $(\sum_i x_i) + L$) nothing but the sum $\sum_i P_i$ again (by the explicit description of arbitrary sums of the submodules P_i . That is we have already arrived at our claim $\sum_i (P_i/L) = (\sum_i P_i)/L$.

- (v) Let us denote $P'_i := P_i + L$, then it is clear that $L \subseteq P'_i$ for any $i \in I$. But on the other hand $\sum_i P'_i = \sum_i (P_i + L) = (\sum_i P_i) + L$ as the finitely many occurances of elements $\ell_i \in L$ can be composed to a single occurance of $\ell := \sum_i \ell_i \in L$. But by assumption L is already contained in $\sum_i P_i$ and hence $(\sum_i P_i) + L = \sum_i P_i$. That is we have obtained $\sum_i P'_i = \sum_i P_i$. Now statement (iv), that has just been proved, yields $(\sum_i P_i)/L = (\sum_i P'_i)/L = \sum_i (P'_i/L)$, as claimed.
- (vi) To prove this identity we directly refer to the definition of the *R*-submodule generated by $X/L \subseteq M/L$. And this is given to be

$$\langle X/_L \rangle_{\mathrm{m}} = \bigcap \left\{ U \leq_{\mathrm{m}} M/_L \mid X/_L \subseteq U \right\}$$

By (ii) the submodules U of M/L correspond bijectively to the submodules P of M containing L. I.e. we may insert P/L for U, yielding

$$\langle X/L \rangle_{\mathrm{m}} = \bigcap \left\{ P/L \mid L \subseteq P \leq_{\mathrm{m}} M, X/L \subseteq P/L \right\}$$

Clearly $X/L \subseteq P/L$ translates into $\forall x \in X : x + L \in P/L$, and due to the equivalency in (i) this is $\forall x \in X : x \in P$, i.e. $X \subseteq P$, therefore

$$\langle X/L \rangle_{\mathrm{m}} = \bigcap \left\{ P/L \mid L \subseteq P \leq_{\mathrm{m}} M, X \subseteq P \right\}$$

Of course $L \subseteq P$ and $X \subseteq P$ can be written more compactly as $X \cap L \subseteq P$. And due to (iii) the intersection commutes with taking to quotients, such that we may reformulate

$$\langle X/L \rangle_{\mathrm{m}} = \bigcap \{ P \mid P \leq_{\mathrm{m}} M, X \cap L \subseteq P \}/L$$

That is we have arrived at $\langle X/L \rangle_{\rm m} = \langle X \cup L \rangle_{\rm m}/L$. But by the explicit representation of the generated submodules (3.11) it is clear, that $\langle X \cap L \rangle_{\rm m} = \langle X \rangle_{\rm m} + \langle L \rangle_{\rm m}$. And as *L* already is a submodule of *M* we have $\langle L \rangle_{\rm m} = L$. Altogether $\langle X/L \rangle_{\rm m} = (\langle X \rangle_{\rm m} + L)/L$.

Proof of (3.16):

- (i) We will first prove that $ANN_R(X)$ is a left-ideal of R. As this is just the intersection of the annihilators $ANN_R(x)$ (where $x \in X$) it suffices to verify $ANN_R(x) \leq_m R$ for any $x \in M$, due to (1.30). Now $0 \in ANN_R(x)$ is clear, as $0 \diamond x = 0$ for any $x \in M$. Now consider any two a, $b \in ANN_R(x)$, that is ax = 0 and bx = 0. Then (a+b)x = (ax)+(bx) = 0 + 0 = 0 and hence $a + b \in ANN_R(x)$ again. Finally consider any $r \in R$, then $(ra)x = r(ax) = r \diamond 0 = 0$ and hence $ra \in ANN_R(x)$, as well. Altogether we have $ANN_R(x) \leq_m R$ and hence $ANN_R(X) \leq_m R$.
- (i) Next we want to prove that $ANN_R(M) \leq_i R$ even is an ideal. As we already know $ANN_R(M) \leq_m R$ it only remains to prove that $ar \in ANN_R(M)$ for any $a \in ANN_R(M)$ and any $r \in R$. As $a \in ANN_R(M)$ we have ay = 0 for any $y \in M$. Now consider any $x \in M$, then $rx \in M$, too as M is an R-module. Thus (ar)x = a(rx) = 0 and as x has been arbitrary this means $ar \in ANN_R(M)$ again.
- (ii) Let us denote $\Phi : R/ANN_R(x) \to Rx : \overline{b} := b + ANN_R(x) \mapsto bx$, we will first prove the well-definedness and injectivity of this map: $ax = \Phi(\overline{a}) = \Phi(\overline{b}) = bx$ is equivalent to (a-b)x = 0, that is $a-b \in ANN_R(x)$ or in other words $\overline{a} = a + ANN_R(x) = b + ANN_R(x) = \overline{b}$. The surjectivity of Φ is clear, as any $b \in R$ is allowed. And Φ also is a homomorphism of R-modules, as by definition of the algebraic operations of $R/ANN_R(x)$ we have $\Phi(\overline{a} + \overline{b}) = \Phi(\overline{a+b}) = (a+b)x = (ax) + (bx) = \Phi(\overline{a}) + \Phi(\overline{b})$ and $\Phi(a\overline{b}) = \Phi(\overline{ab}) = (ab)x = a(bx) = a\Phi(\overline{b})$. NOTA that this claim could have also been proved by regarding the epimorphism $\varphi : R \to$ $Rx : b \mapsto bx$, noting that its kernel is $kn (\varphi) = ANN_R(x)$ and invoking the first isomorphism theorem of R-modules to get Φ .
- (iii) As $R \neq 0$ we have $1 \neq 0$ and as also $1 \diamond 0 = 0$ we already have $0 \in \operatorname{TOR} M$. Now consider any two $x, y \in \operatorname{TOR} M$, that is there are some $0 \neq a, b \in R$ such that ax = 0 and by = 0. As R is an integral domain we also get $ab \neq 0$. Now compute $(ab)(x+y) = (ab)x+(ab)y = (ba)x + (ab)y = b(ax) + a(by) = b \diamond 0 + a \diamond 0 = 0 + 0 = 0$. That is (ab)(x+y) = 0 and hence $x + y \in M$, as $ab \neq 0$. Finally consider any $r \in M$, then we need to show $rx \in \operatorname{TOR} M$. But this is clear from $a(rx) = (ar)x = (ra)x = r(ax) = r \diamond 0 = 0$.

- (iii) Let us abbreviate T := TOR M, now consider any $x + T \in \text{TOR } (M/T)$. That is there is some $0 \neq a \in R$ such that (ax) + T = a(x+T) = 0 + T. This is just $ax \in T$, that is there is some $0 \neq b \in R$, such that (ba)x = b(ax) = 0. As R is an integral domain, we get $ba \neq 0$ and this means $x \in T$, such that x + T = 0 + T. Thus we have just proved $\text{TOR } (M/T) \subseteq \{0 + T\} = \{0\}$ and the converse containment is clear.
- (iv) (a) \implies (c): Consider any $a \in R$ and any $x \in M$ such that ax = 0. If a = 0, then we are done, else we have $x \in \text{TOR } M = \{0\}$ (by definition of TOR M, as ax = 0 and $a \neq 0$) and this is x = 0 again.
- (iv) (c) \implies (b): Consider any $a \in \mathbb{ZD}_R(M)$, that is there is some $x \in M$ such that $x \neq 0$ and ax = 0. Thus by assumption (c) we find a = 0, and as a has been arbitrary, this means $\mathbb{ZD}_R(M) \subseteq \{0\}$, as claimed.
- (iv) (b) \implies (a): As $R \neq 0$ we have $1 \neq 0$ and as $1 \diamond 0 = 0$ this implies $0 \in \text{TOR } M$. Conversely consider any $x \in \text{TOR } M$, that is there is some $a \in R$ such that $a \neq 0$ and ax = 0. Suppose we had $x \neq 0$, then $a \in \text{ZD}_R(M) \subseteq \{0\}$ (by definition of $\text{ZD}_R(M)$, as $x \neq 0$ and ax = 0) which is a = 0 again. But as $a \neq 0$ this is a contradiction. Thus we necessarily have x = 0 and as x has been arbitrary this means $\text{TOR } M \subseteq \{0\}$, as well.
- (v) Let us abbreviate $P := \langle X \rangle_{m}$, then by definition it is clear that $X \subseteq P$ and hence $ANN_R(P) \subseteq ANN_R(X)$. For the converse inclusion consider any $a \in ANN_R(X)$, then we have to show $a \in ANN_R(P)$. That is ap = 0for any $p \in P$. By (3.11) any $p \in P$ is given to be $p = \sum_i a_i x_i$ for some $a_i \in R$ and $x_i \in X$. Therefore $ap = \sum_i (aa_i)x_i = \sum_i a_i(ax_i) = \sum_i a_i \diamond 0 = 0$ as R is commutative.
- (vi) First suppose that x = 0, then ax = a0 = 0 is clear for any $a \in S$ and hence $ANN_S(x) = S$. Secondly consider $x \neq 0$ and $a \in ANN_S(x)$, that is ax = 0. Suppose we had $a \neq 0$, too, then (as S is a skew-field) there was some $a^{-1} \in S$ such that $a^{-1}a = 1$. Then we would be able to compute $x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0 = 0$, a contradiction to $x \neq 0$, such that a = 0 and therefore $ANN_S(x) = 0$.
- (vii) Let $\mathfrak{p} = ANN_R(x)$ be a maximal annihilator ideal of M with $\mathfrak{p} \neq R$. Further consider any $a, b \in R$ with $ab \in \mathfrak{p}$ but $b \notin \mathfrak{p}$, then it remains to verify $a \in \mathfrak{p}$. As $b \notin \mathfrak{p}$ we have $bx \neq 0$. Now consider $\mathfrak{a} := ANN_R(bx)$, as $bx \neq 0$ we have $1 \notin \mathfrak{a}$ and hence $\mathfrak{a} \neq R$. Also if $p \in \mathfrak{p}$, then p(bx) = b(px) = b0 = 0 and hence $p \in \mathfrak{a}$, which means $\mathfrak{p} \subseteq \mathfrak{a}$. But by maximality of \mathfrak{p} this is $\mathfrak{p} = \mathfrak{a}$. Now as $ab \in \mathfrak{p}$ we have a(bx) = (ab)x = 0such that $a \in \mathfrak{a} = \mathfrak{p}$, as has been claimed.

Proof of (3.17):

- Let us first prove the identity part in the modular rule, starting with $(Q \cap U) + P \subseteq Q \cap (P+U)$. Thus we consider any $x \in Q \cap U$ and $p \in P$ and have to verify $x + p \in Q \cap (P+U)$. As $x \in Q$ and $p \in P \subseteq Q$ we have $x + p \in Q$. And as also $x \in U$ we have $x + p \in U + P$ hence the claim. Conversely for $(Q \cap U) + P \supseteq Q \cap (P+U)$ we are given any $p \in P$ and $u \in U$ such that $q := p + u \in Q$ and we have to verify $p + u \in (Q \cap U) + P$. But as u = q p and $p, q \in Q$ we find $u \in Q$ and hence $u \in Q \cap U$. And this already is $p + u = u + p \in (Q \cap U) + P$.
- So it ramains to verify the implication in the modular rule. As $P \subseteq Q$ by assumption it remains to prove $Q \subseteq P$. Thus consider any $q \in Q$, then in particular $q \in Q + U = P + U$. That is there are $p \in P$ and $u \in U$ such that q = p + u. And as $p \in P \subseteq Q$ this yields $u = q p \in Q$, such that $u \in Q \cap U = P \cap U$. In particular $u \in P$ and hence $q = p + u \in P$, as claimed.

Proof of (1.51):

- (i) Clearly $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$ and subtracting $\varphi(0_R)$ from this equation (i.e. adding $-\varphi(0_R)$ to both sides of the equation) we find $0_S = \varphi(0_R)$. Hence $\varphi(a) + \varphi(-a) = \varphi(a-a) = \varphi(0_R) = 0_S$ which proves that $\varphi(-a)$ is the negative $-\varphi(a)$.
- (ii) Analogous to the above we find $1_S = \varphi(1_R) = \varphi(uu^{-1}) = \varphi(u)\varphi(u^{-1})$ and $1_S = \varphi(1_R) = \varphi(u^{-1}u) = \varphi(u^{-1})\varphi(u)$ which proves that $\varphi(u^{-1})$ is the inverse $\varphi(u)^{-1}$.
- (iii) If $a, b \in R$ then $\psi\varphi(a+b) = \psi(\varphi(a) + \psi(b)) = \psi\varphi(a) + \psi\varphi(b)$ and likewise for the multiplication. Hence $\psi\varphi$ is a homomorphism of semirings again. And in the case of rings and homomorphisms of rings we also get $\psi\varphi(1_R) = \psi(1_S) = 1_T$.
- (iv) Consider any $x, y \in S$, as Φ is surjective there are $a, b \in R$ such that $x = \Phi(a)$ and $y = \Phi(b)$. Now $\Phi^{-1}(x+y) = \Phi^{-1}(\Phi(a) + \Phi(b)) = \Phi^{-1}\Phi(a+b) = a+b = \Phi^{-1}(x) + \Phi^{-1}(y)$. Likewise we find $\Phi^{-1}(xy) = \Phi^{-1}(x)\Phi^{-1}(y)$. And if Φ is a homomorphism of rings, then $\Phi^{-1}(1_S) = 1_R$ is clear from $\Phi(1_R) = 1_S$.
- (v) Since $\operatorname{im}(\varphi) = \varphi(R)$ the first statement is clear from (vi) by taking P = R. So we only have to prove, that $\operatorname{kn}(\varphi)$ is an ideal of R. First of all we have $0_R \in \operatorname{kn}(\varphi)$ since $\varphi(0_R) = 0_S$ by (i). And if a, $b \in \operatorname{kn}(\varphi)$ then $\varphi(a + b) = \varphi(a) + \varphi(b) = 0_S + 0_S = 0_S$ and hence

 $a + b \in \operatorname{kn}(\varphi)$. Analogously $\varphi(-a) = -\varphi(a) = -0_S = 0_S$ yields $-a \in \operatorname{kn}(\varphi)$. Now let $a \in \operatorname{kn}(\varphi)$ again and let $b \in R$ be arbitary. Then $\varphi(ab) = \varphi(a)\varphi(b) = 0_S\varphi(b) = 0_S$ and hence $ab \in \operatorname{kn}(\varphi)$ again. Likewise $\varphi(ba) = \varphi(b)\varphi(a) = \varphi(b)0_S = 0_S$ which yields $ba \in \operatorname{kn}(\varphi)$.

- (vi) As P is a sub-semi-ring of R we have $0_R \in P$ and therefore $0_S = \varphi(0_R) \in \varphi(P)$. Now assume that $x = \varphi(a)$ and $y = \varphi(b) \in \varphi(P)$ for some $a, b \in P$. As P is a sub-semi-ring of R we have a + b, -a and $ab \in P$ again. And hence $x + y = \varphi(a) + \varphi(b) = \varphi(a + b) \in \varphi(P)$, $-x = -\varphi(a) = \varphi(-a) \in \varphi(P)$ and $xy = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(P)$. Thus we have proved that $\varphi(P) \leq_{\rm s} R$ is a sub-semi-ring again. And if R and S even are rings, P is a subring of R and φ is a homomorphism of rings, then also $1_S = \varphi(1_R) \in \varphi(P)$ as $1_R \in P$.
- (vi) And as Q is a sub-semi-ring of S we have $0_S \in Q$ and therefore $0_S = \varphi(0_R)$ implies $0_R \in \varphi^{-1}(Q)$. Now suppose $a, b \in \varphi^{-1}(Q)$, that is $\varphi(a), \varphi(b) \in Q$. Then $\varphi(a+b) = \varphi(a) + \varphi(b), \varphi(-a) = -\varphi(a)$ and $\varphi(ab) = \varphi(a)\varphi(b) \in Q$, as $Q \leq_{\mathrm{s}} S$. This means that a+b, -a and $ab \in \varphi^{-1}(Q)$ and hence $\varphi^{-1}(Q) \leq_{\mathrm{s}} S$ is a sub-semi-ring of S. And in the case of rings we also find $1_R \in \varphi^{-1}(Q)$ as in (vi) above.
- (vii) First assume that $\mathfrak{b} \leq_{\mathrm{m}} S$ is a left-ideal of S. We have already proved in (vi) that $\varphi^{-1}(\mathfrak{b}) \leq_{\mathrm{s}} S$ is a sub-semi-ring of S (since $Q := \mathfrak{b} \leq_{\mathrm{s}} R$). Thus it only remains to verify the following: consider any $a \in R$ and $b \in \varphi^{-1}(\mathfrak{b})$. Then $\varphi(b) \in \mathfrak{b}$ and as $\mathfrak{b} \leq_{\mathrm{m}} S$ we hence get $\varphi(ab) = \varphi(a)\varphi(b) \in \mathfrak{b}$. Thus $ab \in \varphi^{-1}(\mathfrak{b})$ which means that $\varphi^{-1}(\mathfrak{b})$ is a leftideal of R again. And in the case that $\mathfrak{b} \leq_{\mathrm{i}} S$ even is an ideal, then by the same reasoning $\varphi(ba) = \varphi(b)\varphi(a) \in \mathfrak{b}$ and hence $ba \in \varphi^{-1}(\mathfrak{b})$.
- (vii) Next assume that $\mathfrak{a} \leq_{\mathrm{m}} R$ is a left-ideal of R and that φ is surjective. Then $\varphi(\mathfrak{a}) \leq_{\mathrm{s}} S$ is a sub-semi-ring of S by (vi) for $P := \mathfrak{a} \leq_{\mathrm{s}} R$. Thus it again remains to prove the following property: Consider any $y \in S$ and $x = \varphi(a) \in \varphi(\mathfrak{a})$ (where $a \in \mathfrak{a}$). As φ is surjective there is some $b \in R$ with $y = \varphi(b)$. And as $ba \in \mathfrak{a}$ we hence find $yx = \varphi(b)\varphi(a) = \varphi(ba) \in \varphi(\mathfrak{a})$. Thus $\varphi(\mathfrak{a}) \leq_{\mathrm{m}} S$ is a left ideal of S. And in the case that $\mathfrak{a} \leq_{\mathrm{i}} R$ even is an ideal, then by the same reasoning $xy = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(\mathfrak{a})$.
- (viii) Let $\varphi : R \to S$ be a homomorphism of semi-rings. If $\varphi(1_R) = 0_S$ then for any $a \in R$ we get $\varphi(a) = \varphi(1_R a) = 0_S \varphi(a) = 0_S$ and hence $\varphi = 0$. Else we have $\varphi(1_R) = \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R)$ and dividing by $0 \neq \varphi(1_R)$ (i.e. multiplying by $\varphi(1_R)^{-1}$) we hence find $1_S = \varphi(1_R)$.
 - (ix) As we have seen in (v) $\operatorname{kn}(\varphi) \leq_i R$ is an ideal of R. And as R is a skew-field, it has precisely two ideals: $\{0\}$ and R. In the first

case $\operatorname{kn}(\varphi) = R$ we trivially have $\varphi = 0$. And in the second case $\operatorname{kn}(\varphi) = \{0\}$ we will soon see, that φ is injective.

Proof of (1.53):

- (i) By definition φ is surjective iff any $x \in S$ can be reached as $x = \varphi(a)$ for some $a \in R$. And this is just $S \subseteq \varphi(R) = \operatorname{im}(\varphi)$, or equivalently $S = \operatorname{im}(\varphi)$. And if φ is injective then there can be at most one $a \in R$ such that $\varphi(a) = 0_S$. And as $\varphi(0_R) = 0_S$ this implies $\operatorname{kn}(\varphi) = \{0_R\}$. Conversely suppose $\operatorname{kn}(\varphi) = \{0_R\}$ and consider $a, b \in R$ with $\varphi(a) = \varphi(b)$. Then $0_S = \varphi(a) - \varphi(b) = \varphi(a - b)$. Hence $a - b \in \operatorname{kn}(\varphi)$ such that $a - b = 0_R$ by assumption. Hence φ is injective.
- (ii) The implication (a) \implies (b) is clear: just let $\Psi := \Phi^{-1}$ then we have already seen, that Ψ is a homomorphism of (semi-)rings again. And the converse (b) \implies (a) is clear (in particular Ψ is an inverse mapping of Φ). The implication (b) \implies (c) is trivial - just let $\alpha := \Psi$ and $\beta := \Psi$. And for the converse (c) \implies (b) we simply compute: $\alpha = \alpha \mathbb{1}_S = \alpha(\Phi\beta) = (\alpha\Phi)\beta = \mathbb{1}_R\beta = \beta$. Thus letting $\Psi := \alpha = \beta$ we are done.
- (iii) Suppose R is a ring, then let $f := \Phi(1_R)$. If now $x \in S$ is any element then we choose $a \in R$ such that $x = \Phi(a)$. And thereby we get $fx = \Phi(1_R)\Phi(a) = \Phi(1_R a) = \Phi(a) = x$ and likewise xf = x. Hence $f = 1_S$ is the unit element of S and hence S is a ring, too. Further we have seen $\Phi(1_R) = 1_S$ such that Φ is a homomorphism of rings.

Suppose S is a ring, then let $e := \Phi^{-1}(1_S)$. If now $a \in R$ is any element, then $\Phi(a) = \Phi(a)1_S = \Phi(a)\Phi(e) = \Phi(ae)$ and hence a = ae. Likewise we see ea = a and hence $e = 1_R$ is the unit element of R. Hence R is a ring, too and $\Phi(1_R) = 1_S$ is a homomorphism of rings.

(iv) Clearly the identity map $1\!\!1_R : R \to R : a \mapsto a$ is both, bijective and a homomorphism of (semi-)rings for any (semi-)ring $(R, +, \cdot)$. But this is nothing but the claim $1\!\!1_R : R \cong_{\mathbf{r}} R$. And if $\Phi : R \to S$ is an isomorphism of (semi-)rings, then Φ^{-1} is a bijective (this is clear) homomorphism of (semi-)rings again (this has already been proved). Hence the second implication. And if both $\Phi : R \cong_{\mathbf{r}} S$ and $\Psi : S \cong_{\mathbf{r}} T$ then $\Psi\Phi$ is bijective and a homomorphism of (semi-)rings (as Φ and Ψ are such). And this has been the third implication.

Proof of (1.56):

(i) We first need to check, that $\tilde{\varphi}$ is well-defined: thus consider $b, c \in R$ such that $b + \mathfrak{a} = c + \mathfrak{a}$. That is $c - b \in \mathfrak{a} \subseteq \operatorname{kn} \varphi$. And hence $0 = \varphi(c - b) = \varphi(c) - \varphi(b)$ which is the well-definedness $\varphi(b) = \varphi(c)$. Now it is straightforward to see, that $\tilde{\varphi}$ also is a homomorphism

$$\begin{split} \widetilde{\varphi}\Big((b+\mathfrak{a})+(c+\mathfrak{a})\Big) &= \widetilde{\varphi}\Big((b+c)+\mathfrak{a}\Big) &= \varphi(b+c) \\ &= \varphi(b)+\varphi(c) &= \widetilde{\varphi}(b+\mathfrak{a})+\widetilde{\varphi}(b+\mathfrak{a}) \\ \widetilde{\varphi}\Big((b+\mathfrak{a})(c+\mathfrak{a})\Big) &= \widetilde{\varphi}\Big((bc)+\mathfrak{a}\Big) &= \varphi(bc) \\ &= \varphi(b)\varphi(c) &= \widetilde{\varphi}(b+\mathfrak{a})\widetilde{\varphi}(b+\mathfrak{a}) \end{split}$$

Thus $\tilde{\varphi}$ always is a homomorphism of semi-rings. And if if R and S even are rings, then R/\mathfrak{a} is a ring as well with the unit element $1 + \mathfrak{a}$. Thus if $\varphi(1) = 1$ is a ring-homomorphism, then $\tilde{\varphi}(1 + \mathfrak{a}) = \varphi(1) = 1$ is a ring-homomorphism, too.

$$\operatorname{im} \Phi = \Phi\left(\frac{R}{\mathfrak{a}}\right) = \varphi(R) = \operatorname{im} \varphi$$

Hence the mapping $\Phi: R/\mathfrak{a} \to \operatorname{im}(\varphi)$ is surjective by definition. But it also is injective (and hence an isomorphism) due, to

$$\varphi(a) = \varphi(b) \iff 0 = \varphi(a) - \varphi(b) = \varphi(a - b)$$
$$\iff a - b \in \operatorname{kn}(\varphi)$$
$$\iff a + \operatorname{kn}(\varphi) = b + \operatorname{kn}(\varphi)$$

(iii) We will first prove that $\mathfrak{b} + R \leq_{\mathrm{r}} S$ is a subring of S: clearly we have $0 = 0 + 0 \in \mathfrak{b} + R$ and (if R is a subring of S) $1 = 0 + 1 \in \mathfrak{b} + R$. Now let b + a and $d + c \in \mathfrak{b} + R$, then

$$(b+a) + (d+a) = (b+d) + (a+c) \in \mathfrak{b} + R$$

$$-(b+a) = (-b) + (-a) \in \mathfrak{b} + R$$

$$(b+a)(d+c) = (bd+bc+ad) + ac \in \mathfrak{b} + R$$

And hence $\mathfrak{b} + R$ is a subring of S. And as $\mathfrak{b} \leq_{\mathbf{i}} R$ is an ideal of S with $\mathfrak{b} \subseteq \mathfrak{b} + R$ it trivially also is an ideal $\mathfrak{b} \leq_{\mathbf{i}} \mathfrak{b} + R$. Now let us denote the restriction of the canonical epimorphism $\sigma : S \to S/\mathfrak{b}$ to R by

$$\varrho : R \to S/\mathfrak{b} : a \mapsto a + \mathfrak{b}$$

Then ρ is a homomorphism with kernel kn $(\rho) = \operatorname{kn}(\sigma) \cap R = \mathfrak{b} \cap R$. In particular this proves that $\mathfrak{b} \cap R \leq_{i} R$ is an ideal of R (as it is the kernel of a homomorphism). And it is straightforward to see, that $\operatorname{im}(\varphi) = (\mathfrak{b} + R)/\mathfrak{b}$. [For any $a \in R$ we have $a \in \mathfrak{b} + R$ and hence $\varrho(a) \in (\mathfrak{b} + R)/\mathfrak{b}$. And if conversely $x = b + a \in \mathfrak{b} + R$ then $\varrho(a) = a + \mathfrak{b} = x + \mathfrak{b}$]. Thus we may apply the first isomorphism theorem (ii) to obtain

$$\frac{R}{\ln(\varrho)} = \frac{R}{\mathfrak{b} \cap R} \cong_{\mathrm{r}} \operatorname{im}(\varrho) = \frac{\mathfrak{b} + R}{\mathfrak{b} \cap R}$$
$$a + \mathfrak{b} \cap R \quad \mapsto \quad \varrho(a) = a + \mathfrak{b}$$

(iv) Suppose c and $d \in R$ with $c + \mathfrak{a} = d + \mathfrak{a}$. Then $c - d \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $c + \mathfrak{b} = d + \mathfrak{b}$. Therfore we may define the following mapping (which clearly is a homomorphism of (semi-)rings)

$$\varphi : {R/\mathfrak{g}} \to {R/\mathfrak{g}} : c + \mathfrak{a} \mapsto c + \mathfrak{b}$$

And clearly kn (φ) = { $b + \mathfrak{a} \mid b + \mathfrak{b} = 0 + \mathfrak{b}$ } = { $b + \mathfrak{a} \mid b \in \mathfrak{b}$ } = $\mathfrak{b}/\mathfrak{a}$. Hence we immediately obtain (iv) from the first isomorphism theorem.

Proof of (1.60):

- (1) We will first prove that $\mathfrak{a} \oplus \mathfrak{b} \leq_{i} R \oplus S$ is an ideal. As \mathfrak{a} and \mathfrak{b} are ideals we have $0 \in \mathfrak{a}$ and $0 \in \mathfrak{b}$ and hence $0 = (0,0) \in \mathfrak{a} \oplus \mathfrak{b}$. Now consider (a,b) and $(p,q) \in \mathfrak{a} \oplus \mathfrak{b}$. Then we have $a + p \in \mathfrak{a}, b + q \in \mathfrak{b}$ and hence $(a,b) + (p,q) = (a+p,b+q) \in \mathfrak{a} \oplus \mathfrak{b}$. Finally consider any $(r,s) \in R \oplus S$ then $ra \in \mathfrak{a}$ and $sb \in \mathfrak{b}$ such that $(r,s)(a,b) = (ra,sb) \in \mathfrak{a} \oplus \mathfrak{b}$ again. And as R and S are commutative rings, so is $R \oplus S$ such that this has been enough to guarantee that $\mathfrak{a} \oplus \mathfrak{b}$ is an ideal of $R \oplus S$.
- (2) Next we will prove 𝔅 = 𝔅(𝔅) ⊕ σ(𝔅). If (a, b) ∈ 𝔅 then it is clear that a = 𝔅(a, b) ∈ 𝔅(𝔅) and b = σ(a, b) ∈ σ(𝔅) such that (a, b) ∈ 𝔅(𝔅) ⊕ σ(𝔅). Conversely if (a, b) ∈ 𝔅(𝔅) ⊕ σ(𝔅) then there are some r ∈ R and s ∈ S such that (a, s) ∈ 𝔅 and (r, b) ∈ 𝔅. But as 𝔅 is an ideal we also have (a, 0) = (1, 0)(a, s) ∈ 𝔅 again and analogously (0, b) ∈ 𝔅. Thereby (a, b) = (a, 0) + (0, b) ∈ 𝔅 proving the equality.
- (3) Now we are ready to prove ideal $R \oplus S = \{ \mathfrak{a} \oplus \mathfrak{b} \mid \mathfrak{a} \leq_{i} R, \mathfrak{b} \leq_{i} S \}$. We have already seen in (1) that $\mathfrak{a} \oplus \mathfrak{b}$ is an ideal of $R \oplus S$ (supposed \mathfrak{a} and \mathfrak{b} are ideals). Conversely if $\mathfrak{u} \leq_{i} R \oplus S$ is an ideal, then we let $\mathfrak{a} := \varrho(\mathfrak{u})$ and $\mathfrak{b} := \sigma(\mathfrak{u})$. Then $\mathfrak{a} \leq_{i} R$ and $\mathfrak{b} \leq_{i} S$ are ideals, since ϱ and σ are surjective homomorphisms. And $\mathfrak{u} = \mathfrak{a} \oplus \mathfrak{b}$ by (2).
- (4) Now let $\mathfrak{a} \leq_{i} R$ and $\mathfrak{b} \leq_{i} S$. Then we will prove $\sqrt{\mathfrak{a} \oplus \mathfrak{b}} = \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}}$. First suppose that $(a, b)^{k} = (a^{k}, b^{k}) \in \mathfrak{a} \oplus \mathfrak{b}$ for some $k \in \mathbb{N}$. Then $a^{k} \in \mathfrak{a}$

and $b^k \in \mathfrak{b}$ such that $a \in \sqrt{\mathfrak{a}}$ and $b \in \sqrt{\mathfrak{b}}$ and thereby $(a, b) \in \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}}$. Conversely suppose $a^k \in \mathfrak{a}$ and $b^l \in \mathfrak{b}$ for some $k, l \in \mathbb{N}$. Then we define $n := \max\{k, l\}$ and thereby get $(a, b)^n = (a^n, b^n) \in \mathfrak{a} \oplus \mathfrak{b}$. And this means that (a, b) is contained in the radical of $\mathfrak{a} \oplus \mathfrak{b}$ again.

(5) This enables us to prove srad $R \oplus S = \{ \mathfrak{a} \oplus \mathfrak{b} \mid \mathfrak{a} = \sqrt{\mathfrak{a}}, \ \mathfrak{b} = \sqrt{\mathfrak{b}} \}$. First suppose that $\mathfrak{u} \leq_{i} R \oplus S$ is a radical ideal and let $\mathfrak{a} := \varrho(\mathfrak{u})$ and $\mathfrak{b} := \sigma(\mathfrak{u})$ again. Then by (4) we may compute

$$\mathfrak{a} \oplus \mathfrak{b} = \mathfrak{u} = \sqrt{\mathfrak{u}} = \sqrt{\mathfrak{a} \oplus \mathfrak{b}} = \sqrt{\mathfrak{a} \oplus \sqrt{\mathfrak{b}}}$$

This proves that $\mathfrak{a} = \sqrt{\mathfrak{a}}$ and $\mathfrak{b} = \sqrt{\mathfrak{b}}$ are radical ideals of R and S respectively. And if conversely \mathfrak{a} and \mathfrak{b} are radical ideals then $\mathfrak{a} \oplus \mathfrak{b}$ is a radical ideal of $R \oplus S$ by virtue of

$$\mathfrak{a} \oplus \mathfrak{b} = \sqrt{\mathfrak{a}} \oplus \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} \oplus \mathfrak{b}}$$

- (6) Next we will prove spec $R \oplus S = \{\mathfrak{p} \oplus S\} \cup \{R \oplus \mathfrak{q}\}$. If $\mathfrak{p} \leq_i R$ is a prime ideal then we have already proved $\mathfrak{P} \oplus S \leq_{i} R \oplus S$ in (1). And it is clear that $\mathfrak{p} \oplus S \neq R \oplus S$ as $(1,0) \notin \mathfrak{p} \oplus S$. Thus suppose $(a,b)(p,q) = (ap,bq) \in \mathfrak{p} \oplus S$. Then $ap \in \mathfrak{p}$ and as \mathfrak{p} is prime this means $a \in \mathfrak{p}$ or $p \in \mathfrak{p}$. Without loss of generality we may take $p \in \mathfrak{p}$ and thereby $(p,q) \in \mathfrak{p} \oplus S$. Altogether we have seen that $\mathfrak{p} \oplus S$ is a prime ideal of $R \oplus S$. And analogously one may prove that $R \oplus \mathfrak{q}$ is prime, supposed $\mathfrak{q} \leq_{\mathbf{i}} S$ is prime. Thus conversely consider a prime ideal $\mathfrak{u} \leq R \oplus S$ let $\mathfrak{p} := \varrho(\mathfrak{u})$ and $\mathfrak{q} := \sigma(\mathfrak{u})$. Clearly $(1,0)(0,1) = (0,0) \in \mathfrak{u}$. And as \mathfrak{u} is prime this means $(1,0) \in \mathfrak{u}$ or $(0,1) \in \mathfrak{u}$. We will assume $(0,1) \in \mathfrak{u}$, as the other case can be dealt with in complete analogy. Then $1 \in \mathfrak{q}$ and hence $\mathfrak{q} = S$. That is $\mathfrak{u} = \mathfrak{p} \oplus S$ and as $\mathfrak{u} \neq R \oplus S$ this means $\mathfrak{p} \neq R$. Thus consider a and $p \in R$ such that $ap \in \mathfrak{p}$. Then $(a,0)(p,0) = (ap,0) \in \mathfrak{p} \oplus S = \mathfrak{u}$. And as \mathfrak{u} is prime this means $(a,0) \in \mathfrak{u}$ or $(p,0) \in \mathfrak{u}$ (which we assume w.l.o.g.). Thereby $p \in \mathfrak{p}$, altogether we have found that $\mathfrak{u} = \mathfrak{p} \oplus S$ for some prime ideal $\mathfrak{p} \leq_i R$.
- (7) It remains to prove smax R ⊕ S = {𝔅 ⊕ S} ∪ {R ⊕ 𝔅}. Thus consider a maximal ideal 𝔅 ≤_𝔅 R and suppose 𝔅 ⊕ S ⊆ 𝔅 ≤_𝔅 R ⊕ S. Then S = σ(𝔅 ⊕ S) ⊆ 𝔅 := σ(𝔅) ≤_𝔅 S and hence 𝔅 = S. Likewise we find 𝔅 = 𝔅(𝔅 ⊕ S) ⊆ 𝔅 := 𝔅(𝔅) ≤_𝔅 R and as 𝔅 is maximal this implies 𝔅 = 𝔅(𝔅 ⊕ S) ⊆ 𝔅 := 𝔅(𝔅) ≤_𝔅 R and as 𝔅 is maximal this implies 𝔅 = 𝔅 or 𝔅 = R. Thus we get 𝔅 = 𝔅 ⊕ 𝔅 = 𝔅 ⊕ S or 𝔅 = 𝔅 ⊕ 𝔅 = R ⊕ S. And this means that 𝔅 ⊕ 𝔅 is a maximal ideal of R ⊕ S. Likewise one can see that R ⊕ 𝔅 is a maximal ideal for any 𝔅 ≤_𝔅 S maximal. Conversely consider a maximal ideal 𝔅 ≤_𝔅 R ⊕ S. In particular 𝔅 is prime and hence - by (6) - 𝔅 = 𝔅 ⊕ 𝔅 or 𝔅 = R⊕ 𝔅 for some prime ideal 𝔅 ≤_𝔅 R or 𝔅 ≤_𝔅 S respectively. We only regard the case 𝔅 = 𝔅 ⊕ 𝔅 again, as the other is completely analogous. Thus consider some ideal

 $\mathfrak{m} \subseteq \mathfrak{a} \leq_{i} R$, then $\mathfrak{u} = \mathfrak{m} \oplus S \subseteq \mathfrak{a} \oplus S \leq_{i} R \oplus S$. By maximality of \mathfrak{u} that is $\mathfrak{u} = \mathfrak{m} \oplus S = \mathfrak{a} \oplus S$ or $\mathfrak{a} \oplus S = R \oplus S$. Again this yields $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = R$ and this means that \mathfrak{m} is maximal.

- (i) From $1 = e + f \in \mathfrak{a} + \mathfrak{b} \leq_{i} R$ it is clear that $\mathfrak{a} + \mathfrak{b} = R$. Now consider any $x \in \mathfrak{a} \cap \mathfrak{b}$. That is there are a and $b \in R$ such that x = ae = bf. Then we get xe = (bf)e = b(fe) = 0 and xf = (ae)f = a(ef) = 0. And thereby x = x1 = x(e+f) = xe + xf = 0 such that $\mathfrak{a} \cap \mathfrak{b} = \{0\}$.
- (ii) It is clear that Φ : x → (x + 𝔅, x + 𝔅) is a well-defined homomorphism of rings (as it fibers into the canonical epimorphisms x → x + 𝔅 and x → x + 𝔅). Now suppose (x + 𝔅, x + 𝔅) = Φ(x) = 0 = (0 + 𝔅, 0 + 𝔅). This means x ∈ 𝔅 and x ∈ 𝔅 and hence x ∈ 𝔅 ∩ 𝔅 = {0}. Thus we have x = 0 which implies kn (Φ) = {0}, which means that Φ is injective. It remains to prove, that Φ also is surjective: Since 𝔅 + 𝔅 = R there are some e ∈ 𝔅 and f ∈ 𝔅 such that e + f = 1. Now suppose we are given any (y + 𝔅, z + 𝔅). Then let x := yf + ze and compute

$$\begin{split} \Phi(x) &= (yf + ze + \mathfrak{a}, yf + ze + \mathfrak{b}) \\ &= (yf + \mathfrak{a}, ze + \mathfrak{b}) \\ &= (yf + ye + \mathfrak{a}, ze + zf + \mathfrak{b}) \\ &= (y(f + e) + \mathfrak{a}, z(e + f) + \mathfrak{b}) \\ &= (y + \mathfrak{a}, z + \mathfrak{b}) \end{split}$$

(iii) We will now prove the chinese remainder theorem in several steps. (1) Let us first consider the following homomorphism of rings

$$\varphi : R \to \bigoplus_{i=1}^n R / \mathfrak{a}_i : x \mapsto (x + \mathfrak{a}_i)$$

We now compute the kernel of $\varphi: \varphi(x) = 0 = (0 + \mathfrak{a}_i)$ holds true if and only if for any $i \in 1 \dots n$ we have $x + \mathfrak{a}_i = 0 + \mathfrak{a}_i$. And of course this is equivalent, to $x \in \mathfrak{a}_i$ for any $i \in 1 \dots n$. And again this can be put as $x \in \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$. Hence we found kn $(\varphi) = \mathfrak{a}$. Now we aim for the surjectivity of $\varphi: (2)$ As a first approach we prove the existence of a solution $x \in R$ of the system $\varphi(x) = (1 + \mathfrak{a}_1, 0 + \mathfrak{a}_2, \dots, 0 + \mathfrak{a}_n)$. Since $\mathfrak{a}_1 + \mathfrak{a}_j = R$ for any $j \in 2 \dots n$ we also find $\mathfrak{a}_1 + \mathfrak{a}_2 \dots \mathfrak{a}_n = R$ due to (1.39.(iii)). That is there are elements $e_1 \in \mathfrak{a}_1$ and $f_1 \in \mathfrak{a}_2 \dots \mathfrak{a}_n$ such that $e_1 + f_1 = 1$. Hence we find $f_1 + \mathfrak{a}_j = 0 + \mathfrak{a}_j$ for any $j \in 2 \dots n$. And also $f_1 + \mathfrak{a}_1 = (1 - e_1) + \mathfrak{a}_1 = 1 + \mathfrak{a}_1$. That is $x := f_1$ does the

Г		
L		J

trick. (3) Analogous to (2) we find $f_2, \ldots, f_n \in \mathbb{R}$ such that for any $j \in 1 \ldots n$ we obtain the system

$$\varphi(f_j) = (\delta_{i,j} + \mathfrak{a}_i)$$

(4) Thus if we are now given any $a_1, \ldots, a_n \in R$ then we let us define $x := a_1 f_1 + \cdots + a_n f_n$ and we thereby obtain

$$x + \mathfrak{a}_i = \sum_{j=1}^n a_j f_j + \mathfrak{a}_i = \sum_{j=1}^n a_j \delta_{i,j} + \mathfrak{a}_i = a_j + \mathfrak{a}_i$$

Hence $\varphi(x) = (a_i + \mathfrak{a}_i)$ and as the a_i have been arbitrary this means that φ is surjective. (5) Thus (1.56.(ii)) yields the desired isomorphy.

Proof of (3.18):

- We will first verify that the exterior direct product P := ∏_i M_i is an R-module again (under the operations given). The well-definedness of the operations is clear. Thus consider x = (x_i), y = (y_i) and z = (z_i) ∈ P. Then x + (y + z) = (x_i + (y_i + z_i)) = ((x_i + y_i) + z_i) = (x + y) + z which is the associativity. Likewise x + y = (x_i + y_i) = (y_i + x_i) = y + x, which is the commutativity. Letting 0 := (0_i), where 0_i ∈ M_i is the zero-element, we find x + 0 = (x_i + 0_i) = (x_i) = x, such that 0 ∈ P is the zero-element. And the negative of x is x̄ = (-x_i) ∈ P, as x + x̄ = (x_i + (-x_i)) = (0_i) = 0. Now consider any a, b ∈ R then a(x + y) = (a(x_i + y_i)) = ((ax_i) + (ay_i)) = (ax_i) + (ay_i) = (ax) + (ay). Likewise (a + b)x = ((a + b)x_i) = ((ax_i) + (bx_i)) = (ax_i) + (bx_i) = (ax) + (bx) and (ab)x = ((ab)x_i) = (a(bx_i)) = a(bx_i) = a(bx). Finally 1x = (1x_i) = (x_i) = x, such that altogether P is an R-module again.
- Let us now verify that the direct sum $S := \bigoplus_i M_i$ is an *R*-submodule of the direct product *P*. Thus we only have to prove that *S* is closed under the operations of *P*. However for any $a \in R$ and any $x, y \in S$ it is clear that $\operatorname{supp}(ax) \subseteq \operatorname{supp}(x)$ and $\operatorname{supp}(x+y) \subseteq \operatorname{supp}(x) \cup \operatorname{supp}(y)$. Hence $\#\operatorname{supp}(ax) \leq \#\operatorname{supp}(x) < \infty$ and $\#\operatorname{supp}(x+y) \leq \#\operatorname{supp}(x) + \#\operatorname{supp}(y) < \infty$. Thereby ax and $x + y \in S$ again.
- Now consider the *R*-module-homomorphisms $\varphi_i : M_i \to N$. By construction of *S* the map $\varphi := \bigoplus_i \varphi_i : S \to N$ is well-defined. And it also is an *R*-module-homomorphism, as for any $a \in R$ and for any $x = (x_i)$, $y = (y_i) \in S$ we get $\varphi(ax) = \sum_i \varphi_i(ax_i) = \sum_i a\varphi_i(x_i) = a\varphi(x)$ and $\varphi(x+y) = \sum_i \varphi_i(x_i+y_i) = \sum_i (\varphi_i(x_i) + \varphi_i(y_i)) = \varphi(x) + \varphi(y)$.

• (a) \implies (b): by definition of the arbitrary sum of the submodules P_i of M and by the assumption $M = \sum_i P_i$ we obtain the identity

$$M = \left\{ \sum_{i \in \Omega} x_i \mid \Omega \subseteq I \text{ finite, } x_i \in P_i \right\}$$

Thus if we are given any $x \in M$ there are finitely many $x_i \in P_i$ $(i \in \Omega)$ such that $x = \sum_i x_i$ Letting $x_i := 0$ for $i \in I \setminus \Omega$ we obtain an extention $(x_i) \in \bigoplus_i P_i$ satisfying $x = \sum_i x_i$. This proves the existence of such a representation. For the uniqueness suppose $\sum_i x_i = \sum_i y_i$ for some $(x_i), (y_i) \in \bigoplus_i P_i$. Fix any $j \in I$ and let

$$\widehat{x}_j := \sum_{i \neq j} x_i \text{ and } \widehat{y}_j := \sum_{i \neq j} y_i \in \widehat{P}_j$$

Then we find $x_j - y_j = \hat{y}_j - \hat{x}_j$, but as $x_j - y_j \in P_j$ and $\hat{y}_j - \hat{x}_j \in \hat{P}_j$ we have $x_j - y_j \in P_j \cap \hat{P}_j = 0$, such that $x_j = y_j$. But as $j \in I$ has been arbitrary this means $(x_i) = (y_i)$, which also is the uniqueness.

• (b) \implies (a): consider any $x \in M$, by asumption (b) there is some $(x_i) \in \bigoplus_i P_i$ such that $x = \sum_i x_i$. And as only finitely many x_i are non-zero this means $x = \sum_i x_i \in \sum_i P_i$. And as x has been arbitrary this already is $M = \sum_i P_i$. Now consider any $j \in I$ and any $x \in P_j \cap \hat{P}_j$. As $x \in P_j$ we may let $\tilde{x}_j := x_j \in P_j$ and $\tilde{x}_i := 0 \in P_i$ (for $i \neq j$) to find $x = \sum_i \tilde{x}_i$. On the other hand we have $x \in \hat{P}_j$, that is there are some $x_i \in P_i$ such that $x = \sum_{i\neq j} x_i$. Finally let $x_j := 0$ then altogether this is $\sum_i x_i = \sum_{i\neq j} x_i = \sum_i \tilde{x}_i$ and due to the uniqueness this means $x_i = \tilde{x}_i$ for any $i \in I$. But by choice of \tilde{x}_i this is $x_i = 0$ for any $i \neq j$ and hence $x = \sum_{i\neq j} 0 = 0$, which had to be shown.

Proof of (3.19):

Let us again abbreviate the exterior direct product by $P := \prod_i M_i$ and the exterior direct sum by $S := \bigoplus_i M_i$. It is immediately clear that $\pi_j : P \to M_j$ is an *R*-module-homomorphism: $\pi_j(ax + y) = \pi_j((ax_i + y_i)) = ax_j + y_j =$ $a\pi_j(x) + \pi_j(y)$ Analogously it is clear that ι_j is an *R*-module homomorphism. Also $\pi_j\iota_j(x_j) = \pi_j(\delta_{i,j}x_j) = \delta_{j,j}x_j = x_j$ such that $\pi_j\iota_j = \mathbb{1}$. And from this it immediately follows that π_j is surjective and that π_j is injective. Note that the latter could have also been seen directly. Now consider any $x = (x_i) \in P$, then by definition $\pi_i(x) = x_i$ such that $x = (x_i) = (\pi_i(x))$. Conversely consider $x = (x_i) \in S$, then by definition $\iota_j(x_j) = (\delta_{i,j}x_j)$ (where the index runs over all $i \in I$). Therefore a straightforard computation yields

$$\sum_{j \in I} \iota_j(x_j) = \sum_{j \in I} \left(\delta_{i,j} x_j \right) = \left(\sum_{j \in I} \delta_{i,j} x_j \right) = (x_i) = x$$

Proof of (3.22):

- (i) It is easy to see that the map given is a homomorphism: $(x_i) + (y_i) = (x_i + y_i) \mapsto \sum_i (x_i + y_i) = (\sum_i x_i) + (\sum_i y_i)$ and $a(x_i) = (ax_i) \mapsto \sum_i (ax_i) = a(\sum_i x_i)$. And the bijectivity is just a reformulation of property (b) of inner direct sums.
- (ii) Let us abbreviate the exterior direct sum by $M := \bigoplus_i M_i$. That is any $x \in M$ is of the form $x = (x_i)$ for some $x_i \in M_i$ of which only finitely many are non-zero. Thus $x = (x_i) = \sum_i \iota_i(x_i) \in \sum_i P_i$. And as x has been arbitrary this means $M = \sum_i P_i$. Now consider any $j \in I$ and any $x \in P_j \cap \hat{P}_j$. As $x \in P_j = \iota_j(M_j)$ there is some $m_j \in M_j$ such that $(x_i) := x = \iota_j(m_j) = (\delta_{i,j}m_j)$. On the other hand there are $p_i \in P_i$ (where $i \neq j$) such that $x = \sum_{i\neq j} p_i$. Likewise we choose $n_i \in M_i$ such that $p_i = \iota_i(n_i)$. If we finally let $n_j := 0$, then $x = \sum_{i\neq j} \iota_i(n_i) = \sum_i \iota_i(n_i) = (n_i)$. Comparing these two expressions of x we find $n_i = x_i = \delta_{i,j}m_j = 0$ for any $i \neq j$. And as also $n_j = 0$ this means $x = (n_i) = (0_i) = 0 \in M$. Therefore $P_j \cap \hat{P}_j = 0$, as claimed.

Proof of (3.23):

- Clearly the map $\varphi \mapsto (\pi_j \varphi \iota_i)$ is well-defined: as π_j and ι_i are *R*-module homomorphisms, so is the composition $\pi_j \varphi \iota_i : M_i \to N_j$. Conversely $(\varphi_{i,j}) \mapsto (\bigoplus_i \varphi_{i,j})$ is well-defined, too - it just is the Carthesian product of the induced homomorphisms $\bigoplus_i \varphi_{i,j} : \bigoplus_i M_i \to N_j$.
- And it is also clear, that $\varphi \mapsto (\pi_j \varphi \iota_i)$ is a homomorphism of R-modules: as ι_i and π_j are homomorphisms of R-modules, so are the push-forward $\varphi \mapsto \varphi \iota_i$ and pull-back $\psi \mapsto \pi_j \psi$. Combining these we see that $\varphi \mapsto \pi_j \varphi \iota_i$ is a homomorphism of R-modules. Thus if we regard any $\varphi, \psi \in \text{mhom}(M, N)$ and any $a \in R$, then $a\varphi + \psi \mapsto (\pi_j(a\varphi + \psi)\iota_i) = (a\pi_j\varphi\iota_i + \pi_j\psi\iota_i) = a(\pi_j\varphi\iota_i) + (\pi_j\psi\iota_i)$, as the composition in the direct product was defined to be component-wise.
- We will now prove that these maps are mutually inverse, we start by regarding $\varphi \mapsto (\pi_j \varphi \iota_i) \mapsto \psi := (\bigoplus_i \pi_j \varphi \iota_i)$. Thus consider an arbitrary $x = (x_i) \in \bigoplus_i M_i$ then we find

$$\psi(x) = \left(\sum_{i \in I} \pi_j \varphi \iota_i(x_i)\right) = \left(\pi_j \varphi \left(\sum_{i \in I} \iota_i(x_i)\right)\right)$$

as $\pi_j \varphi$ is an *R*-module homomorphism. Now recall the identities $x = \sum_i \iota_i(x_i)$ and $y = (\pi_j(y))$, inserting these we obtain $\psi = \varphi$ from

$$\psi(x) = \left(\pi_j \varphi(x)\right) = \varphi(x)$$

• Thus we have to regard $(\varphi_{i,j}) \mapsto (\bigoplus_i \varphi_{i,j}) \mapsto (\psi_{i,j}) := (\pi_j (\bigoplus_i \varphi_{i,j}) \iota_i)$. We need to verify that for any $i \in I$ and $j \in J$ we get $\varphi_{i,j} = \psi_{i,j}$. Thus fix any i, j and $x_i \in M_i$ and compute

$$\psi_{i,j}(x_i) = \pi_j \left(\left(\bigoplus_{a \in I} \varphi_{a,b} \right)_{b \in J} \left(\iota_i(x_i) \right) \right)$$

By definition we have $\iota_i(x_i) = (\delta_{a,i}x_i)$, where the index runs over $a \in I$. Inserting this into the definition of $\bigoplus_a \varphi_{a,b}$ we continue

$$\psi_{i,j}(x_i) = \pi_j \left(\sum_{a \in I} \varphi_{a,b}(\delta_{a,i}x_i) \right)_{b \in J} = \sum_{a \in I} \varphi_{a,j}(\delta_{a,i}x_i)$$

If $a \neq i$ then $\delta_{a,i}x_i = 0 \in M_a$ such that the respective summand vanishes. It only remains the summand of a = i, which is given to be $\varphi_{i,j}(\delta_{i,i}x_i) = \varphi_{i,j}(x_i)$. As x_i has been arbitrary this proves $\psi_{i,j} = \varphi_{i,j}$ which had to be shown.

• We now prove the claim in the remark to the proposition: that is we consider $\varphi_i := (\varphi_{i,j}) \in \bigoplus_j \text{mhom}(M_i, N_j)$ and want to show that the image of the corresponding map $\varphi := (\bigoplus_i \varphi_{i,j})$ is contained in $\bigoplus_j N_j$. Thus consider any $x = (x_i) \in \bigoplus_i M_i$ then we have to verify, that

$$y := \varphi(x) = \left(\sum_{i \in I} \varphi_{i,j}(x_i)\right) \in \bigoplus_{j \in J} N_j$$

That is we have to verify that the support of y is finite. To see this let us abbreviate the support of x by $\Omega := \operatorname{supp}(x) \subseteq I$, which is a finite set, as $x \in \bigoplus_i M_i$. Then it is clear that the support of y satisfies the following inclusions

$$supp(y) = \left\{ j \in J \mid \sum_{i \in I} \varphi_{i,j}(x_i) \neq 0 \right\}$$
$$\subseteq \left\{ j \in J \mid \exists i \in I : \varphi_{i,j}(x_i) \neq 0 \right\}$$
$$\subseteq \left\{ j \in J \mid \exists i \in I : x_i \neq 0 \text{ and } \varphi_{i,j} \neq 0 \right\}$$
$$= \left\{ j \in J \mid \exists i \in \Omega \text{ with } \varphi_{i,j} \neq 0 \right\}$$
$$= \bigcup \left\{ supp(\varphi_i) \mid i \in \Omega \right\}$$

However the latter is a finite (Ω is finite) union of finite (any $\operatorname{supp}(\varphi_i)$ was assumed to be finite) subsets of J. Hence it is a finite set itself which proves $y \in \bigoplus_i N_j$ which had been claimed.

Proof of (6.15):

(i) Let us write out the homogeneous decomposition $1 = \sum_d 1_d$. Then for any homogeneous element $h \in H$ - say $c := \deg(h)$ - we get

$$h = h \cdot 1 = \sum_{d \in D} h \cdot 1_d$$

Thereby $h \cdot 1_d \in A_{c+d}$ according to property (4). But as $h \in H$ is homogeneous we may compare coefficients (this is property (3)) to find $h = \sum_{c+d=c} h \cdot 1_d$. Yet D has been assumed to be integral, hence c + d = c = c + 0 implies d = 0. Thus for any $h \in H$ we have found $h = h \cdot 1_0$. Thus consider any $f \in A$ and decompose $f = \sum_d f_d$ into homogeneous elements. Then we compute

$$f \cdot 1_0 = \sum_{d \in D} f_d \cdot 1_0 = \sum_{d \in D} f_d = 0$$

as the $f_d \in H \cup \{0\}$ are homogeneous. Thus we have proved $f = f \cdot 1_0$ for any element $f \in A$. In particular $1 = 1 \cdot 1_0 = 1_0 \in A_0$.

(ii) Clearly the kernel is an ideal $\mathfrak{a} := \operatorname{kn}(\varphi) \leq_{\mathrm{i}} A$ of A, so we only have to prove the graded property. First of all, it is clear that the submodules $\mathfrak{a} \cap A_d$ intersect trivially

$$(\mathfrak{a} \cap A_c) \cap \left(\sum_{d \neq c} \mathfrak{a} \cap A_d\right) \subseteq A_c \cap \left(\sum_{d \neq c} A_d\right) = \{0\}$$

Thus it remains to show that \mathfrak{a} truly is the sum of the $\mathfrak{a} \cap A_d$. Consider any $f \in \mathfrak{a}$ and decompose f into homogeneous components $f = \sum_d f_d$ where $f_d \in A_d$. Then we get

$$0 = \varphi(f) = \sum_{d \in D} \varphi(f_d)$$

As φ was assumed to be graded, we have $\varphi(f_d) \in B_d$ again. Thus comparing homogeneous coefficients in B we find $\varphi(f_d) = 0$ for any $d \in D$. And this again translated into $f_d \in \mathfrak{a}$ such that $f_d \in \mathfrak{a} \cap A_d$. As f has been arbitrary this also shows

$$\mathfrak{a} = \sum_{d \in D} \mathfrak{a} \cap A_d$$

(iii) As $\mathfrak{a} \trianglelefteq_i A$ is an ideal and A is an R-algebra, $\mathfrak{a} \trianglelefteq_a A$ even is an R-algebra-ideal. And hence the quotient A/\mathfrak{a} is an R-algebra again. And by construction we have $0 + \mathfrak{a} \notin \hom(A/\mathfrak{a})$. Let us now prove the well-definedness of deg : $\hom(A/\mathfrak{a}) \to D$: suppose we are given g and $h \in A$ such that $g + \mathfrak{a} = h + \mathfrak{a} \in \hom(A/\mathfrak{a})$. That is $f := g - h \in \mathfrak{a}$. Let us now denote $b := \deg(g)$ and $c := \deg(h)$ and decompose $f = \sum_d f_d$ (where $f_d \in \mathfrak{a} \cap A_d$ by assumption). Then we find

$$\sum_{d \in D} \left\{ \begin{array}{ll} g & \text{if } d = b \\ 0 & \text{if } d \neq b \end{array} \right. = \left. g \right. f + h = \sum_{d \in D} \left\{ \begin{array}{ll} f_c + h & \text{if } d = c \\ f_d & \text{if } d \neq c \end{array} \right.$$

Now suppose we had $b \neq c$ then comparing coefficients we would find $g = f_b \in \mathfrak{a}$ in contradiction to $g + \mathfrak{a} \in \hom(A/\mathfrak{a})$. Thus we have $\deg(g) = b = c = \deg(h)$ and hence $\deg : \hom(A/\mathfrak{a}) \to D$ is welldefined. We will now prove the identity

$$\left(\frac{A}{\mathfrak{a}}\right)_d = \frac{A_d + \mathfrak{a}}{\mathfrak{a}}$$

For the inclusion " \subseteq " we are given some $h + \mathfrak{a} \in (A/\mathfrak{a})_d$. If thereby $h + \mathfrak{a} = 0 + \mathfrak{a}$ then $h \in \mathfrak{a}$ and hence $h + \mathfrak{a} \in (A_d + \mathfrak{a})/\mathfrak{a}$. If on the other hand $h + \mathfrak{a} \neq 0 + \mathfrak{a}$ then we have $\deg(h) = d$ by assumption and hence $h \in A_d$. Altogether $h + \mathfrak{a} \in (A_d + \mathfrak{a})/\mathfrak{a}$ again. Conversely " \supseteq " consider any $h \in A_d$ and any $f \in \mathfrak{a}$. Then we have to show $(h+f) + \mathfrak{a} \in (A/\mathfrak{a})_d$. If h = 0 then $(h + f) + \mathfrak{a} = 0 + \mathfrak{a} \in (A/\mathfrak{a})_d$ is clear. And if $h \neq 0$ then $\deg(h) = d$ by assumption such that $(h + f) + \mathfrak{a} = h + \mathfrak{a}$ is of degree d, as well. Thus we have established the equality and in particular $(A/\mathfrak{a})_d$ is an R-submodule of A/\mathfrak{a} . Now consider $g \in A_c$, $h \in A_d$ and $a, b \in \mathfrak{a}$. Then $(g + a)(h + b) = gh + (ah + gb + ab) \in A_{c+d} + \mathfrak{a}$. And as all these elements have been arbitrary this also proves property (4) of graded algebras, that is $(A/\mathfrak{a})_c(A/\mathfrak{a})_d \subseteq (A/\mathfrak{a})_{c+d}$. Now

$$A/\mathfrak{a} = \sum_{d\in D} A_d + \mathfrak{a}/\mathfrak{a}$$

is easy to see: if we are given any $f + \mathfrak{a} \in A/\mathfrak{a}$ then we may decompose $f = \sum_d f_d$ into homogeneous components. Thereby $f + \mathfrak{a} = \sum_d (f_d + \mathfrak{a})$. This already yields " \subseteq " and the converse inclusion is clear. Now fix any $c \in D$ then it remains to prove

$$\left(A_{c} + \mathfrak{a}/\mathfrak{a}\right) \cap \left(\sum_{d \neq c} A_{d} + \mathfrak{a}/\mathfrak{a}\right) = \{0 + \mathfrak{a}\}$$

Thus consider any $f + \mathfrak{a}$ contained in the intersection. In particular that is $f + \mathfrak{a} \in (A_c + \mathfrak{a})/\mathfrak{a}$ and hence there is some $f_c \in A_c$ such that

 $f + \mathfrak{a} = f_c + \mathfrak{a}$. And likewise there are $f_d \in A_d$ (where $d \neq c$) such that $f + \mathfrak{a} = \sum_{d \neq c} f_d + \mathfrak{a}$. Thus we find

$$a := f_c - \sum_{d \neq c} f_d \in \mathfrak{a} = \bigoplus_{d \in D} \mathfrak{a} \cap A_d$$

as \mathfrak{a} has been assumed to be a graded ideal we can decompose a into $a = \sum_d a_d$ where $a_d \in \mathfrak{a} \cap A_d$. Comparing the homogeneous coefficients of a in A we find $f_c = a_c \in \mathfrak{a} \cap A_c$. In particular $f + \mathfrak{a} = f_c + \mathfrak{a} = 0 + \mathfrak{a}$, which had to be shown.

Proof of (6.17):

- (i) If $h \in A_d$ but $h \neq 0$ then the homogeneous decomposition $h = \sum_c h_c$ has precisely one non-zero entry $h = h_d$ at c = d (by comparing coefficients). Thus deg $(h) = \max\{d\}$ and this clearly is d.
- (ii) If $f \in \text{hom}(A)$ with $f \in A_d$ then we have just argued in (i) that $\deg(f) = \max\{d\} = d$. And likewise $\operatorname{ord}(f) = \min\{d\} = d$ which yields $\operatorname{ord}(f) = \deg(f)$. Conversely suppose $d := \operatorname{ord}(f) = \deg(f)$, then we use a homogeneous decomposition $f = \sum_c f_c$ again. By construction, if $c < d = \operatorname{ord}(f)$ or $d = \deg(d) < c$ then $f_c = 0$. Thus it only remains $f = f_d \in A_d$ and hence $f \in \operatorname{hom}(A)$.
- (iii) As $\operatorname{ord}(f)$ is the minimum and $\operatorname{deg}(f)$ is the maximum over the common set $\{d \in D \mid f_d \neq 0\}$ it is clear, that $\operatorname{ord}(f) \leq \operatorname{deg}(f)$. Now let $a := \operatorname{deg}(f)$ and $b := \operatorname{deg}(g)$. Then (by construction of the degree) the homogeneous decompositions of f and g are of the form

$$f = \sum_{c \le a} f_c$$
 and $g = \sum_{d \le b} g_d$

Thus the product fg is given by a sum over two indices $c \leq a$ and $d \leq b$. Assorting the (c, d) according to the sum c + d we find that

$$fg = \left(\sum_{c \le a} f_c\right) \left(\sum_{d \le b} g_d\right) = \sum_{c \le a} \sum_{d \le b} f_c g_d = \sum_{e \in D} \sum_{c+d=e} f_c g_d$$

Note that thereby $f_cg_d \in A_{c+d} = A_e$. Thus we have found the homogeneous decomposition of fg again. But as D was assumed to be positive $c \leq a$ and $d \leq b$ implies $e = c + d \leq a + d \leq a + b$. Thus the homogeneous decomposition is of the following form

$$fg = \sum_{e \le a+b} \left(\sum_{c+d=e} f_c g_d \right)$$

And this of course means $\deg(fg) \leq a+b = \deg(f)+\deg(g)$. The claim for the order can be shown in complete analogy. Just let $a := \operatorname{ord}(f)$ and $b := \operatorname{ord}(g)$. Then f and g can be written as

$$f = \sum_{c \ge a} f_c$$
 and $g = \sum_{d \ge b} g_d$

Thus in complete analogy to the above one finds that the homogeneous decomposition of fg is of the following form (which already yields $\operatorname{ord}(fg) \ge a + b = \operatorname{ord}(f) + \operatorname{ord}(g)$)

$$fg = \sum_{e \ge a+b} \left(\sum_{c+d=e} f_c g_d \right)$$

(iv) We commence with the proof given in (iii), that is $a = \deg(f)$ and $b = \deg(g)$. In particular $f_a \neq 0$ and $g_b \neq 0$. But as A is now assumed to be an integral domain this yields $f_a g_b \neq 0$. We have already found the homogeneous decomposition of fg to be

$$fg = \sum_{e \le a+b} \left(\sum_{c+d=e} f_c g_d \right)$$

So let us take a look at the homogeneous component $(fg)_{a+b}$ of degree $a+b \in D$. Given any $c \leq a$ and $d \leq b$ we get the implication

$$c + d = a + b \implies (c, d) = (a, b)$$

Because if we had $c \neq a$ then c < a and hence $c + d < a + d \leq a + b$, as D was assumed to be strictly positive. Likewise $d \neq b$ would imply c + d < a + b in contradiction to c + d = a + b. Thus the homogeneous component $(fg)_{a+b}$ is given to be

$$(fg)_{a+b} = \sum_{c+d=a+b} f_c g_d = f_a g_b \neq 0$$

In particular we find $\deg(fg) \ge a + b = \deg(f) + \deg(g)$ and hence $\deg(fg) = \deg(f) + \deg(g)$. By replacing the above implication with $c \ge a, d \ge b$ and c + d = a + b implies (c, d) = (a, b) the claim for the order $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$ can be proved in complete analogy.

(v) As D is strictly positive it already is integral, according to (6.5.(iii)). Hence by (6.15.(i)) we already know $1 \in A_0$ and hence deg(1) = 0 according to (i). And as 1 is homogeneous we also get ord(1) = deg(1) = 0, according to (ii). Now suppose $f \in A^*$ is an invertible element of A. Then we use (iv) to compute

$$0 = \deg(1) = \deg(ff^{-1}) = \deg(f) + \deg(f^{-1})$$

$$0 = \operatorname{ord}(1) = \operatorname{ord}(ff^{-1}) = \operatorname{ord}(f) + \operatorname{ord}(f^{-1})$$

And as $\operatorname{ord}(f) \leq \operatorname{deg}(f)$ and $\operatorname{ord}(f^{-1}) \leq \operatorname{deg}(f^{-1})$ (due to (iii)) the positivity of D can be used to find the following estimates

$$\begin{array}{rcl} 0 & = & \operatorname{ord}(f) + \operatorname{ord}(f^{-1}) & \leq & \deg(f) + \operatorname{ord}(f^{-1}) \\ & \leq & \deg(f) + \deg(f^{-1}) & = & 0 \end{array}$$

In particular we find $\operatorname{ord}(f) + \operatorname{ord}(f^{-1}) = \operatorname{deg}(f) + \operatorname{ord}(f^{-1})$. Adding $\operatorname{ord}(f)$ this equation turns into $\operatorname{ord}(f) = \operatorname{deg}(f)$ and by (ii) again this means that $f \in \operatorname{hom}(A)$ is homogeneous.

Proof of (3.26):

- (i) Because of (D1) (that is $x \in T \implies T \vdash x$) we have the obvious inclusions $S \subseteq T \subseteq \langle T \rangle$. That is we have $T \vdash S$. If now $x \in M$ with $S \vdash x$, then by (D2) we also get $T \vdash x$. And this is just a reformulation of the claim $\langle S \rangle \subseteq \langle T \rangle$.
- (ii) We will first prove $\langle S \rangle = \bigcap \{ P \in \operatorname{sub}(M) \mid S \subseteq P \}$. For the inclusion " \subseteq " we are given any $x \in \langle S \rangle$. Then we need to show that for any $P \in \operatorname{sub}(M)$ with $S \subseteq P$ we get $x \in P$. As $P \in \operatorname{sub}(M)$ there is some $T \subseteq M$ with $P = \langle T \rangle$. Then $S \subseteq P$ translates into $S \subseteq \langle T \rangle$, which is $T \vdash S$. Together with $S \vdash x$ now property (D2) implies $T \vdash x$. And this is $x \in \langle T \rangle = P$, which had to be shown. Conversely for " \supseteq " we are given some $x \in M$ such that for any $P \in \operatorname{sub}(M)$ we get $S \subseteq P \implies x \in P$. Then we may simply choose $P := \langle S \rangle$, then $S \subseteq P$ is satisfied due to (D1). Thus by assumption on x we get $x \in P = \langle S \rangle$, which had to be shown.

Thus let us now prove $P = \langle P \rangle$, where we abbreviated $P := \langle S \rangle$. The inclusion " \subseteq " is clear by (D1) again. And by what we have shown, we have $\langle P \rangle = \bigcap \{ Q \in \operatorname{sub}(M) \mid P \subseteq Q \}$. But as $P \in \operatorname{sub}(M)$ with $P \subseteq P$ this trivially yields $\langle P \rangle \subseteq P$, the converse inclusion.

(iii) (a) \implies (c): by assumption there is some $s \in S$ such that $S \setminus \{s\} \vdash s$. Due to (D3) there is some finite subset $S_s \subseteq S \setminus \{s\}$ such that $S_s \vdash s$. Now let $S_0 := S_s \cup \{s\}$, then S_0 is finite again, as $\#S_0 = \#S_s + 1 < \infty$ and $S_0 \setminus \{s\} = S_s$. In particular $S_0 \setminus \{s\} \vdash s$, that is S_0 is \vdash dependent. (c) \implies (b): consider $S_0 \subseteq S \subseteq T$, by assumption there is some $s \in S_0$ such that $S_0 \setminus \{s\} \vdash s$. However $S_0 \setminus \{s\} \subseteq T \setminus \{s\}$, such that by (i) we also get $T \setminus \{s\} \vdash s$. That is T is \vdash dependent. (b) \implies (a) finally is trivial, by letting T := S.

- (iv) (a) \Longrightarrow (b): suppose S was \vdash dependent, that is there was some $s \in S$, such that $S \setminus \{s\} \vdash s$. As $S \subseteq T$ we also have $S \setminus \{s\} \subseteq T \setminus \{s\}$, hence we find $S \setminus \{s\} \vdash s$ due to (i). But as also $s \in S \subseteq T$ this is a contradiction to T being \vdash independent. (b) \Longrightarrow (c) is trivial (a finite subset is a subset). (c) \Longrightarrow (a): suppose there was some $x \in T$ such that $T \setminus \{x\} \vdash x$. Then by (D3) there would be a finite subset $T_x \subseteq T \setminus \{x\}$ such that $T_x \vdash x$. Now let $T_0 := T_x \cup \{x\}$, then T_0 is finite again, as $\#T_0 = \#T_x + 1 < \infty$. Also $T_0 \setminus \{x\} = T_x \vdash x$, that is T_0 is \vdash dependent in contradiction to (c).
- (v) (a) \implies (b): clearly $S \subset T := S \cup \{x\}$, such that S is \vdash independent by assumption (a) and (iv). Now suppose we had $S \vdash x$, then clearly $T \setminus \{x\} = S \vdash x$. That is T is \vdash dependent in contradiction to the assumption. (b) \implies (a): if we had $x \in S$, then by property (D1) also $S \vdash x$, in contradiction to the assumption. Now suppose that $S \cup \{x\}$ was \vdash dependent. That is there would be some $s \in S \cup \{x\}$ such that

$$S' := \left(S \cup \left\{x\right\}\right) \setminus \left\{s\right\} \vdash s$$

We now distinguish two cases: (1) if s = x then S' = S and thereby we would get $S = S' \vdash s = x$, a contradiction to $S \nvDash x$. (2) if $s \neq x$ then $s \in S \cup \{x\}$ implies $s \in S$. Now let $R := S \setminus \{s\}$, that is $S = R \cup \{s\}$ and $S' = (S \cup \{x\}) \setminus \{s\} = R \cup \{x\}$. This again means

$$S' \setminus \{x\} = R = S \setminus \{s\}$$

As S is \vdash independent we now have $S' \setminus \{x\} = S \setminus \{s\} \not\vDash s$. Because of $x \in S', S' \vdash s$ and $S' \setminus \{x\} \not\vDash s$ property (D4) implies

$$S = \left(S \setminus \{s\}\right) \cup \{s\} = \left(S' \setminus \{x\}\right) \cup \{s\} \vdash x$$

This is a contradiction to $S \not\vdash x$ again, thus in both cases we have derived a contradiction, that is $S \cup \{x\}$ is \vdash independent, as claimed.

(vi) Let us abbreviate the chain's union by $T := \bigcup_i S_i$ and suppose T would be \vdash dependent. Then by (iii) there would be a finite subset $T_0 \subseteq T$, such that T_0 is \vdash dependent, already. Say $T_0 = \{x_1, \ldots, n_n\}$, where for any $k \in 1 \ldots n$ we have $x_k \in S_{i(k)}$ for some $i(k) \in I$. As $\{S_i \mid i \in I\}$ is totally ordered under \subseteq , so is the finite subset $\{S_{i(k)} \mid k \in 1 \ldots n\}$. Without loss of generality we may assume, that $S_{i(n)}$ is the maximal element among the $S_{i(k)}$. Hence we find $x_k \in S_{i(k)} \subseteq S_{i(n)}$ for any $k \in 1 \ldots n$ and this again means $T_0 \subseteq S_{i(n)}$. Yet as T_0 was \vdash dependent this implies, that $S_{i(n)}$ is \vdash dependent (by (iii) again), a contradiction. Hence T is \vdash independent, as claimed. (vii) Not surprisingly we will prove the claim using a zornification based on

$$\mathcal{Z} := \{ P \subseteq M \mid S \subseteq P \subseteq T, P \text{ is } \vdash \text{independent} \}$$

Of course \mathcal{Z} is non-empty, as $S \in \mathcal{Z}$, and it is partially ordered under the inclusion relation \subseteq . Due to (vi) any ascending chain (S_i) admits an upper bound, namely $T := \bigcup_i S_i \in \mathcal{Z}$. Thus by the lemma of Zorn \mathcal{Z} contains a maximal element B. Because of $B \in \mathcal{Z}$ we have $S \subseteq B \subseteq T$ and B is \vdash independent. Now suppose there was some $x \in T$ with $B \not\vdash x$. However, as B is \vdash independent and $B \not\vdash x$, we find by (v) that even $B \cup \{x\}$ is \vdash independent. But as $x \notin B$ we have $B \subset B \cup \{x\} \subseteq T$. Thus we have found a contradiction to the maximality of B. This contradiction can only be solved, if $T \subseteq \langle B \rangle$. And using (i) and (ii) we thereby get $M = \langle T \rangle \subseteq \langle \langle B \rangle \rangle = \langle B \rangle \subseteq M$. Altogether B is \vdash independent and $M = \langle B \rangle$ - it is a \vdash basis.

- (viii) First suppose x = b, then B' = B and hence there is nothing to show. Thus assume $x \neq b$. The proof now consists of two parts: (1) as $B \setminus \{b\} \subseteq B' \subseteq \langle B' \rangle$ and $B' \vdash b$ by assumption, we have $B = (B \setminus \{b\}) \cup \{b\} \subseteq \langle B' \rangle$. And thereby $M = \langle B \rangle \subseteq \langle \langle B' \rangle \rangle =$ $\langle B' \rangle \subseteq M$, according to (ii). That is $M = \langle B' \rangle$. (2) as $B \setminus \{b\} \subseteq B$ is a subset and B is \vdash independent, so is $B \setminus \{b\}$, due to (iv). Now suppose $B \setminus \{b\} \vdash x$, then we would get $B' = (B \setminus \{b\}) \cup \{x\} \subseteq \langle B \setminus \{b\} \rangle$. And hence $b \in M = \langle B' \rangle \subseteq \langle \langle B \setminus \{b\} \rangle \rangle = \langle B \setminus \{b\} \rangle$, according to (1) and (ii) once more. But this is $B \setminus \{b\} \vdash b$ in contradiction to the \vdash independence of B. Thus we have $B \setminus \{b\} \vdash x$, as $B \setminus \{b\}$ also is \vdash independent (v) now implies, that $B' = (B \setminus \{b\}) \cup \{x\}$ is \vdash independent. Combining (1) and (2) we found that B' is a \vdash basis.
 - (ix) (a) \implies (b): $M = \langle B \rangle$ is clear by definition of a \vdash basis. Now consider some subset $S \subset B$, that is there is some $x \in B$, with $x \notin S$. As B is \vdash independent and $x \in B$ we get $B \setminus \{x\} \not\vdash x$, in other words $x \notin \langle B \setminus \{x\} \rangle$. And as $S \subseteq B \setminus \{x\}$ (i) implies $x \notin \langle S \rangle$. In particular $\langle S \rangle \neq M$, as claimed.

(b) \implies (a): as $M = \langle B \rangle$ by assumption it only remains to verify the \vdash independence of B. Thus assume, there was some $x \in B$ such that $S := B \setminus \{x\} \vdash x$. As $S \subseteq \langle S \rangle$ and $x \in \langle S \rangle$, we have $B = S \cup \{x\} \subseteq \langle S \rangle$. And thereby $M = \langle B \rangle \subseteq \langle \langle S \rangle \rangle = \langle S \rangle \subseteq M$ according to (ii). This is $M = \langle S \rangle$ even though $S \subset B$, a contradiction.

(ix) (a) \implies (c): suppose *B* is a \vdash basis, that by definition *B* already is \vdash independent. Thus suppose $B \subset S$, that is we may choose some $s \in S \setminus B$. As $s \in M = \langle B \rangle$ we get $B \vdash s$. And as $B \subseteq S \setminus \{s\}$ (i) also yields $S \setminus \{s\} \vdash s$. That is *S* is \vdash dependent, as claimed.

(c) \implies (a): as *B* is assumed to be \vdash independent, it remains to show $M = \langle B \rangle$. Thus suppose we had $\langle B \rangle \subset M$, that is there was some $s \in M$ such that $B \not\vdash s$. Then by (v) we find that $S := B \cup \{s\}$ is independent, as well - a contradiction.

- (x) Let us denote m := |A| and n := |B|, then we need to show m = n. In the proof we will have to distinguish two cases: (I) m or n is finite and (II) both m and n are infinite. We will deal with (I) in the following steps (1) to (4), whereas (II) will be treated in (5)
 - (1) Without loss of generality we may assume $m \leq n$ (interchanging A and B if not). Then M is finite by assumption (I), let us denote the elements of A by $A = \{x_1, \ldots, x_m\}$. Thereby let us assume that $x_1, \ldots, x_k \notin B$ and $x_{k+1}, \ldots, x_m \in B$ for some $k \in \mathbb{N}$ [note that for k = 0 this is $A \subseteq B$ and for k = m this is $A \cap B = \emptyset$]. In the case k = 0 we may skip steps (2), (3) and let $A^{(k)} := A$, immediately proceeding with (4).
 - (2) As A is a \vdash basis of M, it is a minimal \vdash generating subset, by (ix). That is $\langle \{x_2, \ldots, x_m\} \rangle \neq M = \langle B \rangle$. Hence there is some point $b \in B$ such that $b \notin \langle \{x_2, \ldots, x_m\} \rangle$ [as else $B \subseteq \langle \{x_2, \ldots, x_m\} \rangle$ and hence $M = \langle B \rangle \subseteq \langle \langle \{x_2, \ldots, x_m\} \rangle \rangle = \langle \{x_2, \ldots, x_m\} \rangle$, according to (ii), a contradiction]. For this $b \in B$ let us define

$$A' := (A \cup \{b\}) \setminus \{x_1\} = \{b, x_2, \dots, x_m\}$$

Then A' is \vdash independent [as A is \vdash independent, the same is true for $\{x_2, \ldots, x_m\}$. And due to $\{x_2, \ldots, x_m\} \not\vDash b$ (v) implies, that A' is independent]. Next we find that $A' \vdash x_1$ [because if we had $A' \not\vdash x_1$ then - using (v) and the fact that A' is \vdash independent - $A' \cup \{x_1\}$ would be \vdash independent, too. However this is untrue, as $(A' \cup \{x_1\}) \setminus \{b\} = A \vdash b$]. Therefore A' even is a \vdash basis [as $A' \vdash x_1$ we have $x_1 \in \langle A' \rangle$ and clearly $A \setminus \{x_1\} \subseteq \langle A' \rangle$, such that $A = (A \setminus \{x_1\}) \cup \{x_1\} \subseteq \langle A' \rangle$. Combined with (ii) this yields $M = \langle A \rangle \subseteq \langle \langle A' \rangle \rangle = \langle A' \rangle \subseteq M$, that is $\langle A \rangle = M$ and the \vdash independence of A' has already been shown].

- (3) In (2) we have replaced $x_1 \in A$ by some $b \in B$ to obtain another \vdash basis $A' := (A \cup \{b\}) \setminus \{x_1\} = \{b, x_2, \dots, x_k\}$. That is: venturing from A to A' we have increased the number of elements in $A' \cap B$ by 1 (with respect to $A \cap B$). Iterating this process k times we establish a \vdash basis $A^{(k)} = \{b_1, \dots, b_k, x_{k+1}, \dots, x_m\} \subseteq B$.
- (4) From the construction it is clear, that $|A'| \leq m \leq n = |B|$. On the other hand - as B is a \vdash basis, $A' \subseteq B$ and $M = \langle A' \rangle$ - item (ix) now implies that A' = B. And thereby $n = |B| = |A'| \leq m$, as well. Together this is m = n as claimed.

(5) It remains to regard case (II), that is m and N are both infinite. As $B \subseteq M = \langle A \rangle$ we obviously have $A \vdash b$ for any $b \in B$. Thus by property (D3) there is a subset $A_b \subseteq A$ such that $\#A_b < \infty$ is finite and $A_b \vdash b$ already. Now let

$$A^* := \bigcup_{b \in B} A_b \subseteq A$$

Then for any $b \in B$ we have $A_b \subseteq A^*$ and hence $A^* \vdash b$, due to (i). That is $b \in \langle A^* \rangle$ for any $b \in B$ and hence $B \subseteq \langle A^* \rangle$. Thus by (i) and (ii) again we get $M = \langle B \rangle \subseteq \langle \langle A^* \rangle \rangle = \langle A^* \rangle \subseteq M$, such that $M = \langle A^* \rangle$. Now, as A is a \vdash basis, if we had $A^* \subset A$, then (ix) would yield $M \neq \langle A^* \rangle$, a contradiction. This is $A = A^*$ and hence we may compute

$$|A| = \left| \bigcup_{b \in B} A_b \right| \le \sum_{b \in B} |A_b| \le |B \times \mathbb{N}| = |B|$$

Hereby $|B \times \mathbb{N}| = |B|$ holds true, as B was assumed to be infinite. Thus we have found $m \leq n$ and by interchanging the roles of A and B we also find $n \leq m$, which had to be shown.

- (xi) As S is independent, $S \subseteq M$ and $M = \langle M \rangle$ we get from (vii) that there is some \vdash basis A of M, with $S \subseteq A \subseteq M$. Thus by (x) we already obtain the claim from $|S| \leq |A| = |B|$.
- (xii) (b) \implies (a) has already been shown in (x), thus it only remains to verify (a) \implies (b): thus consider any \vdash independent subset $S \subseteq M$ with |S| = |B|. As before [S is independent, $S \subseteq M$ and $M = \langle M \rangle$ now use (vii)] there is some \vdash basis A of M, with $S \subseteq A \subseteq M$. Thus by (x) we find $|B| = |S| \leq |A| = |B|$. That is $|A| = |S| = |B| < \infty$ which was assumed to be finite. In particular S is a subset of the finite set A, with the same number of elements #S = #A. Clearly this means S = A and in particular S is a \vdash basis of M.

Proof of (3.30):

(i) (D1): consider an arbitrary subset $X \subseteq M$ and $x \in X$. Then we find $X \vdash x$ simply by choosing $n := 1, x_1 := x$ and $a_1 := 1$, as in this case $a_1x_1 = 1x = x$. (D2): consider any two subsets $X, Y \subseteq M$ such that $Y \vdash X$ and $X \vdash x$. Thus by definition there are some $n \in \mathbb{N}, x_i \in X$ and $a_i \in R$ such that $x = a_1x_1 + \cdots + a_nx_n$. But as $x_i \in X$ and

 $Y \vdash X$ there also are some $m(i) \in \mathbb{N}$, $y_{i,j} \in Y$ and $b_{i,j} \in R$ such that $x_i = b_{i,1}y_{i,1} + \cdots + b_{i,m(i)}y_{i,m(i)}$. Combining these equations, we find

$$x = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} \sum_{j=1}^{m(j)} a_i b_{i,j} y_{i,j}$$

In particular this identity yields $Y \vdash x$, which had to be shown. (D3): consider an arbitrary subset $X \subseteq M$ and $x \in M$ such that $X \vdash x$. Again this means $x = a_1x_1 + \cdots + a_nx_n$ for sufficient $x_i \in X$ and $a_i \in R$. Now let $X_0 := \{x_1, \ldots, x_n\} \subseteq X$. Then X_0 clearly is a finite set and $X_0 \vdash x$, by construction. As (D1), (D2) and (D3) are satisfied, we already obtain (iii), (iv) and (v) from (3.26).

- (ii) The identity $\langle X \rangle = \{ x \in M \mid X \vdash x \} = \ln_R(X)$ is obvious from the definitions of the relation \vdash and the linear hull $\ln_R(X)$. And the identity $\ln_R(X) = \langle X \rangle_{\rm m}$ has already been shown in (3.11).
- (vi) (b) \implies (a): we first prove that *B* is a generating system of *M*: Thus consider any $x \in M$, by assumption there is some $(x_b) \in R^{\oplus B}$ such that $x = \sum_b x_b b$. Now let $\Omega := \{ b \in B \mid x_b \neq 0 \}$. Then $\Omega \subseteq B$ is finite and we further get

$$x = \sum_{b \in B} x_b b = \sum_{b \in \Omega} x_b b \in \operatorname{lh}_R(B)$$

As x has been arbitrary that is $M \subseteq \ln_R(B) = \langle B \rangle_m$. Let us now prove that B also is R-linear independent: thus consider some finite subset $\Omega \subseteq B$ and some $a_b \in R$ (where $b \in \Omega$) such that $\sum_{b \in \Omega} a_b b = 0$. Then for any $b \in B \setminus \Omega$ we let $a_b := 0$ and thereby obtain

$$\sum_{b\in B} a_b b = \sum_{b\in \Omega} a_b b = 0 = \sum_{b\in B} 0 b$$

Due to the uniqueness of this representation (of $0 \in M$) we find $a_b = 0$ for any $b \in B$. And in particular $a_b = 0$ for any $b \in \Omega$. By definition this means that B truly is R-linearly independent.

(vi) (a) \implies (b): Existence: consider any $x \in M$, as $M = \langle B \rangle_{\mathrm{m}} = \mathrm{lh}_{R}(B)$ there are a finite subset $\Omega \subseteq B$ and $a_{b} \in R$ (where $b \in \Omega$) such that $x = \sum_{b \in \Omega} a_{b}b$. Now let $x_{b} := a_{b}$ if $b \in \Omega$ and $x_{b} := 0$ if $b \in B \setminus \Omega$. Then $(x_{b}) \in R^{\oplus B}$ and we also get

$$x = \sum_{b \in \Omega} a_b b = \sum_{b \in B} x_b b$$

Uniqueness: consider any two (x_b) , $(y_b) \in R^{\oplus B}$ representing the same element $\sum_b x_b b = \sum_b y_b b$. Now let $\Omega := \{ b \in B \mid x_b \neq 0, \text{ or } y_b \neq 0 \}$. Then $\Omega \subseteq B$ is finite and we clearly get

$$0 = \sum_{b \in B} (x_b - y_b)b = \sum_{b \in \Omega} (x_b - y_b)b$$

Yet as B is R-linearly independent, this means $x_b - y_b = 0$ for any $b \in \Omega$ and hence $x_b = y_b$ for any $b \in B$ (if $b \notin \Omega$, then $x_b = 0 = y_b$). But this already is the uniqueness of the representation.

Proof of (3.31):

- (i) By $(3.30) \vdash$ already satisfies (D1), (D2) and (D3). Thus it only remains to prove (D4) and we will already do this in the stronger form given in the claim. That is we consider $x \in X$ and $X \vdash y$. By definition of \vdash this is $y = a_1 x_1 + \cdots + a_n x_n$ for some $a_i \in S$ and $x_i \in X$. Of course we may drop any summand with $a_i = 0$ and hence assume $a_i \neq 0$ for any $i \in 1 \dots n$. As $y \neq 0$ we still have $n \geq 1$. Now let $X' := (X \setminus \{x\}) \cup \{y\}$ (that is we have to show $X' \vdash x$) and distinguish two cases: (1) if $x \notin \{x_1, \ldots, x_n\}$ then $\{x_1, \ldots, x_n\} \subseteq X \setminus \{x\} \subseteq X'$ and in particular $X' \vdash x$. (2) if $x \in \{x_1, \ldots, x_n\}$ we may assume $x = x_1$ without loss of generality. Now let $b_i := -a_1^{-1}a_i \in S$ (for any $i \in 2...n$, then $x = x_1 = a_1^{-1}a_1x_1 = b_2x_2 + \cdots + b_nx_n$. And as $\{x_2, \ldots, x_n\} \subseteq X \setminus \{x\} \subseteq X'$ this implies $X' \vdash x$. Thus we have proved the claim in both cases. From this property we can easily derive (D4): suppose $x \in X$, $X \vdash y$ and $X \setminus \{x\} \not\vdash y$. Then $y \neq 0$, as even $\emptyset \vdash 0$ and hence $X \setminus \{x\} \vdash y$. Thus we may apply this property to find $X' \vdash x$, which had to be shown.
- (ii) (b) \implies (a): suppose there was some $x \in X$ such that $X \setminus \{x\} \vdash x$. So by definition there would be some elements $x_i \in X \setminus \{x\}$ and $a_i \in S$ (where $i \in 1 \dots n$) such that $x = a_1x_1 + \dots + a_nx_n$. Now let $x_0 := x$ and $a_0 := -1$, then we get $x_i \in X$ for any $i \in 1 \dots n$ and also $a_0x_0 + a_1x_1 + \dots + a_nx_n = 0$. But as $a_0 \neq 0$ this means that X is S-linear dependent, a contradiction. Thus there is no such $x \in X$ and this is the \vdash independence of X.

(a) \implies (b): suppose there were some (pairwise distinct) elements $x_i \in X$ and $a_i \in R$ (where $i \in 1...n$) such that (without loss of generality) $a_1 \neq 0$ and $a_1x_1 + \cdots + a_nx_n = 0$. As $a_1 \neq 0$ we may let $b_i := -a_1^{-1}a_i$ for $i \in 2...n$. Then $x_1 = a_1^{-1}a_1x_1 = b_2x_2 + \cdots + b_nx_n$ and hence $\{x_2, \ldots, x_n\} \vdash x_1$. As $\{x_2, \ldots, x_n\} \subseteq X \setminus \{x_1\}$ this yields $X \setminus \{x_1\} \vdash x_1$, that is X is \vdash dependent, a contradiction. Thus

there are no such x_i and a_i and this again means, that X is S-linearly independent.

- (iv) As $\langle B \rangle = \ln_S(B)$ S-generation and \vdash -generation are equivalent notions. And in (ii) we have seen that \vdash -dependence and S-linear dependence are equivalent, too. In particular we find (a) \iff (b) according to the respective definitions of S-bases and \vdash -bases. And the equivalencies (a) \iff (c) \iff (d) have already been proved in (3.26.(ix)). Finally the we have already shown (b) \iff (e) in (3.30.(vi)).
- (iii) This is just a reformulation of (3.26.(v)) in the light of (ii). Likewise (v) resp. (vi) is just the contant of (3.26.(vii)) resp. (3.26.(x)) using the equivalencies (a) \iff (b) of (iv). Finally (vii) and (viii) are repetitions of (3.26.(xi)) and (3.26.(xii)) respectively. All we did was bringing the definition of the dimension into play.

Proof of (2.4):

- (i) Let us abbreviate 𝔅 := ∪𝔅𝔅, as 𝔅 is non-empty there is some 𝔅 ∈ 𝔅.
 And as 𝔅 ⊴_i R is an ideal we have 0 ∈ 𝔅 ∈ 𝔅 and hence 0 ∈ 𝔅. If now a, b ∈ 𝔅 then by construction there are 𝔅, 𝔅 ∈ 𝔅 such that a ∈ 𝔅 and b ∈ 𝔅. As 𝔅 is a chain we may assume 𝔅 ⊆ 𝔅 and hence a ∈ 𝔅, too. Therefore we get a + b ∈ 𝔅 and -a, -b ∈ 𝔅, such that a + b, -a and -b ∈ 𝔅 again. And if finally r ∈ R then ra ∈ 𝔅, such that ra ∈ 𝔅.
- (ii) Let $\mathcal{Z} := \{ \mathfrak{b} \leq_{i} R \mid \mathfrak{a} \subseteq \mathfrak{b} \neq R \}$, then $\mathcal{Z} \neq \emptyset$ since $\mathfrak{a} \in \mathcal{Z}$. Now let $\mathcal{A} \subseteq \mathcal{Z}$ be a chain in \mathcal{Z} , then by (i) we know that $\mathfrak{u} := \bigcup \mathcal{A} \leq_{i} R$ is an ideal of R. Suppose $\mathfrak{u} = R$, then $1 \in \mathfrak{u}$ and hence there would be some $\mathfrak{b} \in \mathcal{A}$ with $1 \in \mathfrak{b}$. But as $\mathfrak{b} \leq_{i} R$ is an ideal this would mean $\mathfrak{b} = R$ in contradiction to $\mathfrak{b} \in \mathcal{A} \subseteq \mathcal{Z}$. Hence we find $\mathfrak{u} \in \mathcal{Z}$ again. But by construction we have $\mathfrak{b} \subseteq \mathfrak{u}$ for any $\mathfrak{b} \in \mathcal{A}$, that is \mathfrak{u} is an upper bound of \mathcal{A} . Hence by the lemma of Zorn there is some maximal element $\mathfrak{m} \in \mathcal{Z}^*$. It only remains to show that \mathfrak{m} is maximal: as $\mathfrak{m} \in \mathcal{Z}$ it is an non-full ideal $\mathfrak{m} \neq R$. And if $R \neq \mathfrak{b} \leq_{i} R$ is another non-full ideal with $\mathfrak{m} \subseteq \mathfrak{b}$ then $\mathfrak{a} \subseteq \mathfrak{m} \subseteq \mathfrak{b}$ implies $\mathfrak{b} \in \mathcal{Z}$. But now it follows that $\mathfrak{b} = \mathfrak{m}$ since $\mathfrak{m} \in \mathcal{Z}^*, \mathfrak{b} \in \mathcal{Z}$ and $\mathfrak{m} \subseteq \mathfrak{b}$.
- (iii) Let $a \in R^*$ be a unit of R and $\mathfrak{m} \leq_{\mathbf{i}} R$ be a maximal ideal. Then $a \notin \mathfrak{m}$, as else $1 = a^{-1}a \in \mathfrak{m}$ and hence $\mathfrak{m} = R$. From this we get $R^* \subseteq R \setminus \bigcup \operatorname{smax} R$. For the converse inclusion we go to complements and prove $R \setminus R^* \subseteq \bigcup \operatorname{smax} R$ instead. Thus let $a \in R$ be a non-unit $a \notin R^*$, then $1 \notin aR$ and hence $aR \neq R$. Thus by (i) there is a maximal ideal $\mathfrak{m} \leq_{\mathbf{i}} R$ containing $a \in aR \subseteq \mathfrak{m} \subseteq \bigcup \operatorname{smax} R$. Thus we also have $a \in \bigcup \operatorname{smax} R$ which had to be proved.

(iv) If R = 0 is the zero-ring, then $R = \{0\}$ is the one and only ideal of R. But as this ideal is full, it cannot be maximal and hence smax $R = \emptyset$. If $R \neq 0$ then $\mathfrak{a} := \{0\}$ is a non-full ideal of R. Hence by (ii) there is a maximal ideal $\mathfrak{m} \in \operatorname{smax} R$ containing it. In particular smax $R \neq \emptyset$.

Proof of (2.5):

• (a) \implies (c)

If $\overline{\mathfrak{a}} \leq_{i} R/\mathfrak{m}$ is an ideal, then by the correspondence theorem it is of the form $\overline{\mathfrak{a}} = \mathfrak{a}/\mathfrak{m}$ for some ideal $\mathfrak{a} \leq_{i} R$ with $\mathfrak{m} \subseteq \mathfrak{a}$. But as \mathfrak{m} is maximal this means $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$. Thus we have $\overline{\mathfrak{a}} = \{0 + \mathfrak{m}\}$ (in the case $\mathfrak{a} = \mathfrak{m}$) or $\overline{\mathfrak{a}} = R/\mathfrak{m}$ (in the case $\mathfrak{a} = R$).

• (c) \implies (b)

 R/\mathfrak{m} is a non-zero (since $\mathfrak{m} \neq R$) commutative ring (since R is such). But it has already been shown that a commutative ring is a field if and only if it only contains the trivial ideals (viz. section 1.5).

• (b) \implies (d)

Let $a \notin \mathfrak{m}$, this means $a + \mathfrak{m} \neq 0 + \mathfrak{m}$. And as R/\mathfrak{m} is a field there is some $b \in R$ such that $b + \mathfrak{m}$ is inverse to $a + \mathfrak{m}$. That is

$$ab + \mathfrak{m} = (a + \mathfrak{m})(b + \mathfrak{m}) = 1 + \mathfrak{m}$$

Therefore there is some $m \in \mathfrak{m}$ such that $1 = ab + m \in aR + \mathfrak{m}$ and hence we have truly obtained $aR + \mathfrak{m} = R$.

• (d) \implies (a)

Suppose $\mathfrak{a} \leq_{i} R$ is some ideal with $\mathfrak{m} \subseteq \mathfrak{a}$. We want to show that \mathfrak{m} is maximal hence if $\mathfrak{a} = \mathfrak{m}$ then we are done. Else there is some $a \in \mathfrak{a}$ with $a \notin \mathfrak{m}$. Hence we get $aR + \mathfrak{m} = R$. But as $a \in \mathfrak{a}$ and $\mathfrak{m} \subseteq \mathfrak{a}$ we get $R = aR + \mathfrak{m} \subseteq \mathfrak{a} \subseteq R$.

Proof of (2.6):

- \neg (a) $\implies \neg$ (b): by assumption \neg (a) there is some maximal ideal $\mathfrak{M} \leq_{\mathbf{i}} R$ such that $j \notin \mathfrak{M}$. Hence we have $\mathfrak{M} + jR = R$ such that is there is some $b \in R$ (let a := -b) such that $1 aj = 1 + bj = 1 \in R^*$.
- \neg (b) $\implies \neg$ (a): by assumption \neg (b) there is some $a \in R$ such that $1 aj \notin R^*$. That is $(1 aj)R \neq R$ is a non-full ideal and hence there is a maximal ideal $\mathfrak{m} \leq_i R$ containing it $1 aj \in (1 aj)R \subseteq \mathfrak{m}$ by
(2.4.(ii)). If we now had $j \in \operatorname{JAC} R \subseteq \mathfrak{m}$ then also $aj \in \mathfrak{m}$ and hence we would arrive at the contradiction

$$1 = (1 - aj) + aj \in \mathfrak{m}$$

- (a) \implies (b): if $j \in \mathfrak{a} \subseteq \operatorname{JAC} R$ then we let a := -1 and as we have just proved above this yields $1 + j = 1 aj \in R^*$ and hence (b).
- (b) \implies (c): first of all we have $1 \in 1 + \mathfrak{a}$ since $0 \in \mathfrak{a}$. Now consider any a = 1 + j and $b = 1 + k \in 1 + \mathfrak{a}$, that is j and $k \in \mathfrak{a}$. Then $ab = 1 + (j + k + jk) \in 1 + \mathfrak{a}$ again, as $j + k + jk \in \mathfrak{a}$. Further we get

$$(1+j)(1-(1+j)^{-1}j) = (1+j)-j = 1$$

which implies $a^{-1} = (1+j)^{-1} = 1 - (1+j)^{-1}j$. And hence we also have $a^{-1} \in 1 + \mathfrak{a}$, since $-(1+j)^{-1}j \in \mathfrak{a}$ due to $j \in \mathfrak{a}$.

• (c) \implies (a): fix $j \in \mathfrak{a}$ and consider any $a \in R$. Then we also get $-aj \in \mathfrak{a}$ and hence $1 - aj \in 1 + \mathfrak{a} \subseteq R^*$ by assumption. But as we have alredy proved above $1 - aj \in R^*$ for any $a \in R$ means $j \in JACR$.

Proof of (2.9):

- (a) ⇒ (b): consider a, b ∈ R such that 0+p = (a+p)(b+p) = ab+p. That is ab ∈ p and as p is assumed to be prime this implies a ∈ p or b ∈ p. This again means that a + p = 0 + p or b + p = 0 + p and hence R/p is an integral domain. But R/p ≠ 0 is clear, since p ≠ R and hence 1 + p ≠ 0 + p.
- (b) ⇒ (c): since R/p ≠ 0 is non-zero we have 1 + p ≠ 0 + p or in other words 1 ∉ p which already is (1). Now let u, v ∈ R \ p, then u + p ≠ 0 + p and v + p ≠ 0 + p. But as /p is an integral domain this then yields uv + p = (u + p)(v + p) ≠ 0 + p. Thus we also have uv ∉ p which is (2).
- (c) \implies (a): since $1 \in R \setminus \mathfrak{p}$ we have $\mathfrak{p} \neq R$. Now consider $a, b \in R$ with $ab \in \mathfrak{p}$. Supposed we had $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$ then $a, b \in R \setminus \mathfrak{p}$ and hence $ab \in R \setminus \mathfrak{p}$, a contradiction. Thus we truly have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.
- (a) \implies (d): consider two ideals $\mathfrak{a}, \mathfrak{b} \leq_i \mathbb{R}$ such that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Suppose neither $\mathfrak{a} \subseteq \mathfrak{p}$ nor $\mathfrak{b} \subseteq \mathfrak{p}$ was true. That is there would be $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a, b \notin \mathfrak{p}$. Then $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. But as \mathfrak{p} has is prime this yields $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, a contradiciton.

• (d) \implies (a): consider $a, b \in R$ with $ab \in \mathfrak{p}$. Then we let $\mathfrak{a} := aR$ and $\mathfrak{b} := bR$. Then $\mathfrak{ab} = abR \subseteq \mathfrak{p}$ by (1.37), hence we find $a \in aR = \mathfrak{a} \subseteq \mathfrak{p}$ or $b \in bR = \mathfrak{b} \subseteq \mathfrak{p}$ by assumption. As we have also assumes $\mathfrak{p} \neq R$, this means that \mathfrak{p} is prime.

Proof of (2.7):

Let $i \neq j \in 1...k$, then $\mathfrak{m}_i \subseteq \mathfrak{m}_j$ would imply $\mathfrak{m}_i = \mathfrak{m}_j$ (since \mathfrak{m}_i is maximal and $\mathfrak{m}_j \neq R$). Hence there is some $a_i \in \mathfrak{m}_i$ with $a_i \notin \mathfrak{m}_j$. And as we have just seen in (2.5) this means $a_iR + \mathfrak{m}_j = R$. But as $a_i \in \mathfrak{m}_i$ we find $R = a_iR + \mathfrak{m}_j \subseteq \mathfrak{m}_i + \mathfrak{m}_j \subseteq R$. Hence the \mathfrak{m}_i are pairwise coprime. And the second claim follows from this, as we have proved in (1.39.iv).

Hence it remains to prove the third statement, i.e. the strict desent of the chain $\mathfrak{M}_1 \supset \mathfrak{M}_1 \mathfrak{M}_2 \supset \ldots \supset \mathfrak{M}_1 \ldots \mathfrak{M}_k$. To do this we use induction on k (the foundation k = 1 is trivial), and let $\mathfrak{a} := \mathfrak{M}_1 \ldots \mathfrak{M}_k$ and $\mathfrak{M} := \mathfrak{M}_{k+1}$. For any $i \in 1 \ldots k$ there are $a_i \in \mathfrak{M}_i$ such that $a_i \notin \mathfrak{M}$ again. Now let $a := a_1 \ldots a_k \in \mathfrak{a}$. Then $a \notin \mathfrak{M}$, as maximal ideals are prime (see the remark to (2.9) or (2.19) for a proof) and hence $a = a_1 \ldots a_k \in \mathfrak{M}$ would imply $a_i \in \mathfrak{M}$ for some $i \in 1 \ldots k$. In particular $a \notin \mathfrak{A} \subseteq \mathfrak{M} \subseteq \mathfrak{M}$, that is we have found the induction step

$$a \in (\mathfrak{m}_1 \dots \mathfrak{m}_k) \setminus (\mathfrak{m}_1 \dots \mathfrak{m}_k \mathfrak{m}_{k+1})$$

Proof of (2.11):

- (i) We will prove the statement by induction on k the case k = 1 being trivial. So let now k ≥ 2 and let a := a₁...a_{k-1} and b := a_k. Then ab = a₁...a_{k-1}a_k ∈ 𝔅, but as 𝔅 is prime this implies a ∈ 𝔅 or b ∈ 𝔅. If b ∈ 𝔅 then we are done (with i := k). If not then a = a₁...a_{k-1} ∈ 𝔅, so by induction hypothesis we get a_i ∈ 𝔅 for some i ∈ 1...k 1.
- (ii) Analogous to (i) we prove this statement by induction on k the case k = 1 being trivial again. For $k \ge 2$ we likewise let $\mathfrak{a} := \mathfrak{a}_1 \dots \mathfrak{a}_{k-1}$ and $\mathfrak{b} := \mathfrak{a}_k$. Then $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ due to (2.9). If $\mathfrak{b} \subseteq \mathfrak{p}$ then we are done with i := k. Else $\mathfrak{a} \subseteq \mathfrak{p}$ and hence $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some $i \in 1 \dots k 1$ by induction hypothesis.
- (iii) Let us choose a subset $I \subseteq 1 \dots n$ such that \mathfrak{a} is contained in the union of the \mathfrak{h}_i $(i \in I)$ with a minimal number of elements. That is

$$\mathfrak{a} \subseteq \bigcup_{i\in I}\mathfrak{b}_i$$

$$\forall J \subseteq 1 \dots n \; : \; \mathfrak{a} \subseteq \bigcup_{i \in J} \mathfrak{b}_i \implies \#I \leq \#J$$

It is clear that this can be done, since $J = 1 \dots n$ suffices to cover \mathfrak{a} and the number of elements is a total order and hence allows to pick a minimal element. In the following we will prove that I contains precisely one element. And in this case $I = \{i\}$ we clearly have $\mathfrak{a} \subseteq \mathfrak{b}_i$ as claimed. Thus let us assume $\#I \geq 2$ and derive a contradiction: consider some fixed $j \in I$, as I has minimally many elements we have

$$\mathfrak{a} \not\subseteq \bigcup_{j
eq i \in I} \mathfrak{b}_i$$

That is there is some $a_j \in \mathfrak{a}$ such that $a_j \notin \mathfrak{b}_i$ for any $j \neq i \in I$. In particular we find $a_i \in \mathfrak{b}_i$, as the \mathfrak{b}_i $(i \in I)$ cover \mathfrak{a} . Let us pick one such a_j for every $j \in I$. If #I = 2 then we may assume $I = \{1, 2\}$ without loss of generality. As a_1 and $a_2 \in \mathfrak{a}$ we also have $a_1 + a_2 \in \mathfrak{a}$. Suppose we had $a_1 + a_2 \in \mathfrak{h}_1$ then $a_2 = (a_1 + a_2) + (-a_1) \in \mathfrak{h}_1$ as well, a contradiction. Likewise we find that $a_1 + a_2 \notin \mathfrak{b}_2$. But now $a_1 + a_2 \in \mathfrak{a} \subseteq \mathfrak{b}_1 \cup \mathfrak{b}_2$ provides a contradiction. Hence #I = 2cannot be. Now assume $\#I \ge 3$, then by assumption there is some $k \in I$ such that \mathfrak{b}_k is prime. Without loss of generality (that is by renumbering) we may assume $I = 1 \dots m$ and \mathfrak{b}_1 to be prime. As any $a_i \in \mathfrak{a}$ we also have $a_1 + a_2 \dots a_m \in \mathfrak{a}$. Suppose $a_1 + a_2 \dots a_m \in \mathfrak{b}_i$ for some $i \in 2...m$, then $a_1 = (a_1 + a_2...a_m) + (-a_2...a_m) \in \mathfrak{b}_i$ too, a contradiction. And if we suppose $a_1 + a_2 \dots a_m \in \mathfrak{b}_1$ then $a_2 \dots a_m = (a_1 + a_2 \dots a_m) + (-a_1) \in \mathfrak{h}_1$ too. As \mathfrak{h}_1 is prime we find $a_i \in \mathfrak{b}_1$ for some $i \in 2 \dots m$ due to (i). But this is a contradiction, altogether $a_1 + a_2 \dots a_m$ is contained in \mathfrak{a} but none of the \mathfrak{b}_i for $i \in I$, a contradiction. Hence the assumption $\#I \geq 3$ has to be abandoned, which only leaves #I = 1.

Proof of (2.13):

- We will first show the well-definedness of spec (φ) it is clear that φ⁻¹(𝔅) = { a ∈ R | φ(a) ∈ 𝔅 } is an ideal in R. Thus it only remains to show that φ⁻¹(𝔅) ∈ X truly is prime. First of all φ⁻¹(𝔅) ≠ R as else 1 ∈ φ⁻¹(𝔅) and this would mean 1 = φ(1) ∈ 𝔅. But this is absurd, as 𝔅 is prime and hence 𝔅 ≠ S. Hence we consider ab ∈ φ⁻¹(𝔅), i.e. φ(ab) = φ(a)φ(b) ∈ 𝔅. As 𝔅 ∈ Y is prime, this yields φ(a) ∈ 𝔅 or φ(b) ∈ 𝔅, that is a ∈ φ⁻¹(𝔅) or b ∈ φ⁻¹(𝔅) again.
- Next we will show that for any $a \in R$ we have $(\operatorname{spec} \varphi)^{-1}(X_a) = Y_{\varphi(a)}$. But this is immediate from elementary set theory, since

$$(\operatorname{spec}\varphi)^{-1}(X_a) = \{ \mathfrak{q} \in Y \mid a \notin \varphi^{-1}(\mathfrak{q}) \} = Y_{\varphi(a)}$$

• Likewise $(\operatorname{spec} \varphi)(\mathbb{V}(\mathfrak{b})) \subseteq \mathbb{V}(\varphi^{-1}(\mathfrak{b}))$ is completely obvious, once we translate these sets back into set-theory, then we have to show

$$\left\{ \varphi^{-1}(\mathfrak{q}) \mid \mathfrak{b} \subseteq \mathfrak{q} \in Y \right\} \subseteq \left\{ \mathfrak{p} \in X \mid \varphi^{-1}(\mathfrak{b}) \subseteq \mathfrak{p} \right\}$$

Thus we have to show that $\mathfrak{b} \subseteq \mathfrak{q} \in Y$ implies $\varphi^{-1}(\mathfrak{b}) \subseteq \varphi^{-1}(\mathfrak{q}) \in X$. But $\mathfrak{b} \subseteq \mathfrak{q}$ clearly implies $\varphi^{-1}(\mathfrak{b}) \subseteq \varphi^{-1}(\mathfrak{q})$ and we have just proved, that $\varphi^{-1}(\mathfrak{q}) \in X$ as well.

• Finally it remains to prove $(\operatorname{spec} \varphi)^{-1}(\mathbb{V}(\mathfrak{a})) = \mathbb{V}(\langle \varphi(\mathfrak{a}) \rangle_i)$. So let us first translate the claim back into elementary set-theory again

$$\left\{ \mathfrak{q} \in Y \mid \mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q}) \right\} = \left\{ \mathfrak{q} \in Y \mid \varphi(\mathfrak{a}) \subseteq \mathfrak{q} \right\}$$

But by definition we have $\varphi^{-1}(\mathfrak{q}) = \{ a \in R \mid \varphi(a) \in \mathfrak{q} \}$, and hence the inclusion $\mathfrak{q} \subseteq \varphi^{-1}(\mathfrak{q})$ trivially implies $\varphi(\mathfrak{q}) \subseteq \mathfrak{q}$ and vice versa.

Proof of (2.14):

(i) First of all $\mathfrak{a} := \bigcap \mathcal{P}$ is an ideal of R, due to (1.30). And if we pick any $\mathfrak{p} \in \mathcal{P}$ then $\mathfrak{a} \subseteq \mathfrak{p}$. As $1 \notin \mathfrak{p}$ we also have $1 \notin \mathfrak{a}$ and hence $\mathfrak{a} \neq R$. Now let

$$U := R \setminus \mathfrak{a} = \bigcup \{ R \setminus \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P} \}$$

Then $1 \in U$ as we have just seen. And for any $u, v \in U$ there are \mathfrak{p} , $\mathfrak{q} \in \mathcal{P}$ such that $u \in R \setminus \mathfrak{p}$ and $v \in R \setminus \mathfrak{q}$. But as \mathcal{P} is a chain we may assume $\mathfrak{p} \subseteq \mathfrak{q}$ and hence $v \in R \setminus \mathfrak{q} \subseteq R \setminus \mathfrak{p}$, as well. As \mathfrak{p} is a prime ideal $R \setminus \mathfrak{p}$ is multimplicatively closed, so $u, v \in R \setminus \mathfrak{p}$ implies $uv \in R \setminus \mathfrak{p}$ and hence $uv \in U$. That is U is multiplicatively closed and hence \mathfrak{a} is a prime ideal.

- (ii) Clearly *P* is partially ordered under the inverse inclusion relation "⊇" (as *P* ≠ Ø). Now let *O* ⊆ *P* be a chain in *P*, then by (i) we know that p := ∩ *O* ⊴_i *R* is prime. Now pick any q ∈ *O*, then as p ⊆ q and the assumption on *P* we find p ∈ *P*. Hence p is a ⊇-upper bound of *O*. And by the lemma of Zorn this yields that *P* contains a ⊇-maximal element p_{*}. But clearly ⊇-maximal is ⊆-minimal and hence p_{*} ∈ *P**.
- (iii) Let us take $\mathcal{Z} := \{ \mathfrak{p} \in \operatorname{spec} R \mid \operatorname{condition}(\mathfrak{p}) \}$, then \mathcal{Z} is partially ordered under the inverse inclusion " \supseteq " of sets. In any case $\mathcal{Z} \neq \emptyset$ is non-empty: if we imosed *none* then by assumption $R \neq 0$ and hence R has a maximal (in particular prime) ideal due to (2.4.(iv)). If we imposed $\mathfrak{p} \subseteq \mathfrak{q}$ then $\mathfrak{q} \in \mathcal{Z}$. If we imposed $\mathfrak{a} \subseteq \mathfrak{p}$ then by assumption $\mathfrak{a} \neq R$ and hence there is a maximal (in particular prime) ideal \mathfrak{m} containing $\mathfrak{a} \subseteq \mathfrak{m}$ due to (2.4.(ii)) again. Finally if we supposed

 $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{q}$ then we assumed $\mathfrak{a} \subseteq \mathfrak{q}$ and hence $\mathfrak{q} \in \mathcal{Z}$. Now let $\mathcal{P} \subseteq \mathcal{Z}$ be any chain in \mathcal{Z} and $\mathfrak{p} := \bigcap \mathcal{P}$. Then by (i) \mathfrak{p} is a prime ideal of R again. Also $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \subseteq \mathfrak{q}$ are clear (if they have been imposed). Hence $\mathfrak{p} \in \mathcal{Z}$ is an upper bound of \mathcal{P} (under \supseteq). And hence there is a maximal element $\mathfrak{p}_* \in \mathcal{Z}^*$ by the lemma of Zorn. But as \mathfrak{p}_* is maximal with respect to \supseteq it is minimal with respect to \subseteq .

- (iv) By assumption $\mathfrak{a} \subseteq \mathfrak{q}$ and (iii) there is some prime ideal \mathfrak{p}_* minimal among the ideals $\mathfrak{p}_* \in \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{q}\}_*$ and in particular $\mathfrak{a} \subseteq \mathfrak{p}_* \subseteq \mathfrak{q}$. It remains to prove, that \mathfrak{p}_* also is a minimal element of $\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\}$. Thus suppose we are given any prime ideal \mathfrak{p} with $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{p} \subseteq \mathfrak{p}_*$. Then in particular $\mathfrak{p} \subseteq \mathfrak{q}$ and by the minimality of \mathfrak{p}_* this then implies $\mathfrak{p} = \mathfrak{p}_*$. Thus \mathfrak{p}_* even is minimal in this larger set.
- (v) Let us take $\mathcal{Z} := \{ \mathfrak{b} \leq_{i} R \mid \mathfrak{a} \subseteq \mathfrak{b} \subseteq R \setminus U \}$, then \mathcal{Z} is partially ordered under " \subseteq ". Clearly $\mathcal{Z} \neq \emptyset$ is nonempty, since $\mathfrak{a} \in \mathbb{Z}$, as we have assumed $\mathfrak{a} \cap U = \emptyset$. Now let $\mathcal{B} \subseteq \mathcal{Z}$ be any chain in \mathcal{Z} , then $\mathfrak{c} := \bigcup \mathcal{B}$ is an ideal, due to (2.4). And if we pick any $\mathfrak{b} \in \mathcal{B}$ then $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{c}$ and hence $\mathfrak{a} \subseteq \mathfrak{c}$. And if $b \in \mathfrak{c}$ then there is some $\mathfrak{b} \in \mathcal{B} \subseteq \mathcal{Z}$ such that $b \in \mathfrak{b} \subseteq R \setminus U$. Hence we also find $\mathfrak{c} \subseteq R \setminus U$ such that $\mathfrak{c} \in \mathcal{Z}$ again. That is we have found an upper bound \mathfrak{c} of \mathcal{B} . Hence there is a maximal element $\mathfrak{b}^* \in \mathcal{Z}$ by the lemma of Zorn. Now let $\mathfrak{p} \in \mathcal{Z}^*$ be any maximal element of \mathcal{Z} . As $\mathfrak{p} \subseteq R \setminus U$ and $1 \in U$ we have $1 \notin \mathfrak{p}$ such that $\mathfrak{p} \neq R$ is non-full. Now consider any $a, b \in R$ such that $ab \in \mathfrak{p}$ but suppose $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$. As we have $\mathfrak{p} \subset \mathfrak{p} + aR$ and $\mathfrak{p} \in \mathcal{Z}^*$ is maximal we have $(\mathfrak{p} + aR) \not\subseteq R \setminus U$. That is we may choose $u \in (\mathfrak{p} + aR) \cap U$. That is $u = p + \alpha a$ for some $p \in \mathfrak{p}$ and $\alpha \in R$. Analogously we can find some $v = q + \beta b \in (\mathfrak{p} + bR) \cap U$ with $q \in \mathfrak{p}$ and $\beta \in R$. Thereby we get

$$uv = (p + \alpha a)(q + \beta b) = pq + \alpha aq + \beta bp + \alpha \beta ab \in \mathfrak{p}$$

since p, q and $ab \in \mathfrak{p}$. But as U is multiplicatively closed and $u, v \in U$ we also have $uv \in U$. That is $uv \in \mathfrak{p} \cap U$, a contradiction to $\mathfrak{p} \in \mathcal{Z}$. Hence we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ which means that \mathfrak{p} is prime.

Proof of (2.17):

(i) First of all $\mathfrak{a} \subseteq \mathfrak{a} : b$, because if $a \in \mathfrak{a}$ then also $ab \in \mathfrak{a}$, as \mathfrak{a} is an ideal. Next we will prove that $\mathfrak{a} : b \leq_i R$ is an ideal of R. It is clear that $0 \in \mathfrak{a} : b$ since $0b = 0 \in \mathfrak{a}$. Let now p and $q \in \mathfrak{a} : b$, that is pb and $qb \in \mathfrak{a}$. Then $(p+q)b = pb + qb \in \mathfrak{a}, (-p)b = (-pb) \in \mathfrak{a}$ and for

any $a \in R$ we also get $(ap)b = a(pb) \in \mathfrak{a}$ which means p + q, -p and $ap \in \mathfrak{a} : b$ respectively.

(ii) First of all a ⊆ √a, because if a ∈ a then for k = 1 we get a^k = a ∈ a. Next we will prove that √a ≤_iR is an ideal. It is clear that 0 ∈ a ⊆ √a. Now let a and b ∈ √a that is a^k ∈ a and b^l ∈ a for some k, l ∈ N. Then we get

$$\begin{array}{rcl} (-a)^{k} &=& (-1)^{k}a^{k} \\ (ab)^{l} &=& a^{l}b^{l} \\ (a+b)^{k+l} &=& \sum_{i=0}^{k+l}\binom{k+l}{i}a^{i}b^{k+l-i} \\ &=& \sum_{i=0}^{k}\binom{k+l}{i}a^{i}b^{k+l-i} + \sum_{i=k+1}^{k+l}\binom{k+l}{i}a^{i}b^{k+l-i} \\ &=& \sum_{i=0}^{k}\binom{k+l}{i}a^{i}b^{k+l-i} + \sum_{j=1}^{l}\binom{k+l}{k+j}a^{k+j}b^{l-j} \\ &=& \left(\sum_{i=0}^{k}\binom{k+l}{i}a^{i}b^{k-i}\right)b^{l} + \left(\sum_{j=1}^{l}\binom{k+l}{k+j}a^{j}b^{l-j}\right)a^{k} \end{array}$$

As all these elements are contained in \mathfrak{a} again, we again found a + b, -a and $ab \in \sqrt{\mathfrak{a}}$. Thus it remains to prove that $\sqrt{\mathfrak{a}}$ is a radical ideal. Thus let $a \in R$ be contained in the radical of $\sqrt{\mathfrak{a}}$, that is $a^k \in \sqrt{\mathfrak{a}}$ for some $k \in \mathbb{N}$. And hence there is some $l \in \mathbb{N}$ such that $a^{kl} = (a^k)^l \in \mathfrak{a}$. But this already means $a \in \sqrt{\mathfrak{a}}$ and the converse inclusion is clear.

- (iii) If $a \in \mathfrak{a} : b$ then $ab \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $a \in \mathfrak{b} : b$ again. Likewise if we are given $a \in \sqrt{\mathfrak{a}}$ then there is some $k \in \mathbb{N}$ such that $a^k \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $a \in \sqrt{\mathfrak{b}}$ already.
- (iv) If 1 ∈ R = a : b then b = 1b ∈ a. And if b ∈ a then for any a ∈ R we have ab ∈ a, since a is an ideal. But this also means a : b = R. Now let p be a prime ideal of R, if b ∈ p then we have alredy seen p : b = R. Thus assume b ∉ p. Then a ∈ p : b is equivalent to ab ∈ p for any a ∈ R. But as p is prime this implies a ∈ p or b ∈ p. The latter is untrue by assumption so we get a ∈ p. That is we have proved p : b ⊆ p and the converse inclusion has been proved in (i) generally.
- (v) If $\emptyset \neq \mathcal{A} \subseteq \operatorname{srad} R \subseteq \operatorname{ideal} R$, then the intersection $\bigcap \mathcal{A} \trianglelefteq_i R$ already is an ideal of R due to (1.30). Thus it remains to show that $\bigcap \mathcal{A}$ is radical. Let $a^k \in \bigcap \mathcal{A}$, that is $a^k \in \mathfrak{a}$ for any $\mathfrak{a} \in \mathcal{A}$. But as \mathfrak{a} is radical we find that $a \in \mathfrak{a}$. As this is true for any $\mathfrak{a} \in \mathcal{A}$ we found $a \in \bigcap \mathcal{A}$.

(v) Consider any $a \in R$, then a is contained in the intersection of all $\mathfrak{a}_i : \mathfrak{b}$ iff $a \in \mathfrak{a}_i : b$ for any $i \in I$. And this again is equivalent to $ab \in \mathfrak{a}_i$ for any $i \in I$. Thus we have already found the equivalence

$$a \in \bigcap_{i \in I} (\mathfrak{a}_i : b) \iff ab \in \bigcap_{i \in I} \mathfrak{a}_i \iff a \in \left(\bigcap_{i \in I} \mathfrak{a}_i\right) : b$$

Proof of (2.18):

(c) \iff (a) is trivial and so is (a) \implies (b). For the converse implication it suffices to remark, that $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ is true for any ideal $\mathfrak{a} \leq_{\mathbf{i}} R$ (as $a \in \mathfrak{a}$ implies $a = a^1 \in \mathfrak{a}$). Thus we prove (a) \implies (d): Let $b + \mathfrak{a}$ be a nilpotent of R/\mathfrak{a} , that is $b^k + \mathfrak{a} = (b + \mathfrak{a})^k = 0 + \mathfrak{a}$ for some $k \in \mathbb{N}$. This means $b^k \in \mathfrak{a}$ and hence $b \in \sqrt{\mathfrak{a}} \subseteq \mathfrak{a}$ by assumption. And from $b \in \mathfrak{a}$ we find $b + \mathfrak{a} = 0 + \mathfrak{a}$. Conversely (d) \implies (c): consider any $b \in R$ such that $b^k \in \mathfrak{a}$. Then $(b + \mathfrak{a})^k = b^k + \mathfrak{a} = 0 + \mathfrak{a}$ and hence $b + \mathfrak{a}$ is a nilpotent of R/\mathfrak{a} . By assumption this means $b + \mathfrak{a} = 0 + \mathfrak{a}$ or in other words $b \in \mathfrak{a}$.

Proof of (2.19):

The equivalencies of the respective properties of the ideal and its quotioent ring have been shown in (2.5), (2.9) and (2.18) respectively. Hence if $\mathfrak{m} \leq_{i} R$ is maximal then R/\mathfrak{m} is a field. In particular R/\mathfrak{m} is a non-zero integral domain which means that \mathfrak{m} is prime. And if $\mathfrak{p} \leq_{i} R$ is prime, then R/\mathfrak{p} is an integral domain and hence reduced which again means that \mathfrak{p} is a radical ideal. Yet we also wish to present a direct proof of this:

M maximal ⇒ M prime: consider a, b ∈ M with ab ∈ M, but suppose a ∉ M and b ∉ M. This means M ⊂ M + aR and hence M + aR = R, as M is maximal. Hence there are m ∈ M and α ∈ R such that m+αa = 1. Likeweise there are n ∈ M and β ∈ R such that n + βb = 1. Thereby

$$1 = (m + \alpha a)(n + \beta b) = mn + \alpha an + \beta bm + \alpha \beta ab$$

But as m, n and $ab \in \mathfrak{m}$ we hence found $1 \in \mathfrak{m}$ which means $\mathfrak{m} = R$. But this contradicts \mathfrak{m} being maximal.

• \mathfrak{p} prime $\implies \mathfrak{p}$ radical: consider $a \in R$ with $a^k \in \mathfrak{p}$. As \mathfrak{p} is prime we have $k \ge 0$ (as else $1 = a^0 \in \mathfrak{p}$ such that $\mathfrak{p} = R$). But \mathfrak{p} is prime and hence $a^k \in \mathfrak{p}$ for some $k \ge 1$ implies $a \in \mathfrak{p}$ due to (2.11.(i)). This means that \mathfrak{p} is radical, due to (2.18.(c)).

Proof of (2.20):

- (i) We have to prove √a = ∩ { 𝔅 | 𝔅 ⊆ 𝔅}. Thereby the inclusion "⊆" is clear, as any 𝔅 contains 𝔅. For the converse inclusion we are given some a ∈ R such that a ∈ 𝔅 for any prime ideal 𝔅 ⊴_i R with 𝔅 ⊆ 𝔅. Now let U := { 1, a, a², ... }, then it is clear that U is multiplicatively closed. Suppose 𝔅 ∩ U = ∅, then by (2.14.(iv)) there is an ideal 𝔅 ⊴_i R maximal with 𝔅 ⊆ 𝔅 ⊆ R \ U. And this ideal 𝔅 is prime. But as 𝔅 ∩ U = ∅ and a ∈ U we have a ∉ 𝔅 even though 𝔅 is a prime ideal with 𝔅 ⊆ 𝔅. A contradiction. Thus we have 𝔅 ∩ U ≠ ∅, that is there is some b ∈ U such that b ∈ 𝔅. By construction of U b is of the form b = a^k for some k ∈ ℕ. And this means a ∈ √𝔅.
- (i) Let us denote $\mathbb{V}(\mathfrak{a}) := \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \}$ and $\mathcal{M} := \mathbb{V}(\mathfrak{a})_*$. Then in (i) above we have just seen the identity

$$\sqrt{\mathfrak{a}} = \bigcap \mathbb{V}(\mathfrak{a})$$

We now have to prove $\bigcap \mathbb{V}(\mathfrak{a}) = \bigcap \mathcal{M}$. As $\mathcal{M} \subseteq \mathbb{V}(\mathfrak{a})$ the inclusion " \subseteq " is clear. For the converse inclusion we are given any $a \in \bigcap \mathcal{M}$ and any $\mathfrak{q} \in \mathbb{V}(\mathfrak{a})$ and need to show $a \in \mathfrak{q}$. But as $\mathfrak{a} \subseteq \mathfrak{q}$ by (i) there is some $\mathfrak{p}_* \in \mathcal{M}$ such that $\mathfrak{a} \subseteq \mathfrak{p}_* \subseteq \mathfrak{p}$. And as $a \in \bigcap \mathcal{M}$ we find $a \in \mathfrak{p}_*$ and hence $a \in \mathfrak{q}$. Thus we have also established inclusion " \supseteq ".

- (ii) By definition it is clear that NIL $R = \sqrt{0}$ is the radical of the zero-ideal. And the further equalities given are immediate from (ii) above.
- (iii) Let $a \in R$ be contained in the radical of $\sqrt{\mathfrak{a}}$, that is $a^k \in \sqrt{\mathfrak{a}}$ for some $k \in \mathbb{N}$. And hence there is some $l \in \mathbb{N}$ such that $a^{kl} = (a^k)^l \in \mathfrak{a}$. But this already means $a \in \sqrt{\mathfrak{a}}$ and the converse inclusion is clear.
- (v) As $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ we have $\sqrt{\mathfrak{a}\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}} \cap \mathfrak{b}$ by (i). Next let $a \in \sqrt{\mathfrak{a}} \cap \mathfrak{b}$, that is there is some $k \in \mathbb{N}$ such that $a^k \in \mathfrak{a} \cap \mathfrak{b}$. Now $a^k \in \mathfrak{a}$ and $a^k \in \mathfrak{b}$ implies $a \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. Finally consider some $a \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, that is $a^i \in \mathfrak{a}$ and $a^j \in \mathfrak{b}$ for some $i, j \in \mathbb{N}$. Then $a^{i+j} = a^i a^j \in \mathfrak{a}\mathfrak{b}$ and hence $a \in \sqrt{\mathfrak{a}}\mathfrak{b}$. Altogether we have proved the following chain of inclusions

$$\sqrt{\mathfrak{a}\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}\cap\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}}\cap\sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}\mathfrak{b}}$$

- (vi) By induction on (v) we know that $\sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}} \cap \cdots \cap \sqrt{\mathfrak{a}}$ (k-times). And this obviously equals $\sqrt{\mathfrak{a}}$ such that we get the equality claimed.
- (iv) In a first step let us assume k = 1, that is $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}}$, then in particular we have $\mathfrak{a} \subseteq \mathfrak{p}$ and hence $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{p}}$. Yet as \mathfrak{p} is prime we also have $\sqrt{\mathfrak{p}} = \mathfrak{p}$ due to (2.19). Thereby we get $\sqrt{\mathfrak{a}} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}}$ by assumption. Now consider an arbitrary $k \in \mathbb{N}$. Then by (vi) we have $\mathfrak{a}^k \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}^k}$. Thus by the case k = 1 (using \mathfrak{a}^k instead of \mathfrak{a}) we get $\mathfrak{p} = \sqrt{\mathfrak{a}^k} = \sqrt{\mathfrak{a}}$, the latter by (vi) again.

(vii) By assumption \mathfrak{a} is finitely generated, that is there are $a_i \in R$ such that $\mathfrak{a} = \langle a_1, \ldots, a_n \rangle_i$. And as \mathfrak{a} is contained in the radical of \mathfrak{b} we find that for any $i \in 1 \ldots n$ there is some $k(i) \in \mathbb{N}$ such that $a_i^{k(i)} \in \mathfrak{b}$. Now let $k := k(1) + \cdots + k(n)$ and consider $f_1, \ldots, f_k \in \mathfrak{a}$. That is

$$f_j = \sum_{i=1}^n f_{i,j} a_i$$

for some $f_{i,j} \in \mathbb{R}$. Using (1.21) we now extract the product of the f_j

$$\prod_{j=1}^{k} f_j = \prod_{j=1}^{k} \sum_{i=1}^{n} f_{i,j} a_i = \sum_{i \in I} \prod_{j=1}^{k} f_{i_j,j} a_{i_j}$$

where $I = (1 \dots n)^k$ and $i = (i_1, \dots, i_k) \in I$. For any $h \in 1 \dots n$ we now let $m(h) := \# \{ j \in 1 \dots k \mid i_j = h \}$ the number of times h appears in the collection of i_j . Then it is clear that $m(1) + \dots + m(n) = k =$ $k(1) + \dots + k(n)$ Hence there has to be some index $h \in 1 \dots n$ such that $k(h) \leq m(h)$. Thereby $a_h^{m(h)}$ divides $a_h^{k(h)} \in \mathfrak{b}$ such that

$$b_i := \prod_{j=1}^k a_{i_j} = \prod_{h=1}^n a_h^{m(h)} \in \mathfrak{b}$$

This now can be used to show $f_1 \dots f_k \in \mathfrak{b}$. Simply rearrange to find

$$\prod_{j=1}^{k} f_j = \sum_{i \in I} \prod_{j=1}^{k} f_{i_j,j} a_{i_j} = \sum_{i \in I} \left(\prod_{j=1}^{k} f_{i_j,j} \right) b_i \in \mathfrak{b}$$

Now recall that - by definition - \mathfrak{a}^k consists precisely of sums of elements of the form $f_1 \ldots f_k$ where $f_j \in \mathfrak{a}$. As we have seen any such element is contained in \mathfrak{b} and hence $\mathfrak{a}^k \subseteq \mathfrak{b}$.

- (viii) If a is contained in the radical of the intersection of the \mathfrak{a}_i then there is some $k \in \mathbb{N}$ such that a is contained in the intersection of the \mathfrak{a}_i . That is $a^k \in \mathfrak{a}_i$ for any $i \in I$ and hence $a \in \sqrt{\mathfrak{a}_i}$ for any $i \in I$.
- (viii) Let a be contained in the sum of the radicals $\sqrt{\mathfrak{a}_i}$. That is a is a finite sum of the form $a = a_1 + + \ldots a_n$ where a_j is contained in the radical of $\mathfrak{a}_{i(j)}$. Thereby for any $j \in 1 \ldots n$ we get

$$a_j \in \sqrt{\mathfrak{a}_{i(j)}} \implies \exists k(j) \in \mathbb{N} : a_j^{k(j)} \in \mathfrak{a}_{i(j)}$$

Now let $k := k(1) + \dots + k(n) \in \mathbb{N}$, then by the polynomial rule (1.21)

$$a^k = \sum_{|\alpha|=k} \prod_{j=1}^n a_j^{\alpha(j)}$$

Suppose that for any $j \in 1...n$ we had $\alpha(j) = k(j)$, then $|\alpha| = \alpha(1) + \cdots + \alpha(n) < k(1) + \cdots + k(n) = k$, a contradiction. Hence there is some $j \in 1...n$ such that $k(j) \leq \alpha(j)$. And for this j we have $a_j^{\alpha(j)} \in \mathfrak{a}_{i(j)}$. Thus a^k is contained in the radical of $\mathfrak{a}_{i(1)} + \cdots + \mathfrak{a}_{i(n)}$ and in particular in the radical of the sum of all \mathfrak{a}_i .

Proof of (2.23):

Fix any commutative ring $(E, +, \cdot)$ and consider the polynomial ring $S := E[t_i \mid 1 \leq i \in \mathbb{N}]$ in countable infinitely many variables over E. Then we take to the quotient where for any $1 \leq i \in \mathbb{N}$ we have $t_i^i = 0$. Formally

$$R \ := \ S'_{\mathfrak{Y}} \ \ ext{where} \ \ \mathfrak{v} \ := \ \langle t^i_i \ | \ 1 \leq i \in \mathbb{N} \
angle_i$$

For any $f \in S$ let us denote its residue class in R by $\overline{f} := f + \mathfrak{V}$. And further let us define the *size* of f to be the maximum index i such that t_i appears among the variable symbols of f. Formally that is

size
$$(f) := \max\{1 \le i \in \mathbb{N} \mid \exists \alpha : f[\alpha] \ne 0, \ \alpha_i \ne 0\}$$

Note that this truly is finite, as there only are finitely many α such that $f[\alpha] \neq 0$ and for any $\alpha = (\alpha_i)$ there also are finitely many *i* only, such that $\alpha_i \neq 0$. As our exemplary ideal let us take the zero-ideal $\mathfrak{a} := 0$. By construction we have $(\bar{t}_i)^i = 0$ and hence $\bar{t}_i \in \sqrt{0}$. On the other hand we have (for any $n \in \mathbb{N}$ with n < i)

$$(\overline{t}_i)^n \in (\sqrt{0})^n$$
 but $(\overline{t}_i)^n \neq 0$

Thus for any $n \in \mathbb{N}$ let us just take some $i \in \mathbb{N}$ with n < i. Then \overline{t}_i demonstrates that $(\sqrt{0})^n$ is not contained in 0. Also $\sqrt{0}$ is not finitely generated. Because if we consider a finite collection of elements $\overline{f}_1, \ldots, \overline{f}_k \in \sqrt{0}$ then just take $i > \max\{\operatorname{size}(f_j) \mid j \in 1 \ldots k\}$. Then it is clear that $f_j \in E[t_1, \ldots, t_{i-1}]$ and hence $t_i \notin \langle f_1, \ldots, f_k \rangle_i$. And thereby

$$\overline{t}_i \notin \langle f_1, \dots, f_k \rangle_i /_{\mathfrak{y}} = \langle \overline{f}_1, \dots, \overline{f}_k \rangle_i$$

Proof of (2.26):

(i) Consider any $a \in R$, then $a \in \sqrt{\mathfrak{b}} \cap R$ is equivalent, to $\varphi(a) \in \sqrt{\mathfrak{b}}$. That is iff there is some $k \in \mathbb{N}$ such that $\varphi(a^k) = \varphi(a)^k \in \mathfrak{b}$. This again is $a^k \in \mathfrak{b} \cap R$, which is equivalent to $a \in \sqrt{\mathfrak{b} \cap R}$. (ii) As $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$ we clearly have $\mathfrak{a}S \subseteq \sqrt{\mathfrak{a}S}$ which gives rise to the incusion " \subseteq ". Conversely consider any $f \in S$ such that $f^k \in \sqrt{\mathfrak{a}}S$ for some $k \in \mathbb{N}$. That is there are $g_i \in S$ and $a_i \in \sqrt{\mathfrak{a}}$ such that

$$f^k = g_1 \varphi(a_1) + \dots + g_n \varphi(a_n)$$

As a_i is contained in $\sqrt{\mathfrak{a}}$ there is some $k(i) \in \mathbb{N}$ such that $a_i^{k(i)} \in \mathfrak{a}$. Now let us abbreviate $b_i := \varphi(a_i), l := k(1) + \cdots + k(n)$ and $m := k \cdot l$. Then we get

$$f^m = (g_1b_1 + \dots g_nb_n)^l = \sum_{|\alpha|=l} {l \choose \alpha} (g_1b_1)^{\alpha(1)} \dots (g_nb_n)^{\alpha(n)}$$

Now fix any α and suppose for any $i \in 1...n$ we had $\alpha(i) < k(i)$, then we had $l = |\alpha| = \alpha(1) + \cdots + \alpha(n) < k(1) + \cdots + k(n) = l$ an obvious contradiction. Hence for any α there is some $j \in 1...n$ such that $\alpha(j) \ge k(j)$. And for this j we get

$$b_j^{\alpha(j)} = b_j^{\alpha(j)-k(j)} b_j^{k(j)} = b_j^{\alpha(j)-k(j)} \varphi\left(a_j^{k(j)}\right) \in \mathfrak{a} S$$

But as this holds true for any α with $|\alpha| = l$ we find that $f^m \in \mathfrak{a} S$. And this again means that f is contained in the radical of $\mathfrak{a} S$.

(iii) The equivalence \mathfrak{b} is a \star iff $\varphi^{-1}(\mathfrak{b})$ is a \star has already been proved in the correspondence theorem (1.43). Thus from now on φ is surjective, then $\varphi(\mathfrak{a})$ is a ideal of S due to (1.51). Now compute

$$\varphi^{-1}\varphi(\mathfrak{a}) = \{ b \in R \mid \varphi(b) \in \varphi(\mathfrak{a}) \}$$

= $\{ b \in R \mid \exists a \in \mathfrak{a} : \varphi(b) = \varphi(a) \}$
= $\{ b \in R \mid \exists a \in \mathfrak{a} : b - a \in \operatorname{kn}(\varphi) \}$
= $\{ b \in R \mid \exists a \in \mathfrak{a} : b \in a + \operatorname{kn}(\varphi) \}$
= $\{ a + \operatorname{kn}(\varphi) \mid a \in \mathfrak{a} \}$
= $\mathfrak{a} + \operatorname{kn}(\varphi)$

Now by the first claim $\mathfrak{b} := \varphi(\mathfrak{a})$ is a \star iff $\varphi^{-1}(\mathfrak{b}) = \varphi^{-1}\varphi(\mathfrak{a}) = \mathfrak{a} + \operatorname{kn}(\varphi)$ is a \star . And this already is the second claim.

16		٦
1		
. 8		_

Chapter 17

Proofs - Commutative Algebra

Proof of (2.27):

• (a) \implies (b): suppose there was some nonempty set of ideals $\mathcal{A} \neq \emptyset$ having *no* maximal element. For this set we start by choosing any $\mathfrak{a}_0 \in \mathcal{A}$. Now suppose we have already chosen the ideals $\mathfrak{a}_0, \ldots, \mathfrak{a}_k$ such that $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_k$. As \mathcal{A} does not contain maximal elements, there is some $\mathfrak{a}_{k+1} \in \mathcal{A}$ such that $\mathfrak{a}_k \subset \mathfrak{a}_{k+1}$. That is we have been able to append the chain of ideals, to

 $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots \subset \mathfrak{a}_k \subset \mathfrak{a}_{k+1}$

Then we may iterate the construction and thereby find an infinitely ascending chain of ideals of R (even in \mathcal{A}). But this contradicts the assumption (ACC). Hence \mathcal{A} could not have been chosen in the first place, that is *any* set of ideals $\mathcal{A} \neq \emptyset$ contains a maximal element.

• (b) \implies (c): Consider any ideal $\mathfrak{b} \leq_{\mathbf{i}} R$. Then we denote the set of all ideals generated by a finite subset $B \subseteq \mathfrak{b}$ by \mathcal{A} , that is

 $\mathcal{A} := \left\{ \langle B \rangle_{\mathbf{i}} \mid B \subseteq \mathfrak{h}, \ \#B < \infty \right\}$

As $0 \in \mathfrak{b}$ we have $\{0\} \in \mathcal{A}$, in particular $\mathcal{A} \neq \emptyset$ is non-empty. Hence by assumption (b) - there is a maximal element $\mathfrak{a}^* \in \mathcal{A}^*$ of \mathcal{A} . And as $\mathfrak{a}^* \in \mathcal{A}$ there is some finite set $B = \{a_1, \ldots, a_k\} \subseteq \mathfrak{b}$ generating \mathfrak{a}^* . In particular $\mathfrak{a}^* \subseteq \mathfrak{b}$. Now suppose $\mathfrak{b} \neq \mathfrak{a}^*$, that is there is some $b \in \mathfrak{b}$ such that $b \notin \mathfrak{a}^*$. Then we would also have

$$\mathfrak{a}^* \subset \langle a_1, \ldots, a_k, b \rangle_{\mathbf{i}} \in \mathcal{A}$$

in contradiction to the maximality of \mathfrak{a}^* . Thus \mathfrak{a}^* equals \mathfrak{b} and in particular we conclude that $\mathfrak{b} = \mathfrak{a}^* = \langle a_1, \ldots, a_k \rangle_i$ is finitely generated.

• (c) \implies (a): consider an ascending chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \ldots$ of ideals in R. Then we define the set

$$\mathfrak{b} := igcup_{k\in\mathbb{N}} \mathfrak{a}_k$$

As the \mathfrak{a}_k have been a chain, we find that $\mathfrak{b} \leq_i R$ is an ideal due to (2.4.(i)). And hence by assumption (c) there are finitely many elements $a_1, \ldots, a_n \in R$ generating $\mathfrak{b} = \langle a_1, \ldots, a_n \rangle_i$. So by construction of \mathfrak{b} for any $i \in 1 \ldots n$ (as $a_i \in \mathfrak{b}$) there is some $s(i) \in \mathbb{N}$ such that $a_i \in \mathfrak{a}_{s(i)}$. Now let $s := \max\{s(1), \ldots, s(n)\}$. Then for any $i \in 1 \ldots n$ and any $t \geq s$ we get $a_i \in \mathfrak{a}_{s(i)} \subseteq \mathfrak{a}_s \subseteq \mathfrak{a}_t$. In particular

$$\mathfrak{b} = \langle a_1, \ldots, a_n \rangle_{\mathfrak{i}} \subseteq \mathfrak{a}_t \subseteq \mathfrak{b}$$

Of course this means $\mathfrak{b} = \mathfrak{a}_t$ for any $t \ge s$. And this is just another way of saying that the chain of the \mathfrak{a}_k stabilized at level s.

By now we have proved the equivalence of (a), (b) and (c) in the definition of noetherian rings. And trivially we also have (c) \implies (d). These are the important equivalencies, it merely is a neat fact that (d) also implies (c). Though we will not use it we wish to present a proof (note that this is substantially more complicated than the important implications above).

• We will now prove (d) \implies (c) in several steps: we want to prove that *any* ideal of R is finitely generated. Thus let us take the set of all those ideals of R not being finitely generated:

 $\mathcal{Z} := \{ \mathfrak{a} \leq_{i} R \mid \mathfrak{a} \text{ is } not \text{ finitely generated} \}$

The idea of the proof will then be the following: suppose $\mathcal{Z} \neq \emptyset$, then by an application of Zorn's lemma, there is some maxmal element $\mathfrak{p} \in \mathcal{Z}^*$. In a second step we will then prove that any $\mathfrak{p} \in \mathcal{Z}^*$ is prime. So by assumption (d) \mathfrak{p} is finitely generated. But because of $\mathfrak{p} \in \mathcal{Z}$ it also is not finitely generated. This can only mean $\mathcal{Z} = \emptyset$ and hence any ideal of R is finitely generated. Thus it remains to prove:

• $\mathcal{Z} \neq \emptyset \implies \mathcal{Z}^* \neq \emptyset$: thus consider a chain (\mathfrak{a}_i) (where $i \in I$) in \mathcal{Z} . Then we denote the union of this chain by

$$\mathfrak{b} = \bigcup_{i \in I} \mathfrak{a}_i$$

By (2.4.(i)) $\mathfrak{b} \leq_{\mathbf{i}} R$ is an ideal of R again. Now suppose $\mathfrak{b} \notin \mathbb{Z}$, then \mathfrak{b} would be finitely generated, say $\mathfrak{b} = \langle b, \ldots, b_n \rangle_{\mathbf{i}}$. By construction of \mathfrak{b} for any $k \in 1 \ldots n$ (as $b_k \in \mathfrak{b}$) there is some $i(k) \in I$ such that $b_k \in \mathfrak{a}_{i(k)}$. And as the \mathfrak{a}_i form a chain we may choose $i \in I$ such that $\mathfrak{a}_i := \max\{\mathfrak{a}_{i(1)}, \ldots, \mathfrak{a}_{i(n)}\}$. Thereby $\mathfrak{b} = \langle b_1, \ldots, b_n \rangle_i \subseteq \mathfrak{a}_i \subseteq \mathfrak{b}$. That is $\mathfrak{a}_i = \langle b_1, \ldots, b_n \rangle_i$ would be finitely generated in contradiction to $\mathfrak{a}_i \in \mathcal{Z}$. Thus we have $\mathfrak{b} \in \mathcal{Z}$ again and hence \mathfrak{b} is an upper bound of (\mathfrak{a}_i) . Now - as any chain has an upper bound, by the lemma of Zorn - there is some maximal element $\mathfrak{p} \in \mathcal{Z}^*$.

p∈ Z* ⇒ p prime: First note that p ≠ R, as R = 1R is finitely generated. Now suppose p was not prime, then there would be some f, g∈ R such that f ∉ p, g ∉ p but fg ∈ p. Now let a := p+fR, as f ∉ p we find p ⊂ a. And as p is a maximal element of Z this means that a is finitely generated, say a = ⟨a₁,..., a_k⟩_i. As the a_i ∈ a = p + fR there are some p_i ∈ p and b_i ∈ R such that a_i = p_i + fb_i. Therefore

$$\mathfrak{a} = \langle p_1, \dots, p_k, f \rangle_{\mathbf{i}} = p_1 R + \dots + p_k R + f R$$

The inclusion " \supseteq " is clear, as $p_i \in \mathfrak{P} \subseteq \mathfrak{a}$ and $f \in \mathfrak{a}$. Conversely consider $x \in \mathfrak{a}$, that is there are some $x_i \in R$ such that $x = \sum_i x_i a_i = \sum_i x_i p_i + f \sum_i x_i b_i \in p_1 R + \cdots + p_k R + f R$. Next we note that

$$\mathfrak{p} = f(\mathfrak{p}:f) + p_1 R + \dots + p_k R$$

where $f(\mathfrak{p}:f) = (fR)(\mathfrak{p}:f) = \{fb \mid b \in \mathfrak{p}: f\} \leq_{i} R$. The inclusion " \supseteq " is easy: $p_i \in \mathfrak{p}$ is true by definition. Thus consider any element $x \in f(\mathfrak{p}:f)$. That is x = fb for some $b \in \mathfrak{p}: f = \{b \in R \mid fb \in \mathfrak{p}\}$. In particular $x = bf \in \mathfrak{p}$, too. For the converse inclusion we are given any $q \in \mathfrak{p} \subseteq \mathfrak{a}$. That is there are some $x_i \in R$ and $y \in R$ such that $q = x_1p_1 + \cdots + x_kp_k + yf$. As q and all the p_i are contained in \mathfrak{p} this implies $yf \in \mathfrak{p}$ and thereby $y \in \mathfrak{p}: f$. Thus $yf \in f(\mathfrak{p}:f)$ and hence $q \in p_1R + \cdots + p_kR + f(\mathfrak{p}:f)$. Finally we prove

$$\mathfrak{p}: a \notin \mathcal{Z}$$

Clearly we get $\mathfrak{p} \subseteq \mathfrak{p} : a$ and $b \in \mathfrak{p} : a$ (because of $ab \in \mathfrak{p}$). But $b \notin \mathfrak{p}$ and hence $\mathfrak{p} \subset \mathfrak{p} : a$. But by the maximality of \mathfrak{p} in \mathcal{Z} this means $\mathfrak{p} : a \notin \mathcal{Z}$. Thus $\mathfrak{p} : a$ is finitely generated and hence $a(\mathfrak{p} : a)$ is finitely generated, too. But as the sum of finitely generated ideals is finitely generated by (1.37) this means that $\mathfrak{p} = a(\mathfrak{p} : a) + p_1R + \cdots + p_k$ is finitely generated, too, in contradiction to $\mathfrak{p} \in \mathcal{Z}$. Thus the assumption of \mathfrak{p} not being prime is false.

Proof of (2.30):

(i) We will only prove the noetherian case - the arinian case is an analogous argument involving descending (instead of ascending) chains of ideals. Thus consider an ascending chain of ideals in R/a

 $\mathfrak{u}_0 \subseteq \mathfrak{u}_1 \subseteq \ldots \subseteq \mathfrak{u}_k \subseteq \ldots \trianglelefteq_i \mathbb{R}/\mathfrak{a}$

By the correspondence theorem (1.43) the ideals \mathfrak{u}_k are of the form $\mathfrak{u}_k = \mathfrak{b}_k/\mathfrak{a}$ for sufficient ideals $\mathfrak{b}_k := \varrho^{-1}(\mathfrak{u}_k) \leq_{\mathrm{i}} R$. Now suppose $b \in \mathfrak{b}_k$ then $b + \mathfrak{a} \in \mathfrak{u}_k \subseteq \mathfrak{u}_{k+1} = \mathfrak{b}_{k+1}/\mathfrak{a}$ and hence $b \in \mathfrak{b}_{k+1}$ again. Thus we have found an ascending chain of ideals in R

 $\mathfrak{b}_0 \subseteq \mathfrak{b}_1 \subseteq \ldots \subseteq \mathfrak{b}_k \subseteq \ldots \trianglelefteq_i R$

As R is noetherian this chain has to be eventually constant, that is there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{b}_{s+i} = \mathfrak{b}_s$. But this clearly implies $\mathfrak{u}_{s+i} = \mathfrak{u}_s$ as well and hence R/\mathfrak{a} is noetherian again.

- (ii) If $\varphi : R \twoheadrightarrow S$ is a surjective homomorphism, then by the first isomorphism theorem (1.56) we get $R/\operatorname{kn}(\varphi) \cong_{\mathrm{r}} S$. But by assumption R is \star and hence $R/\operatorname{kn}(\varphi)$ is \star , too, due to (i). And because of this isomorphy we find that S thereby is \star , as well (this is clear by transfering a chain of ideals from S to $R/\operatorname{kn}(\varphi)$ and returning to S).
- (iii) First suppose that $R \oplus S$ is \star . Trivially we have the following surjective ring homomorphisms $R \oplus S \twoheadrightarrow R$: $(a, b) \mapsto a$ and $R \oplus S \twoheadrightarrow R$: $(a, b) \mapsto b$. Thus both R and S are \star due to (ii). Conversely suppose both R and S are noetherian. We will prove that this implies $R \oplus S$ to be noetherian again (the proof in the artinian case is completely analogous). Thus consider an ascending chain of ideals of $R \oplus S$

$$\mathfrak{u}_0 \subseteq \mathfrak{u}_1 \subseteq \ldots \subseteq \mathfrak{u}_k \subseteq \ldots \subseteq \mathfrak{u}_i \ R \oplus S$$

Clearly $R \oplus 0$ and $0 \oplus S \leq_{i} R \oplus S$ are ideals of $R \oplus S$, too. Thus we obtain ideals $\mathfrak{a}_k := \mathfrak{u}_k \cap (R \oplus 0)$ and $\mathfrak{b}_k := \mathfrak{u}_k \cap (0 \oplus S) \leq_{i} R \oplus S$ be intersection. And for these we get

$$\mathfrak{u}_k = \mathfrak{a}_k + \mathfrak{b}_k$$

The inclusion " \supseteq " is clear, as $\mathfrak{a}_k, \mathfrak{b}_k \subseteq \mathfrak{u}_k$. For the converse inclusion " \subseteq " we are given some $(a,b) \in \mathfrak{u}_k$. As \mathfrak{u}_k is an ideal we find (a,0) = (1,0)(a,b) and $(0,b) = (0,1)(a,b) \in \mathfrak{u}_k$. And as also $(a,0) \in R \oplus 0$ and $(0,b) \in 0 \oplus S$ this yields $(a,b) = (a,0) + (0,b) \in \mathfrak{a}_k + \mathfrak{b}_k$. But as \mathfrak{a}_k is an ideal of $R \oplus S$ contained in $R \oplus 0$ it in particular is an ideal of $\mathfrak{a}_k \leq_i R \oplus 0$. But clearly R and $R \oplus 0$ are isomorphic under $R \cong_{\mathrm{r}} R \oplus 0 : a \mapsto (a,0)$. Thus \mathfrak{a}_k corresponds to the following ideal $\mathfrak{a}_k^\circ := \{a \in R \mid (a,0) \in \mathfrak{a}_k\} \leq_i R$. And thus we have found an ascending chain of ideals in R

$$\mathfrak{a}_0^\circ \subseteq \mathfrak{a}_1^\circ \subseteq \ldots \subseteq \mathfrak{a}_k^\circ \subseteq \ldots \trianglelefteq_i R$$

Yet as R was assumed to be noetherian there is some $p \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{a}_{p+i}^{\circ} = \mathfrak{a}_p^{\circ}$. And returning to $R \oplus 0$ (via

 $\mathbf{a}_k = \{ (a, 0) \mid a \in \mathbf{a}_k^{\circ} \} \}$ we find that $\mathbf{a}_{p+i} = \mathbf{a}_p$ as well. With the same argument for the \mathbf{b}_k we find some $q \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathbf{b}_{q+i} = \mathbf{b}_q$. Now let $s := \max\{p, q\}$ then it is clear that for any $i \in \mathbb{N}$ we get

$$\mathfrak{u}_{s+i} = \mathfrak{a}_{s+i} + \mathfrak{b}_{s+i} = \mathfrak{a}_s + \mathfrak{b}_s = \mathfrak{u}_s$$

that is the chain of the \mathfrak{U}_k has been eventually constant. And this means nothin but $R \oplus S$ being noetherian again.

Proof of (2.32):

This proof requires some working knowledge of polynomials as it is presented in sections 6.3 and 6.4. Yet as the techniques used in this proof are fairly easy to see we chose to place the proof here already. In case you encounter problems with the arguments herein refer to these sections first.

(1) In a first step let us consider the case where S = R[t] is the polynomial ring over R. Thus consider an ideal $\mathfrak{u} \leq_i S$, then we want to verify that \mathfrak{u} is finitely generated. The case $\mathfrak{u} = 0$ is clear, thus we assume $\mathfrak{u} \neq 0$. Then for any $k \in \mathbb{N}$ we denote

$$\mathfrak{a}_k := \{ \operatorname{lc}(f) \mid f \in \mathfrak{u}, \operatorname{deg}(f) = k \} \cup \{ 0 \}$$

where lc $(f) := f[\deg(f)]$ denotes the *leading coefficient* of f. We will first prove that $\mathfrak{a}_k \leq_i R$ is an ideal of $R: 0 \in \mathfrak{a}_k$ is clear by construction. Thus suppose $a, b \in \mathfrak{a}_k$ say $a = \operatorname{lc}(f)$ and $b = \operatorname{lc}(g)$. As both f and gare of degree k we get $(f+g)[k] = f[k] + g[k] = \operatorname{lc}(f) + \operatorname{lc}(g) = a + b$. Thus if a+b=0 then $a+b \in \mathfrak{a}_k$ is clear. And else, if $a+b\neq 0$ then f+gis of degree k, too and lc (f+g) = (f+g)[k] = a+b. And as $f+g \in \mathfrak{u}$ again we find $a+b \in \mathfrak{a}_k$ in both cases. Now let $r \in R$ be any element, if ra = 0 then $ra \in \mathfrak{a}_k$ is trivial again. And else $rf : k \mapsto rf[k]$ is of degree k again and satisfies lc $(rf) = (rf)[k] = r(f[k]) = r\operatorname{lc}(f) = ra$. And as also $rf \in \mathfrak{u}$ we again found $ra \in \mathfrak{a}_k$ in both cases. Altogether $\mathfrak{a}_k \leq_i R$ is an ideal. Next we will also prove the containment $\mathfrak{a}_k \subseteq \mathfrak{a}_{k+1}$. That is we consider some $a = \operatorname{lc}(f) \in \mathfrak{a}_k$ again. As $f \in \mathfrak{u}$ we also have $tf : k \mapsto f[k-1] \in \mathfrak{u}$. Obviously $\operatorname{deg}(tf) = \operatorname{deg}(f) + 1 = k + 1$ and lc (tf) = f[k+1] = f[k] = a. Thus we have found $a = \operatorname{lc}(tf) \in \mathfrak{a}_{k+1}$. Altogether we have found the following ascending chain of ideals of R

 $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \ldots \trianglelefteq_i R$

• As R is noetherian this chain has to be eventually constant, that is there is some $s \in \mathbb{N}$ such that for any $i \in \mathbb{N}$ we get $\mathfrak{a}_{s+i} = \mathfrak{a}_s$. And furthermore any \mathbf{a}_k is finitely generated (as R is noetherian). As we may choose generators of \mathbf{a}_k we do so

$$\mathfrak{a}_k = \langle a_{k,1}, \dots, a_{k,n(k)} \rangle_{\mathrm{i}}$$

and pick up polynomials $f_{k,i} \in \mathfrak{U}$ of degree $\deg(f_{k,i}) = k$ such that $\operatorname{lc}(f_{k,i}) = a_{k,i}$. Then we define the following ideal of S

$$\mathfrak{W} := \langle f_{k,1} \mid k \in 0 \dots s, \ i \in 1 \dots n(k) \rangle_{\mathbf{i}}$$

- For the first step it remains to prove that $\mathfrak{l} =$
 - scriptw. Then \mathfrak{u} is finitely generated, as we have given a list of generators explicitly. The inclusion $\mathfrak{W} \subseteq \mathfrak{u}$ is clear, as any $f_{i,k} \in \mathfrak{u}$. For the converse inclusion we start with some $f \in \mathfrak{u}$ and need to show $f \in \mathfrak{W}$. This will be done by induction on the degree $k := \deg(f)$ of f. The case f = 0 is clear. If $\deg(f) = k = 0$ then $f \in R$ is constant, that is $f = \operatorname{lc}(f) \in \mathfrak{a}_0 = \langle a_{0,1}, \ldots, a_{0,n(0)} \rangle_i \subseteq \mathfrak{W}$. Thus for the induction step we suppose $k \geq 1$ and let $a := \operatorname{lc}(f) = f[k]$. If $k \leq s$ then $a \in \mathfrak{a}_k = \langle a_{k,1}, \ldots, a_{k,n(k)} \rangle_i$. That is there are some $b_i \in R$ such that $a = \sum_i a_{k,i} b_i$. Now let us define the polynomial

$$g := \sum_{i=1}^{n(k)} b_i f_{k,i} \in \mathfrak{V}$$

Then it is clear that $lc(g) = \sum_i b_i lc(f_{i,k}) = a = lc(f)$ and hence deg(f-g) < k. Thus by the induction hypothesis we get $d := f-g \in \mathfrak{W}$ again and hence $f = d+g \in \mathfrak{W}$, too. It remains to check the case k > s. Yet this can be dealt with using a similar argument. As $k \ge s$ we have $a \in \mathfrak{a}_k = \mathfrak{a}_s$. That is $a = \sum_i a_{k,i} b_i$ for sufficient $b_i \in R$. This time

$$g := \sum_{i=1}^{n(s)} b_i t^{k-s} f_{k,i} \in \mathfrak{v}$$

Then $lc(g) = \sum_i b_i lc(f_{i,k}) = a = lc(f)$ again and as before this is deg(f - g) < k. By induction hypothesis again $d := f - g \in \mathfrak{W}$ and hence $f = d + g \in \mathfrak{W}$. Thus we have finished the case S = R[t].

(2) As a second case let us regard $S = R[t_1, \ldots, n]$ the polynomial ring in finitely many variables. Again we want to prove that S in noetherian, and this time we use induction on the number n of variables. The case n = 1 has just been treated in (1). Thus consider $R[t_1, \ldots, t_n, t_{n+1}]$. Then we use the isomorphy

$$R[t_1, \ldots, t_n, t_{n+1}] \cong_{\mathbf{r}} R[t_1, \ldots, t_n][t_{n+1}]$$

$$\sum_{\alpha} f[\alpha] t^{\alpha} \mapsto \sum_{i=0}^{\infty} \left(\sum_{\alpha_{n+1}=i} f[\alpha] t_1^{\alpha_1} \dots t_n^{\alpha_n} \right) t_{n+1}^i$$

By induction hypothesis $R[t_1, \ldots, t_n]$ is noetherian already. And by (1) this implies $R[t_1, \ldots, t_n][t_{n+1}]$ to be noetherian, too. And using the above isomorphy we finally find that $R[t_1, \ldots, t_n, t_{n+1}]$ is noetherian.

(3) We now easily derive the the general claim: let S be finitely generated over R. That is there are finitely many $e_1, \ldots, e_n \in S$ such that $S = R[e_1, \ldots, e_n]$. Then we trivially have a surjective homomorphism $R[t_1, \ldots, t_n] \twoheadrightarrow S : f \mapsto f(e_1, \ldots, e_n)$ form the polynomial ring onto S. And by (2.30.(iii)) this implies that S is noetherian, too.

Proof of (2.37):

Let us denote the prime ring of R by $P := \langle \emptyset \rangle_{\mathbf{r}}$. This is the image of the uniquely determined ring-homomorphism from \mathbb{Z} to R (induced by $1 \mapsto 1$). That is $P = \operatorname{im}(\mathbb{Z} \to R)$ and in particular P is noetherian by (2.30.(ii)). Let us now denote the set of finite, non-empty subsets of R by I

 $I := \{ i \subseteq R \mid i \neq \emptyset, \ \#i < \infty \}$

And for any $i \in I$ let us denote $R_i := P[i]$ the *P*-subalgebra of *R* generated by *i*. Then by the Hilbert's basis theorem R_i is noetherian as well. Given any $a \in R$ we clearly have $i := \{a\} \in I$ and $a \in R_i$. In particular the R_i cover *R*. And given any two $i, j \in I$ we have $k := i \cup j \in I$, too. We now claim that $R_i \cup R_j \subseteq R_i$: thus suppose $i = \{i_1, \ldots, i_n\}$ and let $a = f(i_1, \ldots, i_n)$ for some polynomial $f \in P[t_1, \ldots, t_n]$. Then it is clear that $a = g(i_1, \ldots, i_n, j_1, \ldots, j_m) \in P[i \cup j] = R_k$ if we only let $g(t_1, \ldots, t_n, t_{n+1}, \ldots, t_{n+m}) := f(t_1, \ldots, t_n) \in P[t_1, \ldots, t_{n+m}]$. Thus we have seen $R_i \subseteq R_k$ and $R_j \subseteq R_k$ can be proved in complete analogy.

Proof of (2.35):

- (ii) Just let $\mathcal{P} := \{ \mathfrak{b} \in \operatorname{spec} R \mid \mathfrak{p} \subseteq \mathfrak{b} \subset \mathfrak{q} \}$. Then $\mathcal{P} \neq \emptyset$ is non-empty, as $\mathfrak{p} \in \mathcal{P}$. But as we have seen in the definition of noetherian rings this already implies that there is some $\mathfrak{q}_{\circ} \in \mathcal{P}^*$.
- (iii) For any ideal $R \neq \mathfrak{a} \leq_{i} R$ let us denote $\mathbb{V}(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\}$ and $n(\mathfrak{a}) := \#\mathbb{V}(\mathfrak{a})_* \in \mathbb{N} \cup \{\infty\}$. That is $n(\mathfrak{a})$ is the number of minimal prime ideals lying over \mathfrak{a} . By (2.14.(iii)) we know $1 \leq n(\mathfrak{a})$. Now let

$$\mathcal{A} := \{ \mathfrak{a} \leq_{\mathrm{i}} R \mid n(\mathfrak{a}) = \infty \}$$

be the set of all ideals having infinitely many minimal primes lying over it. We want to show that $\mathcal{A} = \emptyset$. Hence assume $\mathcal{A} \neq \emptyset$, then - as R is noetherian - we may choose some maximal ideal $\mathfrak{u} \in \mathcal{A}^*$ in \mathcal{A} . Clearly \mathfrak{u} cannot be prime (if it was then \mathfrak{u} would be the one and only minimal prime ideal lying over \mathfrak{u} . That is $\mathbb{V}(\mathfrak{u})_* = {\mathfrak{u}}$ and hence $n(\mathfrak{u}) = 1 < \infty$). Thus there are some $a, b \in R$ such that $ab \in \mathfrak{u}$ but a, $b \notin \mathfrak{u}$. Then we define the respective ideals

$$\mathfrak{a} := \mathfrak{u} + aR$$
 and $\mathfrak{b} := \mathfrak{u} + bR$

As $a \notin \mathfrak{u}$ we have $\mathfrak{u} \subset \mathfrak{a}$ and hence $\mathfrak{a} \notin \mathcal{A}$ due to the maximality of \mathfrak{u} . Likewise $\mathfrak{b} \notin \mathcal{A}$ and this means that $n(\mathfrak{a}), n(\mathfrak{b}) < \infty$ are finite. But we will now prove

$$\mathbb{V}(\mathfrak{u})_* \subseteq \mathbb{V}(\mathfrak{a})_* \cup \mathbb{V}(\mathfrak{b})_*$$

To see this let $\mathfrak{p} \in \mathbb{V}(\mathfrak{l})_*$ be a minimal prime ideal over \mathfrak{l} . If $a \in \mathfrak{p}$ then $\mathfrak{a} \subseteq \mathfrak{p}$. Else suppose $a \notin \mathfrak{p}$ then $ab \in \mathfrak{l} \subseteq \mathfrak{p}$ implies $b \in \mathfrak{p}$, as \mathfrak{p} is prime. And thereby we get $\mathfrak{b} \subseteq \mathfrak{p}$. In any case \mathfrak{p} lies over one of the ideals \mathfrak{a} or \mathfrak{b} , say $\mathfrak{a} \subseteq \mathfrak{p}$ (w.l.o.g.). If now $\mathfrak{q} \in \mathbb{V}(\mathfrak{a})$ then in particular we get $\mathfrak{q} \in \mathbb{V}(\mathfrak{l})$. Thus if $\mathfrak{q} \subseteq \mathfrak{p}$ then the minimality of \mathfrak{p} over \mathfrak{l} implies $\mathfrak{q} = \mathfrak{p}$. That is \mathfrak{p} is a minimal element of $\mathbb{V}(\mathfrak{a})$ and hence the inclusion. As both $\mathbb{V}(\mathfrak{a})_*$ and $\mathbb{V}(\mathfrak{b})_* < \infty$ are finite, $\mathbb{V}(\mathfrak{l})_* < \infty$ would have to be finite, too. But this contradicts $\mathfrak{l} \in \mathcal{A}$, so the assumption $\mathcal{A} \neq \emptyset$ has to be abandoned. That is any ideal \mathfrak{a} of R only has finitely many prime ideals lying over it.

(i) (■) Consider a set of prime ideals p ≠ Ø of the noetherian ring R. It has already been shown in (2.27) that P* ≠ Ø contains maximal elements. We will now prove that P_{*} ≠ Ø contains a minimal element, as well. Suppose this was untrue, then we start with any p = p₀ ∈ P. As p₀ is not minimal in P, there is some p₁ such that p₀ ⊃ p₁. Again p₁ is not minimal in P, such that we may choose some p₂ ∈ P such that p₁ ⊃ p₂. Continueing that way we find an infinite, strictly descending chain of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \ldots \supset \mathfrak{p}_k \supset \ldots$$

This means that \mathfrak{p} is a prime ideal of infinite height height $(\mathfrak{p}) = \infty$. But in a noetherian ring we have Krull's Principal Ideal Theorem (???). And this states that height $(\mathfrak{p}) \leq \operatorname{rank}(\mathfrak{p}) < \infty$.

Proof of (2.38):

We start with the equivalencies for $a \mid b$. Hereby (a) \implies (c) is clear: $b \in aR = \{ah \mid h \in R\}$ yields b = ah for some $h \in R$. (c) \implies (b): consider $f \in bR$, that is f = bg for some $g \in R$. But as b = ah this yields $f = ahg \in aR$. (b) \implies (a): as $b \in bR \subseteq aR$ we have $b \in aR$.

We also have to check the equivalencies for $a \approx b$ - recall that now R is an integral domain. (a) \implies (b): if aR = bR then in particular $aR \subseteq bR$ and hence $b \mid a$. Likewise we get $a \mid b$. (b) \implies (c): Suppose $b = \alpha a$ and $a = \beta b$. If b = 0 then $a = \beta b = \beta \cdot 0 = 0$, as well. And hence we may choose $\alpha := 1$. Thus we continue with $b \neq 0$. Then $b = \alpha a = \alpha \beta b$. And as R is an integral domain and $b \neq 0$ we may divide by b and thereby obtain $1 = \alpha \beta$. That is $\alpha \in R^*$ and $b = \alpha a$ as claimed. (c) \implies (a): As $b = \alpha a$ we get $bR \subseteq aR$. And from $a = \alpha^{-1}b$ we get $aR \subseteq bR$.

Proof of (2.39):

- (i) By definition of 1 we have $1 \cdot b = b$ and hence $1 \mid b$, likewise we have $a \cdot 0 = 0$ and hence $a \mid 0$ by (1.21). Now ah = ab for h := b and hence $a \mid ab$ is trivial again.
- (i) Next suppose b = 0, then b = 0 ⋅ 1 and hence 0 | b. Conversely suppose 0 | b, that is there is some h ∈ R such that 0 = 0 ⋅ h = b. Then we have just proved 0 = b, as well. If a ∈ R* then 1 = aa⁻¹ and hence a | 1. Conversely suppose a | 1, that is there is some h ∈ R such that ah = 1. As R is commutative this also is ha = 1 and hence a ∈ R*. Finally let a | b, that is ah = b for some h ∈ R again. In particular this yields (ac)h = (ah)c = bc and hence ac | bc.
- (ii) Now suppose $u \in R$ is a non-zero divisor, by (i) we only have to show the implication " \Leftarrow ". Thus let (au)h = bu for some $h \in R$, then (ah - b)u = (au)h - bu = 0. But as u is a non-zero divisor this can only happen if ah - b = 0 and this already is $a \mid b$.
- (iii) First of all $a \mid a$ is clear by $a \cdot 1 = a$. If now $a \mid b$ and $b \mid c$ (say ag = b and bh = c) then we get $a \mid c$ from a(gh) = (ag)h = bh = c. And that $a \mid b$ and $b \mid a$ implies $a \approx b$ is true by definition (2.38).
- (iv) As we have seen in (2.38) $a \approx b$ is equivalent, to aR = bR. And from this it is clear that \approx is reflexive, symmetric and transitive (i.e. an equivalence relation). Thus it only remains to observe that

$$[a] = \{ b \in R \mid a \approx b \} = \{ \alpha a \mid \alpha \in R^* \} = aR^*$$

Proof of (2.47):

- (i) The statement is clear by induction on the number k of elements involved: if k = 1 then $p \mid a_1$ is just the assumption. Thus consider k + 1 elements and let $a := a_1 \dots a_k$ and $b := a_{k+1}$. Then by assumption we have $p \mid ab$ and (as p is prime) hence $p \mid a$ or $p \mid b$. If $p \mid b$ then we are done (with i = k + 1). And if $p \mid a$ then by induction hypothesis we find some $i \in 1 \dots k$ such that $p \mid a_i$. Altogether $p \mid a_i$ for some $i \in 1 \dots k + 1$.
- (ii) If $p \in R$ is prime then $p \neq 0$ by definition. And as also $p \notin R^*$ we have $pR \neq R$, as well. Now $ab \in pR$ translates into $p \mid ab$ and hence $p \mid a$ or $p \mid b$. But this again is $a \in pR$ or $b \in pR$. That is we have proved that pR is prime. Conversely suppose $p \neq 0$ and that pR is a prime ideal. As $pR \neq R$ we have $p \notin R^*$. And as we also assumed $p \neq 0$ this means $p \in R^{\bullet}$. If we are now given $a, b \in R$ with $p \mid ab$, then $ab \in pR$ and hence $a \in pR$ or $b \in pR$, as pR is prime. Thus we find $p \mid a$ or $p \mid b$ again, and altogether p is prime.
- (iii) "p irreducible $\implies \alpha p$ irreducible": suppose $\alpha p = ab$ for some a, $b \in R$. As α is a unit this yields $p = (\alpha^{-1}a)b$ and as p is irreducible hence $\alpha^{-1}a \in R^*$ or $b \in R^*$. But $\alpha^{-1}a \in R^*$ already implies $a \in R^*$ (with inverse $a^{-1} = \alpha^{-1}(\alpha^{-1}a)^{-1}$). Conversely if αp is irreducible then $p = \alpha^{-1}\alpha p$ is irreducible, too by what we have just proved.
- (iii) "p prime $\implies \alpha p$ prime": suppose $\alpha p \mid ab$ for some $a, b \in R$. As α is a unit this yields $p \mid (\alpha^{-1}a)b$ and as p is prime we hence get $p \mid \alpha^{-1}a$ or $p \mid b$. From $p \mid \alpha^{-1}a$ we get $\alpha p \mid a$ and $p \mid b$ implies $p \mid \alpha^{-1}p$ which also implies $\alpha p \mid b$. Thus we have proved, that αp is prime too. Conversely if αp is prime then $p = \alpha^{-1}\alpha p$ is prime, too by what we have just proved.
- (iv) Let f := ab, then it is clear that $a \mid f$ and hence $fR \subseteq aR$. And as both a and $b \neq 0$ are non-zero, so is f (as R is an integral domain). Now suppose we had $a \in fR$, that is a = fg for some $g \in R$. Then we compute a = fg = abg. And as $a \neq 0$ this means 1 = bg. In particular $b \in R^*$ is a unit, in contradiction to $b \in R^{\bullet}$. Hence $a \in aR \setminus fR$ and this yields the claim $fR \subset aR$.
- (v) Now let R be an integral domain, $p \in R$ be prime and suppose p = ab for some $a, b \in R$. In particular $p \mid ab$ and hence $p \mid a$ or $p \mid b$. W.l.o.g. let us assume $p \mid b$, that ph = b for some $h \in R$. Then p = ab = aph and hence p(1 - ah) = 0. Now as $p \neq 0$ this implies ah = 1, that is $a \in R^*$ is a unit or R. Thereby we have verified, that p truly is irreducible.
- (vi) Clearly we have $R^* \subseteq D$, as k = 0 is allowed. And if $c = \alpha p_1 \dots p_k$ and $d = \beta q_1 \dots q_l \in D$ it is clear that $cd = (\alpha \beta)(p_1 \dots p_k q_1 \dots q_l) \in D$

again. Thus it remains to show the implication $cd \in D \implies c \in D$ (due to the symmetry of the statement it also follows that $d \in D$). Thus consider any $c, d \in R$ such that $cd = \alpha p_1 \dots p_k \in D$. We will prove the claim by induction on k - that is we will verify

$$\forall c, d \in R : cd = \alpha p_1 \dots p_k \in D \implies c \in D$$

for any $k \in \mathbb{N}$. The case k = 0 is trivial, since $cd = \alpha \in R^*$ implies $c \in R^* \subseteq D$. Thus regard $k \ge 1$. We let $I := \{i \in 1 \dots k \mid p_i \mid d\}$. (1) If there is some $i \in I$ then $p_i \mid b$. W.l.o.g. we may assume i = k. That is there is some $h \in R$ such that $d = hp_k$. Then

$$\alpha p_1 \dots p_k = cd = chp_k$$

As R is an integral domain and $p_k \neq 0$ we may divide by p_k to find $ch = \alpha p_1 \dots p_{k-1} \in D$. By induction hypothesis that is $c \in D$ already. (2) If $I = \emptyset$ then for any $i \in 1 \dots k$ we've got $p_i \not| d$. But as p_k is prime and $p_k \mid cd$ this yields $p_k \mid c$, say $c = gp_k$. Then

$$\alpha p_1 \dots p_k = cd = gdp_k$$

We divide by p_k again to find $gd = \alpha p_1 \dots p_{k-1} \in D$. And by induction hypothesis this means $g \in D$. But $p_k \in D$ is clear, as well and therefore $c = gp_k \in D$ as claimed.

(vii) First consider the case $\alpha = 1 = \beta$. Without loss of generality we may assume $k \leq l$ and we will use induction k to prove the statement. If k = 0 we have to prove l = 0. Thus assume $l \geq 1$ then $1 = q_1 \dots q_l =$ $q_1(q_2 \dots q_l)$. That is $q_1 \in R^*$ is a unit. But q_1 has been prime and hence $q_1 \notin R^*$ a contradiction. Thus we necessarily have k = l = 0. Now consider the induction step $k \geq 1$, then $p_k \mid p_1 \dots p_k = q_1 \dots q_l$ and as p_k is prime this means $p_k \mid q_j$ for some $j \in 1 \dots l$. Without loss of generality we may assume j = l. Hence we found $q_l = \gamma p_k$ for some $\gamma \in R$. But q_l has been prime and hence is irreducible by (iv). This means $\gamma \in R^*$ (as $p_k \notin R^*$) and hence $p_k \approx q_k$. Further we have

$$(p_1 \dots p_{k-1})p_k = p_1 \dots p_k = q_1 \dots q_l = \gamma(q_1 \dots q_{l-1})p_k$$

As $p_k \neq 0$ and R is an integral domain we may divide by p_k and thereby get $p_1 \ldots p_{k-1} = (\gamma q_1)q_2 \ldots q_{l-1}$. (As γq_1 is prime again) the induction hypothesis now yields that k - 1 = l - 1 and there is some $\sigma \in S_{k-1}$ such that for any $i \in 1 \ldots k - 1$ we have $p_i \approx q_{\sigma(i)}$. But this also is k = l and we may extend σ to S_k by letting $\sigma(k) := k = l$. (As $q_1 \approx \gamma q_1$) we hence found $p_i \approx q_{\sigma(i)}$ for any $i \in 1 \ldots k$. Thus we have completed the case $\alpha = 1 = \beta$. If now α and $\beta \in R^*$ are arbitary, then we let $p'_1 := \alpha p_1, p'_i := p_i$ (for $i \in 2 \ldots k$) and $q'_1 := \beta q_1, q'_j := q_j$ (for $j \in 2...l$). By (iii) p'_i and q'_j are prime again and by construction it is clear that $p'_i \approx p_i$ and $q'_j \approx q_j$ for any $i \in 1...k$ and $j \in 1...l$. As $p'_1 \dots p'_k = q'_1 \dots q'_l$ we may invoke the first case to find k = l and the required permutation $\sigma \in S_k$. But now for any $i \in 1...k$ we get $p_i \approx p'_1 \approx q'_{\sigma(i)} \approx q_{\sigma(i)}$ and hence $p_i \approx q_{\sigma(i)}$ as claimed.

(viii) We only prove the equivalence for the least common multiple (the like statement for the greatest common divisor can be proved in complete analogy). Clearly $m \in mR^* = \operatorname{lcm}(A)$ implies $m \in \operatorname{lcm}(A)$. Thus let us assume $m \in \operatorname{lcm}(A)$, then we need to prove $\operatorname{lcm}(A) = mR^*$. For " \supseteq " we are given any $\alpha \in R^*$. As $A \mid m$ it is clear that $A \mid \alpha m$, as well. And if $A \mid n$ then $m \mid n$ (by assumption) and hence also $\alpha m \mid n$ (by $(\alpha m)(\alpha^{-1}h) = n$ for mh = n). Concersely for " \subseteq " consider $n \in \operatorname{lcm}(A)$. As $A \mid m$ and $n \in \operatorname{lcm}(A)$ we get $n \mid m$. Analogously $A \mid n$ and $m \in \operatorname{lcm}(A)$ impliy $m \mid n$. Together that is $m \approx n$ and hence $n = \alpha n$ for some $\alpha \in R^*$.

Proof of (2.48):

(i) Suppose $\langle a : b \rangle = \infty$ that is for any $k \in \mathbb{N}$ there is some $h_k \in R$ such that $a^k h_k = b$. First suppose there was some $k \in \mathbb{N}$ such that $h_k = 0$. Then $b = a^k \cdot 0 = 0$, too and then $a \mid 0$ also implies a = 0, a contradiction. Thus $h_k \neq 0$ for any $k \in \mathbb{N}$. Now for any $k \in \mathbb{N}$ we find $h_{k+1}a^{k+1} = b = h_ka^k$. And as $a \neq 0$ and R is an integral domain $h_{k+1}a^{k+1} = h_ka^k$ also yields $h_{k+1}a = h_k$. That is $h_{k+1} \mid h_k$ and hence we have found the ascending chain of ideals

 $h_0R \subseteq h_1R \subseteq \ldots \subseteq h_kR \subseteq h_{k+1}R \subseteq \ldots$

Now suppose we had $h_k R = h_{k+1}R$ at any one stage $k \in \mathbb{N}$. That is there is some $\alpha \in R$ such that $h_{k+1} = \alpha h_k$. Thereby we compute $h_k = ah_{k+1} = \alpha ah_k$. And as $h_k \neq 0$ this implies $\alpha a = 1$. That is $a \in R^*$ a contradiction to $a \in R^{\bullet}$. And this only leaves $\langle a : b \rangle < \infty$.

(ii) As p is prime we have $p \in R^{\bullet}$ and hence $\langle p : a \rangle < \infty$ due to (i) (likewise for b and ab). That is we let $k := \langle p : a \rangle$, $l := \langle p : b \rangle$ and $n := \langle p : ab \rangle \in \mathbb{N}$. Then by assumption there are some α , $\beta \in R$ such that $a = \alpha p^k$ and $b = \beta p^l$. In particular $ab = \alpha \beta p^{k+1}$ such that $p^{k+l} \mid ab$ and hence $k + l \leq n$, as n is maximal among the integers with $p^n \mid ab$. Now suppose n > k + l, say $p^n h = ab = \alpha \beta p^{k+l}$. As R is an integral domain we may divide by p^{k+l} and thereby obtain $p^{n-(k+l)}h = \alpha\beta$. And as $n - (k+l) \geq 1$ this yields $p \mid \alpha\beta$. Now recall that p has been prime, then we may assome (w.l.o.g.) that $p \mid \alpha$, say $pg = \alpha$. Then $a = \alpha p^k = gp^{k+1}$ and hence $p^{k+1} \mid a$. But this is a contradiction to k being maximal and hence the assumption n > k+l has to be dropped. Altogether we have found n = k + l.

(\heartsuit) In a first step let us prove, that for any $a \in R^{\bullet}$ there is an irreducible $p \in R$ such that $p \mid a$. To do this we recursively define a sequence of elements, starting with $a_0 := a$. Now suppose we had already constructed $a_0, \ldots, a_k \in R$ such that $a_0R \subset a_1R \subset \ldots \subset a_kR$. Of course $a_k = 0$ cannot be, as $0 \neq a = a_0 \in a_kR$. Then we iterate as follows: if a_k is not irreducible then there are $f, g \in R^{\bullet}$ such that $a_k = fg$. Then by (2.47.(iv)) we get $a_kR = (fg)R \subset fR$. Thus if we now let $a_{k+1} := f$ then we have appended our chain of ideals to

$$a_0R \subset a_1R \subset \ldots \subset a_kR \subset a_{k+1}R$$

As R is noetherian we cannot construct a strictly ascending chain of infinite length. That is our construction has to terminate at some finite level $s \in \mathbb{N}$. And this can only be if $p := a_s$ is irreducible. Thus we have $a = a_0 \in a_0 R \subseteq a_s R = pR$ and thereby $p \mid a$.

(iii) If $a \in R^*$ is a unit, then the claim is clear by choosing $\alpha := a$ and k := 0. Thus let us assume $a \in R^{\bullet}$. Then by (\heartsuit) above there is some irreducible element $p_1 \in R$ such that $p_1 \mid a$, say $p_1a_1 = a$. Thus suppose we have already constructed the elements $a_1, \ldots, a_k \in R$ and $p_1, \ldots, p_k \in R$ such that the p_i are irreducible, $a = a_k p_1 \ldots p_k$ and $aR \subset a_1R \subset \ldots \subset a_kR$. Suppose that $a_k \notin R^*$ is no unit, then we iterate as follows: Note that $a_k \neq 0$ as well (else a = 0) and hence $a_k \in R^{\bullet}$. Thus by (\heartsuit) there is some irreducible element $p_{k+1} \in R$ such that $p_{k+1} \mid a_k$, say $a_k = p_{k+1}a_{k+1}$. We note that by (2.47.(iv)) this implies $a_kR = (p_{k+1}a_{k+1})R \subset a_{k+1}R$. So we have found a_{k+1} and p_{k+1} irreducible such that $a_{k+1}p_1 \ldots p_{k+1} = a_kp_1 \ldots p_k = a$ and

$$aR \subset a_1R \subset \ldots \subset a_kR \subset a_{k+1}R$$

As R is noetherian we cannot construct a strictly ascending chain of infinite length. That is our construction has to terminate at some finite level $s \in \mathbb{N}$. And this can only be if $a_s \in R^*$ is a unit. Thus we let $\alpha := a_s$ and thereby get $a = \alpha p_1 \dots p_s$ as claimed.

(iv) As R is noetherian and $\mathfrak{p} \leq_i R$ is an ideal there are finitely many $a_i \in R$ such that $\mathfrak{p} = \langle a_1, \ldots, a_k \rangle_i$. Without loss of generality we may assume $a_i \neq 0$ (else we might just as well drop it). Then we use (iii) to find a decomposition of a_i into irreducible elements $p_{i,j} \in R$

$$a_i = \alpha_i \prod_{j=1}^{n(i)} p_{i,j}$$

As $a_i \in \mathfrak{p}$ and \mathfrak{p} is prime this means that for any $i \in 1 \dots k$ there is some $j(i) \in 1 \dots n(i)$ such that $p_{i,j} \in \mathfrak{p}$ (note that $\alpha_i \neq \mathfrak{p}$ as else $1 = \alpha_i^{-1} \alpha_i \in \mathfrak{p}$). Now let $p_i := p_{i,j(i)} \in \mathfrak{p}$. Then it is clear that

$$a_i \in p_i R \subseteq \langle p_1, \dots, p_k \rangle_i \subseteq \mathfrak{p} = \langle a_1, \dots, a_k \rangle_i$$

for any $i \in ..., k$. And thereby $\mathfrak{p} = \langle a_1, ..., a_k \rangle_i \subseteq \langle p_1, ..., p_k \rangle_i$ as well such that we truly find $\mathfrak{p} = \langle p_1, ..., p_k \rangle_i$ as claimed.

(vi) Let us prove the first statement $a \mid b$ by induction over k. If k = 0 then a = 1 and hence $a \mid b$ is clear. Let us now fix some some abbreviations: let $n(i) := \langle q_i : b \rangle \in \mathbb{N}$ due to (i). And by definition of $\langle q_i : b \rangle$ it is clear that $q_i^{n(i)} \mid b$, say $b = b_i q_i^{n(i)}$ for any $i \in 1...k$. Hence in case k = 1 we are done already, as $a = q_1^{n(1)} \mid b$. Thus we may assume $k \geq 2$. Then the induction hypothesis reads as

$$h := \prod_{i=1}^{k-1} q_i^{n(i)} \mid b$$

Assume that $q_k \mid h$, as q_k is prime (by construction of h) this would mean $q_k \mid q_i$ for some $i \in 1...k - 1$. That is $q_i = \alpha_i q_k$ for some $\alpha_i \in R$. But as R is an integral domain and q_i is prime it also is irreducible by (2.47.(v)). This yields $\alpha_i \in R^*$ and hence $q_i \approx q_k$. But by assumption this is i = k in contradiction to $i \in 1...k - 1$. Thus we have seen $q_k \not\mid h$, or in other words $\langle q_k : h \rangle = 0$. Now recall that $h \mid b$, that is there is some $g \in R$ such that b = gh. then we may easily compute (using (ii))

$$n(k) = \langle q_k : b \rangle = \langle q_k : gh \rangle = \langle q_k : g \rangle + \langle q_k : h \rangle = \langle q_k : g \rangle$$

That is $q_k^{n(k)} = q_k^{\langle q_k:g \rangle} \mid g$ such that $g = q_k^{n(k)} f$ for some $f \in R$. Multiplying this identity with h we finally find $a \mid b$ from

$$b = gh = q_k^{n(k)}fh = af$$

It remains to verify the second claim in (vi). That is consider any prime element $p \in R$ such that $p \mid b = af$. As p is prime this means $p \mid a \text{ or } p \mid f$. In the first case $p \mid a$ (by construction of a) we find some $i \in 1 \dots k$ such that $p \mid q_i$. That is $\alpha p = q_i$ for some $\alpha \in R$. Again we use that q_i is prime and hence irreducible to deduce that $\alpha \in R^*$ and hence $p \approx q_i$. In the second case $p \mid f$ we are done already, as f = b/a. Thus we have proved $p \mid (b/a)$ or $p \approx p_i$ for some $i \in 1 \dots k$. Now suppose both statements would be true, that is $p \mid f$ and (w.l.o.g.) $p \mid q_k$. That is f = pr and $q_k = \alpha p$ for some $r \in R$ and $\alpha \in R^*$. Then we compute

$$b = af = (hq_k^{n(k)})(\alpha^{-1}q_kr) = q_k^{n(k)+1}(\alpha^{-1}hr)$$

In particular $q_k^{n(k)+1} \mid b$. But this clearly is a contradiction to the maximality of $n(k) = \langle q_k : b \rangle$. Thus we have proved the truth of *either* $p \mid (b/a)$ or $p \approx q_i$ (and not *both*) as claimed.

(v) Suppose we had $a \in pR$ for infinitely many $p \in P$. In particular we may choose a countable subset $(p_i) \subseteq P$ such that $a \in p_i R$ for any $i \in \mathbb{N}$. By (vi) we get

$$a_k := \prod_{i=0}^k p_i^{\langle p_i:a \rangle} \mid a$$

From the construction it is clear that for $f_k := p_k^{\langle p_k:a \rangle}$ we get $a_{k-1}f_k = a_k$. And as $p_k \mid a$ we have $\langle p_k:a \rangle \geq 1$ such that $f_k \neq 1$. In fact $f_k \in \mathbb{R}^{\bullet}$ as $p_k \in \mathbb{R}^{\bullet}$ and \mathbb{R} is an integral domain. Next let us choose some $g_k \in \mathbb{R}$ such that $a = a_k g_k$. Then for any $k \in \mathbb{N}$ we get $a_k g_k = a = a_{k+1}g_{k+1} = a_k f_{k+1}g_{k+1}$. It is clear that $a_k \neq 0$, as else $a = 0 \cdot g_k = 0$. Thus we may divide a_k from $a_k g_k = a_k f_{k+1}g_{k+1}$ and thereby find $g_k = f_{k+1}g_{k+1}$. Now using (2.47.(iv)) with $g_{k+1} \neq 0$ and $f_{k+1} \in \mathbb{R}^{\bullet}$ we find $g_k \mathbb{R} \subset g_{k+1}\mathbb{R}$. As this is true for any $k \in \mathbb{N}$ we have found an infinitely ascending chain

$$g_0 R \subset g_1 R \subset g_2 R \subset \ldots$$

of ideals in R. But this is a contradiction to R being noetherian. Thus the assumption has to be false and that is: there are only finitely many $p \in P$ with $a \in pR$.

Proof of (2.49):

In a first step we will prove the equivalence of (a), (b) and (c). Using these as a definition we will prove some more porperties of UFDs first, before we continue with the proof of the equivalencies of (d), (e) and (f) on page (362).

(a) ⇒ (c): By (2.47.(v)) we already know that prime elements are irreducible (as R is an integral domain). From this (1) and the one part of (2) are trivial by assumption (a). We only have to prove the second part of (2): ∀q ∈ R : q irreducible ⇒ q prime. By assumption (a) q admits a prime decomposition q = αp₁...p_k. It is clear that k ≠ 0 as else q ∈ R*. Now suppose k ≥ 2 then we would write q as q = (αq₁)(q₂...q_k). And as q is irreducible this would mean αp_i ∈ R* or p₂...p_k ∈ R*. But as p₁ is prime, so is αp₁ - by (2.47.(iii)) - and as R is an integral domain R[•] is closed under multiplication such that p₂...p_k ∈ R[•]. Hence none of this can be and this only leaves k = 1. That is q = αp₁ and hence q is prime.

- (c) \implies (b): consider any $0 \neq a \in R$, property (1) in (b) and (c) are identical so we only need to verify (2) in (b). Thus let $(\alpha, p_1, \ldots, p_k)$ and $(\beta, q_1, \ldots, q_l)$ be two irreducible decompositions of a. By assumption (2) in (c) all the p_i and p_j are prime already. Therefore $\alpha p_1 \ldots p_k = a = \beta q_1 \ldots q_l$ implies k = l and $p_i = q_{\sigma(i)}$ (for some $\sigma \in S_k$ and any $i \in 1 \ldots k$) by (2.47.(vii)). And by definition this already is $(\alpha, p_1, \ldots, p_k) \approx (\beta, q_1, \ldots, q_l)$.
- (b) ⇒ (a): By assumption (b) any 0 ≠ a ∈ R has an irreducible decomposition. Thus it suffices to show that any irreducible element p ∈ R already is prime. Thus consider an irreducible p ∈ R and arbitrary a, b ∈ R. Then we need to show p | ab ⇒ p | a or p | b. To do this we write down irreducible decompositions of a and b

$$a = \alpha p_1 \dots p_k$$
 and $b = \beta p_{k+1} \dots p_{k+l}$

As $p \mid ab$ there is some $h \in R$ with ab = ph. Again we use an irreducible decomposition of $h = \gamma q_1 \dots q_m$. Finally let $q_{m+1} := p$

$$\gamma q_1 \dots q_m q_{m+1} = ph = ab = \alpha \beta p_1 \dots p_{k+l}$$

As all the p_i and q_j are irreducible assumption (2) now yields that n := m + 1 = k + l and that there is some $\sigma \in S_n$ such that for any $i \in 1 \dots n$ we get $q_i \approx p_{\sigma(i)}$. Now let $j := \sigma(m+1)$, that is $p = q_{m+1} \approx p_j$. If $j \in 1 \dots k$ then $p \approx p_j \mid a$ and hence $p \mid a$. Likewise if $j \in k + 1 \dots k + l$ then $p \approx p_j \mid b$ and hence $p \mid b$. Together this means that p is truly prime.

Proof of (2.53):

Until now we only have proved the equivalence of (a), (b) and (c) in the definition of an UFD. That is we understand by an UFD an integral domain satisfying (a) (equivalently (b) or (c)). And using this definition only we are able to prove the theorem given:

(i) Let $I := \{i \in 1 \dots k \mid p \approx p_i\}$ and n := #I. Then for any $i \in I$ there is some $\alpha_i \in R^*$ such that $p_i = \alpha_i p$. Then it is immediately clear that

$$a \ = \ \beta bp^n \quad \text{where} \quad \beta := \alpha \prod_{i \in I} \alpha_i \quad \text{and} \quad b := \prod_{j \not\in I} p_j$$

In particular $p^n \mid a$ and this means $n \leq \langle p : a \rangle$. Conversely suppose $p^m \mid a$ for some m > n, say $p^m h = a = \beta b p^n$. Then $p^{m-n} \beta^{-1} h = b$ and hence $p \mid b$ as $p \dim p^{m-n}$. By definition of b this would imply $p \mid p_j$ for some $j \notin I$. Say $p_j = \gamma p$ for some $\gamma \in R$. But as p_j

is irreducible (and $p \notin R^*$ this yields $\gamma \in R^*$ and hence $p \approx p_j$ in contradiction to $j \notin I$. Thus we have proved the maximality of n and hence $n = \langle p : a \rangle$.

(ii) Using (i) this boils down to an easy computation: pick up two prime decompositions $a = \alpha p_1 \dots p_k$ and $b = \beta q_1 \dots q_l$. For $j \in 1 \dots l$ we let $p_{k+j} := q_j$. Then it is clear that $ab = \alpha \beta p_1 \dots p_{k+l}$ and thereby

$$\begin{aligned} \langle p:ab \rangle &= \# \{ i \in 1 \dots (k+l) \mid p \approx p_i \} \\ &= \# \{ i \in 1 \dots k \mid p \approx p_i \} + \# \{ j \in 1 \dots l \mid p \approx q_j \} \\ &= \langle p:a \rangle + \langle p:b \rangle \end{aligned}$$

(iv) Existence: consider any $0 \neq a \in R$ and pick up a prime decomposition $a = \beta q_1 \dots q_k$ of a. As the q_i is prime there is a uniquely determined $p_i \in \mathbb{P}$ such that $q_i \approx p_i$, say $q_i = \alpha_i p_i$ for some $\alpha_i \in R^*$. Then

$$a = \alpha p_1 \dots p_k$$
 where $\alpha := \alpha_1 \dots \alpha_k$

For any $p \in \mathbb{P}$ now let $n(p) := \# \{ i \in 1 \dots k \mid p_i = p \} \in \mathbb{N}$. Then it is clear that only finitely many n(p) are non-zero, as they sum up to

$$\sum_{p\in\mathbb{P}}n(p) \ = \ k$$

That is $n \in \bigoplus_p \mathbb{N}$ And further it is clear that a has the representation

$$a = \alpha \prod_{i=1}^{k} p_i = \alpha \prod_{p \in \mathbb{P}} p^{n(p)}$$

Uniqueness: Consider any $a \neq 0$ represented as $a = \alpha \prod_p p^{n(p)}$ as presented in the theorem. Then we fix any $q \in \mathbb{P}$, it is clear that

$$a = \alpha h q^{n(q)}$$
 where $h := \prod_{p \neq q} p^{n(p)}$

It is clear that $\langle q:q^n\rangle = n$, as $q^n \mid q^n$ and $q^{n+1} \mid q$ would imply $q \mid 1$ and hence $q \in R^*$. Further it is easy to see that $\langle q:\alpha h\rangle = 0$. Because if $q \mid \alpha h$ then $q \mid h$ (as $\alpha \in R^*$) and hence there has to be some $p \neq q$ such that $q \mid p$. That would be $q \approx p$ due to the irreducibility of p in contradiction to $p \neq q$ (as \mathbb{P} was a representing system). Hence we may use (i) again to find

$$\langle q:a\rangle = \langle q:\alpha hq^{n(q)}\rangle = \langle q:\alpha h\rangle + \langle q:q^{n(q)}\rangle = n(q)$$

In particular the exponent n(q) in this representation of a is uniquely determined to be $\langle q : a \rangle$. And as q has been arbitrary this means that n is uniquely determined. And as R is an integral domain this finally yields that α is uniquely determined, as well. (iii) Suppose b = ah for some $h \in R$. Then for any $p \in R$ prime we get $\langle p : b \rangle = \langle p : ah \rangle = \langle p : a \rangle + \langle p : h \rangle \ge \langle p : a \rangle$. Conversely suppose $\langle p : a \rangle \le \langle p : b \rangle$ for any $p \in R$ prime. Pick up a pepresenting system \mathbb{P} and use it to write a and b in the form

$$a = \alpha \prod_{p \in \mathbb{P}} p^{m(p)}$$
 and $b = \beta \prod_{p \in \mathbb{P}} p^{n(p)}$

By assumption we have $m(p) = \langle p : a \rangle \leq \langle p : b \rangle = n(p)$. That is $k(p) := n(p) - m(p) \geq 0$. Hence we explicitly find some $h \in \mathbb{R}$ such that

$$b = ah$$
 where $h := \alpha^{-1}\beta \prod_{p \in \mathbb{P}} p^{k(p)}$

- (v) Let us abbreviate $d := \prod_p p^{m(p)}$ then we need to verify that d is a greatest common divisor of A. By definition of m(p) we have $\langle p : d \rangle = m(p) \leq \langle p : a \rangle$ for any $p \in \mathbb{P}$ and any $a \in A$. And by (iii) that is $d \mid a$ and for any $a \in A$ and hence $d \mid A$. Conversely consider any $c \in R$ with $c \mid A$. In particular we have $c \neq 0$ as $0 \notin A \neq \emptyset$. And hence $c \mid a$ implies $\langle p : c \rangle \leq \langle p : a \rangle$ for any $p \in \mathbb{P}$ (and $a \in A$) by (iii) again. This is $\langle p : c \rangle \leq m(p) = \langle p : d \rangle$ for any $p \in \mathbb{P}$ and hence $c \mid d$ by (iii). The statement for the least common multiple can be proved in complete analogy. We only have to note that the assumption $\#A < \infty$ guarantees $n \in \bigoplus_p \mathbb{N}$ again.
- (vi) Once more we choose a representing system \mathbb{P} of the primes of R. And for any $p \in \mathbb{P}$ let us abbreviate $m(p) := \min\{\langle p : a \rangle, \langle p : b \rangle\}$ and likewise $n(p) := \min\{\langle p : a \rangle, \langle p : b \rangle\}$. Then it is a standard fact that $m(p) + n(p) = \langle p : a \rangle + \langle p : b \rangle$. By (ii) and (v) that is

$$\begin{array}{lll} \langle p:ab\rangle &=& \langle p:a\rangle + \langle p:b\rangle &=& m(p) + n(p) \\ &=& \langle p:a\rangle + \langle p:b\rangle &=& \langle p:dm\rangle \end{array}$$

And as this holds true for any $p \in \mathbb{P}$ (iv) immediately yields the claim.

(vii) We commence with the notation of (vi) and choose any $e \in \gcd\{a, b, c\}$. Then by (v) the order of $p \in \mathbb{P}$ in c is given to be the following

$$\begin{array}{lll} \langle p:e\rangle &=& \min\{\,\langle p:a\rangle, \langle p:b\rangle, \langle p:c\rangle\,\} \\ &=& \min\{\,\min\{\,\langle p:a\rangle, \langle p:b\rangle\,\}, \langle p:c\rangle\,\} \\ &=& \min\{\,\langle p:d\rangle, \langle p:c\rangle\,\} \,=\, \langle p:e'\rangle \end{array}$$

And the latter is the order of any greatest common divisor of $e' \in \gcd\{c, d\}$. As this is true for any $p \in \mathbb{P}$ we thereby find that e and e' are associated. The claim for the greatest common divisors follows immediately. The aanalogous argumentation also rests the case for the least common multiples.

Proof of (2.54):

As R is an UFD, it is an integral domain, by definition. Thus choose any $0 \neq x = b/a \in \text{QUOT } R$ that is integral over R, i.e. $\exists a_1, \ldots, a_n \in R$ with

$$x^n + a_1 x^{n-1} + \dots + a_n = 0$$

Then we need to show that $a \mid b$ already. But as R is an UFD we may let $d := \gcd\{a, b\}$ and write $a = \alpha d$ and $b = \beta d$. Then α and β are relatively prime and $a \mid b$ can be put as $\alpha \in R^*$ (as then $b = (\alpha^{-1}\beta)a$). By multiplying the above equation with α^n we find (note $x = \beta/\alpha$)

$$\beta^n + \alpha \left(a_1 \beta^{n-1} + \dots + \alpha^{n-1} a_n \right) = 0$$

And hence α divides β^n - but as α and β were relatively prime, so are α and β^n . But together this implies that α truly is a unit of R.

Proof of (2.55):

(ii) We first prove the irreducibility of $2 \in \mathbb{Z}[\sqrt{-3}]$. Thus let $\omega := i\sqrt{3}$ and suppose $2 = (a + b\omega)(c + d\omega)$. Then by complex conjugation we find $2 = (a - b\omega)(c - d\omega)$. Multiplying these two equations we get

$$4 = 2 \cdot 2 = (a^2 + 3b^2)(c^2 + 3d^2) \ge 9(bd)^2$$

Thus if both $b \neq 0$ and $d \neq 0$ this formula ends up with the contradicion $4 \ge 9(bd)^2 \ge 9$. Thus without loss of generality (interchanging a, c and b, d if necessary) we may assume d = 0. Then we have

$$4 = (a^2 + 3b^2)c^2$$

Of course c = 0 cannot be (else 4 = 0). If |c| = 1 then $c + d\omega = \pm 1$ which of course is a unit in $\mathbb{Z}[\sqrt{-3}]$. Thus suppose $|c| \ge 2$ then $c^2 \ge 4$ such that necessarily $a^2 + 3b^2 = 1$. This of course can only be if a = 1 and b = 0 such that now $a + b\omega$ is a unit of $\mathbb{Z}[\sqrt{-3}]$. Altogether 2 is irreducible.

- On the other hand $2 \mid 4 = (1 + \omega)(1 \omega)$. Now suppose we had $2 \mid 1 + \omega$, say $2(a + b\omega) = 1 + \omega$. Then 2a = 1 and hence $2 = \in \mathbb{Z}^*$ which is false. Likewise we see that 2 does not divide 1ω and this means that 2 is not prime.
- (iii) We first prove that $p = s^2 + t^2 1$ is irreducible in $\mathbb{R}[s, t]$. To do this we fix the graded lexicographic order on $\mathbb{R}[s, t]$, that is $\mathbb{R}[s, t]$ is ordered

by (total) degree and by s < t. Now consider any two polynomials f, $g \in \mathbb{R}[s,t]$ such that fg = p. Then

$$lt(f)lt(g) = lt(fg) = lt(p) = lt(-1 + s^{2} + t^{2}) = t^{2}$$

By prime decomposition of the leading coefficient in $\mathbb{R}[s, t]$ we see that either lt(f) = 1, lt(f) = t or $lt(f) = t^2$. If lt(f) = 1 then f is a unit in $\mathbb{R}[s, t]$, likewise if $lt(f) = t^2$ then lt(g) = 1 and hence g is a unit in $\mathbb{R}[s, t]$. thus we only have to exclude the case lt(f) = t. But in this case lt(g) = t as well such that

$$f = a + bs + ct$$
$$g = u + vs + wt$$

for some coefficients a, b, c, u, v and $w \in \mathbb{R}$. From this we may compute fg and compare its coefficients with those of p. Doing this an easy computation yields

(1)	au	=	-1	constant term
(2)	av + bu	=	0	s-term
(3)	aw + cu	=	0	t-term
(4)	bv	=	1	s^2 -term
(5)	bw + cv	=	0	<i>st</i> -term
(6)	cw	=	1	t^2 -term

In particular $a \neq 0$ and hence we may regard (f/a)(ag) = fg = pinstead. That is we may assume a = 1, then u = -1 by (1). And thus (2) turns into b = v and (3) becomes c = w. From this and (5) we get 2bc = 0. That is b = 0 or c = 0. But b = 0 would be a contradiction to (4) and c = 0 would be a contradiction to (6). Thus lc (f) = t cannot occur and this is the irreducibility of p.

• We now prove that $R = \mathbb{R}[s, t]/\mathfrak{p}$ is no UFD. To do this let us denote the set $X := \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \}$. And thereby we define the following multiplicatively closed subset of R

$$U := \{ f + \mathfrak{p} \in R \mid \forall (x, y) \in X : f(x, y) \neq 0 \}$$

By construction it is clear that U is truly well defined (if $f - g = q \in \mathfrak{p}$ then for any $(x, y) \in X$ we get f(x, y) = g(x, y) + q(x, y) = g(x, y)) and multiplicatively closed (as \mathbb{R} is an integral domain). Let us now denote the element $r := s + \mathfrak{p} \in R$. Then we will prove that $r/1 \in U^{-1}R$ is irreducible but not prime. Thus $U^{-1}R$ is no UFD and hence R has not been an UFD by virtue of (2.109).

- Let us first prove that r/1 is not prime. To do this let us define the following elements $a := 2(t+1) + \mathfrak{p}$ and $b := -2(t-1) + \mathfrak{p} \in R$. Then $ab = -4(t^2 1) + \mathfrak{p} = 4s^2 + \mathfrak{p} = 4r^2$. In particular $r \mid ab$ and hence $r/1 \mid (ab)/1 = (a/1)(b/1)$. Now assume $r/1 \mid a/1$ that is there are some $h + \mathfrak{p} \in R$ and $u + \mathfrak{p} \in U$ such that $a/1 = (r/1)(h + \mathfrak{p}/u + \mathfrak{p})$. As $\mathbb{R}[s,t]$ is an integral domain that is $2(t+1)u + \mathfrak{p} = sh + \mathfrak{p}$ or in other words $2(t+1)u sh =: q \in \mathfrak{p}$. Now regard $(0,1) \in X$ then $0 = q(0,1) = 4u(0,1) \neq 0$, a contradiction. That is $r/1 \not\mid a/1$ and likewise we find $r/1 \not\mid b/1$ by regarding $(0,-1) \in X$.
- So it only remains to prove that r/1 is irreducible. Thus suppose there are some $f, g \in \mathbb{R}[s, t]$ and $u + \mathfrak{p}, v + \mathfrak{p} \in U$ such that

$$\frac{s+\mathfrak{p}}{1} = \frac{r}{1} = \frac{f+\mathfrak{p}}{u+\mathfrak{p}}\frac{g+\mathfrak{p}}{v+\mathfrak{p}} = \frac{fg+\mathfrak{p}}{uv+\mathfrak{p}}$$

That is $suv + \mathfrak{p} = fg + \mathfrak{p}$ or in other words $suv - fg =: q \in \mathfrak{p}$. As $q \in \mathfrak{p} = p\mathbb{R}[s, t]$ and p vanishes on X identically, so does q. And this means that for any $(x, y) \in X$ we have the following identity

$$xu(x,y)v(x,y) = f(x,y)g(x,y)$$

In particular fg and suv and have the same roots. And as u, v do not vanish on X these are precisely the points (0, 1) and $(0, -1) \in X$. If fdoes not vanish on X then $f + \mathfrak{p} \in U$ and hence $f + \mathfrak{p}/u + \mathfrak{p}$ is a unit of $U^{-1}R$. Likewise if g does not vanish on X then $g + \mathfrak{p}/v + \mathfrak{p}$ is a unit of $U^{-1}R$. Thus in order to prove the irreducibility of r/1 it suffices to check that at f or g does not vanish on X.

• Thus assume this was false, that is f and g vanish on at least one point, say f(0,1) = 0 and g(0,-1) = 0 (else interchange f and g). We now parametrisize X using the following curve

$$\Omega : [0, 2\pi] \twoheadrightarrow X : \omega \mapsto \begin{pmatrix} \cos(\omega) \\ \sin(\omega) \end{pmatrix}$$

First suppose neither f(0,-1) = 0 nor g(0,1) = 0, that is f and gboth have precisely one root on X. Then f cannot change signs on X (else $[0,2\pi] \to \mathbb{R} : \omega \mapsto f\Omega(\omega)$ would have to have at least two roots because of $f\Omega(0) = f\Omega(2\pi) \neq 0$). And the same is true for g. Thus $(x,y) \mapsto f(x,y)g(x,y)$ does not change sign on X. Likewise uvdoes not have a single root on X and hence its sign on X is constant. Hence $(x,y) \mapsto xu(x,y)v(x,y)$ does change sign in contradiction to the equality of these two functions. Thus at least one of the two f or g even has to have two roots on X. • We only regard the case f(0,1) = 0 and g(0,1) = 0 = g(0,-1). The other case (where f has both roots) is completely analogous. The basic ideas is the following: as both f and g vanish in (0,1) this is a root of order 2 for fg. But xuv only has a root of order 1 in (0,1). Thus let us do same basic calculus - we have $\Omega(\pi/2) = (0,1)$ and in this point we get $\Omega'(\pi/2) = (1,0)$. Thus in this case we find another contradiction to suv = fg by evaluating

$$\begin{aligned} & ((suv)\Omega)'(\pi/2) &= \langle \begin{pmatrix} uv + sv\partial_s u + su\partial_s v \\ sv\partial_t u + su\partial_t v \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \\ &= u(0,1)v(0,1) \neq 0 \end{aligned}$$

$$((fg)\Omega)'(\pi/2) = \langle \begin{pmatrix} g\partial_s f + g\partial_s g \\ g\partial_t f + g\partial_t f \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle$$
$$= \langle (0,0) : (1,0) \rangle = 0$$

Proof of (2.58):

- (ii) First consider a > 0, then it is clear that q := b div $a \in \mathbb{Z}$ exists, as the set $\{q \in \mathbb{Z} \mid aq \leq b\} =] \infty, b/a] \cap \mathbb{Z}$ contains the maximal element q = a/b rounded down. And from the construction of $r := b \mod a$ it is clear that b = aq + r. From the definition of q it is also clear that $0 \leq r$. Now assume $r \geq a$ then $a(q+1) = aq+a \leq aq+r = b$ and hence q would not have been maximal a contradiction. Thus we also have $0 \leq r < a$ and hence $\alpha(r) = r < a = \alpha(a)$. Thus we have established the division with remainder for a > 0. If conversely a < 0 then -a > 0 and hence we may let q := (-b) div (-a) and r := -((-b) div (-a)). Then we have just proved -b = q(-a) r which yields b = qa + r and $\alpha(r) = \alpha(-r) < \alpha(-a) = \alpha(a)$.
- (iii) Consider any $g \in E[t]$, $0 \neq f \in E[t]$ and let $\alpha := \operatorname{lc}(f)$. Then $\overline{f} := \alpha^{-1}f \in E[t]$ is normed. Further let $\overline{g} := \alpha^{-1}g$. Then by (??) there are $q, r \in E[t]$ such that $\overline{g} = q\overline{f} + r$. Multiplying with α we find $g = qf + \alpha r$ and $\operatorname{deg}(\alpha r) = \operatorname{deg}(r) < \operatorname{deg}(f)$ (as $\alpha \in E^*$). Thus we have established the division with remainder on E[t].
- (iv) It is straightforward to check that $\mathbb{Z}[\sqrt{d}]$ truly is a subring of \mathbb{C} . Clearly $0 = 0 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ and $1 = 1 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Now consider $x = a + b\sqrt{d}$ and $y = f + g\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Then it is clear that

$$\begin{array}{rcl} x+y &=& (a+f)+(b+g)\sqrt{d} &\in \ \mathbb{Z}[\sqrt{d}] \\ xy &=& (af+dbg)+(ag+bf)\sqrt{d} &\in \ \mathbb{Z}[\sqrt{d}] \end{array}$$

Thus $\mathbb{Z}[\sqrt{d}]$ is a subring of \mathbb{C} and in particular an integral domain. Now assume x = y, then we wish to verify (a, b) = (f, g) (the converse implication is clear). Assume we had $b \neq g$ then we would be able to divide by $b - g \neq 0$ and hence get

$$\sqrt{d} = \frac{f-a}{b-g} \in \mathbb{Q}$$

a contradiction to the assumption $\sqrt{d} \notin \mathbb{Q}$. Thus we have b = g and hence (substracting $b\sqrt{d} = g\sqrt{d}$) also a = f. Thus $x \mapsto \overline{x}$ is truly well defined and the bijectivity is clear. We also see $\overline{0} = 0 - 0\sqrt{d} = 0$ and $\overline{1} = 1 - 0\sqrt{d} = 1$ immediately. It remains to prove that $x \mapsto \overline{x}$ also is additive and multiplicative, by computing

$$\overline{x} + \overline{y} = (a - b\sqrt{d}) + (f - g\sqrt{d}) = (a + f) - (b + g)\sqrt{d} = \overline{x + y}$$
$$\overline{xy} = (a - b\sqrt{d})(f - g\sqrt{d}) = (af + dbg) - (ag + bf)\sqrt{d} = \overline{xy}$$

But from this it is clear that ν also is multiplicative. Just compute $\nu(xy) = |xy\overline{xy}| = |x\overline{x}y\overline{y}| = |x\overline{x}| \cdot |y\overline{y}| = \nu(x)\nu(y)$. We finally note that for any $0 \neq x \in \mathbb{Z}[\sqrt{d}]$ we get $\nu(x) \neq 0$, since $\nu(x) = |a^2 - db^2| = 0$ is equivalent to $a^2 = db^2$. Thus if b = 0 then a = 0 and hence x = 0 as claimed. And if $b \neq 0$ then we may divide by b to find $(a/b)^2 = d$. In other words $\sqrt{d} = a/b \in \mathbb{Q}$, a contradiction to the assumption $\sqrt{d} \notin \mathbb{Q}$. Thus the case $b \neq 0$ cannot occur in the first place.

Next we prove that the units of $\mathbb{Z}[\sqrt{d}]$ are precisely the elements x such that $\nu(x) = 1$. If $x \in \mathbb{Z}[\sqrt{d}]^*$ is a unit, then we have $1 = \nu(1) = \nu(xx^{-1}) = \nu(x)\nu(x^{-1})$ and hence $\nu(x) \in \mathbb{Z}^*$. But as also $\nu(x) \ge 0$ this yields $\nu(x) = 1$. Thus consider any $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ such that $\nu(x) = 1$. Then $x\overline{x} = a^2 - db^2 = \pm 1$ and hence $x^{-1} = \pm \overline{x}$ is invertible.

Now assume that $d \leq -3$ then we want to prove that 2 is an irreducible element of $\mathbb{Z}[\sqrt{d}]$ that is not prime. We begin by proving that 2 is not prime: as either d or d-1 is even we have

2 |
$$d(d-1) = d^2 - d = (d + \sqrt{d})(d - \sqrt{d})$$

but we have $2 \not| d \pm \sqrt{d}$, because if we assume $2(a+b\sqrt{d}) = d \pm \sqrt{d}$ then (comparing the \sqrt{d} -coefficient) we had $2b = \pm 1 \in \mathbb{Z}$ in contradiction to $2 \notin \mathbb{Z}^*$. However 2 is irreducible, assume 2 = xy for some $x, y \in \mathbb{Z}[\sqrt{d}]$. Then $4 = \nu(2) = \nu(xy) = \nu(x)\nu(y)$. Hence we have $\nu(x) \in \{1, 2, 4\}$. If $\nu(x) = 1$ then $x \in \mathbb{Z}[\sqrt{d}]^*$ is a unit. And if $\nu(x) = 4$ then $\nu(y) = 1$ and hence $y \in \mathbb{Z}[\sqrt{d}]^*$ is a unit. It suffices to exclude the case $\nu(x) = 2$, that is assume $\nu(x) = 2$. As $d \leq -3$ we have $2 = \nu(x) = a^2 - db^2$. Thus in the case $b \neq 0$ we obtain $2 = a^2 - db^2 \geq 0 + 3 \cdot 1 = 3$ a contradiction. And in case b = 0 we get $2 = a^2$ for some $a \in \mathbb{Z}$, in contradiction to the irreducibility of 2 in \mathbb{Z} . Thus $\nu(x) = 2$ cannot occur and this means that $2 \in \mathbb{Z}[\sqrt{d}]$ is irreducible. It remains to prove that $(\mathbb{Z}[\sqrt{d}], \nu)$ even is an Euclidean domain for $d \in \{-2, -1, 2, 3\}$. We consider the elements $0 \neq x = a + b\sqrt{d}$ and $y = f + g\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then (as $\nu(y) \neq 0$) we may define

$$p := \frac{af - dbg}{a^2 - db^2}$$
$$q := \frac{ag - bf}{a^2 - db^2}$$

That is $p + q\sqrt{d} := (1/(a^2 - db^2))y\overline{x}$. And therefore we obtain the identity $(p + q\sqrt{d})x = (1/(f^2 - dg^2))y\overline{x}x = y$. In other words we have found y/x to be $p+q\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Now choose $r, s \in \mathbb{Z}$ such that |p-r| and $|q-s| \leq 1/2$ (which is possible, as the intervals [r-1/2, r+1/2] (for $r \in \mathbb{Z}$) cover \mathbb{Q}) and define

$$u := r + s\sqrt{d}$$
$$v := y - ux$$

Then it is clear that $u, v \in \mathbb{Z}[\sqrt{d}]$ and y = ux + v. But further we find

$$x((p-r) + (q-s)\sqrt{d}) = x\left(\frac{y}{x} - u\right) = y - ux = v$$

Due to the multiplicativity of ν (which even remains true for coefficients (here p-r and q-s) in \mathbb{Q}) we find $\nu(v) = \nu(x)|(p-r)^2 - d(q-s)^2|$. But as $|d| \leq 3$ we can estimate

$$|(p-r)^2 - d(q-s)^2| \le (p-r)^2 + |d|(q-s)^2 \le (1/2)^2 + 3(1/2)^2 = 1$$

The case $|(p-r)^2 - d(q-s)^2| = 1$ can only occur if |p-r| = |p-s| = 1/2and d = 3. But in this case we have $|(p-r)^2 - d(q-s)^2| = |1/4 - 3/4| = 1/2 < 1$. Thus we have even proved the strict estimate

$$\nu(v) = \nu(x)|(p-r)^2 - d(q-s)^2| < \nu(x)$$

Altogether we have seen that $\mathbb{Z}[\sqrt{d}]$ is an integral domain and that given $0 \neq x, y \in \mathbb{Z}[\sqrt{d}]$ we can find $u, v \in \mathbb{Z}[\sqrt{d}]$ such that y = ux + v and $\nu(v) < \nu(x)$. But this is the condition to be an Euclidean domain.

Proof of (2.59):

• Without loss of generality we assume $\nu(a) \leq \nu(b)$ and let $f_1 := b$ and $f_2 := a$. That is if f and g are determined using the initialisation of the algorithm, then we get $f_1 = g$ and $f_2 = f$. Suppose we have

already computed $f_1, \ldots, f_k \in R$ and $f_k \neq 0$, then in the next step the algorithm computes $q_k := q$ and $f_{k+1} := r \in R$ such that

$$f_{k-1} = q_k f_k + f_{k+1}$$

and $\nu(f_{k+1}) < \nu(f_k)$. Thus by induction on k we find the following strictly decreasing sequence of natural numbers

 $\nu(b) \ = \ \nu(f_1) \ \ge \ \nu(f_2) \ > \ \nu(f_3) \ > \ \ldots \ > \ \nu(f_k) \ > \ \nu(f_{k+1}) \ > \ \ldots$

As $\nu(b)$ is finite this chain cannot decrease indefinitely but has to terminate at some level n. That is $f = f_{n+1} = 0$. And therefore $f_{n-1} = q_n g$ where $g = f_n$.

- We will now prove that for any $1 \le k \le n$ we have $g \mid f_k$. For k = n we trivially have $g \mid g = f_n$. And for k = n 1 we have $f_{n-1} = q_n g$ by construction. Thus by induction we can assume $k \le n 1$ and $g \mid f_n$ to $g \mid f_k$. Then from $f_{k-1} = q_k f_k + f_{k+1}$ it also is clear that $g \mid f_{k-1}$ completing the induction. In particular we have $g \mid f_2 = a$ and $g \mid f_1 = b$.
- Now suppose we are given some $d \in R$ with $d \mid a = f_2$ and $d \mid b = f_1$. Then we will prove that for any $k \in 1 \dots n$ we get $d \mid f_n$ by induction on k. Thus assume $k \geq 2$ and $d \mid f_1$ to $d \mid f_k$. Then from $f_{k+1} = f_{k-1} + q_k f_k$ we also get $d \mid f_{k+1}$ completing the induction. In particular we get $d \mid f_n = g$. And hence g truly is the greatest common divisor of a and b.
- We will now prove the correctness of the refined Euclidean algorithm. The first part (the computation of g) is just a reformulation of the standard Euclidean algorithm. And as the second part is a finite computation, it is clear that the algorithm terminates. Next we will first prove that for any $2 \le k \in \mathbb{N}$ we have $f_k = r_k f_2 + s_k f_1$. For k = 2 this is trivial $f_2 = 1 \cdot f_2 + 0 \cdot f_1 = r_2 f_2 + s_2 f_1$. And for $k \ge 3$ we have computed $q_k \in R$ such that $f_{k-1} = q_k f_k + f_{k+1}$ for some $f_{k+1} \in R$. In particular $f_3 = f_1 q_2 f_2 = (-q_2) f_2 + 1 \cdot f_1 = r_3 f_2 + s_3 f_1$. Now we will use induction on k. That is we assume $f_{k-1} = r_{k-1} f_2 + s_{k-1} f_1$ and $f_k = r_k f_2 + s_k f_1$. Then a computation immediately yields

$$r_{k+1}f_2 + s_{k+1}f_1 = (r_{k-1} - q_k r_k)f_2 + (s_{k-1} - q_k s_k)f_1$$

= $(r_{k-1}f_2 + s_{k-1}f_1) - q_k(r_k f_2 + s_k f_1)$
= $f_{k-1} - q_k f_k = f_{k+1}$

In particular for k = n we find $g = f_n = r_n f_2 + s_n f_1$. Thus let us distinguish the two cases. If $\nu(a) \leq \nu(b)$ we have $f_1 = b$, $f_2 = a$, $r = r_n$ and $s = s_n$. Thereby we get $g = r_n f_2 + s_n f_1 = ra + sb$. And
conversely if $\nu(a) > \nu(b)$ then $f_1 = a$, $f_2 = b$, $r = s_n$ and $s = r_n$. Thereby we get $g = r_n f_2 + s_n f_1 = sb + ra$. Thus in any case we have obtained r and $s \in R$ such that g = ra + sb.

Proof of (2.61):

- (i) We use induction on n to prove the statement. For n = 0 and any $a \in R_0 = R^*$ it is clear that $a \in R_1$, as for any $b \in R$ we may choose r = 0 and thereby get $a(ba^{-1}) = b$ such that $a \mid b r$. Thus for $n \mapsto n+1$ we are given $a \in R_n$ and any $b \in R$. That is we have $a \mid b r$ for some $r \in R_{n-1}$. But by induction hypothesis we know $R_{n-1} \subseteq R_n$ and hence $r \in R_n$. But this again means $a \in R_{n+1}$ (as b has been arbitary) which had to be proved.
- (ii) We use induction on n again. For n = 0 we are given any $a \in R$ such that $\nu(a) \leq 0$. If $\nu(a) < 0$ then $\nu(a) = -\infty$ and hence a = 0. Otherwise $\nu(a) = 0$ and we use division with remainder to find some q, $r \in R$ such that 1 = qa + r and $\nu(r) < \nu(a) = 0$. But this can only be if $\nu(r) = -\infty$ which is r = 0. Hence we have 1 = qa, that is $a \in R^* = R_0$ is a unit of R. In the induction step $n \mapsto n + 1$ we are given some $a \in R$ with $\nu(a) \leq n + 1$. Given $b \in R$ we use division with remainder to find $q, r \in R$ such that b = qa + r and $\nu(r) < \nu(a) \leq n + 1$. Thus we have $\nu(r) \leq n$ and by induction hypothesis this yields $r \in R_n \cup \{0\}$. That is $a \mid b - r$ for some $r \in R_n \cup \{0\}$. And as b has been arbitary this means $a \in R_{n+1}$, which had to be shown.
- (iii) Clearly μ is well defined, as by assumption any $0 \neq a \in R$ is contained in some R_n . We need to prove that μ truly allows division with remainder: thus consider any $0 \neq a$ and $b \in R$, then we need to find $q, r \in R$ such that b = qa + r and $\mu(r) < \mu(a)$. If $\mu(a) = 0$ then $a \in R_0 = R^*$ and hence we may choose $q := ba^{-1}$ and r = 0. If $\mu(a) \ge 1$ then we let $n := \mu(a) - 1 \in \mathbb{N}$. As $a \in R_{n+1}$ and $b \in R$ we have $a \mid b - r$ for some $r \in R_n \cup \{0\}$. This again yields $\mu(r) \le n < n + 1 = \mu(a)$ and b = qa + r for some $q \in R$, just what we wanted.
- (iii) Next we want to prove $\mu(a) \leq \mu(ab)$. If ab = 0 then (as $b \neq 0$ and R is an itegral domain) we have a = 0. Thereby $\mu(a) = -\infty = \mu(ab)$. Thus assume $ab \neq 0$, and let $n := \mu(ab) \in \mathbb{N}$. If n = 0 then $ab \in R_0 = R^*$ and hence $a \in R^* = R_0$ (with $a^{-1} = b(ab)^{-1}$). Thus we likewise have $\mu(a) = 0 = \mu(ab)$. If now $n \geq 1$ then for any $c \in R$ there is some $r \in R_{n-1} \cup \{0\}$ such that $ab \mid c - r$. But as $a \mid ab$ this yields $a \mid c - r$, too and hence $a \in R_n$ again. Thereby $\mu(a) \leq n = \mu(ab)$.

- (iii) If $a \in R^*$ then by (iii) above we have $\mu(b) \leq \mu(ab) \leq \mu(a^{-1}ab) = \mu(b)$ and hence $\mu(b) = \mu(ab)$. Conversely suppose $\mu(b) = \mu(ab)$. As $b \neq 0$ we also have $ab \neq 0$ (else $\mu(ab) = -\infty \neq \mu(b)$). Thus we may use division with remainder to find some $q, r \in R$ such that b = q(ab) + rand $\mu(r) < \mu(b)$. Rearranging this equation we find (1 - qa)b = r. Now suppose we had $1 - qa \neq 0$, then by (iii) above again we had $\mu(b) \leq \mu((1 - qa)b) = \mu(r) < \mu(b)$, a contradiction. Thus we have qa = 1 and this means $a \in R^*$ as claimed.
- (iv) If $R \setminus \{0\} = \bigcup_n R_n$ then (R, μ) is an Euclidean domain by (iii). Conversely suppose (R, ν) is an Euclidean domain for some Euclidean function ν . Now consider any $0 \neq a \in R$, and let $n := \nu(a)$. Then we have already seen in (ii) that $a \in R_n$ and hence we have $R \setminus \{0\} = \bigcup_n R_n$.
- (v) As (R, ν) is an Euclidean domain we have $R \setminus \{0\} = \bigcup_n R_n$ by (iv). But by (iii) this implies that (R, μ) is an Euclidean domain, too. Thus consider any $a \in R$, if a = 0 then $\mu(a) = -\infty = \nu(a)$ by convention. Else let $n := \nu(a) \in \mathbb{N}$. Then $a \in R_n$ by (ii) and hence $\mu(a) \leq n = \nu(a)$ by construction of μ .

Proof of (2.64):

We will only prove parts (i), (ii) and (iii) here. Part (iv) requires the theory of Dedekind domains an will be postponed until then - see page (382).

- (i) Clearly 0 ≤_i R is a prime ideal, as R is an integral domain (if ab ∈ 0 then ab = 0 and hence a = 0 or b = 0 such that a ∈ 0 or b ∈ 0 again). And further any maximal ideal is prime, because of (2.19). Conversely consider any non-zero prime ideal 0 ≠ p ≤_i R. As R is a PID there is some p ∈ R such that p = pR. By (2.47.(ii)) this means that p is prime and due to (2.47.(v)) this implies that p is irreducible (as R is an integral domain). Now consider any ideal a such that p ⊆ a ≤_i R. As R is a PID there is some a ∈ R with a = aR again. Now p ∈ pR ⊆ aR means that there is some b ∈ R such that p = ab. But p has been irreducible, that is a ∈ R* or b ∈ R*. In the case a ∈ R* we have a = aR = R. And in the case b ∈ R* we have a ≈ b and hence a = aR = pR = p. As a has been arbitrary this means that p already is maximal.
- (ii) As R is a PID every ideal \mathfrak{a} of R is generated by *one* element $\mathfrak{a} = aR$. In particular any ideal \mathfrak{a} is generated by *finitely many* elements. Thus R is notherian by property (c) in (2.27). We will now prove property (d) of UFDs. As R is noetherian property (1) in (2.49.(d)) is trivially satisfied by (ACC) of noetherian rings. Hence it suffices to check

property (2) of (2.49.(d)). But as R is an integral domain any prime element $p \in R$ already is irreducible, due to (2.47.(ii)). This leaves

 $p \in R$ irreducible $\implies p \in R$ prime

Thus suppose $p \mid ab$ for some p, a and $b \in R$, say pq = ab. As R is a PID and $aR + pR \leq_i R$ is an ideal we find some $d \in R$ such that dR = aR + pR. That is there are $r, s \in R$ such that d = ar + ps. And as $a \in aR + pR = dR$ there is some $f \in R$ with a = df. Likewise we find some $g \in R$ with p = dg. But as p is irreducible we have $g \in R^*$ or $d \in R^*$. If $g \in R^*$ then we get $p \mid a$ from

$$p(fg^{-1}) = (g^{-1}p)f = df = a$$

And if $d \in R^*$ we get $p \mid b$ by the equalities below. Thus we have found $p \mid a$ or $p \mid b$ which means that p is prime

$$p(d^{-1}qr + d^{-1}bs) = d^{-1}(pqr + pbs) = d^{-1}(abr + pbs)$$

= $bd^{-1}(ar + ps) = bd^{-1}d = b$

(iii) If $\mathfrak{a} = 0$ then $\mathfrak{a} = 0R$ is a principal ideal (generated by $0 \in R$). And if $\mathfrak{a} \neq 0$ there is some $0 \neq b \in \mathfrak{b}$. Therefore we may choose a as given in the claim of (iii). Now consider any $b \in \mathfrak{a}$ and choose $q, r \in R$ such that b = qa + r and $\nu(r) < \nu(a)$. Then $r = b - qa \in \mathfrak{a}$ (as $a, b \in \mathfrak{a}$). But a has minimal value $\nu(a)$ among all those $b \in \mathfrak{a}$ with $b \neq 0$. Therefore $r \in \mathfrak{a}$ and $\nu(r) < \nu(a)$ implies r = 0. Thus $b = qa \in aR$, and as b has been arbitary this means $\mathfrak{a} \subseteq aR$. And as $a \in R$ we have $aR \subseteq \mathfrak{a}$. Together we find that $\mathfrak{a} = aR$ is a principal ideal. And as \mathfrak{a} has been arbitary this means that R is a PID.

Proof of (2.66):

(i) As R is an UFD by (2.64.(ii)) the length $\ell(a) \in \mathbb{N}$ of $0 \neq a \in R$ is well defined, due to (2.49.(b)). Therefore $\delta: R \to \mathbb{N}$ is a well-defined function and it is clear that it satisfies properties (1) and (2). Thus consider any $0 \neq a, b \in R$, as R is a PID we may choose some $r \in R$ such that rR = aR + bR. It is clear that $r \neq 0$, as $0 \neq a \in rR$. Now suppose $b \notin aR$, Then it is clear that $r \in aR + bR$ and it remains to prove $\delta(r) < \delta(a)$. As $a \in aR + bR = rR$ there is some $s \in R$ such that a = rs. Suppose $s \in R^*$, then $a \approx r$ and hence aR = rR. But $b \in aR + bR = rR = aR$ is a contradiction to $b \notin aR$. Thus $s \notin R^*$ which means $\ell(s) \geq 1$. Hence we have $\delta(s) \geq 2$ and as $\delta(r) > 0$ (recall $r \neq 0$) this finally is

$$\delta(r) < 2\delta(r) \le \delta(r)\delta(s) = \delta(rs) = \delta(a)$$

- (ii) As a ≠ 0 there is some 0 ≠ b ∈ a. And hence we may choose a ∈ a as given in the claim of (ii). We now want to verify a = aR, as a ∈ a the inclusion aR ⊆ a is clear. Conversely choose any 0 ≠ b ∈ a (0 ∈ aR is clear). If we had b ∉ aR, then by property (3) there would be some r ∈ aR + bR such that δ(r) < δ(a). But as a, b ∈ a we have aR + bR ⊆ a and hence r ∈ a. As a has been chosen to have minimal value δ(a) this only leaves r = 0 and hence 0 ≠ a ∈ aR + bR = rR = 0, a contradiction. Thus we have b ∈ aR and hence a ⊆ aR as well.
- (iii) By construction of δ it is clear that $\delta : R \to \mathbb{N}$ and that δ satisfies (2). It remains to verify (3), thus consider any $0 \neq a, b \in R$ then we choose $q, r \in R$ such that b = qa + r and $\nu(r) < \nu(a)$. If r = 0 then $b = qa \in aR$. And if $r \neq 0$ we have $r = -qa + b \in aR + bR$ and $\delta(r) = \nu(r) + 1 < \nu(a) + 1 = \delta(a)$.

Proof of (2.67):

- (i) First suppose $mR = \bigcap_a aR$, in particular $mR \subseteq aR$ for any $a \in R$. But this is $a \mid m$ for any $a \in A$ and hence $A \mid m$. Now consider any $n \in R$ such that $A \mid n$, that is $a \mid n$ and hence $n \in aR$ for any $a \in A$. Therfore $n \in \bigcap_a aR = mR$ and hence $m \mid n$. Thus we have proved $m \in \text{lcm}(A)$. Conversely suppose $m \in \text{lcm}(A)$, then $A \mid m$ and hence $m \in \bigcap_a aR$ again. In particular we have $mR \subseteq \bigcap_a aR$. Now consider any $n \in \bigcap_a aR$, then $A \mid n$ again and hence $m \mid n$ by assumption on m. Thus we have $n \in mR$ and as n has been arbitrary this is the converse inclusion $\bigcap_a aR \subseteq mR$.
- (ii) Let $dR = \sum_a aR$ then for any $a \in A$ we have $aR \subseteq dR$ and hence $d \mid a$. Thus we found $d \mid A$, as a has been arbitrary. Now consider some $c \in R$ such that $c \mid A$. That is for any $a \in A$ we get $c \mid a$ and hence $aR \subseteq cR$. But from this we get $dR = \sum_a aR \subseteq cR$ which also is $c \mid d$. Together we have proved $d \in \operatorname{gcd}(A)$ again.
- (iii) Now assume that R is a PID, then we will also prove the converse implication. By assumption on R there is some $g \in R$ such that $gR = \sum_{a} aR$ and by (ii) this means $g \in \text{gcd}(A)$. Now from (2.47.(viii)) and $d, g \in \text{gcd}(A)$ we get $d \approx g$ and hence $dR = gR = \sum_{a} aR$.
- (iv) For n = 1 the statement is trivial for $b_1 := b$, thus let us assume $n \ge 2$. Then we denote $a := a_1 \dots a_n$ and $\hat{a}_i := a/a_i \in R$. Now consider $d \in \gcd\{\hat{a}_1, \dots, \hat{a}_n\}$ and suppose we had $d \notin R^*$. Then (as R is an UFD) there would be a prime element $p \in R$ dividing $p \mid d$. Thus we had $p \mid d \mid \hat{a}_1$ and hence (as p is prime) there would be some $i \in 2 \dots n$ such that $p \mid a_i$. Likewise for i we have $p \mid d \mid \hat{a}_i$

and hence $p \mid a_j$ for some $j \neq i$. But a_i and a_j are relatively prime by assuption, a contradiction. Thus we have $d \in R^*$, that is $1 \in \gcd\{\widehat{a}_1, \ldots, \widehat{a}_n\}$. And by (iii) this means that there are some $h_1, \ldots, h_n \in R$ such that $1 = h_1\widehat{a}_1 + \cdots + h_n\widehat{a}_n$. Now let $b_i := bh_i$, then the claim is immediate from

$$\sum_{i=1}^{n} \frac{b_i}{a_i} = \sum_{i=1}^{n} \frac{bh_i \widehat{a}_i}{a} = \frac{b}{a} \sum_{i=1}^{n} h_i \widehat{a}_i = \frac{b}{a}$$

Proof of (2.68):

- (a) \implies (b): consider $a, b \in R$, by assumption there are $r, s \in R$ such that $d = ra + sb \in \gcd(a, b)$. By construction we have $d \in aR + bR$ and hence $dR \subseteq aR + bR$. On the other hand we have $d \in \gcd(a, b)$ and hence $d \mid a$ and $d \mid b$. But that is $aR \subseteq dR$ and $bR \subseteq dR$ such that $aR + bR \subseteq dR$ as well. Together that is dR = aR + bR.
- (b) ⇒ (c): a being finitely generated means that there are some a₁,..., a_n ∈ R such that a = a₁R + ··· + a_nR. We will now use induction on n to prove that a is principal. In the case n = 0 we have a = 0 = 0R and in the case n = 1 trivially a = a₁R is principal. Thus we may assume n ≥ 2. Then by induction hypothesis u := a₁R + ··· + a_{n-1}R ≤_i R is principal, that is there is some u ∈ R such that u = uR. Now a = a₁R + ··· + a_nR = u + a_nR = uR + a_nR. Thus by assumption (b) there is some d ∈ R such that a = dR is principal.
- (c) \implies (a): consider any $a, b \in R$ and let $\mathfrak{a} := aR + bR$. By construction \mathfrak{a} is finitely generated and hence there is some $d \in R$ such that $\mathfrak{a} = dR$. Now $d \in aR + bR$ means that there are some r, $s \in R$ such that d = ra + sb. And by (2.67.(ii)) dR = aR + bR yields that $ra + sb = d \in \gcd(a, b)$ as well.

Proof of (2.69):

- (a) \implies (b) and (c): if R is a PID then R is a noetherian UFD due to (2.64.(ii)). And it is clear that R also is a Bezout domain (e.g. by property (c) in (2.68)).
- (c) \implies (a): consider any ideal $\mathfrak{a} \leq_{i} R$, as R is noetherian \mathfrak{a} is finitely generated, due to property (c) of noetherian rings (2.27). And due to poroperty (c) of Bezout domains (2.68) this means that \mathfrak{a} is principal. As a Bezout domain also is an integral domain this means that R is a PID.

• (b) \implies (a): consider any ideal $\mathfrak{a} \leq_i R$. If $\mathfrak{a} = 0$ then $\mathfrak{a} = 0R$ trivially is principal. Thus we assume $\mathfrak{a} \neq 0$ and choose any $0 \neq a \in R$ with

$$\ell(a) = \min\{\,\ell(b) \mid 0 \neq b \in \mathfrak{a}\,\}$$

where $\ell(a)$ is the number of prime factors of a, that is $\ell(a) = k$, where $a = p_1 \dots p_k$ for some prime elements $p_i \in R$. As $a \in \mathfrak{a}$ we have $aR \subseteq \mathfrak{a}$. Conversely consider any $0 \neq b \in \mathfrak{a}$. As R is a Bezout domain the ideal aR + bR is principal aR + bR = dR for some $d \in R$, due to property (b) in (2.68). As $a, b \in \mathfrak{a}$ we have $d \in aR + bR \subseteq \mathfrak{a}$ and clearly $d \neq 0$ (as $a \neq 0$). Thus by construction of a we have $\ell(a) \leq \ell(d)$. But on the other hand we have $a \in aR + bR = dR$ and hence $d \mid a$ which implies $\ell(d) \leq \ell(a)$ by (2.53.(iii)). But from $d \mid a$ and $\ell(a) = \ell(d)$ we get $a \approx d$ by choosing prime decompositions of a and d as in (2.53.(iv)). Therefore we have $b \in aR + bR = dR = aR$. This proves $b \in aR$ and hence $\mathfrak{a} \subseteq aR$, as b has been arbitary (b = 0 is clear). Altogether we have $\mathfrak{a} = aR$ is principal and hence R is a PID, as \mathfrak{a} has been arbitary.

Proof of (2.72):

- (a) \implies (b): consider $a + \mathfrak{a} \in \mathbb{ZD} R/\mathfrak{a}$, that is $a \in \mathbb{ZD}_R R/\mathfrak{a}$, then by assumption we have $a \in \sqrt{\mathfrak{a}}$. That is $a^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$ and hence $(a + \mathfrak{a})^k = a^k + \mathfrak{a} = 0 + \mathfrak{a}$ such that $a + \mathfrak{a}$ is a nilpotent of R/\mathfrak{a} .
- (b) \implies (c): the nil-radical of R/\mathfrak{a} is trivially included in the set of zero-divisors of R/\mathfrak{a} due to (1.26.(ii)), which implies equality.
- (c) \implies (a): consider $a \in \mathbb{ZD}_R R/\mathfrak{a}$, that is $a + \mathfrak{a} \in \mathbb{ZD} R/\mathfrak{a}$. Then by assumption $a + \mathfrak{a}$ is a nilpotent of R/\mathfrak{a} , that is $a^k + \mathfrak{a} = (a + \mathfrak{a})^k = 0 + \mathfrak{a}$ for some $k \in \mathbb{N}$. But this again means $a^k \in \mathfrak{a}$ and hence $a \in \sqrt{\mathfrak{a}}$.
- (c) ⇒ (d): consider a, b ∈ R such that ab ∈ a but b ∉ a. That is (a + a)(b + a) = ab + a = 0 + a and as b + a ≠ 0 + a this means that a + a ∈ ZD R/a is a zero-divisor of R/a. By assumption this means that a + a is a nilpotent of R/a and hence a^k + a = (a + a)^k = 0 + a for some k ∈ N. But this again is a^k ∈ a and hence a ∈ √a.
- (d) \implies (b): consider $a + \mathfrak{a} \in \mathbb{ZD} R/\mathfrak{a}$ that is there is some $0 + \mathfrak{a} \neq b + \mathfrak{a} \in R/\mathfrak{a}$ such that $ab + \mathfrak{a} = (a + \mathfrak{a})(b + \mathfrak{a}) = 0 + \mathfrak{a}$. But this means $ab \in \mathfrak{a}$ and as also $b \notin \mathfrak{a}$ we find $a \in \sqrt{\mathfrak{a}}$ by assumption. That is $a^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$ and hence $(a + \mathfrak{a})^k = a^k + \mathfrak{a} = 0 + \mathfrak{a}$ such that $a + \mathfrak{a}$ is a nilpotent of R/\mathfrak{a} .

• The equivalency (d) \iff (e) is finally true by elementary logical operations (note that we may commute the quantifiers $\forall a \text{ and } \forall b$)

(d)
$$\iff \forall a, b \in R : \neg ((ab \in \mathfrak{a}) \land (b \notin \mathfrak{a})) \lor (a \in \sqrt{\mathfrak{a}})$$

 $\iff \forall a, b \in R : (ab \notin \mathfrak{a}) \lor (b \in \mathfrak{a}) \lor (a \in \sqrt{\mathfrak{a}})$
 $\iff \forall b, a \in R : (ba \notin \mathfrak{a}) \lor (a \in \mathfrak{a}) \lor (b \in \sqrt{\mathfrak{a}})$
 $\iff \forall a, b \in R : (ab \notin \mathfrak{a}) \lor (b \in \sqrt{\mathfrak{a}}) \lor (a \in \mathfrak{a})$
 $\iff \forall a, b \in R : \neg ((ab \in \mathfrak{a}) \land (b \notin \sqrt{\mathfrak{a}})) \lor (a \in \mathfrak{a})$
 $\iff (e)$

Proof of (2.74):

We will only prove statements (i) to (vii) here. Statement (viii) is concerned with localisations and requires the correspondence theorem of ideals in localisations. Its proof is hence postponed until we have shown this theorem. Hence it can be found on page (363).

- (i) If $\mathfrak{P} \leq_{i} R$ is prime and we assume $ab \in \mathfrak{P}$ for some $a, b \in R$, then $a \notin \mathfrak{P}$ or $b \in \mathfrak{P}$. Thus if also $b \notin \mathfrak{P}$ then necessarily $a \in \mathfrak{P} \subseteq \sqrt{\mathfrak{P}}$. Thus \mathfrak{P} is primary, by property (d) in (2.72).
- (ii) Let p := √a, then p is an ideal of R, due to (2.17.(ii)). Now assume 1 ∈ p, then there would be some k ∈ N such that 1 = 1^k ∈ a. That is 1 ∈ a and hence a = R in contradiction to a being a primary ideal. Now assume ab ∈ p for some a, b ∈ R. That is there is some k ∈ N such that (ab)^k = a^kb^k ∈ a. If we have b^k ∈ √a = p then b ∈ p, as p is a radical ideal. Thus assume b^k ∉ √a. Then by property (e) we get a^k ∈ a and hence a ∈ p. Thus p is a prime ideal.
- (ii) It remains to prove that $\mathfrak{p} = \sqrt{\mathfrak{a}}$ is the uniquely determined minimal prime ideal containing \mathfrak{a} . Thus assume $\mathfrak{a} \subseteq \mathfrak{q} \trianglelefteq_i R$ is any prime ideal containing \mathfrak{a} . Then we have $\mathfrak{p} = \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}$. Thus if $\mathfrak{q} \subseteq \mathfrak{p}$, then $\mathfrak{p} = \mathfrak{q}$, such that \mathfrak{p} is a minimal prime ideal containing \mathfrak{a} . And if \mathfrak{p}_* is minimal then $\mathfrak{p} \subseteq \mathfrak{p}_*$ again and hence $\mathfrak{p}_* = \mathfrak{p}$, due to minimality. Thus \mathfrak{p} also is uniquely determined.
- (iii) Let $\mathfrak{m} := \sqrt{\mathfrak{a}}$ and assume that \mathfrak{m} is maximal. Now consider any a, $b \in R$ such that $ab \in \mathfrak{a}$ but $b \notin \mathfrak{a}$. Then we have to prove $a \in \mathfrak{m}$ (in order to satisfy property (d) of primary ideals). Thus suppose $a \notin \mathfrak{m}$, then (because of the maximality of \mathfrak{m}) we had $R = \mathfrak{m} + aR$. That is there would be some $h \in R$ such that $1 ah \in \mathfrak{m}$. And by definition

of \mathfrak{m} this is $(1-ah)^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$. Now define

$$f := -\sum_{i=1}^{k} (-1)^i \binom{k}{i} \frac{(ah)^i}{a} \in R$$

Then using the binomial rule we find $1 - af = (1 - ah)^k \in \mathfrak{a}$ by a straughtforward computation. That is $af + \mathfrak{a} = 1 + \mathfrak{a}$ and hence $0 + \mathfrak{a} = (f + \mathfrak{a})(0 + \mathfrak{a}) = (f + \mathfrak{a})(ab + \mathfrak{a}) = (fa + \mathfrak{a})(b + \mathfrak{a}) = (1 + \mathfrak{a})(b + \mathfrak{a}) = b + \mathfrak{a}$. That is $b \in \mathfrak{a}$ in contradiction to the assumption. Thus we have $a \in \mathfrak{m}$, which we had to prove.

- (iv) From the assumption we get $\mathfrak{m} = \sqrt{\mathfrak{m}} = \sqrt{\mathfrak{m}^k} \subseteq \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$ due to (2.17.(vi)) (and as any maximal ideal is prime and hence radical). Thus we have $\sqrt{\mathfrak{a}} = \mathfrak{m}$ and hence \mathfrak{a} is a primary ideal by (iii).
- (v) Denote $\mathfrak{a} := \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_k$, then we first note that according to (2.20.(v))

$$\sqrt{\mathfrak{a}} = \sqrt{igcap_{i=1}^k \mathfrak{a}_i} = igcap_{i=1}^k \sqrt{\mathfrak{a}_i} = igcap_{i=1}^k \mathfrak{p} = \mathfrak{p}$$

Now consider any $a, b \in R$ such that $b \notin \mathfrak{a}$. That is there is some $i \in 1 \dots k$ such that $b \notin \mathfrak{a}_i$. But as $ab \in \mathfrak{a} \subseteq \mathfrak{a}_i$ and \mathfrak{a}_i is primary we find $a \in \sqrt{\mathfrak{a}_i} = \mathfrak{p} = \sqrt{\mathfrak{a}}$. That is \mathfrak{a} satisfies property (d) in (2.72).

- (vi) Consider any $a \in \sqrt{\mathfrak{a}: u}$, that is there is some $k \in \mathbb{N}$ such that $a^k u \in \mathfrak{a}$. As $u \notin \mathfrak{a}$ and \mathfrak{a} is primary, we find $a^k \in \sqrt{\mathfrak{a}}$ and hence $a \in \sqrt{\mathfrak{a}} = \mathfrak{p}$, as $\sqrt{\mathfrak{a}}$ is a radical ideal. That is we have proved $\sqrt{\mathfrak{a}: u} \subseteq \mathfrak{p}$, but as $\mathfrak{a} \subseteq \mathfrak{a}: u$ the converse incluison is clear from $\mathfrak{p} = \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}: u}$. Thus we have $\sqrt{\mathfrak{a}: u} = \mathfrak{p}$. Now consider any $a, b \in R$ such that $ab \in \mathfrak{a}: u$ but $b \notin \mathfrak{a}: u$. This means $abu \in \mathfrak{a}$ but $bu \notin \mathfrak{a}$. As \mathfrak{a} is primary we again find $a \in \sqrt{\mathfrak{a}} = \mathfrak{p} = \sqrt{\mathfrak{a}: u}$ and hence $\mathfrak{a}: u$ is primary, as well.
- (vii) First observe that the radical of \mathfrak{a} is truly given to be \mathfrak{p} , as we compute

$$\begin{split} \sqrt{\mathfrak{a}} &= \left\{ a \in R \mid \exists k \in \mathbb{N} : a^k \in \mathfrak{a} = \varphi^{-1}(\mathfrak{b}) \right\} \\ &= \left\{ a \in R \mid \exists k \in \mathbb{N} : \varphi(a)^k = \varphi(a^k) \in \mathfrak{p} \right\} \\ &= \left\{ a \in R \mid \exists \varphi(a) \in \sqrt{\mathfrak{b}} = \mathfrak{q} \right\} = \varphi^{-1}(\mathfrak{q}) = \mathfrak{p} \end{split}$$

Thus consider $a, b \in R$ such that $ab \in \mathfrak{a}$ but $b \notin \mathfrak{a}$, that is $\varphi(a)\varphi(b) = \varphi(ab) \in \mathfrak{b}$ but $\varphi(b) \notin \mathfrak{b}$. As \mathfrak{b} is primary this yields $\varphi(a) \in \sqrt{\mathfrak{b}} = \mathfrak{q}$ and hence $a \in \varphi^{-1}(\mathfrak{q}) = \sqrt{\mathfrak{a}}$. That is \mathfrak{a} is primary again.

Proof of (2.75):

- (i) Let us denote p := pR, then p is a prime ideal, as p is a prime element. Also we have pⁿ = pⁿR = a and hence √a = √pⁿ = √p = p. That is a is associated to p. We will now prove, that a is primary, by using induction on n. For n = 1 we have a = pR = p, that is a is prime and hence primary by (2.74.(i)). Now consider any n ≥ 2, and a, b ∈ R such that ab ∈ a but b ∉ √a = p. That is there is some h ∈ R such that ab = pⁿb but p ∤ b. As p is prime, p | hpⁿ = ab and p ∤ b we have p | a, that is there is some α ∈ R such that a = αp. As R is an integral domain we get αb = (ab)/p = (pⁿh)/p = pⁿ⁻¹h. Now from ab ∈ pⁿ⁻¹R and b ∉ √pⁿ⁻¹R = p the induction hypothesis yields α ∈ pⁿ⁻¹R and therefore a = αp ∈ pⁿR = a, that is a prime p.
- (ii) If $\mathfrak{a} = 0$ then \mathfrak{a} is prime (as R is an integral domain) and hence primary (by (2.74.(i))). And if $\mathfrak{a} = p^n R$ for some prime element $p \in R$ and $1 \leq n \in \mathbb{N}$, then **a** is primary, as we have seen in (i). Conversely consider any primary ideal $\mathfrak{a} \leq_{i} R$. As R is a PID it is generated by a single element $\mathfrak{a} = aR$. Clearly $a \notin R^*$ (as else $\mathfrak{a} = R$ would not be primary). If a = 0 then $\mathfrak{a} = 0$ and hence there is nothing to prove. Thus assume $a \neq 0$, recall that R is an UFD by (2.64) and assume there would be two non-associate prime elements $p, q \in R$ such that $p \mid a \text{ and } q \mid a$. Then we let $m := \langle a : p \rangle$ and $n := \langle a : q \rangle$ (clearly $1 \leq m, n \in \mathbb{N}$ by (2.53.(iv))) and thereby get $p^m q^m \mid a$. That is there is some $b \in R$ such that $p^m q^n b = a$ and $p \not\mid b$ and $q \not\mid b$. It is clear that $p^m \notin \sqrt{\mathfrak{a}}$ as else there would be some $k \in \mathbb{N}$ such that $q \mid a \mid p^{mk}$. On the other hand we have $q^n b \notin \mathfrak{a}$, as else $p \mid a \mid q^n b$. This contradicts \mathfrak{a} being a primary ideal and hence there is only one prime element $p \in R$ (up to associateness) dividing a. Thus $a = \alpha p^m$ for some $\alpha \in R^*$ and this finally means $\mathfrak{a} = aR = p^n R$.
- (iii) First of all $\mathfrak{m} = \langle s, t \rangle_{\mathbf{i}}$ is a maximal ideal, as R/\mathfrak{m} is a field (in fact we find $R/\mathfrak{m} \cong_{\mathbf{r}} E : f + \mathfrak{m} \mapsto f(0,0)$). Further we have $\mathfrak{a} = \langle s, t^2 \rangle_{\mathbf{i}} \subseteq \langle s, t \rangle_{\mathbf{i}} = \mathfrak{m}$. It is even true that $t \notin \mathfrak{a}$ and hence $\mathfrak{a} \subset \mathfrak{m}$ (suppose $t = fs + gt^2$ for some $f, g \in R$. Then letting t = 0 we would find 0 = fs and hence f = 0. But this yields 1 = gt a contradiction to $t \notin R^*$). Next we have $\mathfrak{m} = \langle s^2, st, t^2 \rangle_{\mathbf{i}} \subseteq \langle s, t^2 \rangle_{\mathbf{i}} = \mathfrak{a}$. And in analogy to the above we find $s \notin \mathfrak{m}^2$, altogether this means

$$\mathfrak{m}^2 \subset \mathfrak{a} \subset \mathfrak{m}$$

As \mathfrak{m} is maximal (2.74.(iv)) yields that \mathfrak{a} is primary and associated to \mathfrak{m} . Now suppose there would be some $k \in \mathbb{N}$ and $\mathfrak{p} \in \operatorname{spec} R$ such that $\mathfrak{a} = \mathfrak{p}^k$. Then from $\mathfrak{m}^2 \subseteq \mathfrak{a} = \mathfrak{p}^k \subseteq \mathfrak{m}$ we would get $\mathfrak{m} = \sqrt{\mathfrak{m}^2} \subseteq \mathfrak{p} = \sqrt{\mathfrak{p}^k} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m}$. That is $\mathfrak{p} = \mathfrak{m}$ and hence $\mathfrak{m}^2 \subset \mathfrak{a} = \mathfrak{m}^k \subset \mathfrak{m}$. If $k \leq 1$ then we have $\mathfrak{m}^k \supseteq \mathfrak{m}$ a contradiction. And if $k \geq 2$ then $\mathfrak{m}^2 \supseteq \mathfrak{m}^k$ a contradiction, too. Thus there is no prime ideal $\mathfrak{p} \leq_i R$ and $k \in \mathbb{N}$ with $\mathfrak{a} = \mathfrak{p}^k$. (iv) First of all it is clear that $\mathfrak{u} = \langle u^2 - st \rangle_i \subseteq \langle t, u \rangle_i$. And as $\langle t, u \rangle_i$ is a prime ideal of E[s, t, u] we find that $\mathfrak{p} = \langle t, u \rangle_i / \mathfrak{u}$ is a prime ideal of R, due to the corresondence theorem (1.43). Now regard

$$\mathfrak{a} = \langle b, c \rangle_{\mathbf{i}}^2 = \langle b^2, bc, c^2 \rangle_{\mathbf{i}} = \langle b^2, bc, ba \rangle_{\mathbf{i}} = (bR) \langle a, b, c \rangle_{\mathbf{i}}$$

Then it is clear that $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{p}^2} = \mathfrak{p}$ and $ab = c^2 \in \mathfrak{a}$. However a (a bit cumbersome) computation yields $b \notin \mathfrak{a}$ and $a \notin \mathfrak{p} = \sqrt{\mathfrak{a}}$. This means that \mathfrak{a} is not primary.

Proof of (2.77):

- (i) Suppose p = a ∩ b for some ideals a, b ≤_i R with a ≠ p and p ≠ b. As p = a ∩ b ⊆ a this means p ⊂ a, that is there is some a ∈ a with a ∉ p. Likewise there is some b ∈ b with b ∉ p. Yet ab ∈ a ∩ b = p, and as p is prime this yields a ∈ p or b ∈ p, a contradiction. Thus there are no such a, b and this means that p is irreducible.
- (ii) Consider $a, b \in R$ such that $ab \in \mathfrak{p}$ but $b \notin \mathfrak{p}$. We will prove $a \in \sqrt{\mathfrak{p}}$ which is property (d) of primary ideals. Thus let $\mathfrak{b} := \mathfrak{p} + bR$. Then we regard the following ascending chain of ideals
 - $\mathfrak{p} \ \subseteq \ \mathfrak{p} : a \ \subseteq \ \mathfrak{p} : a^2 \ \subseteq \ \ldots \ \subseteq \ \mathfrak{p} : a^k \ \subseteq \ \mathfrak{p} : a^{k+1} \ \subseteq \ \ldots$

As R is noetherian this chain has to stabilize. That is there is some $s \in \mathbb{N}$ such that for all $i \in \mathbb{N}$ we get $\mathfrak{p} : a^s = \mathfrak{p} : a^{s+i}$. Now let $\mathfrak{a} := \mathfrak{p} + a^s R$. Then we will prove

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$$

The inclusion " \subseteq " is clear, as $\mathfrak{p} \subseteq \mathfrak{a}$ and $\mathfrak{p} \subseteq \mathfrak{b}$ by construction. Thus consider any $h \in \mathfrak{a} \cap \mathfrak{b}$. As $h \in \mathfrak{b} = \mathfrak{p} + bR$ there are some $q \in \mathfrak{p}$ and $g \in R$ such that h = q + bg. Therefore $ah = aq + abg \in \mathfrak{p}$ as we have $ab \in \mathfrak{p}$. And as $h \in \mathfrak{a} = \mathfrak{p} + a^s R$ as well, there are some $p \in \mathfrak{p}$ and $f \in R$ such that $h = p + a^s f$. Hence $ah = ap + a^{s+1}f$ such that $a^{s+1}f = ah - ap$. Now recall that $ah \in \mathfrak{p}$, then $a^{s+1}f = ah - ap \in \mathfrak{p}$ and this means $f \in \mathfrak{p} : a^{s+1} = \mathfrak{p} : a^s$. Therefore we have $a^s f \in \mathfrak{p}$ and this finally means $h = p + a^s f \in \mathfrak{p}$. Thus we have established $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$. However as $b \notin \mathfrak{p}$ we have $\mathfrak{p} \subset \mathfrak{b}$. And hence the irreducibility of \mathfrak{p} yields $\mathfrak{p} = \mathfrak{a} = \mathfrak{p} + a^s R$. In particular $a^s \in \mathfrak{p}$ and that is $a \in \sqrt{\mathfrak{p}}$ which had to be shown.

(iii) Let us denote the set of all proper ideals that do *not* satisfy the claim (i.e. that are *no* finite intersection of irreducible ideals) by

$$\mathcal{A} := \left\{ \mathfrak{a} \leq_{\mathbf{i}} R \mid \mathfrak{a} \neq R, \not\exists \mathfrak{p}_1, \dots, \mathfrak{p}_k \leq_{\mathbf{i}} R : (1) \text{ and } (2) \right\}$$

We have to prove $\mathcal{A} = \emptyset$, thus assume $\mathcal{A} \neq \emptyset$, as R is a noetherian ring this would mean that \mathcal{A} contains a maximal element $\mathfrak{a}^* \in \mathcal{A}^*$. As $\mathfrak{a}^* \in \mathcal{A}$ we in particular have that \mathfrak{a}^* is not irreducible (else \mathfrak{a}^* would be its own irreducible decomposition). And as also $\mathfrak{a}^* \neq R$ this means that there are ideals $\mathfrak{a}, \mathfrak{b} \leq_i R$ such that $\mathfrak{a}^* = \mathfrak{a} \cap \mathfrak{b}$ and $\mathfrak{a}^* \subset \mathfrak{a}$ and $\mathfrak{a}^* \subset \mathfrak{b}$. By maximality of \mathfrak{a}^* this means $\mathfrak{a}, \mathfrak{b} \notin \mathcal{A}$ and hence there are irreducible decompositions $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$ of \mathfrak{a} and $(\mathfrak{q}_1, \ldots, \mathfrak{q}_l)$ of \mathfrak{b} . Hence

$$\mathfrak{a}^* \ = \ \mathfrak{a} \cap \mathfrak{b} \ = \ \left(igcap_{i=1}^k \mathfrak{p}_i
ight) \cap \left(igcap_{j=1}^l \mathfrak{q}_i
ight)$$

This means that \mathfrak{a}^* admits $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k, \mathfrak{q}_1, \ldots, \mathfrak{q}_l)$ as an irreducible decomposition and hence $\mathfrak{a}^* \notin \mathcal{A}$, a contradiction. Thus we have $\mathcal{A} = \emptyset$, that is *every* proper ideal of R admits an irreducible decomposition.

Proof of (2.80):

By assumption (2) we have $\mathfrak{a} = \bigcap_j \mathfrak{a}_j$ for $J := 1 \dots k$. And hence we may choose a subset I of minimal cardinality with this property. Now it is clear that \approx is an equivalency relation on I, as it belongs to the function

$$p : I \to \operatorname{spec} R : i \mapsto \sqrt{\mathfrak{a}_i}$$

Hence $A = I/\approx$ is a well defined partition of I (the equivalency classes $\alpha \in A$ are just the fibers of p). And for any $\alpha = [i] \in A$ we may define $\mathfrak{p}_{\alpha} := \sqrt{\mathfrak{a}_i}$. That is for any $\alpha \in A$ the set $\{\mathfrak{a}_i \mid i \in \alpha\}$ is a finite collection of primary ideals associated to \mathfrak{p}_{α} . Hence by (2.74.(v)) \mathfrak{a}_{α} is a primary ideal associated to \mathfrak{p}_{α} as well. In particular (\mathfrak{a}_{α}) (where $\alpha \in A$) satisfies property (1) of primary decompositions. Further we have

$$\bigcap_{\alpha \in A} \mathfrak{a}_{\alpha} = \bigcap_{\alpha \in A} \bigcap_{i \in \alpha} \mathfrak{a}_i = \bigcap_{i \in I} \mathfrak{a}_i = \mathfrak{a}$$

as the α partition I and construction of I. Thus also property (2) of primary decompositions is satisfied. And property (4) is clear from the construction of A precisely by this relation. It remains to verify property (3). That is fix any $\beta = [j] \in A$ and assume $\mathfrak{a} = \bigcap_{\alpha \neq \beta} \mathfrak{a}_{\alpha}$. As $j \in \beta$ we in particular find

$$\mathfrak{a} = \bigcap_{i \in I} \mathfrak{a}_i \subseteq \bigcap_{j \neq i \in I} \mathfrak{a}_i \subseteq \bigcap_{\beta \neq \alpha \in A} \mathfrak{a}_\alpha = \mathfrak{a}$$

But this would mean $\mathfrak{a} = \bigcap_{i \neq j} \mathfrak{a}_i$ in contradiction to the minimality of I. Altogether we have proved properties (1) to (4), that is (\mathfrak{a}_{α}) (where $\alpha \in A$) is a minimal primary decomposition of \mathfrak{a} .

Proof of (2.81):

- (i) By definition $\#ass(\mathfrak{a}_1, \ldots, \mathfrak{a}_k) = \#\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} \leq k$. And if we suppose $\mathfrak{p}_i = \mathfrak{p}_j$ then by minimality of $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ we have i = j (this is property (4)). Hence we even find $\#\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} = k$ as claimed.
- (ii) As $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$ and using (2.17.(vi)) and (2.20.(v)) we can easily compute

$$\sqrt{\mathfrak{a}:u} = \sqrt{\left(\bigcap_{i=1}^{k} \mathfrak{a}_{i}\right):u} = \sqrt{\bigcap_{i=1}^{k} (\mathfrak{a}_{i}:u)} = \bigcap_{i=1}^{k} \sqrt{\mathfrak{a}_{i}:u}$$

If $u \in \mathfrak{a}_i$ then we have $\mathfrak{a}_i : u = R$ according to (2.17.(iv)). And if $u \notin \mathfrak{a}_i$ then $\mathfrak{a}_i : u$ is primary again with $\sqrt{\mathfrak{a}_i : u} = \sqrt{\mathfrak{a}_i} = \mathfrak{p}_i$ by virtue of (2.74.(vi)). Thus we have obtained

$$\sqrt{\mathfrak{a}: u} = \bigcap_{i=1}^{k} \begin{cases} R & \text{if } u \in \mathfrak{a}_i \\ \mathfrak{p}_i & \text{if } u \notin \mathfrak{a}_i \end{cases}$$

Thus we may ignore any $i \in 1...k$ with $u \in \mathfrak{a}_i$, as they do not contribute to the intersection. What remains is precisely the claim

$$\sqrt{\mathfrak{a}:u} = \bigcap_{u \not\in \mathfrak{a}_i} \mathfrak{p}_i$$

(iv) If $\mathfrak{p} \in \operatorname{ass}(\mathfrak{a})$ then by definition of $\operatorname{ass}(\mathfrak{a})$ there is some $u \in R$ such that $\mathfrak{p} = \sqrt{\mathfrak{a} : u}$. Thus by (ii) we have the identity

$$\mathfrak{p} \;=\; igcap_{u
ot\in\mathfrak{a}_i}\mathfrak{p}_i$$

And hence by (2.11.(ii)) there is some $i \in 1 \dots k$ satisfying $(u \notin \mathfrak{a}_i)$ and) $\mathfrak{p}_i \subseteq \mathfrak{p}$. And as $\mathfrak{p} \subseteq \mathfrak{p}_i$ is clear this is $\mathfrak{p} = \mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$. Conversely choose any $j \in 1 \dots k$. As $(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$ is minimal we have $\mathfrak{a} \subset \bigcap_{i \neq j} \mathfrak{a}_i$ and hence there is some $u_i \in \mathfrak{a}_i$ for any $i \neq j$ but $u_j \notin \mathfrak{u}_j$. Thus for this u_j by (ii) we get

$$\bigcap_{u_j \not\in \mathfrak{a}_i} \mathfrak{p}_i = \mathfrak{p}_j = \sqrt{\mathfrak{a} : u_j} \in \operatorname{ass}(\mathfrak{a})$$

(iii) Without loss of generality we consider $\mathfrak{p}_1 \in \operatorname{ass}(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)_*$. That is for any $i \in 2 \ldots k$ we have $\mathfrak{p}_i \not\subseteq \mathfrak{p}_1$. And this again means that there is some $a \in \mathfrak{p}_i$ with $a \notin \mathfrak{p}_1$. Now let $U := R \setminus \mathfrak{p}_1$, in particular $a \in U$. Then because of $a \in \mathfrak{p}_i = \sqrt{\mathfrak{a}_i}$ there is some $n \in \mathbb{N}$ such that $a^n \in \mathfrak{a}_i$. And as $a^n \in U$, too, we get $1/1 = (a^n)/(a^n) \in U^{-1}\mathfrak{a}_i$. Hence we get $U^{-1}\mathfrak{a}_i = U^{-1}R$ and this again means

$$R = (U^{-1}\mathfrak{a}_i) \cap R = \mathfrak{a}_i : U$$

for any $i \in 2...k$. This now can be used to prove $\mathfrak{a} : U = \mathfrak{a}_1$ by virtue of the following computation (see (2.104) - for convenience we even gave an elementary proof of $(\mathfrak{a} \cap \mathfrak{b}) : U = (\mathfrak{a} : U) \cap (\mathfrak{b} : U)$ there)

$$\mathfrak{a}: U = \left(\bigcap_{i=1}^{k} \mathfrak{a}_{i}\right): U = \bigcap_{i=1}^{k} (\mathfrak{a}_{i}: U) = \mathfrak{a}_{1}: U = \mathfrak{a}_{1}$$

Hereby $\mathfrak{a}_1 : U = \mathfrak{a}_1$ holds true because \mathfrak{a}_1 is primary and $U = R \setminus \mathfrak{p}_1$. To be precise consider $a \in \mathfrak{a}_i : U$, that is there is some $u \in U$ such that $au \in \mathfrak{a}_i$. But by definition of U we have $u \notin \mathfrak{p}_1 = \sqrt{\mathfrak{a}_1}$, and as \mathfrak{a}_1 is primary this yields $a \in \mathfrak{a}_1$. Thus we have $\mathfrak{a}_1 : U \subseteq \mathfrak{a}_1$ and the converse inclusion is trivial.

(v) If $\mathfrak{p} \in \operatorname{ass}(\mathfrak{a})_*$ then by virtue of (iv) we have $\mathfrak{p} = \mathfrak{p}_i$ for some $i \in 1 \dots k$. And as \mathfrak{p}_i is minimal (iii) implies $\mathfrak{a} : (R \setminus \mathfrak{p}) = \mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$. Conversely consider any $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$. Then by definition $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)_*$ and by (iii) this means $\mathfrak{a}_i = \mathfrak{a} : (R \setminus \mathfrak{p})$. And by (iv) we also have $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})_*$ and thereby $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a})$.

Proof of (2.83):

- By (2.77.(iii)) there are some irreducible ideals p₁,..., p_k ≤_i R such that a = p₁ ∩ ··· ∩ p_k. And by (2.77.(ii)) these irreducible ideals already are primary. Thus (p₁,..., p_k) is a primary decomposition of a. And by (2.80) we find that a then already has a minimal primary decomposition.
- (2) Now assume that (\$\mathbf{a}_1, \ldots, \$\mathbf{a}_k\$) and (\$\mathbf{b}_1, \ldots, \$\mathbf{b}_l\$) are minimal primary decompositions of \$\mathbf{a}\$. Then by (2.81.(iii)) we get the identity

$$\operatorname{ass}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) = \operatorname{ass}(\mathfrak{a}) = \operatorname{ass}(\mathfrak{b}_1,\ldots,\mathfrak{b}_l)$$

(Note that by definition $ass(\mathfrak{a})$ and $iso(\mathfrak{a})$ only depend on \mathfrak{a} , not on the decomposition). And by (2.81.(i)) this in particular implies k = l. The third identity we finally get from (2.81.(iv))

$$\operatorname{iso}(\mathfrak{a}_1,\ldots,\mathfrak{a}_k) = \operatorname{iso}(\mathfrak{a}) = \operatorname{iso}(\mathfrak{b}_1,\ldots,\mathfrak{b}_l)$$

(3) Let us denote the minimal prime ideals over \mathfrak{a} by \mathfrak{p}_i , that is we let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} := \{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\}_*$ (note that there are only finitely many \mathfrak{p}_i , due to (2.35.(iii))). Then by (2.20.(i)) we have

$$\mathfrak{a} = \sqrt{\mathfrak{a}} = \bigcap \left\{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \right\}_* = \bigcap_{i=1}^k \mathfrak{p}_i$$

And as the \mathfrak{p}_i are prime they in particular are primary according to (2.77.(i)). That is $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$ is a primary decomposition of \mathfrak{a} . And as $\sqrt{\mathfrak{p}_i} = \mathfrak{p}_i \neq \mathfrak{p}_j = \sqrt{\mathfrak{p}_j}$ (for $i \neq j$) it even satisfies property (4) of minimal primary decompositions. Now assume that for some index $j \in 1 \ldots k$ we had the equality

$$igcap_{i
eq j}\mathfrak{p}_i = \mathfrak{a} \subseteq \mathfrak{p}_j$$

Then by (2.11.(ii)) there would be some $i \neq j$ such that $\mathfrak{a} \subseteq \mathfrak{p}_i \subseteq \mathfrak{p}_j$. And by minimality of \mathfrak{p}_j this would mean $\mathfrak{p}_i = \mathfrak{p}_j$, a contradiction. Thus $(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$ also satisfies property (3), that is it *is* a minimal primary decomposition of \mathfrak{a} . In fact this even is $\operatorname{ass}(\mathfrak{p}_1, \ldots, \mathfrak{p}_k) =$ $\operatorname{iso}(\mathfrak{p}_1, \ldots, \mathfrak{p}_k)$, that is every associated ideal is an isolated component. Now assume that $(\mathfrak{a}_1, \ldots, \mathfrak{a}_l)$ is any minimal primary decomposition of \mathfrak{a} , then by (2) we have l = k and

$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} = \operatorname{ass}(\mathfrak{p}_1, \dots, \mathfrak{p}_k)$$
$$= \operatorname{iso}(\mathfrak{p}_1, \dots, \mathfrak{p}_k)$$
$$= \operatorname{iso}(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$$

That is for any $i \in 1...k$ we have $\mathbf{a}_i \in \mathrm{iso}(\mathbf{a}_1, \ldots, \mathbf{a}_k) = {\{\mathbf{p}_1, \ldots, \mathbf{p}_k\}}$ and this again means that for any $i \in 1...k$ there is some $\sigma(i) \in 1...k$ such that $\mathbf{a}_i = \mathbf{p}_{\sigma(i)}$. Clearly σ is injective, because if we assume $\sigma(i) = \sigma(j)$ then $\mathbf{a}_i = \mathbf{p}_{\sigma(i)} = \mathbf{p}_{\sigma(j)} = \mathbf{a}_j$ in contradiction to the minimality of $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$. But as k is finite this already means that σ is bijective, that is $\sigma \in S_k$. Altogether $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ is just a rearranged version of $(\mathbf{p}_1, \ldots, \mathbf{p}_k)$.

Proof of (2.85):

(i) Let (a₁,..., a_k) be a minimal primary decomposition of a (which exists, due to (2.83)) and p_i := √a_i. Then we have seen in (2.81.(iv)) that ass(a) = {p₁,..., p_k}. Thus from ∩_i a_i = a ⊆ q we get a_i ⊆ q for some i ∈ 1...k, according to (2.11.(ii)). Therefore p_i = √a_i ⊆ √q = q and p_i ∈ ass(a). Now let p_i ⊆ q for some p_i ∈ ass(a). Then we may

choose some minimal $\mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})_*$ with $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ (as $\operatorname{ass}(\mathfrak{a})$ is finite). And hence we get $\mathfrak{a}_i \subseteq \mathfrak{p}_i \subseteq \mathfrak{p}_j \subseteq \mathfrak{q}$, that is $\mathfrak{a}_i \subseteq \mathfrak{q}$. Finally consider $\mathfrak{a}_i \subseteq \mathfrak{q}$ then $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{q}$ is clear.

- (ii) We stick to the notation used for (i) that is $(\mathfrak{a}_1, \ldots, \mathfrak{a}_k)$ is a minimal primary decomposition and $\mathfrak{p}_i := \sqrt{\mathfrak{a}_i}$. " \subseteq " if $\mathfrak{a} \subseteq \mathfrak{q}$ then by (i) there exists some $\mathfrak{a}_i \in \operatorname{iso}(\mathfrak{a})$ such that $\mathfrak{a}_i \subseteq \mathfrak{q}$. Then $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{p}_i = \sqrt{\mathfrak{a}_i} \subseteq \sqrt{\mathfrak{q}} = \mathfrak{q}$. By minimality of \mathfrak{q} this yields $\mathfrak{q} = \mathfrak{p}_i \in \operatorname{ass}(\mathfrak{a})_*$. " \supseteq " conversely, if $\mathfrak{p}_i \in \operatorname{ass}_*$ then $\mathfrak{a} \subseteq \mathfrak{a}_i \subseteq \mathfrak{p}_i$. Thus if we consider any prime ideal $\mathfrak{p} \leq_i R$ such that $\mathfrak{a} \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$, then by (i) there is some $\mathfrak{p}_j \in \operatorname{ass}(\mathfrak{a})$ such that $\mathfrak{p}_j \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$. By minimality of \mathfrak{p}_i in ass(\mathfrak{a}) this means $\mathfrak{p}_j = \mathfrak{p}_i$ and hence $\mathfrak{p} = \mathfrak{p}_i$. Hence \mathfrak{p}_i is a minimal prime ideal containing \mathfrak{a} .
- (iii) This follows immediately from (ii) and (2.20.(i)): by the propositions cited, we have $\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{q} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{q}\} = \bigcap \operatorname{ass}(\mathfrak{a})_*$. And it is clear that $\bigcap \operatorname{ass}(\mathfrak{a}) \subseteq \bigcap \operatorname{ass}(\mathfrak{a})_*$, as $\operatorname{ass}(\mathfrak{a})_* \subseteq \operatorname{ass}(\mathfrak{a})$. But on the other hand, if $\mathfrak{l} \in \operatorname{ass}(\mathfrak{a})$ there some $\mathfrak{l}_* \in \operatorname{ass}(\mathfrak{a})_*$ such that $\mathfrak{l}_* \subseteq \mathfrak{l}$ (as $\operatorname{ass}(\mathfrak{a})$ is finite). Thus we also have $\bigcap \operatorname{ass}(\mathfrak{a})_* \subseteq \bigcap \operatorname{ass}(\mathfrak{a})$.

Proof of (2.86):

We will first prove the ζ truly is a homomorphism of rings. By definition we have $\zeta(0) = 0_R$ and $\zeta(1) = 1_R$. If now $k \in \mathbb{N}$ then $\zeta(-k) = k(-1_R) = -(k1_R) = -\zeta(k)$ by general distributivity. Hence we have $\zeta(-k) = -\zeta(k)$ for any $k \in \mathbb{Z}$ (because if k < 0 then $-k \in \mathbb{N}$ and hence $-\zeta(k) = -\zeta(-k) = -\zeta(-k) = -\zeta(-k) = -\zeta(-k)$). This will be used to prove the additivity of ζ . First of all it is clear that for $i, j \in \mathbb{N}$ we get

$$\zeta(i+j) = (i+j)1_R = (i1_R) + (j1_R) = \zeta(i) + \zeta(j)$$

And likewise $\zeta((-i) + (-j)) = \zeta(-(i+j)) = -\zeta(i+j) = -(\zeta(i) + \zeta(j)) = -\zeta(i) + -\zeta(j) = \zeta(-i) + \zeta(-j)$. Now assume $i \ge j$ then by general associativity it is clear that $\zeta(i+(-j)) = \zeta(i-j) = (i-j)\mathbf{1}_R = (i\mathbf{1}_R) - (j\mathbf{1}_R) = \zeta(i) - \zeta(j) = \zeta(i) + \zeta(-j)$. And if $i \le j$ then $\zeta(i+(-j)) = \zeta(-(j-i)) = -\zeta(j-i) = -\zeta(j) + \zeta(-i) = \zeta(-j) + -\zeta(-i) = \zeta(i) + \zeta(-j)$. Thus in any case we have $\zeta(i+(-j)) = \zeta(i) + \zeta(-j)$ and likewise we see $\zeta((-i)+j) = \zeta(-i) + \zeta(j)$. Thus we have finally arrived at $\zeta(i+j) = \zeta(i) + \zeta(j)$ for any $i, j \in \mathbb{Z}$. For the multiplicativity things are considerably simpler: let $i, j \in \mathbb{N}$ again, then by the general rule of distributivity we get $\zeta(ij) = (ij)\mathbf{1}_R = (i\mathbf{1}_R)(j\mathbf{1}_R) = \zeta(i)\zeta(j)$. And as also $\zeta(-k) = -\zeta(k)$ this clearly yields $\zeta(ij) = \zeta(i)\zeta(j)$ for any $i, j \in \mathbb{Z}$. Thus ζ is a homomorphism of rings. And if $\varphi : \mathbb{Z} \to R$ is any homomorphism, then $\varphi(1) = \mathbf{1}_R$. By induction on $k \in \mathbb{N}$ we see $\varphi(k) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1) = \mathbf{1}_R + \dots + \mathbf{1}_R = k\mathbf{1}_R = \zeta(k)$.

And of course $\varphi(-k) = -\varphi(k) = -\zeta(k) = \zeta(-k)$ such that $\varphi = \zeta$. This also is the uniqueness of ζ .

Thus $\operatorname{im}(\zeta)$ is a subring of R by virtue of (1.51.(v)). Let us denote the intersection of all subrings of R by P - note that this is a subring again, due to (1.30). From the construction of P it is clear, that $P \subseteq \operatorname{im}(\zeta) \leq_{\mathrm{r}} R$. But as $1_R \in P$ we have and hence $\zeta(k) = k 1_R \in P$ for any $k \in \mathbb{N}$. Likewise $-1_R \in P$ and hence $\zeta(-k) = k(-1_R) \in P$. This is the converse inclusion $\operatorname{im}(\zeta) \subseteq P$ and hence $\operatorname{im}(\zeta) = P$.

Now kn $(\zeta) \leq_i \mathbb{Z}$ is an ideal in \mathbb{Z} due to (1.51.(v)) again. But as (\mathbb{Z}, α) is an Euclidean domain \mathbb{Z} is a PID due to (2.64.(iii)). Hence there is some $n \in \mathbb{Z}$ such that kn $(\zeta) = n\mathbb{Z}$. Thereby n is determined up to associateness. And as $\mathbb{Z}^* = \{1, -1\}$ this is n is uniquely determined up to sign $\pm n$. Thus by fixing $n \geq 0$ it is uniquely determined. Now

$$\begin{aligned} \operatorname{kn}\left(\zeta\right) &= \left\{k \in \mathbb{Z} \mid \zeta(k) = 0_R\right\} \\ &= \left\{\pm k \mid k \in \mathbb{N}, \ \zeta(k) = 0_R\right\} \\ &= \left\{\pm k \mid k \in \mathbb{N}, \ k 1_R = 0_R\right\} \end{aligned}$$

Thus if n = 0 then kn $(\zeta) = 0$ and hence $k1_R = 0_R$ implies $k \in \text{kn}(\zeta) = 0$ which is k = 0. And if $n \neq 0$ then kn $(\zeta) \neq 0$. And hence we have seen in (2.64.(iii)) that $\alpha(n) = |n| = n$ is minimal in kn (ζ) . And due to the explict realisation of the kernel above this is $n = \min\{1 \le k \in \mathbb{N} \mid k1_R = 0\}$.

Proof of (2.88):

(i) As R is an integral domain, so are its subrings $P \leq_{\rm r} R$. In particular $\operatorname{im}(\zeta) \leq_{\rm r} R$ is an integral domain. But by definition and (1.56.(ii)) we've got the isomorphy (where $n := \operatorname{CHAR} R$)

$$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}/_{\operatorname{kn}(\zeta)} \cong_{\mathrm{r}} \operatorname{im}(\zeta) = \operatorname{prr} R \leq_{\mathrm{r}} R$$

Hence $\mathbb{Z}/n\mathbb{Z}$ is an integral domain, too and by (2.9) this implies that $n\mathbb{Z} = \mathbb{Z}$ or $n\mathbb{Z}$ is a prime ideal in \mathbb{Z} . If we had $n\mathbb{Z} = \mathbb{Z}$, then n = 1, which would mean $1_R = 0_R$ in contradiction to $R \neq 0$. This only leaves, that $n\mathbb{Z}$ is a prime ideal. But this again means that n = 0 or that n is prime because of (2.47.(ii)).

(ii) Suppose n := CHAR R = 0 and $k_R = 0_R$, then $k \in \text{kn}(\zeta) = n\mathbb{Z} = 0$ which is k = 0. Conversely suppose $n \in n\mathbb{Z} = \text{kn}(\zeta)$, that is $n_R = \zeta(n) = 0_R$ and by assumption this implies n = 0. We now prove the second equivalency. That is we assume n = 0 and want to show $\zeta : \mathbb{Z} \cong_{\mathrm{r}} \text{PRR } R$. But as in (i) we find the following isomorphies

$$\mathbb{Z} \cong_{\mathbf{r}} \mathbb{Z}/_{0\mathbb{Z}} = \mathbb{Z}/_{\mathrm{kn}(\zeta)} \cong_{\mathbf{r}} \mathrm{im}(\zeta) = \mathrm{PRR}R$$

where $k \mapsto k + 0\mathbb{Z} = k + \operatorname{kn}(\zeta) \mapsto \zeta(k)$ - which precisely is ζ again. Conversely suppose $\Phi : \mathbb{Z} \cong_{\mathrm{r}} \operatorname{PRR} R$ for some isomorphism Φ . If we had $n \neq 0$, then $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ would be finite. But as we have the isomorphy $\mathbb{Z} \cong_{\mathrm{r}} \operatorname{PRR} R \cong_{\mathrm{r}} \mathbb{Z}_n$ once more this cannot be (as we thereby find the contradiction $\infty = \#\mathbb{Z} = \#\mathbb{Z}_n = n < \infty$).

(iii) If $n := \text{CHAR } R \neq 0$, then we have already proved the minimality of n, that is $n = \min\{1 \leq k \in \mathbb{N} \mid k_R = 0_R\}$ in (2.86). Conversely supposes n is this minimum and denote c := CHAR R. As $c_R = 0_R$ and n is minimal with this property we have $n \leq c$. On the other hand we have $\zeta(n) = n_R = 0_R$ and hence $n \in \operatorname{kn}(\zeta) = c\mathbb{Z}$. That is $c \mid n$ and hence $c \leq n$, altogether $n = c = \operatorname{CHAR } R$. And $n \neq 0$ is trivial (as n is contained in a subset of $\{k \mid 1 \leq k \in \mathbb{N}\}$). The second equivalency results from the following isomorphy again (refer to (1.56.(ii)))

$$\mathbb{Z}_{n} = \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}/_{\operatorname{kn}(\zeta)} \cong_{\mathrm{r}} \operatorname{im}(\zeta) = \operatorname{prr} R$$

where $k + n\mathbb{Z} = k + \operatorname{kn}(\zeta) \mapsto \zeta(k)$. Thus if CHAR $R = n \neq 0$ we are done already. Conversely suppose there was some isomorphism Φ such that $\Phi : \mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRR}\mathbb{Z}$. Then we had (where $c := \operatorname{CHAR} R$ again)

$$\mathbb{Z}_{c} = \mathbb{Z}/_{\operatorname{kn}(\zeta)} \cong_{\mathrm{r}} \operatorname{im}(\zeta) = \operatorname{prr} R \cong_{\mathrm{r}} \mathbb{Z}_{n}$$

In particular we find $c = \#\mathbb{Z}_c = \#\mathbb{Z}_n = n$ (as $n \neq 0$ and hence $c \neq 0$). That is we have found n = c = CHAR R and $n \neq 0$ has been assumed.

- (iv) If $n := \operatorname{CHAR} R = 0$, then by (ii) we have $\zeta : \mathbb{Z} \cong_{\mathrm{r}} \operatorname{PRR} R$. And as $\operatorname{PRF} R$ is the quotient field of $\operatorname{PRR} R$ this implies $\mathbb{Q} \cong_{\mathrm{r}} \operatorname{PRF} R$ under the isomorphy $a/b \mapsto \zeta(a)\zeta(b)^{-1}$. Likewise if $n := \operatorname{CHAR} R \neq 0$ then by (iii) we have $\mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRR} R$. As R is a field it is a non-zero integral domain. Thus by (i) n is prime. Hence $n\mathbb{Z}$ is a non-zero prime ideal and hence maximal (due to $(2.64.(\mathrm{i})))$, such that \mathbb{Z}_n is a field. As $\operatorname{PRF} R$ is the quotient field of (the field) $\operatorname{PRR} R$ this implies $\mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRR} R = \operatorname{PRF} R$. Conversely if $\mathbb{Q} \cong_{\mathrm{r}} \operatorname{PRF} R$, then $\operatorname{CHAR} R = 0$ as else $\mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRF} R \cong_{\mathrm{r}} \mathbb{Q}$ (where $n = \operatorname{CHAR} R \neq 0$) by what we have just proved. And if $\Phi : \mathbb{Z}_n \cong_{\mathrm{r}} \operatorname{PRF} R$ for some isomorphism Φ , then we have $n_R = n1_R = n\Phi(1 + n\mathbb{Z}) = \Phi(n + n\mathbb{Z}) = \Phi(0 + n\mathbb{Z}) = 0_R$. Thus if $c := \operatorname{CHAR} R$, then $n \in \operatorname{kn}(\zeta) = c\mathbb{Z}$ and hence $c \mid n$. On the other hand we have $0_R = c_R = c1_R = c\Phi(1 + n\mathbb{Z}) = \Phi(c + n\mathbb{Z})$. From the injectivity of Φ we get $c + n\mathbb{Z} = 0 + n\mathbb{Z}$ and hence $n \mid c$. As both n and c are positive this only leaves n = c.
- (v) First suppose we had $c := \operatorname{CHAR} R = 0$, then $\zeta : \mathbb{Z} \hookrightarrow R$ would be injective (as kn (ζ) = $c\mathbb{Z} = 0$), which contradicts R being finite. Thus we have $c \neq 0$, now let $P := \operatorname{PRR} R$, then by (iii) we have $P \cong_{\mathrm{r}} \mathbb{Z}_c$ and

hence $\#P = \#\mathbb{Z}_c = c$. But - being a subring - $P \leq_{g} R$ is a subgroup (under the addition + on R). Thus by the theorem of Lagrange (1.6) we have $c = \#P \mid \#R$.

Proof of (2.89):

(i) Consider a unit $a \in R^*$ of R and suppose ab = 0, then $b = a^{-1}0 = 0$ and hence a is no zero-divisor of R. Conversely suppose that $a \notin ZDR$ is a non-zero-divisor of R. Then the mapping

$$R \hookrightarrow R : b \mapsto ab$$

is injective (as ab = ac implies a(b-c) = 0 and as $a \notin \mathbb{ZD} R$ this yields b-c = 0 such that b = c). But as R is finite any injective map on R also is surjective (and vice versa). Hence there is some $b \in R$ such that ab = 1. But this means that $a \in R^*$ is a unit of R.

(ii) If f = pa then we easily have $(f + p^n S)(p^{n-1} + p^n S) = p^n a + p^n S = 0 + p^n S$. And as S is an integral domain we have $p^n \not\mid p^{n-1}$ or in other words $p^{n-1} + p^n S \neq 0 + p^n S$. And hence $f + p^n S$ is a zerodivisor of $S/p^n S$. Conversely suppose $(f + p^n S)(g + p^n S) = 0 + p^n S$ for some $g + p^n S \neq 0 + p^n S$. This means $p^n \not\mid g$ and hence we obtain a well-defined $l \in 1 \dots n-1$ by letting

$$l := g[p] := \max\{k \in \mathbb{N} \mid p^k \mid g\}$$

If we now write $g = p^l b$ then by assumption we have $p^n \mid fg = fp^l b$ and hence $p \mid p^{n-l} \mid fb$. As p is prime we get $p \mid f$ or $p \mid b$. But as l has been chosen maximally $p \mid b$ is absurd, which only leaves $p \mid f$.

(iii) As $R \neq 0$ (because of $p^n S \subseteq pS \neq S$) we have already seen the inclusions NIL $R \subseteq \text{ZD } R \subseteq R \setminus R^*$ in (1.26.(ii)). And by (ii) we already know $\text{ZD } R = (p + p^n S)R$. And if $pa + p^n S \in \text{ZD } R$ then

$$(pa + p^n S)^n = p^n a^n + p^n S = 0 + p^n S$$

which also proves $\text{ZD} R \subseteq \text{NIL}(R)$. Thus it only remains to prove the inclusion $R \setminus R^* \subseteq (p + p^n S)R$. Thus consider $x = f + p^n S \notin R^*$, in particular we have $f \notin S^*$ (as else $x^{-1} = f^{-1} + p^n S$). Thus f has a true (i.e. $r \geq 1$) prime factorisation

$$f = \alpha q$$
 where $q := \prod_{i=1}^{\prime} q_i$

with $\alpha \in S^*$ and $q_i \in S$ prime. Now suppose that p is not associated to any of the q_i (formally that is $\neg(p \approx q_i)$ for any $i \in 1 \dots r$) then we had $gcd(p^n, q) = 1$. The lemma of Bezout (2.67.(iii)) then implies

$$p^n S + qS = \gcd(p^n, q)S = S$$

Therefore there are a and $b \in S$ such that $ap^n + bq = 1$ or in other words $bq = 1 - ap^n$. Now let $g := ap^n + \alpha^{-1}b$, then it is clear that

$$fg = \alpha q(ap^n + \alpha^{-1}b) = (\alpha aq - a)p^n + 1$$

And hence $(f + p^n S)(g + p^n S) = 1 + p^n S$ which implies $x^{-1} = g + p^n S$ and in particular $x \in R^*$, a contradiction. Hence there has to be some $i \in 1 \dots r$ such that $p \approx q_i$. And therefore we find $p \approx q_i \mid f$ such that $p \mid f$, or in other words again $f \in (p + p^n S)R$. Thus we got

NIL
$$R = \operatorname{ZD} R = R \setminus R^* = (p + p^n S) R$$

Now consider any prime ideal $\mathfrak{p} \leq_{\mathbf{i}} R$, then it is clear that NIL $R \subseteq \mathfrak{p} \subseteq R \setminus R^*$. But by the equality NIL $R = R \setminus R^*$ this means $\mathfrak{p} = \text{NIL } R$. Therefore NIL R is the one and only prime ideal of R. But NIL R already is maximal - if NIL $R \subset \mathfrak{q} \leq_{\mathbf{i}} R$, then there is some $\alpha \in \mathfrak{q} \cap R^*$ and hence $\mathfrak{q} = R$. Thus we have also proved the second equality

$$\operatorname{spec} R = \operatorname{smax} R = \{\operatorname{NIL} R\}$$

(iv) We will poove the claim in several steps: (1) given any commutative ring R and any ideal $\mathfrak{a} \leq_i R$ let us first denote the following set

$$X_n(R, \mathfrak{a}) := \{ \mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}, \ \#R/\mathfrak{p} \le n \}$$

Then it is clear that $\mathfrak{a} \subseteq \mathfrak{b} \implies X_n(R, \mathfrak{b}) \subseteq X_n(R, \mathfrak{a})$ (because if we are given $\mathfrak{p} \in X_n(R, \mathfrak{b})$, then $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{p}$ and hence $\mathfrak{a} \subseteq \mathfrak{p}$, such that $\mathfrak{p} \in X_n(R, \mathfrak{a})$). Further $X_n(R, \mathfrak{a}\mathfrak{b}) \subseteq X_n(R, \mathfrak{a}) \cup X_n(R, \mathfrak{b})$ (because if we are given $\mathfrak{p} \in X_n(R, \mathfrak{a}\mathfrak{b})$ then $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ and as \mathfrak{p} is prime this implies $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ such that $\mathfrak{p} \in X_n(R, \mathfrak{a})$ or $\mathfrak{p} \in X_n(R, \mathfrak{b})$). Now suppose $\mathfrak{a} \subseteq \mathfrak{b} \leq \mathfrak{a}_i R$, then we will prove

$$#X_n(R,\mathfrak{b}) = #X_n\left(\frac{R}{\mathfrak{a}}, \frac{\mathfrak{b}}{\mathfrak{a}}\right)$$

This is clear once we prove that $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ is a bijection from $X_n(R, \mathfrak{h})$ to $X_n(R/\mathfrak{a}, \mathfrak{h}/\mathfrak{a})$. But by the correspondence theorem (1.43) (and the remarks following it) $\overline{\mathfrak{p}} \leq_{\mathbf{i}} R/\mathfrak{a}$ is prime if and only if $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{a}$ for some $\mathfrak{p} \leq_{\mathbf{i}} R$ prime, with $\mathfrak{a} \subseteq \mathfrak{p}$. And due to the correspondence theorem we also have $\mathfrak{h} \subseteq \mathfrak{p}$ if and only if $\mathfrak{h}/\mathfrak{a} \subseteq \mathfrak{p}/\mathfrak{a}$. Finally we've got the third isomorphism theorem (1.56.(iv)) which provides the isomorphy $R/\mathfrak{p} \cong_{\mathrm{r}} (R/\mathfrak{a})/(\mathfrak{p}/\mathfrak{a})$. In particular we have $\#R/\mathfrak{p} = \#(R/\mathfrak{a})/(\mathfrak{p}/\mathfrak{a})$. Thus $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ is well-defined and surjective. But the injectivity is clear (by the correspondence theorem) and hence it is bijective. In a second step (2) let us now denote the set

$$\mathcal{A} := \{ \mathfrak{a} \leq_{\mathrm{i}} R \mid \#X_n(R, \mathfrak{a}) = \infty \}$$

Suppose $\mathcal{A} \neq \emptyset$ was non-empty, then (as R is noetherian) there would be a maximal element $\mathfrak{a}^* \in \mathcal{A}^*$. We now claim that this maximal element \mathfrak{a}^* is prime. It is clear, that $\mathfrak{a}^* \neq R$, as R/R = 0 has not a single prime ideal, in particular $\#X_n(R, R) = 0$. Thus suppose there would be some $a, b \in R$ such that $ab \in \mathfrak{a}^*$ but $a, b \notin \mathfrak{a}^*$. Then we let $\mathfrak{a} := \mathfrak{a}^* + aR$ and $\mathfrak{b} := \mathfrak{a}^* + bR$ and thereby get $\mathfrak{a}^* \subset \mathfrak{a}$, \mathfrak{b} and $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}^*$. Thus by the inclusions in (1) we would find

$$X_n(R, \mathfrak{a}^*) \subseteq X_n(R, \mathfrak{a}\mathfrak{b}) \subseteq X_n(R, \mathfrak{a}) \cup X_n(R, \mathfrak{b})$$

But as \mathfrak{a}^* is maximal in \mathcal{A} we have $\mathfrak{a}, \mathfrak{b} \notin \mathcal{A}$. That is both $X_n(R, \mathfrak{a})$ and $X_n(R, \mathfrak{b})$ are finite. Thus by the above inclusion $X_n(R, \mathfrak{a}^*)$ is finite, too, in contradiction to $\mathfrak{a}^* \in \mathcal{A}$ - thus \mathfrak{a}^* is prime. For the third step (3) let $Q := R/\mathfrak{a}^*$, then by (2) Q is an integral domain. And if $0 \neq \mathfrak{u} \leq_i Q$ is a non-zero ideal, then by the correspondence theorem there is some ideal $\mathfrak{b} \leq_i R$ with $\mathfrak{a}^* \subset \mathfrak{b}$ such that $\mathfrak{u} = \mathfrak{b}/\mathfrak{a}^*$. But as \mathfrak{a}^* has been maximal the equality in (1) yields

$$\#X_n(Q,\mathfrak{u}) = X_n\left(\frac{R}{\mathfrak{a}^*}, \mathfrak{b}/\mathfrak{a}^*\right) = \#X_n(R,\mathfrak{b}) < \infty$$

(4) the same reasonin yields $\#X_n(Q,0) = \#X_n(R,\mathfrak{a}^*) = \infty$, such that Q is infinite (if it was finite, that so was its spectrum and hence the subset $X_n(Q,0)$ was finite as well). Thus we may choose pairwise distince elements $f_1, \ldots, f_{n+1} \in Q$ and let

$$f := \prod_{i \neq j} (f_i - f_j) \in Q$$

as $f_i - f_j \neq 0$ for any $i \neq j$ and Q is an integral domain we have $f \neq 0$ as well. Now consider any prime ideal $\mathfrak{q} \leq_i Q$, if we have $f \notin \mathfrak{q}$ then (as \mathfrak{q} is an ideal) for any $i \neq j \in 1 \dots n+1$ we have $f_i - f_j \notin \mathfrak{q}$. Thus for any $i \neq j \in 1 \dots n+1$ we have $f_i + \mathfrak{q} \neq f_j + \mathfrak{q}$. That is Q/\mathfrak{q} contains (at least) n + 1 distinct elements and hence $\mathfrak{q} \notin X_n(Q, 0)$. Thus for any $\mathfrak{q} \in X_n(Q, 0)$ we necessarily have $f \in \mathfrak{q}$ and hence

$$X_n(Q,0) = X_n(Q,fQ)$$

But as $f \neq 0$ we have $fQ \neq 0$ such that (3) yields $\#X_n(Q, fQ) < \infty$. By the equalities above this means $\infty = \#X_n(R, \mathfrak{a}^*) = \#X_n(Q, 0) = X_n(Q, fQ) < \infty$ a contradiction. This means that our assumption $\mathcal{A} \neq \emptyset$ has to be false. In other words $\mathcal{A} = \emptyset$ and in particular $0 \notin \mathcal{A}$. That is $\#X_n(R, 0) < \infty$ which is a trivial reformulation of the claim.

Proof of (2.91):

The implications (a) \implies (b) and (a) \implies (c) are trivial. Thus it only remains to check the converse implications. The proof of (c) \implies (a) is elementary and hes been given in (2.89.(i)). Yet (b) \implies (a) requires knowledge of group actions (which will be presented in book 2, or any other standard text on algebra) and cyclotomic fields (which also will be presented in book 2, or any standard text on Galois theory). Never the less we want to give a proof of (b) \implies (a) and the reader is asked to refer to the sources given for the statements not contained in this text:

Let us regard the multiplicative group $F^* = F \setminus \{0\}$ (this truly is a group, as F is a skew-field) of F. And let us denote the *center* of the ring F by

$$C := \{ a \in F \mid \forall x \in F : ax = xa \}$$

It is obvious that $C \leq_{\mathbf{r}} F$ is a commutative subring of F and hence it even is a field. Thus (F, +) is a C-vectorspace under its own multiplication. And as F is finite it clearly has to be finite-dimensional $n := \dim_C F < \infty$. If we denote q := #C then this implies

$$\#F^* = \#F - 1 = \#C^n - 1 = q^n - 1$$

For any $x \in E^*$ let us now denote the *conjugacy class*, the *centralizer* and the centralizer appended by 0, using the notations

$$con(x) := \{ yxy^{-1} \mid y \in E^* \} cen(x) := \{ y \in E^* \mid xy = yx \} C(x) := \{ y \in E \mid xy = yx \}$$

It is well-known from group theory that the conjugacy classes $\operatorname{con}(x)$ form a partition of F^* and that $\operatorname{con}(a) = \{a\}$ for any $a \in C$. Thus let us denote by $X \subseteq F \setminus C$ a representing system of the conjugacy classes, that is $X \longleftrightarrow \{\operatorname{con}(x) \mid x \in F \setminus C\}$ under $x \mapsto \operatorname{con}(x)$. As the conjugacy classes form a partition of F^* we find the equality

$$q^{n} - 1 = \#F^{*} = \sum_{0 \neq a \in C} \#con(a) + \sum_{x \in X} \#con(x)$$
$$= \#C^{*} + \sum_{x \in X} \#con(x)$$
$$= (q - 1) + \sum_{x \in X} \#con(x)$$

It is clear that (C(x), +) is a subgroup of the additive group (F, +). But it even is a C-subspace of F, we denote its (finite) dimension by $n(x) := \dim_C C(x)$, then we get

$$\# \operatorname{cen}(x) = \# C(x) - 1 = \# C^{n(x)} - 1 = q^{n(x)} - 1$$

We now apply the orbit formula $\#F^* = \#con(x) \cdot \#cen(x)$. Yet as #con(x) is an iteger we find the divisibility $\#cen(x) \mid \#F^*$. Using division with remainder we obtain

$$q^{n} - 1: q^{n(x)} - 1 = q^{n-n(x)} + q^{n-2n(x)} + \dots + q^{n-r(x)n(x)}$$

As this division leaves no remainder we necessarily find n = r(x)n(x), i.e. n(x) divides n. On the other hand the orbit formula yields

$$\#con(x) = \frac{q^n - 1}{q^{n(x)} - 1}$$

Substituting this into our partition formula for the cardinality of F^* we find

$$q^{n} - 1 = (q - 1) + \sum_{x \in X} \frac{q^{n} - 1}{q^{n(x)} - 1}$$

This is the point where the cyclotomic polynomials $\Phi_m \in \mathbb{Z}[t]$ come into play. Let $m \in \mathbb{N}$ and $\omega_m := \exp(2\pi i/m) \in \mathbb{C}$, further denote $k \perp m :\iff k \in 1...m$ and $\gcd(k, m) = \pm 1$. Then the *m*-th cyclotomic polynomial is defined to be

$$\Phi_m := \prod_{k \perp m} (t - \omega_m^k)$$

In book 2 it will be shown that $\Phi_m \in \mathbb{Z}[t]$ has integer coefficients in fact and (if we denote $d \mid m :\iff d \in 1 \dots m$ and $d \mid m$) satisfies

$$\prod_{d \mid m} \Phi_d = t^m - 1$$

We now assume $F \neq C$ (i.e. F is not commutative) and regard any $x \in X$. It is clear that we find $\Phi_n(q) \mid q^n - 1$. But as $x \notin C$ we get $\# \operatorname{con}(x) \neq 1$ and hence $n \neq n(x)$ on the other hand we have seen $n(x) \mid n$ and hence

$$(t^{n(x)} - 1)\Phi_n = \left(\prod_{d \mid n(x)} \Phi_d\right)\Phi_n \mid \prod_{d \mid n} \Phi_d = t^n - 1$$

Thus we get $\Phi_n(q) \mid (q^n - 1)/(q^{n(x)} - 1)$, too and substituting this and $\Phi_n(q) \mid q^n - 1$ into the equation of the partition we obtain

$$\Phi_n(q) \mid (q^n - 1) - \sum_{x \in X} \frac{q^n - 1}{q^{n(x)} - 1} = q - 1$$

In particular we get $\Phi_n(q) \leq q-1$. But this clearly cannot be - as $q \geq 2$ (at least 0 and $1 \in C$) we see by the triange inequality that $|q-1| < |q-w_n^k|$ for any $k \in 1 \dots n-1$. Hence we arrived at a contradiction (to $C \neq F$)

$$q-1 \geq |\Phi_n(q)| = \prod_{k \perp n} |q - \omega_n^k| > \prod_{k \perp n} |q-1| \geq q-1$$

Proof of (2.93):

- (i) R^* and NZD R are multiplicatively closed, due to (1.26). And if conversely $uv \in R^*$, then there is some $a \in R$ such that 1 = a(uv) = u(av). Hence we also have $u \in R^*$. Likewise, if $uv \in NZD R$ and $a \in R$ then au = 0 implies auv = 0 and hence a = 0 such that $u \in NZD R$.
- (iii) $1 = 1 \cdot 1 \in UV$ is clear and if $u, u' \in U$ and $v, v' \in V$, then for any uv and $u'v' \in UV$ we get $(uv)(u'v') = (uu')(vv') \in UV$ again.
- (iv) Immediate: if a and $b \in \mathfrak{a}$ then $(1+a)(1+b) = 1 + (a+b+ab) \in 1 + \mathfrak{a}$.
- (v) Clearly $1 \in \varphi(U)$, as $1 \in U$ and $\varphi(1) = 1$. And if $p, q \in \varphi(U)$ then there are $u, v \in U$ such that $p = \varphi(u)$ and $q = \varphi(v)$. Hence $pq = \varphi(u)\varphi(v) = \varphi(uv) \in \varphi(U)$ since $uv \in U$. Likewise $1 \in \varphi^{-1}(V)$ is clear, as $\varphi(1) = 1 \in V$. And if $u, v \in \varphi^{-1}(V)$ then $\varphi(u), \varphi(v) \in V$. thereby we get $uv \in \varphi^{-1}(V)$ from $\varphi(uv) = \varphi(u)\varphi(v) \in V$. So let us finally suppose V is saturated and $uv \in \varphi^{-1}(V)$. Then $\varphi(uv) = \varphi(u)\varphi(v) \in V$ implies $\varphi(u) \in V$ and hence $u \in \varphi^{-1}(V)$, as well.
- (vi) As $\mathcal{U} \neq \emptyset$ there is some $1 \in U \in \mathcal{U}$ and hence $1 \in \bigcup \mathcal{U}$. And if now $uv \in \bigcup \mathcal{U}$ then there are some $U, V \in \mathcal{U}$ such that $u \in U$ and $v \in V$. As \mathcal{U} is a chain we may assume $U \subseteq V$ and hence $u \in V$. This yields $uv \in V$ and hence $uv \in \bigcup \mathcal{U}$.
- (vii) Since $1 \in U$ for any $U \in \mathcal{U}$ we also have $1 \in \bigcap \mathcal{U}$. And if $u, v \in \bigcap \mathcal{U}$, then $u, v \in U$ for any $U \in \mathcal{U}$. Thereby $uv \in U$, as U is multiplicatively closed and hence $uv \in \bigcap \mathcal{U}$. Likewise if any $U \in \mathcal{U}$ is saturated, then $uv \in \bigcap \mathcal{U}$ implies $uv \in U$ and hence $u \in U$ for any $U \in \mathcal{U}$. And the latter translates into $u \in \bigcap \mathcal{U}$ again.
- (viii) Clearly $1 = u^0 \in U$ and if u^i and $u^j \in U$ then also $u^i u^j = u^{i+j} \in U$. That is U is a multiplicatively closed set with $u \in U$. And if conversely $V \subseteq R$ is any multiplicatively closed set with $u \in V$, then by induction on k we also find $u^k \in V$ and hence $U \subseteq V$. Together this proves, that U is the smallest multiplicatively closed set containing u.

(ix) Let us define \overline{U} to be the set given, then we need to show that \overline{U} is the intersection of all saturated multiplicatively closed subsets $V \subseteq R$ containing U. " \subseteq ": Thus consider any saturated multiplicatively closed $V \subseteq R$ with $U \subseteq V$. If now $a \in \overline{U}$ then there are $b \in R$ and $u, v \in U$ such that $uab = uv \in U \subseteq V$. In particular a(ub) = $uab \in V$ and as V is saturated this implies $a \in V$. Hence $\overline{U} \subseteq V$ is contained in any such V. " \supseteq ": If $a \in U$ that 1a1 = 1a and hence $a \in \overline{U}$. Hence we have $U \subseteq \overline{U}$ so it remains to prove that \overline{U} is saturated multiplicatively closed. Thus consider a and $a' \in \overline{U}$, that is uab = uv and u'a'b' = u'v' for sufficient $b, b' \in R$ and $u, v, u', v' \in U$. Then (uu')aa'(bb') = (uu')(vv') and hence $aa' \in \overline{U}$, as $uu', vv' \in U$. Conversely suppose $aa' \in \overline{U}$, that is u(aa')b = uv for sufficient $b \in R$, $u, v \in U$. Then ua(a'b) = u(aa')b = uv and hence $a \in \overline{U}$.

Proof of (2.94):

We first prove (b) \implies (a): consider any prime ideal $\mathfrak{p} \leq_{i} R$, then $1 \in R \setminus \mathfrak{p}$, as $1 \in \mathfrak{p}$ would imply $\mathfrak{p} = R$ which is disallowed. And as \mathfrak{p} is both, *prime* and an *ideal* we get the following equivalence for all $u, v \in R$

$$uv \in \mathfrak{p} \iff u \in \mathfrak{p} \text{ or } v \in \mathfrak{p}$$

Hence if we go to complements (i.e. if we negate this equivelency) then we find that $R \setminus \mathfrak{p}$ is a saturated multiplicative set, since

$$uv \in R \setminus \mathfrak{p} \iff u \in R \setminus \mathfrak{p} \text{ or } v \in R \setminus \mathfrak{p}$$

And from this we find that $R \setminus \bigcup \mathcal{P}$ is a saturated multiplicative set, as it is the intersection of such sets $R \setminus \mathfrak{p}$ for $\mathfrak{p} \in \mathcal{P}$, formally

$$R \setminus \bigcup \mathcal{P} = R \setminus \bigcup_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathcal{P}} R \setminus \mathfrak{p}$$

Next we prove (a) \implies (a): fix $a \in R \setminus U$ then also $aR \subseteq R \setminus U$: consider $b \in R$, then $ab \in U$ - because of the saturation of U - would imply $a \in U$, in contradiction to $a \notin U$. And as U is multiplicatively closed we max choose an ideal $\mathfrak{p}(a)$ maximal among the ideals \mathfrak{b} with $aR \subseteq \mathfrak{b} \subseteq R \setminus U$. And this $\mathfrak{p}(a)$ is prime (for all this refer to (2.14.(iv))). Thus we get

$$R \setminus U \subseteq \bigcup_{a \notin U} aR \subseteq \bigcup_{a \notin U} \mathfrak{p}(a) \subseteq R \setminus U$$
$$\implies U = R \setminus \bigcup \{ \mathfrak{p}(a) \mid a \notin U \}$$

Proof of (2.95):

- We will first prove that ~ is an equivalence relation: the reflexivity is due to 1 ∈ U, as u1a = u1a implies (u, a) ~ (u, a). For the symmetry suppose (u, a) ~ (v, b), i.e. there is some w ∈ U such that vwa = uwb. As = is symmetric we get uwb = vwa and this is (v, b) ~ (u, a) again. To finally prove the transitivity we regard (u, a) ~ (v, b) and (v, b) ~ (w, c). That is there are p, q ∈ U such that pva = pub and qwb = qvc. Since p, q and v ∈ U we also have pqv ∈ U. Now compute (pqv)wa = qw(pva) = qw(pub) = pu(qwb) = pu(qvc) = (pqv)uc, this yields that truly (u, a) ~ (w, c) are equivalent, too.
- Next we need to check that the operations + and \cdot are well-defined. Suppose a/u = a'/u' and b/v = b'/v' that is there are p and $q \in U$ such that pu'a = pua' and qv'b = qvb. Then we let $w := pq \in U$ and compute

$$u'v'w(av + bu) = vv'q(pu'a) + uu'p(qv'b)$$

$$= vv'q(pua') + uu'p(qvb')$$

$$= uvw(a'v' + u'b')$$

$$u'v'wab = (pu'a)(qv'b)$$

$$= (pua')(qvb')$$

$$= uvwa'b'$$

That is (a/u) + (b/v) = (av + bu)/uv = (a'v' + b'u')/u'v' = (a'/u') + (b'/v') and (a/u)(b/v) = ab/uv = a'b'/u'v' = (a'/u')(b'/v') respectively. And this is just the well-definedness of sum and product.

- Next it would be due to verify that $U^{-1}R$ thereby becomes a commutative ring. That is we have to check that + and \cdot are associative, commutative and satisfy the distributivity law. Further that for any $a/u \in U^{-1}R$ we have a/u + 0/1 = a/u and a/u + (-a)/u = 0/1 and finally that $a/u \cdot 1/1 = a/u$. But this can all be done in straightforward computations, that we wish to omit here.
- It is obvious that thereby κ becomes a homomorphism of rings, $\kappa(0) = 0/1$ is the zero-element and $\kappa(1) = 1/1$ is the unit element. Further $\kappa(a+b) = (a+b)/1 = (a1+b1)/1 \cdot 1 = a/1 + b/1 = \kappa(a) + \kappa(b)$ and $\kappa(ab) = ab/1 = ab/1 \cdot 1 = (a/1)(b/1) = \kappa(a)\kappa(b)$.
- Next we wish to prove that κ is injective, if and only if $U \subseteq \text{NZD } R$. To do this we take a look at the kernel of κ

By (1.53.(i)) κ is injective iff kn (κ) = {0}. That is iff for any $u \in U$ we get $au = 0 \implies a = 0$. And this is just a reformulation of $U \subseteq \text{NZD } R$. • So it remains to prove that κ is bijective if and only if $U \subseteq R^*$. First suppose $U \subseteq R^* \subseteq \text{NZD } R$ by (1.26). Then as we have just seen κ is injective. Now consider any $a/u \in U^{-1}R$, then

$$\frac{a}{u} = \frac{au^{-1}u}{u} = \frac{au^{-1}}{1} = \kappa(au^{-1}) \in \text{ im }(\kappa)$$

Hence we found that κ also is surjective. Conversely suppose that κ is bijective. In particular κ is injective and hence $U \subseteq \text{NZD } R$. But κ also is surjective, that is for any $u \in U$ there is some $b \in R$ such that $1/u = \kappa(b) = b/1$. That is there is some $w \in U$ such that w = uwb. Equivalently w(ub-1) = 0, but as $w \in \text{NZD } R$ this implies ub = 1 and hence $u \in R^*$. As u has been arbitrary we found $U \subseteq R^*$.

Proof of (2.98):

Two of the three implications are clear, thus we are only concerned with: if for any maximal ideal $\mathfrak{m} \leq R$ we have $a/1 = b/1 \in R_{\mathfrak{m}}$ then already $a = b \in R$. But since a/1 = b/1 is equivalent to (a - b)/1 = 0/1 it suffices

$$\forall \mathfrak{m} : \frac{a}{1} = \frac{0}{1} \in R_{\mathfrak{m}} \implies a = 0$$

By definition a/1 = 0/1 means that there is some $u \notin \mathfrak{m}$ such that ua = 0. And the latter can again be formulated as $u \in ANN(a)$. Thus we have

$$\forall \mathfrak{m} : \operatorname{ANN}(a) \nsubseteq \mathfrak{m}$$

Hence there is no maximal ideal \mathfrak{m} containing ANN (a). But as the annulator ANN (a) is an ideal this is only possible if ANN (a) = R and hence $a = 1 \cdot a = 0$.

In the second claim it is clear that for any prime ideal $\mathfrak{P} \leq_{\mathbf{i}} R$ we get $R \subseteq R_{\mathfrak{p}} \subseteq F := \text{QUOT } R$. Hence it is clear that $R \subseteq \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$. And as $\operatorname{smax} R \subseteq \operatorname{spec} R$ it also is clear that $\bigcap_{\mathfrak{p}} R_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ such that we only have to verify $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} \subseteq R$. Thus consider any $a/b \in F$ with $a/b \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. That is for any maximal ideal $\mathfrak{m} \leq_{\mathbf{i}} R$ ther are some $a(\mathfrak{m}) \in R$ and $b(\mathfrak{m}) \notin \mathfrak{m}$ auch that $a/b = a(\mathfrak{m})/b(\mathfrak{m})$. Now define the ideal

$$\mathfrak{b} := \langle b(\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{smax} R \rangle_{\mathbf{i}} \quad \trianglelefteq_{\mathbf{i}} \quad R$$

Suppose we had $\mathfrak{b} \neq R$, then there would be some maximal ideal \mathfrak{m} such that $\mathfrak{m} \subseteq \mathfrak{m}$. But clearly $b(\mathfrak{m}) \in \mathfrak{b}$ although $b(\mathfrak{m}) \notin \mathfrak{m}$, a contradiction. That is $\mathfrak{b} = R$ and hence $1 \in \mathfrak{b}$. That is there is a finite subset $M \subseteq \operatorname{smax} R$ and there are $r(\mathfrak{m}) \in R$ (where $\mathfrak{m} \in M$) such that $1 = \sum_{\mathfrak{m}} r(\mathfrak{m})b(\mathfrak{m})$. Now recall that $a/b = a(\mathfrak{m})/b(\mathfrak{m})$, then we find $a/b \in R$ by virtue of

$$\frac{a}{b} = 1 \cdot \frac{a}{b} = \left(\sum_{\mathfrak{m} \in M} r(\mathfrak{m}) b(\mathfrak{m})\right) \frac{a}{b} = \sum_{\mathfrak{m} \in M} r(\mathfrak{m}) a(\mathfrak{m}) \in R$$

Proof of (2.99):

In the first part we will prove the existance of the induced homomorphism $\overline{\varphi}$. And of course we start with the well-definedness of $\overline{\varphi}$ as a mapping. Thus let us regard $a/u = b/v \in U^{-1}R$. That is there is some $w \in U$ such that vwa = uwb. And thereby we get $\varphi(a)\varphi(u)^{-1} = \varphi(b)\varphi(v)^{-1}$ from

$$\varphi(v)\varphi(w)\varphi(a) \;=\; \varphi(vwa) \;=\; \varphi(uwb) \;=\; \varphi(u)\varphi(w)\varphi(b)$$

Next we have to check that $\overline{\varphi}$ truly is a homomorphism of rings. To do this consider any a/u and $b/v \in U^{-1}R$ and compute

$$\begin{aligned} \overline{\varphi} \left(\frac{a}{u} \cdot \frac{b}{v} \right) &= \overline{\varphi} \left(\frac{ab}{uv} \right) &= \varphi(a)\varphi(b)\varphi(u)^{-1}\varphi(v)^{-1} \\ &= \left(\varphi(a)\varphi(u)^{-1} \right) \left(\varphi(b)\varphi(v)^{-1} \right) &= \overline{\varphi} \left(\frac{a}{u} \right) \cdot \overline{\varphi} \left(\frac{b}{v} \right) \\ \overline{\varphi} \left(\frac{a}{u} + \frac{b}{v} \right) &= \overline{\varphi} \left(\frac{av + bu}{uv} \right) &= \left(\varphi(a)\varphi(v) + \varphi(b)\varphi(u) \right) \varphi(u)^{-1}\varphi(v)^{-1} \\ &= \varphi(a)\varphi(u)^{-1} + \varphi(b)\varphi(v)^{-1} &= \overline{\varphi} \left(\frac{a}{u} \right) + \overline{\varphi} \left(\frac{b}{v} \right) \end{aligned}$$

So we have proved the existence of the homomorphism $\overline{\varphi}$. It remains to verify that this is the unique homomorphism such that $\overline{\varphi}\kappa = \varphi$. That is we consider some homomorphism $\psi : U^{-1}R \to S$ such that for any $a \in R$ we get $\psi(a/1) = \varphi(a)$. Then for any $u \in U \subseteq R$ we get

$$\psi\left(\frac{1}{u}\right) = \psi\left(\left(\frac{u}{1}\right)^{-1}\right) = \psi\left(\frac{u}{1}\right)^{-1} = \varphi(u)^{-1}$$

And thereby we find for any $a/u \in U^{-1}R$ that $\psi(a/u) = \psi(a/1 \cdot 1/u) = \psi(a/1)\psi(1/u) = \varphi(a)\varphi(u)^{-1} = \overline{\varphi}$. That is $\psi = \overline{\varphi}$, that is $\overline{\varphi}$ is unique.

Proof of (2.101):

- By definition $\kappa^{-1}(\mathfrak{u})$ is the set of all $a \in R$ such that $a/1 = \kappa(a) \in \mathfrak{u}$, and this has already been the first claim. And $\kappa^{-1}(\mathfrak{a})$ is an ideal of R by virtue of (1.51.(vii)).
- " \supseteq " If $a \in \mathfrak{a}$ then $a/1 = \kappa(a) \in \kappa(\mathfrak{a}) \subseteq U^{-1}\mathfrak{a}$. And for any $u \in U$ we hence also get $a/u = (1/u)(a/1) \in U^{-1}\mathfrak{a}$. " \subseteq " Conversely consider any $x \in \langle \kappa(\mathfrak{a}) \rangle_{i}$. I.e. there are $a_i \in \mathfrak{a}$ and $x_i = b_i/v_i \in U^{-1}R$ such that

$$x = \sum_{i=1}^{n} x_i \kappa(a_i) = \sum_{i=1}^{n} \frac{a_i b_i}{v_i}$$

We now let $v := v_1 \dots v_n \in U$ and $\hat{v}_i := v/v_i \in U$ then a straightforward computation shows x = a/v for some $a := \sum_i a_i b_i \hat{v}_i \in \mathfrak{a}$

$$x = \sum_{i=1}^{n} \frac{a_i b_i}{v_i} = \sum_{i=1}^{n} \frac{a_i b_i \widehat{v}_i}{v} = \frac{a}{v}$$

Proof of (2.103):

- First of all $\mathfrak{a} : U$ is an ideal $0 \in \mathfrak{a} : U$ since $0 = 1 \cdot 0 \in \mathfrak{a}$. Now consider $a, b \in \mathfrak{a} : U$. That is there are some $u, v \in V$ such that ua and $vb \in \mathfrak{a}$. This yields $uv(a + b) = v(ua) + u(vb) \in \mathfrak{a}$ and hence $a + b \in \mathfrak{a} : U$. Likewise for any $r \in R$ we get $u(ra) = r(ua) \in \mathfrak{a}$ and hence $ra \in \mathfrak{a} : U$.
- Next it is clear that $\mathfrak{a} \subseteq \mathfrak{a} : U$, because if $a \in \mathfrak{a}$ then $a = 1 \cdot a \in \mathfrak{a}$ (due to $1 \in U$) and hence $a \in \mathfrak{a} : U$.
- We finally wish to prove $(U^{-1}\mathfrak{a}) \cap R = \mathfrak{a} : U$. Consider any $b \in \mathfrak{a} : U$, that is $vb \in \mathfrak{a}$ for some $v \in U$. Then $b/1 = vb/v \in U^{-1}\mathfrak{a}$ and hence $b \in (U^{-1}\mathfrak{a}) \cap R$. Conversely let $b \in (U^{-1}\mathfrak{a}) \cap R$, by definition this means $b/1 \in U^{-1}\mathfrak{a}$. That is there is some $a \in \mathfrak{a}$, $u \in U$ such that b/1 = a/u. That is there is some $v \in U$ such that $uvb = va \in \mathfrak{a}$. And as $uv \in U$ this means $b \in \mathfrak{a} : U$.

Proof of (2.104):

- U⁻¹(**a** ∩ **b**) = (U⁻¹**a**) ∩ (U⁻¹**b**): if x ∈ U⁻¹(**a** ∩ **b**) then by definition there are some a ∈ **a** ∩ **b** and u ∈ U such that x = a/u. But as a ∈ **a** and a ∈ **b** this already means x ∈ U⁻¹**a** and x ∈ U⁻¹**b**. If conversely x = a/u ∈ U⁻¹**a** and x = b/v ∈ U⁻¹**b** then a/u = b/v means that there is some w ∈ U such that vwa = uwb ∈ **a** ∩ **b**. Hence x = (vwa)/(uvw) = (uwb)/(uvw) ∈ U⁻¹(**a** ∩ **b**).
- $U^{-1}(\mathfrak{a} + \mathfrak{b}) = (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$: if $x \in U^{-1}(\mathfrak{a} + \mathfrak{b})$ then there are some $a \in \mathfrak{a}, b \in \mathfrak{b}$ and $u \in U$ such that $x = (a + b)/u = (a/u) + (b/u) \in (U^{-1}\mathfrak{a}) + (U^{-1}\mathfrak{b})$. And if we are conversely given any $a/u \in U^{-1}\mathfrak{a}$ and $b/v \in U^{-1}\mathfrak{b}$ then $a/u + b/v = (au + bv)/(uv) \in U^{-1}(\mathfrak{a} + \mathfrak{b})$.
- $U^{-1}(\mathfrak{a}\mathfrak{b}) = (U^{-1}\mathfrak{a})(U^{-1}\mathfrak{b})$: if $x \in U^{-1}(\mathfrak{a}\mathfrak{b})$ then there are some $f \in \mathfrak{a}\mathfrak{b}$ and $u \in U$ such that x = f/u. Again f is of the form $f = \sum_i a_i b_i$ for some $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. Altogether we get

$$x = \frac{f}{u} = \sum_{i=1}^{n} \frac{a_i b_i}{u} = \sum_{i=1}^{n} \frac{a_i}{1} \frac{b_i}{u} \in (U^{-1}\mathfrak{a}) (U^{-1}\mathfrak{b})$$

Conversely consider $a_i/u_i \in U^{-1}\mathfrak{a}$ and $b_i/v_i \in U^{-1}\mathfrak{b}$. As always we let $u := u_1 \dots u_n$ and $\widehat{u}_i := u/u_i \in U$ again, likewise $v := v_1 \dots v_n$ and $\widehat{v}_i := v/v_i \in U$. Then $a_i/u_i = (a_i\widehat{u}_i)/u$, $b_i/v_i = (b_i\widehat{v}_i)/v$ and

$$\sum_{i=1}^{n} \frac{a_i}{u_i} \frac{b_i}{v_i} = \sum_{i=1}^{n} \frac{a_i \widehat{u}_i}{u} \frac{b_i \widehat{v}_i}{v} = \frac{1}{uv} \sum_{i=1}^{n} \widehat{u}_i a_i \widehat{v}_i a_i b_i \in U^{-1}(\mathfrak{ab})$$

- $U^{-1}\sqrt{\mathfrak{a}} = \sqrt{U^{-1}\mathfrak{a}}$: if $x \in U^{-1}\sqrt{\mathfrak{a}}$ then x = b/v for some $b \in \sqrt{\mathfrak{a}}$ and $v \in U$. That is there is some $k \in \mathbb{N}$ such that $b^k \in \mathfrak{a}$. And therefore $x^k = b^k/v^k \in U^{-1}\mathfrak{a}$. Hence x is contained in the radical of $U^{-1}\mathfrak{a}$. Conversely consider any x = b/v such that there is some $k \in \mathbb{N}$ with $x^k = b^k/v^k \in U^{-1}\mathfrak{a}$. Then there is some $a \in \mathfrak{a}$ and $u \in U$ such that $b^k/v^k = a/u$. That is $uwb^k = v^kwa \in \mathfrak{a}$ for some $w \in U$. Hence $(uwb)^k = (uw)^{k-1}(uwb^k) \in \mathfrak{a}$, that is $uwb \in \sqrt{\mathfrak{a}}$. And this agian yields $x = b/v = (uwb)/(uvw) \in U^{-1}\sqrt{\mathfrak{a}}$.
- Next we prove $(\mathfrak{a}: U): U = \mathfrak{a}: U$. Clearly, as $1 \in U$ we have $\mathfrak{a}: U \subseteq (\mathfrak{a}: U): U$ (as for any $a \in \mathfrak{a}: U$ we have $a = a \cdot 1 \in (\mathfrak{a}: U): U$). Conversely if $a \in (\mathfrak{a}: U): U$ then there is some $u \in U$ such that $au \in \mathfrak{a}: U$. Again this means that there is some $v \in U$ such that $a(uv) = (au)v \in \mathfrak{a}$. But as $uv \in U$ this again yields $a \in \mathfrak{a}: U$.
- For (𝔅 ∩𝔅): U = (𝔅: U) ∩ (𝔅: U) we use a straightforward reasoning again: If a ∈ (𝔅 ∩𝔅): U then there is some u ∈ U such that au ∈ 𝔅 ∩𝔅. And this again means a ∈ 𝔅: U and a ∈ 𝔅: U. Conversely consider a ∈ (𝔅: U) ∩ (𝔅: U). That is there are v, w ∈ U such that av ∈ 𝔅 and aw ∈ 𝔅. Now let u := vw ∈ U then au = (av)w = (aw)v ∈ 𝔅 ∩𝔅 such that a ∈ (𝔅 ∩𝔅): U.
- We turn our attention to √a: U = √a : U. If a : U = R then we get √a: U = √R = R. And as a ⊆ √a we also have R = a : U ⊆ √a : U ⊆ R. And hence we get √a: U = R = √a : U. Thus assume a: U ≠ R. If x ∈ √a: U then by definition there is some k ∈ N such that x^k ∈ a : U. And this means x^ku ∈ a for some u ∈ U. Clearly we have k ≥ 1 as else u ∈ a such that a : U = R. And thereby we get (xu)^k = (x^ku)u^{k-1} ∈ a, too. But this means xu ∈ √a and hence x ∈ √a : U. Conversely if x ∈ √a : U then there is some u ∈ U such that xu ∈ √a. Thus there is some k ∈ N such that x^ku^k = (xu)^k ∈ a. But as u^k ∈ U this yields x^k ∈ a : U and hence x ∈ √a : U.
- $(\mathfrak{u} \cap \mathfrak{W}) \cap R = \kappa^{-1}(\mathfrak{u} \cap \mathfrak{W}) = \kappa^{-1}(\mathfrak{u}) \cap \kappa^{-1}(\mathfrak{W}) = (\mathfrak{u} \cap R) \cap (\mathfrak{W} \cap R) = \mathfrak{a} \cap \mathfrak{b}.$
- $(\mathfrak{u} + \mathfrak{w}) \cap R = (\mathfrak{a} + \mathfrak{b}) : U$: if $c \in (\mathfrak{a} + \mathfrak{b}) : U$ then there are some $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ and $u \in U$ such that uc = a + b. That is $(uc)/1 = (a+b)/1 = (a/1) + (b/1) \in \mathfrak{u} + \mathfrak{w}$. And thereby also $c/1 = (1/u)((uc)/1) \in \mathfrak{u} + \mathfrak{w}$.

But this finally is $c \in (\mathfrak{u} + \mathfrak{w}) \cap R$. Conversely let $c \in (\mathfrak{u} + \mathfrak{w}) \cap R$, that is $c/1 \in \mathfrak{u} + \mathfrak{w}$. Thereby we find $a/u \in \mathfrak{u}$ and $b/v \in \mathfrak{w}$ such that c/1 = a/u + b/v = (va + ub)/uv. Hence there is some $w \in U$ such that $uvwc = vwa + uwb \in \mathfrak{a} + \mathfrak{b}$ (as $a/u \in \mathfrak{u}$ implies $a/1 = (u/1)(a/u) \in \mathfrak{u}$ and hence $a \in \mathfrak{a}$, likewise $b \in \mathfrak{b}$). And as $uvw \in U$ this is $c \in (\mathfrak{a} + \mathfrak{b}) : U$.

• $(\mathfrak{u}\,\mathfrak{w})\cap R = (\mathfrak{a}\,\mathfrak{b}) : U$: if $c \in (\mathfrak{a}\,\mathfrak{b}) : U$ then there are some $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ and $u \in U$ such that $uc = \sum_i a_i b_i \in \mathfrak{a}\mathfrak{b}$. Thereby $(uc)/1 = \sum_i (a_i/1)(b_i/1) \in \mathfrak{u}\,\mathfrak{w}$ and hence $c/1 = (1/u)((uc)/1) \in \mathfrak{u}\,\mathfrak{w}$ which means $c \in (\mathfrak{u}\,\mathfrak{w})\cap R$. And if conversely $c \in (\mathfrak{u}\,\mathfrak{w})\cap R$ then there are $a_i/u_i \in \mathfrak{u}$ and $b_i/v_i \in \mathfrak{w}$ such that

$$\frac{c}{1} = \sum_{i=1}^{n} \frac{a_i}{u_i} \frac{b_i}{v_i} = \sum_{i=1}^{n} \frac{a_i b_i \widehat{u}_i \widehat{v}_i}{uv} \in \mathfrak{um}$$

where as usual $u := u_1 \dots u_n$, $v := v_1 \dots v_n$ and $\hat{u}_i := u/u_i$, $\hat{v}_i := v/v_i \in U$. From this equality we again get $uvwc = \sum_i a_i b_i \hat{u}_i \hat{v}_i \in \mathfrak{ab}$ for some $w \in U$ (as $a_i/u_i \in \mathfrak{u}$ implies $a_i/1 = (u_i/1)(a_i/u_i) \in \mathfrak{u}$ and hence $a_i \in \mathfrak{a}$, likewise $b_i \in \mathfrak{b}$). And as $uvw \in U$ this is $c \in (\mathfrak{ab}) : U$.

• $\sqrt{\mathfrak{l}} \cap R = \sqrt{\mathfrak{a}}$: if $b \in \sqrt{\mathfrak{l}} \cap R$ then $b/1 \in \sqrt{\mathfrak{l}}$, that is there is some $k \in \mathbb{N}$ such that $(b/1)^k = b^k/1 \in \mathfrak{l}$. Again this is $b^k \in \mathfrak{l} \cap R = \mathfrak{a}$ and hence $b \in \sqrt{\mathfrak{a}}$. Conversely if $b \in \sqrt{\mathfrak{a}}$ then $b^k \in \mathfrak{a}$ for some $k \in \mathbb{N}$. Hence $(b/1)^k = b^k/1 \in \mathfrak{l}$ which yields $b/1 \in \sqrt{\mathfrak{l}}$ and thereby $b \in \sqrt{\mathfrak{l}} \cap R$.

Proof of (2.106):

Nearly all of the statements are purely definitional. The two exceptions to this are the equalities claimed for U^{-1} spec R and U^{-1} smax R: Consider any prime ideal $\mathfrak{P} \leq_{\mathbf{i}} R$ with $\mathfrak{P} \cap U = \emptyset$. If now $ua \in \mathfrak{P}$ then $u \in \mathfrak{P}$ or $a \in \mathfrak{P}$, as \mathfrak{P} is prime. But $u \in \mathfrak{P}$ is absurd, due to $\mathfrak{P} \cap U = \emptyset$. This only leaves $a \in \mathfrak{P}$ and hence $\mathfrak{P} \in U^{-1}$ ideal R. Conversely let $\mathfrak{P} \leq_{\mathbf{i}} R$ be a prime ideal with $\mathfrak{P} = \mathfrak{P} : U$. If now $u \cdot 1 = u \in \mathfrak{P} \cap U$ then $1 \in \mathfrak{P} : U = \mathfrak{P}$ in contradiction to $\mathfrak{P} \neq R$. Hence we get $\mathfrak{P} \cap U = \emptyset$. Now recall that any maximal ideal is prime. Then repeating the arguments above we also find $\mathfrak{M} = \mathfrak{M} : U \iff \mathfrak{M} \cap U = \emptyset$ for any maximal ideal $\mathfrak{M} \leq_{\mathbf{i}} R$.

Proof of (2.107):

• First of all it is clear that the mapping $\mathfrak{u} \mapsto \mathfrak{u} \cap R = \kappa^{-1}(\mathfrak{u})$ maps ideals to ideals, as it is just the pull back along the homomorphism κ . Now suppose that $ua \in \mathfrak{u} \cap R$ - this is $ua/1 \in \mathfrak{u}$ and hence a/1 =

 $(1/u)(ua/1) \in \mathfrak{u}$. But this again implies $a \in \mathfrak{u} \cap R$ and hence $\mathfrak{u} \cap R \in U^{-1}$ ideal R. Conversely for any ideal $\mathfrak{a} \leq_{\mathbf{i}} R$ the set $U^{-1}\mathfrak{a}$ is an ideal of $U^{-1}R$ by (2.101). Thus both of the mappings are well-defined.

• Next we remark that for any $\mathfrak{a} \in U^{-1}$ ideal R and $\mathfrak{u} \leq_i U^{-1}R$ we obtain

$$(U^{-1}\mathfrak{a}) \cap R = \mathfrak{a} : U = \mathfrak{a}$$
$$U^{-1}(\mathfrak{u} \cap R) = \{a/u \mid a/1 \in \mathfrak{u}, u \in U\} = \mathfrak{u}$$

Thereby the first equality follows from (2.103) and the definition of U^{-1} ideal R. And for the second equality consider a/u where $a/1 \in \mathfrak{u}$. Then we find that $a/u = (1/u)(a/1) \in \mathfrak{u}$ as well. And if conversely $a/u \in \mathfrak{u}$ then we likewise get $a/1 = (u/1)(a/u) \in \mathfrak{u}$ again. Altogether these equalities yield that the maps given are mutually inverse.

- If $\mathfrak{a} \subseteq \mathfrak{b}$ and we consider any $a/u \in U^{-1}\mathfrak{a}$ then $a \in \mathfrak{a} \subseteq \mathfrak{b}$ and hence $a/u \in U^{-1}\mathfrak{b}$. And if conversely $\mathfrak{u} \subseteq \mathfrak{w}$ and $a \in \mathfrak{u} \cap R$ then $a/1 \in \mathfrak{u} \subseteq \mathfrak{w}$ such that $a \in \mathfrak{w} \cap R$. That is both of the mappings are order preserving.
- Next we want to prove that this correspondence preserves radical ideals. Thus if $\mathfrak{a} \in U^{-1}$ ideal R is a radical ideal then we have $\mathfrak{a} = \sqrt{\mathfrak{a}}$ and thereby $U^{-1}\mathfrak{a}$ is a radical ideal due to (2.104) (see below). Likewise we see that if $\mathfrak{u} \in$ ideal $U^{-1}R$ is a radical ideal, then $\mathfrak{u} \cap R$ is radical, too:

$$\sqrt{U^{-1}\mathfrak{a}} = U^{-1}(\sqrt{\mathfrak{a}}) = U^{-1}\mathfrak{a}$$
$$\sqrt{\mathfrak{u} \cap R} = \sqrt{\mathfrak{u}} \cap R = \mathfrak{u} \cap R$$

• Thus it only remains to verify that prime (resp. maximal) ideals are truly correspond to prime (resp. maximal) ideals. For prime ideals this is an easy, straightforward computation: $ab/uv \in U^{-1}\mathfrak{p}$ implies $ab \in \mathfrak{p}$ thus $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ which again is $a/u \in U^{-1}\mathfrak{p}$ or $b/v \in U^{-1}\mathfrak{p}$. Conversely $ab \in \mathfrak{r} \cap R$ implies $ab/1 \in \mathfrak{r}$ and hence $a/1 \in \mathfrak{r} \cap R$ or $b/1 \in \mathfrak{r} \cap R$. And for maximal ideals this is clear, as the mappings given obviously preserve inclusions.

Proof of (2.111):

(i) We will first prove the injectivity of the map given: thus suppose f/uand g/v are mapped to the same point in $(U^{-1}R)[t]$. Comparing the coefficients for these polynomials we find that $f[\alpha]/u = g[\alpha]/v \in U^{-1}R$ for any $\alpha \in \mathbb{N}$. That is there is some $w(\alpha) \in U$ such that $vw(\alpha)f[\alpha] =$ $uw(\alpha)g[\alpha]$. Without loss of generality assume deg $f \leq \deg g$ and let $w := w(0)w(1) \dots w(\deg g) \in U$. Then clearly also $vwf[\alpha] = uwg[\alpha]$ for any $\alpha \in 0 \dots \deg g$ and hence even for any $\alpha \in \mathbb{N}$. This now yields

$$vwf(t) = \sum_{\alpha=0}^{\infty} vwf[\alpha]t^{\alpha} = \sum_{\alpha=0}^{\infty} uwg[\alpha]t^{\alpha} = uwg(t)$$

And hence we have just seen that f/u = g/v as elements of $U^{-1}(R[t])$. For the surjectivety we are given a polynomial \overline{f} in $(U^{-1}R)[t]$

$$\overline{f} = \sum_{\alpha=0}^{\infty} \frac{f[\alpha]}{u(\alpha)} t^{\alpha}$$

Let now $u := u(0)u(1) \dots u(\deg(\overline{f})) \in U$ and $\widehat{u}(\alpha) := u/u(\alpha) \in R$, then it is clear that we get $f/u \mapsto \overline{f}$ for the polynomial

$$f := \sum_{\alpha=0}^{\infty} \widehat{u}(\alpha) f[\alpha] t^{\alpha}$$

(ii) We regard the homomorphism $R[t] \mapsto R_u : f \mapsto f(1/u)$. It is clear that this is surjective, since $at^k \mapsto a/u^k$ reaches all the elements of R_u . We will now show that the kernel is given to be

$$\operatorname{kn}\left(f \mapsto f(1/u)\right) = (ut - 1)R[t]$$

The inclusion " \supseteq " is clear, as $ut-1 \mapsto u/u-1/1 = 0/1$. Thus suppose $f \mapsto 0/1$, then we need to show that $ut-1 \mid f$ in R[t]. Let $f/1 := \kappa(f) \in (U^{-1}R)[t]$ then it is clear that 1/u is a root (f/1)(1/u) = f(1/u) = 0/1 of f/1 and hence $t - 1/u \mid f/1$ in $(U^{-1}R)[t]$. Since u/1 is a unit in R_u multiplication with u/1 changes nothing and hence $(ut-1)/1 \mid f/1 \in (U^{-1}R)[t]$. Thus

$$\frac{f}{1}(U^{-1}R)[t] \subseteq \frac{ut-1}{1}(U^{-1}R)[t]$$

But it is clear that the ideal $f/1(U^{-1}R)[t]$ corresponds to fR[t] formally $(f/1(U^{-1}R)[t]) \cap R[t] = fR[t]$. And likewise the other ideal $(ut-1)/1f/1(U^{-1}R)[t]$ corresponds to (ut-1)R[t]. As the correspondence respects inclusions we have finally found

$$fR[t] \subseteq (ut-1)R[t]$$

This means $f \in (ut-1)R[t]$ and hence we have also proved " \subseteq ". Thus $f \mapsto f(1/u)$ induces the isomorphism given its inverse is obviously given by $a/u^k \mapsto at^k + (ut-1)R[t]$.

(iii) First of all $U^{-1}R$ is an integral domain by (2.109) and hence the quotient field QUOT $U^{-1}R$ is well-defined again. We will now prove the well-definedness and injectivity of the map $a/b \mapsto (a/1)/(b/1)$. As R is an integral domain (and $0 \notin U$) we get (for any a, b, c and $d \in R$)

$$\frac{a/1}{b/1} = \frac{c/1}{d/1} \quad \Longleftrightarrow \quad \frac{ad}{1} = \frac{a}{1} \cdot \frac{d}{1} = \frac{b}{1} \cdot \frac{c}{1} = \frac{bc}{1}$$
$$\Leftrightarrow \quad \exists u \in U : uad = ubv$$
$$\Leftrightarrow \quad ad = bc$$
$$\Leftrightarrow \quad \frac{a}{b} = \frac{c}{d}$$

The homomorphism property of $a/b \mapsto (a/1)/(b/1)$ is clear by definition of the addition and multiplication in localisations. Thus it only remains to check the surjectivity: consider any $(a/u)/(b/v) \in$ QUOT $U^{-1}R$, then we claim $av/bu \mapsto (a/u)/(b/v)$. To see this we have to show (av/1)/(bu/1) = (a/u)/(b/v) and this follows from:

$$\frac{a}{u}\frac{bu}{1} = \frac{abu}{u} = \frac{ab}{1} = \frac{abv}{v} = \frac{b}{v}\frac{av}{1}$$

(iv) We first check the well-definedness and injectivity of the map given. This can be done simultaneously by th following computation (recall that R was assumed to be an integral domain and $a, b \neq 0$)

$$\frac{x/a^{h}}{(b/a^{n})^{i}} = \frac{y/a^{j}}{(b/a^{n})^{k}} \iff \left(\frac{b}{a^{n}}\right)^{k} \frac{x}{a^{h}} = \left(\frac{b}{a^{n}}\right)^{i} \frac{x}{a^{j}}$$

$$\iff \frac{xb^{k}}{a^{kn+h}} = \frac{yb^{i}}{a^{in+j}}$$

$$\iff xa^{in+j}b^{k} = ya^{kn+h}b^{i}$$

$$\iff a^{i+k}b^{h+j}\left(xa^{in+j}b^{k} - ya^{kn+h}b^{i}\right) = 0$$

$$\iff xa^{in+i+j+k}b^{h+j+k} = ya^{kn+h+i+k}b^{h+i+j}$$

$$\iff (ab)^{j+k}xa^{(n+1)i}b^{h} = (ab)^{h+i}ya^{(n+1)k}b^{j}$$

$$\iff \frac{xa^{(n+1)i}b^{h}}{(ab)^{h+i}} = \frac{ya^{(n+1)k}b^{j}}{(ab)^{j+k}}$$

Hence we have a well-defined injective mapping and it is straightforward to check that it even is a homomorphism of rings. Thus it only remains to check the surjectivity. That is we are given any $x/(ab)^k \in R_{ab}$, then we obtain a preimage by

$$\frac{x/a^{(n+1)k}}{(b/a^n)^k} \ \mapsto \ \frac{xa^{(n+1)k}b^{(n+1)k}}{(ab)^{n+1)k+k}} \ = \ \frac{x}{(ab)^k}$$

(v) Let us regard the map $b/v \mapsto (b + \mathfrak{a})/(v + \mathfrak{a})$. We first check its welldefinedness: suppose $a/u = b/v \in U^{-1}R$, that is there is some $w \in U$ such that vwa = uwb. Of course this yields $(v + \mathfrak{a})(w + \mathfrak{a})(a + \mathfrak{a}) =$ $(u + \mathfrak{a})(w + \mathfrak{a})(b + \mathfrak{a})$. But as $w \in U$ we also have $w + \mathfrak{a} \in U/\mathfrak{a}$ and hence $(a + \mathfrak{a})/(u + \mathfrak{a}) = (b + \mathfrak{a})/(v + \mathfrak{a})$. And it is immediately clear that this map even is a homomorphism of rings. Next we will prove its surjectivity, that is we are given any $(b + \mathfrak{a})/(v + \mathfrak{a}) \in (U/\mathfrak{a})^{-1}(R/\mathfrak{a})$. As $v + \mathfrak{a} \in U/\mathfrak{a}$ there is some $u \in U$ such that $v + \mathfrak{a} = u + \mathfrak{a}$. But from this we find $b/u \in U^{-1}R$ and $b/u \mapsto (b + \mathfrak{a})/(u + \mathfrak{a}) = (b + \mathfrak{a})/(v + \mathfrak{a})$. Thus it remains to prove

$$\ln\left(\frac{b}{v}\mapsto\frac{b+\mathfrak{a}}{v+\mathfrak{a}}\right) = U^{-1}\mathfrak{a} = \left\{\frac{a}{u} \mid a\in\mathfrak{a}, u\in U\right\}$$

The inclusion " \supseteq " is clear, given a/u where $a \in \mathfrak{a}$ we immediately find that $(a + \mathfrak{a})/(u + \mathfrak{a}) = (0 \cdot u + \mathfrak{a})/(1 \cdot u + \mathfrak{a}) = (0 + \mathfrak{a})/(1 + \mathfrak{a}) = 0$. Conversely consider some $b/v \in U^{-1}R$ such that $(b + \mathfrak{a})/(v + \mathfrak{a}) = 0 = (0 + \mathfrak{a})/(1 + \mathfrak{a})$. That is there is some $x + \mathfrak{a} \in U/\mathfrak{a}$ such that $xb + \mathfrak{a} = (x + \mathfrak{a})(b + \mathfrak{a}) = 0 + \mathfrak{a}$. And this means $xb \in \mathfrak{a}$. Further since $x + \mathfrak{a} \in U/\mathfrak{a}$ - there is some $w \in U$ such that $x + \mathfrak{a} = w + \mathfrak{a}$. That is $a := w - x \in \mathfrak{a}$. Now compute $bw = bw - bx + bx = ba + bx \in \mathfrak{a}$. Hence we found $b/v = (bw)/(vw) \in U^{-1}\mathfrak{a}$. Thus according to the isomorphism theorem $b/v \mapsto (b + \mathfrak{a})/(v + \mathfrak{a})$ induces the isomorphy as given in the claim.

- (vi) Let us denote $U := R \setminus \mathfrak{p}$, as $\mathfrak{a} \subseteq \mathfrak{p}$ we get $U \cap \mathfrak{a} = \emptyset$ and $\mathfrak{a}_{\mathfrak{p}} = U^{-1}\mathfrak{a}$ is just the definition. Hence the claim is already included in (v).
- (vii) We first show that this mapping is well defined, i.e. $u/1 \notin \overline{p}$ for $u \notin \mathfrak{p}$. But this is clear, since $\mathfrak{p} = \overline{p} \cap R$. Thus we concern ourselves with the surjectivety: given $(r/a^k)/(u/a^l) \in (R_a)_{\overline{\mathfrak{p}}}$ we see that

$$\frac{ra^{l}}{ua^{k}} \ \mapsto \ \frac{ra^{l}/1}{ua^{k}/1} \ = \ \frac{1/a^{k+l}}{1/a^{k+l}} \cdot \frac{ra^{l}/1}{ua^{k}/1} \ = \ \frac{r/a^{k}}{u/a^{l}}$$

And for the injectivety we have to consider (r/1)/(u/1) = (s/1)/(v/1). Hence there is some $w/a^m \notin \overline{\mathfrak{p}}$ such that $vwr/a^m = uws/a^m \in R_a$. Thus there is some $n \in \mathbb{N}$ such that $a^{m+n}vwr = a^{m+n}uws \in R$. But $w/a^m \notin \overline{\mathfrak{p}}$ means that $w \notin \mathfrak{p}$ and as also $a \notin \mathfrak{p}$ we get that $z := a^{m+n}w \notin \mathfrak{p}$. But as vrz = usz this means that $r/u = s/v \in R_{\mathfrak{p}}$.

Proof of (2.109):

- R integral domain ⇒ U⁻¹R integral domain Suppose (ab)/(uv) = (a/u)(b/v) = 0/1 ∈ U⁻¹R. By definition of the localisation this means that there is some w ∈ U such that wab = 0. But w ≠ 0 (as 0 ∉ U) and R is an itegral domain, thus we get ab = 0. And this again yields a = 0 or b = 0. Of course this yields a/u = 0/1 or b/v = 0/1, that is U⁻¹R is an itegral domain.
- *R* noetherian/artinian $\implies U^{-1}R$ noetherian/artinian Suppose that *R* is noetherian and consider an ascending chain of ideals $\mathfrak{U}_1 \subseteq \mathfrak{U}_2 \subseteq \mathfrak{U}_3 \subseteq \ldots$ in $U^{-1}R$. Let us denote the corresponding ideals of *R* by $\mathfrak{a}_k := \mathfrak{U}_k \cap R$. Then the \mathfrak{a}_k form an ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$ of ideals of *R*, too. And as *R* is noetherian this means that there is some $s \in \mathbb{N}$ such that the chain stabilizes

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots \subseteq \mathfrak{a}_s = \mathfrak{a}_{s+1} = \mathfrak{a}_{s+2} = \ldots$$

Yet the ideals correspond to one and another, that is $\mathfrak{u}_k = U^{-1}\mathfrak{a}_k$. So if we transfer this stabilized chain back to $U^{-1}R$ we find that

 $\mathfrak{u}_1 \subseteq \mathfrak{u}_2 \subseteq \mathfrak{u}_3 \subseteq \ldots \subseteq \mathfrak{u}_s = \mathfrak{u}_{s+1} = \mathfrak{u}_{s+2} = \ldots$

the corresponding chain stabilized, too. And as the chain has been arbitrary this means, that $U^{-1}R$ is noetherian, as well. The fact that R artinian implies $U^{-1}R$ artinian can be proved in complete analogy.

• $R \text{ PID} \implies U^{-1}R \text{ PID}$

Consider any ideal $\mathfrak{u} \leq_{i} U^{-1}R$, by the correspondence theorem (2.107) \mathfrak{u} corresponds to the ideal $\mathfrak{a} := \mathcal{U} \cap R \leq_{i} R$ of R. But as R is a PID there is some $a \in R$ such that $\mathfrak{a} = aR$. And the following computation yields that $\mathfrak{u} = (a/1)U^{-1}R$ is a principal ideal, too

$$\mathfrak{u} = U^{-1}(aR) = \left\{ \left. \frac{ab}{u} \right| b \in R, u \in U \right\} = \frac{a}{1} U^{-1}R$$

• $R \text{ UFD} \implies U^{-1}R \text{ UFD}$

If $0 \in U$ then $U^{-1}R = 0$ and hence $U^{-1}R$ is a UFD. Thus suppose $0 \notin U$. By definition any UFD R is an integral domain, and hence $U^{-1}R$ is an integral domain, too. Thus it suffices to check that any $a/u \in U^{-1}R$ admits a decomposition into prime factors. To see this we will first prove the following assertion

$$p \in R$$
 prime $\implies \frac{p}{1} \in (U^{-1}R)^*$ or $\frac{p}{1} \in (U^{-1}R)$ prime

Thus let $p \in R$ be prime and assume $p/1 \mid (a/u)(b/v) = (ab)/(uv)$. That is there is some $h/w \in U^{-1}R$ such that ph/w = ab/uv. And as R is an integral domain this implies uvph = wab. In particular $p \mid wab$ and as p is prime this means $p \mid w$ or $p \mid a$ or $p \mid b$. First suppose $p \mid w$, i.e. there is some $\gamma \in R$ such that $\gamma p = w$. Then $(p/1)(\gamma/w) = w/w = 1$ and hence $p/1 \in (U^{-1}R)^*$ is a unit. Otherwise, if $p \mid a$ - say $\alpha p = a$ - then $(p/1)(\alpha/u) = a/u$. That is $p/1 \mid a/u$. Analogously we find $p \mid b \implies p/1 \mid b/v$. Thus either p/1 is a unit or prime, as claimed. Now we may easily verify that $U^{-1}R$ is an UFD: consider any $0 \neq a/u \in U^{-1}R$. As R is an UFD we find a decomposition of $a \neq 0$ into prime elements $a = \alpha p_1 \dots p_k$ (where $\alpha \in R^*$ and $p_i \in R$ prime). Now let $I := \{i \in I \mid p_i/1 \in (U^{-1}R)^*\}$ be the set of indices i for which $p_i/1$ is a unit. Then

$$\frac{a}{u} = \frac{\alpha}{u} \frac{p_1}{1} \dots \frac{p_k}{1} = \left(\frac{\alpha}{u} \prod_{i \in I} \frac{p_i}{1}\right) \prod_{i \notin I} \frac{p_i}{1}$$

That is we have found a decomposition of a/u into (a unit and) prime factors. And as a/u has been an arbitrary non-zero element, this proves that $U^{-1}R$ truly is an UFD.

• $R \text{ normal} \implies U^{-1}R \text{ normal}$

We have already seen that $U^{-1}R$ is an integral domain, since R is an integral domain. To prove that $U^{-1}R$ is integrally closed in its quotient field we will make use of the isomorphy (2.111.(iii))

$$\Phi : \operatorname{QUOT} R \xrightarrow{\sim} \operatorname{QUOT} U^{-1}R : \frac{r}{s} \mapsto \frac{r/1}{s/1}$$

Recall that R is embedded canonically into QUOT R by $a \mapsto a/1$. Hence QUOT R is considered to be an R-algebra under the scalar multiplication $a(r/s) := (a/1) \cdot (r/s) = ar/s$. Analogously, for any $a/w \in U^{-1}R$ and any r/u, $s/v \in U^{-1}R$ we have

$$\frac{a}{w}\frac{r/u}{s/v} = \frac{a/w}{1/1} \cdot \frac{r/u}{s/v} = \frac{ar/uw}{s/v}$$

Thus if we consider any $a \in R$ and any $r/s \in \text{QUOT } R$, then the isomorphism φ satisfies $\Phi(ax) = (a/1)\Phi(x)$, which can be seen in a straightforward computation

$$\Phi(ax) = \Phi\left(\frac{ar}{s}\right) = \frac{ar/1}{s/1} = \frac{a/1}{1/1} \cdot \frac{r/1}{s/1}$$
$$= \frac{a}{1}\frac{r/1}{s/1} = \frac{a}{1}\Phi\left(\frac{r}{s}\right) = \frac{a}{1}\Phi(x)$$

Now consider any $x/y \in \text{QUOT } U^{-1}R$, that is integral over $U^{-1}R$. That is there are some $n \in \mathbb{N}$ and $p_0, \ldots, p_{n-1} \in U^{-1}R$ such that

$$\left(\frac{x}{y}\right)^n + \sum_{k=0}^{n-1} p_k \left(\frac{x}{y}\right)^k = 0$$
Then we need to show that $x/y \in U^{-1}R$. To do this let us pick up some $r/s \in \text{QUOT }R$ such that $x/y = \Phi(r/s)$. Further note that $p_k \in U^{-1}R$, that is $p_k = a_k/u_k$ for some $a_k \in R$ and $u_k \in U$ and let $u := u_0 \dots u_{n-1} \in U$. Then multiplication with $u^n/1 \in U^{-1}R$ yields

$$\left(\frac{u}{1}\Phi\left(\frac{r}{s}\right)\right)^n + \sum_{k=0}^{n-1} \frac{a_k u^{n-k}}{u_k} \left(\frac{u}{1}\Phi\left(\frac{r}{s}\right)\right)^k = 0$$

Now recall that $(u/1)\Phi(r/s) = \Phi(u(r/s)) = \Phi(ur/s)$. Further note that due to k < n we have $u_k \mid u \mid u^{n-k}$. Therefore we may define $b_k := a_k u^{n-k}/u_k \in R$. Inserting this in the above equation yields

$$\Phi\left(\frac{ur}{s}\right)^n + \sum_{k=0}^{n-1} \frac{b_k}{1} \Phi\left(\frac{ur}{s}\right)^k = 0$$

Again we use $(b_k/1)\Phi(ur/s) = \Phi(b_k(ur/s))$ and use the homorphism properties of Φ to place Φ in front, obtaining an equation of the form $\Phi(\ldots) = 0$. But as Φ has been an isomorphism it can be eliminated from this equation ultimatly yielding

$$\left(\frac{ur}{s}\right)^n + \sum_{k=0}^{n-1} b_k \left(\frac{ur}{s}\right)^k = 0$$

Thus we have found that $ur/s \in \text{QUOT } R$ is integral over R. Hence by assumption on R we have $ur/s \in R$, that is there is some $a \in R$ such that ur/s = a/1. And this is ur = as such that $r/s = a/u \in U^{-1}R$. Thus we have finally found

$$\frac{x}{y} = \Phi\left(\frac{r}{s}\right) = \Phi\left(\frac{a}{u}\right) = \frac{a/1}{u/1} = \frac{a/u}{1/1} \in U^{-1}R$$

• R Dedekind domain $\implies U^{-1}R$ Dedekind domain

If R is a Dedekind domain, then R is noetherian, integrally closed and spec $R = \{0\} \cup \operatorname{smax} R$. As we have seen this implies, that $U^{-1}R$ is noetherian and integrally closed, too. Thus consider a non-zero prime ideal $0 \neq \mathfrak{W} \leq_{i} U^{-1}R$. Then $\mathfrak{M} := \mathfrak{W} \cap R \leq_{i} R$ is a nonzero prime ideal of R, too (if we had $\mathfrak{M} = 0$ then $\mathfrak{W} = U^{-1}\mathfrak{M} = 0$, a contradiction). Thus \mathfrak{M} is maximal and hence $\mathfrak{W} = \mathfrak{M}R$ is maximal, too. That is spec $U^{-1}R = \{0\} \cup \operatorname{smax} U^{-1}R$. Altogether $U^{-1}R$ is a Dedekind domain, too.

Proof of (2.110):

We have already proved (a) \implies (b) in (2.109) and (b) \implies (c) is trivial.

Thus it only remains to verify (c) \implies (a): we denote F := QUOT R the quotient field of R and regard R and any localisation $R_{\mathfrak{m}}$ as a subring of R (also refer to (2.98) for this). Now regard any $x \in F$ integral over R, that is f(x) = 0 for some normed polynomial $f \in R[t]$. If we interpret $f \in R_{\mathfrak{m}}[t]$, then f(x) = 0 again and hence x is integral over $R_{\mathfrak{m}}$ (where $\mathfrak{m} \leq_{i} R$ is any maximal ideal of R). By assumption $R_{\mathfrak{m}}$ is normal and hence $x \in R_{\mathfrak{m}}$ again. And as \mathfrak{m} has been arbitary the local global principle (2.98) yields:

$$x \in \bigcap_{\mathfrak{M} \in \operatorname{smax} R} R_{\mathfrak{M}} = R$$

Proof of (2.49): (continued)

• (c) \implies (d): property (2) of (c) and (d) are identical so we only need to verify (1) in (d). If all $a_i = 0$ are zero then there is nothing to prove (s := 0). And if at least one $a_r \neq 0$ is non-zero, then so are all a_{r+i} for $i \in \mathbb{N}$. Omitting the a_0 to a_{r-1} we may assume $a_i \neq 0$ for any $i \in \mathbb{N}$. By assumption we have $a_i R \subseteq a_{i+1}R$ for any $i \in \mathbb{N}$. And this translates into $a_{i+1} \mid a_i$. By (2.53.(iii)) this yields a descending chain of natural numbers for any prime element $p \in R$

$$\langle p:a_0\rangle \geq \langle p:a_1\rangle \geq \ldots \geq \langle p:a_i\rangle \geq \ldots \geq 0$$

Of course this means that the sequence $\langle p : a_i \rangle$ has to become startionary. That is there is some $s(p) \in \mathbb{N}$ such that for all $i \in \mathbb{N}$ we get $\langle p : a_{s(p)+i} \rangle = \langle p : a_{s(p)} \rangle$. We now choose a representing system \mathbb{P} of the prime elements of R modulo associateness. Then there only are finitely many $p \in \mathbb{P}$ such that $\langle p : a_0 \rangle \neq 0$. And for those $p \in \mathbb{P}$ with $\langle p : a_0 \rangle = 0$ we may clearly take s(p) = 0. Thereby we may define

 $s := \max\{s(p) \mid p \in \mathbb{P}\} \in \mathbb{N}$

Then it is clear that for any $p \in \mathbb{P}$ and any $i \in \mathbb{N}$ we get $\langle p : a_{s+i} \rangle = \langle p : a_s \rangle$. And by (2.53.(iv)) this is nothing but $a_{s+i} \approx a_s$ which again translates into $a_{s+i}R = a_sR$. And this is just what had to be proved.

(d) ⇒ (c): property (2) of (c) and (d) are identical so we only need to verify (1) in (c). But the proof of this would be a literal repetition of (2.48.(iii)). There we have proved the existence of an irreducible decomposition using the ascending chain condition of noetherian rings. But in fact this property has only been used for principal ideals and hence is covered by the assumption (1) in (d). Hence the same proof can be applied here, too.

- (a) ⇒ (e): As p ≠ 0 is non-zero, there is some 0 ≠ a ∈ R with a ∈ p. Clearly a ∉ R* as else p = R. We now use a prime decomposition of a, that is αp₁...p_k = a ∈ p. Thereby k ≥ 1 as else a ∈ R*. And as p is prime we either get α ∈ p or p_i ∈ p for some i ∈ 1...k. But again α ∈ p would yield p = R which cannot be. Thus p := p_i ∈ p where p is prime by construction.
- (e) \implies (f): We assume $R \neq 0$ (else the stetements herin do not make sense!). It is clear that $0 \notin D$ (as R is an integral domain $\alpha \in R^*$ and $p_i \neq 0$). Therefore $D \subseteq R \setminus \{0\}$ such that we obtain the canonical homomorphism

$$D^{-1}R \to \operatorname{QUOT} R : \frac{a}{d} \mapsto \frac{a}{d}$$

Due to $0 \notin D$ we also see that $D^{-1}R \neq 0$ is not the zero-ring. Therefore $D^{-1}R$ contains a maximal ideal $\mathfrak{u} \leq_{i} D^{-1}R$ - by (2.4.(iv)) - such that $\mathfrak{p} := \mathfrak{u} \cap R \in D^{-1}$ smax R is maximal too - by (2.107) - in particular prime. Suppose $\mathfrak{p} \neq 0$ then by assumption (e) there is some prime element $p \in \mathfrak{p}$. And thereby $p \in \mathfrak{p} \cap D$ in contradiction to $\mathfrak{p} \in D^{-1}$ smax R. Thus $\mathfrak{p} = 0$ and therefore $\mathfrak{u} = D^{-1}\mathfrak{p} = 0$, too. But $0 \in D^{-1}R$ being maximal yields that $D^{-1}R$ is a field. In particular the canonical homomorphism is injective (as it is non-zero). Now choose any $a/b \in \text{QUOT } R$ then $a, b \in R$ and hence $a/1, b/1 \in D^{-1}R$. Yet $b \neq 0$ and hence $(1/b)^{-1} = 1/b \in D^{-1}R$, as $D^{-1}R$ is a field. Therefore $a/b \in D^{-1}R$ such that the canonical homomorphism also is surjective. By construction this even is an equality of sets.

• (f) \implies (a): Consider any $0 \neq a \in R$. Then $1/a \in \text{QUOT } R = D^{-1}R$, that is there are $b \in R$ and $d \in D$ such that 1/a = b/d. And as R is an integral domain this is $ab = d \in D$. Yet D is saturated by (2.47.(vi)) and therefore $a \in D$. But this just means that a admits a prime decomposition.

Proof of (2.74):

We have already proved statements (i) to (vii) on page (331), so it only remains to prove statement (viii). We have already seen in (vii) that the map $\mathfrak{b} \mapsto \mathfrak{b} \cap R = \kappa^{-1}(\mathfrak{b})$ is well-defined (as $\kappa^{-1}(\mathfrak{q}) = \mathfrak{q} \cap R = \mathfrak{p}$ again). Thus we next check the well-definedness of $\mathfrak{a} \mapsto U^{-1}\mathfrak{a}$. First of all we have $\sqrt{U^{-1}\mathfrak{a}} = U^{-1}\sqrt{\mathfrak{a}} = U^{-1}\mathfrak{p} = \mathfrak{q}$ due to (2.104). Now consider a/u and $b/v \in U^{-1}R$ such that $(ab)/(uv) = (a/u)(b/v) \in U^{-1}\mathfrak{a}$ but $b/v \notin U^{-1}R$. Then $ab \in (U^{-1}\mathfrak{a}) \cap R = \mathfrak{a} : U$, that is there is some $w \in U$ such that $abw \in \mathfrak{a}$. But $bw \notin \mathfrak{a}$, as else $b/v = (bw)/(vw) \in U^{-1}\mathfrak{a}$. As \mathfrak{a} is primary this implies $a \in \sqrt{\mathfrak{a}} = \mathfrak{p}$ and hence $a/u \in U^{-1}\mathfrak{p} = \mathfrak{q} = \sqrt{U^{-1}\mathfrak{a}}$. This means that $U^{-1}\mathfrak{a}$ is primary again and hence $\mathfrak{a} \mapsto U^{-1}\mathfrak{a}$ is well-defined.

Proof of (2.15):

- (i) As the union ranges over all prime ideals \mathfrak{p} with $\mathfrak{p} \subseteq \mathbb{ZD} R$ it is clear that the union is contained in $\mathbb{ZD} R$ again. That is the incluison " \supseteq " is trivial. For the converse inclusion let us denote $U := \mathbb{NZD} R$, then Uis multiplicatively closed. Let now $a \in \mathbb{ZD} R$ be a zero-divisor. That is we may choose some $0 \neq b \in R$ such that ab = 0. This implies $aR \subseteq \mathbb{ZD} R$ (because given any $x \in R$ we get (ax)b = x(ab) = x0 = 0) or in other words $aR \cap U = \emptyset$. Thus by (2.4.(iii)) we may choose an ideal \mathfrak{p} maximal among the ideals satisfying $aR \subseteq \mathfrak{b} \subseteq R \setminus U = \mathbb{ZD} R$ and this is prime. In particular $a \in \mathfrak{p}$ such that a is also contained in the union of prime ideals contained in $\mathbb{ZD} R$.
- (ii) Let \mathfrak{p} be a minimal prime ideal of R, then by the correspondence theorem (2.107) the spectrum of the localised ring $R_{\mathfrak{p}}$ corresponds to

 $\operatorname{spec} R_{\mathfrak{p}} \longleftrightarrow \{\mathfrak{q} \in \operatorname{spec} R \mid \mathfrak{q} \subseteq \mathfrak{p}\} \longleftrightarrow \{\mathfrak{p}\}$

Hence $R_{\mathfrak{p}}$ has precisely one prime ideal, namely the ideal $\overline{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}\mathfrak{p}$ corresponding to \mathfrak{p} . And by (2.17.(v)) this yields

NIL
$$R_{\mathfrak{p}} = \bigcap \operatorname{spec} R_{\mathfrak{p}} = \overline{\mathfrak{p}}$$

Now consider any $a \in \mathfrak{P}$, then $a/1 \in \overline{\mathfrak{P}}$ and hence there is some $k \in \mathbb{N}$ such that $a^k/1 = (a/1)^k = 0/1$. That is there is some $u \in R \setminus \mathfrak{P}$ such that $ua^k = 0$. But $k \neq 0$ as else $u = 0 \in \mathfrak{P}$. Hence we may choose $1 \leq k$ minimally such that $ua^k = 0$. Then we let $b := ua^{k-1}$ and thereby get $b \neq 0$ (as k has been minimal) and ab = 0. That is $a \in \mathbb{ZD}R$ and hence $\mathfrak{P} \subseteq \mathbb{ZD}R$ (as a has been arbitary).

Proof of (2.112):

(b) \implies (a): of course R = 0 cannot occur, as else $R^* = R$ and hence $R \setminus R^* = \emptyset$ was no ideal of R. Thus $R \neq 0$ and hence R contains a maximal ideal, by (2.4.(iv)). And if $\mathfrak{m} \leq_i R$ is any maximal ideal of R then we have $\mathfrak{m} \neq R$ and hence $\mathfrak{m} \subseteq R \setminus R^* \neq R$. By maximality of \mathfrak{m} we get $\mathfrak{m} = R \setminus R^*$ which also is the uniqueness of the maximal ideal. (a) \Longrightarrow (b): let \mathfrak{m} be the one and only maximal ideal of R. As $\mathfrak{m} \neq R$ we again get $\mathfrak{m} \subseteq R \setminus R^*$. Conversely, if $a \in R \setminus R^*$ then $aR \neq R$. Hence there is a maximal ideal containing aR, by (2.4.(ii)). But the only maximal ideal is \mathfrak{m} such that $a \in aR \subseteq \mathfrak{m}$. And as a has been arbitary this proves $R \setminus R^* \subseteq \mathfrak{m}$ and hence $\mathfrak{m} = R \setminus R^*$. In particular $R \setminus R^*$ is an ideal of R.

Proof of (2.113):

(a) \implies (b): consider any $\mathfrak{a} \neq R$, then by (2.4.(ii)) \mathfrak{a} is contained in some maximal ideal, and the only maximal ideal available is \mathfrak{m} , such that $\mathfrak{a} \subseteq \mathfrak{m}$. (b) \implies (a): first of all \mathfrak{m} is a maximal ideal, as (due to (b)) $\mathfrak{m} \subseteq \mathfrak{a} \leq_{\mathrm{i}} R$ implies $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = R$. And if $\mathfrak{n} \leq_{\mathrm{i}} R$ is any maximal ideal of R, then we have $\mathfrak{n} \neq R$ and hence (due to (b)) $\mathfrak{n} \subseteq \mathfrak{m}$. But by maximality of \mathfrak{n} and $\mathfrak{m} \neq R$ we now conclude $\mathfrak{n} = \mathfrak{m}$. Altogether we have smax $R = \{\mathfrak{m}\}$ as claimed. (a) \implies (c): has already been proved in (2.112) - in the form $R \setminus R^* = \mathfrak{m}$. (c) \implies (d) is trivial, so it only remains to prove the implication (d) \implies (b): consider any ideal $\mathfrak{a} \neq R$ again, then we have $\mathfrak{a} \subseteq R \setminus R^*$ and due to (d) this yields $\mathfrak{a} \subseteq R \setminus R^* \subseteq \mathfrak{m}$.

Proof of (2.115):

By the correspondence theorem (2.107) it is clear that $\mathfrak{m}_{\mathfrak{p}}$ is in fact a maximal ideal of $R_{\mathfrak{p}}$. Now suppose $\mathfrak{m}_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1} \mathfrak{n} \leq_{i} R_{\mathfrak{p}}$ is any maximal ideal of $R_{\mathfrak{p}}$. In particular $\mathfrak{m}_{\mathfrak{p}}$ is a prime ideal and hence (by the correspondence theorem again) $\mathfrak{n} \cap (R \setminus \mathfrak{p}) = \emptyset$. In other words that is $\mathfrak{n} \subseteq \mathfrak{p}$ and hence $\mathfrak{n}_{\mathfrak{p}} \subseteq \mathfrak{m}_{\mathfrak{p}}$. But by the maximality of $\mathfrak{m}_{\mathfrak{p}}$ this is $\mathfrak{n}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$. Thus $\mathfrak{m}_{\mathfrak{p}}$ is the one and only maximal ideal of $R_{\mathfrak{p}}$ - that is $R_{\mathfrak{p}}$ is a local ring.

Now regard $R_{\mathfrak{p}} \twoheadrightarrow \text{QUOT } R/\mathfrak{p} : a/u \mapsto (a + \mathfrak{p})/(u + \mathfrak{p})$. This is welldefined and surjective, since $u + \mathfrak{p} \neq 0 + \mathfrak{p}$ if and only if $u \notin \mathfrak{p}$. And since R/\mathfrak{p} is an integral domain we have $(a + \mathfrak{p})/(u + \mathfrak{p}) = (0 + \mathfrak{p})/(1 + \mathfrak{p})$ if and only if $a + \mathfrak{p} = 0 + \mathfrak{p}$ which is equivalent to $a \in \mathfrak{p}$ again. Thus the kernel of this epimorphism is just $\mathfrak{m}_{\mathfrak{p}}$ and hence it induces the isomorphism given.

Proof of (2.118):

- (U) As $R \neq 0$ we have $1 \neq 0$ and hence by property (1) we find $\nu(1) \in \mathbb{N}$. Thus by (2) we get $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \in \mathbb{Z}$. And together this implies $\nu(1) = 0$. Now consider any $\alpha \in R^*$ then by (2) again $0 = \nu(1) = \nu(\alpha \alpha^{-1}) = \nu(\alpha) + \nu(\alpha^{-1}) \geq \nu(\alpha) \geq 0$ hence $\nu(\alpha) = 0$.
- (I) If we are given $a, b \in R$ with ab = 0 then by (1) and (2) we have $\infty = \nu(ab) = \nu(a) = \nu(b)$. Thus $\nu(a)$ and $\nu(b)$ may not both be finte and by (1) this means a = 0 or b = 0.
- (P) First of all $0 \in [\nu]$ as by (1) we have $\nu(0) = \infty \ge 1$ and $1 \notin [\nu]$ as $\nu(1) = 0 < 1$ by (U). If now $a, b \in [\nu]$ and $c \in R$ then we compute

$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\} \geq 1$$

$$\nu(ac) = \nu(a) + \nu(c) \geq \nu(a) \geq 1$$

And hence a + b and $ac \in [\nu]$ again. Hence $[\nu]$ truly is an ideal of Rand $[\nu] \neq R$ as $1 \notin [\nu]$. Now suppose $ab \in [\nu]$ for some $a, b \in R$, that is $\nu(ab) = \nu(a) + \nu(b) \ge 1$. Then it cannot be that $\nu(a) = 0 = \nu(b)$ and hence $a \in [\nu]$ or $b \in [\nu]$, which means $[\nu]$ is prime.

- (iii) It is clear that $1 \mid a$ for any $a \in R$ and hence $0 \in \{k \in \mathbb{N} \mid p^k \mid a\}$. Therefore $a[p] \in \mathbb{N} \cup \{\infty\}$ is well-defined.
 - As any $p^k \mid 0$ it is clear that $\nu(0) = \infty$. Conversely suppose that $\nu(a) = \infty$ for some $a \in R$. Then for any $k \in \mathbb{N}$ we may choose some $a_k \in R$ such that $a = p^k a_k$. Then $p^{k+1}a_{k+1} = a = p^k a_k$ and as R is an integral domain this implies $pa_{k+1} = a_k$, in particular $a_{k+1} \mid a_k$. Going to ideals this yields an ascending chain

$$a_0S \subseteq a_1S \subseteq \ldots \subseteq a_kS \subseteq \ldots$$

As R is noetherian there is some $s \in \mathbb{N}$ such that $a_s R = a_{s+1}R$, i.e. there is some $\alpha \in R^*$ such that $a_{s+1} = \alpha a_s = \alpha p a_{s+1}$. If $a_{s+1} \neq 0$ this would mean $p = \alpha^{-1}$ (as R is an integral domain) which is absurd, since p is prime. Thus we have $a_{s+1} = 0$ and hence $a = p^{s+1}a_{s+1} = 0$.

- If g = 0 then $\nu(fg) = \infty = \nu(f) + \nu(g)$, thus we only need to consider $0 \neq f, g \in R$. Now write $f = p^k a$ and $g = p^l b$ where k = f[p] and l = g[p], then by maximality we have $p \nmid a$ and $p \not\mid b$ and hence $p \not\mid ab$, since p is prime. Hence $\nu(fg) = \nu(p^{k+l}ab) = k + l = \nu(f) + \nu(g)$.
- If g = 0 then ν(f+g) = ν(f) = min{ν(f), ν(g)}, thus we only need to consider 0 ≠ f, g ∈ R. As above let us write f = p^ka and g = p^lb where k = f[p] and l = g[p]. Without loss of generality we may assume k ≤ l then f + g = p^k(a + p^{l-k}b) and hence ν(f + g) = ν(p^k(a + p^{l-k}b)) = k + ν(a + p^{l-k}b) ≥ k = min{ν(f), ν(g)}. Thus by now ν is a valuation on R and it is normed, since ν(p) = 1.
- Continuing with the previous item now prove the fifth property: i.e. we even have k < l. If we now had $p \mid a+p^{l-k}b$, then there would be some $h \in S$ such that $a = ph p^{l-k}b$. But this would imply $p \mid a$ which is absurd, by maximality of k. Hence $\nu(f+g) = k = \min\{\nu(f), \nu(g)\}$.
- (iv) $\nu \mapsto [\nu]$ is well-defined:

As ν is normed, we have $[\nu] \neq 0$. Hence $[\nu]$ is a non-zero-prime ideal, and as R is a PID this even implies maximality.

- $\mathfrak{M} \mapsto \nu_p$ is well-defined: If we have $pR = \mathfrak{M} = qR$ then there is some $\alpha \in R^*$ with $\alpha p = q$ and as $(\alpha p)^k \mid a \iff p^k \mid a$ we then also get $\nu_q = \nu_{\alpha p} = \nu_p$.
- $\mathfrak{M} \mapsto \nu_p \mapsto [\nu_p] = \mathfrak{M}$: It is clear that $[\nu_p] = pR$ and as also $\mathfrak{M} = pR$ by construction $[\nu_p] = \mathfrak{M}$.

• $\nu \mapsto [\nu] \mapsto \nu_p = \nu$:

By construction we have $[\nu] = pR$, thus if $a \in R$ with $p \not\mid a$ then $a \notin pR = [\nu]$ and hence $\nu(a) = 0$. And as ν is normed, there is some $q \in S$ such that $\nu(q) = 1$. Hence $q \in [\nu] = pR$, which means $p \mid q$. Therefore $1 \leq \nu(p)$ (as $p \in pR = [\nu]$) and $\nu(p) \leq \nu(q) = 1$ (as $p \mid q$) imply $\nu(p) = 1$. If now $f \in R$ is given aribitarily then we write $f = p^k a$ where $p \not\mid a$, then $\nu(f) = k\nu(p) + \nu(a) = k = \nu_p(f)$. And hence $\nu = \nu_p$.

 \square

Proof of (2.120):

- (i) The properties (1), (2) and (3) of valued rings and discrete valuation rings are identical. Hence it suffices to check that R is non-zero. But by (N) there is some $m \in R$ with $\nu(m) = 1 \neq \infty$ and by (1) this is $m \neq 0$. In particular $R \neq 0$.
- (ii) We have already seen in (??.(i)) that $[\nu]$ is a prime ideal of R. Thus by (2.113) it suffices to check $R \setminus [\nu] \subseteq R^*$. Thus consider any $a \in R \setminus [\nu]$, that is $\nu(a) = 0 = \nu(1)$ and hence $\nu(1) \leq \nu(a)$ and $\nu(a) \leq \nu(1)$. By (4) this implies $1 \mid a$ and $a \mid 1$ which again is $a \approx 1$ or in other words $a \in R^*$.
- (iii) By (i) and (??.(i)) we know that R is an integral domain. Thus consider $a, b \in R$ with $a \neq 0$, then we need to find some $q, r \in R$ such that b = qa + r and $(r = 0 \text{ or } \varepsilon(r) < \varepsilon(a))$. To do this we distinguish three cases: if b = 0, then we may choose q := 0 and r := 0. If $b \neq 0$ and $\nu(b) < \nu(a)$, then we may let q := 0 and r := b. Thus if $b \neq 0$ and $\nu(a) \leq \nu(b)$, then by (4) we get $a \mid b$. That is there is some $q \in R$ such that b = qa. Hence we are done by letting r := 0.
- (iv) By induction on $k \in \mathbb{N}$ it is clear that $\nu(m^k) = k\nu(m) = k$. Thus for $\nu(a) = k = \nu(m^k)$ we obtain $a \mid m^k$ and $m^k \mid a$. That is $a \approx m^k$ are associates and hence there is some $\alpha \in R^*$ such that $a = \alpha m^k$. And the uniqueness of α is clear, as R is an integral domain.
- (v) Let $\mathfrak{a} \leq_{\mathbf{i}} R$ be any ideal of R, combining (iii) and (2.64.(iii)) we know that R is a PID. That is there is some $a \in R$ such that $\mathfrak{a} = aR$. In case a = 0 we have $\mathfrak{a} = 0$, else using (iv) we may write a as $a = \alpha m^k$ for some $\alpha \in R^*$. Thus we have $\mathfrak{a} = aR = \alpha m^k R = m^k R$ as claimed.
- (vi) As $\nu(0) = \infty \ge 0$ and $\nu(1) = 0 \ge 0$ we have $0, 1 \in R$. Also we have $\nu(-1) = \nu((-1)(-1)) = 2\nu(-1)$ such that $\nu(-1) = 0$ and hence $-1 \in R$, too. If now $a, b \in R$ then by (3) we get $a + b \in R$ and by (2) also $ab \in R$. Altogether R is a subring of F. We will now prove that ν is a discrete valuation on R again. Properties (1), (2), (3) and (N) are

inherited trivially. And for (4) we are given $a, b \in R$ with $\nu(a) \leq \nu(b)$. In case b = 0 we have $a \cdot 0 = 0 = b$ and hence $a \mid b$ trivially. Thus assume $b \neq 0$, then we have $0 \leq \nu(a) \leq \nu(b) < \infty$ and hence $a \neq 0$, as well. Therefore we may let $x := ba^{-1} \in F$. Then by (2) we get $\nu(b) = \nu(xa) = \nu(x) + \nu(a)$, such that $\nu(x) = \nu(b) - \nu(a) \geq 0$. This again means $x \in R$ and hence $a \mid b$. It only remains to verify, that F truly is the quotient field of R. Thereby the inclusion " \supseteq " is trivial. Hence consider any $x \in F$, if $\nu(x) \geq 0$ then $x = x \cdot 1^{-1}$ and we are done. Else we have $\nu(x^{-1}) = -\nu(x) > 0$ and hence $x^{-1} \in R$. Thus we likewise obtain $x = 1 \cdot (x^{-1})^{-1}$.

Proof of (2.122):

- (a) \implies (c): If (R, ν) is a discrete valuation ring, then R already is a local ring (with maximal ideal $[\nu]$) and an Euclidean ring, due to (2.120). But the latter implies that R is a PID, by (2.64.(iii)). And of course R cannot be a field, as there is some $m \in R$ with $\nu(m) = 1$ (and hence we have both $m \neq 0$ and $m \notin R^*$ as else $\nu(m) = 0$).
- (c) \implies (d): As R is a PID it is a UFD according to (2.64.(ii)). Now consider two prime elements $p, q \in R$, that is the ideals pR and qR are non-zero prime ideals. Hence as R is a PID pR and qR already are maximal by (2.64.(i)). But as R also is local this means pR = qR.
- (d) ⇒ (b): Choose any 0 ≠ n ∈ R \ R* which is possible, as R is not a field. As R is an UFD we may choose some prime factor m of n and let 𝔅 := mR. Now consider any 0 ≠ a ∈ R, as R is an UFD a admits a primary decomposition a = αp₁...p_k. But by assumption any prime factor p_i is associated to m, that is a admits the representation a = ωm^k for some ω ∈ R* and k ∈ 𝔅. If we had a ∉ R* then we necessarily have k ≥ 1 and hence a ∈ mR = 𝔅. Thus we have proved R \ R* ⊆ 𝔅. And as m ∉ R* we have 𝔅 ∉ R such that R is a local ring with maximal ideal 𝔅, according to (2.113). And this again yields R \ 𝔅 = R* as claimed. Now suppose 0 ≠ a ∈ ∩_k m^kR, as we have seen we may write a = ωm^k for some ω ∈ R* and k ∈ 𝔅. But by assumption on a we also have a = bm^{k+1} for some b ∈ R. Dividing by m^k (R is an integral domain) we get ω = bm and hence m ∈ R* a contradiction. Thus we also got ∩_k m^kR = 0.
- (b) \implies (a): Let $\nu : R \to \mathbb{N} \cup \{\infty\} : a \mapsto \sup\{k \in \mathbb{N} \mid m^k \mid a\}$, then we will prove that ν is a discrete valuation on R: (1) if a = 0then for any $k \in \mathbb{N}$ we clearly have $m^k \mid a$ and hence $\nu(0) = \infty$. Conversely if $\nu(a) = \infty$, then we have $m^k \mid a$ for any $k \in \mathbb{N}$ and

hence $a \in \bigcap_k m^k R = 0$. (2) and (3) are easy by definition of ν - refer to the proof of (2.118.(ii)) for this. (4) Consider a and $b \in R$ with $\nu(a) \leq \nu(b)$. If b = 0 then $a \mid b$ is clear, otherwise we write $a = \alpha m^i$ and $b = \beta m^j$ for $i = \nu(a)$ and $j = \nu(b)$. By maximality of i we get $m \not\mid \alpha$ and hence $\alpha \in R \setminus mR = R^*$. Thus we may define $h := \alpha^{-1}\beta m^{j-i}$ and thereby obtain ha = b such that $a \mid b$. (N) suppose $m^2 \mid m$, then there was some $h \in R$ such that $hm^2 = m$ and hence hm = 1, which is $m \in R^*$. But in this case we had $R^* = R \setminus mR = \emptyset$ - a contradiction. Thus we have $\nu(m) \leq 1$ which clearly is $\nu(m) = 1$.

- (c) \implies (f): Any PID is a noetherian UFD and by (2.54) an UFD is a normal ring. And the maximal ideal \mathfrak{m} is non-zero, as we would else find $R^* = R \setminus \mathfrak{m} = R \setminus \{0\}$, which would mean that R was a field. Thus let $\mathfrak{p} \leq_i R$ be any prime ideal of R, if $\mathfrak{p} \neq 0$ is non-zero, then \mathfrak{p} already is maximal, due to (2.64.(i)). But in this case we necessarily have $\mathfrak{p} = \mathfrak{m}$, as R was assumed to be local.
- (f) ⇒ (e): First of all m is a finitely generated R-module, as R is a noetherian ring. Thus if we had m = m² = m m then (as JAC R = m) Nakayama's lemma (??) would imply m = 0 a contradiction. Thus we have m² ⊂ m, that is there is some m ∈ m with m ∉ m². In what follows we will prove m = mR. (1) First note that m ≠ 0 (as else m ∈ m²), thus by assumption and (2.20.(i)) we get

$$\sqrt{mR} = \bigcap \left\{ \mathfrak{p} \in \operatorname{spec} R \mid mR \subseteq \mathfrak{p} \right\} = \mathfrak{m}$$

In particular $\mathfrak{m} \subseteq \sqrt{mR}$ and hence there is some $k \in \mathbb{N}$ such that $\mathfrak{m}^k \subseteq mR$, by (2.20.(vii)). And of course we may choose k minimal with this property (that is $\mathfrak{m}^{k-1} \not\subseteq mR$). Clearly k = 0 cannot occur (as $m \in \mathfrak{m}$ and hence m is not a unit of R). And if k = 1 we are done, as in this case we get $\mathfrak{m} \subseteq mR \subseteq \mathfrak{m}$. Thus in the following we will assume $k \geq 2$ and derive a contradiction. (2) by minimality of k there is some $a \in \mathfrak{m}^{k-1}$ with $a \notin mR$. Let $a\mathfrak{m} := \{ab \mid b \in \mathfrak{m}\}$, as $a \in \mathfrak{m}^{k-1}$ we have $a\mathfrak{m} \subseteq \mathfrak{m}^{k-1}\mathfrak{m} = \mathfrak{m}^k \subseteq mR$. Now let $x := a/m \in E$, where E := QUOT R is the quotient field of R. Then clearly $x \notin R$ (that is $m \not\mid a$) as else $a \in mR$ in contradiction to the choice of a. (3) Now it is easy to see that $x\mathfrak{m} := \{xb \mid b \in \mathfrak{m}\}$ is a subset $x\mathfrak{m} \subseteq R$ of R: for any $b \in \mathfrak{M}$ we have $xb = ab/m \in (1/m) mR = R$. And in fact $x\mathfrak{M}$ even is an ideal $x\mathfrak{m} \leq_{\mathbf{i}} R$ of R $(0 \in x\mathfrak{m}$ is clear, and obviously $x\mathfrak{m}$ is closed under +, - and multiplication with elements of R). Now by construction we even get $x\mathfrak{m} \neq R$ (as else there would be some $b \in \mathfrak{m}$ such that xb = 1. But this would imply $m = ab \in a\mathfrak{m} \subseteq \mathfrak{m}^k \subseteq \mathfrak{m}^2$ (as we assumed $k \geq 2$) in contradiction to the choice of m). Thus $x\mathfrak{m}$ is a proper ideal of R and as R is a local ring with maximal ideal \mathfrak{m} this implies $x\mathfrak{m} \subseteq \mathfrak{m}$. (4) Let us now choose generators of \mathfrak{m} , say

 $\mathfrak{m} = b_1 R + \cdots + b_n R$. As $x\mathfrak{m} \subseteq \mathfrak{m}$ there are coefficients $a_{i,j} \in R$ (where $j \in 1 \dots n$) such that for any $i \in 1 \dots n$

$$xb_i = a_{i,1}b_1 + \dots + a_{i,n}b_n$$

Let us now define $b := (b_1, \ldots, b_n)$ and the $n \times n$ matrix $A := (a_{i,j})$ over R. Then the above equations can be reformulated as Ab = xb, that is $b \in \operatorname{kn}(x\mathbb{1} - A)$. Thereby $(x\mathbb{1} - A)$ is a $n \times n$ matrix over the field E, and as it has a kernel we have $\det(x\mathbb{1} - A) = 0 \in E$. Thus if $f := \det(t\mathbb{1} - A) \in R[t]$ is the characteristic polynomial of A then we have $f(x) = \det(x\mathbb{1} - A) = 0$. But as R was assumed to be normal and as f is a normed polynomial over R, this implies $x = a/m \in R$ or in other words $a \in mR$, a contradiction. This contradiction can only be solved in case k = 1 and then we have already seen $\mathfrak{M} = mR$.

• (e) \implies (c): First of all R is not a field, as \mathfrak{m} is a proper non-trivial ideal of R (that is $0 \neq \mathfrak{m} \neq R$). It remains to verify, that R is a PID, where $\mathfrak{m} = mR$ was assumed to be a principal ideal. To do this we first let $\mathfrak{z} := \bigcap_k \mathfrak{m}^k \leq_i R$, as R is noetherian \mathfrak{z} is a finitely generated R-module. And further we have $\mathfrak{m}\mathfrak{z} = \mathfrak{z}$ (" \subseteq " is clear and conversely if $a \in \mathfrak{z}$ then for any $k \in \mathbb{N}$ there is some $h_k \in R$ such that $a = h_k m^k$. Therefore $a/m = h_{k+1}m^k$ for any $k \in \mathbb{N}$ and hence $a/m \in \mathfrak{z}$ which is $a \in \mathfrak{m}\mathfrak{z}$ again). As $\mathfrak{m} = \operatorname{JAC} R$ the lemma of Nakayama (??) implies that $\mathfrak{z} = 0$. We now define the following map

$$\nu : \leq_{\mathbf{i}} R \to \mathbb{N} \cup \{\infty\} : \mathfrak{a} \mapsto \sup\{k \in \mathbb{N} \mid \mathfrak{a} \subseteq \mathfrak{m}^k\}$$

Obviously ν is well defined, as $\mathfrak{a} \subseteq R = \mathfrak{m}^0$ for any $\mathfrak{a} \leq_i R$. And if $\mathfrak{a} \neq R$, then \mathfrak{a} is contained in some maximal ideal, which is $\mathfrak{a} \subseteq \mathfrak{m}$ and hence $\nu(\mathfrak{a}) \geq 1$. Now suppose $\nu(\mathfrak{a}) = \infty$, this means $\mathfrak{a} \subseteq \bigcap_k \mathfrak{m}^k = 0$ and hence $\mathfrak{a} = 0$. Of course both 0 and R are principal ideals. Thus consider any ideal $\mathfrak{a} \leq_i R$ with $0 \neq \mathfrak{a} \neq R$. As we have just seen, this yields $1 \leq k := \nu(\mathfrak{a}) \in \mathbb{N}$. And as $\mathfrak{a} \not\subseteq \mathfrak{m}^{k+1}$ we may choose some $a \in \mathfrak{a}$ with $a \notin \mathfrak{m}^{k+1}$. As $\mathfrak{a} \subseteq \mathfrak{m}^k$ we in particular have $a \in \mathfrak{m}^k$, that is $a = \alpha m^k$ for some $\alpha \in R$. If we had $\alpha \in \mathfrak{m}$ then $a \in \mathfrak{m}^{k+1}$ would yield a contradiction. Hence $\alpha \in R \setminus \mathfrak{m} = R^*$ is a unit. Therefore we found $\mathfrak{m}^k = m^k R = \alpha m^k R = aR \subseteq \mathfrak{a} \subseteq \mathfrak{m}^k$ and hence $\mathfrak{a} = m^k R$ is a principal ideal. Altogether R is a PID.

Proof of (2.125):

(i) By definition of a local ring it suffices to check $R \setminus R^* \leq_i R$. As $R \neq 0$ we have $0 \in R \setminus R^*$. Now consider any $a, b \in R \setminus R^*$ and $r \in R$. Then

 $ra \in R \setminus R^*$, as else $a^{-1} = r(ar)^{-1}$ and in particular $-a \in R \setminus R^*$. It remains to show that $a+b \in R \setminus R^*$. Without loss of generality we may assume $a \mid b$ (else we may interchange a and b). That is b = ab for some $h \in R$ and hence a+b = a(1+h). Thus we have $a+b \in R \setminus R^*$, as else $a^{-1} = (1+h)(a+b)^{-1}$.

- (i) By assumption R is an integral domain. Thus regard any finitely generated ideal $\mathfrak{a} \leq_{i} R$. That is there are $a_{1}, \ldots, a_{k} \in R$ (where we may choose k minimally) such that $\mathfrak{a} = a_{1}R + \cdots + a_{k}R$. We need to show that \mathfrak{a} is a principal ideal, that is k = 1. Thus assume $k \neq 1$, then $\mathfrak{a} \neq a_{1}R$ (as k is minimal) and hence there is some $b \in \mathfrak{a}$ such that $b \notin a_{1}R$. Now write $b = a_{1}b_{1} + \cdots + a_{k}b_{k}$ and let $d := a_{2}b_{2} + \cdots + a_{k}b_{k}$. If we had $a_{1} \mid d$ then $d \in a_{1}R$ and hence $b = a_{1}b_{1} + d \in a_{1}R$, a contradiction. Thus we have $d \mid a_{1}$ as R is a valuation ring. But this means $a_{1} \in dR \subseteq a_{2}R + \cdots + a_{k}R$ and hence $\mathfrak{a} = a_{1}R + \cdots + a_{k}R = a_{2}R + \cdots + a_{k}R$ in contradiction to the minimality of k. This only leaves k = 1 which had to be shown.
- (ii) (c) \implies (b) is true by (2.120.(iii)) and (b) \implies (a) is clear. Thus it remains to verify (a) \implies (c): as R is a valuation ring, it is a Bezout domain, by (i). Thus if R also is noetherian it clearly is a PID. But R also is local by (i) and a local PID is a field or a DVR by (2.122).

Proof of (2.128):

It is clear that $\mathfrak{f} + \mathfrak{g}$, $\mathfrak{f} \cap \mathfrak{g}$ and $\mathfrak{f} \mathfrak{g}$ are *R*-submodules again. If now $r\mathfrak{f} \subseteq R$ and $s\mathfrak{g} \subseteq R$ then we can also check property (2) of fraction ideals

$$\begin{aligned} (rs)(\mathbf{f} + \mathbf{g}) &= s(r\mathbf{f}) + r(s\mathbf{g}) &\subseteq R \\ r(\mathbf{f} \cap \mathbf{g}) &\subseteq r\mathbf{f} &\subseteq R \\ (rs)(\mathbf{f}\mathbf{g}) &= (r\mathbf{f})(s\mathbf{g}) &\subseteq R \end{aligned}$$

Further $\mathfrak{f} : \mathfrak{g}$ is an *R*-submodule of *F* since: if $x, y \in \mathfrak{f} : \mathfrak{g}$ and $a \in R$ then $(ax + y)\mathfrak{g} \subseteq a\mathfrak{f} + \mathfrak{f} = \mathfrak{f}$. Thus it remains to prove that $\mathfrak{f} : \mathfrak{g} \leq_{\mathfrak{f}} R$ truly is a fraction ideal. To do this let $r\mathfrak{f} \subseteq R$ and $s\mathfrak{g} \subseteq R$. As $\mathfrak{g} \neq 0$ we may choose some $0 \neq g \in \mathfrak{g}$, then clearly $sg \in \mathfrak{g} \cap R$ and $sg \neq 0$, as *R* is an integral domain. But now $(rsg)(\mathfrak{f} : \mathfrak{g}) \subseteq R$ as for any $x \in \mathfrak{f} : \mathfrak{g}$ we get $(rsg)x = r(xsg) \in r\mathfrak{f} \subseteq R$.

Proof of (2.130):

(b) \implies (a) is trivial, by choosing $\mathfrak{g} := R : \mathfrak{f}$. Thus consider (a) \implies (b): that is we assume $\mathfrak{fg} = R$ for some $\mathfrak{g} \leq_{\mathfrak{f}} R$. Then by construction we have

Proof of (2.131):

(a) \implies (b): by assumption (a) we've got $1 \in R = \mathfrak{a}\mathfrak{g}$. Hence there are some $a_i \in \mathfrak{a}$ and $x_i \in \mathfrak{g}$ such that $1 = a_1x_1 + \ldots a_nx_n \in \mathfrak{a}\mathfrak{g}$. And as the x_i are contained in $x_i \in \mathfrak{g} = \mathfrak{a}^{-1} = R : \mathfrak{a}$ we have $x_i\mathfrak{a} \in R$ as claimed. (b) \implies (a): conversely suppose we are given such a_i and x_i then by definition $a_i \in \mathfrak{a}$ and $x_i \in R : \mathfrak{a}$. And as $a_1x_1 + \ldots a_nx_n = 1$ we also we have $R \subseteq \mathfrak{a}(R : \mathfrak{a}) \subseteq R$ and hence $R = \mathfrak{a}(R : \mathfrak{a})$. Thus we next concern ourselves with the implication (b) \implies (c): suppose we have chosen some $a_i \in \mathfrak{a}$ and $x_i \in F$ as noted under (b), then we define two *R*-module homomorphisms

$$\psi : R^n \to \mathfrak{a} : (r_1, \dots, r_n) \mapsto a_1 r_1 + \dots a_n r_n$$
$$\psi' : \mathfrak{a} \to R^n : a \mapsto (a x_1, \dots, a x_n)$$

Note that the latter is well-defined, since $x_i \mathfrak{a} \subseteq R$ by assumption. But if now $a \in \mathfrak{a}$ is chosen arbitrarily then we get

$$\psi\psi'(a) = aa_1x_1 + \dots + aa_nx_n = a$$

as $a_1x_1 + \cdots + a_nx_n = 1$. This is $\psi\psi' = 1$ on \mathfrak{a} . Now regard the following (obviously exact) chain of *R*-modules

$$0 \longrightarrow \operatorname{kn} \psi \xrightarrow{\subseteq} R^n \xrightarrow{\psi} \mathfrak{a} \longrightarrow 0$$

As we have just seen, this chain splits, as $\psi\psi' = 1$ and hence **a** is a direct summand of the free *R*-module R^n (which in particular means that **a** is projective) by virtue of

$$R^n \cong_{\mathrm{m}} \mathfrak{a} \oplus \operatorname{kn} \psi : r \mapsto (\psi(r), r - \psi' \psi(r))$$

Conversely suppose (c), that is $M = \mathfrak{a} \oplus P$, then we need to prove (b). To do this we define the *R*-module homomorphisms $\varrho : M \twoheadrightarrow \mathfrak{a} : (a, p) \mapsto a$ and $\iota : \mathfrak{a} \hookrightarrow M : a \mapsto (a, 0)$. Then clearly $\varrho \iota = \mathbb{1}$. As *M* is free by assumption it has an *R*-basis $\{m_i \mid i \in I\}$. And hence any $a \in \mathfrak{a}$ has a representation in the form

$$a = \varrho\iota(a) = \varrho\left(\sum_{i\in I} a_i m_i\right) = \sum_{i\in I} a_i \varrho(m_i)$$

Note that only finitely many of the a_i are non-zero, as these are the coefficients of the basis representation of $\iota(a)$. This representation allows us to define another *R*-module homomorphism

$$\pi_i : \mathfrak{a} \to R : a \mapsto a_i$$

Now consider any two non-zero elements $0 \neq a, b \in \mathfrak{a}$ then we see that $b\pi_i(a) = \pi_i(ba) = \pi_i(ab) = a\pi_i(b)$. And hence we may define an element $x_i \in F$ independently of the choice of $0 \neq a \in \mathfrak{a}$ by letting

$$x_i := \frac{\pi_i(a)}{a}$$

Note that only finitely many a_i were non-zero and hence only finitely many x_i are non-zero. The one property is easy to see: if $0 \neq a \in \mathfrak{a}$ is any element then we get $x_i a = \pi_i(a) \in R$ and hence $x_i \mathfrak{a} \subseteq R$. The other property requires only slightly more effort: just compute

$$a = \sum_{i \in I} \pi_i(a) \varrho(m_i) = \sum_{i \in I} a x_i \varrho(m_i) = a \left(\sum_{i \in I} x_i \varrho(m_i) \right)$$

Recall that only finitely many x_i were non-zero and for these let us denote $h_i := \rho(m_i)$. As a was non-zero we may divide by a to see that $1 = \sum_i x_i h_i$ which was all that remained to prove.

Proof of (2.132):

- (a) \implies (b): as $\mathfrak{a} \neq 0$ is non-zero $a \neq 0$ is non-zero and hence we may choose $\mathfrak{g} := (1/a)R$. Then we clearly get $\mathfrak{ag} = (aR)(1/aR) = R$.
- (b) \implies (a): as **a** is invertible, it is a projective *R*-module. But *R* is a local ring and hence any projective *R*-module already is free. Now **a** being free implies that **a** is a principal ideal (if the basis contained more than one element say b_1 and b_2 then $b_2b_1 + (-b_1)b_2 = 0$ would be a non-trivial linear combination).

Proof of (2.134):

We will now prove the equivalencies in the definition of Dedekind domains. Amongother useful statements we will thereby proof (2.136.(i)) already. Note that the order of proofs is somewhat unusual: (d) \iff (e) followed by (e) \implies (a) \implies (b) \implies (c) \implies (b) \implies (d).

- (d) \implies (e): consider any prime ideal $\mathfrak{q} \leq_i R$ and let $U := R \setminus \mathfrak{q}$, that is $R_{\mathfrak{q}} = U^{-1}R$. Then $R_{\mathfrak{q}}$ is a local ring by (2.115). And as Rwas assumed to be normal, so is $R_{\mathfrak{q}}$, by (2.109). And by (2.107) the spectrum of $R_{\mathfrak{q}}$ corresponds to $\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \subseteq \mathfrak{q}\}$. Yet if $\mathfrak{p} \neq 0$, then \mathfrak{p} already is maximal by assumption and hence $\mathfrak{p} = \mathfrak{q}$. Thus we have $\{\mathfrak{p} \in \operatorname{spec} R \mid \mathfrak{p} \subseteq \mathfrak{q}\} = \{0, \mathfrak{q}\}$. Thereby spec $R_{\mathfrak{q}}$ has precisely the prime ideals 0 (corresponding to 0 in R) and its maximal ideal (corresponding to \mathfrak{q}) in R. Altogether it satisfies condition (f) of DVRs.
- (e) ⇒ (d): by assumption R is a noetherian integral domain. Thus it remains to prove, that it is normal and satisfies spec R = smax R ∩ {0}. By assumption any localisation R_p is a DVR, hence a PID, hence an UFD and hence normal by (2.54). And as R is an integral domain this implies that R itself is normal, too by (2.110). Thus consider any prime ideal 0 ≠ p ≤_i R. It remains to prove that p is maximal. Thus we choose any maximal ideal ideal m with p ⊆ m. By assumption R_m is a DVR, and hence has precisely the prime ideals 0 and m_m (2.122). But as 0 ≠ p ⊆ m by (2.107) the localisation p_m is a non-zero prime ideal of R_m and hence p_m = m_m. Invoking the correspondence again we find p = m and hence p truly is maximal.
- R DVR ⇒ (a): let m be the maximal ideal of R and m a uniformizing parameter, that is m = mR. (1) If now 0 ≠ f ≤_fR is a non-zero fraction ideal, then a := f ∩ R ≤_i R is an ideal of R. And by definition there is some 0 ≠ r ∈ R such that rf ⊆ R. Recall that by (2.120.(iv)) in a DVR r ∈ R is uniquely represented, as r = ρm^k with ρ ∈ R* and k = ν(r) ∈ N. Among those r ∈ R with rf ⊆ R we now choose one with minimal k = ν(r). (2) We first note that a ≠ 0, just choose some 0 ≠ x ∈ f, then rx ∈ a and as r, x ≠ 0 we also have rx ≠ 0. Thus by (2.120.(v)) a is of the form a = mⁿR for some n ∈ N. (3) Now

$$f = m^{n-k} R$$

" \subseteq " if $x \in \mathfrak{f}$ then by (2) we have $rx \in \mathfrak{a} = m^n R$, say $rx = m^n p$. Therefore $x = m^n p/r = \varrho^{-1} p m^{n-k} \in m^{n-k} R$." \supseteq " If k = 0, then $r = \varrho \in R^*$ is a unit and hence $\mathfrak{f} = r\mathfrak{f} \subseteq R$. Thus we get $\mathfrak{f} = \mathfrak{a} = m^n R = m^{n-k} R$. Now suppose $k \ge 1$, as k has been chosen minimally, there is some $x = a/b \in \mathfrak{f}$ such that $m^{k-1}x \notin R$. That is $b \not\mid m^{k-1}a$ and hence $\nu(b) > \nu(m^{k-1}a) = k - 1 + \nu(a)$ by the properties of discrete valuations. However $rx \in R$ and hence $b \mid m^k a$. This yields $\nu(b) \le \nu(am^k) = k + \nu(a)$ altogether $\nu(b) = k + \nu(a)$. Thus if we represent $a = \alpha m^i$ with $\alpha \in R^*$ and $i = \nu(a)$ then $b = \beta m^j$ with $\beta \in R^*$ and $j = \nu(b) = k + i$. Therefore $x = a/b = \alpha \beta^{-1} m^{-k}$ such that $rx = \alpha \varrho \beta^{-1} \in R^*$. On the other hand $rx \in \mathfrak{a} = m^n R$ and hence $\mathfrak{a} = R$, that is n = 0. Thus $m^{-k} = \beta \alpha^{-1} x \in \mathfrak{f}$ such that $m^{n-k}R = m^{-k}R \subseteq \mathfrak{f}$. This settles the proof of the equality (3). But now we have seen, that $\mathfrak{f} = m^{n-k}R$ is a principal ideal, in particular it is invertible, with inverse $\mathfrak{f}^{-1} = m^{k-n}R$.

- (e) \implies (a): if R is a field, then $\mathfrak{f} = R$ is the one and only non-zero fraction ideal of R. And $\mathfrak{f} = R$ trivially is invertible, with inverse $\mathfrak{f}^{-1} = R$. Thus in the following we assume that R is not a field, then we choose any non-zero prime ideal $0 \neq \mathfrak{p} \leq_{\mathfrak{i}} R$ in R and let $U := R \setminus \mathfrak{p}$. That is $U^{-1}R = R_{\mathfrak{p}}$ and by assumption $R_{\mathfrak{p}}$ is a DVR. Thus consider a non-zero fraction ideal $0 \neq \mathfrak{f} \leq_{\mathfrak{f}} R$, then $0 \neq U^{-1}\mathfrak{f} \leq_{\mathfrak{f}} R_{\mathfrak{p}}$ is a fraction ideal of $R_{\mathfrak{p}}$. But as we have just seen this implies, that $U^{-1}R$ is invertible (regarding $R_{\mathfrak{p}}$). But by the remarks in section 2.11 this already yields that \mathfrak{f} is invertible (regarding R).
- (a) \implies (b) is trivial, so we will now prove (b) \implies (c): by assumption (b) any non-zero ideal is invertible and hence finitely generated (by the remarks in section 2.11). And as 0 trivially is finitely generated R is a noetherian ring. Now consider any non-trivial ideal $\mathfrak{a} \leq_i R$, that is $\mathfrak{a} \notin \{0, R\}$ and let $\mathfrak{a}_0 := \mathfrak{a}$. As $\mathfrak{a} \neq R$ we may choose some prime ideal $\mathfrak{p}_1 \in \operatorname{spec} R$ containing $\mathfrak{a} \subseteq \mathfrak{p}_1$, by (2.4.(ii)). Now let

$$\mathfrak{a}_1 := \mathfrak{a}_0(\mathfrak{p}_1)^{-1} = \mathfrak{a}_0(R:\mathfrak{p}_1) \subseteq \mathfrak{a}_0(R:\mathfrak{a}_0) = R$$

Here the inclusion $R : \mathfrak{p}_1 \subseteq R : \mathfrak{a}_0$ holds because of $\mathfrak{a}_0 \subseteq \mathfrak{p}_1$ and $\mathfrak{a}_0(R : \mathfrak{a}_0) = R$ is true because \mathfrak{a}_0 is invertible by assumption (a). Hence $\mathfrak{a}_1 \leq_i R$ is an ideal of R and by construction

$$\mathfrak{a} = \mathfrak{a}_0 = \mathfrak{p}_1 \mathfrak{a}_1$$

We will now construct an ascending chain $\mathfrak{a} = \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \ldots$ of ideals of R. Suppose we have already constructed $\mathfrak{a}_k \leq_i R$ and the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \operatorname{spec} R$ such that $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_k \mathfrak{a}_k$. If $\mathfrak{a}_k = R$ then we are done as we have already decomposed $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_k$ in this case. Thus assume $\mathfrak{a}_k \neq R$. Then we may choose any prime ideal \mathfrak{p}_{k+1} containing $\mathfrak{a}_k \subseteq \mathfrak{p}_{k+1}$ again. As for the case k = 1 above, we let $\mathfrak{a}_{k+1} := \mathfrak{a}_k(\mathfrak{p}_{k+1})^{-1}$ and find that $\mathfrak{a}_{k+1} \leq_i R$ is an ideal of R. Then by construction we get

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k \mathfrak{a}_k = \mathfrak{p}_1 \dots \mathfrak{p}_k \mathfrak{p}_{k+1} \mathfrak{a}_{k+1}$$

As R is noetherian this chain stabilizes at some point $\mathfrak{a}_n = \mathfrak{a}_{n+1}$ and by construction this means $\mathfrak{a}_{n+1} = \mathfrak{a}_n = \mathfrak{p}_{n+1}\mathfrak{a}_{n+1}$. As \mathfrak{a}_{n+1} is a finitely generated R-module the lemma of Dedekind implies that there is some $p \in \mathfrak{p}_{n+1}$ such that $(1-p)\mathfrak{a}_{n+1} = 0$. But as R is an integral domain and $\mathfrak{a}_{n+1} \neq 0$ this means that p = 1, which is absurd, since $\mathfrak{p}_{n+1} \neq R$ is prime. Thus the construction fails at this stage, which can only be if $\mathfrak{a}_n = R$. And as we have mentioned already this is $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n$. • (b) \implies (2.136.(i)): the existence of the factorisation of non-trivial ideals into prime non-zero ideals has been shown in (b) \implies (c) already. Hence it only remains to show that the factorisation is unique up to permutations. Thus assume $\mathfrak{p}_1 \ldots \mathfrak{p}_m = \mathfrak{q}_1 \ldots \mathfrak{q}_n$ where $0 \neq \mathfrak{p}_i$ and $\mathfrak{q}_j \leq_{\mathrm{i}} R$ are non-zero prime ideals. Whithout loss of generality we assume $m \leq n$ and use induction on n. The case m = 1 = n is trivial so we are only concerned with the induction step: by renumbering we may assume that \mathfrak{q}_1 is minimal among $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$. And as

$$\mathfrak{p}_1 \dots \mathfrak{p}_m \subseteq \bigcap_{i=1}^m \mathfrak{p}_i \subseteq \mathfrak{q}_1$$

and \mathfrak{q}_1 is prime (2.11.(ii)) implies that there is some $i \in 1 \dots m$ such that $\mathfrak{p}_i \subseteq \mathfrak{q}_1$. Now conversely as \mathfrak{p}_i is prime and $\mathfrak{q}_1 \dots \mathfrak{q}_n \subseteq \mathfrak{p}_i$ there is some $j \in 1 \dots n$ such that $\mathfrak{q}_j \subseteq \mathfrak{p}_i \subseteq \mathfrak{q}_1$. By minimality of \mathfrak{q}_1 this means $\mathfrak{q}_j = \mathfrak{q}_1$ and hence $\mathfrak{p}_i = \mathfrak{q}_1$. By renumbering we may assume i = 1. Then multiplying by $\mathfrak{p}_1^{-1} = \mathfrak{q}_1^{-1}$ yields $\mathfrak{p}_2 \dots \mathfrak{p}_m = \mathfrak{q}_2 \dots \mathfrak{q}_n$ so we are done by the induction hypothesis.

• (c) \implies any invertible prime ideal is maximal. Thus consider some invertible prime ideal $\mathfrak{p} \leq_{\mathbf{i}} R$, in particular $\mathfrak{p} \neq 0$. We will show that for any $u \in R \setminus \mathfrak{p}$ we get $\mathfrak{p} + uR = R$. Suppose we had $\mathfrak{p} + uR \neq R$ then by (b) we could decompose $\mathfrak{p} + uR = \mathfrak{p}_1 \dots \mathfrak{p}_m$ for some prime ideals $\mathfrak{p}_i \leq_{\mathbf{i}} R$. Now take to the quotient ring R/\mathfrak{p} , then by (1.43)

$$0 \neq (u+\mathfrak{p})^R/\mathfrak{p} = \mathfrak{p} + uR/\mathfrak{p} = \mathfrak{p}_1/\mathfrak{p} \dots \mathfrak{p}_m/\mathfrak{p}$$

But $(u + \mathfrak{p})(R/\mathfrak{p})$, being a principal ideal, is invertible. In particular any of its factors $\mathfrak{p}_i/\mathfrak{p}$ is invertible with inverse given to be

$$\left(\mathfrak{p}_{i}/\mathfrak{p}\right)^{-1} = \left(\frac{1}{u+\mathfrak{p}} R/\mathfrak{p}\right) \left(\prod_{i \neq j} \mathfrak{p}_{j}/\mathfrak{p}\right)$$

Now we open up a second line of argumentation: we decompose the ideal $\mathfrak{p} + u^2 R = \mathfrak{q}_1 \dots \mathfrak{q}_n$ and take to the quotient ring again

$$0 \neq (u^2 + \mathfrak{p})^R/\mathfrak{p} = \mathfrak{p} + u^2 R/\mathfrak{p} = \mathfrak{q}_1/\mathfrak{p} \cdots \mathfrak{q}_n/\mathfrak{p}$$

As $((u + \mathfrak{p})R/\mathfrak{p})^2 = (u^2 + \mathfrak{p})R/\mathfrak{p}$ we have found two decompositions of $(u^2 + \mathfrak{p})R/\mathfrak{p}$ into prime ideals - to be precise we found

$$\left(\mathfrak{p}_{1/\mathfrak{p}}\right)^{2} \cdots \left(\mathfrak{p}_{m/\mathfrak{p}}\right)^{2} = \mathfrak{q}_{1/\mathfrak{p}} \cdots \mathfrak{q}_{n/\mathfrak{p}}$$

 R/\mathfrak{p} also satisfies the assumption (c) because of the correspondence theorem and as any $\mathfrak{p}_i/\mathfrak{p}$ is invertible the decomposition is unique

up to permutations - note that these truly are the only assumptions that were used in the proof of (iii). Hence (by the uniqueness) we get 2m = n and $(\mathfrak{p}_1/\mathfrak{p}, \mathfrak{p}_1/\mathfrak{p}, \ldots, \mathfrak{p}_m/\mathfrak{p}, \mathfrak{p}_m/\mathfrak{p}) \longleftrightarrow (\mathfrak{q}_1/\mathfrak{p}, \ldots, \mathfrak{q}_n/\mathfrak{p})$. But by the correspondence theorem (1.43) again we can return to the original ring R getting $(\mathfrak{p}_1, \mathfrak{p}_1 \ldots, \mathfrak{p}_m, \mathfrak{p}_m) \longleftrightarrow (\mathfrak{q}_1, \ldots, \mathfrak{q}_n)$. Therefore

$$\begin{aligned} \mathfrak{p} + u^2 R &= \mathfrak{q}_1 \dots \mathfrak{q}_n \\ &= \mathfrak{p}_1 \mathfrak{p}_1 \dots \mathfrak{p}_m \mathfrak{p}_m \\ &= (\mathfrak{p} + uR)^2 \\ &= \mathfrak{p}^2 + u \mathfrak{p} + u^2 R \end{aligned}$$

Hence $\mathfrak{p} \subseteq \mathfrak{p} + u^2 R = \mathfrak{p}^2 + u(\mathfrak{p} + uR) \subseteq \mathfrak{p}^2 + uR$. Thus any $p \in \mathfrak{p}$ has a representation as p = a + ub where $a \in \mathfrak{p}^2$ and $b \in R$. Thus $ub = p - a \in \mathfrak{p}$ such that $b \in \mathfrak{p}$. This is $p = a + ub \in \mathfrak{p}^2 + u\mathfrak{p}$ and as p has been arbitrary $\mathfrak{p} \subseteq \mathfrak{p}^2 + u\mathfrak{p} = \mathfrak{p}(\mathfrak{p} + uR)$. Multiplying with \mathfrak{p}^{-1} this is $R \subseteq \mathfrak{p} + uR$ and hence finally $\mathfrak{p} + uR = R$.

• (c) \implies (b): we will first show that non-zero prime ideals $0 \neq \mathfrak{P} \leq_{i} R$ are invertible. To do this choose some $0 \neq a \in \mathfrak{P}$ and decompose $aR = \mathfrak{p}_1 \dots \mathfrak{p}_n$. As aR is invertible - with inverse $(aR)^{-1} = (1/a)R$ any \mathfrak{p}_i is invertible, as its inverse is just

$$\left(\mathfrak{p}_i\right)^{-1} = \frac{1}{a}R \prod_{i \neq j} \mathfrak{p}_j$$

As \mathfrak{p} is prime and $\mathfrak{p}_1 \ldots \mathfrak{p}_n = aR \subseteq \mathfrak{p}$ there is some $i \in 1 \ldots n$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. But \mathfrak{p}_i is invertible and hence maximal (see above) such that $\mathfrak{p}_i = \mathfrak{p}$. Thus \mathfrak{p} is invertible. If now $0 \neq \mathfrak{a} \leq_i R$ is any non-zero ideal then we decompose $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$ and as any \mathfrak{p}_i is now known to be irreducible we have $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_n^{-1}$ invertible.

- (b) \iff (c) and (b) \implies spec $R = \operatorname{smax} R \cup \{0\}$. We have just established the equivalence (b) \iff (c). And we have seen above that (because of (c)) any invertible prime ideal is maximal. But because of (b) *any* non-zero prime ideal already is invertible and hence maximal.
- (b) \implies (d): we have already seen in (b) \implies (c) that R is noetherian and that spec $R = \operatorname{smax} R \cup \{0\}$. Thus it only remains to show that R is normal. If R is a field already then there is nothing to prove, else let $F := \operatorname{QUOT} R$ and regard $x = a/b \in F$. If x is integral over R then R[x] is an R-module of finite rank $k + 1 := \operatorname{rank} R[x]$. Let now $r := b^k$ - as any element of R[x] is of the form $a_k x^k + \cdots + a_1 x + a_0$ (for some $a_i \in R$) we clearly have $rR[x] \subseteq R$ (in particular $R[x] \leq_f R$ is a fraction ideal of R). And hence for any $n \in \mathbb{N}$ we have $s_n := rx^n \in R$.

For any prime ideal $\mathfrak{p} \leq_i R$ let us now denote by $\nu_{\mathfrak{p}}(\mathfrak{a})$ the multiplicity of \mathfrak{p} in the primary decomposition of \mathfrak{a} , i.e. we let

$$\nu_{\mathfrak{p}}(\mathfrak{p}_{1}\dots\mathfrak{p}_{m}) := \#\{i \in 1\dots m \mid \mathfrak{p} = \mathfrak{p}_{i}\} \in \mathbb{N}$$

Then clearly $\nu_{\mathfrak{p}}$ turns the multiplication of ideals into an addition of multiplicities and hence $ra^n = s_n b^n$ turns into

$$\nu_{\mathfrak{p}}(rR) + n\nu_{\mathfrak{p}}(aR) = \nu_{\mathfrak{p}}(s_nR) + n\nu_{\mathfrak{p}}(bR)$$

Hence for any $n \in \mathbb{N}$ and any prime ideal $\mathfrak{p} \leq_i R$ we get the estimate

$$\nu_{\mathfrak{p}}(rR) + n(\nu_{\mathfrak{p}}(aR) - \nu_{\mathfrak{p}}(bR)) \geq \nu_{\mathfrak{p}}(s_nR) \geq 0$$

By choosing $n > \nu_{\mathfrak{p}}(rR)$ this implies that for any prime ideal \mathfrak{p} we have $\nu_{\mathfrak{p}}(bR) \leq \nu_{\mathfrak{p}}(aR)$. Writing down decompositions of aR and bR we hence find that $aR \subseteq bR$. But this is $b \mid a$ or in other words $x \in R$ which had to be shown.

Proof of (2.138):

The proof of the equivalencies in the definition (2.137) and the properties (2.138) of valuations of ideals in Dedekind domains is interwoven tightly. Thus we do not attempt to give separate proofs, but verify the properties and equivalencies simultaneously.

- $\mathfrak{b} \mid \mathfrak{a} \iff \mathfrak{a} \subseteq \mathfrak{b}$: if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, then $\mathfrak{b} \subseteq \mathfrak{a}$ is clear. Conversely suppose we had $\mathfrak{a} \subseteq \mathfrak{b}$. If additionally $\mathfrak{b} = 0$ then $\mathfrak{a} = 0$, too and hence we may already take $\mathfrak{c} := R$. Thus suppose $\mathfrak{b} \neq 0$ and let $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a} \leq_{\mathrm{f}} R$. Then $\mathfrak{c} \subseteq \mathfrak{b}^{-1}\mathfrak{b} = R$ and hence $\mathfrak{c} = \mathfrak{c} \cap R \leq_{\mathrm{i}} R$. But on the other hand $\mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{b}^{-1}\mathfrak{a} = \mathfrak{a}$ is clear, such that $\mathfrak{b} \mid \mathfrak{a}$.
- (i) In case $\mathfrak{m} \notin \mathcal{M}$ we may pick up $\mathfrak{m}_0 := \mathfrak{m}$ and k(0) := 0 reducing this to to the case $\mathfrak{m} \in \mathcal{M}$. And if $\mathfrak{m} \in \mathcal{M}$ then by renumbering we may assume that $\mathfrak{m} = \mathfrak{m}_1$. Thus regard $\mathfrak{a} := \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$, then $\mathfrak{a} \subseteq \mathfrak{m}^{k(1)}$ is clear and hence $\nu_{\mathfrak{m}}(\mathfrak{a}) \geq k(1)$, by definition of $\nu_{\mathfrak{m}}$. Thus assume $\nu_{\mathfrak{m}} > k(1)$, this means $\mathfrak{a} \subseteq \mathfrak{m}^{k(1)+1}$ and by what we have just shown there is some $\mathfrak{c} \leq_i R$ such that $\mathfrak{a} = \mathfrak{m}^{k(1)+1}\mathfrak{c}$. Therefore

$$\mathfrak{m}_1^{k(2)}\ldots\mathfrak{m}_n^{k(n)} = \mathfrak{m}^{-k(1)}\mathfrak{a} = \mathfrak{m}\mathfrak{c} \subseteq \mathfrak{m}$$

But as \mathfrak{m} is prime this means that there is some $i \in 2...n$ such that $\mathfrak{m}_i^{k(i)} \subseteq \mathfrak{m}$. Clearly $k(i) \neq 0$ as else $R \subseteq \mathfrak{m}$ and hence $\mathfrak{m}_i \subseteq \mathfrak{m}$ by the same argument. But \mathfrak{m}_i has been maximal and hence $\mathfrak{m}_i = \mathfrak{m} = \mathfrak{m}_1$ in contradition to the \mathfrak{m}_i being pairwise distinct.

- (ii) Decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ and $\mathfrak{b} = \mathfrak{m}_1^{l(1)} \dots \mathfrak{m}_n^{l(n)}$ as in the formulation of (iii). Also as in the proof of (i) we may also assume that $\mathfrak{m} = \mathfrak{m}_1$ (by picking up $\mathfrak{m}_0 := \mathfrak{m}$, k(0) := 0 and l(0) := 0 if necessary and renumbering). Then it is clear that $\mathfrak{ab} = \mathfrak{m}_1^{k(1)+l(1)} \dots \mathfrak{m}_n^{k(n)+l(n)}$. And using (i) the claim follows readily: $\nu_{\mathfrak{m}}(\mathfrak{ab}) = k(1) + l(1) = \nu_{\mathfrak{m}}(\mathfrak{a}) + \nu_{\mathfrak{m}}(\mathfrak{b})$.
 - $\mathfrak{a} \mid \mathfrak{b} \iff \forall \mathfrak{m} : \nu_{\mathfrak{m}}(\mathfrak{b}) \leq \nu_{\mathfrak{m}}(\mathfrak{a})$. Clearly if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ then by (ii) we get $\nu_{\mathfrak{m}}(\mathfrak{a}) = \nu_{\mathfrak{m}}(\mathfrak{b}) + \nu_{\mathfrak{m}}(\mathfrak{b}) \geq \nu_{\mathfrak{m}}(\mathfrak{b})$. Conversely decompose $\mathfrak{a} = \mathfrak{m}_{1}^{k(1)} \dots \mathfrak{m}_{n}^{k(n)}$ and $\mathfrak{b} = \mathfrak{m}_{1}^{l(1)} \dots \mathfrak{m}_{n}^{l(n)}$ once more. By (i) that is $k(i) = \nu_{\mathfrak{m}_{i}}(\mathfrak{a})$ and $l(i) = \nu_{\mathfrak{m}_{i}}(\mathfrak{b})$. Thus by assumption we have $l(i) \leq k(i)$ and may hence define $\mathfrak{c} = \mathfrak{m}_{1}^{k(1)-l(1)} \dots \mathfrak{m}_{n}^{k(n)-l(1)} \leq_{i} R$. Then by construction we immediately get $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$.
- (iii) First let $m(\mathfrak{m}) := \min\{\nu_{\mathfrak{m}}(\mathfrak{a}), \nu_{\mathfrak{m}}(\mathfrak{b})\}\$ for any $\mathfrak{m} \in \operatorname{smax} R$. Note that for $\mathfrak{m} = \mathfrak{m}_i$ we in particular get $m(\mathfrak{m}) = m(i)$ and if \mathfrak{m} is not contained in the \mathfrak{m}_i then $m(\mathfrak{m}) = 0$. And therefore we get

$$\mathfrak{m}_1^{m(1)}\ldots\mathfrak{m}_n^{m(n)} = \prod_{\mathfrak{m}} \mathfrak{m}^{m(\mathfrak{m})}$$

Now consider any ideal $\mathfrak{c} \leq_{i} R$, then by the equivalencies we have already proved for $\mathfrak{a} \mid \mathfrak{b}$ it is evident that we obtain the following chain of equivalent statements

$$\begin{array}{rcl} \forall \mathfrak{m} & : & \nu_{\mathfrak{m}}(\mathfrak{c}) \leq \nu_{\mathfrak{m}}(\mathfrak{a} + \mathfrak{b}) \\ \Longleftrightarrow & \mathfrak{a} + \mathfrak{b} & \subseteq & \mathfrak{c} \\ \Leftrightarrow & \mathfrak{a} \subseteq \mathfrak{c} \text{ and } \mathfrak{b} \subseteq \mathfrak{c} \\ \Leftrightarrow & \forall \mathfrak{m} & : & \nu_{\mathfrak{m}}(\mathfrak{c}) \leq \nu_{\mathfrak{m}}(\mathfrak{a}) \text{ and } \nu_{\mathfrak{m}}(\mathfrak{c}) \leq \nu_{\mathfrak{m}}(\mathfrak{b}) \\ \Leftrightarrow & \forall \mathfrak{m} & : & \nu_{\mathfrak{m}}(\mathfrak{c}) \leq m(\mathfrak{m}) \end{array}$$

Thus for a fixed $\mathfrak{m} \in \operatorname{smax} R$ we may regard $\mathfrak{c} := \mathfrak{m}^j$. And by (i) this satisfies $\nu_{\mathfrak{m}}(\mathfrak{c}) = j$, that is we may take $\nu_{\mathfrak{m}}(\mathfrak{c})$ to be any $j \in \mathbb{N}$ of our liking. And therefore the above equivalency immediately yields $\nu_{\mathfrak{m}}(\mathfrak{a} + \mathfrak{b}) = m(\mathfrak{m})$ and hence the equality for $\mathfrak{a} + \mathfrak{b}$ claimed.

- (iv) Consider any two non-zero ideals \mathfrak{a} , \mathfrak{b} of R, then by (iii) \mathfrak{a} and \mathfrak{b} are coprime (i.e. $\mathfrak{a} + \mathfrak{b} = R$) if and only if for any $\mathfrak{m} \in \operatorname{smax} R$ we get $\nu_{\mathfrak{m}}(\mathfrak{a}) = 0$ or $\nu_{\mathfrak{m}}(\mathfrak{b}) = 0$. In perticular for any $\mathfrak{m} \neq \mathfrak{m} \in \operatorname{smax} R$ and any $k, l \in \mathbb{N}$ we see that \mathfrak{m}^k and \mathfrak{n}^l are coprime. Thus the claim follows immediately from the original chinese remainder theorem (1.61).
- (v) If $\mathfrak{a} = aR$ is a principal ideal, then we may take $\mathfrak{b} := R$, then $\mathfrak{a} + \mathfrak{b} = R$ and $\mathfrak{a}\mathfrak{b} = \mathfrak{a} = aR$ are satisfied trivially. Thus suppose \mathfrak{a} is no principal ideal (in particular $\mathfrak{a} \neq 0$), then we may decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$

as usual. Now for any $i \in 1 \dots n$ pick up some $b_i \in R$ such that $b_i \in \mathfrak{m}_i^{k(i)}$ but $b_i \notin \mathfrak{m}_i^{k(i)+1}$ (therefore $\mathfrak{m}_i^{k(i)} \setminus \mathfrak{m}_i^{k(i)+1} \neq \emptyset$ is nonempty, as we else had $R = \mathfrak{m}_i$ by multiplication with $\mathfrak{m}_i^{-k(i)}$). Hence by (iv) there is some $b \in R$ that is mapped to $(b_i \in \mathfrak{m}_i^{k(i)+1})$ under the isomorphism of the chinese remainder theorem. That is for any $i \in 1 \dots n$ we have $b + \mathfrak{m}_i^{k(i)+1} = b_i + \mathfrak{m}_i^{k(i)+1}$. In particular we find $b \in \mathfrak{m}_i^{k(i)}$ and $b \notin \mathfrak{m}_i^{k(i)+1}$ again. This is to say that $\nu_{\mathfrak{m}_i}(b) = k_i$ for any $i \in 1 \dots n$. That is if we decompose bR then there are some $n \leq N \in \mathbb{N}$, $\mathfrak{m}_i \in \operatorname{smax} R$ and $1 \leq k(i) \in \mathbb{N}$ (where $i \in n + 1 \dots N$) such that

$$bR = \prod_{\mathfrak{m}} \mathfrak{m}^{k(\mathfrak{m})} = \prod_{i=1}^{N} \mathfrak{m}_{i}^{k(i)}$$

Note that n < N, if we had n = N then $bR = \mathfrak{a}$ already would be a principal ideal, which had been dealt with already. Thus if we let $\mathfrak{b} := \mathfrak{m}_{n+1}^{k(n+1)} \dots \mathfrak{m}_{N}^{k(N)}$, then it is evident, that $\mathfrak{a}\mathfrak{b} = bR$ is principal. But also by construction \mathfrak{a} and \mathfrak{b} satisfy $\nu_{\mathfrak{m}}(\mathfrak{a}) = 0$ or $\nu_{\mathfrak{m}}(\mathfrak{b}) = 0$ for any $\mathfrak{m} \in \operatorname{smax} R$. And as we have already argued in (iv) this is $\mathfrak{a} + \mathfrak{b} = R$.

Proof of (2.136):

Note that (i) has already been shown while proving the equivalencies in the definition of Dedekind domains on page 373. Thus it only remains to verify (ii) to (v), which we will do now:

(v) Let us denote the mapping (of course we still have to check the welldefinedness) given by Φ , that is $\Phi(a + \mathfrak{m}^k) := a/1 + \mathfrak{m}^k R_{\mathfrak{m}}$. Now consider any $a, b \in R$ and $u, v \notin \mathfrak{m}$, then in a first step, we will prove

$$\frac{a}{u} + \mathfrak{m}^k R_{\mathfrak{m}} + \frac{b}{v} + \mathfrak{m}^k R_{\mathfrak{m}} \iff av - bu \in \mathfrak{m}^k$$

If $av - bu \in \mathfrak{M}^k$ then (as $uv \notin \mathfrak{M}$) it is clear, that $(a/u) - (b/v) = (av - bu)/uv \in \mathfrak{M}^k R_{\mathfrak{M}}$. And thereby also $a/u + \mathfrak{M}^k R_{\mathfrak{M}} + b/v + \mathfrak{M}^k R_{\mathfrak{M}}$. Conversely let us assume $(av - bu)/uv = (a/u) - (b/v) \in \mathfrak{M}^k R_{\mathfrak{M}}$. That is there are some $m \in \mathfrak{M}^k$ and $w \notin \mathfrak{M}$ such that (av - bu)/uv = m/wand hence $w(av - bu) = muv \in \mathfrak{M}^k$. Therefore $w(av - bu)R \subseteq \mathfrak{M}^k$ such that by (2.137) and (2.138)

$$k = \nu_{\mathfrak{M}}(\mathfrak{M}^k) \leq \nu_{\mathfrak{M}}(w(av - bu)) = \nu_{\mathfrak{M}}(w) + \nu_{\mathfrak{M}}(av - bu)$$

Yet $w \notin \mathfrak{m}$ and hence $\nu_{\mathfrak{m}}(w) = 0$. Therefore we get $\nu_{\mathfrak{m}}(av - bu) = k$ and this translates into $av - bu \in \mathfrak{m}^k$ as claimed. And this immediately yields the equivalencies: $a + \mathfrak{m}^k = b + \mathfrak{m}^k$ iff $a - b \in \mathfrak{m}^k$ iff $\Phi(a + \mathfrak{m}^k) =$ $\Phi(b + \mathfrak{m}^k)$. And this has been the well-definedness and injectivity of Φ . Thus it remains to prove the surjectivity of Φ : we are given any $a/u + \mathfrak{m}^k R_{\mathfrak{m}}$ and need to find some $b \in R$ such that $a/u + \mathfrak{m}^k R_{\mathfrak{m}} = b/1 + \mathfrak{m}^k R_{\mathfrak{m}}$. Yet $u \notin \mathfrak{m}$ and \mathfrak{m} is a maximal ideal, that is R/\mathfrak{m} is a field and hence there is some $v \notin \mathfrak{m}$ such that $v + \mathfrak{m} = (u + \mathfrak{m})^{-1}$. That is $1 - uv \in \mathfrak{m}$ and in particular $(1 - uv)^k \in \mathfrak{m}^k$. But by the binomial rule we may compute

$$(1 - uv)^{k} = (-1)^{k} (uv - 1)^{k} = (-1)^{k} \sum_{i=0}^{k} \binom{k}{i} (uv)^{i} (-1)^{k-i}$$
$$= \sum_{i=0}^{k} (-1)^{i} \binom{k}{i} (uv)^{i} = 1 + u \sum_{i=1}^{k} (-1)^{i} \binom{k}{i} u^{i-1} v^{i}$$

That is we get $(1 - uv)^k = 1 + uq$ for some adequately chosen $q \in R$. Then we define b := -aq, now an easy computation yields $a - bu = a(1 + uq) = a(1 - uv)^k \in \mathbb{M}^k$. Thus by the above equivalency we find $\Phi(b + \mathbb{M}^k) = a/u + \mathbb{M}^k R_{\mathbb{M}}$.

(ii) (1) Let us first assume, that $\mathfrak{a} = \mathfrak{m}^k$ is a power of a maximal ideal $\mathfrak{m} \leq_i R$. If k = 0, then $\mathfrak{a} = R$ such that $R/\mathfrak{a} = 0$ such that we have nothing to prove. Thus assume $k \geq 1$, then by (v) R/\mathfrak{a} is isomorphic to $R_{\mathfrak{m}}/\mathfrak{a}R_{\mathfrak{m}}$. But as R is a Dedekind domain $R_{\mathfrak{m}}$ is a DVR (by (2.134.(e))) and in particular a PID (by (2.122.(c))). Therefore the quotient $R_{\mathfrak{m}}/\mathfrak{a}R_{\mathfrak{m}}$ is a principal ring (see section 2.6). Thus the isomorphy shows, that R/\mathfrak{a} is a principal ring. (2) Now consider any $0 \neq \mathfrak{a} \leq_i R$. We have already dealt with the case $\mathfrak{a} = R$ in (1).(k = 0). Thus suppose $\mathfrak{a} \neq R$ and decompose $\mathfrak{a} = \mathfrak{m}_1^{k(1)} \dots \mathfrak{m}_n^{k(n)}$ (with $n(i) \geq 1$). Then by the chinese remainder theorem in (2.138)

$$R/\mathfrak{a} \cong_{\mathrm{r}} R/\mathfrak{m}_1^{k(1)} \oplus \cdots \oplus R/\mathfrak{m}_n^{k(n)}$$

Now every $R/\mathfrak{m}_i^{k(i)}$ is a principal ring due to case (1). But the direct sum of principal rings is a principal again, due to the some remark in section 2.6. Thus the isomorphy shows, that R/\mathfrak{a} is a principal ring.

(iii) Consider any $\mathfrak{a} \leq_{\mathbf{i}} R$ and $0 \neq a \in R$, then by (ii) R/aR is a principal ring and hence \mathfrak{a}/aR is a principal ideal - say $\mathfrak{a}/aR = (b+aR)(R/aR)$ for some $b \in R$. As $b + aR \in \mathfrak{a}/aR$ it is clear that $b \in \mathfrak{a}$, in particular $aR + bR \subseteq \mathfrak{a}$. Now consider any $c \in \mathfrak{a}$, then $c + aR \in \mathfrak{a}/aR =$ (b + aR)(R/aR). That is there is some $v \in R$ such that c + aR =(b + aR)(v + aR) = bv + aR. Hence $c - bv \in aR$ which means that c - bv = au for some $u \in R$. And as $c = au + bv \in \mathfrak{a}$ has been arbitrary this also is $\mathfrak{a} \subseteq aR + bR$ (iv) Let us denote the set of all prime ideals that are not principal by \mathcal{P} - formally $\mathcal{P} := \{ \mathfrak{p} \in \operatorname{spec} R \mid \nexists p \in R : \mathfrak{p} = pR \}$. (1) clearly $n := \#\mathcal{P} < \infty$, as $\mathcal{P} \subseteq \operatorname{spec} R \setminus \{0\} = \operatorname{smax} R$ and the maximal spectrum of R is finite by assumption. If we have n = 0 then any prime ideal is principal. Thus if $\mathfrak{a} \leq_i R$ is any ideal decompose $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k$ where $\mathfrak{p}_i \leq_i R$ is prime (using (c)). Then $\mathfrak{p}_i = p_i R$ is principal and hence $\mathfrak{a} = aR$ is principal, too by letting $a := p_1 \dots p_k$. Thus it suffices to assume $n \geq 1$ and to derive a contradiction. (2) Let us denote $\mathfrak{b} := \mathfrak{p}_1 \dots \mathfrak{p}_n$ and $\mathfrak{a} := \mathfrak{p}_1 \mathfrak{b} = \mathfrak{p}_1^2 \mathfrak{p}_2 \dots \mathfrak{p}_n$. Then $\mathfrak{a} \neq \mathfrak{b}$, as else $R = \mathfrak{b} \mathfrak{b}^{-1} = \mathfrak{a} \mathfrak{b}^{-1} = \mathfrak{p}_1 - \mathfrak{a}$ contradiction (recall that $\mathfrak{b} \neq 0$, as R is an integral domain and hence we may apply (b)). (3) Next we claim that there is some $u \in \mathfrak{p}_1$ such that $u \notin \mathfrak{p}_1^2$, $u \notin \mathfrak{p}_i$ for any $i \in 2 \dots n$ and $\mathfrak{p}_1 = \mathfrak{a} + uR$. In fact $\mathfrak{a} \neq 0$, as R is an integral domain and hence R/\mathfrak{a} is a principal ring by (ii). And as $\mathfrak{p}_1/\mathfrak{a}$ is an ideal of R/\mathfrak{a} , there is some $u \in R$ such that

$$\mathfrak{P}_1/\mathfrak{a} = (u+\mathfrak{a})R/\mathfrak{a} = \mathfrak{a} + uR/\mathfrak{a}$$

By the correspondence theorem we find $\mathfrak{p}_1 = \mathfrak{a} + uR$ as $\mathfrak{a} \subseteq \mathfrak{p}_1$. Thus suppose $u \in \mathfrak{p}_1^2$, then $\mathfrak{p} = \mathfrak{a} + uR \subseteq \mathfrak{p}_1^2 \subseteq \mathfrak{p}_1$ and hence $\mathfrak{p}_1 = \mathfrak{p}_1^2$. Dividing by \mathfrak{p}_1 we would find $R = \mathfrak{p}_1$, a contradiction. And if we suppose $u \in \mathfrak{p}_i$ then likewise $\mathfrak{p}_1 = \mathfrak{a} + uR \subseteq \mathfrak{p}_i$. But as \mathfrak{p}_1 already is maximal this would imply $\mathfrak{p}_1 = \mathfrak{p}_i$ a contradiction (to $i \neq 1$). (4) now we prove that $uR = \mathfrak{p}_1 \mathfrak{q}_1 \dots \mathfrak{q}_m$ for some prime ideals $\mathfrak{q}_j \notin \mathcal{P}$. First of all uR admits a decomposition $uR = \mathfrak{q}_0 \dots \mathfrak{q}_m$ according to (b). Then $\mathfrak{q}_0 \dots \mathfrak{q}_m = uR \subseteq \mathfrak{p}_1$ and hence $\mathfrak{q}_0 \subseteq \mathfrak{p}_1$ for some $j \in 0 \dots m$, as \mathfrak{p}_1 is prime. Without loss of generality we may assume j = 0. Then $\mathfrak{q}_0 \subseteq \mathfrak{p}_1$ and this means $\mathfrak{q}_0 = \mathfrak{p}_1$, as \mathfrak{q}_0 is maximal (it is non-zero, prime). Thus we have established the decomposition $uR = \mathfrak{p}_1 \mathfrak{q}_1 \dots \mathfrak{q}_m$, now assume $\mathfrak{q}_j \in \mathcal{P}$ for some $j \in 1 \dots m$. If we had $\mathfrak{q}_j = \mathfrak{p}_i$ for some $i \in 2 \dots n$ then $u \in uR \subseteq \mathfrak{p}_1$ in contradiction to (3). And if we had $\mathfrak{q}_j = \mathfrak{p}_1$ then $u \in uR \subseteq \mathfrak{p}_1^2$ in contradiction to (3) again. (5) Thus the $\mathfrak{q}_i \notin \mathcal{P}$ are principal ideals, say $\mathfrak{q}_j = q_j R$. Then we let $q := q_1 \dots q_m$ and thereby find $uR = \mathfrak{p}_1 \mathfrak{q}_1 \dots \mathfrak{q}_m = \mathfrak{p}_1 (qR)$. Thus $uR \subseteq qR$, say u = qv for some $v \in R$. Then dividing by qR we find $\mathfrak{p}_1 = (u/q)R = vR$ such that $\mathfrak{p}_1 \in \mathcal{P}$ - a contradiciton at last.

Proof of (2.64):

It remains to prove statement (iv) of (2.64), as parts (i), (ii) and (iii) have already been proved on page 326. So by assumption every prime ideal \mathfrak{p} of R is generated by *one* element $\mathfrak{p} = pR$. In particular any prime ideal \mathfrak{p} is generated by *finitely many* elements. Thus R is notherian by property (d) in (2.27). Further $0 \neq \mathfrak{p} = pR$ implies p to be prime by (2.47.(ii)) (and as R is an integral domain this also means that p is irreducible due to (2.47.(v))). In particular any nonzero prime ideal $0 \neq \mathfrak{p} \leq_{i} R$ contains a prime element $p \in \mathfrak{p}$ (namely p with $\mathfrak{p} = pR$). And thus R is an UFD according to property (e) in (2.49). And by (??) this implies that R even is a normal domain. Now regard a non-zero prime ideal $0 \neq \mathfrak{p} = pR \leq_{i} R$ again and suppose $\mathfrak{p} \subseteq \mathfrak{a} \leq_{i} R$ for some ideal \mathfrak{a} of R. If $\mathfrak{a} \neq R$ then \mathfrak{a} is contained in some maximal ideal $\mathfrak{a} \subseteq \mathfrak{m} \trianglelefteq_i R$ of R. And as any maximal ideal \mathfrak{m} is prime, by assumption there is some $m \in R$ such that $\mathfrak{m} = mR$. Now $pR = \mathfrak{p} \subseteq \mathfrak{a} \subseteq \mathfrak{m} = mR$ implies $m \mid p$. That is there is some $q \in R$ such that qm = p. But as p is irreducible, this implies $q \in R^*$ (as $m \in R^*$ would imply $\mathfrak{m} = R$). That is $p \approx m$ and hence $\mathfrak{p} = \mathfrak{m}$ such that $\mathfrak{p} = \mathfrak{q}$, as well. This mean that \mathfrak{p} already is a maximal ideal of R. Altogether we have proved, that R is a normal, noetherian domain in which any non-zero prime ideal is maximal. But this means that R is a Dedekind domain according to (c) in (2.134). Now consider any ideal $\mathfrak{a} \leq R$. Then due to (b) (2.134) there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \leq_i R$ such that $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_n$. By assumption there are $p_i \in R$ such that $\mathfrak{p}_i = p_i R$ and hence $\mathfrak{a} = (p_1 R) \dots (p_n R) = (p_1 \dots p_n) R$ is a principal ideal, too. As \mathfrak{a} has been arbitrary, this finally means that R is a PID.

Proof of (2.116):

" \leq " as R is noetherian we may find finitely many $m_1, \ldots, m_k \in \mathfrak{m}$ such that $\mathfrak{m} = Rm_1 + \cdots + Rm_k$. We now choose k minimal with this property, that is $k = \operatorname{rank}_R(\mathfrak{m})$. Then it is clear that $\{m_i + \mathfrak{m}^2 \mid i \in 1 \ldots k\}$ is a generating set of $\mathfrak{m}/\mathfrak{m}^2$ (given any $n + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$ we may choose $a_1, \ldots, a_k \in R$ such that $n = a_1m_1 + \ldots a_kn_k$ and thereby $n + \mathfrak{m}^2 = a_1(m_1 + \mathfrak{m}^2) + \cdots + a_k(m_k + \mathfrak{m}^2)$). And thereby we have

$$\dim_E \left(\mathfrak{M}/\mathfrak{m}^2 \right) \leq \# \left\{ m_i + \mathfrak{m}^2 \mid i \in 1 \dots k \right\} \leq k = \operatorname{rank}_R(\mathfrak{m})$$

">" choose any E-basis $\{m_i + \mathfrak{m}^2 \mid i \in 1...k\}$ of $\mathfrak{m}/\mathfrak{m}^2$, then we let $\mathfrak{a} := Rm_1 + \cdots + Rm_k$. Then by construction we have $\mathfrak{m} = \mathfrak{a} + \mathfrak{m}^2$ (it is clear that $\mathfrak{m}^2 \subseteq \mathfrak{m}$ and as any $m_i \in \mathfrak{m}$ we also have $\mathfrak{a} \subseteq \mathfrak{m}$, together $\mathfrak{a} + \mathfrak{m}^2 \subseteq \mathfrak{m}$. Conversely if we are given any $n \in \mathfrak{m}$ then we may choose $a_i + \mathfrak{m} \in E$ such that $n + \mathfrak{m}^2 = \sum_i (a_i + \mathfrak{m})(m_i + \mathfrak{m}^2) = (\sum_i a_i m_i) + \mathfrak{m}^2$. Hence we have $n - \sum_i a_i m_i \in \mathfrak{m}^2$ which means $n \in \mathfrak{a} + \mathfrak{m}^2$). Now remark that JAC $R = \mathfrak{m}$, as R is a local ring. Further we have $\mathfrak{m}^2 = \mathfrak{m}\mathfrak{m}$ and \mathfrak{m} is a finitely generated R-module, as R is noetherian. Thus by the lemma of Nakayama (??.(??)) we find $\mathfrak{m} = \mathfrak{a}$ and in particular rank_R(\mathfrak{m}) $\leq k = \dim_E(\mathfrak{m}/\mathfrak{m}^2)$.