Commutative Algebra

Prof. Richard Pink

Summary
Fall Semester 2016
ETH Zürich

Final Version

8 February 2017

This summary contains the definitions, theorems and most relevant examples from the lecture course, without proofs or further explanations. For these, see your own notes and useful textbooks, as listed in the section on literature.

The summary was compiled with the help of Nadir Bayo, Zheng Gong, and Niklas Itänen.

Content

1 Ouverture

Fix an algebraically closed field K, an integer $n \geqslant 0$, and consider the ring

$$R := K[X_1, \ldots, X_n].$$

Definition: The *affine algebraic variety* defined by a subset $S \subset R$ is the subset

$$V(S) := \{x \in K^n \mid \forall f \in S\colon f(x) = 0\} \subset K^n.$$

Basic Properties:

(a) $V(\varnothing) = K^n$.

(b) $V(\{1\}) = \varnothing$.

(c) $\bigcap_{i\in I} V(S_i) = V(\bigcup_{i\in I}(S_i))$ for any non-empty collection of subsets $S_i \subset R$.

(d) $V(S) \cup V(S') = V(\{f \cdot g \mid f \in S,\ g \in S'\})$.

That is, the $V(S)$ are the closed sets of a topology on K^n.

Definition: This topology is called the *Zariski topology* on K^n.

Note: The Zariski topology on $\mathbb{C}^n$ is coarser than the usual topology.

Example: For $n = 1$ the Zariski closed subsets of K are K and all finite subsets. This topology is called the *cofinite topology.* For example $\mathbb{Z} \subset \mathbb{C}$ is Zariski dense.

Example: For $n = 2$ the variety $V\big(Y(X^2 + Y^2 - 1) \cdot \{X - 1, Y - 1\}\big)$ is the union of the x-axis $y = 0$, the unit circle $x^2 + y^2 = 1$, and the single point $(1, 1)$.

Definition: For any subset $X \subset K^n$ we consider the subset

$$I(X) := \{f \in R \mid \forall x \in X\colon f(x) = 0\} \subset R.$$

Proposition: For any subsets $S, S' \subset R$ and $X, X' \subset K^n$ we have:

(a) $X \subset V(S) \iff S \subset I(X)$

(b) $V(S \cup S') = V(S) \cap V(S')$

(b′) $I(X \cup X') = I(X) \cap I(X')$

(c) $S \subset S' \implies V(S) \supset V(S')$

(c′) $X \subset X' \implies I(X) \supset I(X')$

(d) $S \subset I(V(S))$

(d′) $X \subset V(I(X))$

(e) $V(S) = V(I(V(S)))$

(e′) $I(X) = I(V(I(S)))$

Definition: The *radical* of an ideal $\mathfrak{a} \subset R$ is

$$\mathrm{Rad}(\mathfrak{a}) := \{a \in R \mid \exists n \geqslant 1 : a^n \in \mathfrak{a}\}.$$

Proposition: This is an ideal containing $\mathfrak{a}$.

Definition: An ideal $\mathfrak{a}$ with $\mathfrak{a} = \mathrm{Rad}(\mathfrak{a})$ is called *radical.*

Fact: (a) $I(X)$ is an ideal.

(b) $V(S) = V((S))$.

(c) $I(X)$ is radical.

Theorem: *(Hilbert's Nullstellensatz)* For any ideal $\mathfrak{a} \subset R$ we have

$$I(V(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a}).$$

Consequence: The maps V and I induce mutually inverse bijections

$$\begin{array}{ccc} \mathcal{P}(R) & \overset{V}{\searrow\!\swarrow} \overset{I}{} & \mathcal{P}(K^n) \\ \cup & & \cup \\ \{I(X) \mid X \subset K^n\} & \underset{bij.}{\rightleftarrows} & \{V(S) \mid S \subset R\} \\ \| & & \| \\ \{\text{radical ideals of } R\} & & \{\text{Zariski closed subsets of } K^n\} \end{array}$$

Example: For any point $x = (x_1, \ldots, x_n) \in K^n$ the following ideal is maximal:

$$I(\{x\}) = \mathfrak{m}_x := (X_1 - x_1, \ldots, X_n - x_n).$$

Theorem: *(Weak Nullstellensatz)* The ideals of the form $\mathfrak{m}_x$ are precisely all maximal ideals of $K[X_1, \ldots, X_n]$.

Proposition: For any ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \subset R$ we have:

(a) $V(\mathfrak{a}_1 + \ldots + \mathfrak{a}_r) = V(\mathfrak{a}_1) \cap \ldots \cap V(\mathfrak{a}_r)$

(b) $V(\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r) = V(\mathfrak{a}_1) \cup \ldots \cup V(\mathfrak{a}_r)$

(c) $V(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_r) = V(\mathfrak{a}_1) \cup \ldots \cup V(\mathfrak{a}_r)$

Example: $V(Y(X^2+Y^2-1)\cdot\{X-1, Y-1\}) = V(Y) \cup V(X^2+Y^2-1) \cup V((X-1, Y-1))$.

Definition: A topological space is called

(a) *connected* if it is non-empty and not a union of two *disjoint* proper closed subsets;

(b) *irreducible* if it is non-empty and not a union of two proper closed subsets.

Clearly irreducible implies connected.

(Strangely, some people allow the empty set to be connected.)

Proposition: A Zariski closed subset $X \subset K^n$ is irreducible if and only if $I(X)$ is a prime ideal.

Examples: (a) K^n is irreducible with $I(K^n) = (0)$.

(b) Every singleton $\{x\}$ is irreducible with the prime ideal $\mathfrak{m}_x$.

(c) $V(Y)$ and $V(X^2+Y^2-1)$ are irreducible in K^2.

Theorem: For any Zariski closed $X \subset K^n$ there exist $r \geqslant 0$ and irreducible Zariski closed subsets X_i of K^n, none contained in any other, such that $X = X_1 \cup \ldots \cup X_r$. Furthermore r, and the X_i up to permutation, are unique.

Equivalently:

Theorem: *(Prime decomposition)* For any radical ideal $\mathfrak{a} \subset R$ there exist $r \geqslant 0$ and prime ideals $\mathfrak{p}_i$ of R, none contained in any other, such that $\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$. Furthermore r, and the $\mathfrak{p}_i$ up to permutation, are unique.

Definition: For a Zariski closed $X \subset K^n$ we call the ring $R/I(X)$ the *coordinate ring* of X. There exists a natural injective homomorphism

$$\begin{array}{ccc} R/I(X) & \hookrightarrow & \mathrm{Maps}(X,K) \\ f+I(X) & \mapsto & (x \mapsto f(x)). \end{array}$$

Proposition: X is irreducible if and only if $R/I(X)$ is an integral domain.

Definition: Then $K(X) := \mathrm{Quot}(R/I(X))$ is called the *function field* of X.

Definition: Then the *dimension of* X is $\dim(X) := \mathrm{trdeg}(K(X)/K)$.

Generalization: In the above discussion, the study of a Zariski closed subset $X \subset K^n$ translates into the study of its coordinate ring $R/I(X)$. But these rings are very special in that:

- $I(X)$ is a radical ideal,
- The base field K is algebraically closed,
- The ring R contains a field (unlike $\mathbb{Z}$),
- R is finitely generated.

Get rid of radical ideals: Working with arbitrary ideals will permit us to count multiplicities correctly, as in the following example:

Example: Consider the unit circle $C := V(X^2+Y^2-1) \subset K^2$, where K is algebraically closed of characteristic $\neq 2$. For any $a \in K$ consider the intersection of C with the line $L_a := V(Y-a)$, that is

$$C \cap L_a = V(Y-a, X^2-(1-a^2)).$$

This consists of two distinct points for $a \neq \pm 1$, but of the single point $(\pm 1, 0)$ for $a = \pm 1$. In the latter case the intersection is given by the non-radical ideal $(Y \mp 1, X^2)$

with radical $(Y \mp 1, X)$. Here the ideal $(Y \mp 1, X^2)$ retains the information about the multiplicity of this "double point", whereas the radical does not.

Get rid of algebraic closure: Let K be a non-necessarily algebraically closed field, set $R := K[X_1, \dots X_n]$, and consider an ideal $\mathfrak{a} \subset R$. Then $R/\mathfrak{a}$ can be viewed as the coordinate ring of an affine algebraic variety over K, in that it contains all information about the L-valued points for all overfields L of K:

Proposition: For any field $L \supset K$ we have a natural bijection

$$\begin{array}{rcl} \{x \in L^n \mid \forall f \in \mathfrak{a}\colon f(x) = 0\} & \longleftrightarrow & \mathrm{Hom}_{K\text{-alg}}(R/\mathfrak{a}, L), \\ x & \longmapsto & (f + \mathfrak{a} \mapsto f(x)). \end{array}$$

Example: $\mathbb{Q}[X,Y]/(X^2 + Y^2 + 1)$ is the coordinate ring of an affine conic with no points over $\mathbb{Q}$ or $\mathbb{R}$, but which over $\mathbb{C}$ becomes isomorphic to the unit circle.

Get rid of subfields: Dropping the assumption that the ring contain a field allows us to speak of "algebraic varieties" defined over an arbitrary ring, say over $\mathbb{Z}$:

Example: Define $\overline{R} := \mathbb{Z}[X,Y]/(X^2 + Y^2 + 1)$. Then for every field L we have the following natural bijection:

$$\{(x,y) \in L^2 \mid x^2 + y^2 + 1 = 0\} \quad \longleftrightarrow \quad \mathrm{Hom}_{\mathbb{Z}\text{-alg}}(\overline{R}, L).$$

Get rid of finiteness conditions: This allows many useful generalizations:

Example: All sorts of rings from analysis.

Example: The power series ring $K[[X_1, \dots, X_n]]$.

Let now R be an arbitrary ring.

Definition: (a) The set of all prime ideals of R is called the *spectrum* of R and is denoted by $\mathrm{Spec}\, R$.

(b) The subset of all maximal ideals of R is called the *maximal spectrum* of R and is denoted by $\mathrm{Specmax}\, R$.

Definition: For any ideal $\mathfrak{a} \subset R$ set

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}\, R \mid \mathfrak{a} \subset \mathfrak{p}\}.$$

Note: There is a natural bijection

$$\begin{array}{rcl} V(\mathfrak{a}) & \longleftrightarrow & \mathrm{Spec}(R/\mathfrak{a}) \\ \mathfrak{p} & \longmapsto & \mathfrak{p}/\mathfrak{a} \end{array}$$

Proposition: These sets form the closed sets of a topology on $\operatorname{Spec} R$.

Definition: This topology is called the *Zariski topology* on $\operatorname{Spec} R$.

Definition: For any $g \in R$ set $D_g := (\operatorname{Spec} R) \setminus V((g)) = \{\mathfrak{p} \in \operatorname{Spec} R \mid g \notin \mathfrak{p}\}$.

Exercise: These form a basis for the Zariski topology on $\operatorname{Spec} R$.

Example: $\operatorname{Spec} K[X] = \{(0)\} \cup \operatorname{Specmax} K[X]$.

Example: $\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \operatorname{Specmax} \mathbb{Z} = \{(0)\} \cup \{(p) \mid p \in \mathbb{Z} \text{ prime}\}$.

Example: The spectrum of $\mathbb{Z}[X]$ consists of the minimal ideal (0), the maximal ideals (p, f) for all primes p and all $f \in \mathbb{Z}[X]$ such that $f \bmod (p)$ is irreducible, and the intermediate ideals (f) for all irreducible elements $f \in \mathbb{Z}[X]$.

Definition: The *residue field* of a point $\mathfrak{p} \in \operatorname{Spec} R$ is the field

$$k(\mathfrak{p}) := \operatorname{Quot}(R/\mathfrak{p}).$$

Definition: The *value* of an element $f \in R$ at a point $\mathfrak{p} \in \operatorname{Spec} R$ is the element

$$\text{“}f(\mathfrak{p})\text{”} := \frac{f + \mathfrak{p}}{1 + \mathfrak{p}} \in k(\mathfrak{p}).$$

Note: For the maximal ideal $\mathfrak{m}_x \subset R := K[X_1, \ldots, X_n]$ associated to a point $x \in K^n$, the usual value $f(x) \in K$ corresponds to the value $f(\mathfrak{m}_x)$ by the natural isomorphism:

$$K \xrightarrow{\sim} R/\mathfrak{m}_x = k(\mathfrak{m}_x),\ a \mapsto a + \mathfrak{m}_x.$$

In this sense the notion is *backward compatible.*

Example: Any integer a determines the “value” $a \bmod (p) \in \mathbb{F}_p$ at every prime p, as well as the “value” $\frac{a}{1} \in \mathbb{Q}$ at (0).

2 Localization

Fix a ring R.

Definition: A *multiplicative subset* $S \subset R$ is one with

(a) $1 \in S$, and

(b) $\forall s, s' \in S\colon ss' \in S$.

Construction: Fix a multiplicative subset $S \subset R$. For any $(a, s), (a', s') \in R \times S$, define

$$(a, s) \sim (a', s')\colon \iff \exists t \in S\colon (as' - a's)t = 0.$$

Proposition: (a) This is an equivalence relation.

Let $S^{-1}R$ be the set of the equivalence classes $[(a, s)]$.

(b) There exist well defined maps $+, \cdot\colon S^{-1}R \times S^{-1}R \to S^{-1}R$ such that

$$\begin{aligned} [(a, s)] + [(a', s')] &:= [(as' + a's, ss')] \\ [(a, s)] \cdot [(a', s')] &:= [(aa', ss')] \end{aligned}$$

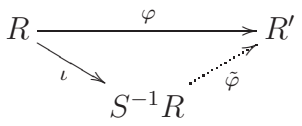
(c) With the neutral elements $0_{S^{-1}R} := [(0, 1)]$ and $1_{S^{-1}R} := [(1, 1)]$ and the above defined maps $S^{-1}R$ is a ring.

(d) The map $\iota\colon R \to S^{-1}R$, $a \mapsto [(a, 1)]$ is a ring homomorphism satisfying $\iota(S) \subset (S^{-1}R)^\times$.

Abbreviation: We usually write $\frac{a}{s} := [(a, s)]$.

Definition: We call $S^{-1}R$ the *localization of R with respect to S*.

Proposition: *(Universal Property)* For any ring R' and any ring homomorphism $\varphi\colon R \to R'$ such that $\varphi(S) \subset R'^\times$ there exists a unique ring homomorphism $\tilde{\varphi}\colon S^{-1}R \to R'$ such that $\tilde{\varphi} \circ \iota = \varphi$, i.e. the following diagram commutes:



Remark: The universal property characterizes the pair $(S^{-1}R, \iota)$ up to unique isomorphism and could therefore be used as definition of the localization.

Basic Properties: (a) $\ker(\iota) = \{a \in R \mid \exists s \in S\colon as = 0\}$.

(b) $S^{-1}R = 0$ if and only if $0 \in S$.

(c) If $R \neq 0$, then ι is injective if and only if S contains neither zero divisors nor the zero element.

(d) ι is an isomorphism if and only if $S \subset R^\times$.

Example: For any integral domain R we have $(R \smallsetminus \{0\})^{-1}R = \mathrm{Quot}(R)$.

Aside: Consider a ring homomorphism $\varphi\colon R \to R'$.

Definition: (a) The *pullback* (or *contraction*) of an ideal $\mathfrak{a}' \subset R'$ is the ideal

$$\varphi^*\mathfrak{a}' := \varphi^{-1}(\mathfrak{a}') \text{ of } R.$$

(b) The *pushforward* (or *extension*) of an ideal $\mathfrak{a} \subset R$ is the ideal

$$\varphi_*\mathfrak{a} := R' \cdot \varphi(\mathfrak{a}) \text{ of } R'.$$

Basic Properties: (a) $\mathfrak{a} \subset \varphi^*\mathfrak{a}' \iff \varphi_*(\mathfrak{a}) \subset \mathfrak{a}'$.

(b) $\mathfrak{a} \subset \varphi^*\varphi_*\mathfrak{a}$.

(c) $\varphi_*\varphi^*\mathfrak{a}' \subset \mathfrak{a}'$.

(d) $\varphi_*\mathfrak{a} = \varphi_*\varphi^*\varphi_*\mathfrak{a}$.

(e) $\varphi^*\varphi_*\varphi^*\mathfrak{a}' = \varphi^*\mathfrak{a}'$.

Proposition: For any prime ideal $\mathfrak{q} \subset R'$, the ideal $\varphi^*\mathfrak{q}$ is a prime ideal of R, and there are natural injective homomorphisms

$$\begin{array}{ccc} R/\varphi^*\mathfrak{q} & \hookrightarrow & R'/\mathfrak{q} \\ \cap & & \cap \\ k(\varphi^*\mathfrak{q}) & \hookrightarrow & k(\mathfrak{q}) \end{array}$$

We return to the homomorphism $\iota\colon R \to S^{-1}R$.

Proposition: (a) For any ideal $\mathfrak{a} \subset R$, we have $\iota_*\mathfrak{a} = \{\frac{a}{s} \mid a \in \mathfrak{a},\ s \in S\}$.

(b) For any ideal $\mathfrak{a} \subset R$, we have $\iota_*\mathfrak{a} = (1)$ if and only if $\mathfrak{a} \cap S \neq \varnothing$.

(c) For any ideal $\mathfrak{b} \subset S^{-1}R$ we have $\iota_*\iota^*\mathfrak{b} = \mathfrak{b}$.

(d) We have mutually inverse bijections

$$\begin{array}{ccc} \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \varnothing\} & \longleftrightarrow & \operatorname{Spec} S^{-1}R \\ \mathfrak{p} & \longmapsto & \iota_*\mathfrak{p} \\ \iota^*\mathfrak{q} & \longmapsfrom & \mathfrak{q} \end{array}$$

(e) $\mathfrak{q} \subset \mathfrak{q}' \iff \iota^*\mathfrak{q} \subset \iota^*\mathfrak{q}'$.

(f) There exists a natural isomorphism $k(\iota^*\mathfrak{q}) \xrightarrow{\sim} k(\mathfrak{q})$.

Special Case: For any $g \in R$ set $S := \{g^i \mid i \geqslant 0\}$ and abbreviate $R_g := S^{-1}R$. Then Proposition (d) above yields a natural bijection:

$$D_g := \{\mathfrak{p} \in \operatorname{Spec} R \mid g \notin \mathfrak{p}\} \rightleftarrows \operatorname{Spec} R_g$$

We can therefore view R_g as the coordinate ring of D_g.

Special Case: For any integral domain R and any multiplicative subset $S \subset R \smallsetminus \{0\}$, there is a natural isomorphism

$$S^{-1}R \xrightarrow{\sim} \{\tfrac{a}{s} \mid a \in R,\, s \in S\} \subset \mathrm{Quot}(R).$$

Example: For $g \in K[X] \smallsetminus \{0\}$, we have $K[X]_g \cong \{\frac{f}{g^i} \mid f \in K[X],\, i \geqslant 0\} \subset K(X)$.

Note: The passage to open subsets of a topological space can reasonably be called a *localization* (of any question we might be interested in).

Note: The example shows that shrinking the space often has the effect of enlarging the ring; so we are looking locally at the space, not locally at the ring.

Definition: (a) A ring with exactly one maximal ideal is called a *local ring.*

(b) A ring with at most finitely many maximal ideals is called a *semilocal ring.*

Proposition: For any ring R and any ideal $\mathfrak{m} \subsetneqq R$, the following are equivalent:

(a) R is a local ring with maximal ideal $\mathfrak{m}$.

(b) Every element of $R \smallsetminus \mathfrak{m}$ is a unit in $R^\times$.

(c) $\mathfrak{m}$ is a maximal ideal and for any $m \in \mathfrak{m}$ we have $1 + m \in R^\times$.

Special Case:

Proposition: For any prime ideal $\mathfrak{p} \subset R$:

(a) The set $R \smallsetminus \mathfrak{p}$ is multiplicative.

(b) The ring $R_\mathfrak{p} := (R \smallsetminus \mathfrak{p})^{-1}R$ is a local ring with maximal ideal $\mathfrak{p}_\mathfrak{p} := \iota_*\mathfrak{p}$.

Definition: $R_\mathfrak{p}$ is called the *localization of R at $\mathfrak{p}$*.

Note: $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong k(\mathfrak{p})$ naturally by Proposition (f) above.

Example: For $R = K[X_1, \ldots, X_n]$ and $\mathfrak{m} = (X_1, \ldots, X_n)$ we get

$$\begin{aligned} R_\mathfrak{m} &\cong \{\tfrac{f}{g} \mid f, g \in R,\, g(0) \neq 0\} \subset K(X_1, \ldots, X_n) \\ &= \{\text{germs of rational functions defined on a neighborhood of } 0\}. \end{aligned}$$

Example: Ring of germs on holomorphic functions defined on a neighborhood of 0.

Example: For $R = K[X, Y]$ and $\mathfrak{p} = (Y)$ we get

$$\begin{aligned} R_\mathfrak{p} &\cong \{\tfrac{f}{g} \mid f, g \in R,\, Y \nmid g\} \subset K(X, Y) \\ &= \{\text{germs of rational functions defined on almost all points of the } x\text{-axis}\}. \end{aligned}$$

Example: For $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$ for a prime p we get

$$\mathbb{Z}_{(p)} \cong \{\tfrac{a}{b} \mid a, b \in \mathbb{Z},\, p \nmid b\} \subset \mathbb{Q}.$$

3 Radicals

Definition: (a) An element $a \in R$ is called *nilpotent* if there exists $n \geqslant 1$ with $a^n = 0$.

(b) The set $\operatorname{rad}(R)$ of all nilpotent elements is called the *nilradical* (or *radical*) of R.

Fact: For any ideal $\mathfrak{a} \subset R$ we have $\operatorname{rad}(R/\mathfrak{a}) = \operatorname{Rad}(\mathfrak{a})/\mathfrak{a}$.

Proposition: (a) $\operatorname{rad}(R)$ is an ideal of R.

(b) $R/\operatorname{rad}(R)$ has only 0 as nilpotent element.

(c) $\operatorname{rad}(R)$ is the intersection of all prime ideals of R.

Definition: The intersection of all maximal ideals of R is called the *Jacobson radical of* R and is denoted by $j(R)$.

Note: We always have $\operatorname{rad}(R) \subset j(R)$.

Example: For R local with the maximal ideal $\mathfrak{m}$ we have $j(R) = \mathfrak{m}$.

Example: For $R = K[X_1, \ldots, X_m]$, we have $\operatorname{rad}(R) = j(R) = (0)$.

Proposition: $j(R) = \{a \in R \mid \forall x \in R\colon 1 - xa \in R^\times\}$.

4 Noetherian rings

Proposition: The following are equivalent:

(a) Every ascending chain $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots$ of ideals of R becomes stationary, i.e., there exists n_0 such that for all $n \geqslant n_0$ we have $\mathfrak{a}_{n_0} = \mathfrak{a}_n$.

(b) Every non-empty collection of ideals of R possesses a maximal element.

(c) Every ideal of R is finitely generated.

Definition: A ring with these properties is called *noetherian.*

Proposition: If R is noetherian, then the following hold:

(a) For any ideal $\mathfrak{a} \subset R$ the ring $R/\mathfrak{a}$ is noetherian.

(b) The image of R under any homomorphism is noetherian.

(c) For any multiplicative set S the ring $S^{-1}R$ is noetherian.

(d) In particular R_f and $R_{\mathfrak{p}}$ are noetherian.

Theorem: *(Hilbert's basis theorem)* If R is noetherian, so is $R[X_1, \ldots, X_n]$.

Corollary: Any ring that is finitely generated over a noetherian ring is noetherian.

Example: Fields and principal ideal domains are noetherian.

Theorem: Let L/K be a field extension which is finitely generated as a ring over K. Then L/K is finite.

Corollary: Let R be a finitely generated ring over a field K. Then for any maximal ideal $\mathfrak{m} \subset R$ the residue field $R/\mathfrak{m}$ is a finite field extension of K.

Theorem: *(The weak Nullstellensatz)* Let K be an algebraically closed field. Then the ideals of the form $\mathfrak{m}_x = (X_1 - x_1, \ldots, X_n - x_n)$ for all $x = (x_1, \ldots, x_n) \in K^n$ are precisely the maximal ideals of $K[X_1, \ldots, X_n]$.

Theorem: *(The strong Nullstellensatz)* Let K be an algebraically closed field. Then for any ideal $\mathfrak{a} \subset K[X_1, \ldots, X_n]$ we have $I(V(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$.

5 Modules

General Terminology: Let M and N be mathematical objects of the same kind.

(a) A *homomorphism* $f\colon M \to N$ is a structure-preserving map of the underlying sets. The meaning of "structure-preserving" depends on the context, so there are ring homomorphisms, group homomorphisms, module homomorphisms, etc.

(b) An *isomorphism* is a homomorphism which admits a two-sided inverse homomorphism, often written $M \xrightarrow{\sim} N$.

(c) An *endomorphism* is a homomorphism from M to itself.

(d) An *automorphism* is an isomorphism from M to itself.

There are also general versions of surjective resp. injective homomorphisms, whose definitions require categories. In the case of modules over a ring they boil down to:

Definition: (e) An *epimorphism* is a surjective homomorphism, often written $M \twoheadrightarrow N$.

(f) A *monomorphism* is an injective homomorphism, often written $M \hookrightarrow N$.

Fix an arbitrary ring R. Consider an R-Module M and distinct elements m_i for $i \in I$.

Definition: (a) We call M *free with basis* $\{m_i \mid i \in I\}$ if for any $m \in M$ there exist unique coefficients $a_i \in R$, almost all being zero, such that $m = \sum'_{i\in I} a_i m_i$.

(b) We call M *free* if it is free with respect to some basis.

Example: For any set I consider the R-modules

$$\begin{aligned} R^I &:= \bigtimes\nolimits_{i\in I} R := \{(a_i)_{i\in I} \mid \forall i\colon a_i \in R\}, \\ R^{(I)} &:= \boxplus\nolimits_{i\in I} R := \{(a_i)_{i\in I} \mid \forall i\colon a_i \in R, \text{ almost all } a_i = 0\}. \end{aligned}$$

Setting $e_i := (\delta_{ij})_{j\in I}$, the module $R^{(I)}$ is free with basis $(e_i)_{i\in I}$. They are equal if and only if I is finite.

Proposition: *(Universal Property)* The module M is free with basis $\{m_i \mid i \in I\}$ if and only if for any R-module N and any choice of elements $n_i \in N$, there exists a unique R-module homomorphism $\varphi\colon M \to N$ with

$$\forall i \in I\colon \varphi(m_i) = n_i.$$

Proposition: If $R \neq 0$ the cardinality of any basis of a free R-module M is unique.

Definition: This cardinality is called the *rank* of M.

Proposition: For any set I, the module M is free of rank $|I|$ if and only if $M \cong R^{(I)}$.

Homomorphism Theorem: For any R-module homomorphism $\varphi\colon M \to N$ there exists a natural isomorphism

$$M/\ker(\varphi) \xrightarrow{\sim} \operatorname{im}(\varphi),\ m + \ker(\varphi) \mapsto \varphi(m).$$

First Isomorphism Theorem: For any submodules N, N' of an R-module M there exists a natural isomorphism

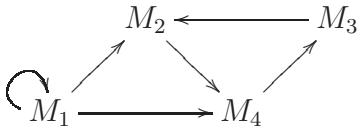
$$\frac{N}{N \cap N'} \xrightarrow{\sim} \frac{N + N'}{N'}.$$

Second Isomorphism Theorem: Let $N \subset M$ be a submodule. Then the submodules of M/N are precisely the N'/N for all submodules N' with $N \subset N' \subset M$, and for any such N' there exists a natural isomorphism

$$\frac{M/N}{N'/N} \xrightarrow{\sim} \frac{M}{N'}.$$

Definition: A tuple (I, J, d, t) consisting of sets I and J and maps $d,\ t\colon J \to I$ is called a *directed graph*. We view I as the set of *vertices* and J as the set of *edges*. To any edge the map d associates the *starting point* and t the *end point*.

Definition: A *diagram* of R-modules indexed by (I, J, d, t) consists of an R-module M_i for every $i \in I$ and a homomorphism $M_{d(j)} \to M_{t(j)}$ for every $j \in J$. For instance:



Definition: A diagram *is commutative* or *commmutes* if for any $i,\ j \in I$, any two homomorphisms $M_i \to M_j$ obtained by composing along a directed path $i \to \ldots \to j$ are equal.

Example: The following diagram commutes if and only if $b \circ a = a' \circ b'$:

$$\begin{array}{ccc} M_1 & \xrightarrow{a} & M_2 \\ {\scriptstyle b'}\downarrow & & \downarrow{\scriptstyle b} \\ N_1 & \xrightarrow{a'} & N_2. \end{array}$$

Consider a finite or one-sided or two-sided infinite sequence of R-module homomorphisms $d_i\colon M_i \to M_{i+1}$ for all $a \leqslant i < b$ where $-\infty \leqslant a < b \leqslant \infty$:

$$\ldots \to M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} M_{i+2} \to \ldots$$

Definition: The sequence is called

(a) a *complex* if for all i we have $d_{i+1} \circ d_i = 0$, or equivalently $\operatorname{im}(d_i) \subset \ker(d_{i+1})$;

(b) *exact* if for all i we have $\operatorname{im}(d_i) = \ker(d_{i+1})$.

Definition: An exact sequence of the form:

(a) $0 \to M_1 \xrightarrow{i} M_2 \xrightarrow{p} M_3 \to 0$ is called a *short exact sequence,*

(b) $0 \to M_1 \to M_2 \to M_3$ is called a *left exact sequence,*

(c) $M_1 \to M_2 \to M_3 \to 0$ is called a *right exact sequence.*

Note: In (a) the sequence is exact if and only if i is injective and p surjective and $\operatorname{im}(i) = \ker(p)$.

Definition: (a) A *homomorphism of sequences* with the same index set is a collection of R-module homomorphisms making the following diagram commute:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & M_i & \longrightarrow & M_{i+1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_{i+1}} & & \\ \cdots & \longrightarrow & N_i & \longrightarrow & N_{i+1} & \longrightarrow & \cdots \end{array}$$

(b) An *isomorphism of sequences* is a homomorphism where all φ_i are isomorphisms. If an isomorphism exists, the sequences are called *isomorphic.*

Proposition: For any short exact sequence $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ the following are equivalent:

(a) There exists a homomorphism $M \xleftarrow{j} M''$ with $p \circ j = \mathrm{id}_{M''}$.

(b) There exists a homomorphism $M' \xleftarrow{q} M$ with $q \circ i = \mathrm{id}_{M'}$.

(c) There exist homomorphisms $M \xleftarrow{j} M''$ and $M' \xleftarrow{q} M$ with $p \circ j = \mathrm{id}_{M''}$ and $q \circ i = \mathrm{id}_{M'}$ and $j \circ p + i \circ q = \mathrm{id}_M$.

(d) The sequence is isomorphic to the sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M' \boxplus M'' & \longrightarrow & M'' & \longrightarrow & 0 \\ & & m' & \xmapsto{i} & (m', 0), & (m', m'') & \xmapsto{p} & m'' & \\ & & (\text{with } m' & \xmapsto{q} & (m', m''), & (0, m'') & \xmapsto{j} & m'') & \end{array}$$

Definition: Such a sequence is called *split.*

Definition: The *cokernel* of a homomorphism $\varphi\colon M_1 \to M_2$ is the module

$$\operatorname{coker} := M_2 / \operatorname{im}(\varphi).$$

Proposition: Every homomorphism $\varphi\colon M_1 \to M_2$ lies in a natural exact sequence:

$$0 \to \ker(\varphi) \to M_1 \xrightarrow{\varphi} M_2 \to \operatorname{coker}(\varphi) \to 0.$$

Proposition: Every commutative square

$$\begin{array}{ccc} M_1 & \xrightarrow{\varphi} & M_2 \\ {\scriptstyle a}\downarrow & & \downarrow{\scriptstyle b} \\ N_1 & \xrightarrow{\psi} & N_2 \end{array}$$

extends to a unique commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\varphi) & \hookrightarrow & M_1 & \xrightarrow{\varphi} & M_2 & \twoheadrightarrow & \operatorname{coker}(\varphi) & \longrightarrow & 0 \\ \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle z} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle 0} \\ 0 & \longrightarrow & \ker(\psi) & \hookrightarrow & N_1 & \xrightarrow{\psi} & M_2 & \twoheadrightarrow & \operatorname{coker}(\psi) & \longrightarrow & 0 \end{array}$$

Snake Lemma: For every commutative diagram with exact rows

$$\begin{array}{ccccccc} & & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & & \end{array}$$

consider the resulting commutative diagram with exact columns and rows:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \ker(\varphi') & \longrightarrow & \ker(\varphi) & \longrightarrow & \ker(\varphi'') & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \operatorname{coker}(\varphi') & \longrightarrow & \operatorname{coker}(\varphi) & \longrightarrow & \operatorname{coker}(\varphi'') & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

There exists a natural *connecting homomorphism* $\delta\colon \ker(\varphi'') \to \operatorname{coker}(\varphi')$ such that

$$\ker(\varphi') \to \ker(\varphi) \to \ker(\varphi'') \xrightarrow{\delta} \operatorname{coker}(\varphi') \to \operatorname{coker}(\varphi) \to \operatorname{coker}(\varphi'')$$

is exact.

Variant: (a) If in addition $N \to N'' \to 0$ is exact, so is $\operatorname{coker}(\varphi) \to \operatorname{coker}(\varphi'') \to 0$.

(b) If in addition $0 \to M' \to M$ is exact, so is $0 \to \ker(\varphi') \to \ker(\varphi)$.

Simple 5-Lemma: For any commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0, \end{array}$$

if φ' and φ'' are isomorphisms, so is φ.

Definition: An R-module is *finitely generated* or *of finite type* if:

$$\exists n \geqslant 0\ \exists m_1, \dots, m_n \in M\colon \forall m \in M\ \exists x_1, \dots, x_n \in R\colon m = \sum_{i=1}^{n}{}' x_i m_i.$$

Proposition: This is equivalent to an epimorphism $R^n \twoheadrightarrow M$ for some n.

Proposition: For any short exact sequence $0 \to M' \to M \to M'' \to 0$:

(a) if M is finitely generated, so is M'';

(b) if M' and M'' are finitely generated, so is M.

Definition: A *presentation* of an R-module M is an exact sequence of the following form for sets I and J:

$$R^{(J)} \xrightarrow{\varphi} R^{(I)} \to M \to 0.$$

Note: The homomorphism φ is given by a matrix of elements of R, and the exact sequence yields an isomorphism $\operatorname{coker}(\varphi) \xrightarrow{\sim} M$.

Definition: A module M is called *finitely presented* or *of finite presentation* if there exists a presentation of the form $R^m \to R^n \to M \to 0$ for some $m, n \geqslant 0$.

Clearly finitely presented implies finitely generated.

Proposition: A module M is finitely presented if and only if it is finitely generated and for any epimorphism $\varphi\colon \tilde{M} \twoheadrightarrow M$ where $\tilde{M}$ is a finitely generated module, $\ker(\varphi)$ is finitely generated.

Example: The module $R/\mathfrak{a}$ is finitely presented if and only if $\mathfrak{a}$ is finitely generated.

Example: The ideal $(X_1, X_2, \dots) \subset K[X_1, X_2, \dots]$ is not finitely generated, so the factor module is not finitely presented.

Proposition: For any exact short sequence $0 \to M' \to M \to M'' \to 0$, if M' and M'' are finitely presented, so is M.

Definition: M is *noetherian* if every submodule of M is finitely generated. (This includes M, of course.)

Proposition: If R is noetherian, for every R-module M we have:

$$M \text{ is noetherian} \iff M \text{ is finitely generated} \iff M \text{ is finitely presented.}$$

Definition: For any two R-modules M and N we endow the set $\mathrm{Hom}_R(M,N)$ with addition, scalar multiplication of functions and the constant function 0 as zero element.

Proposition: This defines an R-module.

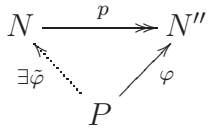
Proposition: For any R-module M and any exact sequence of R-modules

$$0 \to N' \xrightarrow{i} N \xrightarrow{p} N''$$

the following sequence is exact:

$$\begin{array}{ccccccc} 0 & \to & \mathrm{Hom}_R(M,N') & \to & \mathrm{Hom}_R(M,N) & \to & \mathrm{Hom}_R(M,N'') \\ & & \varphi & \mapsto & i\circ\varphi, & \psi & \mapsto & p\circ\psi \end{array}$$

Definition: An R-module P is called *projective* if for any epimorphism $p\colon N \twoheadrightarrow N''$ the map $\mathrm{Hom}_R(P,N) \to \mathrm{Hom}_R(P,N'')$ is surjective, i.e., if for any homomorphism $\varphi\colon P \to N''$ there exists a homomorphism $\tilde{\varphi}\colon P \to N$ such that $p\circ\tilde{\varphi} = \varphi$:



Equivalent: For any exact sequence $0 \to N' \to N \to N'' \to 0$ the following sequence is exact:

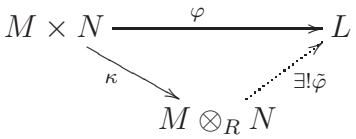
$$0 \to \mathrm{Hom}_R(P,N') \to \mathrm{Hom}_R(P,N) \to \mathrm{Hom}_R(P,N'') \to 0.$$

Example: For $n \geqslant 2$ the module $\mathbb{Z}/n\mathbb{Z}$ is not a projective $\mathbb{Z}$-module.

Proposition: An R-module P is projective if and only if it is isomorphic to a direct summand of a free module.

Remark: The dual notion of *injective* modules, defined in the same way as projective ones but with all arrows reversed, is discussed in the exercises.

Definition: A *tensor product* of R-modules M and N is an R-module $M \otimes_R N$ together with an R-bilinear map $\kappa\colon M \times N \to M \otimes_R N, (m,n) \mapsto m \otimes n$ such that for any R-module L and any R-bilinear map $\varphi\colon M \times N \to L$ there exists a unique R-linear map $\tilde{\varphi}\colon M \otimes_R N \to L$ such that following diagram commutes:



Theorem: A tensor product exists and the pair $(M \otimes_R N, \kappa)$ is unique up to unique isomorphism.

Proposition-Definition: Any two homomorphisms $\varphi\colon M \to M'$ and $\psi\colon N \to N'$ yield a unique homomorphism $\varphi \otimes \psi\colon M \otimes_R N \to M' \otimes_R N'$, such that

$$\forall m \in M\ \forall n \in N\colon (\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n).$$

Proposition: (a) $M \otimes_R N \cong N \otimes_R M$ with $m \otimes n \mapsto n \otimes m$.

(b) $R \otimes_R M \cong M$ with $x \otimes m \mapsto xm$.

(c) $(\bigoplus_{i\in I} M_i) \otimes_R N \cong \bigoplus_{i\in I}(M_i \otimes_R N)$.

Consequence: $R^{(I)} \otimes_R M \cong M^{(I)}$.

Consequence: $R^{(I)} \otimes_R R^{(J)} \cong R^{(I\times J)}$.

Proposition: For any exact sequence $M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$ the following sequence is exact:

$$N \otimes_R M' \xrightarrow{\mathrm{id}\otimes\varphi} N \otimes_R M \xrightarrow{\mathrm{id}\otimes\psi} N \otimes_R M'' \to 0.$$

Consequence: Any presentation of M and N yields one of $M \otimes_R N$.

Example: $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\gcd(m,n)\mathbb{Z}$.

Definition: An R-module F is called *flat*, if for any monomorphism $\iota\colon N' \hookrightarrow N$ the homomorphism $\mathrm{id} \otimes \iota\colon F \otimes N' \to F \otimes N$ is a monomorphism.

Equivalent: For any short exact sequence $0 \to N' \to N \to N'' \to 0$ the following sequence is exact:

$$0 \to F \otimes N' \to F \otimes N \to F \otimes N'' \to 0.$$

Proposition: Every projective R-module is flat.

Example: $\mathbb{Z}/n\mathbb{Z}$ is a flat $\mathbb{Z}$-module if and only if $n = 0$ or $n = \pm 1$.

Definition: An R-algebra is a ring R' together with a ring homomorphism $R \to R'$.

Equivalent: An R-module R' with an R-bilinear associative commutative multiplication and an identity element $1_{R'}$.

Examples: Polynomial rings, localizations, and factor rings thereof.

Proposition: For any R-algebra R' and any R-module M, there exists a unique map $R' \times (R' \otimes_R M) \to R' \otimes_R M$ sending any element $(x, \sum y_i \otimes m_i)$ to $\sum xy_i \otimes m_i$. Together with the already given additive group structure this turns $R' \otimes_R M$ into an R'-module.

Definition: This module is called the *R'-module obtained from M by base change*.

Proposition: Any R-homomorphism $\varphi\colon M \to N$ induces an R'-homomorphism

$$\mathrm{id} \otimes \varphi\colon R' \otimes_R M \to R' \otimes_R N.$$

Example: There is a natural isomorphism $(R/\mathfrak{a}) \otimes_R M \cong M/\mathfrak{a}M$.

Universal property/Adjunction formula: For any R-module M and any R'-module N' there is a natural isomorphism of R'-modules

$$\begin{array}{ccc} \mathrm{Hom}_R(M, N') & \xrightarrow{\sim} & \mathrm{Hom}_{R'}(R' \otimes_R M, N'), \\ (m \mapsto \tilde{\varphi}(1 \otimes m)) & \longleftarrow\!\shortmid & \tilde{\varphi}. \end{array}$$

Example: The localization of modules can be defined as $S^{-1}M := (S^{-1}R) \otimes_R M$. It can also be defined directly as set of equivalence classes in $M \times S$ with the same steps as in the construction of $S^{-1}R$. The adjunction formula yields a universal property of $S^{-1}M$ (see the exercises), which can also be used as a definition.

Nakayama Lemma: For any finitely generated R-module M and any ideal $\mathfrak{a} \subset j(R)$, if $\mathfrak{a}M = M$, then $M = 0$.

Following Matsumura we abbreviate it *NAK* for the initials of Nakayama, Azumaya and Krull, who all contributed to it. Several related statements, including the following corollaries, are also known as Nakayama Lemma.

Corollary: For any finitely generated R-module M, any ideal $\mathfrak{a} \subset j(R)$, and any submodule $N \subset M$ with $M = N + \mathfrak{a}M$ we have $N = M$.

The most common special case is this:

Corollary: Let R be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module. Then any elements $m_1, \ldots, m_n \in M$, whose residue classes $m_1 + \mathfrak{m}M, \ldots, m_n + \mathfrak{m}M$ generate the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, already generate M.

Caution: The analogue is not true for not finitely generated modules:

Example: For any local integral domain R with maximal ideal $\mathfrak{m} \neq 0$, we have $K := \mathrm{Quot}(R) \neq 0$, but $\mathfrak{m}K = K$.

Corollary: Let R be an integral domain which is not a field. Then $\mathrm{Quot}(R)$ is not finitely generated as R-module.

6 Primary decomposition

Definition: An ideal $\mathfrak{q} \subset R$ is called *primary* if it is not R and for any elements $a, b \in R$ with $ab \in \mathfrak{q}$ we have $a \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$ for some $n \geqslant 1$.

Equivalently: If $R/\mathfrak{q} \neq 0$, and every zero divisor in $R/\mathfrak{q}$ is nilpotent.

Proposition-Definition 1: If $\mathfrak{q}$ is primary, then $\mathfrak{p} := \mathrm{Rad}(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$, and we say that $\mathfrak{q}$ is $\mathfrak{p}$-*primary*.

Proposition 2: If $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are $\mathfrak{p}$-primary for the same $\mathfrak{p}$, so is $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$.

Proposition 3: (a) Any ideal $\mathfrak{q}$ for which $\mathfrak{m} := \mathrm{Rad}(\mathfrak{q})$ is a maximal ideal is $\mathfrak{m}$-primary.

(b) For any maximal ideal $\mathfrak{m}$ and any $n \geqslant 1$, the ideal $\mathfrak{m}^n$ is $\mathfrak{m}$-primary.

Example 1: If $R = K[X, Y]$ for a field K and $\mathfrak{m} = (X, Y)$, the ideals (X^n, Y^n) and $\mathfrak{m}^n = (X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n)$ are $\mathfrak{m}$-primary.

Example 2: If $R = K[X, Y]$ for a field K, the ideal (X^2) is (X)-primary.

Example 3: Set $R := K[X, Y, Z]/(XY - Z^2)$ and let $\bar{X}, \bar{Y}, \bar{Z} \in R$ denote the residue classes of X, Y, Z. Then the ideal $\mathfrak{p} := (\bar{X}, \bar{Z})$ is prime, but $\mathfrak{p}^2 = (\bar{X}^2, \bar{X}\bar{Z}, \bar{Z}^2) = (\bar{X}^2, \bar{X}\bar{Z}, \bar{X}\bar{Y}) = (\bar{X})(\bar{X}, \bar{Z}, \bar{Y})$ is not primary although $\mathfrak{p} = \mathrm{Rad}(\mathfrak{p}^2)$ is prime.

Definition: A *primary decomposition* of an ideal $\mathfrak{a} \subset R$ is an expression

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$$

for primary ideals $\mathfrak{q}_i \subset R$. An ideal $\mathfrak{a} \subset R$ is called *decomposable* if it admits a primary decomposition.

Definition: A primary decomposition $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$ is called *minimal* if it satisfies the following properties:

(a) The prime ideals $\mathfrak{p}_i = \mathrm{Rad}(\mathfrak{q}_i)$ are all distinct.

(b) For all $i = 1, \ldots, r$ we have $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$.

Proposition 4: If $\mathfrak{a}$ is decomposable, it possesses a minimal primary decomposition.

Note: We also allow $(1) = \bigcap_{i=1}^{0} \mathfrak{q}_i$.

Example 4: In $R = K[X, Y]$ we have a primary decomposition

$$\big(Y(X^2 + Y^2 - 1) \cdot \{X - 1, Y - 1\}\big) \;=\; (Y) \cap (X^2 + Y^2 - 1) \cap (X - 1, Y - 1).$$

Example 5: In $R = K[X, Y]$ we have two distinct primary decompositions

$$(X^2, XY) \;=\; (X) \cap (X^2, XY, Y^2) \;=\; (X) \cap (X^2, Y).$$

Example 3': The ideal in Example 3 has a primary decomposition

$$\mathfrak{p}^2 \;=\; (\bar{X}^2, \bar{X}\bar{Z}, \bar{X}\bar{Y}) \;=\; (\bar{X}) \cap (\bar{X}^2, \bar{X}\bar{Z}, \bar{Y}, \bar{Z}^2).$$

Counterexample 6: Let $R := K[X_1, X_2, \ldots]$ and $\mathfrak{a} := (\{X_1 \cdots X_n(X_n - 1) \mid n \geqslant 1\})$. Then $\mathfrak{p}_n := (X_1 - 1, \ldots, X_{n-1} - 1, X_n)$ is a prime ideal and $\mathfrak{p}_\infty := (X_1 - 1, X_2 - 1, \ldots)$ a maximal ideal. Also, we have $\mathfrak{a} = \bigcap_{1 \leqslant n < \infty} \mathfrak{p}_n = \bigcap_{1 \leqslant n \leqslant \infty} \mathfrak{p}_n$, corresponding to the disjoint decomposition of the associated "variety" $V(\mathfrak{a}) = \bigcup_{1 \leqslant n \leqslant \infty} V(\mathfrak{p}_n)$. But $\mathfrak{a}$ does not have a *finite* primary decomposition.

Definition-Proposition: The *quotient* of two ideals $\mathfrak{a}, \mathfrak{b} \subset R$ is an ideal:

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in R \mid x\mathfrak{b} \subset \mathfrak{a}\}.$$

Remark: This generalizes the notion of quotient in an integral domain, because there for any $b, c \in R \smallsetminus \{0\}$ we have $\big((bc) : (b)\big) = (c)$.

Special Cases: The quotient by an element $b \in R$, or the *annihilator* of an ideal $\mathfrak{b}$ or an element $b \in R$:

$$\begin{aligned}(\mathfrak{a} : b) := \big(\mathfrak{a} : (b)\big) &= \{x \in R \mid xb \in \mathfrak{a}\},\\ \mathrm{Ann}(\mathfrak{b}) := \big((0) : \mathfrak{b}\big) &= \{x \in R \mid x\mathfrak{b} = (0)\},\\ \mathrm{Ann}(b) := \mathrm{Ann}\big((b)\big) &= \{x \in R \mid xb = 0\}.\end{aligned}$$

Proposition 5: For any ideas $\mathfrak{a}, \mathfrak{b}, \mathfrak{a}_i, \mathfrak{b}_i \subset R$, we have:

(a) $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$.

(b) $(\mathfrak{a} : \mathfrak{b}) \cdot \mathfrak{b} \subset \mathfrak{a}$.

(c) $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = \big((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}\big)$.

(d) $(\bigcap_{i=1}^r \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i=1}^r (\mathfrak{a}_i : \mathfrak{b})$.

(e) $(\mathfrak{a} : \sum_{i=1}^r \mathfrak{b}_i) = \bigcap_{i=1}^r (\mathfrak{a} : \mathfrak{b}_i)$.

Definition: The ideals of the form $\mathrm{Rad}\big((\mathfrak{a} : x)\big)$ for all $x \in R$, which happen to be prime ideals, are called the *prime ideals associated to* $\mathfrak{a}$. The set of these is denoted by $\mathrm{Ass}(\mathfrak{a})$. Any such which is not *minimal* in $\mathrm{Ass}(\mathfrak{a})$ is called *embedded*.

Lemma 1: For any $\mathfrak{p}$-primary ideal $\mathfrak{q}$ and any $x \in R$ we have:

(a) If $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = R$.

(b) If $x \notin \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary and $\mathrm{Rad}\big((\mathfrak{q} : x)\big) = \mathfrak{p}$.

(c) If $x \notin \mathfrak{p}$ then $(\mathfrak{q} : x) = \mathfrak{q}$.

Theorem 1: In any minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{q}_i$, the ideals $\mathfrak{p}_i = \mathrm{Rad}(\mathfrak{q}_i)$ are precisely the associated prime ideals of $\mathfrak{a}$. Thus r is unique, and the $\mathfrak{p}_i$ are independent of the chosen decomposition, up to permutation.

Proposition 6: For any decomposable ideal $\mathfrak{a}$ we have:

(a) The set $\mathrm{Ass}(\mathfrak{a})$ of associated prime ideals is finite.

(b) Any prime ideal containing $\mathfrak{a}$ contains an associated prime of $\mathfrak{a}$.

(c) The minimal prime ideals containing $\mathfrak{a}$ are precisely the minimal elements of $\mathrm{Ass}(\mathfrak{a})$.

Proposition 7: For any decomposable ideal $\mathfrak{a}$ we have

$$\mathrm{Rad}(\mathfrak{a}) = \bigcap_{\mathfrak{p}\in\mathrm{Ass}(\mathfrak{a})} \mathfrak{p}.$$

Recall that $x \in R$ is called a *zero divisor* if there exists a non-zero $y \in R$ with $xy = 0$.

Proposition 8:
$$\{\text{zero divisors of } R\} = \bigcup_{y\in R\smallsetminus\{0\}} \mathrm{Rad}\big(\mathrm{Ann}(y)\big).$$

Proposition 9: If the ideal (0) is decomposable, then

$$\{\text{zero divisors of } R\} = \bigcup_{\mathfrak{p}\in\mathrm{Ass}((0))} \mathfrak{p}.$$

Proposition 10: For any ideals $\mathfrak{b} \subset \mathfrak{a} \subset R$ and any prime ideal $\mathfrak{p} \subset R$, we have:

(a) The ideal $\mathfrak{a}$ is $\mathfrak{p}$-primary if and only if $\mathfrak{a}/\mathfrak{b}$ is $\mathfrak{p}/\mathfrak{b}$-primary in $R/\mathfrak{b}$.

(b) The primary decompositions of $\mathfrak{a}/\mathfrak{b}$ are precisely the expressions $\mathfrak{a}/\mathfrak{b} = \bigcap_{i=1}^{r} \mathfrak{q}_i/\mathfrak{b}$ for all primary decompositions $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$.

(c) The minimal primary decomposition of $\mathfrak{a}/\mathfrak{b}$ are precisely the $\mathfrak{a}/\mathfrak{b} = \bigcap_{i=1}^{r} \mathfrak{q}_i/\mathfrak{b}$ for all minimal primary decomposition of $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$.

Proposition 11: If $\mathfrak{a} \subset R$ is decomposable, then

$$\{x \in R \mid (\mathfrak{a} : x) \neq \mathfrak{a}\} = \bigcup_{\mathfrak{p}\in\mathrm{Ass}(\mathfrak{a})} \mathfrak{p}.$$

Proposition 12: Consider the localization homomorphism $\iota\colon R \to S^{-1}R$ for a multiplicative subset $S \subset R$ and a prime ideal $\mathfrak{p} \subset R$.

(a) If $S \cap \mathfrak{p} \neq \varnothing$, for any $\mathfrak{p}$-primary ideal $\mathfrak{q} \subset R$ we have $\iota_*\mathfrak{q} = (1)$.

(b) If $S \cap \mathfrak{p} = \varnothing$, we have mutually inverse bijections:

$$\begin{array}{rcl} \{\mathfrak{p}\text{-primary ideals of } R\} & \longleftrightarrow & \{\iota_*\mathfrak{p}\text{-primary ideals of } S^{-1}R\} \\ \mathfrak{q} & \longmapsto & \iota_*\mathfrak{q} \\ \iota^*\mathfrak{q}' & \longmapsfrom & \mathfrak{q}' \end{array}$$

Proposition 13: Consider the localization homomorphism $\iota\colon R \to R_\mathfrak{p}$ for a prime ideal $\mathfrak{p} \subset R$. Then the $\mathfrak{p}$-primary ideals of R are precisely the ideals $\iota^*\mathfrak{q}'$ for all ideals $\mathfrak{q}' \subset R_\mathfrak{p}$ with $\mathrm{Rad}(\mathfrak{q}') = \iota_*\mathfrak{p}$.

Definition: For any $n \geqslant 1$, the *n-th symbolic power* of a prime ideal $\mathfrak{p}$ is the ideal $\mathfrak{p}^{(n)} := \iota^*(\mathfrak{p}_\mathfrak{p}^n)$ for ι above. This is $\mathfrak{p}$-primary with $\mathfrak{p}^n \subset \mathfrak{p}^{(n)} \subset \mathfrak{p}$.

Interpretation: It consists of those elements of R which vanish to order at least n at the generic point of $V(\mathfrak{p})$.

Example 3": In Example 3 we had $R = K[X,Y,Z]/(XY - Z^2)$ and $\mathfrak{p} = (\bar{X}, \bar{Z})$ and $\mathfrak{p}^2 = (\bar{X}^2, \bar{X}\bar{Z}, \bar{X}\bar{Y})$. Thus $\mathfrak{p}^2$ is properly contained in $\mathfrak{p}^{(2)} = (\bar{X})$.

Proposition 14: Consider $\iota\colon R \to S^{-1}R$ for a multiplicative subset $S \subset R$.

(a) Any minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{q}_i$ in R induces a minimal primary decomposition $\iota_*\mathfrak{a} = \bigcap_{S\cap\mathfrak{p}_i=\varnothing} \iota_*\mathfrak{q}_i$ in $S^{-1}R$.

(b) Any minimal primary decomposition $\mathfrak{a}' = \bigcap_{i=1}^r \mathfrak{q}_i'$ in $S^{-1}R$ induces a minimal primary decomposition $\iota^*\mathfrak{a}' = \bigcap_{i=1}^r \iota^*\mathfrak{q}_i'$ in R.

(c) Any minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{q}_i$ in R induces a minimal primary decomposition $\iota^*\iota_*\mathfrak{a} = \bigcap_{S\cap\mathfrak{q}_i=\varnothing} \mathfrak{q}_i$ in R.

Theorem 2: In any minimal primary decomposition $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{q}_i$, the $\mathfrak{q}_i$ for which $\mathfrak{p}_i = \mathrm{Rad}(\mathfrak{q}_i)$ minimal in $\mathrm{Ass}(\mathfrak{a})$ are unique.

Now assume R is a noetherian ring.

Definition: We call an ideal $\mathfrak{a} \subset R$ *irreducible* if for any ideals $\mathfrak{b}, \mathfrak{c} \subset R$ with $\mathfrak{b} \cap \mathfrak{c} = \mathfrak{a}$ we have $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{c} = \mathfrak{a}$.

Lemma 2: Every ideal is a finite intersection of irreducible ideals.

Lemma 3: Every irreducible proper ideal is primary.

Theorem 3: If R is noetherian, every ideal of R is decomposable.

Proposition 15: For any ideal $\mathfrak{a}$ of a noetherian ring, there exists $n \geqslant 1$ with $\mathrm{Rad}(\mathfrak{a})^n \subset R \subset \mathrm{Rad}(\mathfrak{a})$.

Counterexample: Let $R := K[X_1, X_2, \ldots]$ and $\mathfrak{a} := (X_1, X_2^2, X_3^3, \ldots)$. Then $\mathrm{Rad}(\mathfrak{a}) = (X_1, X_2, \ldots)$, but for any $n \geqslant 1$ we have $\mathrm{Rad}(\mathfrak{a})^n \not\subset \mathfrak{a}$.

Proposition 16: For any ideal $\mathfrak{q}$ and any maximal ideal $\mathfrak{m}$ of a noetherian ring, the following are equivalent:

(a) $\mathfrak{q}$ is $\mathfrak{m}$-primary.

(b) $\mathrm{Rad}(\mathfrak{q}) = \mathfrak{m}$.

(c) There exists $n \geqslant 1$, such that $\mathfrak{m}^n \subset \mathfrak{q} \subset \mathfrak{m}$.

Proposition 17: In noetherian ring, the associated prime ideals of $\mathfrak{a}$ are precisely the prime ideals of the form $(\mathfrak{a} : x)$ for $x \in R$.

7 Artinian rings

Proposition 1: For any R-module M the following are equivalent:

(a) Every ascending chain of submodules becomes stationary.

(b) Every non-empty collection of submodules has a maximal element.

(c) Every submodule of M is finitely generated.

Definition: Such a module is called *noetherian*.

Proposition 2: For every R-module M the following are equivalent:

(a) Every descending chain of submodules becomes stationary.

(b) Every non-empty collection of submodules has a minimal element.

Definition: Such a module is called *artinian*.

Definition: The *length* of an R-module M is

$$\text{length}(M) := \sup\big\{r \geqslant 0 \;\big|\; \exists \text{ submodules } 0 = M_0 \subsetneqq M_1 \subsetneqq \ldots \subsetneqq M_r = M\big\} \in \mathbb{Z}^{\geqslant 0} \cup \{\infty\}.$$

Special Case: We have $\text{length}(M) = 0$ if and only if $M = 0$.

Special Case: A module M with $\text{length}(M) = 1$ is called *simple*. This is the case if and ony if M is non-zero and has no submodules except 0 and M.

Proposition 3: For any short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$ we have:

(a) M is noetherian if and only if M' and M'' are noetherian.

(b) M is artinian if and only if M' and M'' are artinian.

(c) $\text{length}(M) = \text{length}(M') + \text{length}(M'')$.

Proposition 4: $\text{length}(M) < \infty$ if and only if M is both noetherian and artinian.

Proposition 5: For any field K and any K-vector space V we have:

$$V \text{ is noetherian} \iff V \text{ is artinian} \iff \text{length}(V) < \infty \iff \dim(V) < \infty.$$

Moreover, in this case $\text{length}(V) = \dim(V)$.

Proposition 6: Assume that R possesses maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ (not necessary distinct) such that $\mathfrak{m}_1 \cdots \mathfrak{m}_r = 0$. Then:

$$R \text{ is noetherian} \iff R \text{ is artinian} \iff \text{length}(R) < \infty.$$

Definition: A ring is called *artinian* if it is artinian as a module over itself.
(That is, if the descending chain condition holds for ideals.)

Example: Any ring with only finitely many ideals is artinian, e.g. any field and $R/(f)$ for any principal ideal domain R and any ideal $(f) \neq (0)$.

Example: Any K-algebra of finite dimension.

Example: $\mathbb{Z}/n\mathbb{Z}$ for $n > 0$.

Example: $K[X]/(X^n)$ and $K[X,Y]/(X,Y)^n$ for $n > 0$.

Proposition 7: If R is artinian, every prime ideal of R is maximal.

Proposition 8: If R is artinian, it has only finitely many maximal ideals.

Proposition 9: If R is artinian, there exists $n \geqslant 1$ with $\mathrm{rad}(R)^n = 0$.

Theorem 1: For any ring R the following are equivalent:

(a) R is artinian.

(b) R is noetherian and every prime ideal is maximal.

(c) R has finite length as R-module.

Proposition 10: For any noetherian local ring R with maximal ideal $\mathfrak{m}$, we have exactly one of the two cases:

(a) For all $n \geqslant 1$ we have $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$, or

(b) R is artinian and there exists $n \geqslant 1$ such that $\mathfrak{m}^n = 0$.

Definition: Ideals $\mathfrak{a}$ and $\mathfrak{b}$ with $\mathfrak{a} + \mathfrak{b} = R$ are called *relatively prime* or *coprime*.

Preposition 11: If $\mathfrak{a}$ is coprime to each of $\mathfrak{b}_1, \ldots, \mathfrak{b}_r \subset R$, then it is also coprime to $\mathfrak{b}_1 \cdots \mathfrak{b}_r$ and to $\mathfrak{b}_1 \cap \ldots \cap \mathfrak{b}_r$.

Proposition 12: *(Chinese Remainder Theorem)* Any given ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \subset R$ are pairwise coprime if and only if the naural homomorphism

$$\begin{array}{ccc} R/\bigcap_{i=1}^r \mathfrak{a}_i & \longrightarrow & \bigtimes_{i=1}^r R/\mathfrak{a}_i \\ x + \bigcap_{i=1}^r \mathfrak{a}_i & \mapsto & (x + \mathfrak{a}_i)_i \end{array}$$

is an isomorphism, and then $\bigcap_{i=1}^r \mathfrak{a}_i = \prod_{i=1}^r \mathfrak{a}_i$.

Theorem 2: A ring R is artinian if and only if it is isomorphic to a finite product of artinian local rings R_i.

8 Graded rings and modules

Definition: Let I be an abelian group written additively. An *I-graded ring* is a ring R together with a decomposition as additive group $R = \bigoplus_{i\in I} R_i$ such that for all $i, j \in I$, we have $R_i \cdot R_j \subset R_{i+j}$. Elements of R_i are called *homogeneous of degree i*.

Note: If I is not specified, we usually assume $I = \mathbb{Z}$.

Example: Let $R := K[X_1, \ldots, X_r]$, and for every $i \in I := \mathbb{Z}$ let R_i be the set of homogeneous polynomials of degree i. Note that 0 is homogeneous of every degree!

Variant: Endow each X_i with its own weight $\mu_i \in I$.

Example: Let $R := K[X_1, \ldots, X_r]$, and for every *pluridegree* $\underline{i} \in I := \mathbb{Z}^r$ define $R_{\underline{i}} := K \cdot \underline{X}^{\underline{i}}$.

Example: A ring with a decomposition $R = R_0 \oplus R_1$ satisfying $R_0R_0 \subset R_0$ and $R_0R_1 \subset R_1$ and $R_1R_1 \subset R_0$ is I-graded for $I := \{0, 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

Definition: An *I-graded module M* over an I-graded ring R is an R-module together with a decomposition $M = \bigoplus_{i\in I} M_i$ such that for all $i, j \in I$, we have $R_i \cdot M_j \subset M_{i+j}$. Elements of M_i are called *homogeneous of degree i*.

Example: A graded ring as a module over itself.

Example: Any ideal of a graded ring that is generated by homogeneous elements.

Example: Any product, intersection, sum of graded ideals.

Definition: A *graded submodule M'* of a graded module M is a submodule satisfying $M' = \bigoplus_{i\in I}(M_i \cap M')$.

Equivalent: A submodule of a graded module that is generated by homogeneous elements.

Example: The factor module of a graded module by a graded submodule is a graded module.

Example: The factor ring of a graded ring by a graded ideal is a graded ring.

Example: For any field K the factor ring $K[W, X, Y, Z]/(XY - WZ)$ is $\mathbb{Z}$-graded.

Note: Many other operations, such as sum and intersection of submodules, homomorphisms and tensor products, preserve grading.

Proposition: A graded module is finitely generated if and only if it is finitely generated by homogeneous elements.

Construction: Let I^+ be a commutative monoid, i.e., a set with an associative commutative binary operation $+\colon I^+ \times I^+ \to I^+$ and an identity element 0. For every $i \in I^+$ let $[i]$ be a new symbol and endow the R-module

$$R[I^+] := \coprod_{i \in I^+} R \cdot [i] \cong R^{(I^+)}$$

with the unique R-bilinear multiplication satisfying $[i] \cdot [j] := [i+j]$ for all $i, j \in I^+$. Then $R[I^+]$ is a commutative unitary R-algebra with the identity element $[0]$.

Definition: This is called the *monoid ring of I^+ over R.*

Note: If instead we assume that I^+ is a group G, this construction yields the *group ring* $R[G]$ of G over R. This ring is commutative if and only if G is commutative.

Fact: If I^+ is a submonoid of an abelian group I, then $R[I^+]$ is naturally I-graded with

$$(R[I^+])_i := \begin{cases} R[i] & \text{if } i \in I^+, \\ 0 & \text{otherwise.} \end{cases}$$

Example: $R[(\mathbb{Z}^{\geqslant 0})^r] = R[X_1, \ldots, X_r]$ via $[\underline{i}] = \underline{X}^{\underline{i}}$.

Example: $R[\mathbb{Z}^r] = R[X_1^{\pm 1}, \ldots, X_r^{\pm 1}]$ via $[\underline{i}] = \underline{X}^{\underline{i}}$.

Example: $R[\mathbb{Q}^{\geqslant 0}] = R[\{X^\alpha \mid \alpha \in \mathbb{Q}^{\geqslant 0}\}] = R[\{X^{\frac{1}{n}} \mid n \geqslant 1\}]$ via $[\alpha] = X^\alpha$. This is the ring of *Puiseux polynomials* over R. It is not noetherian if $R \neq 0$. It is related to the field of *Puiseux series* $K((t)) = \bigcup_{n \geqslant 0} K((t^{\frac{1}{n}}))$ over a field K.

Example: Take $I^+ := \{(i,j,k,l) \in (\mathbb{Z}^{\geqslant 0})^4 \mid i + j = k + l\}$. Then $R[I^+]$ is generated by the elements

$$X := [(1,0,1,0)], \quad Z := [(1,0,0,1)], \quad W := [(0,1,1,0)], \quad Y := [(0,1,0,1)]$$

satisfying $XY = ZW$, and in fact $R[I^+] \cong R[W,X,Y,Z]/(XY - WZ)$.

Theorem: *(Artin-Rees Lemma)* Consider a noetherian ring R, an ideal $\mathfrak{a} \subset R$, a finitely generated R-module M and a submodule M'. Then

$$\exists k_0 \; \forall i \geqslant k \geqslant k_0 \colon \; M' \cap \mathfrak{a}^i M = \mathfrak{a}^{i-k}(M' \cap \mathfrak{a}^k M).$$

Theorem: *(Krull Intersection Theorem)* For any noetherian ring R, any ideal $\mathfrak{a} \subset j(r)$ and any finitely generated R-module M we have:

$$\bigcap_{i \geqslant 0} \mathfrak{a}^i M = 0.$$

In particular $\bigcap_{i \geqslant 0} \mathfrak{a}^i = 0$.

Counterexample: For any ideal $\mathfrak{a} \not\subset j(R)$ there exists an ideal $\mathfrak{b} \subsetneqq R$ with $\mathfrak{a} + \mathfrak{b} = (1)$, and then we have $\bigcap_{i \geqslant 0} \mathfrak{a}^i(R/\mathfrak{b}) = R/\mathfrak{b} \neq 0$.

Counterexample: For any prime number p the ring $R := \mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$ is local with maximal ideal $\mathfrak{a} := (p) = j(R)$. For the non-finitely generated R-module $M := \mathbb{Q}$ we have $\bigcap_{i \geqslant 0} \mathfrak{a}^i M = M \neq 0$.

Proposition: For any prime ideal $\mathfrak{p}$ of a noetherian ring R the kernel of the localization map $R \to R_{\mathfrak{p}}$ is the intersection of all symbolic powers $\bigcap_{n \geqslant 0} \mathfrak{p}^{(n)}$.

9 Krull dimension

Definition: (a) The *(Krull) dimension* of a ring R is:

$$\dim R := \sup\{r \geqslant 0 \mid \exists \text{ prime ideals } \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r \subset R\}.$$

(b) The *height* of a prime ideal $\mathfrak{p} \subset R$ is:

$$\mathrm{ht}(\mathfrak{p}) := \sup\{r \geqslant 0 \mid \exists \text{ prime ideals } \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r = \mathfrak{p}\}.$$

(c) The *height* of an arbitrary ideal $\mathfrak{a} \subset R$ is:

$$\mathrm{ht}(\mathfrak{a}) := \inf\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{a} \subset \mathfrak{p} \text{ prime}\}.$$

(d) The *coheight* of an ideal $\mathfrak{a} \subset R$ is:

$$\mathrm{coht}(\mathfrak{a}) := \dim(R/\mathfrak{a}) = \sup\{\mathrm{coht}(\mathfrak{p}) \mid \mathfrak{a} \subset \mathfrak{p} \text{ prime}\}.$$

All of them lie in $\mathbb{Z}^{\geqslant 0} \cup \{\pm\infty\}$.

Example 1: We have $\dim R = -\infty$ if and only if $R = 0$.

Example 2: We have $\dim R = 0$ if and only if $R \neq 0$ and every prime ideal is maximal.

Example 3: The zero ideal (0) always has height 0.

Example 4: For any principal ideal domain R and any non-zero maximal ideal $\mathfrak{m}$ we have $\dim R = \mathrm{coht}((0)) = \mathrm{ht}(\mathfrak{m}) = 1$.

Example 5: Set $R := K[X_1, \ldots, X_n]$ for a field K. Then the prime ideals $\mathfrak{p}_i := (X_1, \ldots, X_i)$ form a chain

$$(0) = \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \ldots \subsetneqq \mathfrak{p}_n = \text{maximal ideal}.$$

Therefore $\dim R \geqslant n$ and $\mathrm{ht}(\mathfrak{p}_i) \geqslant i$ and $\mathrm{coht}(\mathfrak{p}_i) \geqslant n - i$ for all i. This chain of prime ideals cannot be refined.

Example 6: In $R := K[X_1, X_2, \ldots]$ we have prime ideals $(0) \subsetneqq (X_1) \subsetneqq (X_1, X_2) \subsetneqq \ldots$. Hence, $\dim R = \mathrm{ht}\big((X_1, X_2, \ldots)\big) = +\infty$.

Explanation: If R is the coordinate ring of a variety X, we interpret $\dim R$ as the *dimension of* X. If a prime ideal $\mathfrak{p} \subset R$ corresponds to an irreducible subvariety $Y \subset X$, we likewise view $\mathrm{coht}(\mathfrak{p}) = \dim(R/\mathfrak{p})$ as the *dimension of* Y. In this case we also interpret $\mathrm{ht}(\mathfrak{p})$ as the *codimension of* Y *in* X. The object of dimension theory is to analyze under which conditions these invariants have the expected properties, for instance that the dimension of Y plus its codimension in X is the dimension of X.

Proposition 1: (a) $\dim R = \sup\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec} R\} = \sup\{\mathrm{coht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec} R\}$.

(b) $\dim R \geqslant \mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p})$.

(c) $\mathrm{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.

(d) $\dim R = \dim(R/\operatorname{rad}(R))$.

(e) If $\mathfrak{a}$ is decomposable and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the minimal prime ideals above $\mathfrak{a}$, then

$$\begin{aligned} \mathrm{ht}(\mathfrak{a}) &= \min\{\mathrm{ht}(\mathfrak{p}_i) \mid 1 \leqslant i \leqslant r\}, \\ \mathrm{coht}(\mathfrak{a}) &= \max\{\mathrm{coht}(\mathfrak{p}_i) \mid 1 \leqslant i \leqslant r\}. \end{aligned}$$

Theorem 2: *(Krull's principal ideal theorem)* If R is noetherian and $a \in R$ is not a zero divisor, any minimal prime ideal $\mathfrak{p}$ containing (a) satisfies $\mathrm{ht}(\mathfrak{p}) = 1$.

Corollary: If in addition $a \in R$ is not a unit, then $\mathrm{ht}\big((a)\big) = 1$.

Theorem 3: *(Krull's dimension theorem)* If R is noetherian and $\mathfrak{a} = (a_1, \ldots, a_r)$ is an ideal generated by r elements, then for any minimal prime ideal $\mathfrak{p}$ above $\mathfrak{a}$, we have $\mathrm{ht}(\mathfrak{p}) \leqslant r$. In other words, we have $\mathrm{ht}(\mathfrak{a}) \leqslant r$, provided that $\mathfrak{a} \neq (1)$.

Theorem 4: If R is noetherian local with maximal ideal $\mathfrak{m}$, then $\dim R \leqslant \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. In particular the Krull dimension is finite.

Lemma 5: If an ideal of a ring is contained in a finite union of prime ideals $\mathfrak{p}_i$, it is contained in one of these $\mathfrak{p}_i$.

Lemma 6: Let R be noetherian and $\mathfrak{a}$ an ideal of height r. Let $0 \leqslant s \leqslant r$ and consider elements $a_1, \ldots, a_s \in \mathfrak{a}$ with $\mathrm{ht}\big((a_1, \ldots, a_s)\big) = s$. Then there exist $a_{s+1}, \ldots, a_r \in \mathfrak{a}$ such that $\mathrm{ht}\big((a_1, \ldots, a_r)\big) = r$.

Proposition 7: Let R be local noetherian with maximal ideal $\mathfrak{m}$ and $\dim R = d$. Then there exists $x_1, \ldots, x_d \in \mathfrak{m}$ such that $(x_1, \ldots, x_d)$ is an $\mathfrak{m}$-primary ideal. Conversely, no $\mathfrak{m}$-primary ideal can be generated by fewer than d elephants.

Definition: Such elements $x_1, \ldots, x_d$ are called a *system of parameters* of R.

Proposition 8: Let R be local noetherian with maximal ideal $\mathfrak{m}$ and $\dim R = d$. Then for any $x_1, \ldots, x_r \in \mathfrak{m}$ we have

$$\dim R/(x_1, \ldots, x_r) = \mathrm{coht}\big((x_1, \ldots, x_r)\big) \geqslant d - r.$$

Proposition 9: Let R be local noetherian with maximal ideal $\mathfrak{m}$ and $\dim R = d$. Then for any $x_1, \dots, x_r \in \mathfrak{m}$ we have the implications (a)$\Longrightarrow$(b)$\Longleftrightarrow$(c) for the statements:

(a) $\mathrm{ht}((x_1, \dots, x_r)) = r$,

(b) $x_1, \dots, x_r$ can be extended to a system of parameters of R,

(c) $\dim(R/(x_1, \dots, x_r)) = d - r$,

Corollary 10: Let R be local noetherian with maximal ideal $\mathfrak{m}$ and $\dim R = d$. Then for any $a \in \mathfrak{m}$ which is not a zero divisor, we have $\dim R/(a) = (\dim R) - 1$.

Theorem 11: For any noetherian ring R and any $n \geqslant 0$, we have $\dim R[x_1, \dots, x_n] = (\dim R) + n$.

Corollary 12: For any field K, we have $\dim K[x_1, \dots, x_n] = n$.

Example 5': In Example 5 we have $\mathrm{ht}(\mathfrak{p}_i) = i$ and $\mathrm{coht}(\mathfrak{p}_i) = n - i$, and therefore $\mathrm{ht}(\mathfrak{p}_i) + \mathrm{coht}(\mathfrak{p}_i) = \dim R = n$ for all i.

10 Integral ring extensions

Throughout the chapter consider a subring $R \subset S$.

Definition: An element $b \in S$ is called *integral over* R if there exists a monic polynomial $f \in R[X]$ with $f(b) = 0$, or equivalently if

$$\exists\, n \geqslant 1\ \exists\, a_1, \ldots, a_n \in R\colon\ b^n + \textstyle\sum_{i=1}^{n} a_i b^{n-i} = 0.$$

Example: If R and S are fields, then b is integral over R if and only if b is algebraic over R.

Proposition 1: For any $b \in S$ the following are equivalent:

(a) The element b is integral over R.

(b) The subring $R[b] \subset S$ is finitely generated as an R-module.

(c) The element b lies in a subring $T \subset S$ that is finitely generated as an R-module.

(d) There exists an $R[b]$-module M which is finitely generated as an R-module, such that $\mathrm{Ann}_{R[b]}(M) := \{a \in R \mid aM = 0\} = 0$.

Lemma 2: Let $R \subset S \subset T$ be ring extensions such that S is finitely generated as an R-module and T is finitely generated as an S-module. Then T is finitely generated as an R-module.

Proposition 3: If $b_1, \ldots, b_n \in S$ are integral over R, then $R[b_1, \ldots, b_n]$ is finitely generated as an R-module.

Proposition 4: The set $\{b \in S \mid b \text{ integral over } R\}$ is a subring of S containing R.

Definition: (a) This subring is called the *integral closure* of R in S.

(b) If this subring is S, then S is called *integral* over R, and the ring extension $R \subset S$ is called *integral*.

(c) If this subring is R, then R is called *integrally closed in* S.

Proposition 5: For any ring extensions $R \subset S \subset T$ the extension $R \subset T$ is integral if and only if both $R \subset S$ and $S \subset T$ are integral.

Proposition 6: The integral closure of R in S is integrally closed in S.

Proposition 7: For any integral ring extension $R \subset S$ and any ideal $\mathfrak{b} \subset S$ the ring extension $R/(\mathfrak{b} \cap R) \hookrightarrow S/\mathfrak{b}$ is integral.

Proposition 8: Let $R \subset S$ be a ring extension, $\tilde{R} \subset S$ the integral closure of R in S and $\Sigma \subset R$ a multiplicative subset. Then:

(a) $\Sigma^{-1}R \subset \Sigma^{-1}\tilde{R} \subset \Sigma^{-1}S$ are ring extensions.

(b) $\Sigma^{-1}\tilde{R}$ is the integral closure of $\Sigma^{-1}R$ in $\Sigma^{-1}S$.

(c) If $R \subset S$ is integral, so is $\Sigma^{-1}R \subset \Sigma^{-1}S$.

(d) If R is integrally closed in S, so is $\Sigma^{-1}R$ in $\Sigma^{-1}S$.

Special Case: Take an integral ring extension $R \subset S$ and let $\Sigma := R \setminus \mathfrak{m}$ for a maximal ideal $\mathfrak{m} \subset R$. Then $R_{\mathfrak{m}} \subset (R \setminus \mathfrak{m})^{-1}S$ is an integral ring extension.

Caution: Integrality is in general not preserved under localization at corresponding prime ideals of R and S. For instance, if $\mathfrak{n} \subset S$ is a maximal ideal and $\mathfrak{m} := \mathfrak{n} \cap R$, then $R_{\mathfrak{m}} \subset S_{\mathfrak{n}}$ is not necessarily integral.

Example: For any field K the ring extension $R := K[X] \hookrightarrow S := K[Y]$ defined by $f(X) \mapsto f(Y^2-1)$ is integral. For the maximal ideal $\mathfrak{m} := (X)$ of R there are precisely two maximal ideals $\mathfrak{n}$ of S with $\mathfrak{n} \cap R = \mathfrak{m}$, namely $\mathfrak{n} := (Y-1)$ and $\mathfrak{n}' := (Y+1)$. The integral closure of $R_{\mathfrak{m}}$ in $K(Y)$ is $R_{\mathfrak{m}} \cdot S = S_{\mathfrak{n}} \cap S_{\mathfrak{n}'}$ and is properly contained in both $S_{\mathfrak{n}}$ and $S_{\mathfrak{n}'}$.

Definition: (a) An integral domain R is called *normal* if it is integrally closed in $\mathrm{Quot}(R)$.

(b) The *normalization* of an integral domain R is its integral closure in $\mathrm{Quot}(R)$.

Fact: The normalization is normal by Proposition 6.

Proposition 9: Any unique factorization domain is normal.

Proposition 10: Let R be an integral domain and $\Sigma \subset R \setminus \{0\}$ a multiplicative subset.

(a) If R is a unique factorization domain, so is $\Sigma^{-1}R$.

(b) If R is normal, so is $\Sigma^{-1}R$.

Example: Any localization of $K[X_1, \ldots, X_n]$ is normal.

Lemma 11: For any integral domain R we have $R = \bigcap_{\mathfrak{m} \subset R} R_{\mathfrak{m}}$ within $\mathrm{Quot}(R)$, where $\mathfrak{m}$ runs through all maximal ideals of R.

Note: Using the proof one can see that $\mathrm{Spec}\, R$ is a (quasi-) compact topological space.

Proposition 12: For any integral domain R, the following are equivalent:

(a) R is normal.

(b) $R_{\mathfrak{p}}$ is normal for every $\mathfrak{p} \subset R$ prime.

(c) $R_{\mathfrak{m}}$ is normal for every $\mathfrak{m} \subset R$ maximal.

Lemma 13: Let $R \subset S$ be an integral ring extension of integral domains. Then R is a field if and only if S is a field.

Proposition 14: Let $R \subset S$ be an integral ring extension and $\mathfrak{q} \subset S$ a prime ideal. Then $\mathfrak{q}$ maximal if and only if $\mathfrak{p} := \mathfrak{q} \cap R$ is maximal.

Theorem 15: *(Lying over)* Let $R \subset S$ be an integral ring extension.

(a) For any prime ideal $\mathfrak{p} \subset R$ there exists a prime ideal $\mathfrak{q} \subset S$ with $\mathfrak{q} \cap R = \mathfrak{p}$.

(b) For any prime ideals $\mathfrak{q} \subset \mathfrak{q}' \subset S$ with $\mathfrak{q} \cap R = \mathfrak{q}' \cap R$ we have $\mathfrak{q} = \mathfrak{q}'$.

The Going up and Going down theorems below are due to Cohen and Seidenberg:

Theorem 16: *(Going up)* Let $R \subset S$ be an integral ring extension. Then for any chain of prime ideals $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_r$ of R and any prime ideal $\mathfrak{q}_0$ of S with $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$ there exist prime ideals $\mathfrak{q}_0 \subset \ldots \subset \mathfrak{q}_r$ of S such that $\forall i\colon \mathfrak{q}_i \cap R = \mathfrak{p}_i$.

Proposition 17: Let R be a normal integral domain with $K := \mathrm{Quot}(R)$, let L be a normal algebraic field extension of K, and let S be the integral closure of R in L. Then:

(a) $\mathrm{Aut}_K(L)$ acts on S and on $\operatorname{Spec} S$.

(b) For any prime ideal $\mathfrak{p} \subset R$, this action is transitive on $\{\mathfrak{q} \in \operatorname{Spec} S \mid \mathfrak{q} \cap R = \mathfrak{p}\}$.

Theorem 18: *(Going down)* Let $R \subset S$ be an integral ring extension of integral domains where R is normal. Then for any chain of prime ideals $\mathfrak{p}_n \subset \ldots \subset \mathfrak{p}_0$ of R and any prime ideal $\mathfrak{q}_0$ of S with $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$ there exist prime ideals $\mathfrak{q}_n \subset \ldots \subset \mathfrak{q}_0$ of S such that $\forall i\colon \mathfrak{q}_i \cap R = \mathfrak{p}_i$.

Proposition 19: Consider an integral ring extension $R \subset S$ and an ideal $\mathfrak{b} \subset S$, and set $\mathfrak{a} := \mathfrak{b} \cap R$. Then:

(a) $\dim S = \dim R$.

(b) $\mathrm{coht}(\mathfrak{b}) = \mathrm{coht}(\mathfrak{a})$.

(c) $\mathrm{ht}(\mathfrak{b}) \leqslant \mathrm{ht}(\mathfrak{a})$.

(d) $\mathrm{ht}(\mathfrak{b}) = \mathrm{ht}(\mathfrak{a})$ if R and S are integral domains and R is normal.

Let K be a field.

Lemma 20: For any polynomial $f \in K[X_1, \ldots, X_n] \smallsetminus \{0\}$ there exist $g_1, \ldots, g_{n-1} \in K[X_1, \ldots, X_n]$ such that the ring extension $K[g_1, \ldots, g_{n-1}, f] \subset K[X_1, \ldots, X_n]$ is integral.

Definition: Elements $a_1, \ldots, a_n$ of a K-algebra R are called *algebraically independent over* K if for any polynomial $f \in K[X_1, \ldots, X_n]$ with $f(a_1, \ldots, a_n) = 0$ we have $f = 0$, or equivalently if the following ring homomorphism is an isomorphism:

$$K[X_1, \ldots, X_n] \to K[a_1, \ldots, a_n] \subset R, \ f \mapsto f(a_1, \ldots, a_n).$$

Theorem 21: (*Noether normalization*) For any non-zero finitely generated K-algebra R, there exist $m \geqslant 0$ and $b_1, \ldots, b_m \in R$ algebraically independent over K such that $K[b_1, \ldots, b_m] \subset R$ is an integral ring extension.

Theorem 22: Let R be an integral domain that is finitely generated over a field K. Then:

(a) $\dim R = \operatorname{trdeg}(\operatorname{Quot}(R)/K)$.

(b) $\forall \mathfrak{p} \subset R$ prime: $\operatorname{ht}(\mathfrak{p}) + \operatorname{coht}(\mathfrak{p}) = \dim R$.

(c) $\forall \mathfrak{m} \subset R$ maximal: $\operatorname{ht}(\mathfrak{m}) = \dim R$.

Lemma 23: Let R be an integral domain that is finitely generated over a field, and $\mathfrak{p} \subsetneqq \mathfrak{p}'$ prime ideals without further prime ideals between them. Then $\operatorname{ht}(\mathfrak{p}') = \operatorname{ht}(\mathfrak{p})+1$.

Lemma 24: In a noetherian ring, any chain of prime ideals is finite and can be refined to a maximal chain.

Definition: A noetherian ring is called *catenary* if for any prime ideals $\mathfrak{p} \subset \mathfrak{p}' \subset R$ the length r of all maximal chains of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \subsetneqq \ldots \subsetneqq \mathfrak{p}_r = \mathfrak{p}'$ is the same.

Theorem 25: Any ring that is finitely generated over a field is catenary.

Theorem 26: *(without proof)* Any ring that is finitely generated over $\mathbb{Z}$ is catenary. If in addition the ring is an integral domain, the statements of Theorem 22 hold as well.

11 Completions

Definition: The *inverse limit* of a diagram of sets X_i for $i \in I$ with maps $\varphi_j \colon X_{d(j)} \to X_{t(j)}$ for all $j \in J$ is the set

$$\varprojlim_i X_i \;:=\; \Big\{(x_i)_i \in \bigtimes_{i\in I} X_i \;\Big|\; \forall j \colon \varphi_j(x_{d(j)}) = x_{t(j)}\Big\}.$$

Fact: If all X_i are groups, rings, resp. R-modules and all φ_j are homomorphisms, then $\varprojlim_i X_i$ is a subgroup, subring, resp. R-submodule of $\bigtimes_{i\in I} X_i$.

Special Case: If $I = J = \mathbb{Z}^{\geqslant 0}$ and $d(j) = j+1$ and $t(j) = j$ for all j, then

$$\varprojlim_i X_i \;:=\; \Big\{(x_i)_i \in \bigtimes_{i\in I} X_i \;\Big|\; \forall i \colon \varphi_i(x_{i+1}) = x_i\Big\}.$$

Definition: The *completion* of a group G with respect to a system of normal subgroups $\ldots \subset G_1 \subset G_0 = G$ is

$$\hat{G} \;:=\; \varprojlim_n (G/G_n) \;=\; \varprojlim_n \left(\ldots \to G/G_n \to G/G_{n-1} \to \ldots\right).$$

Thus an element of $\hat{G}$ is a system of residue classes $(g_nG_n)_{n\geqslant 0}$ which are all contained in each other:

$$\ldots \subset g_nG_n \subset g_{n-1}G_{n-1} \subset \ldots.$$

Fact: The natural homomorphism $\kappa \colon G \to \hat{G}$, $g \mapsto (gG_n)_{n\geqslant 0}$ has

$$\begin{aligned} \text{kernel}(\kappa) \;&=\; G_\infty \;:=\; \textstyle\bigcap_{n\geqslant 0} G_n, \\ \text{image}(\kappa) \;&=\; \Big\{(g_nG_n)_n \in \varprojlim_n G/G_n \;\Big|\; \textstyle\bigcap_{n\geqslant 0} g_nG_n \neq \varnothing\Big\}. \end{aligned}$$

Example 1: Taking $G := \mathbb{Z}$ and $G_n := p^n\mathbb{Z}$ for a prime number p we obtain the *ring of p-adic integers*

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

This is an integral domain with quotient field $\mathbb{Q}_p := \mathbb{Z}_p[\frac{1}{p}]$, which is called the *field of p-adic numbers.* A simple p-adic integer, constructed via the geometric series as $\hat{a} := (1 + p + \ldots + p^{n-1} + p^n\mathbb{Z})_{n\geqslant 0} \in \mathbb{Z}_p$ satisfies $\hat{a} \cdot (1-p) = (1 + p^n\mathbb{Z})_{n\geqslant 0} = 1$; hence $\hat{a} = \frac{1}{1-p}$ does not lie in the image of $\mathbb{Z}$ if $p > 2$.

Proposition 1: For $g, g' \in G$ define $d(g,g') := \inf\{2^{-n} \mid n \geqslant 0 \text{ with } gG_n = g'G_n\}$. Then $d(g,g') = 0$ if and only if $gG_\infty = g'G_\infty$; and d induces a metric on G/G_∞. Its completion as a metric space is naturally isomorphic to $\hat{G} := \varprojlim_n G/G_n$.

Interpretation: We can view $\hat{G}$ as the "set of limits af all Cauchy sequences in G".

Proposition 2: For any two systems of normal subgroups $\ldots \subset G_1 \subset G_0 = G$ and $\ldots \subset G'_1 \subset G'_0 = G$ which are *cofinal*, i.e., with $\forall n\ \exists m(n)\colon G_{m(n)} \subset G'_n \wedge G'_{m(n)} \subset G_n$ the completions are naturally isomorphic.

Remark: In particular one can leave out finitely many terms of the sequence and pass to any infinite monotone subsequence $G_{k(n)}$ with $\lim_{n\to\infty} k(n) = \infty$.

Remark: The completion $\hat{G}$ depends only on the topology on G defined by the basis $\{gG_n \mid g \in G, n \geqslant 0\}$. This topology is Hausdorff if and only if $G_\infty = 1$.

Proposition 3: Any short exact sequence $1 \to G' \xrightarrow{i} G \xrightarrow{p} G'' \to 1$ induces an exact sequence

$$1 \longrightarrow \varprojlim_n G'/i^{-1}(G_n) \longrightarrow \varprojlim_n G/G_n \longrightarrow \varprojlim_n G''/p(G_n) \longrightarrow 1.$$

Proposition 4: For all $n \geqslant 0$ set $\hat{G}_n := \varprojlim_{m\geqslant n} G_n/G_m$. Then we have natural isomorphisms

(a) $\hat{G}/\hat{G}_n \cong G/G_n$ for all n, and

(b) $\hat{\hat{G}} := \varprojlim_n \hat{G}/\hat{G}_n \cong \varprojlim_n G/G_n = \hat{G}$.

Construction: Fix an ideal $\mathfrak{a}$ of R.

Definition: The $\mathfrak{a}$-*adic topology* on an R-module M is the one with basis $\{m+\mathfrak{a}^n M \mid m \in M, n \geqslant 0\}$. The $\mathfrak{a}$-*adic completion* of M is $\hat{M} := \varprojlim_n M/\mathfrak{a}^n M$.

Special Case: For $M = R$ the basis is $\{x + \mathfrak{a}^n \mid x \in R, n \geqslant 0\}$ and the completion is the ring $\hat{R} := \varprojlim_n R/\mathfrak{a}^n$.

Fact: The completion $\hat{M}$ of any R-module is an $\hat{R}$-module via the natural map

$$\begin{array}{ccc} \hat{R} \times \hat{M} & \to & \hat{M} \\ (x+\mathfrak{a}^n, m+\mathfrak{a}^n)_{n\geqslant 0} & \mapsto & (xm+\mathfrak{a}^n)_{n\geqslant 0}. \end{array}$$

Functoriality: (a) Any homomorphism of R-modules $\varphi\colon M \to N$ induces a natural homomorphism of $\hat{R}$-modules $\hat{\varphi}\colon \hat{M} \to \hat{N}$.

(b) For any homomorphisms of rings $\varphi\colon R \to S$ and any ideals $\mathfrak{a} \subset R$ and $\mathfrak{b} \subset S$ with $\varphi(\mathfrak{a}) \subset \mathfrak{b}$ we get a natural ring homomorphism $\hat{\varphi}\colon \hat{R} \to \hat{S}$.

Proposition 5: Any two ideals $\mathfrak{a}$ and $\mathfrak{a}'$ with $\exists k \geqslant 1\colon \mathfrak{a}^k \subset \mathfrak{a}' \ \wedge\ \mathfrak{a}'^k \subset \mathfrak{a}$ induce naturally isomorphic completions.

Note: The natural map $M \to \hat{M},\ m \mapsto (m + \mathfrak{a}^n)_{n\geqslant 0}$ is injective if and only if $\bigcap_{n\geqslant 0} \mathfrak{a}^n M = 0$. (Compare Krull's intersection theorem in Chapter 8.)

Proposition 6: Any short exact sequence of finitely generated modules over a noetherian ring

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

induces a short exact sequence

$$0 \to \hat{M}' \xrightarrow{\hat{i}} \hat{M} \xrightarrow{\hat{p}} \hat{M}'' \to 0.$$

Proposition 7: If R is noetherian, for any finitely generated R-module M we have a natural isomorphism $\hat{R} \otimes_R M \xrightarrow{\sim} \hat{M}$.

Proposition 8: If R is notherian, we have:

(a) $\hat{R} \otimes_R \mathfrak{a} = \hat{\mathfrak{a}}$.

(b) $\forall n \geqslant 0\colon \widehat{\mathfrak{a}^n} = \hat{\mathfrak{a}}^n$.

(c) $\forall m \geqslant n \geqslant 0\colon \mathfrak{a}^n/\mathfrak{a}^m \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^m$.

(d) $\hat{R}$ is its own $\mathfrak{a}$-adic or $\hat{\mathfrak{a}}$-adic completion.

(e) $\hat{\mathfrak{a}} \subset j(\hat{R})$.

Proposition 9: If R is noetherian and $\mathfrak{a} = \mathfrak{m}$ is a maximal ideal, then

(a) $\hat{R}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$, and

(b) $\hat{R}$ is isomorphic to the completion of $R_{\mathfrak{m}}$ with respect to $\mathfrak{m}_{\mathfrak{m}}$.

Caution: Completion does not preserve prime ideals (see exercise).

Example 2: $R[[X_1, \ldots, X_n]]$ is the completion of $R[X_1, \ldots, X_n]$ with respect to the ideal $(X_1, \ldots, X_n)$.

Caution: Completion does not commute with arbitrary localization:

Example 3: Let K be a field. Set $R := K[X, Y]$ and $\mathfrak{p} := R \cdot Y$. If we first localize we get $R_{\mathfrak{p}} = \{\frac{f}{g} \mid f, g \in R, Y \nmid g\}$ with maximal ideal $\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}} \cdot Y$, and the $\mathfrak{p}_{\mathfrak{p}}$-adic completion of $R_{\mathfrak{p}}$ is $\widehat{R_{\mathfrak{p}}} = K(X)[[Y]]$. If we first complete R with respect to $\mathfrak{p}$ we get $\hat{R} = K[X][[Y]]$ with the prime ideal $\hat{\mathfrak{p}} = R \cdot Y$, whose associated localization is $\hat{R}_{\hat{\mathfrak{p}}} = \{\frac{f}{g} \mid f, g \in K[X][[Y]], Y \nmid g\}$. There is a natural injective homomorphism $\hat{R}_{\hat{\mathfrak{p}}} \hookrightarrow \widehat{R_{\mathfrak{p}}}$ which, however, is not surjective.

Lemma 10: If R is noetherian and $\mathfrak{a} = (a_1, \ldots, a_r)$, there is a natural isomorphism $\hat{R} \cong R[[X_1, \ldots, X_r]]/(X_1 - a_1, \ldots, X_r - a_r)$.

Proposition 11: If R is noetherian, so is $\hat{R}$.

12 Valuation rings

Definition: A *totally ordered abelian group* is an abelian group $(\Gamma, +, 0)$ with a total order $\leqslant$ on Γ such that

$$\forall a, b, c \in \Gamma\colon\ a \leqslant b \implies a + c \leqslant b + c.$$

Example: Any additive subgroup of $\mathbb{R}$.

Fact: For any elements a, b, c, d of a totally ordered abelian group we have:

(a) $a \leqslant b \iff a + c \leqslant b + c$.

(b) $a \leqslant b \ \wedge\ c \leqslant d \implies a + c \leqslant b + d$.

(c) $a \leqslant b \iff -b \leqslant -a$.

Example: For any totally ordered abelian groups $\Gamma_1, \ldots, \Gamma_n$, the *lexicographical order* on $\Gamma := \Gamma_1 \boxplus \ldots \boxplus \Gamma_n$ is defined by

$$(a_1, \ldots, a_n) < (b_1, \ldots, b_n) \iff \exists k\colon a_k < b_k \ \wedge\ \forall i < k\colon a_i = b_i.$$

Definition: A *valuation* on a field K is a map $v\colon K \to \Gamma \cup \{\infty\}$ for a totally ordered abelian group $(\Gamma, +, 0)$ such that

(a) $\forall x \in K\colon v(x) = \infty \iff x = 0$.

(b) $\forall x, y \in K\colon v(xy) = v(x) + v(y)$.

(c) $\forall x, y \in K\colon v(x + y) \geqslant \min\{v(x), v(y)\}$.

In particular v induces a homomorphism $K^\times \to \Gamma$.

Definition: A valuation v is called *nontrivial* if

(d) $\exists x \in K\colon v(x) \neq 0, \infty$.

Definition: Valuations $v\colon K \to \Gamma \cup \{\infty\}$ and $v'\colon K \to \Gamma' \cup \{\infty\}$ are called *equivalent* if there exists an isomorphism of totally ordered groups $\varphi\colon v(K^\times) \xrightarrow{\sim} v'(K^\times)$ with $v'|_{K^\times} = \varphi \circ v|_{K^\times}$.

Fact: Every valuation is equivalent to one with $v(K^\times) = \Gamma$.

Lemma 1: Condition (c) is equivalent to saying that for every $a \in \Gamma$ the set $\{x \in K \mid v(x) \geqslant a\}$ is an additive subgroup of K, and it implies:

(c') $\forall x, y \in K\colon v(x) \neq v(y) \implies v(x + y) = \min\{v(x), v(y)\}$.

Definition: A valuation v on K

(a) has *rank 1* if $v(K^\times)$ is isomorphic to a subgroup of $(\mathbb{R}, +)$,

(b) is *(nontrivial) discrete* if $v(K^\times) \cong (\mathbb{Z}, +)$,

(c) is *normalized discrete* if $v(K^\times) = (\mathbb{Z}, +)$.

Fact: Any discrete valuation is equivalent to a unique normalized one.

Proposition 2: For any valuation v on K we have:

(a) $R := \{x \in K \mid v(x) \geqslant 0\}$ is a subring of K.

(b) $\forall x \in K \smallsetminus \{0\}\colon\ x \in R \ \vee\ x^{-1} \in R$.

(c) $\mathrm{Quot}(R) = K$.

(d) $R^\times = \{x \in K \mid v(x) = 0\}$.

(e) There exists a natural bijection

$$\begin{array}{rcl} \{\text{ideals of } R\} & \longleftrightarrow & \{I \subset \Gamma^{\geqslant 0} \cup \{\infty\} \text{ with } \infty \in I \text{ and } \forall a \in I\colon a + \Gamma^{\geqslant 0} \subset I\} \\ \mathfrak{a} & \longmapsto & v(\mathfrak{a}) \\ v^{-1}(I) & \longmapsfrom & I \end{array}$$

(f) R is a local ring.

Definition: This R is called the *valuation ring* associated to v.

Proposition 3: Any subring R of a field K with the property (b) from Proposition 2 is the valuation ring for some valuation v on K, and this v is unique up to equivalence.

Conclusion: One can introduce and study valuation rings without actually speaking of valuations, as in [Atiyah-Macdonald §5].

Definition: The valuation ring associated to a discrete valuation is called a *discrete valuation ring* or *DVR*.

Construction: Let p be a prime element of a unique factorization domain R_0. For any $f \in K := \mathrm{Quot}(R_0)$ define

$$\mathrm{ord}_p(f) := \begin{cases} \infty & \text{if } f = 0, \text{ respectively} \\ n & \text{if } f = p^n \cdot u \cdot p_1^{\pm 1} \cdots p_r^{\pm 1} \text{ for } n \in \mathbb{Z},\ u \in R^\times, \\ & \text{and primes } p_1, \ldots, p_r \text{ not associated to } p. \end{cases}$$

This is well defined since R_0 is a unique factorization domain. The associated discrete valuation ring is the localization $R_{0,(p)} = \{\frac{f}{g} \mid f, g \in R_0 \colon p \nmid g\}$.

Example 1: Take $R_0 := \mathbb{Z}$ and a prime number p. Then $K = \mathbb{Q}$, and the associated valuation ring is $R := \mathbb{Z}_{(p)}$.

Example 2: Take $R_0 := k[X]$ for a field k and an irreducible polynomial $p \in R_0$. In the special case $p = X - \xi$ for some $\xi \in k$, the number $\mathrm{ord}_p(f)$ is the vanishing order or minus the pole order of f at ξ.

Example 3: For $\frac{f}{g} \in K := k(X)$ with $f, g \in k[X]$ set

$$\mathrm{ord}_\infty(\tfrac{f}{g}) := \begin{cases} \infty & \text{if } f = 0, \\ \deg(g) - \deg(f) & \text{if } f \neq 0. \end{cases}$$

This valuation is the same as that for $R_0 := k[\frac{1}{X}]$ with the prime element $p := \frac{1}{X}$.

Proposition 4: The above examples yield all nontrivial valuations on $\mathbb{Q}$, and all nontrivial valuations on $k[X]$ that are trivial on k.

Example 4: Endow $\Gamma := \mathbb{Z}^2$ with the lexicographic order

$$(i, j) \leqslant (i', j') \iff (i < i') \vee (i = i \wedge j \leqslant j').$$

For $f = \sum'_{(i,j)\in\Gamma} a_{ij} X^i Y^j \in k[X, Y]$ define $v(f) := \inf\{(i, j) \in \Gamma \mid a_{ij} \neq 0\} \in \Gamma \cup \{\infty\}$. For any $f, g \in k[X, Y]$ with $g \neq 0$ set $v(\frac{f}{g}) := v(f) - v(g)$. This is a well-defined valuation on $k(X, Y)$ which is neither discrete nor of rank 1.

Now for some general abstract results.

Proposition 5: For any valuation ring R, we have:

(a) Any ring R' with $R \subset R' \subset \mathrm{Quot}(R)$ is a valuation ring.

(b) R is normal.

Example 4': The valuation ord_X on $k[X,Y]$ has the valuation ring $R' := k[X,Y]_{(X)}$, and with R the valuation ring from Example 4 we have $R \subsetneqq R' \subsetneqq \mathrm{Quot}(R)$.

Theorem 6: For any integral domain R and any prime ideal $\mathfrak{p} \subset R$ there exists a valuation ring $\widetilde{R} \subset K := \mathrm{Quot}(R)$ with $R \subset \widetilde{R}$ and maximal ideal $\mathfrak{m}$ such that $\mathfrak{m} \cap R = \mathfrak{p}$.

Definition: In that case we say that the valuation associated to $\widetilde{R}$ *lies over* $\mathfrak{p}$.

Proposition 7: For any integral domain R, the normalization $\widetilde{R}$ is the intersection of all valuation rings in $\mathrm{Quot}(R)$ which contain R.

Finally we discuss discrete valuation rings.

Proposition 8: Any discrete valuation ring is a local principal ideal domain of Krull dimension 1.

Proposition 9: For any noetherian local integral domain R of Krull dimension 1, with maximal ideal $\mathfrak{m}$, the following are equivalent:

(a) R is a discrete valuation ring.

(b) R is normal.

(c) $\mathfrak{m}$ is a principal ideal.

(d) $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$.

(e) Every non-zero ideal is a power of $\mathfrak{m}$.

(f) There exists $p \in R$ such that the non-zero ideals are the (p^r) for all $r \geqslant 0$.

Definition: For any normalized discrete valuation v on K, any element $p \in K$ with $v(p) = 1$ is called a *uniformizer of* R.

13 Dedekind rings

Definition: A noetherian normal integral domain of Krull dimension 1 is called a *Dedekind ring*.

Example: Any principal ideal domain which is not a field. In particular any discrete valuation ring.

Proposition 1: For any noetherian integral domain of Krull dimension 1 the folllowing are equivalent:

(a) R is Dedekind.

(b) Every primary ideal of R is a power of a prime ideal.

(c) $R_{\mathfrak{p}}$ is a discrete valuation ring for every maximal ideal $\mathfrak{p}$.

Note: For any $\mathfrak{p}$-primary ideal $\mathfrak{q}$ we have $\mathfrak{q} = \mathfrak{p}^n$ for a unique $1 \leqslant n < \infty$.

Note: Any localization of a Dedekind ring R, which is not 0 or $\mathrm{Quot}(R)$, is Dedekind.

Theorem 2: Any non-zero ideal of a Dedekind ring is a product of prime ideals and the factors are unique up to permutation.

Note: This unique factorization of ideals replaces unique factorization of elements, which does not hold in a general Dedekind ring.

Proposition 3: Let R be a normal noetherian integral domain and L a finite separable field extension of $K := \mathrm{Quot}(R)$. Let S be the integral closure of R in L. Then:

(a) S is a finitely generated R-module.

(b) S is a normal noetherian integral domain.

Proposition 4: For any Dedekind ring R and any finite separable field extension L of $\mathrm{Quot}(R)$, the integral closure of R in L is a Dedekind ring.

Definition: A finite field extension K of $\mathbb{Q}$ is called a *number field*. The integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called *the ring of (algebraic) integers in* K.

Proposition 5: Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K/\mathbb{Q}]$ and a Dedekind ring.

Example: An integer $a \in \mathbb{Z}$ with the property that $\forall b \in \mathbb{Z} : b \geqslant 2 \Longrightarrow b^2 \nmid a$ is called *square free*. The quadratic number fields $K/\mathbb{Q}$ with $[K/\mathbb{Q}] = 2$ are up to isomorphism in bijection with the set of square free integers $\neq 1$ by $K := \mathbb{Q}(\sqrt{a})$. For square free a we have:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} \bigoplus \mathbb{Z}\sqrt{a} & \text{if } a \not\equiv 1 \bmod 4, \\ \mathbb{Z} \bigoplus \mathbb{Z}\frac{1+\sqrt{a}}{2} & \text{if } a \equiv 1 \bmod 4. \end{cases}$$

Fix a Dedekind ring R with $K = \mathrm{Quot}(R)$.

Definition: A non-zero finitely generated R-submodule of K is called a *fractional ideal* of R. The set of fractional ideals is denoted I.

Lemma 6: Every fractional ideal of R is contained in $\frac{1}{a} \cdot R$ for some $a \in R \smallsetminus \{0\}$.

Proposition 7: The set I is an abelian group with respect to the multiplication

$$\mathfrak{a}\mathfrak{b} := \left\{ \textstyle\sum'_i a_i b_i \;\middle|\; a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

and with the identity elelement $(1) = R$. Moreover we have an isomorphism

$$\mathbb{Z}^{(\mathrm{Specmax}\, R)} \xrightarrow{\sim} I,\ (n_\mathfrak{p})_\mathfrak{p} \mapsto \prod_\mathfrak{p}{}' \mathfrak{p}^{n_\mathfrak{p}}.$$

Definition: A fractional ideal of the form $(a) := Ra$ for some $a \in K^\times$ is called *principal.* These form a subgroup of I, denoted by P.

Definition: The factor group $H := I/P$ is called the *(ideal) class group* of R. Its order $h := |H|$ is called the *(ideal) class number* of R.

Proposition 8: The following are equivalent:

(a) $H = 1$.

(b) R is a principal ideal domain.

(c) All prime ideals of R are principal.

(d) R is a unique factorization domain.

Interpretation: The class number measures how much R deviates from being a principal ideal domain.

Note: The natural exact sequence

$$1 \longrightarrow R^\times \longrightarrow K^\times \longrightarrow I \longrightarrow H \longrightarrow 0$$

connects the group of units $R^\times$ with the class group H.

Theorem 9: *(without proof)* For any Dedekind ring which is finitely generated over $\mathbb{Z}$ or $\mathbb{F}_p$ we have:

(a) $R^\times$ is finitely generated.

(b) H is finite.

For the moment R be an arbitrary integral domain with $K = \mathrm{Quot}(R)$.

Definition: Let M be an R-module.

(a) An element $m \in M$ is *torsion* if $\exists a \in R \smallsetminus \{0\} : am = 0$.

(b) M is called *torsion* if each $m \in M$ is torsion.

(c) M is called *torsion free* if it has no non-zero torsion elements.

Proposition 10: The set M^{tor} of torsion elements of M is the unique R-submodule N which is torsion such that M/N is torsion free.

Example: $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module, but it is not annihilated by a single element of $\mathbb{Z} \smallsetminus \{0\}$.

Definition: The *rank* of an R-module M is $\mathrm{rank}_R(M) := \dim_K(K \otimes_R M)$.

Note: This is equal to $\sup\{i \geqslant 0 \mid \exists m_1, \ldots, m_n \in M \text{ linearly independent over } R\}$.

Proposition 11: If M is generated by n elements, then $\mathrm{rank}_R(M) \leqslant n$.

Proposition 12: $\mathrm{rank}(M) = 0$ if and only if $M = M^{tor}$.

Proposition 13: For any short exact sequence $0 \to M' \to M \to M'' \to 0$ of R-modules we have $\mathrm{rank}(M) = \mathrm{rank}(M') + \mathrm{rank}(M'')$.

Now we return to a Dedekind ring R with $K = \mathrm{Quot}(R)$.

Lemma 14: For any fractional ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ we have:

(a) $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathfrak{ac} \subset \mathfrak{bc}$.

(b) There exists $x \in K^\times$ such that $x\mathfrak{b} \subset \mathfrak{a}$.

(c) For any such x there exists $y \in K^\times$ such that $x\mathfrak{b} + y\mathfrak{c} = \mathfrak{a}$.

Proposition 15: Every fractional ideal is generated by two elements.

Proposition 16: For any two fractional ideals $\mathfrak{b}, \mathfrak{c}$ there exists an isomorphism of R-modules $\mathfrak{b} \boxplus \mathfrak{c} \cong R \boxplus \mathfrak{bc}$.

Example: For any fractional ideal of $\mathfrak{a} \in K$ we have $K \otimes_R \mathfrak{a} \cong K$ and $\mathfrak{a}$ is torsion free of rank 1.

Proposition 17: Every torsion free finitely generated R-module of rank 1 is isomorphic as a module to a fractional ideal.

Proposition 18: Any fractional ideal is a projective R-module.

Proposition 19: For any finitely generated R-module M the following are equivalent:

(a) M is torsion free.

(b) M is flat.

(c) M is projective.

(d) M is isomorphic to a direct sum of fractional ideals.

(e) $M = 0$ or $M \cong R^{r-1} \boxplus \mathfrak{a}$ for $r := \operatorname{rank}_R(M) \geqslant 1$ and a fractional ideal $\mathfrak{a}$.

Proposition 20: For any fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ and $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ the following are equivalent:

(a) $\mathfrak{a}_1 \boxplus \ldots \boxplus \mathfrak{a}_r \cong \mathfrak{b}_1 \boxplus \ldots \boxplus \mathfrak{b}_r$.

(b) $\mathfrak{a}_1 \cdots \mathfrak{a}_r \cong \mathfrak{b}_1 \cdots \mathfrak{b}_r$.

(c) $\mathfrak{a}_1 \cdots \mathfrak{a}_r$ and $\mathfrak{b}_1 \cdots \mathfrak{b}_r$ represent the same ideal class.

Corollary 21: In Proposition 19 (e) the ideal $\mathfrak{a}$ is unique up to equivalence.

Proposition 22: For any finitely generated R-module M we have $M \cong M^{tor} \boxplus M/M^{tor}$.

Proposition 23: Every finitely generated torsion module M is isomorphic to $\boxplus_{i=1}^{t} R/\mathfrak{p}_i^{\nu_i}$ for maximal ideals $\mathfrak{p}_i$ and $\nu_i \in \mathbb{Z}^{\geqslant 0}$, and the pairs $(\mathfrak{p}_i, \nu_i)$ are unique up to permutation.

Theorem 24: Every finitely generated R-module is isomorphic to

$$\left\{ \begin{array}{c} 0 \\ R^{r-1} \boxplus \mathfrak{a} \end{array} \right\} \boxplus \bigboxplus_{i=1}^{t} R/\mathfrak{p}_i^{\nu_i},$$

where everything is unique up to equivalence resp. permutation.

The following two appendices are copied from the lecture course Algebra I of Fall Semester 2015, which was held in German.

Anhang A Ringe

Kommutative unitäre Ringe sowie Moduln über solchen sind Gegenstand des Gebiets der *Kommutativen Algebra*. Wir behandeln einige Grundlagen daraus.

A.1 Grundbegriffe

Sei R eine Menge mit Abbildungen

$$\begin{aligned} +: &\quad R \times R \to R, \quad (x,y) \mapsto x+y, \\ \cdot: &\quad R \times R \to R, \quad (x,y) \mapsto x \cdot y = xy, \end{aligned}$$

und ausgezeichneten Elementen $0 = 0_R$ sowie $1 = 1_R \in R$. Betrachte die Axiome:

(1)	$\forall x,y,z \in R$:	$x+(y+z) = (x+y)+z$	Assoziativität der Addition
(2)	$\forall x,y \in R$:	$x+y = y+x$	Kommutativität der Addition
(3)	$\forall x \in R$:	$0+x = x$	Neutrales Element der Addition
(4)	$\forall x \in R\ \exists x' \in R$:	$x+x' = 0$	Inverses Element der Addition
(5)	$\forall x,y,z \in R$:	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	Assoziativität der Multiplikation
(6)	$\forall x,y,z \in R$:	$\left\{ \begin{array}{l} x \cdot (y+z) = x \cdot y + x \cdot z \\ (y+z) \cdot x = y \cdot x + z \cdot x \end{array} \right\}$	Distributivität
(7)	$\forall x,y \in R$:	$x \cdot y = y \cdot x$	Kommutativität der Multiplikation
(8)	$\forall x \in R$:	$1 \cdot x = x$	Neutrales Element der Multiplikation
(9)		$1 \neq 0$	Nichttrivialität
(10)	$\forall x \in R \smallsetminus \{0\}\ \exists x' \in R$:	$x' \cdot x = 1$	Inverses Element der Multiplikation

Definition: Ein Tupel $(R, +, \cdot, 0, 1)$

(a) mit den Axiomen (1) bis (8) heisst ein *kommutativer unitärer Ring* oder *kommutativer Ring mit Eins*.

(b) mit den Axiomen (1) bis (10) heisst ein *Körper*.

Konvention: Einen kommutativen unitären Ring nennen wir in diesem Abschnitt nur kurz *Ring*. (Aber Vorsicht: Gewisse weitere Begriffe werden beim Fehlen eines Einselementes anders definiert.) Wie üblich schreiben wir nur kurz R anstelle des ganzen Tupels und sehen die Zusatzdaten als implizit mitgegeben an.

Sei also R ein Ring.

Bemerkung: Die Axiome (1) bis (4) besagen, dass $(R, +, 0)$ eine abelsche Gruppe ist, genannt die *additive Gruppe von* R. Insbesondere ist das inverse Element $-x$ von x

bezüglich der Addition eindeutig bestimmt. Für $x + (-y)$ schreibt man auch kürzer $x - y$. Für jede ganze Zahl n ist das *n-te Vielfache von x* definiert durch

$$n \cdot x := \begin{cases} x + \ldots + x \text{ mit } n \text{ Summanden} & \text{falls } n > 0, \\ 0 & \text{falls } n = 0, \\ -(x + \ldots + x) \text{ mit } |n| \text{ Summanden} & \text{falls } n < 0. \end{cases}$$

Rechenregeln: Für alle $x, y \in R$ und alle $m, n \in \mathbb{Z}$ gilt:

$$\begin{aligned} (\pm n) \cdot x &= \pm(n \cdot x) \\ (m \pm n) \cdot x &= m \cdot x \pm n \cdot x \\ m \cdot (x \pm y) &= m \cdot x \pm m \cdot y \\ (m \cdot n) \cdot x &= m \cdot (n \cdot x) \\ m \cdot (x \cdot y) &= (m \cdot x) \cdot y \end{aligned}$$

Bemerkung: Für jede ganze Zahl $n \geqslant 0$ ist die *n-te Potenz von x* definiert durch

$$x^n := \begin{cases} x \cdots x \text{ mit } n \text{ Faktoren} & \text{falls } n > 0, \\ 1 & \text{falls } n = 0. \end{cases}$$

Rechenregeln: Für alle $x, y \in K$ und alle $m, n \geqslant 0$ gilt:

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \\ (x \cdot y)^m &= x^m \cdot y^m \\ x^{m \cdot n} &= (x^m)^n \end{aligned}$$

Bemerkung: Für Summen $\sum_{i \in I} x_i$ und Produkte $\prod_{i \in I} x_i$ in einem Ring gelten die gleichen Konventionen und Grundregeln wie in einem Körper.

Proposition: Es ist $1 = 0$ genau dann, wenn der Ring der Nullring ist.

A.2 Einheiten

Definition: Ein Element $x \in R$ mit der Eigenschaft

$$\exists x' \in R\colon \; x' \cdot x = 1$$

heisst *invertierbar* oder eine *Einheit von R*. Die Menge aller Einheiten von R bezeichnen wir mit $R^\times$ (sprich „R Kreuz“) oder auch R^*.

Proposition: Die Menge $R^\times$ ist bezüglich Multiplikation eine abelsche Gruppe, genannt die *Einheitengruppe von R*.

Insbesondere ist das inverse Element x' jeder Einheit x eindeutig bestimmt. Es wird bezeichnet mit x^{-1} oder $\frac{1}{x}$. Für $\frac{1}{x} \cdot y$ schreibt man auch $\frac{y}{x}$. Weiter ist jedes Produkt und

jeder Quotient von Einheiten eine Einheit, und das Einselement 1 ist eine Einheit. Für jede Einheit x und jede natürliche Zahl n definieren wir $x^{-n} := (x^{-1})^n$, mit denselben Rechenregeln wie oben.

Beispiel: Für jeden Körper K ist $K^\times = K \smallsetminus \{0\}$.

Beispiel: Es ist $\mathbb{Z}^\times = \{\pm 1\}$.

A.3 Homomorphismen

Betrachte zwei Ringe R und S.

Definition: Ein *(Ring)-Homomorphismus* $\varphi\colon R \to S$ ist eine Abbildung mit

(a) $\varphi(1_R) = 1_S$.

(b) $\forall x, y \in R\colon\ \varphi(x+y) = \varphi(x) + \varphi(y)$.

(c) $\forall x, y \in R\colon\ \varphi(xy) = \varphi(x)\varphi(y)$.

Proposition: Für jeden Homomorphismus $\varphi\colon R \to S$ gilt:

(a) $\forall x \in R\ \forall n \in \mathbb{Z}\colon\ \varphi(nx) = n\varphi(x)$.

(b) $\forall x \in R\ \forall n \in \mathbb{Z}^{\geqslant 0}\colon\ \varphi(x^n) = \varphi(x)^n$.

(c) φ induziert einen Gruppenhomomorphismus $R^\times \to S^\times$.

Proposition: Die Identität $\mathrm{id}_R\colon R \to R$ ist ein Homomorphismus. Die Komposition zweier Homomorphismen ist ein Homomorphismus.

Proposition: Jeder Homomorphismus zwischen zwei Körpern ist injektiv.

Beispiel: Für jeden Ring R existiert genau ein Ringhomomorphismus $\mathbb{Z} \to R$, nämlich die Abbildung $n \mapsto n \cdot 1_R$.

Definition: Ein Homomorphismus $\varphi\colon R \to S$ mit einem beidseitigem Inversen φ^{-1} heisst ein *Isomorphismus*, und wir schreiben dann $\varphi\colon R \xrightarrow{\sim} S$. Existiert ein Isomorphismus $R \xrightarrow{\sim} S$, so heissen R und S *isomorph* und wir schreiben $R \cong S$.

Proposition: Ein Homomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

Proposition: Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von Ringen ist eine Äquivalenzrelation.

Definition: Ein Isomorphismus $R \xrightarrow{\sim} R$ heisst ein *Automorphismus von R*.

A.4 Polynomringe

Sei N eine Menge, und sei $\underline{X} = (X_\nu)_{\nu\in N}$ ein System paarweise verschiedener neuer Symbole X_ν.

Konstruktion: Sei I_N die Menge aller Abbildungen $\underline{i}\colon N \to \mathbb{Z}^{\geqslant 0}$, $\nu \mapsto i_\nu$ mit endlichem Träger, das heisst, mit $i_\nu = 0$ für fast alle ν. Sei $R[\underline{X}]$ die Menge aller Abbildungen $I_N \to R$, $\underline{i} \mapsto a_{\underline{i}}$ mit endlichem Träger, das heisst, mit $a_{\underline{i}} = 0$ für fast alle $\underline{i}$. Für zwei Elemente von $R[\underline{X}]$ definieren wir

$$\begin{aligned}(a_{\underline{i}})_{\underline{i}} + (b_{\underline{i}})_{\underline{i}} &:= (a_{\underline{i}} + b_{\underline{i}})_{\underline{i}}\\ (a_{\underline{i}})_{\underline{i}} \cdot (b_{\underline{i}})_{\underline{i}} &:= \big(\textstyle\sum_{\underline{i}+\underline{j}=\underline{k}} a_{\underline{i}} \cdot b_{\underline{j}}\big)_{\underline{k}}\end{aligned}$$

Betrachte weiter die Abbildung

$$\iota\colon\ R \to R[\underline{X}],\ a \mapsto \Big(\begin{cases} a & \text{wenn alle } i_\nu = 0 \text{ sind,} \\ 0 & \text{sonst} \end{cases} \Big)_{\underline{i}}$$

und bezeichne $0 := \iota(0)$ und $1 := \iota(1)$. Für jedes $\nu \in N$ sei

$$X_\nu := \Big(\begin{cases} 1 & \text{wenn } i_\nu = 1 \text{ ist und alle anderen } i_{\nu'} = 0, \\ 0 & \text{sonst} \end{cases} \Big)_{\underline{i}} \in R[\underline{X}].$$

Proposition: $(R[\underline{X}], +, \cdot, 0, 1)$ ist ein Ring und ι ein injektiver Ringhomomorphismus.

Wir identifizieren R mit seinem Bild unter ι. Für alle $\underline{i} \in I_N$ schreiben wir

$$\underline{X}^{\underline{i}} := \prod_{\nu\in N}{}' X_\nu^{i_\nu} \overset{!}{=} \Big(\begin{cases} 1 & \text{wenn } \underline{i}' = \underline{i}, \\ 0 & \text{sonst} \end{cases} \Big)_{\underline{i}'}.$$

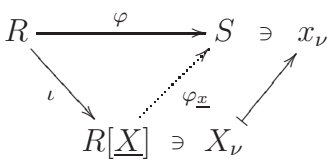
Dann hat jedes Element von $R[\underline{X}]$ die Form

$$(a_{\underline{i}})_{\underline{i}} = \sum_{\underline{i}\in I_N}{}' a_{\underline{i}} \underline{X}^{\underline{i}}.$$

Einen solchen Ausdruck nennen wir ein *Polynom*. Ein Ausdruck der Form $a\underline{X}^{\underline{i}}$ für $a \in R$ heisst ein *Monom*. Für alle $\underline{i}, \underline{j} \in I_N$ gilt

$$\underline{X}^{\underline{i}} \cdot \underline{X}^{\underline{j}} = \underline{X}^{\underline{i}+\underline{j}}.$$

Proposition: *(Universelle Eigenschaft)* Für jeden Ring S, jeden Ringhomomorphismus $\varphi\colon R \to S$, und jedes System $\underline{x} = (x_\nu)_{\nu\in N} \in S^N$ existiert genau ein Ringhomomorphismus $\varphi_{\underline{x}}\colon R[\underline{X}] \to S$ mit $\varphi_{\underline{x}} \circ \iota = \varphi$ und $\forall \nu \in N\colon \varphi_{\underline{x}}(X_\nu) = x_\nu$, das heisst, so dass das folgende Diagramm kommutiert:



Genauer ist $\varphi_{\underline{x}}$ die *Auswertungsabbildung*

$$R[\underline{X}] \to S,\ F(\underline{X}) = \sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}} \mapsto F(\underline{x}) := \sum_{\underline{i}\in I_N}{}' \varphi(a_{\underline{i}})\underline{x}^{\underline{i}}.$$

Wir nennen $F(\underline{x})$ den *Wert von F an der Stelle $\underline{x}$*. Jedes Polynom F induziert somit für alle $\varphi\colon R \to S$ eine *Polynomfunktion*

$$S^N \to S,\ \underline{x} \mapsto F(\underline{x}).$$

Bemerkung: Man könnte den Polynomring auch durch die universelle Eigenschaft abstrakt definieren und zeigen, dass er durch diese bis auf eindeutige Isomorphie bestimmt ist.

Spezialfall: *(Funktorialität)* Jeder Ringhomomorphismus $\varphi\colon R \to S$ induziert einen eindeutigen Ringhomomorphismus $\tilde{\varphi}\colon R[\underline{X}] \to S[\underline{X}]$ mit $\tilde{\varphi}|_R = \varphi$ und $\tilde{\varphi}(X_\nu) = X_\nu$, nämlich

$$\sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}} \ \mapsto \sum_{\underline{i}\in I_N}{}' \varphi(a_{\underline{i}})\underline{X}^{\underline{i}}.$$

Proposition: Seien K ein Körper und V ein K-Vektorraum mit Basis $\underline{X} = (X_\nu)_{\nu\in N}$. Dann existiert ein natürlicher Isomorphismus auf die symmetrische Algebra

$$K[\underline{X}] \xrightarrow{\sim} SV := \coprod_{r\geqslant 0} S^r V, \quad \sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}} \ \mapsto \sum_{\underline{i}\in I_N}{}' a_{\underline{i}}\underline{X}^{\underline{i}}.$$

Notation: Im Fall $\underline{X} = (X_1, \ldots, X_n)$ schreiben wir auch $R[X_1, \ldots, X_n] := R[\underline{X}]$.

Proposition: Für alle $0 \leqslant m \leqslant n$ existiert ein natürlicher Isomorphismus

$$R[X_1, \ldots, X_n] \ \cong\ R[X_1, \ldots, X_m][X_{m+1}, \ldots, X_n].$$

Variante: Für $\underline{X} = (X_1, \ldots, X_n)$ sei $R[[\underline{X}]]$ die Menge aller Abbildungen $(\mathbb{Z}^{\geqslant 0})^n \to R$, $\underline{i} \mapsto a_{\underline{i}}$, ohne Endlichkeitsbedingungen. Definiere Summe und Produkt zweier Elemente von $R[[\underline{X}]]$ sowie die Inklusion $\iota\colon R \hookrightarrow R[[\underline{X}]]$ durch die gleichen Formeln wie oben.

Proposition: $(R[[\underline{X}]], +, \cdot, 0, 1)$ ist ein Ring und ι ein injektiver Ringhomomorphismus.

Wieder identifizieren wir R mit seinem Bild unter ι. Ein Element von $R[[\underline{X}]]$ schreiben wir in der Form

$$(a_{\underline{i}})_{\underline{i}} \ = \ \sum_{\underline{i}\in I_N} a_{\underline{i}}\underline{X}^{\underline{i}},$$

was aber nur als Notation und nicht als irgendeine Art von unendlicher Summe oder Reihe zu verstehen ist. Einen solchen Ausdruck nennen wir eine *formale Potenzreihe in den Variablen $X_1, \ldots, X_n$ über R*. Mit dieser Notation unterliegen alle Rechnungen denselben Regeln wie für Potenzreihen in der Analysis.

A.5 Unterringe, Produkte

Definition: Ein *Unterring von R* ist eine Teilmenge $R' \subset R$ mit den Eigenschaften:

(a) $\forall x, y \in R' \colon\ x + y \in R'$.
(b) $\forall x, y \in R' \colon\ xy \in R'$.
(c) $\forall x \in R' \colon\ -x \in R'$.
(d) $1 \in R'$.

Die Teilmenge R' bildet dann zusammen mit den Restriktion der Operationen von R selbst einen Ring, und die Inklusionsabbildung $R' \hookrightarrow R$ einen Ringhomomorphismus.

Beispiel: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Beispiel: $R \subset R[\underline{X}] \subset R[[\underline{X}]]$.

Proposition: Der Durchschnitt jeder nichtleeren Kollektion von Unterringen von R ist ein Unterring von R.

Proposition: Für jeden Unterring $R' \subset R$ und jede Teilmenge $A \subset R$ existiert ein eindeutiger kleinster Unterring von R, welcher R' und A enthält. Dieser besteht aus allen Elementen der Form

$$\sum_{i_1,\ldots,i_n \geqslant 0}{}' x_{i_1,\ldots,i_n} a_1^{i_1} \cdots a_n^{i_n}$$

mit $n \geqslant 0$ und $a_1, \ldots, a_n \in A$ und $x_{i_1,\ldots,i_n} \in R'$, fast alle gleich 0.

Definition: Dieser Unterring heisst *der von A über R' erzeugte Unterring* und wird bezeichnet mit $R'[A]$. Für endlich viele Elemente $a_1, \ldots, a_n \in R$ schreiben wir auch $R'[a_1, \ldots, a_n] := R'[\{a_1, \ldots, a_n\}]$.

Bemerkung: Dies bewirkt keine Kollision mit der Notation für den Polynomring $R[X_1, \ldots, X_n]$, da letzterer tatsächlich der von den Elementen $X_1, \ldots, X_n$ über R erzeugte Unterring von $R[X_1, \ldots, X_n]$ ist.

Beispiel: Der Unterring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ von $\mathbb{C}$.

Beispiel: Es ist $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Beispiel: Der Unterring $\mathbb{Z}[\sqrt{7}\,] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$ von $\mathbb{R}$.

Beispiel: Es ist $\mathbb{Z}[\sqrt{7}\,]^\times = \{\pm(8 + 3\sqrt{7})^n \mid n \in \mathbb{Z}\}$.

Proposition-Definition: Das *kartesische Produkt* von Ringen $R_1 \times \ldots \times R_n$ mit komponentenweiser Addition und Multiplikation sowie dem Nullelement $(0, \ldots, 0)$ und dem Einselement $(1, \ldots, 1)$ ist ein Ring. Für diesen gilt weiter $(R_1 \times \ldots \times R_n)^\times = R_1^\times \times \ldots \times R_n^\times$ und darin $(x_1, \ldots, x_n)^{-1} = (x_1^{-1}, \ldots, x_n^{-1})$.

Proposition-Definition: Für jeden Ring R und jede Menge X ist die Menge R^X aller Funktionen $f\colon X \to R$ mit punktweiser Addition $(f+g)(x) = f(x)+g(x)$ und Multiplikation $(f\cdot g)(x) = f(x)\cdot g(x)$ sowie den konstanten Funktionen 0 als Nullelement und 1 als Einselement ein Ring.

Bemerkung: Für $R^n = R\times\ldots\times R = R^{\{1,\ldots,n\}}$ stimmen beide Konstruktionen überein.

Bemerkung: Viele interessante Ringe sind Unterringe von Funktionenringen, zum Beispiel die Ringe aller stetigen oder differenzierbaren oder holomorphen Funktionen auf Teilmengen von $\mathbb{R}$ oder $\mathbb{R}^d$ oder $\mathbb{C}$.

A.6 Matrizen

Für alle natürlichen Zahlen m, n bezeichnet $\mathrm{Mat}_{m\times n}(R)$ die Menge aller $m\times n$-Matrizen mit Koeffizienten in R. Summe und Produkt von Matrizen über R sind durch dieselben Formeln definiert wie über einem Körper.

Lemma: Sei K ein unendlicher Körper, und sei $f \in K[X_1,\ldots,X_n]$ mit $f(\underline{a}) = 0$ für alle $\underline{a} \in K^n$. Dann ist $f = 0$.

Meta-Proposition: Jede Rechenregel für Matrizen über $\mathbb{Q}$, die nur die Operationen $+$ und $-$ und $\cdot$ sowie die Konstanten 0 und 1 beinhaltet, gilt auch für Matrizen über einem beliebigen Ring.

Beispiel: Für alle Matrizen entsprechender Grösse über einem beliebigen Ring gilt

(a) $A(BC) = (AB)C$.

(b) $I_m A = AI_n = A$.

(c) $\det(AB) = \det(A)\det(B)$.

(d) $A\tilde{A} = \tilde{A}A = \det(A)\cdot I_n$ für die Adjunkte $\tilde{A} := \big((-1)^{i+j}\cdot\det(A_{ji})\big)_{i,j}$ von A.

(e) $\mathrm{char}_A(A) = 0$ für das charakteristische Polynom $\mathrm{char}_A(X) := \det(X\cdot I_n - A)$.

Proposition-Definition: Für jede Matrix $A \in \mathrm{Mat}_{n\times n}(R)$ sind äquivalent:

(a) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $AA' = A'A = I_n$. Dann heisst A *invertierbar*.

(b) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $AA' = I_n$.

(c) Es existiert $A' \in \mathrm{Mat}_{n\times n}(R)$ mit $A'A = I_n$.

(d) $\det(A) \in R^\times$.

Die Matrix A' ist durch (b) oder (c) eindeutig bestimmt und heisst die *Inverse* A^{-1}.

Proposition-Definition: Die Menge $\mathrm{GL}_n(R)$ aller invertierbaren $n\times n$-Matrizen über R ist eine Gruppe mit der Matrixmultiplikation und dem neutralen Element I_n. Sie heisst die *allgemeine lineare Gruppe vom Grad n über R.*

A.7 Integritätsbereiche

Definition: Ein *Nullteiler von* R ist ein Element $x \in R$ mit

$$\exists y \in R \smallsetminus \{0\}\colon \ xy = 0.$$

(Manche Autoren verlangen zusätzlich $x \neq 0$.)

Definition: Ein Ring mit $1 \neq 0$ und ohne Nullteiler $\neq 0$ heisst ein *Integritätsbereich*.

Proposition: In jedem Integritätsbereich gilt die *Kürzungsregel*:

$$\forall x, y, z \in R\colon \ (x \neq 0 \text{ und } xy = xz) \longrightarrow y = z.$$

Beispiel: Jeder Körper ist ein Integritätsbereich.

Beispiel: Jeder Unterring eines Integritätsbereichs ist ein Integritätsbereich.

Proposition: Für jeden Integritätsbereich R ist auch $R[\underline{X}]$ und $R[[\underline{X}]]$ ein Integritätsbereich.

A.8 Quotientenkörper

Sei R ein Integritätsbereich.

Konstruktion-Proposition: Auf der Menge der Paare $R \times (R \smallsetminus \{0\})$ ist durch

$$(x,y) \sim (x',y') \;:\Longleftrightarrow\; xy' = x'y.$$

eine Äquivalenzrelation definiert. Bezeichne die Äquivalenzklasse eines Paars (x,y) mit $[(x,y)]$ und die Menge aller Äquivalenzklassen mit $\mathrm{Quot}(R)$. Dann sind die Operationen

$$\begin{aligned}[(x,y)] + [(x',y')] &:= [(xy'+x'y, yy')] \\ [(x,y)] \cdot [(x',y')] &:= [(xx', yy')]\end{aligned}$$

wohldefiniert auf $\mathrm{Quot}(R)$. Betrachte weiter die Abbildung

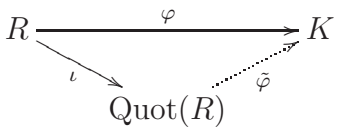
$$\iota\colon\ R \to \mathrm{Quot}(R),\ x \mapsto [(x,1)]$$

und bezeichne $0 := \iota(0)$ und $1 := \iota(1)$. Dann ist $(\mathrm{Quot}(R), +, \cdot, 0, 1)$ ein Körper und ι ein injektiver Ringhomomorphismus.

Definition: Der Körper $\mathrm{Quot}(R)$ heisst der *Quotientenkörper von R*. Wir identifizieren R mit seinem Bild unter ι. In $\mathrm{Quot}(R)$ gilt dann

$$[(x,y)] \;=\; \frac{\iota(x)}{\iota(y)} \;=\; \frac{x}{y}.$$

Proposition: *(Universelle Eigenschaft)* Für jeden injektiven Ringhomomorphismus $\varphi\colon R \to K$ in einen Körper K existiert genau ein Ringhomomorphismus $\tilde{\varphi}\colon \mathrm{Quot}(R) \to K$ mit $\tilde{\varphi} \circ \iota = \varphi$, das heisst, so dass das folgende Diagramm kommutiert:



Bemerkung: Man könnte den Quotientenkörper auch durch die universelle Eigenschaft abstrakt definieren und zeigen, dass er durch diese bis auf eindeutige Isomorphie bestimmt ist.

Folge: *(Funktorialität)* Jeder injektive (und nur jeder solche) Ringhomomorphismus von Integritätsbereichen $\varphi\colon R \to S$ setzt sich fort zu einem eindeutigen Ringhomomorphismus $\tilde{\varphi}\colon \mathrm{Quot}(R) \to \mathrm{Quot}(S)$.

Beispiel: Der Körper der rationalen Zahlen $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$.

Beispiel: Es ist $\mathrm{Quot}(\mathbb{Z}[i]) \cong \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

Definition: Für jeden Körper K heisst $K(X_1, \ldots, X_n) := \mathrm{Quot}(K[X_1, \ldots, X_n])$ der Körper der *rationalen Funktionen in den Variablen $X_1, \ldots, X_n$ über K*.

Beispiel: In der Funktionentheorie definiert man den Körper der meromorphen Funktionen auf einer zusammenhängenden offenen Teilmenge $U \subset \mathbb{C}$. Dieser stellt sich heraus als der Quotientenkörper des Unterrings der holomorphen Funktionen.

A.9 Ideale

Sei R ein Ring.

Definition: Ein *Ideal von* R ist eine Teilmenge $\mathfrak{a} \subset R$ mit den Eigenschaften:

(a) $\mathfrak{a} \neq \varnothing$.

(b) $\forall a, b \in \mathfrak{a}\colon\ a + b \in \mathfrak{a}$.

(c) $\forall x \in R\ \forall a \in \mathfrak{a}\colon\ xa \in \mathfrak{a}$.

Wegen (c) gilt dann auch $\forall a \in \mathfrak{a}\colon\ -a \in \mathfrak{a}$; wegen (a) und (b) ist das Ideal also eine additive Untergruppe von R. Die Bedingungen bedeuten auch, dass für alle $n \geqslant 0$, alle $x_i \in R$, und alle $a_i \in \mathfrak{a}$ auch $\sum_{i=1}^{n} x_i a_i \in \mathfrak{a}$ ist.

Proposition-Definition: Für jedes Element $a \in R$ ist

$$(a) \ := \ \{xa \mid x \in R\}$$

ein Ideal von R, genannt das *von a erzeugte Hauptideal*.

Beispiel: Das *Nullideal* $(0) = \{0\}$.

Beispiel: Das *Einsideal* $(1) = R$.

Proposition: (a) Es ist $(a) = (1)$ genau dann, wenn a eine Einheit von R ist.

(b) Ein Ideal $\mathfrak{a}$ ist gleich (1) genau dann, wenn es das Einselement enthält.

Proposition: Für alle $a, b \in R$ gilt

$$a|b \iff (a) \ni b \iff (a) \supset (b).$$

Proposition: Der Durchschnitt jeder nichtleeren Kollektion von Idealen ist ein Ideal.

Proposition-Definition: Die Summe jeder Kollektion von Idealen $\{\mathfrak{a}_\nu \mid \nu \in N\}$ ist ein Ideal:

$$\sum_{\nu \in N} \mathfrak{a}_\nu := \Big\{ \sum_{\nu \in N}{}' a_\nu \ \Big|\ \begin{array}{l} \text{alle } a_\nu \in \mathfrak{a}_\nu, \\ \text{fast alle } a_\nu = 0 \end{array} \Big\}.$$

Proposition-Definition: Für jede Teilmenge $A \subset R$ ist die folgende Menge ein Ideal:

$$(A) \ := \ \Big\{ \sum_{a \in A}{}' x_a a \ \Big|\ \begin{array}{l} \text{alle } x_a \in R, \\ \text{fast alle } x_a = 0 \end{array} \Big\} \ = \ \sum_{a \in A} (a),$$

genannt *von A erzeugt*. Für endlich viele Elemente $a_1, \ldots, a_n \in R$ schreiben wir auch

$$(a_1, \ldots, a_n) \ := \ (\{a_1, \ldots, a_n\}) \ = \ (a_1) + \ldots + (a_n)$$

und hoffen auf möglichst wenig Verwechslung mit dem Tupel $(a_1, \ldots, a_n)$.

Proposition: Für jede Teilmenge A eines Ideals $\mathfrak{a}$ gilt $(A) \subset \mathfrak{a}$.

Bemerkung: Jeder gemeinsame Teiler von Elementen $a_1, \dots, a_n$ ist ein gemeinsamer Teiler aller Elemente des Ideals $(a_1, \dots, a_n)$. Der Begriff des Ideals enthält also alle Informationen über Teilbarkeit, auch wenn der Ring nicht faktoriell ist. Genau zu diesem Zweck hat Dedekind den Begriff des Ideals erfunden, um seine Vorstellung von *idealen Zahlen* zu konkretisieren.

Proposition: Für jedes $x \in R$ und jedes Ideal $\mathfrak{a}$ ist die folgende Menge ein Ideal

$$x\mathfrak{a} \;:=\; x \cdot \mathfrak{a} \;:=\; \{xa \mid a \in \mathfrak{a}\}.$$

Definition: Das *Produkt* zweier Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R ist das von den Elementen ab für alle $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ erzeugte Ideal

$$\mathfrak{a}\mathfrak{b} \;:=\; \mathfrak{a} \cdot \mathfrak{b} := \Big\{ \sum_{i=1}^{n} a_i b_i \;\Big|\; \text{alle } n \geqslant 0,\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \Big\}.$$

Definition: Die *n-te Potenz* eines Ideals $\mathfrak{a}$ ist definiert durch

$$\mathfrak{a}^n \;:=\; \begin{cases} \mathfrak{a} \cdots \mathfrak{a} \ \text{ mit } n \text{ Faktoren} & \text{falls } n > 0, \\ R & \text{falls } n = 0. \end{cases}$$

Proposition: Für alle Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, alle $x, y \in R$, und alle $m, n \in \mathbb{Z}^{\geqslant 0}$ gilt

$$\begin{aligned}
(x)\mathfrak{a} &= x\mathfrak{a} \\
(x)(y) &= (xy) \\
\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) &= \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} \\
x(\mathfrak{a}+\mathfrak{b}) &= x\mathfrak{a} + x\mathfrak{b} \\
\mathfrak{a}(\mathfrak{b}\mathfrak{c}) &= (\mathfrak{a}\mathfrak{b})\mathfrak{c} \\
x(\mathfrak{a}\mathfrak{b}) &= (x\mathfrak{a})\mathfrak{b} \\
x(y\mathfrak{a}) &= (xy)\mathfrak{a} \\
(a)^n &= (a^n) \\
\mathfrak{a}^m\mathfrak{a}^n &= \mathfrak{a}^{m+n} \\
\mathfrak{a}^n\mathfrak{b}^n &= (\mathfrak{a}\mathfrak{b})^n
\end{aligned}$$

Proposition: Für jeden Ringhomomorphismus $\varphi\colon R \to S$ ist

$$\begin{aligned}
\operatorname{Kern}(\varphi) &:= \{a \in R \mid \varphi(a) = 0\} && \text{ein Ideal von } R, \text{ und} \\
\operatorname{Bild}(\varphi) &:= \{\varphi(a) \mid a \in R\} && \text{ein Unterring von } S.
\end{aligned}$$

Dabei ist $\operatorname{Kern}(\varphi) = (0)$ genau dann, wenn φ injektiv ist, und $\operatorname{Bild}(\varphi) = S$ genau dann, wenn φ surjektiv ist,

A.10 Faktorringe

Sei $\mathfrak{a}$ ein Ideal von R. Für jedes $x \in R$ heisst die Teilmenge

$$x + \mathfrak{a} \;:=\; \{x + a \mid a \in \mathfrak{a}\} \;\subset\; R$$

eine *Nebenklasse von* $\mathfrak{a}$. Betrachte die Menge aller Nebenklassen

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

Proposition: Je zwei Nebenklassen $x + \mathfrak{a}$ sind entweder gleich oder disjunkt, und die Vereinigung aller ist R. Genauer gilt für alle $x, x' \in R$:

$$x + \mathfrak{a} = x' + \mathfrak{a} \iff x \in x' + \mathfrak{a} \iff x' \in x + \mathfrak{a} \iff (x + \mathfrak{a}) \cap (x' + \mathfrak{a}) \neq \varnothing.$$

Proposition: Die Menge $R/\mathfrak{a}$ besitzt eine eindeutige Ringstruktur, so dass gilt:

(a) $\forall x, x' \in R : (x + \mathfrak{a}) + (x' + \mathfrak{a}) = (x + x') + \mathfrak{a}$.

(b) $\forall x, x' \in R : (x + \mathfrak{a}) \cdot (x' + \mathfrak{a}) = xx' + \mathfrak{a}$.

Für diese gilt weiter:

(c) Das Nullelement von $R/\mathfrak{a}$ ist $0 + \mathfrak{a} = \mathfrak{a}$.

(d) Das Einselement von $R/\mathfrak{a}$ ist $1 + \mathfrak{a}$.

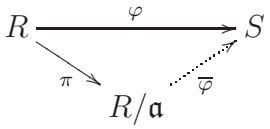
(e) $\pi\colon R \to R/\mathfrak{a}$, $x \mapsto x + \mathfrak{a}$ ist ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$.

Definition: Der Ring $R/\mathfrak{a}$ heisst der *Faktorring von R nach $\mathfrak{a}$*.

Beispiel: (a) Es ist $\mathfrak{a} = R$ genau dann, wenn $R/\mathfrak{a}$ der Nullring ist.

(b) Es ist $\mathfrak{a} = 0$ genau dann, wenn π ein Isomorphismus ist.

Proposition: *(Universelle Eigenschaft)* Für jeden Ring S und jeden Ringhomomorphismus $\varphi\colon R \to S$ mit $\mathfrak{a} \subset \operatorname{Kern}(\varphi)$ existiert genau ein Ringhomomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \to S$ mit $\overline{\varphi} \circ \pi = \varphi$, das heisst, so dass das folgende Diagramm kommutiert:



Proposition: *(Homomorphiesatz)* Jeder Ringhomomorphismus $\varphi\colon R \to S$ induziert einen Isomorphismus

$$R/\operatorname{Kern}(\varphi) \xrightarrow{\sim} \operatorname{Bild}(\varphi).$$

Beispiel: Es ist $\mathbb{R}[X]/(X^2 + 1) \xrightarrow{\sim} \mathbb{C}$.

A.11 Primideale

Definition: Ein *Primideal von* R ist ein echtes Ideal $\mathfrak{p} \subsetneqq R$ mit der Eigenschaft:

$$\forall x, y \in R\colon xy \in \mathfrak{p} \longrightarrow (x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}).$$

Proposition: Ein von Null verschiedenes Hauptideal (p) in einem Integritatsbereich ist ein Primideal genau dann, wenn das Erzeugende p ein Primelement ist.

Proposition: Ein Ideal $\mathfrak{p}$ von R ist ein Primideal genau dann, wenn der Faktorring $R/\mathfrak{p}$ ein Integritätsbereich ist.

Definition: Ein *maximales Ideal von* R ist ein echtes Ideal $\mathfrak{m} \subsetneqq R$, welches unter allen echten Idealen maximal ist, das heisst, so dass jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subset \mathfrak{a}$ entweder gleich $\mathfrak{m}$ oder gleich R ist.

Proposition: Ein Ideal $\mathfrak{m}$ von R ist maximal genau dann, wenn der Faktorring $R/\mathfrak{m}$ ein Körper ist.

Folge: Jedes maximale Ideal ist ein Primideal.

Beispiel: (a) Das Nullideal ist prim genau dann, wenn R ein Integritätsbereich ist.

(b) Das Nullideal ist maximal genau dann, wenn R ein Körper ist.

Satz: *(Krull)* Für jedes echte Ideal $\mathfrak{a} \subsetneqq R$ existiert ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subset \mathfrak{m}$.

Folge: Jeder nichttriviale Ring besitzt ein maximales Ideal.

Beispiel: Betrachte eine Menge X, einen Körper K, und einen Unterring R des Rings aller Funktionen $\mathrm{Abb}(X, K)$, welcher alle konstanten Funktionen $X \to K$ enthält. Für jedes $x \in X$ ist dann $\mathfrak{m}_x := \mathrm{Kern}(R \to K,\ f \mapsto f(x))$ ein maximales Ideal.

A.12 Moduln

Definition: Ein *Modul über R* oder kurz ein *R-Modul* ist ein Tupel $(M, +, \cdot, 0)$ bestehend aus einer Menge M mit zwei Abbildungen

$$\begin{aligned} + :&\quad M \times M \to M, \quad (m,n) \mapsto m+n \\ \cdot :&\quad R \times M \to M, \quad (x,m) \mapsto xm \end{aligned}$$

und einem ausgezeichneten Element $0 \in M$, so dass gilt:

(a) $(M, +, 0)$ ist eine abelsche Gruppe.
(b) $\forall x \in R\ \forall m, n \in M\colon\ x(m+n) = xm + xn$ (Linksdistributivität)
(c) $\forall x, y \in R\ \forall m \in M\colon\ (x+y)m = xm + ym$ (Rechtsdistributivität)
(d) $\forall x, y \in R\ \forall m \in M\colon\ x(ym) = (xy)m$ (Assoziativität)
(e) $\forall m \in M\colon\ 1 \cdot m = m$ (Einselement)

Beispiel: Ein Modul über einem Körper K ist also einfach ein K-Vektorraum.

Beispiel: Jede Menge mit einem Element besitzt eine eindeutige Struktur als R-Modul und heisst dann *Nullmodul*.

Beispiel: Mit den Operationen $+$ und $\cdot$ von R ist R selbst ein R-Modul.

Definition: Ein *Untermodul* eines R-Moduls M ist eine Teilmenge $N \subset M$ mit den Eigenschaften:

(a) $N \neq \varnothing$.
(b) $\forall n, n' \in N\colon\ n + n' \in N$.
(c) $\forall x \in R\ \forall n \in N\colon\ xn \in N$.

Proposition: Eine Teilmenge $N \subset M$ ist ein Untermodul genau dann, wenn sie zusammen mit den Restriktionen der Addition und der skalaren Multiplikation von M selbst einen R-Modul bildet.

Beispiel: Jeder R-Modul M hat die Untermoduln $\{0\}$ und M selbst.

Beispiel: Die Untermoduln von R als R-Modul sind genau die Ideale von R.

Proposition: Der Durchschnitt jeder nichtleeren Kollektion von Untermoduln von M ist ein Untermodul von M.

Proposition-Definition: Für jede Teilmenge S eines R-Moduls M existiert ein eindeutiger kleinster Untermodul $\langle S \rangle \subset M$, welcher S enthält. Dieser heisst das *Erzeugnis von S* oder *von S erzeugt*. Für endlich viele Elemente $m_1, \ldots, m_n \in M$ gilt

$$\langle \{m_1, \ldots, m_n\} \rangle \;=\; \big\{\, x_1 m_1 + \ldots + x_n m_n \;\big|\; \forall i\colon x_i \in R \,\big\}.$$

Ein von endlich vielen Elementen erzeugter Modul heisst *endlich erzeugt*.

Proposition-Definition: Die *Summe* von Untermoduln $M_1, \ldots, M_n$

$$M_1 + \ldots + M_n \;:=\; \left\{ m_1 + \ldots + m_n \;\middle|\; \forall i\colon m_i \in M_i \right\}$$

ist ein Untermodul. Ist die Abbildung

$$M_1 \times \ldots \times M_n \to M_1 + \ldots + M_n,\ (m_1, \ldots, m_n) \mapsto m_1 + \ldots + m_n$$

bijektiv, so heisst die Summe *direkt* oder eine *innere direkte Summe* und wird bezeichnet mit

$$M_1 \oplus \ldots \oplus M_n \;=\; \bigoplus_{i=1}^{n} M_i.$$

Proposition-Definition: Das kartesische Produkt von R-Moduln $M_1 \times \ldots \times M_n$ versehen mit komponentenweiser Addition und skalarer Multiplikation sowie dem Nullelement $(0, \ldots, 0)$ ist ein R-Modul. Er heisst das *(direkte) Produkt* oder, da endlich, die *äussere direkte Summe* von $M_1, \ldots, M_n$ und wird bezeichnet mit

$$M_1 \boxplus \ldots \boxplus M_n \;=\; \boxplus_{i=1}^{n} M_i.$$

Sind alle Faktoren gleich, so schreibt man auch $M^n := \boxplus_{i=1}^{n} M$.

Konvention: Oft werden innere und äussere direkte Summe mit demselben Symbol $\bigoplus$ bezeichnet. Welche dann jeweils gemeint ist, muss man aus dem Zusammenhang erschliessen.

Definition: Eine Abbildung zwischen zwei R-Moduln $\varphi\colon M \to N$ mit

(a) $\forall m, m' \in M : \varphi(m + m') = \varphi(m) + \varphi(m')$ und

(b) $\forall m \in M\ \forall x \in R : \varphi(xm) = x \cdot \varphi(m)$

heisst *R-linear* oder ein *(R-Modul)-Homomorphismus*. Die Menge aller Homomorphismen $M \to N$ wird bezeichnet mit $\mathrm{Hom}_R(M, N)$. Ein Homomorphismus $M \to M$ heisst ein *Endomorphismus von M*, und wir schreiben $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$.

Proposition: Für jeden Homomorphismus $\varphi\colon M \to N$ gilt:

(a) $\mathrm{Kern}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ ist ein Untermodul von M.

(b) $\mathrm{Bild}(\varphi)$ ist ein Untermodul von N.

(c) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 0$ ist.

(d) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = N$ ist.

Beispiel: Die *identische Abbildung* $\mathrm{id}_M\colon M \to M$, $m \mapsto m$ ist ein Homomorphismus.

Proposition: Die Komposition zweier Homomorphismen ist ein Homomorphismus.

Proposition: Schreibe die Elemente der R-Moduln R^n und R^m als Spaltenvektoren. Dann induziert jede Matrix $A \in \mathrm{Mat}_{m\times n}(R)$ einen Homomorphismus

$$L_A\colon\ R^n \to R^m,\ m \mapsto Am.$$

Umgekehrt ist jeder Homomorphismus $R^n \to R^m$ gleich L_A für ein eindeutiges A. Weiter gilt für je zwei komponierbare Matrizen $L_{AB} = L_A \circ L_B$.

Definition: Ein Homomorphismus $\varphi\colon M \to N$ mit einem beidseitigem Inversen $\varphi^{-1}\colon N \to M$ heisst ein *Isomorphismus*, und wir schreiben dann $\varphi\colon M \xrightarrow{\sim} N$. Existiert ein Isomorphismus $M \xrightarrow{\sim} N$, so heissen M und N *isomorph* und wir schreiben $M \cong N$.

Proposition: Ein Homomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

Proposition: Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von R-Moduln ist eine Äquivalenzrelation.

Definition: Jeder zu R^n isomorphe R-Modul heisst *frei vom Rang n*.

Beispiel: Für jedes Ideal $(0) \subsetneqq \mathfrak{a} \subsetneqq R$ ist der R-Modul $R/\mathfrak{a}$ nicht frei.

Definition: Ein Isomorphismus $M \xrightarrow{\sim} M$ heisst ein *Automorphismus von M*.

Proposition-Definition: Die Menge $\mathrm{Aut}_R(M)$ aller Automorphismen von M ist eine Gruppe bezüglich Komposition mit dem Einselement id_M, genannt die *Automorphismengruppe von M*.

Proposition: Für jede natürliche Zahl n haben wir einen Gruppen-Isomorphismus

$$\mathrm{GL}_n(R) \xrightarrow{\sim} \mathrm{Aut}_R(R^n),\ A \mapsto L_A.$$

Proposition-Definition: Sei N ein Untermodul von M. Für jedes $m \in M$ betrachte die *Nebenklasse*

$$m + N\ :=\ \{m + n \mid n \in N\}\ \subset\ M.$$

Für alle $m, m' \in M$ gilt

$$m+N = m'+N \iff m \in m'+N \iff m' \in m+N \iff (m+N)\cap(m'+N) \neq \varnothing.$$

Insbesondere ist M die disjunkte Vereinigung aller Nebenklassen von N. Die Menge aller Nebenklassen

$$M/N\ :=\ \{m + N \mid m \in M\}$$

besitzt eine eindeutige Struktur eines R-Moduls, so dass gilt:

(a) $\forall m, m' \in M : (m + N) + (m' + N) = (m + m') + N$.

(b) $\forall m \in M\ \forall x \in R : x \cdot (m + N) = xm + N$.

Für diese gilt weiter:

(c) Das Nullelement von M/N ist $0 + N = N$.

(d) Das additive Inverse jedes Elements $m + N$ ist $-(m + N) = (-m) + N$.

Definition: Der Modul M/N heisst der *Faktormodul von M nach N*.

Proposition: Die Abbildung $\pi\colon M \to M/N$, $m \mapsto m + N$ ist ein surjektiver Modulhomomorphismus mit Kern N.

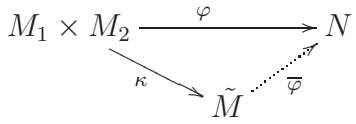
Homomorphiesatz: Jeder Homomorphismus $\varphi\colon M \to N$ induziert einen Isomorphismus

$$M/\operatorname{Kern}(\varphi) \xrightarrow{\sim} \operatorname{Bild}(\varphi),\ m + \operatorname{Kern}(\varphi) \mapsto \varphi(m).$$

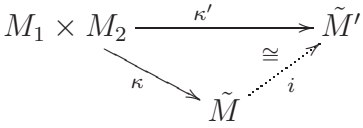
Das Tensorprodukt von R-Moduln wird genauso definiert und konstruiert wie das Tensorprodukt von Vektorräumen:

Definition: Ein *Tensorprodukt zweier R-Moduln M_1 und M_2* besteht aus einem R-Modul $\tilde{M}$ und einer R-bilinearen Abbildung $\kappa\colon M_1 \times M_2 \to \tilde{M}$ mit der *universellen Eigenschaft:*

Für jeden R-Modul N und jede R-bilineare Abbildung $\varphi\colon M_1 \times M_2 \to N$ existiert genau eine R-lineare Abbildung $\overline{\varphi}\colon \tilde{M} \to N$ mit $\overline{\varphi} \circ \kappa = \varphi$, das heisst, so dass das folgende Diagramm kommutiert:



Proposition: Ein Tensorprodukt ist eindeutig bis auf eindeutige Isomorphie, mit anderen Worten: Ist sowohl $(\tilde{M}, \kappa)$ wie $(\tilde{M}', \kappa')$ ein Tensorprodukt von M_1 und M_2, so existiert ein eindeutiger R-Modul-Isomorphismus $i\colon \tilde{M} \xrightarrow{\sim} \tilde{M}'$ mit $i \circ \kappa = \kappa'$, das heisst, so dass das folgende Diagramm kommutiert:



Satz: Ein Tensorprodukt existiert immer.

Konvention: Wir fixieren ein für alle Mal ein Tensorprodukt $(\tilde{M}, \kappa)$ und bezeichnen den Modul $\tilde{M}$ mit $M_1 \otimes_R M_2$ und die Abbildung κ mit

$$M_1 \times M_2 \to M_1 \otimes_R M_2,\ (m_1, m_2) \mapsto m_1 \otimes m_2.$$

Deren Rechenregeln sowie die Grundeigenschaften des Tensorprodukts entsprechen denen im Fall von Vektorräumen. Analog werden höhere Tensorpotenzen, symmetrische und alternierende Potenzen, sowie die Tensor-, symmetrische, bzw. äussere Algebra eines Moduls konstruiert.

Anhang B Teilbarkeit

In diesem Kapitel bezeichnet R einen Integritätsbereich.

B.1 Irreduzible und Primelemente

Definition: Betrachte Elemente $a, b \in R$.

(a) Gilt $\exists x \in R\colon ax = b$, so schreiben wir $a|b$ und sagen a *teilt* b, und nennen a einen *Teiler von* b, und b ein *Vielfaches von* a.

(b) Gilt $\exists x \in R^\times\colon ax = b$, so schreiben wir $a \sim b$ und nennen a und b *assoziiert*.

Proposition: Für alle $a, b, c, a', b', x_i, b_i \in R$ gilt:

(a) $1|a$ und $a|a$ und $a|0$.

(b) Aus $a|b$ und $b|c$ folgt $a|c$.

(c) Gilt $a|b_i$ für alle i, so auch $a \mid \sum_i x_i b_i$.

(d) Es ist $a \sim b$ genau dann, wenn $a|b$ und $b|a$.

(e) $\sim$ ist eine Äquivalenzrelation.

(f) Gilt $a \sim a'$ und $b \sim b'$, so ist $a|b$ genau dann, wenn $a'|b'$.

(g) Gilt $a|b$ und $b \in R^\times$, so ist auch $a \in R^\times$.

Definition: Ein Element $p \in R$ mit $p \neq 0$ und $p \notin R^\times$ heisst

(a) *irreduzibel* oder *unzerlegbar*, wenn gilt

$$\forall a, b \in R\colon\ p = ab \longrightarrow (a \in R^\times \text{ oder } b \in R^\times).$$

(b) *prim* oder ein *Primelement*, wenn gilt

$$\forall a, b \in R\colon\ p|ab \longrightarrow (p|a \text{ oder } p|b).$$

Proposition: Gilt $p \sim p'$, so ist p *irreduzibel* bzw. *prim* genau dann, wenn p' es ist.

Proposition: Jedes Primelement ist irreduzibel.

Bemerkung: Eine *Primzahl* ist nach Definition eine natürliche Zahl $\geqslant 2$, welche ausser der 1 und sich selbst keine natürlichen Zahlen als Teiler hat. Nach obiger Definition bedeutet dies irreduzibel und positiv. In dem Ring $\mathbb{Z}$ ist irreduzibel aber äquivalent zu prim, und es hat sich herausgestellt, dass die Eigenschaft „prim“ die bessere Verallgemeinerung darstellt.

Beispiel: Im Ring $\mathbb{Z}$ ist 2 ein Primelement. In $\mathbb{Z}[i]$ gilt dagegen $2 = (1+i)(1-i)$ mit Nichteinheiten $1 \pm i$, also ist 2 nicht irreduzibel in $\mathbb{Z}[i]$. In $\mathbb{Z}[i\sqrt{5}]$ ist 2 zwar irreduzibel, aber nicht prim, denn es ist $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ und $2 \nmid 1 \pm i\sqrt{5}$.

B.2 Faktorielle Ringe

Definition: Ein Integritätsbereich, in dem jedes von 0 verschiedene Element ein Produkt von Einheiten und/oder Primelementen ist, heisst *faktoriell*.

Beispiel: Der Ring $\mathbb{Z}$ ist faktoriell.

Beispiel: Jeder Körper ist ein faktorieller Ring. (Er hat zwar keine Primelemente, aber auch nichts zu faktorisieren.)

Sei nun R beliebig faktoriell. Dann hat jedes Element von $R \smallsetminus \{0\}$ die Form

$$a \;=\; u \cdot p_1 \cdots p_m$$

für eine Einheit $u \in R^\times$, eine Zahl $m \geqslant 0$, und Primelemente $p_1, \ldots, p_m$.

Satz: Diese *Primfaktorzerlegung* ist eindeutig bis auf Umordnung und Assoziiertheit, das heisst: Für jede weitere Zerlegung mit $v \in R^\times$ und Primelementen $q_1, \ldots, q_n$

$$a \;=\; v \cdot q_1 \cdots q_n$$

gilt $m = n$ und es existiert eine Permutation $\sigma \in S_m$ mit $\forall i\colon p_i \sim q_{\sigma i}$.

Bemerkung: Wegen der eindeutigen Primfaktorzerlegung nennt man einen faktoriellen Ring auch einen *ZPE-Ring* für *„Zerlegung in Primfaktoren Eindeutig“*.

Proposition: In jedem faktoriellen Ring ist irreduzibel äquivalent zu prim.

Proposition: Sei $\{p_i \mid i \in I\}$ ein Repräsentantensystem der Primelemente unter Assoziiertheit.

(a) Jedes Element von $R \smallsetminus \{0\}$ kann man auf eindeutige Weise schreiben in der Form

$$a \;=\; u \cdot \prod_{i \in I}{}' p_i^{\mu_i}$$

für eine Einheit $u \in R^\times$ und Exponenten $\mu_i \in \mathbb{Z}^{\geqslant 0}$, fast alle gleich 0.

(b) Für $a = u \cdot \prod'_{i\in I} p_i^{\mu_i}$ und $b = v \cdot \prod'_{i\in I} p_i^{\nu_i}$ mit $u, v \in R^\times$ gilt $a|b$ genau dann, wenn für alle i gilt $\mu_i \leqslant \nu_i$.

(c) Jedes Element von $\mathrm{Quot}(R) \smallsetminus \{0\}$ kann man auf eindeutige Weise schreiben in der Form

$$a \;=\; u \cdot \prod_{i \in I}{}' p_i^{\mu_i}$$

für eine Einheit $u \in R^\times$ und Exponenten $\mu_i \in \mathbb{Z}$, fast alle gleich 0.

B.3 Grösster gemeinsamer Teiler

Sei R faktoriell.

Proposition-Definition: Betrachte Elemente $a_1, \ldots, a_n \in R$.

(a) Ein Element $b \in R$ mit $\forall i\colon b|a_i$ heisst ein *gemeinsamer Teiler von* $a_1, \ldots, a_n$.

(b) Es existiert ein gemeinsamer Teiler b von $a_1, \ldots, a_n$, so dass für jeden gemeinsamen Teiler b' von $a_1, \ldots, a_n$ gilt $b'|b$.

(c) Dieser *grösste gemeinsame Teiler von* $a_1, \ldots, a_n$ ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jeden solchen mit $\mathrm{ggT}(a_1, \ldots, a_n)$.

Da der ggT nur eindeutig bis auf Assoziiertheit ist, sollte man ihn immer nur auf Assoziiertheit testen und nicht auf Gleichheit.

Proposition: Für alle $a_1, \ldots, a_n, x_1, \ldots, x_n \in R$ gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) \;\sim\; \mathrm{ggT}(a_1, \ldots, a_n, \textstyle\sum_{i=1}^n x_i a_i).$$

Definition: Elemente $a_1, \ldots, a_n \in R$ mit

(a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$ heissen *teilerfremd*.

(b) $\mathrm{ggT}(a_i, a_j) \sim 1$ für alle $i \neq j$ heissen *paarweise teilerfremd*.

Proposition-Definition: Betrachte Elemente $a_1, \ldots, a_n \in R$.

(a) Ein Element $b \in R$ mit $\forall i\colon a_i|b$ heisst *gemeinsames Vielfaches von* $a_1, \ldots, a_n$.

(b) Es existiert ein gemeinsames Vielfaches b von $a_1, \ldots, a_n$, so dass für jedes gemeinsame Vielfache b' von $a_1, \ldots, a_n$ gilt $b|b'$.

(c) Dieses *kleinste gemeinsame Vielfache von* $a_1, \ldots, a_n$ ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jedes solche mit $\mathrm{kgV}(a_1, \ldots, a_n)$.

Proposition: Für alle $a, a_1, \ldots, a_n \in R$ gilt

$$\begin{aligned} \mathrm{ggT}(aa_1, \ldots, aa_n) &\;\sim\; a \cdot \mathrm{ggT}(a_1, \ldots, a_n), \\ \mathrm{kgV}(aa_1, \ldots, aa_n) &\;\sim\; a \cdot \mathrm{kgV}(a_1, \ldots, a_n). \end{aligned}$$

Proposition: Für alle $a_1, a_2 \in R$ gilt

$$\mathrm{ggT}(a_1, a_2) \cdot \mathrm{kgV}(a_1, a_2) \;\sim\; a_1 \cdot a_2.$$

B.4 Hauptidealringe

Definition: Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heisst ein *Hauptidealring*.

Satz: Sei R ein Hauptidealring.

(a) Jede aufsteigende Folge von Idealen $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots$ wird stationär, das heisst, es existiert $n \geqslant 0$ mit $\mathfrak{a}_n = \mathfrak{a}_m$ für alle $m \geqslant n$. (Ein Ring mit dieser Eigenschaft heisst *noethersch*.)

(b) Für jedes $a \in R \smallsetminus (\{0\} \cup R^\times)$ existiert ein Primelement $p \in R$ mit $p|a$.

(c) R ist faktoriell.

Proposition: Ist R ein Hauptidealring, so gilt für alle $a_1, \ldots, a_n \in R$

$$\big(\mathrm{ggT}(a_1, \ldots, a_n)\big) \;=\; (a_1, \ldots, a_n).$$

Insbesondere existieren $x_1, \ldots, x_n \in R$ mit

$$\mathrm{ggT}(a_1, \ldots, a_n) \;=\; x_1 a_1 + \ldots + x_n a_n.$$

Bemerkung: Nicht jeder faktorielle Ring ist ein Hauptidealring. Zum Beispiel ist für jeden Körper K der Ring $K[X,Y]$ faktoriell, aber sein Ideal (X,Y) ist kein Hauptideal. In diesem Fall ist $\mathrm{ggT}(X,Y) \sim 1$, aber $(X,Y) \neq (1)$. Der ggT lässt sich hier nicht als Linearkombination von X und Y darstellen.

Beispiel: Für jeden Körper K ist $K[[X]]$ ein Hauptidealring. Genauer sind seine Ideale das Nullideal (0) sowie die Ideale (X^n) für alle $n \geqslant 0$.

Satz: *(Chinesischer Restsatz)* Seien $a_1, \ldots, a_n$ paarweise teilerfremde Elemente eines Hauptidealrings R. Dann ist die folgende Abbildung ein Ring-Isomorphismus:

$$\begin{array}{ccc} R/(a_1 \cdots a_n) & \longrightarrow & R/(a_1) \times \ldots \times R/(a_n), \\ x + (a_1 \cdots a_n) & \mapsto & \big(x + (a_1), \ldots, x + (a_n)\big). \end{array}$$

Der älteste bekannte Beleg dieses Satzes ist eine mathematische Veröffentlichung in China im 5. Jahrhundert unserer Zeitrechnung. Gemäss einer Legende benutzte ein chinesischer General den Satz für $R = \mathbb{Z}$, um seine Soldaten zu zählen. Er liess sie in Reihen von $a_1 := 19$ aufstellen und erhielt den Rest 1, in Reihen von $a_2 := 17$ mit dem Rest 14, sowie in Reihen von $a_3 := 12$ mit dem Rest 1. Da er auch die ungefähre Grössenordnung wusste, konnte er die Gesamtzahl bestimmen, nämlich 3193 gegenüber $19 \cdot 17 \cdot 12 = 3876$.

Computeralgebrasysteme benutzen den chinesischen Restsatz, um eine Rechnung mit grossen Zahlen in $\mathbb{Z}$ durch mehrere voneinander unabhängige Rechnungen in endlichen Körpern $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ zu ersetzen. Je nach Situation kann das den Rechenaufwand deutlich verringern; ausserdem eignet sich die Methode gut für parallele Programmierung.

B.5 Euklidische Ringe

Definition: Ein *euklidischer Ring* ist ein Integritätsbereich R zusammen mit einer Abbildung $\delta\colon R \smallsetminus \{0\} \to \mathbb{Z}^{\geqslant 0}$, so dass gilt

$$\forall a \in R\ \forall b \in R \smallsetminus \{0\}\colon\ \exists q, r \in R\colon\ a = bq + r \text{ und } (r = 0 \text{ oder } \delta(r) < \delta(b)).$$

Dieser Prozess heisst *Division mit Rest*, nämlich *Division von a durch b mit Quotient q und Rest r*. Die Funktion δ misst die Grösse oder Komplexität eines Elements.

Satz: Jeder euklidische Ring ist ein Hauptidealring.

Beispiel: Der Ring $\mathbb{Z}$ ist euklidisch mit der Funktion $\delta(a) := |a|$.

(a) Seine Ideale sind genau die Ideale $(n) = n\mathbb{Z}$ für alle $n \geqslant 0$.

(b) Die maximalen Ideale von $\mathbb{Z}$ sind die (p) für alle Primzahlen p, mit dem zugehörigen Restklassenkörper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(c) Das einzige weitere Primideal von $\mathbb{Z}$ ist das Nullideal (0).

(d) Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ besteht aus den Restklassen $a + n\mathbb{Z}$ für alle zu n teilerfremden Zahlen a.

Beispiel: Für jeden Körper K ist $K[X]$ euklidisch mit der Funktion $\delta(f) := \deg(f)$.

Beispiel: Für eine natürliche Zahl $d \geqslant 1$ ist der Ring $\mathbb{Z}[i\sqrt{d}]$ euklidisch, bzw. ein Hauptidealring, bzw. faktoriell genau dann, wenn $d \leqslant 2$ ist. Die Funktion $\delta(a + i\sqrt{d} \cdot b)$ $:= a^2 + db^2$ erfüllt dann die gewünschte Bedingung.

Vorsicht: Nicht jeder Hauptidealring lässt sich zu einem euklidischen Ring machen. Zum Beispiel ist $\mathbb{Z}\big[\frac{1}{2} \cdot (1 + i\sqrt{163})\big]$ ein Hauptidealring, aber nicht euklidisch.

Euklidischer Algorithmus: Sei (R, δ) euklidisch und betrachte Elemente $a_1, a_2 \in R$, nicht beide gleich Null. Wir setzen diese fort zu einer Folge $a_1, \ldots, a_n$ wie folgt. Ist das letzte konstruierte Element a_n gleich Null, so halte an. Andernfalls benutze Division mit Rest und schreibe $a_{n-1} = a_n q_n + a_{n+1}$ mit $a_{n+1} = 0$ oder $\delta(a_{n+1}) < \delta(a_n)$.

Proposition: Dieser Algorithmus endet nach endlich vielen Schritten, und für das letzte von Null verschiedene Element a_{m-1} gilt

$$a_{m-1} \ \sim\ \mathrm{ggT}(a_1, a_2).$$

Bemerkung: Der euklidische Algorithmus produziert zusätzlich Elemente $u_n, v_n \in R$ mit $a_n = u_n a_1 + v_n a_2$ für alle $n \geqslant 1$, nämlich durch $(u_1, v_1) := (1, 0)$ und $(u_2, v_2) := (0, 1)$ und $(u_{n+1}, v_{n+1}) := (u_{n-1} - u_n q_n, v_{n-1} - v_n q_n)$ für alle $n \geqslant 2$. Für das letzte von Null verschiedene Element a_{m-1} liefert dies eine Linearkombination

$$\mathrm{ggT}(a_1, a_2) \ \sim\ a_{m-1} \ =\ u_{m-1} a_1 + v_{m-1} a_2.$$

Beispiel: In $\mathbb{Z}$ ist $\mathrm{ggT}(2015, 1959) \sim 1 = 35 \cdot 2015 - 36 \cdot 1959$.

B.6 Polynomringe

Proposition: Für jeden Integritätsbereich R gilt $R[X]^\times = R^\times$.

Sei nun R ein faktorieller Ring mit Quotientenkörper K. Für zwei Elemente $a, b \in K^\times$ schreiben wir $a \sim b$ genau dann, wenn $\frac{b}{a} \in R^\times$ ist. Für Elemente von $R \smallsetminus \{0\}$ stimmt dies mit der Definition aus §B.1 überein.

Definition: (a) Der *Inhalt* eines Polynoms $f(X) = \sum_{i=0}^n a_i X^i \in R[X] \smallsetminus \{0\}$ ist

$$I(f) \;:=\; \mathrm{ggT}(a_0, \ldots, a_n) \;\in\; R \smallsetminus \{0\}.$$

(b) Ein Polynom $f \in R[X] \smallsetminus \{0\}$ mit $I(f) \sim 1$ heisst *primitiv*.

Lemma: Für alle $f \in R[X] \smallsetminus \{0\}$ und $a \in R \smallsetminus \{0\}$ gilt:

(a) $\frac{f}{I(f)}$ ist ein primitives Element von $R[X] \smallsetminus \{0\}$.

(b) $I(af) \sim a \cdot I(f)$.

Lemma: Der Inhalt setzt sich fort zu einer Abbildung $K[X] \smallsetminus \{0\} \to K^\times$, $f \mapsto I(f)$ mit denselben Eigenschaften für alle $f \in K[X] \smallsetminus \{0\}$ und $a \in K^\times$.

Gauss-Lemma: Für alle $f, g \in K[X] \smallsetminus \{0\}$ gilt $I(fg) \sim I(f) \cdot I(g)$.

Satz: (a) Die Primelemente von $R[X]$ sind genau die Primelemente von R sowie die primitiven Polynome in $R[X] \smallsetminus \{0\}$, die in $K[X]$ prim sind.

(b) Der Ring $R[X]$ ist faktoriell.

Folge: Ein primitives Polynom in $R[X]$ ist irreduzibel in $R[X]$ genau dann, wenn es irreduzibel in $K[X]$ ist.

Folge: Für jedes normierte Polynom in $R[X]$ liegt jede Nullstelle in K schon in R.

Satz: Für jeden faktoriellen Ring R und jedes $n \geqslant 0$ ist $R[X_1, \ldots, X_n]$ faktoriell. Insbesondere ist für jeden Körper K der Ring $K[X_1, \ldots, X_n]$ faktoriell.

Beispiel: Für jeden Körper K ist $X^3 - Y^5$ irreduzibel in $K[X, Y]$.

B.7 Irreduzibilitätskriterien

Betrachte einen faktoriellen Ring R und ein Primelement p. Der Reduktionshomomorphismus $R \twoheadrightarrow R/(p)$, $a \mapsto \overline{a} := a + (p)$ induziert einen Homomorphismus

$$R[X] \twoheadrightarrow (R/(p))[X],\ f = \sum{}' a_i X^i \mapsto \overline{f} := \sum{}' \overline{a_i} X^i.$$

Insbesondere gilt für alle $f, g \in R[X]$ die Gleichung $\overline{(fg)} = \overline{f} \cdot \overline{g}$.

Proposition: Jedes primitive Element $f \in R[X] \smallsetminus \{0\}$ mit $\deg(f) = \deg(\overline{f})$ und $\overline{f}$ irreduzibel ist selbst irreduzibel.

Beispiel: Das Polynom $X^5 + 2X^2 + 1 \in \mathbb{Z}[X]$ ist irreduzibel. (Benutze $p = 3$.)

Beispiel: Das Polynom $X^4 + 3X^3 - X^2 + 1 \in \mathbb{Z}[X]$ ist irreduzibel. (Benutze $p = 5$. Aliter: Untersuche die Reduktionen bei $p = 2$ und $p = 3$ und vergleiche Grade.)

Satz: *(Eisenstein-Kriterium)* Sei $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv mit $n \geqslant 1$ und $p \nmid a_n$ und $\forall i < n\colon p | a_i$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.

Beispiel: Das Polynom $X^n - 2 \in \mathbb{Z}[X]$ ist irreduzibel.

Proposition: Für jede Primzahl p ist das *p-te Kreisteilungspolynom*

$$\Phi_p(X) \ := \ 1 + X + ... + X^{p-1} \ = \ \frac{X^p - 1}{X - 1}$$

in $\mathbb{Z}[X]$ irreduzibel.

Beispiel: Für jedes $n \geqslant 1$ ist das Polynom $X^n + Y^n + Z^n \in \mathbb{C}[X, Y, Z]$ irreduzibel.

Satz: *(Kronecker)* Es existiert ein Algorithmus, der jedes Polynom in beliebig vielen Variablen über $\mathbb{Z}$ oder $\mathbb{Q}$ in irreduzible Faktoren zerlegt.

B.8 Elementarteilersatz

Satz: Sei A eine $m \times n$-Matrix über einem Hauptidealring R. Dann existieren Matrizen $U \in \mathrm{GL}_m(R)$ und $V \in \mathrm{GL}_n(R)$ sowie eine Zahl $0 \leqslant k \leqslant \min\{m,n\}$ und Elemente $e_1, \dots, e_k \in R \smallsetminus \{0\}$ mit $e_1 | e_2 | \dots | e_k$, so dass gilt

$$UAV = \left(\begin{array}{ccc|c} e_1 & & & \\ & \ddots & & \\ & & e_k & \\ \hline & & & \end{array}\right),$$

wobei alle nicht gezeigten Matrixkoeffizienten gleich 0 sind.

Zusatz: (a) Die Zahl k ist der Rang von A als Matrix über dem Körper $\mathrm{Quot}(R)$.

(b) Für jedes $1 \leqslant \ell \leqslant k$ ist $e_1 \cdots e_\ell$ der grösste gemeinsame Teiler aller $\ell \times \ell$-Unterdeterminanten von A.

(c) Insbesondere sind sowohl k, als auch $e_1, \dots, e_k$ bis auf Assoziiertheit, durch A eindeutig bestimmt.

Definition: Die Elemente $e_1, \dots, e_k$ heissen die *Elementarteiler* von A.

Folge: Für alle $n \geqslant 1$ und alle $a_1, \dots, a_n$ in einem Hauptidealring R sind äquivalent:

(a) $\mathrm{ggT}(a_1, \dots, a_n) \sim 1$.

(b) Es existiert eine Matrix in $\mathrm{GL}_n(R)$ mit erster Spalte $(a_1, \dots, a_n)^T$.

Beispiel: Sei p ein Primelement eines Hauptidealrings R und seien $i, j \in \mathbb{Z}^{\geqslant 0}$ und $a \in R$. Ist $a \neq 0$, so sei k der grösste Exponent mit $p^k | a$. Dann sind die Elementarteiler der Matrix $\begin{pmatrix} p^i & a \\ 0 & p^j \end{pmatrix}$ gleich $(e_1, e_2) = \begin{cases} (p^i, p^j) & \text{falls } i \leqslant j \text{ und } p^i | a, \\ (p^j, p^i) & \text{falls } j \leqslant i \text{ und } p^j | a, \\ (p^k, p^{i+j-k}) & \text{falls } p^i \nmid a \text{ und } p^j \nmid a. \end{cases}$

B.9 Moduln über Hauptidealringen

Sei R ein Hauptidealring.

Proposition: Jeder Untermodul von R^n ist von n Elementen erzeugt.

Satz: Für jeden endlich erzeugten R-Modul M existieren Zahlen $r, k \geqslant 0$ und Elemente $e_1, \ldots, e_k \in R \smallsetminus (\{0\} \cup R^\times)$ mit $e_1 | e_2 | \ldots | e_k$, so dass gilt

$$M \;\cong\; R^r \boxplus \coprod_{i=1}^{k} R/(e_i).$$

Definition: Elemente $m_1, \ldots, m_\ell$ von M heissen *linear unabhängig*, wenn für alle $a_1, \ldots, a_\ell \in R$ gilt $a_1 m_1 + \ldots + a_\ell m_\ell = 0 \Rightarrow a_1 = \ldots = a_\ell = 0$.

Zusatz: (a) Die Zahl r ist die maximale Anzahl linear unabhängiger Elemente von M. Insbesondere ist sie eindeutig bestimmt. Sie heisst der *„freie Rang" von M*.

(b) Die Zahl $r + k$ ist die minimale Anzahl von Erzeugenden von M. Insbesondere ist k eindeutig bestimmt.

(c) Die Elemente $e_1, \ldots, e_k$ sind bis auf Assoziiertheit durch M eindeutig bestimmt. Sie heissen die *Elementarteiler von M*.

Satz: Für jeden endlich erzeugten R-Modul M existieren Zahlen $r, \ell \geqslant 0$ und Primelemente $p_i \in R$ und Exponenten $\nu_i \geqslant 1$, so dass gilt

$$M \;\cong\; R^r \boxplus \coprod_{i=1}^{\ell} R/(p_i^{\nu_i}).$$

Zusatz: Für jedes Primelement $p \in R$ und jedes $\nu \geqslant 0$ gilt

$$\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) \;=\; r + \big|\{1 \leqslant i \leqslant \ell \mid p_i \sim p \wedge \nu_i > \nu\}\big|.$$

Insbesondere sind die Zahlen r und ℓ, sowie die Paare (p_i, ν_i) bis auf Vertauschung und Assoziiertheit der p_i, durch M eindeutig bestimmt.

Beispiel: Es gibt genau zwei Isomorphieklassen von endlichen $\mathbb{Z}$-Moduln der Kardinalität $28 = 2^2 \cdot 7$, nämlich die von

$$\begin{aligned} \mathbb{Z}/28\mathbb{Z} &\;\cong\; \mathbb{Z}/7\mathbb{Z} \boxplus \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \boxplus \mathbb{Z}/14\mathbb{Z} &\;\cong\; \mathbb{Z}/7\mathbb{Z} \boxplus \mathbb{Z}/2\mathbb{Z} \boxplus \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

B.10 Jordansche Normalform

Konstruktion: Sei K ein Körper. Jeder K-Vektorraum V mit einem Endomorphismus $\varphi \in \mathrm{End}_K(V)$ wird durch

$$K[X] \times V \to V,\ \big(\textstyle\sum' a_i X^i, v\big) \mapsto \sum' a_i \varphi^i(v)$$

zu einem $K[X]$-Modul. Umgekehrt können wir jeden $K[X]$-Modul als einen K-Vektorraum mit dem zusätzlichen Endomorphismus $m \mapsto Xm$ ansehen. Die Theorie der $K[X]$-Moduln ist deshalb äquivalent zu der Theorie der Paare (V, φ).

Proposition: Sei $M \cong K[X]/(f)$ für ein normiertes Polynom $f \in K[X]$. Dann ist $\dim_K(M) = \deg(f)$, und der obige Endomorphismus $\varphi \in \mathrm{End}_K(M)$ hat das charakteristische Polynom f und das Minimalpolynom f.

Satz: Für jeden $K[X]$-Modul V mit $\dim_K(V) < \infty$ existieren $k \geqslant 0$ und normierte irreduzible Polynome $p_i \in K[X]$ sowie Exponenten $\nu_i \geqslant 1$, so dass gilt

$$V \ \cong\ \coprod_{i=1}^{k} K[X]/(p_i^{\nu_i}).$$

Dabei sind k, und die Paare (p_i, ν_i) bis auf Vertauschung, eindeutig bestimmt.

Zusatz: Für $\varphi \in \mathrm{End}_K(V)$ wie oben gilt:

(a) Das charakteristische Polynom von φ ist gleich $p_1^{\nu_1} \cdots p_k^{\nu_k}$.

(b) Das Minimalpolynom von φ ist gleich $\mathrm{kgV}(p_1^{\nu_1}, \ldots, p_k^{\nu_k})$.

(c) Der Hauptraum von φ zum normierten irreduziblen Polynom p entspricht den Summanden in der obigen Zerlegung mit $p_i = p$.

(d) Jordansche Normalform.

Satz: Sei φ ein Endomorphismus eines endlich-dimensionalen Vektorraums V über einem algebraisch abgeschlossenen Körper K.

(a) Es existieren ein diagonalisierbarer Endomorphismus φ_s und ein nilpotenter Endomorphismus φ_n mit $\varphi_s\varphi_n = \varphi_n\varphi_s$ und $\varphi_s + \varphi_n = \varphi$.

(b) Diese sind durch φ eindeutig bestimmt.

(c) Beide können durch Polynome in φ mit Koeffizienten in K ausgedrückt werden.

Definition: Die Zerlegung $\varphi = \varphi_s + \varphi_n$ heisst die *Jordan-Chevalley-Zerlegung von* φ. Die Endomorphismen φ_s und φ_n heissen der *halbeinfache*, beziehungsweise *nilpotente Anteil* von φ.

Variante: Für jede quadratische Matrix A über einem algebraisch abgeschlossenen Körper K existieren eine diagonalisierbare Matrix A_s und eine nilpotente Matrix A_n über K mit $A_sA_n = A_nA_s$ und $A_s + A_n = A$. Diese sind durch A eindeutig bestimmt.

Literature

These are some Commutative Algebra text books, which can be recommended as accompanying literature. None of these books does however match the content of the lecture.

Primary reference:

1. *Introduction to Commutative Algebra* by M. F. Atiyah and I. G. Macdonald (Addison-Wesley Publ., 1969)

Secundary reference:

2. *Algebraic Geometry and Commutative Algebra* by S. Bosch (Springer 2013)

Tertiary references:

3. *Commutative algebra. With a view towards algebraic geometry* by D. Eisenbud (GTM 150, Springer Verlag, 1995)
4. *Commutative ring theory* by H. Matsumura (Cambridge University Press 1989)
5. *Commutative Algebra* by N. Bourbaki (Hermann, Masson, Springer)