Commutative Algebra

Prof. Richard Pink

Summary
Fall Semester 2016
ETH Zürich

Preliminary Version

7. Oktober 2016

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) $\bigcap_{i \in I} V(S_i) = V\big(\bigcup_{i \in I}(S_i)\big)$ 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) $X \subset V(S) \Longleftrightarrow S \subset I(X)$

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

(b′) $I(X \cup X') = I(X) \cap I(X')$

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

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

(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

$$\begin{tikzcd}
\mathcal{P}(R) \arrow[ddrr, "V"] & & \mathcal{P}(K^n) \arrow[ddll, "I"'] \\
\cup & & \cup \\
\{I(X) \mid X \subset K^n\} \arrow[rr, shift left] & & \{V(S) \mid S \subset R\} \arrow[ll, shift left, "bij."] \\
\| & & \| \\
\{\text{radical ideals of } R\} & & \{\text{Zariski closed subsets of } K^n\}
\end{tikzcd}$$

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 $\mathfrak{a} = \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$. 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

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

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

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

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

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 $D_g := (\operatorname{Spec} R) \smallsetminus V((g)) = \{\mathfrak{p} \in \operatorname{Spec} R \mid g \notin \mathfrak{p}\}$.

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 elephant

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

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

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

(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 with $S \subset (S^{-1}R)^\times$.

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:

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & R' \\ & S^{-1}R \arrow[ur, dotted, "\tilde\varphi"'] & \end{tikzcd}$$

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

$$\begin{array}{rcl} \{\mathfrak{p} \in \mathrm{Spec}\, R \mid \mathfrak{p} \cap S = \varnothing\} & \longleftrightarrow & \mathrm{Spec}\, S^{-1}R \\ \mathfrak{p} & \longmapsto & \iota_*\mathfrak{p} \\ \iota^*\mathfrak{q} & \longleftarrow\!\shortmid & \mathfrak{q} \end{array}$$

(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:

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

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

Special Case: For any integral domain R and any multiplicative subset $S \subset R \setminus \{0\}$, 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 $g \in K[X] \setminus \{0\}$, 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 $R \setminus \mathfrak{m}$ 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 $R \setminus \mathfrak{p}$ is multiplicative.

(b) The ring $R_\mathfrak{p} := (R \setminus \mathfrak{p})^{-1}R$ 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

5 Modules

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

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

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

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

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

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

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

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

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 $\varphi\colon R \stackrel{\sim}{\to} S$. Existiert ein Isomorphismus $R \stackrel{\sim}{\to} S$, 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 $R \stackrel{\sim}{\to} R$ 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

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

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

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

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

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

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:

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & S & \ni & x_\nu \\
& R[\underline{X}] \arrow[ur, dotted, "\varphi_{\underline{x}}"'] & \ni & X_\nu \arrow[ur, mapsto] &
\end{tikzcd}$$

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

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

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) $I_m A = A I_n = A$.

(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 $x \in R \setminus \{0\}$ mit

$$\exists y \in R \setminus \{0\}\colon\ xy = 0.$$

Definition: Ein Ring mit $1 \neq 0$ und ohne Nullteiler 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:

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & K \\ & \mathrm{Quot}(R) \arrow[ur, dotted, "\tilde\varphi"'] & \end{tikzcd}$$

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:

$$\sum_{\nu \in N} \mathfrak{a}_\nu := \left\{ \sum_{\nu \in N}{}' a_\nu \;\middle|\; \begin{array}{l} \text{alle } a_\nu \in \mathfrak{a}_\nu, \\ \text{fast alle } a_\nu = 0 \end{array} \right\}.$$

Proposition-Definition: Für jede Teilmenge $A \subset R$ ist die folgende Menge ein Ideal:

$$(A) \ := \ \left\{ \sum_{a \in A}{}' x_a a \;\middle|\; \begin{array}{l} \text{alle } x_a \in R, \\ \text{fast alle } x_a = 0 \end{array} \right\} \ = \ \sum_{a \in A} (a),$$

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 $a_1, \ldots, a_n$ ist ein gemeinsamer Teiler aller Elemente des Ideals $(a_1, \ldots, a_n)$. 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

$$\mathfrak{a}\mathfrak{b} \;:=\; \mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; \text{alle } n \geqslant 0,\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}.$$

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

$$\begin{aligned}
\mathrm{Kern}(\varphi) &:= \{a \in R \mid \varphi(a) = 0\} && \text{ein Ideal von } R\text{, und} \\
\mathrm{Bild}(\varphi) &:= \{\varphi(a) \mid a \in R\} && \text{ein Unterring von } S.
\end{aligned}$$

Dabei ist $\mathrm{Kern}(\varphi) = (0)$ genau dann, wenn φ injektiv ist, und $\mathrm{Bild}(\varphi) = S$ 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 $\mathfrak{a} \subset \mathrm{Kern}(\varphi)$ 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:

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\ & R/\mathfrak{a} \arrow[ur, dotted, "\overline{\varphi}"'] & \end{tikzcd}$$

Proposition: *(Homomorphiesatz)* Jeder Ringhomomorphismus $\varphi\colon R \to S$ induziert einen Isomorphismus

$$R/\mathrm{Kern}(\varphi) \xrightarrow{\sim} \mathrm{Bild}(\varphi).$$

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 $M_1, \ldots, M_n$

$$M_1 + \ldots + M_n \ := \ \big\{\, m_1 + \ldots + m_n \ \big|\ \forall i\colon m_i \in M_i \,\big\}$$

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

$$M_1 \boxplus \ldots \boxplus M_n \ = \ \mathop{\boxplus}_{i=1}^n M_i.$$

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:

$$\begin{tikzcd} M_1 \times M_2 \arrow[rr, "\varphi"] \arrow[dr, "\kappa"'] & & N \\ & \tilde{M} \arrow[ur, dotted, "\overline{\varphi}"'] & \end{tikzcd}$$

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:

$$\begin{tikzcd} M_1 \times M_2 \arrow[rr, "\kappa'"] \arrow[dr, "\kappa"'] & & \tilde{M}' \\ & \tilde{M} \arrow[ur, dotted, "\cong", "i"'] & \end{tikzcd}$$

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 $a \bigm| \sum_i x_i b_i$.

(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 *„<u>Z</u>erlegung in <u>P</u>rimfaktoren <u>E</u>indeutig“*.

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:

$$\begin{array}{rcl} R/(a_1 \cdots a_n) & \longrightarrow & R/(a_1) \times \ldots \times R/(a_n), \\ x + (a_1 \cdots a_n) & \mapsto & \big(x + (a_1), \ldots, x + (a_n)\big). \end{array}$$

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 $R \setminus \{0\}$ stimmt dies mit der Definition aus §B.1 überein.

Definition: (a) Der *Inhalt* eines Polynoms $f(X) = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$ ist

$$I(f) \;:=\; \mathrm{ggT}(a_0, \ldots, a_n) \;\in\; R \setminus \{0\}.$$

(b) Ein Polynom $f \in R[X] \setminus \{0\}$ mit $I(f) \sim 1$ heisst *primitiv.*

Lemma: Für alle $f \in R[X] \setminus \{0\}$ und $a \in R \setminus \{0\}$ gilt:

(a) $\frac{f}{I(f)}$ ist ein primitives Element von $R[X] \setminus \{0\}$.

(b) $I(af) \sim a \cdot I(f)$.

Lemma: Der Inhalt setzt sich fort zu einer Abbildung $K[X] \setminus \{0\} \to K^\times$, $f \mapsto I(f)$ mit denselben Eigenschaften für alle $f \in K[X] \setminus \{0\}$ und $a \in K^\times$.

Gauss-Lemma: Für alle $f, g \in K[X] \setminus \{0\}$ 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 $R[X] \setminus \{0\}$, 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

$$R[X] \twoheadrightarrow (R/(p))[X],\ f = \textstyle\sum' a_i X^i \mapsto \overline{f} := \textstyle\sum' \overline{a_i} X^i.$$

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 $e_1,\ldots,e_k \in R \smallsetminus \{0\}$ mit $e_1|e_2|\ldots|e_k$, 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 $e_1,\ldots,e_k$ bis auf Assoziiertheit, durch A eindeutig bestimmt.

Definition: Die Elemente $e_1,\ldots,e_k$ heissen die *Elementarteiler* von A.

Folge: Für alle $n \geqslant 1$ und alle $a_1,\ldots,a_n$ in einem Hauptidealring R sind äquivalent:

(a) $\mathrm{ggT}(a_1,\ldots,a_n) \sim 1$.

(b) Es existiert eine Matrix in $\mathrm{GL}_n(R)$ mit erster Spalte $(a_1,\ldots,a_n)^T$.

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

$$M \;\cong\; R^r \boxplus \bigboxplus_{i=1}^{k} R/(e_i).$$

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

$$M \;\cong\; R^r \boxplus \bigboxplus_{i=1}^{\ell} R/(p_i^{\nu_i}).$$

Zusatz: Für jedes Primelement $p \in R$ und jedes $\nu \geqslant 0$ gilt

$$\dim_{R/(p)}(p^\nu M/p^{\nu+1}M) \;=\; r + \bigl|\{1 \leqslant i \leqslant \ell \mid p_i \sim p \wedge \nu_i > \nu\}\bigr|.$$

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

$$K[X] \times V \to V,\ \left(\sum\nolimits' a_i X^i, v\right) \mapsto \sum\nolimits' a_i \varphi^i(v)$$

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

$$V \;\cong\; \boxplus_{i=1}^{k} K[X]/(p_i^{\nu_i}).$$

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)