Inhaltsverzeichnis

Kapitel 1: Kommutative Ringe

1.1 Ringe

Definition 1.1.1

Ein *Ring* ist eine Menge R ausgestattet mit Elementen $0 \in R$, $1 \in R$ und drei Abbildungen

$$\begin{cases} + : R \times R \to R \\ - : R \to R \\ \cdot : R \times R \to R \end{cases}$$

so dass folgende Axiome gelten.

$(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und Inversem $-$ d.h.

$$(a+b)+c = a+(b+c)$$
$$0+a = a$$
$$(-a)+a = 0$$
$$a+b = b+a$$

für alle $a, b, c \in R$.

$(R, \cdot)$: Assoziativität $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ und Einselement $1 \cdot a = a = a \cdot 1$.

Distributivität: $a(b+c) = ab + ac$ und $(b+c)a = ba + ca$.

Falls zusätzlich Kommutativität von $\cdot$ gilt: $ab = ba$, dann sprechen wir von einem *kommutativen Ring*.

Bemerkung.

- 0 ist eindeutig durch die Axiome bestimmt.
- Ebenso ist $-a$ durch die Axiome für jedes $a \in R$ eindeutig bestimmt.

- $0 \neq 1$ wurde nicht verlangt.
- $0 \cdot a = 0$ für jedes $a \in R$:

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 = 0 \cdot a.$$

Konvention.

- Klammern bei $+$ (und ebenso bei $\cdot$) lassen wir auf Grund der Assoziativität der Addition (Mult.) weg also $a+b+c+d$.
- Punktrechnung vor Strichrechnung, d.h. $a \cdot b + c = (a \cdot b) + c$.
- Den Multiplikationspunkt lässt man oft weg.

Notation.

$$0 \cdot a = 0 \quad 1 \cdot a = a \quad 2 \cdot a = a + a \quad 3 \cdot a = a + a + a$$
$$(n+1) = n \cdot a + a, (-n) \cdot a = -(n \cdot a) \text{ für } n \in \mathbb{N}.$$

Dies definiert eine Abbildung $\mathbb{Z} \times R \to R, (n, a) \mapsto n \cdot a$. Diese erfüllt: $(m+n) \cdot a = m \cdot a + n \cdot a$, $n \cdot (a+b) = n \cdot a + n \cdot b$.

Ebenso definieren wir

$$a^0 = 1_R \quad a^1 = a \quad a^2 = a \cdot a \quad a^{n+1} = a^n \cdot a \text{ für } n \in \mathbb{N}$$

Diese erfüllt

$$a^{m+n} = a^m + a^n \quad (a^m)^n = a^{m \cdot n} \quad (ab)^n = a^n b^n$$

in kommutativen Ringen.

Definition 1.1.2

Angenommen R, S sind Ringe und $f : R \to S$ ist eine Abbildung. Wir sagen f ist ein *Ringhomomorphismus* falls

$$f(1_R) = 1_S \quad f(a+b) = f(a) + f(b) \quad f(a \cdot b) = f(a) \cdot f(b)$$

für alle $a, b \in R$. Falls f invertierbar ist, so nennen wir f einen *Ringisomorphismus*.

Bemerkung. $f(0_R = 0_S$ denn $f(0_R) = f(0+0) = f(0) + f(0) \geq 0_S = f(0_R)$.
$f(-a) = -f(a)$ für $a \in R$ (ähnlicher Beweis).

Definition 1.1.3

Sei R ein Ring und $S \subseteq R$ auch ein Ring. Wir sagen S ist ein *Unterring*, falls $\mathrm{id} : S \to R, s \mapsto s$ ein Ringhomomorphismus ist.

Lemma 1.1.1

Falls in einem Ring R gilt $0 = 1$, dann ist $R = \{0\}$.

Lemma 1.1.2 Binomialformel

Sei R ein Ring und $a, b \in R$ mit $ab = ba$ (z.B. weil R kommutativ ist). Dann gilt für jedes $n \in \mathbb{N}$ $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Falls $n = 2$ ist und $(a+b)^2 = a^2 + 2ab + b^2$ gilt. Dann folgt $ab = ba$.

⚠Achtung 1.1.3

Ab nun werden wir nur kommutative Ringe betrachten.

1.2 Einheiten, Teilbarkeit, Quotientenkörper (Seite 34)

Definition 1.2.1

Sei R ein Ring. Ein Element $a \in \mathbb{R} \setminus \{0\}$ heißt ein Nullteiler falls es ein $b \in \mathbb{R} \setminus \{0\}$ mit $ab = 0$ gibt.

Definition 1.2.2

Ein kommutativer Ring heißt ein Integritätsbereich falls $0 \neq 1$ und falls aus $ab = ac$ und $a \neq 0$ $b = c$ folgt (Kürzen).

Lemma 1.2.1

Sei R ein kommutativer Ring mit $0 \neq 1$. Dann ist R ein Integritätsbereich gdw. R keine Nullteiler besitzt.

Definition 1.2.3

Sei R ein kommutativer Ring und $a, b \in R$. Wir sagen a *teilt* b, $a|b$ [in R] falls es ein c in R gibt mit $b = a \cdot c$.

Definition 1.2.4

Wir sagen $a \in R$ ist eine *Einheit* falls $a|1 \Leftrightarrow \exists b$ mit $ab = 1 \Leftrightarrow \exists a^{-1} \in R$. Einheiten mit $R^x = \{a \in R \mid a|1\}$

Bemerkung. R^x bildet eine Gruppe, $1 \in R^x$, $a, b \in R^x \implies (ab)(a^{-1}b^{-1}) = aa^{-1}bb^{-1} = 1 \implies ab \in R^x$.

Definition 1.2.5

Ein *Körper (field)* K ist ein kommutativer Ring in dem $0 \neq 1$ und jede Zahl ungleich Null eine multiplikative Inverse besitzt.

Lemma 1.2.2

Ein Körper ist ein Integritätsbereich.

Proposition 1.2.3

Sei $m \geq 1$ eine natürliche Zahl. Dann ist $\mathbb{Z}_m$ ein Körper genau dann wenn m eine Primzahl ist.

Satz 1.2.4 Quotientenkörper (S.38)

Sei R ein Integritätsbereich. Dann gibt es einen Körper K, der R enthält und so dass $K = \{\frac{p}{q} : p, q \in R, q \neq 0\}$. z.B. für $R = \mathbb{Z}$ haben wir $K = \mathbb{Q}$.

Ab sofort schreiben wir $\frac{a}{b} = [(a, b)]_\sim$. Wir identifizieren $a \in R$ mit $\frac{a}{1} \in K$. Hierzu bemerken wir, dass $\iota : a \in R \mapsto \frac{a}{1} \in K$ ein injektiver Ringhomomorphismus ist.

Definition 1.2.6

Sei K ein Körper und $L \subseteq K$ ein Unterring der auch ein Körper ist. Dann nennen wir L auch einen *Unterkörper*.

1.3 Ring der Polynome (Seite 41)

Im Folgenden ist R immer ein kommutativer Ring. Wir wollen einen neuen Ring, den Ring $R[X]$ der Polynome in der Variablen X und Koeffizienten in R definieren.

Definition 1.3.1

Sei R ein kommutativer Ring. Wir definieren den *Ring der formalen Potentreihen* (in einer Variable über dem Ring R) als

1. die Menge aller Folgen $(a_n)_{n=0}^\infty \in R^{\mathbb{N}}$
2. $0 = (0)_{n=0}^\infty, 1 = (1, 0, 0, \ldots)$
3. $+ : (a_n)_{n=0}^\infty + (b_n)_{n=0}^\infty = (a_n + b_n)_{n=0}^\infty$
4. $\cdot : (a_n)_{n=0}^\infty \cdot (b_n)_{n=0}^\infty = (c_n)_{n=0}^\infty$ wobei

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{\substack{i+j=n \\ i,j \geq 0}}^{\infty} a_i b_j.$$

Die Menge aller Folgen mit $a_n = 0$ für alle hinreichend großen $n \geq 0$ wird als der *Polynomring* (in einer Variable und über R) bezeichnet.

Notation. Wir ühren ein neues Symbol, eine Variable, z.B. X ein und identifizieren X mit

$$X^0 = 1 = (1, 0, 0, \ldots) \quad X^1 = (0, 1, 0, 0, \ldots) \quad X^2 = (0, 0, 1, 0, \ldots) \quad \ldots.$$

Allgemeiner: Sei a ein Polynom, dann ist

$$X \cdot a = (0, a_0, a_1, a_2, \ldots)$$

denn $(X \cdot a)_n = \sum_{i+j=n} X_i a_j = a_{n-1}$ da $X = 0$ außer wenn $i = 1$ ist. $(X \cdot a)_0 = X_0 \cdot a_0 = 0$.

Wir schreiben $R[X] = \{\sum_{i=0}^{n} a_i X^i : n \in \mathbb{N}, a_0, \ldots, a_n \in R\}$ (R-adjungiert-X) für den *Ring der Polynome in der Variablen X* und $R[\![X]\!] = \{\sum_{n=0}^{\infty} a_i X^i : a_0, a_1, \ldots \in R\}$ für den *Ring der formalen Potenzreihen in der Variable X*

Definition 1.3.2

Sei $p \in R[X] \setminus \{0\}$. Der Grad von p $\deg(p)$ ist gleich $n \in \mathbb{N}$ falls $p_n \neq 0$ ist und $p_k = 0$ für $k > n$. In diesem Fall nennen wir p_n auch den *führenden Koeffizienten.*

Wir definieren $\deg(0) = -\infty$.

Proposition 1.3.1

Sei R ein Integritätsbereich. Dann ist $R[X]$ auch ein Integritätsbereich. Des weiteren gilt für $p, q \in R[X] \setminus \{0\}$

- $\deg(pq) = \deg(p) + \deg(q)$ *und der führende Koeffizient von pq ist das Produkt der führenden Koeffizienten von p und q.*
- $\deg(p + q) \leq \max(\deg(p), \deg(q))$
- *Falls $p \mid q$, dann gilt* $\deg(p) \leq \deg(q)$.

Definition 1.3.3

Sei K ein Körper. Dann wird der Quotientenkörper von $K[X]$ als der *Körper der rationalen Funktionen* $K(X) = \{\frac{f}{g} : f, g \in K[x], g \neq 0\}$ bezeichnet.

Wenn wir obige Konstruktion (des Polynomrings) iterieren, erhalten wir den Ring der Polynome in mehreren Variablen

$$R[X_1, X_2, \ldots, X_d] := (R[X_1])[X_2][X_3] \ldots [X_d].$$

Falls $R = K$ ein Körper ist, definieren wir auch

$$K(X_1, X_2, \ldots, X_d) = \mathrm{Quot}(K[X_1, \ldots, X_d]).$$

Bemerkung. Auf $R[X_1, \ldots, X_d]$ gibt es mehrere Grad-Funktionen

$$\deg(x_1), \deg(x_2), \ldots \deg(x_d)$$
$$\deg_{\text{total}}(f) = \max\{m_1 + \ldots + m_d \mid f_{m_1,\ldots,m_d} \neq 0\}$$

für $f = \sum_{m_1,\ldots,m_d} f_{m_1,\ldots,m_d} X_1^{m_1} \ldots X_d^{m_d}$. z.B.

$$\deg_{\text{total}}(1 + X_1^3 + X_2 X_3) = 3 \qquad \deg_{X_2}(1 + X_1^3 + X_2 X_3) = 1.$$

Satz 1.3.2

Seien R, S zwei kommutative Ringe. Ein Ringhomomorphismus Φ von $R[x]$ nach S ist eindeutig durch seine Einschränkung $\varphi = \Phi \mid_R$ und durch das Element $x = \Phi(X) \in S$ bestimmt. Des weiteren definiert

$$\Phi(\sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} \phi(a_n) x^n \qquad (*)$$

einen Ringhomomorphismus falls $\varphi : R \to S$ ein Ringhomomorphismus ist und $x \in S$ beliebig ist.

Notation. Wir schreiben für zwei kommutative Ringe R, S

$$\mathrm{Hom}_{Ring}(R, S = \{\varphi : R \to S \mid \varphi \text{ ist ein Ringhomomorphismus}\}$$

in dieser Notation können wir obigen Satz in der Form

$$\mathrm{Hom}_{Ring}(R[X], S) \cong \mathrm{Hom}_{Ring}(R, S) \times S$$

schreiben. Dies kann iteriert werden:

$$\mathrm{Hom}_{Ring}(R[x_1, \ldots, x_d], S) \cong \mathrm{Hom}_{Ring}(R, S) \times \underbrace{S \times \ldots \times S}_{d-\text{mal}}.$$

1.4 Ideale und Faktorringe

Definition 1.4.1

Sei R ein kommutativer Ring. Ein Ideal in R ist eine Teilmenge $I \subseteq R$ so dass

(i) $0 \in I$

(ii) $a, b \in I \implies a + b \in I$

(iii) $a \in I, x \in R \implies xa \in I$

Satz 1.4.1

Sei R ein kommutativer Ring un $I \subseteq R$ ein Ideal.

1. *Die Relation $a \sim b \Leftrightarrow a - b \in I$ ist eine Äquivalenzrelation auf R. Wir schreiben auch $a \equiv b \mod I$ für die Äquivalenzrelation und ${}^R/_I$ für den Quotienten, den wir Faktorring nennen wollen.*
2. *Die Addition, Multiplikation, das Negative induzieren wohldefinierte Abbildungen*
$$ {}^R/_I \times {}^R/_I \to {}^R/_I \quad bzw. \quad {}^R/_I \to {}^R/_I. $$
3. *Mit diesen Abbildungen, $0_{R/I} = [0]_\sim, 1_{R/I} = [1]_\sim$ ist ${}^R/_I$ ein Ring und die kanoische Projektion $p : R \to {}^R/_I$ mit $a \in R \mapsto [a]_\sim = a + I$ ist ein surjektiver Ringhomomorphismus.*

Lemma 1.4.2

Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring. Dann gilt
$$ I = R \Leftrightarrow 1 \in I \Leftrightarrow I \cap R^X \neq \varnothing. $$

Definition 1.4.2

Sei R ein kommutativer Ring und seien $a_1, \ldots, a_n \in R$. Dann wird
$$ I = (a_1, \ldots, a_n) = \{x_1a_1 + x_2a_2 + \ldots + x_na_n : x_1, \ldots, x_n \in R\} $$
das von $a_1, \ldots, a_n$ *erzeugte Ideal* genannt.
Für $a \in I$ wird $I = (a) = Ra$ das von a *erzeugte Hauptideal* genannt.

Lemma 1.4.3

Sei R ein kommutativer Ring.

1) $(a) \subseteq (b) \Leftrightarrow b \mid a$

2) Falls R ein Integritätsbereich ist, dann gilt $(a) = (b) \Leftrightarrow \exists u \in R^x$ mit $b = ua$

Falls $I \subseteq R$ ein Ideal ist und $a \in R$, dann ist die Restklasse für Äuivalent modulo I gleich
$$ [a]_N = \{x \in R : x \sim a\} = a + I. $$

Satz 1.4.4 Erster Isomorphiesatz

Angenommen R, S sind kommutative Ringe und $\varphi : R \to S$ ist ein Ringhomomorphismus.

1. *Dann induziert φ einen Ringisomorphismus*
$$ \overline{\varphi} : {}^R/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}(\varphi) = \varphi(R) \subseteq S $$
so dass $\varphi = \overline{\varphi} \circ p$ wobei $p : R \to {}^R/_{\mathrm{Ker}(\varphi)}$ die kanonische Projektion ist (Diagramm links).
2. *Sei $I \subseteq \mathrm{Ker}(\varphi)$ ein Ideal in R. Dann induziert φ einen Ringhomomorpismus $\overline{\varphi} : {}^R/_I \to S$ mit $\varphi = \overline{\varphi} \circ p_I$ (Diagramm rechts). Des weiteren gilt $\mathrm{Ker}(\overline{\varphi}) = {}^{\mathrm{Ker}(\varphi)}/_I$ und $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$*

Bemerkung. Sei $I_0 \subseteq R$ ein Ideal in einem kommutativen Ring. Dann gibt es eine Korrespondenz (kanonische Bijektion) zwischen Idealen in ${}^R/_{I_0}$ und Idealen in R, die I_0 enthalten.
$$ I \subseteq R, I_0 \subseteq I \quad \mapsto \quad {}^I/_{I_0} = \{x + I_0 : x \in I\} \subseteq {}^R/_{I_0} $$
$$ J \subseteq {}^R/_{I_0} \quad \mapsto \quad p_{I_0}^{-1}(J) \subseteq R \qquad (p_{I_0} : \begin{cases} R \to {}^R/_{I_0} \\ x \mapsto x + I_0 \end{cases}). $$

Definition 1.4.3

Wir sagen zwei Ideale I, J in einem kommutativen Ring sind *coprim*, falls $I + J = R$ ist. D.h. $\exists a \in I, b \in J$ mit $1 = a + b$.

Proposition 1.4.5 Chinesischer Restsatz

Sei R ein kommutativer Ring und seien $I_1, \ldots, I_n$ paarweise coprime Ideale. Dann ist der Ringhomomorphismus $\varphi : R \to {}^R/_{I_1} \times \ldots \times {}^R/_{I_n}$ mit $x \mapsto (x + I_1, \ldots, x + I_n)$ surjektiv mit $\mathrm{Ker}(\varphi) = I_1 \cap \ldots \cap I_n$.
Dies induziert einen Ringisomorphismus ${}^R/_{I_1 \cap \ldots \cap I_n} \to {}^R/_{I_1} \times \ldots \times {}^R/_{I_n}$.

1.5 Charakteristik eines Körpers

Sei K ein Körper. Dann gibt es einen Ringhomomorphismus $\varphi : \mathbb{Z} \to K$ mit
$$ \begin{cases} n \in \mathbb{N} \mapsto \underbrace{1 + \ldots + 1}_{n-\text{mal}} \\ -n \in \mathbb{N} \mapsto -(\underbrace{1 + \ldots + 1}_{n-\text{mal}}) \end{cases} $$

Sei $I = \mathrm{Ker}(\varphi)$ so, dass ${}^{\mathbb{Z}}/_{I} \equiv \mathrm{Im}(\varphi) \subseteq K$. Da K ein Körper ist, ist $\mathrm{Im}(\varphi)$ ein Integritätsbereich.

Lemma 1.5.1

Sei $I \subseteq \mathbb{Z}$ ein Ideal. Dann gilt $I = (m)$ für ein $m \in \mathbb{N}$. Der Quotient ist ein Integritätsbreich genau dann wenn $m = 0$ oder m eine Primzahl ist.

Definition 1.5.1

Sei K ein Körper. Wir sagen, dass K Charakteristik 0 hat, falls $\varphi : \mathbb{Z} \to K$ injektiv ist. Wir sagen, dass K Charakteristik $p \in N_{>0}$ hat falls $\varphi : \mathbb{Z} \to K$ den Kern (p) hat.

Proposition 1.5.2

Sei K ein Körper mit Charakteristik $p > 0$. Dann ist die Frobeniusabbildung *$F : x \in K \to x^p \in K$ ein Ringhomomorphismus. Falls $|K| < \infty$, dann ist F ein Ringautomorphismus.*

1.6 Primideale und Maximalideale

Definition 1.6.1

Sei R ein kommutativer Ring, und sei $I \subseteq R$ ein Ideal. Wir sagen I ist ein *Primideal*, falls ${}^{R}/_{I}$ ein Integritätsbreich ist. Wir sagen I ist ein *Maximalideal*, falls ${}^{R}/_{I}$ ein Körper ist.

Proposition 1.6.1

Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring.

1) Dann ist I ein Primideal genau dann wenn $I \neq R$ und für alle $a, b \in R$ gilt $ab \in I \implies a \in I$ oder $b \in I$.

2) Dann ist I ein Maximalideal genau dann wenn $I \neq R$ und es gibt kein Ideal J mit $I \subsetneq J \subsetneq R$.

Bemerkung. Der Hilbert'sche Nullstellensatz besagt, dass jedes Maximalideal in $\mathbb{C}[X_1, \ldots, X_n]$ von dieser Gestalt ist.

Satz 1.6.2

Sei R ein kommutativer Ring, und $I \subsetneq R$ ein Ideal. Dann existiert ein Maximalideal $m \supseteq I$. Insbesondere existiert in jedem Ring $R \neq [0]$ ein Maximalideal.

1.7 Unterring

Definition 1.7.1

Sei R ein Ring und $S \subseteq R$ auch ein Ring. Wir sagen S ist ein *Unterring* falls $\mathrm{id} : S \to R, s \mapsto s$ ein Ringhomomorphismus ist.

Alternativ Definition: Sei R ein Ring und $S \subseteq R$. Dann ist S ein Unterring falls

1. $0, 1 \in S$.
2. $a - b \in S$ für alle $a, b \in S$.
3. $a \cdot b \in S$ für alle $a, b \in S$.

Notation. Sei $S \subseteq R$ ein Unterring in einem Ring R. Seien $a_1, \ldots, a_n \in R$. Wir definieren

$$S[a_1, \ldots, a_n] = \bigcap_{\substack{T \subseteq R \text{ Unterring} \\ T \supseteq S \\ a_1, \ldots, a_n \in T}} T.$$

genannt „S-adjungiert $a_1, \ldots, a_n$“.

$$= \mathrm{ev}_{a_1, \ldots, a_n}(S[x_1, \ldots, x_n]) = \{ \sum_{k_1, \ldots, k_n \in M} c_{k_1, \ldots, k_n} a_1^{k_1} \ldots a_n^{k_n} \}.$$

mit $|M| < \infty, M \subseteq \mathbb{N}^n, c_{k_1, \ldots, k_n} \in S$.

1.8 Matrizen

Sei R ein kommutativer Ring, $m, n \in N_{>0}$. Dann bezeichnen wir die Menge $\mathrm{Mat}_{mn}(R)$ als die Menge aller $m \times n$-Matrizen

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m_1} & \ldots & a_{mn} \end{pmatrix}.$$

mit Koeffizienten oder Eintragungen $a_{11}, \ldots, a_{mn} \in R$. Für $m = n$ i definieren wir auch auf $\mathrm{Mat}_{mm}(R)$ auf übliche Weise die Addition und Multipliaktion. Dies definiert auf $\mathrm{Mat}_{mm}(R)$ gemeinsam mit dem Einselement $I_m = (\delta_{ij})_{i,j}$ eine Ringstruktur. Sobald $m > 1$ sit, ist dieser Ring nichtkommutativ.

Die Einheiten in $\mathrm{Mat}_{mm}(R)$ werden auch als invertierbare Matrizen bezeichnet. Die Menge wird auch die allgemeine lineare Gruppe vom Grad m über R genannt:

$$\mathrm{Gl}_m(R) = \mathrm{Mat}_{mm}(R)^{\times} = \{A \in \mathrm{Mat}_{mm}(R) \mid \text{es existiert ein } B \in \mathrm{Mat}_{mm}(R) \text{ mit } AB = BA = I_n\}.$$

Proposition 1.8.1 META

Jede Rechenregel für Matrizen über R die nur $+, -, \cdot, 0, 1$ beinhalten, gilt auch über einem beliebigen kommutativen Ring.

Proposition 1.8.2

Sei R ein kommutativer Ring

- $\mathrm{Mat}_{mm}(R)$ *erfüllt die Ringaxiome, also z.B.* $A(BC) = (AB)C$
- $\det(AB) = \det(A)\det(B)$
- $A\widetilde{A} = \widetilde{A}A = \det(A)I_m$, *wobei* $\widetilde{A}$ *die komplementäre Matrix*

$$\widetilde{A} = ((-1)^{i+j}\det(A_{ji}))_{i,j}.$$

- $\mathrm{char}_A(A) = 0$ *für das charakteristische Polynom* $\mathrm{char}_A(X) = \det(XI_m - A)$ *einer Matrix* A.

Bemerkung. $\det(A)$, jeder Koeffizient von $A(BC), (AB)C, A\widetilde{A}, \widetilde{A}A, \det(A)I, \mathrm{char}_A(X)$, $\mathrm{char}_A(A)$ hängt polynomiell von den Eintragungen von A, B, C ab, wobei die Koeffizienten in $\mathbb{Z}$liegen z.B.

$$\det(A) = \sum_{\sigma \in S_n} \underbrace{\mathrm{sgn}(\sigma)}_{\in \mathbb{Z}} a_{1\sigma(1)}a_{2\sigma(2)}\dots a_{n\sigma(n)}$$

welche Monome in den Eintragungen von A sind.

Lemma 1.8.3

Wenn ein Polynom $f \in \mathbb{R}[X_1, \dots, X_n]$ auf ganz $\mathbb{R}^n$ verschwindet, dann ist $f = 0$.

Bemerkung. Das Lemma gilt analog für jeden Körper K mit $|K| = \infty$.

Kapitel 2: Faktorisierungen von Ringen

Buch Seiten 83-114. Wir wollen in diesem Kapitel Ringe mit eindeutiger Primfaktorzerlegung betrachten. Im Folgenden ist R immer ein Integritätsbereich.

Definition 2.0.1 WIEDERHOLUNG

$a \mid b \Leftrightarrow \exists c$ mit $b = ac$ für $a, b \in R$.
$a \in R^\times$ ist eine Einheit $\Leftrightarrow a \mid 1$.

Definition 2.0.2

Wir sagen $p \in R \setminus \{0\}$ ist *irreduzibel*, falls $p \notin R^\times$ und für alle $a, b \in R$ gilt $p = ab \implies a \in R^\times$ oder $b \in R^\times$.

Definition 2.0.3

Wir sagen $p \in R \setminus \{0\}$ ist *prim* falls (p) ein Primideal ist, in anderen Worten falls $p \notin R^\times$ und für alle $a, b \in R$ gilt $p \mid ab \implies p \mid a$ oder $p \mid b$.

Lemma 2.0.1

Sei R ein Integritätsbereich. Dann ist jedes prim $p \in R$ auch irreduzibel.

Bemerkung. Die Umkehrung des Lemmas stimmt im Allgemeinen nicht. Wenn sie doch stimmt, so hilft dies für die Eindeutigkeit in einer Primfaktorzerlegung. Siehe später in 3.3.

2.1 Euklidische Ringe

Definition 2.1.1

Ein Integritätsbereich R heißt ein *Euklidischer Ring* falls es eine gradfunktion $N : R \setminus \{0\} \to \mathbb{N}$ gibt, so fass die beiden folgenden Eigenschaften gelten:

- *Gradungleichung*: $N(f) \leq N(fg)$ für alle $f, g \in \mathbb{R} \setminus \{0\}$.
- *Division mit Rest*: Für $f, g \in R$ mit $f \neq 0$ gibt es $q, r \in R$ mit $g = q \cdot f + r$ wobei $r = 0$ oder $N(r) < N(f)$ ist. Wir nennen r den *Rest* (bei Division durch f).

Satz 2.1.1

In einem Euklidischen Ring ist jedes Ideal ein Hauptideal.

2.2 Hauptidealring

Definition 2.2.1

Sei R ein Integritätsbereich. Dann heißt R ein *Hauptidealring* falls jedes Ideal in R ein Hauptideal ist.

Bemerkung. Der Ring $\mathbb{Z}[\frac{1}{2}(1 + i \cdot \sqrt{163})]$ ist ein Hauptidealring und kann nicht zu einem Euklidischen Ring gemacht werden.

Proposition 2.2.1

Sei R ein Hauptidealring. Für je zwei Elemente $f, g \in R \setminus \{0\}$ gibt es einen größten gemeinsamen Teiler d mit $(d) = (f) + (g)$.

Definition 2.2.2

Seien $f, g, d \in R \setminus \{0\}$. Wir sagen d ist ein gemeinsamer Teiler von f und g falls $d \mid f$ und $d \mid g$. Wir sagen d ist ein größter gemeinsamer Teiler falls d ein gemeinsamer Teiler ist und jeder gemeinsame Teiler t auch d teilt.

Bemerkung. Zwei ggT's unterscheiden sich um eine Einheit (wenn R ein Integritätsbereich ist).

In einem Euklidischen Ring kann man einen ggT von $f, g \in R \setminus \{0\}$ durch den *euklidischen Algorithmus* bestimmen.

0) Falls $N(f) > N(g)$, so vertauschen wir f und g. Also dürfen wir annehmen, dass $N(f) \leq N(g)$.

1) Dividiere g durch f mit Rest: $g = qf + r$

2) Falls $r =$ ist, so ist f ein ggT und der Algorithmus stoppt.

3) Falls $r \neq 0$ ist, so ersetzen wir (f, g) durch (r, f) und springen nach 1).

Lemma 2.2.2

Der Euklidische Algorithmus (wie oben beschrieben) endet nach endlich vielen Schritten und berechnet einen ggT.

Satz 2.2.3 PRIME ELEMENTE

Sei R ein Hauptidealring.

1) *Dann ist $p \in R \setminus \{0\}$ prim genau dann wenn p irreduzibel ist.*
2) *Jedes $f \in R \setminus \{0\}$ lässt sich als Produkt einer Einheit und endlich vielen primen Elementen schreiben.*

Anhang A: Auswahlaxiom und das Zornsche Lemma

Auswahlaxiom (in der Mengenlehre)
Sei I eine nichtleere Menge und seien X_i für $i \in I$ nichtleere Mengen. Dann ist $\prod_{i\in I} X_i \neq \varnothing$, d.h. es existiert eine Funktion

$$f : I \to \bigcup_{i\in I} X_i$$

mit $f(i) \in X_i$ für alle $i \in I$.

Bemerkung.
- unabhängig von den anderen ZF-Axiomen der Mengenlehre
- kritisiert wegen der Nichtkonstruktivität des Axioms und mancher scheinbar paradoxen Folgerung
- notwendig für einen großen Teil der Mathematik

Häufig wird nicht das Auswahlaiom sondern ein dazu äquivalentes Lemma, das Zornsche Lemma, verwendet. Für dieses benötigen wir etwas mehr Begriffe:

Definition A.0.1

Sei X eine Menge. Eine *Ordnung* auf X ist eine Relation $\leq$ so dass

1) reflexivität: $x \leq x$
2) antisymmetrie: $x \leq y$ und $y \leq x$
3) transitivität: $x \leq y$ und $y \leq z \implies x \leq z$ für alle $x, y, z \in X$.

Die Ordnung heißt *total* oder *linear* falls zusätzlich

4) linearität: $x \leq y$ oder $y \leq x$

gilt. Ansonsten heißt sie *partiell*.

Definition A.0.2

Sei $\leq$ eine Ordnung auf einer Menge X. Ein Element $x \in X$ heißt *maximal* falls für alle $y \in X$ gilt $x \leq y \implies x = y$. Ein Element $m \in X$ ein *Maximum* falls $x \leq m$ für alle $x \in X$ gilt.

Definition A.0.3

Sei $\leq$ eine Ordnung auf einer Menge X und sei $A \subseteq X$. Ein Element $x \in X$ heißt eine *obere Schranke von* A falls $a \leq x$ für alle $a \in A$. Analog definiert man *untere Schranke von* A.

Definition A.0.4

Sei $\leq$ eine Ordnung auf einer Menge X. Eine Teilmenge $K \subseteq X$ heißt eine *Kette* falls für alle $x, y \in K$ gilt $x \leq y$ oder $y \leq x$. Wir sagen die Ordnung $\leq$ sei *induktiv* falls jede Kette in X eine obere Schranke besitzt.

Satz A.0.1 ZORNSCHES LEMMA

Sei $\leq$ eine induktive Ordnung auf einer Menge X. Dann existiert ein maximales Element in X.

Typische Anwendung: Jeder Vektorraum über K hat eine Hamel-Basis.
Vorerst einige Definitionen und Lemmata:

Definition A.0.5

Für eine Teilmenge $C \subseteq X$ definieren wir

$$\widehat{C} = \{x \in X \setminus C \mid x \text{ ist eine obere Schranke}\}.$$

Um die Beweisidee umzusetzen verwenden wir eine *Auswahlfunktion* auf der Menge $\{\widehat{C} : C \subseteq X \text{ s.d. } \hat{C} \neq \varnothing\}$

Definition A.0.6

Eine Teilkette $K \subseteq X$ heißt eine *f-Kette* falls für jede Teilmenge $C \subseteq K$ mit $\widehat{C} \cap K \neq \varnothing$ das Element $f(\widehat{C})$ zu K gehört und eine minimale obere Schranke von C in K ist, also $f(\widehat{C}) \leq y$ für alle $y \in \widehat{C} \cap K$ gilt. Dies vermeidet „unnötige Zwischenschritte“, die zu Problemen bei einer Vereinigung von Ketten führen würde.

Lemma A.0.2 VERLÄNGERUNG

Falls K eine f-Kette ist und $\widehat{K} \neq \varnothing$ ist, so ist $K_{neu} = K \cup \{f(\widehat{K})\}$ wieder eine f-Kette.

Lemma A.0.3 ZWEI f-KETTEN

Angenommen K, K' sind zwei f-Ketten und $K' \setminus K \neq \varnothing$. Dann ist $K \subseteq K'$ und es gilt $x \leq x'$ für alle $x \in K$ und $x' \in K' \setminus K$.
Informell: „K ist eine Anfangsabschrift von K'“.

Lemma A.0.4 VEREINIGUNG

Wir definieren $K_{max} = \bigcup_{\substack{K \text{ ist eine} \\ f-Kette}} K$. Dann ist K_{max} eine f-Kette.