Ringtheorie: kurze Wiederholung

Themen

Unterringe
Ideale: maximale Ideale, Primideale
Faktorringe
Homomorphiesatz
Isomorphiesätze
Polynomalgebren
Integritätsringe
Faktorielle Ringe
Euklidische Ringe
Division mit Rest
Quotientenringe
Quarakteristik
Teilbarkeit, Irreduzibilität
Chinesischer Restsatz

Einige wichtige Konzepte

Ringaxiome

Eine Menge R zusammen mit zwei Abbildungen $+ : R \times R \to R, (r,s) \mapsto r+s$ und $\cdot : R \times R \to R, (r,s) \mapsto rs$, heißt Ring mit Einselement, wenn gilt:

(a) Additive Gruppe: $(R,+)$ ist abelsche Gruppe; neutrales Element sei 0, Inverses von $r \in R$ sei $-r$.
(b) Multiplikatives Monoid: $(R,\cdot)$ ist Monoid (nicht notwendigerweise Inverses); neutrales Element sei 1.
(c) Distributivgesetz: Für alle $r,s,t \in R$ gilt: $(r+s)t = rt+st$ und $r(s+t) = rs+rt$.

— Einheitengruppe: $R^\times = \{$ invertierbare Elemente $\}$
— Kommutativer Ring: $(R,\cdot)$ kommutativ
— Schiefkörper: $1 \neq 0$ und $R^\times = (R\backslash\{0\})$
— Körper: R kommutativ, $1 \neq 0$ und $R^\times = (R\backslash\{0\})$

Unterringe

Sei R ein Ring. Eine Teilmenge $S \subset R$ heißt Unterring, wenn S Untergruppe von $(R,+)$ und Untermonoid von $(R,\cdot)$ ist. Dann ist S bezüglich $+$ und $\cdot$ ein Ring.
S ist genau dann Unterring von R, wenn gilt $1 \in S$ und für alle $s,t \in S$ ist $s-t \in S$ und $st \in S$.

Ideale

Eine Teilmenge $A \subset R$ heißt Linksideal von R, wenn A Untergruppe von $(R,+)$ ist, und für alle $a \in A$, $r \in R$ gilt $ra \in A$.
Genauso Rechtsideal/ beidseitiges Ideal.

— Beliebige Schnitte von Idealen: Ist $(A_i)_{i\in I}$ Familie von (Links-/Rechts-)Idealen, dann ist auch

$$\bigcap_{i\in I} A_i$$

(Links-/Rechts-)Ideal.

— Endliche Summen von Idealen: Sind $A_1, \dots A_n$ (Links-/Rechts-)Ideale, dann ist

$$A_1 + \ldots + A_n = \left\{ x \in R \;\middle|\; \exists a_i \in A_i, 1 \leqslant i \leqslant n : x = a_1 + \ldots + a_n \right\}$$

(Links-/Rechts-)Ideal.

— Erzeugtes Ideal: Ist $X \subset R$ Teilmenge, dann ist

$$\begin{aligned} {}_R(X) &= \bigcap \{A \mid A \text{ Linksideal von } R \text{ mit } X \subset A\} \\ &= \left\{ r \in R \;\middle|\; \exists n \in \mathbb{N}_0, x_1, \ldots, x_n \in X, r_1, \ldots, r_n \in R : r = \sum_{i=1}^{r} r_i x_i \right\} \end{aligned}$$

das kleinste Linksideal, das X enthält.
Sind $a_1, \ldots, a_r \in R$, dann

$$Ra_1 + \ldots + Ra_n = {}_R(a_1, \ldots, a_n) = {}_R(\{a_1, \ldots, a_n\}) = \left\{ r \in R \;\middle|\; \exists r_1, \ldots, r_n \in R : r = \sum_{i=1}^{n} r_i a_i \right\}.$$

Ringhomomorphismen

Eine Abbildung $\varphi : R \to R'$ zwischen zwei Ringen heißt Ringhomomorphismus, falls $\varphi : (R, +) \to (R', +)$ Gruppenhomomorphismus ist, und $\varphi : (R, \cdot) \to (R', \cdot)$ Monoidhomomorphismus ist.
Bilder/Urbilder von Unterringen sind Unterringe.
Urbilder von Idealen sind Ideale. Ist ein Homomorphismus surjektive, so sind auch Bilder von Idealen Ideale.
Sei R ein kommutativer Ring. Ein Ring R' (mit Eins) heißt R-Algebra, wenn es einen Ringhomomorphismus $\varphi : R \to R'$ gibt mit $\operatorname{im}(\varphi) \subset Z(R')$. Man definiert dann eine Skalarmultiplikation von R auf R' durch

$$r.r' = \varphi(r)r' \quad \text{für } r \in R, r' \in R'.$$

Eine Algebra ist gleichzeitig ein Ring und ein Vektorraum.

Faktorringe

R ein Ring, $A \subset R$ ein zweiseitiges Ideal.
Der Faktorring von R modulo A ist die Menge R/A der Nebenklassen additiven Nebenklassen $r + A$ mit Addition

$$R/A \times R/A \to R/A, (r + A, s + A) \mapsto r + s + A$$

und Multiplikation

$$R/A \times R/A \to R/A, (r + A, s + A) \mapsto rs + A.$$

Die kanonische Projektion:

$$\pi : R \to R/A, r \mapsto r + A$$

ist ein surjektiver Ringhomomorphismus mit $\ker(\pi) = A$.
Sei $\varphi : R \to R'$ ein Ringhomomorphismus.

(a) Ist A Ideal von R mit $A \subset \ker(\varphi)$, dann gibt es genau einen Ringhomomorphismus $\varphi' : R/A \to R$ mit $\varphi = \varphi' \circ \pi$.

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & R' \\ & R/A \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

(b) **(Homomorphiesatz)** Es gibt genau einen injektiven Ringhomomorphismus $\varphi' : R/\ker(\varphi) \to R'$ mit $\varphi = \varphi' \circ \pi$.

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & R' \\ & R/\ker(\varphi) \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

Insbesondere ist die Abbildung

$$\varphi : R/\ker(\varphi) \to \operatorname{im}(\varphi), r + \ker(\varphi) \mapsto \varphi(r)$$

ein Ringisomorphismus.

(c) **(1. Isomorphiesatz)** Sei $S \subset R$ ein Unterring, $A \subset R$ ein Ideal. Dann ist $S \cap A \subset S$ ein Ideal, $S + A \subset R$ Unterring, $A \subset S + A$ ein Ideal, und die Abbildung

$$S/S \cap A \to S + A/A, s + S \cap A \mapsto s + A$$

ein Ringisomorphismus.

(d) **(2. Isomorphiesatz)** Seien A, B Ideale von R mit $A \subset B$. Dann ist $B/A \subset R/A$ ein Ideal, und die Abbildung

$$R/B \to (R/A)/(B/A), r + B \mapsto (r + A) + B/A$$

ein Ringisomorphismus.

Polynomalgebren

Sei R ein komutativer Ring. Ein Polynom über R in einer Variablen ist ein formale Summe

$$f = a_n X^n + \ldots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i$$

Die Variable X ist unabhängig von den Elementen des Rings.

$$R[X] = \left\{ f = \sum_{i \geqslant 0} a_i X^i \;\middle|\; \text{fast alle } a_i = 0 \right\}$$

ist ein kommutativer Ring mit der "gewöhnlichen" Addition und Multipikation.

$$\begin{aligned}
(\sum_{i \geqslant 0} a_i X^i) + (\sum_{i \geqslant 0} b_i X^i) &= \sum_{i \geqslant 0} (a_i + b_i) X^i \\
(\sum_{i \geqslant 0} a_i X^i) \cdot (\sum_{i \geqslant 0} b_i X^i) &= \sum_{i \geqslant 0} (\sum_{k+l=i} a_k b_l) X^i
\end{aligned}$$

mit additivem beziehungsweise multiplikativem Inversen

$$\begin{aligned}
1_{R[X]} &= 1X^0 = 1 \\
0_{R[X]} &= 0X^0 = 0
\end{aligned}$$

Grad eines Polynoms $f \in R[X]$:

$$\deg(f) := \begin{cases} \infty & \text{falls } f = 0 \\ \max\{n \in \mathbb{N}_0 : a_n \neq 0\} & \text{sonst} \end{cases}$$

Es gilt $\deg(f \cdot g) \leqslant \deg(f) + \deg(g)$.
Rekursiv definiert man Polynomringe in mehreren Variablen:

$$R[X_1, \ldots, X_n] := R[X_1, \ldots, X_{n-1}][X_n].$$

Man betrachtet hier also Polynome in der Variablen X_n mit Koeffizienten in dem kommutativen Ring $R[X_1, \ldots, X_{n-1}]$.

Einsetzungshomomorphismus

Sei S eine kommutative R-Algebra, sei $n \in \mathbb{N}$ und $(s_1, \ldots, s_n) \in S^n$. Dann gibt es genau einen R-Algebren-Homomorphismus $\rho : R[X_1, \ldots, X_n] \to S$, mit $\rho(X_i) = s_i$, $1 \leqslant i \leqslant n$.

$$\begin{tikzcd}
R[X_1, \ldots, X_n] \arrow[rr] & & S \\
& R \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Man schreibt $\rho(f) = f(s_1, \ldots, s_n)$.
$(s_1, \ldots, s_n)$ heißt Nullstelle von f, falls $\rho(f) = f(s_1, \ldots, s_n) = 0$.

Division mit Rest in $R[X]$

Sei R ein kommutativer Ring, $0 \neq f \in R[X]$ ein Polynom, dessen höchster Koeffizient eine Einheit in R ist. Zu jedem $g \in R[X]$ gibt es dann eindeutig bestimmte Polynome $q, h \in R[X]$ mit $g = qf + h$ und $\deg(h) < \deg(f)$.
Seien $f \in R[X]$, $c \in R$.

(a) Es gibt $g \in R[X]$ mit $f = (X - c)g + f(c)$.

(b) c ist genau dann Nullstelle von f, wenn es $g \in R[X]$ gibt mit $f = (X - c)g$.

Integritätsringe

Ein kommutativer Ring heißt Integritätsring oder Integritätsbereich, wenn $1 \neq 0$ und $(R\backslash\{0\}, \cdot)$ Untermonoid von $(R, \cdot)$ ist, das heißt, wenn $1 \neq 0$ und für alle $r, s \in R\backslash\{0\}$ gilt $rs \neq 0$.

„Kürzungsregel“: Ein kommutativer Ring R ist genau dann Integritätsbereich, wenn $1 \neq 0$ und für alle $r, s, t \in R$ mit $rs = rt$ und $r \neq 0$ folgt $s = t$.

Für einen Integritätsbereich R gelten viele nützliche Eigenschaften.

— $R[X_1, \dots, X_n]$ ist Integritätsring, für $f, g \in R[X_1, \dots, X_n]$ gilt $\deg(fg) = \deg(f) + \deg(g)$.

— $R[X_1, \dots, X_n]^\times = R^\times$.

— Jedes Polynom $0 \neq f \in R[X]$ hat höchstens $\deg(f)$ Nullstellen.

Euklidische Ringe

Ein Integritätsring R heißt euklidisch, wenn es eine Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}_0$ gibt, so daß gilt: Für alle $a, b \in R$, $b \neq 0$, gibt es $q, r \in R$ mit $a = bq + r$ und wenn $r \neq 0$ ist, dann $\delta(r) < \delta(b)$. Eine solche Abbildung heißt euklidische Norm.

Ein Integritätsring R heißt Hauptidealring, wenn jedes Ideal von R Hauptideal ist.
In einem euklidischen Ring ist jedes Ideal ein Hauptideal, das heißt, von einem Element erzeugt.

Merkregel: Es gelten folgende Inklusionen für kommutative Ringe:

Körper $\subset$ Euklidische Ringe $\subset$ Hauptidealringe $\subset$ faktorielle Ringe $\subset$ Integritätsringe

Quotientenringe

Idee: Man will eine multiplikativ abgeschlossene Teilmenge eines (kommutativen) Rings $S \subset R \setminus \{0\}$ invertieren.

Konstruktion: Definiere auf $R \times S$ eine Äquivalenzrelation:

$$(r, s) \sim (r', s') \text{ genau dann wenn es } t \in S \text{ gibt, so daß } (rs' - r's)t = 0.$$

Man setzt $R_S = R \times S/\sim$ und bezeichnet die Äquivalenzklasse von (r, s) mit $\frac{r}{s}$. Also gilt $\frac{r}{s} = \frac{r'}{s'}$ genau dann wenn es $t \in S$ gibt mit $(rs' - r's)t = 0$.

— Dies ist ein kommutativer Ring mit Null $\frac{0}{1}$ und Eins $\frac{1}{1}$.

— Kanonische Abbildung: $i : R \to R_S$, $r \mapsto \frac{r}{1}$ ist Ringhomomorphismus mit $\ker(i) = \{r \in R \mid \exists s \in S : rs = 0\}$.

— Für alle $s \in S$ ist $i(s) = \frac{s}{1}$ Einheit von R_S.

— Ist R ein Integritätsring, dann ist das t aus der Definition nicht notwendig, und i injektiv. Schreibe $r = \frac{r}{1}$.

— Universelle Eigenschaft: Ist T ein kommutativer Ring, $\varphi : R \to T$ Ringhomomorphismus mit $\varphi(S) \subset T^\times$, dann gibt es genau einen Ringhomomorphismus $\widetilde{\varphi} : R_S \to T$ mit $\widetilde{\varphi} \circ i = \varphi$, das heißt, das Diagramm

$$\begin{tikzcd} R \arrow[rr, "i"] \arrow[dr, "\varphi"'] & & R_S \arrow[dl, dashed, "\exists!\widetilde{\varphi}"] \\ & T & \end{tikzcd}$$

— Ideale: gegeben durch $(i(A)) = \left\{ \frac{a}{s} \ ; \ a \in A, s \in S \right\}$, $A \subset R$ Ideal.

Charakteristik

R Integritätsring.
Primring: $R_0 = \mathbb{Z} \cdot 1$ ist der kleinste Unterring von R.

Zwei Fälle sind möglich:

(a) $R_0 \cong \mathbb{Z}$; genau dann, wenn $z1 \neq 0$ für alle $z \in \mathbb{Z} \setminus \{0\}$.

(b) Es gibt eine Primzahl $p \in \mathbb{N}$ mit $R_0 \cong \mathbb{Z}/(p)$; p ist die kleinste natürliche Zahl $z \in \mathbb{N}$ mit $z.1 = 0$.

K Körper.
Primkörper: K_0 ist der kleinste Unterkörper von K.

Zwei Fälle sind möglich:

(a) $K_0 \cong \mathbb{Q}$; genau dann, wenn $z.1 \neq 0$ für alle $z \in \mathbb{Z} \setminus \{0\}$.

(b) Es gibt eine Primzahl $p \in \mathbb{N}$ mit $K_0 \cong \mathbb{Z}/(p)$; p ist die kleinste natürliche Zahl $z \in \mathbb{N}$ mit $z.1 = 0$.

Charakteristik von K:

$$\operatorname{char}(K) = \begin{cases} 0 & \text{falls für alle } 0 \neq z \in \mathbb{Z} : z.1 \neq 0 \\ p & \text{Primzahl, falls } p \text{ die kleinste natürliche Zahl ist mit } z.1 = 0 \end{cases}$$

Maximale Ideale

Sei R ein Ring. Ein (Links-/Rechts-/beidseitiges) Ideal $A \subset R$ heißt maximal, wenn $A \neq R$ ist und es kein (Links-/Rechts-/beidseitiges) Ideal $B \subset R$ gibt, mit $A \subsetneq B \subsetneq R$.

— Jedes (Links-/Rechts-/beidseitige) Ideal ist in einem maximalen enthalten.
— Jeder kommutative Ring $R \neq 0$ besitzt ein maximales Ideal.
— Sei R ein kommutativ, $A \subset R$ ein Ideal. A ist genau dann maximal, wenn R/A ein Körper ist.

Primideale

Sei R ein kommutativer Ring. Ein Ideal $P \subset R$ heißt Primideal, wenn $P \neq R$ und wenn für alle $r, s \in R$ gilt: ist $rs \in P$, dann ist $r \in P$ oder $s \in P$.
Äquivalent dazu:

— $R \backslash P$ ist multiplikativ abgeschlossen.
— R/P ist Integritätsbereich.

In einem kommutativen Ring ist jedes maximale Ideal auch Primideal.

Irreduzible Elemente, Primelemente

Sei R ein kommutativer Ring, $r, s \in R$.

Teiler: $r \big| s$, wenn $\exists t \in R$ mit $s = rt$, genau dann, wenn $(s) \subset (r)$.

Assoziiert: $r \sim s$, wenn $r \big| s$ und $s \big| r$, genau dann, wenn $(s) = (r)$.

Echter Teiler: $r \big| s$, $r \notin R^\times$ und r nicht zu s assoziiert ist, genau dann, wenn $(s) \subsetneq (r) \subsetneq R$.

Irreduzibel: r heißt irreduzibel oder unzerlegbar, wenn $r \notin R^\times \cup \{0\}$ und r keine echten Teiler hat,

Sei R Integritätsring. Ein Element $p \in R$ heißt Primelement, wenn $p \in R \backslash (R^\times \cup \{0\})$ und für alle $r, s \in R \backslash \{0\}$ gilt: falls $p \big| rs$, dann $p \big| r$ oder $p \big| s$, das heißt, wenn $p \neq 0$ und (p) Primideal ist.
Sei R Integritätsring.

— Ist $p \in R$ ein Primelement, $p \big| r_1 \cdots r_n$, dann gibt es $1 \leqslant i \leqslant n$ so daß $p \big| r_i$.
— Jedes Primelement ist irreduzibel.
— Ist R sogar Hauptidealring, dann ist ein Element genau dann Primelement, wenn es irreduzibel ist.
— Die Zerlegung eines Elements in Primelemente ist eindeutig (bis auf Ordnung und Einheiten), falls sie existiert.

Faktorieller Ring: Ein Integritätsring heißt faktoriell, wenn jedes Element $r \in R\backslash(R^\times \cup \{0\})$ Produkt von Primelementen ist.

Äquivalent dazu:

— Jedes Element $r \in R\backslash(R^\times \cup \{0\})$ ist Produkt von irreduziblen Elementen, und je zwei solche Zerlegungen sind äquivalent.

— Es gibt eine Teilmenge $P \subset R\backslash\{0\}$ mit der Eigenschaft, daß es zu jedem Element $r \in R\backslash\{0\}$ eine eindeutig bestimmte Einheit $u_r \in R^\times$ und eine eindeutig bestimmte Familie $(\nu_p(r))_{p\in P}$ von Zahlen in $\mathbb{N}_0$, fast alle Null, gibt, mit $r = u_r \prod_{p\in P} p^{\nu_p(r)}$.

kgV und ggT

Sei R Integritätsring und $r_1, \dots, r_n, v, t \in R\backslash\{0\}$.

kgV v heißt kleinstes gemeinsames Vielfaches von $r_1, \dots, r_n$, wenn:

(a) v ist Vielfaches der r_i, d.h. $r_i \big| v$ für alle $1 \leqslant i \leqslant n$

(b) v teilt alle anderen Vielfachen der r_i, d.h. für alle $s \in R\backslash\{0\}$ mit $r_i \big| s$ für alle $1 \leqslant i \leqslant n$ folgt $v \big| s$.

ggT t heißt größter gemeinsamer Teiler der $r_1, \dots, r_n$, wenn:

(a) t ist Teiler der r_i, d.h. $t \big| r_i$ für alle $1 \leqslant i \leqslant n$,

(b) t wird von allen anderen Teilern der r_i geteilt, d.h. falls $s \big| r_i$ für alle $1 \leqslant i \leqslant n$, dann $s \big| t$.

Teilerfremd $r_1, \dots, r_n$ heißen teilerfremd bzw. relativ prim, wenn 1 ein ggT von ihnen ist.

Sei R ein Integritätsring, $r_1, \dots, r_n, v, t \in R\backslash\{0\}$.

(a) v ist genau dann ein kgV von $r_1, \dots, r_n$, wenn $(v) = \bigcap_{i=1}^n (r_i)$.

(b) Gilt $(t) = \sum_{i=1}^n (r_i) = (r_1, \dots, r_n)$, dann ist t ein ggT von $r_1, \dots, r_n$.
Ist R Hauptidealring, gilt die Umkehrung: t ist genau dann ein ggT von $r_1, \dots, r_n$, wenn $(t) = (r_1, \dots, r_n)$.

Bekannte historische Resultate:

Lemma von Bezout Sei R Hauptidealring. $r_1, \dots, r_n$ sind genau dann teilerfremd, wenn es $s_1, \dots, s_n \in R$ gibt, mit $\sum_{i=1}^n s_i r_i = 1$.

Lemma von Euklid Sei R faktoriell, $r, s, t \in R\backslash\{0\}$. Gilt $r \big| st$ und sind r und s teilerfremd, dann gilt $r \big| t$.

euklidischer Algorithmus Seien $r, s \in R\backslash\{0\}$. Dann gibt es $n \in \mathbb{N}_0$, und Folgen

$$r_{-1} = r, r_0 = s, r_1, \dots, r_n \in R\backslash\{0\} \quad \text{und} \quad q_1, \dots q_{n+1} \in R$$

mit

$$\begin{aligned}
r &= q_1 s + r_1, \quad \delta(r_1) < \delta(s) \\
s &= q_2 r_1 + r_2, \quad \delta(r_2) < \delta(r_1) \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \quad \delta(r_n) < \delta(r_{n-1}) \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Für $0 \neq c \in R$ gilt

$$c \big| r, s \Leftrightarrow c \big| s, r_1 \Leftrightarrow c \big| r_1, r_2 \Leftrightarrow \cdots \Leftrightarrow c \big| r_{n-2}, r_{n-1} \Leftrightarrow c \big| r_n.$$

Durch rekursives Einsetzen im Euklidischen Algorithmus erhält man $a, b \in R$ mit $r_n = ra + sb$.

Faktorielle Polynomringe

Sei R ein faktorieller Ring und $K = \mathrm{Frac}(R)$.

— $R[X]$ und $R[X_1, X_2, \ldots, X_n]$ sind faktoriell.

— Ist $A \subset R$ ein Ideal, so ist

$$R[X]/AR[X] \to (R/A)[X], f + AR[X] \mapsto \overline{f}$$

ein R-Algebrenisomorphismus.

— $A \subset R$ ist Primideal $\Leftrightarrow$ $AR[X] \subset R[X]$ ist Primideal. $p \in R$ ist ein Primelement in R, genau dann, wenn es Primelement in $R[X]$ ist.

— $f \in R[X]$ heißt primitiv, wenn die Koeffizienten teilerfremd sind. Sind $f, g \in R[X]$ primitiv, so auch fg.

— Die Primelemente in $R[X]$ sind die Primelemente in R und die primitiven irreduziblen Polynome.

— In K: Für $0 \neq f \in K[X]$ gibt es x in K und $\widetilde{f} \in R[X]$ primitiv mit $f = x\widetilde{f}$ (eindeutig bis auf Einheiten in R). $\Rightarrow$ für Irreduziblität genügt es in $R[X]$ zu arbeiten.
Sei $f \in R[X] \backslash R$.

(a) Ist f nicht Produkt von nichtkonstanten Polynomen in $R[X]$, dann ist f in $K[X]$ irreduzibel.

(b) Ist f in $R[X]$ irreduzibel, dann ist f auch in $K[X]$ irreduzibel.

(c) Ist f primitiv und irreduzibel in $K[X]$, dann ist f irreduzibel in $R[X]$.

(d) Sind $f, g \in R[X]$, sei f primitiv. Gilt $f \big| g$ in $K[X]$, dann gilt $f \big| g$ auch in $R[X]$.

(e) Ist $f \in R[X]$ normiert, und und $g, h \in K[X]$ normiert mit $f = gh$, dann gilt $g, h \in R[X]$.

Irreduzibilitätskriterien

R Integritätsring.

Homomorphismus SeiR' ein weiterer Integritätsring, $f \in R[X] \backslash R$ primitiv, $\varphi : R[X] \to R'$, der nichtkonstante Faktoren von f auf Nichteinheiten abbildet. Ist $\varphi(f)$ irreduzibel, dann ist auch f irreduzibel. (Sehr allgemein, selten so verwendet.)

Automorphismus Sei $\varphi : R[X] \to R[X]$ ein Automorphismus, $f \in R[X] \backslash R$ primitiv. Ist $\varphi(f)$ irreduzibel, dann ist auch f irreduzibel. (Hilfreich, wenn man “den Trick sieht”.)

Reduktionskriterium Seien $\mathfrak{P} \subset R$ ein Primideal, $\pi : R \to R/\mathfrak{P}$ der kanonische Homomorphismus, sei $f = \sum_{i=0}^n r_i X^i \in R[X] \backslash R$ primitiv mit $r_n \notin \mathfrak{P}$. Ist ${}^{\pi}f \in (R/\mathfrak{P})[X]$ irreduzibel, dann ist auch f irreduzibel. (Sehr nützlich.)

Eisensteinkriterium Sei $0 \neq f = \sum_{i=0}^n r_i X^i \in R[X]$ primitiv, $p \in R$ ein Primelement mit $p \nmid r_n$ aber $p \big| r_j$ für alle $0 \leqslant j \leqslant n-1$, und $p^2 \nmid r_0$. Dann ist f in $R[X]$ irreduzibel.

Chinesischer Restsatz

Allgemeine Version:
Seien $A_1, \ldots, A_n$ paarweise fremde Ideale von R.

(a) Die Abbildung

$$\begin{array}{rcl} R/A_1 \cdots A_n & \to & \prod_{i=1}^n R/A_i \\ r + A_1 \cdots A_n & \mapsto & (r + A_1, \ldots, r + A_n) \end{array}$$

ist ein R-Algebrenisomorphismus.

(b) Die Abbildung

$$\begin{array}{rcl} (R/A_1 \cdots A_n)^* & \to & \prod_{i=1}^n (R/A_i)^* \\ r + A_1 \cdots A_n & \mapsto & (r + A_1, \ldots, r + A_n) \end{array}$$

ist ein Gruppenisomorphismus.

Bekanntere Version: R Hauptidealring (z.B. $R = \mathbb{Z}$)
Seien $a_1, \dots, a_n \in R \backslash \{0\}$ paarweise teilerfremd.

(a) Die Abbildung

$$\begin{array}{rcl} R/(a_1 \cdots a_n) & \to & \prod_{i=1}^{n} R/(a_i) \\ r + (a_1 \cdots a_n) & \mapsto & (r + (a_1), \dots, r + (a_n)) \end{array}$$

ist ein R-Algebrenisomorphismus.

(b) Die Abbildung

$$\begin{array}{rcl} (R/(a_1 \cdots a_n))^* & \to & \prod_{i=1}^{n} (R/(a_i))^* \\ r + (a_1 \cdots a_n) & \mapsto & (r + (a_1), \dots, r + (a_n)) \end{array}$$

ist ein Gruppenisomorphismus.

Zu $b_1, \dots, b_n \in R$ gibt es also $r \in R$ mit $r \equiv b_i \mod a_i$ für $1 \leqslant i \leqslant n$, und r ist modulo $a_1 \cdots a_n$ eindeutig bestimmt.

Beispiele

Beispiele: Ringe

(a) $\mathbb{Z}$, $\mathbb{Z} / \mathbb{Z}\, a$ für $a \in \mathbb{Z}$ sind kommutative Ringe. $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. $\mathbb{Q}$ ist Unterring von $\mathbb{R}$, $\mathbb{C}$.

(b) Sei $d \in \mathbb{Z} \backslash \{0, 1\}$.

$$R = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

ist Unterring von $\mathbb{C}$, sogar Körper.

$$S = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

ist Unterring von R.

(c) Sei R ein Ring, $n \in \mathbb{N}$. Die Menge $R^{n \times n}$ der (n, n)-Matrizen mit Koeffizienten in R ist Ring bezüglich der üblichen Addition und Multiplikation von Matrizen. $(R^{n,n})^\times = \mathbf{GL}_n(R)$ ist die Gruppe der invertierbaren Matrizen in $R^{n \times n}$.

(d) Sei R Ring. Dann ist das Zentrum

$$Z(R) = \{r \in R \mid \forall s \in R : rs = sr\}$$

ein kommutativer Unterring von R

(e) Sei R ein kommutativer Ring, $n \in \mathbb{N}$. Dann ist $R^{n,n}$ eine R-Algebra bezüglich

$$\varphi : R \to R^{n,n}, r \mapsto \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & r & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & r \end{pmatrix}.$$

Die Skalarmultiplikation dazu ist $r.(r_{ij}) = (rr_{ij})$.

(f) Sei R ein Ring. Dann ist

$$\varphi : \mathbb{Z} \to R, z \mapsto z.1$$

ein Ringhomomorphismus mit $\mathrm{im}(\varphi) \subset Z(R)$. Also ist R eine $\mathbb{Z}$-Algebra. Die Skalarmultiplikation dazu ist die von den abelschen Gruppen her bekannte.

Beispiele: Ideale

(a) In einem Ring R sind $\{0\}$ und R selbst stets Ideale.

(b) Sei R ein Ring, A (Links-/Rechts-)Ideal mit $R^\times \cap A \neq \emptyset$. Dann gilt $A = R$. Für Linksideal sieht man das wie folgt: Sei $a \in R^\times \cap A$. Dann gibt es $a' \in R$ so daß $a'a = 1$. Damit gilt für alle $r \in R$: $r = ra'a \in A$.

(c) Sei R kommutativer Ring. R ist genau dann Körper, wenn $1 \neq 0$ und $\{0\}$ und R die einzigen Ideale von R sind.

(d) Die Ideale von $\mathbb{Z}$ sind genau die Untergruppen $\mathbb{Z}\,a$, für $a \in \mathbb{Z}$.

Beispiele: Integritätsringe

(a) $\mathbb{Z}$ ist ein Integritätsbereich, Körper sind Integritätsbereiche.

(b) Unterringe von Integritätsringen sind Integritätsringe. Insbesondere sind Unterringe von Körpern Integritätsringe.

(c) Sei $n \in \mathbb{N}_0$. $\mathbb{Z}\,/n\,\mathbb{Z}$ ist genau dann Integritätsbereich, wenn $n = 0$ oder n Primzahl ist.

(d) Ist R ein Integritätsbereich, so ist auch $R[X_1, \ldots X_n]$ ein Integritätsbereich.

Beispiele: Euklidische Ringe

(a) $\mathbb{Z}$ ist euklidisch bezüglich $\delta : \mathbb{Z} \to \mathbb{N}_0$, $z \mapsto |z|$.

(b) Sei K ein Körper. $K[X]$ ist euklidisch bezüglich $K[X]\backslash\{0\} \to \mathbb{N}_0$, $f \mapsto \deg(f)$.

(c) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} = \mathbb{Z} \oplus \mathbb{Z}\,i$ ist Unterring von $\mathbb{C}$, der $\mathbb{Z}$ enthält; er heißt Ring der ganzen Gaußschen Zahlen. $\delta : \mathbb{Z}[i] \to \mathbb{N}_0$, $x = a + bi \mapsto x\overline{x} = a^2 + b^2$ ist euklidische Norm.

Beispiele: Hauptidealringe

(a) $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$ für einen Körper K sind Hauptidealringe, sogar euklidische Ringe.

(b) $\mathbb{Z}[X]$ und $K[X, Y]$ sind **keine** Hauptidealringe, also auch nicht euklidisch.

Beispiele: Quotientenringe

(a) Ist R Integritätsring, dann ist S=$R\backslash\{0\}$ multiplikativ abgeschlossen. Dann ist $\mathrm{Frac}(R) := R_S$ ein Körper (Quotientenkörper.
— $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$
— K ein Körper: $K(X_1, \ldots, X_n) = \mathrm{Frac}(K[X_1, \ldots, X_n])$, Körper der rationalen Funtionen
— $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i] = \big\{a + bi \in \mathbb{C} \bigm| a, b \in \mathbb{Q}\big\}$, es genügt $S = \mathbb{Z}\setminus\{0\}$ zu invertieren.

(b) $s \in R$. $S = \{s^n \mid n \in \mathbb{N}_0\}$ ist genau dann multiplikativ abgschlossen, wenn $s^n \neq 0$ für alle $n \in \mathbb{N}$ ist, das heißt, wenn s nicht nilpotent ist. Dies ist in einem Integritätsring für alle $s \neq 0$ erfüllt.

$$R_S = \{\frac{r}{s^k} \mid r \in R\}.$$

(c) Sei $p \in \mathbb{N}$ Primzahl. Dann ist $\mathbb{Z}\setminus(p)$ multiplikativ abgeschlossene Teilmenge von $\mathbb{Z}$.

$$\mathbb{Z}_S =: \mathbb{Z}_{(p)} = \left\{\frac{r}{s} \mid r \in R, s \in S\right\} = \left\{\frac{r}{s} \mid r, s \in R, p \nmid s\right\}.$$

Ideale: $B = \mathbb{Z}_{(p)} \cdot A$, wobei $A \subset \mathbb{Z}$ Ideal mit $A \cap \{\mathbb{Z}\setminus(p)\} = \emptyset$, also $A \subset (p)$.
In $\mathbb{Z}_{(p)}$ ist (p) maximal bezüglich Inkusion (das einzige Ideal mit dieser Eigenschaft). Ein solcher Ring heißt lokal, $\mathbb{Z}_{(p)}$ heißt Lokalisierung von $\mathbb{Z}$ bei (p).

Beispiele: Maximale Ideale und Primideale

(a) Die maximalen Ideale von $\mathbb{Z}$ sind die Ideale (p), wobei p eine Primzahl ist. (Denn für $n \in \mathbb{N}_0$ gilt: (n) maximal genau dann, wenn $\mathbb{Z}/(n)$ Körper, genau dann, wenn n Primzahl.)

(b) Sei K Körper, dann ist $(X) = K[X]X$ maximales Ideal. (Denn $K[X]/X \to K, f + (X) \mapsto f(0) =$ konstanter Koeffizient von f ist Ringisomorphismus.)

(c) Die Primideal von $\mathbb{Z}$ sind (0) und die Ideale (p), p eine Primzahl. Das Ideal (0) ist nicht maximal.

(d) Sei R kommutativer Ring. Das Ideal (0) ist genau dann Primideal, bzw. maximales Ideal, wenn R Integritätsring, bzw. Körper, ist.

(e) Sei R Integritätsring. Dann ist $(X) = R[X]X$ Primideal in $R[X]$. (Denn $R[X]/X \to R, f + (X) \mapsto f(0)$ ist Ringisomorphismus.)

Beispiele: Irreduzible Elemente

(a) Sei K ein Körper, R der Unterring von $K[X]$ bestehend aus den Polynomen $f = \sum_{i=0}^{n} a_i X^i$, mit $a_1 = 0$. Es gilt $R = K[X^2, X^3]$. Außerdem gilt $R^\times = K^\times$. Die Elemente X^2 und X^3 sind in R irreduzibel: Sei $X^2 = fg$ mit $f, g \in R$, dann gilt $\deg(f), \deg(g) \in \{0, 2\}$, also $f \in R^\times$ oder $g \in R^\times$. Ebenso für X^3.
Die Elemente X^2 und X^3 sind in R nicht prim: Es gilt $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$, und $X^2 \nmid X^3$ bzw. $X^3 \nmid X^2$. Also hat man zwei nicht-äquivalente Zerlegungen von X^6 in irreduzible Elemente gefunden.

Beispiele: Faktorielle Ringe

(a) Jeder Hauptidealring R ist faktoriell.

(b) $\mathbb{Z}$ ist faktoriell, mit $\mathbb{Z}^\times = \{-1, +1\}$, $P = \{p \in \mathbb{N} \mid p \text{ prim}\}$ ist Transversale der Primelemente von $\mathbb{Z}$ „modulo Einheiten". P ist unendlich.

(c) Sei K Körper. Dann ist $K[X]$ faktoriell mit $K[X]^\times = K^\times$, $P = \{f \in K[X] \mid f \text{ normiert und irreduzibel }\}$ ist eine Transversale der Primelemente „modulo Einheiten". P ist unendlich.

(d) Ist R faktoriell, so auch $R[X]$.

Beispiele: Irreduzibilität

(a) R faktoriell, $K = \operatorname{Frac} R$. Ein Polynom $f \in R[X]$, das reduzibel in $R[X]$ ist, aber irreduzibel in $K[X]$:
Sei $p \in R$ prim $r \in R$ beliebig, dann ist $f = pX - rp = p(X - r)$ nicht irreduzibel in $R[X]$ (insbesondere nicht primitiv), aber irreduzibel in $K[X]$, denn p ist invertierbar in K.

(b) Sei R ein Integritätsring. Ein normiertes Polynom $f \in R[X]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es in R keine Nullstellen hat (Denn f ist genau dann reduzibel, wenn es einen Faktor $X - a$ mit $a \in R$ hat.) Dies ist nur der Fall für **normierte** Polynome. Gegenbeispiel: $6X^2 + 11X + 3 = (2X + 3)(3X + 1)$ ist reduziebel in $\mathbb{Z}[X]$ hat aber keine Nullstelle in $\mathbb{Z}$, nur in $\mathbb{Q}$.

(c) Sei R faktoriell, $K = \operatorname{Frac}(R)$. Seien $a \in R$, $p \in R$ Primelement mit $p \big| a$, $p^2 \nmid a$, $n \in \mathbb{N}$. Dann ist $f = X^n - a$ irreduzibel in $R[X]$ nach Eisenstein, damit auch in $K[X]$.

(d) Sei K Körper, $n \in \mathbb{N}$. $f = X^n - Y \in K[X, Y] = K[X][Y]$ ist trivialerweise irreduzibel, oder $f \in K[Y][X]$ ist irreduzibel nach (c), denn Y ist Primelement in $K[Y]$.

(e) Sei K Körper, $\operatorname{char}(K) \neq 2$. $f = X^2 + Y^2$ ist irreduzibel, da f als Polynom in $K[Y]$ keine Nullstelle hat. $g = X^2 + Y^3 + Z^n \in K[X, Y, Z] = K[X, Y][Z]$ ist irreduzibel nach (c).