Teilbarkeit

Sei $n \in \mathbb{N}$. $d \in \mathbb{N}$ ist Teiler von n, falls $\exists t \in \mathbb{N} : d \cdot t = n$. Man schreibt $d \mid n$. n ist Vielfaches von d.

Die Menge aller Teiler ist endlich da $\forall d \mid n : d \leq n$.

Der *größte gemeinsame Teiler* von m und n wird notiert als $ggT(m,n)$ oder (m,n).

Das *kleinste gemeinsame Vielfache* ist $kgV(m,n)$.

Zahlen $m,n \in \mathbb{N}$ heißen *teilerfremd*, wenn $1 \in \mathbb{N}$ der einzige gemeinsame Teiler ist.

ggT als Linearkombination

Für $m,n \in \mathbb{Z}$ ex. $c,d \in \mathbb{Z}$ s.d. $mc + nd = ggT(m,n)$

Division mit Rest

$\forall k \in \mathbb{Z}, n \in \mathbb{N} \exists! d \in \mathbb{Z}, r \in \{0,\cdots,n-1\} : k = dn + r$.
r ist Rest der Division von k durch n.

Primzahlen

Eine *Primzahl* ist ein $1 < n \in \mathbb{N}$ welches keinen natürlichen Teiler außer 1 und p hat.
$\mathbb{P} = \{n \in \mathbb{N} | n > 1, \forall d,t < n : d \cdot t \neq n\}$

Fundamentalsatz der Arithmetik

Jedes $n \in \mathbb{N}$ lässt sich eindeutig als sortiertes Produkt von Primzahlen schreiben.

p-adische Bewertung

Sei $p \in \mathbb{P}$. Dann:
$\forall 0 \neq k \in \mathbb{Z} \exists! v_p(k) \in \mathbb{N}_0 : p^{v_p(k)} \mid k \wedge p^{v_p(k)+1} \nmid k$
Insb.: $k = \pm \prod_{p \in \mathbb{P}} p^{v_p(k)}$

$$\forall k,l \in \mathbb{Z} : v_p(k+l) \geq \min\{v_p(k), v_p(l)\}$$
$$v_p(k \cdot l) = v_p(k) + v_p(l)$$

Weiterhin gilt für $a,b \in \mathbb{N}$:
$b \mid a \iff \forall p \in \mathbb{P} : v_p(b) \leq v_p(a)$
$ggT(a,b) = \prod_{p \in \mathbb{P}} p^{e_p}$ mit $e_p = \min\{v_p(a), v_p(b)\}$
$kgV(a,b) = \prod_{p \in \mathbb{P}} p^{f_p}$ mit $f_p = \max\{v_p(a), v_p(b)\}$

Kleiner Satz von Fermat

Sei $p \in \mathbb{P}, c \in \mathbb{Z}$. Dann gilt $p \mid c^p - c$.

Primzahlverteilung

Sei $k \in \mathbb{N}$. Dann ex. $M \in \mathbb{N}$ s.d. zwischen M und $M+k$ keine Primzahl liegt.

$\forall \epsilon > 0 \exists x_0 \in \mathbb{R} \forall x \geq x_0 \exists p \in \mathbb{P} : p \in [x, (1+\epsilon)x]$

Die Funktion $\pi(x) := \#\{p \in \mathbb{P} | p \leq x\}$ zählt die Anzahl der Primzahlen unterhalb $x \in \mathbb{R}$.
Der *Primzahlsatz* besagt: $\lim_{x \to \infty} \pi(x) \cdot \frac{\log x}{x} = 1$.
Der *Dichtheitssatz* besagt: Die Menge aller Brüche p/l mit $p,l \in \mathbb{P}$ liegt dicht in $\mathbb{R}_{\geq 0}$.

Magmen

Ein Magma ist Menge mit Verknüpfung $(M, \star)$ wobei $\star : M \times M \to M$ eine Abbildung ist.

Ein Magma ist *assoziativ* gdw.:
$\forall l,m,n \in M : (l \star m) \star n = l \star (m \star n)$
Ein Magma ist *kommutativ* gdw.:
$\forall m,n \in M : m \star n = n \star m$
Ein assoziatives Magma heißt *Halbgruppe*.
Ein assoziatives Magma mit beiseitigem Neutralelement heißt *Monoid*.

Magmenhomomorphismen

Seien $(M, \star)$, $(N, \circ)$ Magmen.
$\Phi : M \to N$ ist Magmenhomomorphismus, wenn:
$\forall m_1, m_2 \in M : \Phi(m_1 \star m_2) = f(m_1) \circ f(m_2)$

Untermagmen

$U \subseteq M$ ist Untermagma gdw.: $U \star U \subseteq U$.

$\cap_{i \in I} U_i$ ist Untermagma von M.
Für $X \subseteq M$ ist $\langle X \rangle_{\text{Magma}}$ Schnitt aller Untermagmen U von M mit $X \subseteq U$.
$\langle X \rangle_{\text{Magma}}$ heißt Magmenerzeugnis von X in M.

Untermonoide

Ein Untermonoid eines Monoids M, d.h. eines assoziativen Magmas mit Neutralelement, ist ein Untermagma mit beidseitigem Neutralelement.

Symmetrische Gruppen

$\text{Sym}(D) := \{\sigma \in \text{Abb}(D,D) | \sigma \text{ ist bijektiv}\}$
$\text{Sym}(D)$ ist Untermagma von $\text{Abb}(D,D)$.
S_d für $d \in \mathbb{N}$ ist die aus genau d Elementen bestehende symmetrische Gruppe.

Gruppen

Eine Gruppe ist ein assoziatives Magma $(M, \star)$ mit beidseitig neutralem Element e und mindestens einer Inversen bzgl. $\star$ für $\forall m \in M$.
Eine Gruppe heißt *kommutativ* bzw. *abelsch* wenn sie als Magma kommutativ ist.

Untergruppen

Eine Untergruppe ist ein Untermagma $\emptyset \neq U \leq G$ welches unter Inversenbildung abgeschlossen ist.
$U \neq \emptyset \implies x \in U \implies x^{-1} \in U \implies e_G \in U$
$U \leq G \iff \emptyset \neq U \subseteq G \wedge \forall x,y \in U : xy^{-1} \in U$
Schnitt von Untergruppen ist selbst Untergruppe.

Gruppenerzeugnis

Der Schnitt aller ein $M \subset G$ beinhalten Untergruppen wird geschrieben als $\langle M \rangle$ und bezeichnet als (Gruppen-)Erzeugnis von M.
$\langle M \rangle = \{x_1 \cdots x_k | k \in \mathbb{N}_0, \forall i \leq k : x_i \in M \vee x_i^{-1} \in M\}$

Zyklische Gruppen

Gruppe G ist *zyklisch*, wenn $\exists a \in G : G = \langle a \rangle$.
$\forall n \in \mathbb{N} : [1]$ erzeugt $\mathbb{Z}/n\mathbb{Z}$.
$\langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ ist von g erzeugte zyklische Grp.

Ordnung

Die Ordnung einer Gruppe ist ihre Kardinalität.
Die Ordnung eines $g \in G$ ist die Ordnung der von g erzeugten Untergruppe.
Hat $\langle g \rangle$ endliche Ordnung so $\exists k \in \mathbb{N} : g^k = e_G$.

Satz von Lagrange

Sei G endliche Gruppe und $H \leq G$. Dann ist die Ordnung von H ein Teiler der Ordnung von G.

Index

Sei $g_1 \sim g_2 := g_1 g_2^{-1} \in H$ Äquivalenzrel. auf G.
Die Äquivalenzklasse von $g \in G$ ist definiert als: $[g] = Hg := \{hg | h \in H\}$.
Für Gruppen $H \leq G$ heißt die Anzahl der Äquivalenzklassen bzgl. $\sim$ Index von H in G, geschrieben als $(G : H)$.
Entsprechend gilt für endl. Grp.: $\#G = \#H \cdot (G : H)$.

Primzahlordnung einer Gruppe

In jeder endlichen Gruppe ist Ordnung jedes Elements ein Teiler der Gruppenordnung. Daraus folgt, dass jede Gruppe mit Primzahlordnung eine zyklische Gruppe ist. $G = \langle g \rangle \iff g \neq e_G$

Normalteiler

Eine $N \leq G$ ist Normalteiler, falls $\forall n \in N, g \in G : gng^{-1} \in N$ gilt. d.h. N ist invariant unter allen inneren Automorphismen.
Es gilt für Normalteiler N: $\forall g \in G : gN = Ng$
Ist $U \leq G$ ein Normalteiler, so schreibt man $U \triangleleft G$.
Untergruppen abelscher Gruppen sind normal.

Einfachheit

Die nichttriviale Gruppe G heißt *einfach*, wenn sie keine Normalteiler außer G und $\{e_G\}$ besitzt.

Übersicht Gruppeneigenschaften

Primzahlordnung $\implies$ zyklisch und einfach
zyklisch $\implies$ abelsch
einfach und abelsch $\implies$ Primzahlordnung

Nebenklassen

Seien $U \leq G$ Gruppen. Dann sind $g,h \in G$ *kongruent modulo* U, wenn $g^{-1}h \in U$. Diese Relation bildet Äquivalenzklassen $gU = \{gu | u \in U\}$.
Diese Äquivalenzklassen heißen *Linksnebenklassen* nach U, die Menge aller Nebenklassen heißt *Faktorraum* G/U.
$\pi_U : G \to G/U, g \mapsto gU$ ist kanonische Projektion.

Faktorgruppen

Sei $N \triangleleft G$. $(gN) \cdot (hN) := ghN$ definiert auf G/N eine wohldefinierte Verknüpfung. G/N ist mit dieser Verknüpfung die *Faktorgruppe von G modulo N*.
Die kanonische Projektion π_N ist Gruppenhomomorphismus mit Kern N. Jeder Normalteiler kann also als Kern eines Gruppenhomomorphismus realisiert werden.

Gruppenhomomorphismen

Seien $(G, \star)$, $(H, \circ)$ Gruppen.
$f : G \to H$ ist Gruppenhomomorphismus, wenn:

(a) $\forall x,y \in G : f(x \star y) = f(x) \circ f(y)$
(b) $f(e_G) = e_H$
(c) $\forall x \in G : f(x^{-1}) = f(x)^{-1}$

Ist $f : G \to H$ ein Magmenhomomorphismus gilt:

(a) f ist Gruppenhomomorphismus
(b) $f^{-1}(\{e_H\}) \leq G$
(c) $f(G) \leq H$
(d) f ist injektiv $\iff f^{-1}(\{e_H\}) = \{e_G\}$

Kern

Sei $f : G \to H$ Gruppenhomomorphismus.
Dann heißt $f^{-1}(\{e_H\}) \leq G$ Kern von f.

Konjugation

Sei G Gruppe, $g \in G$ fest gewählt.
$\kappa_g : G \to G, x \mapsto gxg^{-1}$ heißt *Konjugation* und ist Gruppenautomorphismus. $x,y \in G$ heißen *zueinander konjugiert*, wenn $\exists g \in G : y = gxg^{-1}$.

Freie Gruppe

Sei S eine Menge. F ist eine *freie Gruppe über* S mit Abbildung $f : S \to F$ wenn für beliebige Gruppen G, Abbildungen $\varphi : S \to G$ genau ein Gruppenhomomorphismus $\Phi : F \to G$ existiert, für den $\forall s \in S : \varphi(s) = \Phi(f(s))$ gilt.

Gruppenoperationen

Sei $(G,*)$ Gruppe, M Menge.
$\circ : G \times M \to M$ ist Gruppenoperation, wenn:

(a) $\forall m \in M : e_G \circ m = m$

(b) $\forall m \in M, g_1, g_2 \in G : g_1 \circ (g_2 \circ m) = (g_1 * g_2) \circ m$

Es gilt: $\forall \Phi \in Hom(G, Sym(M)) : g \circ m := \Phi(g)(m)$ ist Operation von G auf M.
Für jede Operation $\circ$ von G auf M ex. ein $\Phi \in Hom(G,M)$ s.d. $\circ$ so konstruiert werden kann.

Bahnen

Auf M definiert $m_1 \sim m_2 := \exists g \in G : m_1 = g \circ m_2$ eine Äquivalenzrelation.
Ihre Äquivalenzklassen werden *Bahnen* oder *Orbiten* genannt. d.h. $G \circ m = \{g \circ m | g \in G\}$ ist Bahn.

Transitivität

Operation mit genau einer Bahn heißt *transitiv*. d.h. $\exists m_0 \in M \forall m \in M \exists g \in G : m = g \circ m_0$.

Stabilisator

$Stab_G(m) := \{g \in G | g \circ m = m\}$ ist Stab. von m in G.
Fixpunkt von G auf M ist $m \in M$: $Stab_G(m) = G$.

Bahnbilanzformel

Sei G auf endlichem M operierende Gruppe und $R \subseteq M$ ein Vertretersystem der Bahnen. Dann:
$\#M = \sum_{r \in R} (G : Stab_G(r))$

Sylowsätze

Eine endliche Gruppe G heißt *p-Gruppe* wenn ihre Kardinalität eine Potenz von $p \in \mathbb{P}$ ist.
Eine $U \leq G$ heißt *p-Sylowgruppe* wenn ihre Kardinalität gleich der maximalen, die Ordnung von G teilenden, p-Potenz ist.
Der Satz von Lagrange liefert so die Maximalität einer p-Sylowgruppe unter den p-Untergruppen.

Erster Sylowsatz

Sei G endliche Gruppe, $p \in \mathbb{P}$.
Dann $\exists U \leq G : U$ ist p-Sylowgruppe.

Zweiter Sylowsatz

Sei G endliche Gruppe, $p \in Primes$, $\#G = p^e \cdot f$:

(a) Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

(b) Je zwei p-Sylowgruppen sind konjugiert.

(c) Die Anzahl der p-Sylowgruppen teilt f.

(d) Die Anzahl der p-Sylowgruppen lässt bei Division durch p Rest 1.

Ringe

Ein *Ring* ist Menge R mit Verknüpfungen + und $*$ s.d. $(R,+)$ abelsche Gruppe mit Neutralelement 0 ist, $*$ assoziativ ist, neutrales Element 1 besitzt und die Distributivgesetze gelten:
$\forall a,b,c,d \in R : (a+b)*c = ac+bc \wedge a*(c+d) = ac+ad$
Ist $*$ kommutativ, heißt R kommutativer Ring.

Ringhomomorphismen

$\Phi : R \to S$ ist *Ringhomomorphismus* zwischen Ringen R und S, wenn es bzgl. + und $*$ ein Magmenhomomorphismus ist und $\Phi(1_R) = 1_S$ gilt.

Einheitengruppe

$R^\times := \{r \in R : \exists r^{-1} \in R : rr^{-1} = r^{-1}r = 1_R\}$
$(R^\times, *)$ ist Einheitengruppe.

Teilringe

Ein *Teilring* von Ring R ist $T \subseteq R$ s.d. T bzgl. + Untergruppe und bzgl. $*$ Untermonoid von R ist.

Nullteiler

$a \in R$ ist *Nullteiler* in Ring R, wenn:
$\exists b \in R, b \neq 0 : ab = 0 \vee ba = 0$
Ist 0 einziger Nullteiler in R, so ist R *nullteilerfrei*.
R heißt *Integritätsbereich*, wenn R kommutativ und nullteilerfrei ist.
Teilringe von Integritätsbereichen sind integer.

Charakteristik

Sei R Ring. Dann $\exists! \Phi \in Hom_{Ring}(\mathbb{Z}, R)$.
Sei $n \in \mathbb{N}_0$ nichtnegativer Erzeuger des Kerns von Φ. Dann heißt n die Charakteristik $char(R)$ von R.
Die Charakteristik eines nullteilerfreien Rings R ist entweder 0 oder Primzahl $p \in \mathbb{P}$.

Ideale

Ein *Ideal* in Ring R ist $I \subseteq R$ s.d. $(I,+) \leq R$ und $\forall x \in I, r \in R : xr \in I \wedge rx \in I$.
Kerne von Ringhomomorphismen sind ideal und Ideale sind Kerne von Ringhomomorphismen.

Körper

Ring R heißt Körper, wenn R kommutativ ist und $0 \neq 1$ sowie $R^\times = R \setminus \{0\}$ gelten. Ein Körper ist insb. ein Integritätsbereich.

Chinesischer Restsatz

Seien $M, N \in \mathbb{N}$ teilerfremd, dann gibt es einen Isomorphismus von Ringen:
$\mathbb{Z}/(MN\mathbb{Z}) \to \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$

Algebraischer Chinesischer Restsatz

Seien R kommutativer Ring, I, J Ideale in R s.d. $I + J = R$. Dann existiert ein Isomorphismus:
$\Phi : R/(I \cap J) \to R/I \times R/J$

Moduln

Sei R Ring. Ein R-Modul ist eine abelsche Gruppe M mit Abbildung $\cdot : R \times M \to M$ s.d.:

$$\begin{aligned}
&\forall r,s \in R, m \in M &&: (r+s) \cdot m &&= r \cdot m + s \cdot m \\
&\forall r \in R, m,n \in M &&: r \cdot (m+n) &&= r \cdot m + r \cdot n \\
&\forall r,s \in R, m \in M &&: (rs) \cdot m &&= r \cdot (s \cdot m) \\
&\forall m \in M &&: 1 \cdot m &&= m
\end{aligned}$$

Diese Bedingungen sind von VRäumen bekannt.

Untermoduln

Sei M ein R-Modul und $U \subseteq M$.
Dann ist U *Untermodul* von M, wenn U additive Untergruppe ist und unter der skalaren Multiplikation $\cdot$ mit Elementen aus R invariant ist:
$U \leq M \wedge \forall r \in R, u \in U : r \cdot u \in U$

Polynomringe

Für kommutativen Ring R ist definiert:

$$R[X] := \left\{ \sum_{i=0}^{d} r_i X^i \,\middle|\, d \in \mathbb{N}_0, r_i \in R \right\}$$

$(R[X], +, *)$ ist kommutativer Ring.
Für $f, g \in R[X]$ gilt:

(a) $deg(f+g) \leq \max(deg(f), deg(g))$

(b) $deg(f*g) \leq deg(f) + deg(g)$

(c) Für nullteilerfreie R gilt in (b) Gleichheit

Ist R nullteilerfrei so ist auch $R[X]$ nullteilerfrei und es gilt $(R[X])^\times = R^\times$.

Polynomdivison

Sei R kommutativer Ring, $f, g \in R[X]$ und $g \neq 0$ mit Einheit als Leitkoeffizient.
Dann $\exists h, r \in R[X] : f = gh + r$ mit $deg(r) < deg(g)$.

Algebren

Eine R-Algebra über Ring R ist Ring $\mathcal{A}$ mit Ringhomomorphismus $\sigma : R \to \mathcal{A}$ s.d. $\forall r \in R, a \in \mathcal{A} : \sigma(r) \cdot a = a \cdot \sigma(r)$ gilt. d.h. $\sigma(r)$ kommutiert mit a.
σ ist *Strukturhomomorphismus* von $\mathcal{A}$.
$\mathcal{A}$ ist ein R-Modul mit Vorschrift $(r,a) \mapsto \sigma(r) \cdot a$.
Die Multiplikation in $\mathcal{A}$ ist bilinear.
Insb. gilt $\forall r,s \in R : \sigma(r)\sigma(s) = \sigma(s)\sigma(r)$

Zentrum

Für Ring A ist das *Zentrum* definiert als:
$Z(A) := \{r \in A | \forall a \in A : ra = ar\}$
$Z(A)$ ist Teilring von A und zugleich größter Teilring R s.d. A durch die Inklusion von R nach A zu einer R-Algebra wird.

Für bel. kommutative Ringe R ist $R[X]$ eine R-Algebra vermöge $\sigma : R \to R[X], r \mapsto r = rX^0$.

Algebrenhomomorphismen

Seien $(A,\sigma), (B,\tau)$ R-Algebren.
Ein Ringhomomorphismus $\Phi : A \to B$ ist zugleich Algebrenhomomorphismus, wenn $\Phi \circ \sigma = \tau$ gilt.

Quotientenkörper

Sei R Integritätsbereich. Dann ex. Körper Q mit Teilring R und Eigenschaften:
Ist K bel. Körper und $\phi : R \to K$ injektiver Ringhomomorphismus, dann lässt sich ϕ zu einem Ringhomomorphismus $\tilde{\phi} : Q \to K$ fortsetzen.
Der Körper Q heißt *Quotientenkörper* von R.

Der Quotientenkörper von $\mathbb{Z}$ ist $\mathbb{Q}$.
Der Quotientenkörper von $K[X]$ ist Körper rationaler Funktionen $K(X) := \{\frac{f}{g} | f, g \in K[X], g \neq 0\}$.

Quadratische Reste

Sei F endlicher Körper mit q Elementen und Charakteristik $p > 2$. Ein $a \in F^\times$ ist *Quadrat* in F, wenn $\exists b \in F : b^2 = a$.
Das Bild von $F^\times \to F^\times, b \mapsto b^2$ ist Quadratmenge.

Legendre-Symbole

Sei $p \geq 3$ Primzahl. Für $a \in \mathbb{Z}$ ist def.:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ 1 & \exists x \in \mathbb{Z} \setminus p\mathbb{Z} : a \equiv x^2 \ (mod\ p) \\ -1 & \text{sonst} \end{cases}$$

$\left(\frac{a}{p}\right)$ ist das *Legendre-Symbol* von a modulo p.

Berechnen von Legendre-Symbolen

Sei $a \in \mathbb{Z}, m, n \in \mathbb{Z} : a = mn, p \in \mathbb{P}$:

$$\left(\frac{a}{p}\right) = \left(\frac{a-p}{p}\right) \qquad \left(\frac{m \cdot n}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Sei $l, p \in \mathbb{P}$ mit $l, p \neq 2$:

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{l-1}{2} \cdot \frac{p-1}{2}}$$
$$\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2} \cdot \frac{p-1}{2}} \left(\frac{l}{p}\right)$$

Teilbarkeit in Ringen

Sei R kommutativer Ring. $a \in R$ ist Teiler von $b \in R$, falls $\exists c \in R : b = c \cdot a$. Kurz $a|b$ bzw. $a|_R b$.
In R ist Faktor c i.A. nicht eindeutig.
Ist R nullteilerfrei und $a \neq 0$, so ist c eindeutig.

Assoziiertheit

$a, b \in R$ sind *assoziiert*, wenn $\exists e \in R^\times : b = a \cdot e$.
$a, b \in \mathbb{Z}$ sind also assoziiert, wenn sie bis auf ihr Vorzeichen übereinstimmen.
Assoziiertheit ist eine Äquivalenzrelation auf R.
Die Äquivalenzklasse von $a \in R$ ist $a \cdot R^\times$.

Ordnungsrelation

Sei R kommutativ und nullteilerfrei. Dann ist $aR^\times \preccurlyeq bR^\times \iff a|b$ eine Ordnungsrelation auf der Menge der Assoziiertenklassen.

ggT in Ringen

$g \in R$ ist *größter gemeinsamer Teiler* von $a, b \in R$, wenn g gemeinsamer Teiler ist und alle gemeinsamen Teiler von a, b auch g teilen.
$a, b \in R$ sind *teilerfremd*, wenn die Einheiten in R die einzigen gemeinsamen Teiler sind.

$ggT(a, e)$ für $a \in R, e \in R^\times$ ist Assoziiertenklasse von 1, also $R^\times$. $ggT(a, 0) = a \cdot R^\times$ da alles 0 teilt.
Ist d ein gemeinsamer Teiler von a, b, dann gilt auch $d|(ax + by)$ für $x, y \in R$.

Hauptidealringe

$\{ax + by | x, y \in R\}$ ist Ideal in R.
$I \subseteq R$ ist *Hauptideal*, wenn $\exists g \in I : I = Rg$.
Menge aller Vielfachen von g in R ist $(g) := Rg$.

Ein nullteilerfreier kommutativer Ring R, in dem jedes Ideal Hauptideal ist, heißt *Hauptidealring*.

Assoziiertenklassen und Ideale

Sei R ein solcher Hauptidealring. Dann:

(a) $g, h \in R$ sind Erzeuger des selben Hauptideals $Rg = Rh \iff g$ und h assoziiert sind.

(b) $\forall \emptyset \neq S \subseteq R \exists m \in S : m$ ist bzgl. Teilbarkeit minimal.

Chinesischer Restsatz für Hauptidealringe

Seien R Hauptidealring, $r, s \in R$ teilerfremd (d.h. $1 = rx + sy$ für geeignete $x, y \in R$). Dann gilt für Ideale $I = Rr, J = Rs$ der Chinesische Restsatz s.d.:

$$R/(Rrs) \cong R/(Rr) \times R/(Rs)$$

$\forall a, b \in R \exists x \in R : x \equiv a \ (mod\ Rr) \wedge x \equiv b \ (mod\ Rs)$

Arithmetik in Hauptidealringen

Sei R kommutativer Ring.
$m \in R$ ist *irreduzibel*, wenn $m \notin R^\times$ und $\forall a, b \in R : m = ab \implies a \in R^\times \vee b \in R^\times$.
$p \in R$ ist *Primelement*, wenn $p \notin R^\times$ und $\forall a, b \in R : p|ab \implies p|a \vee p|b$.

Die Irreduzibilität eines $m \in R$ heißt, dass die Assoziiertenklasse $mR^\times$ in R unter Klassen $\neq R^\times$ bzgl. der Teilbarkeitsordnungsrelation minimal ist. Jeder Teiler von m ist entweder Einheit oder zu m assoziiert.

Sei R nullteilerfreier kommutativer Ring:

(a) Primelement $\neq 0$ in R ist irreduzibel.

(b) R ist Hauptidealring $\implies$ irreduzibles R-Element ist auch prim.

Primzerlegung in Hauptidealringen

Sei R Hauptidealring, $\mathbb{P}_R$ Vertretersystem der Assoziiertenklassen von Primelementen $\neq 0$. Dann:

$\forall r \in R \setminus \{0\} : r$ ist assoziiert zu Produkt endlich vieler Elemente in $\mathbb{P}_R$. (vgl. Fundamentalsatz)
Sind $s, t \in \mathbb{N}_0, p_1, \ldots, p_s, q_1, \ldots, q_t \in \mathbb{P}_R$ s.d. Einheiten $\delta, \epsilon \in R^\times$ ex. mit $r = \delta \cdot p_1 \cdot \cdots \cdot p_s = \epsilon \cdot q_1 \cdot \cdots \cdot q_t$, so gilt $\epsilon = \delta$, $s = t$ und es gilt bis auf Vertauschung der Faktorreihenfolge $\forall 1 \leq i \leq s : p_i = q_i$.

Summen zweier Quadrate

Ein $n \in \mathbb{N}$ ist als Summe zweier Quadrate von Zahlen $\in \mathbb{Z}$ schreibbar $\iff$ Der quadratfreie Anteil von n hat keinen Primteiler, der bei Division durch 4 Rest 3 lässt.

$n \in \mathbb{N}$ ist Summe zweier Quadrate gdw. sie die komplexe Norm von einem $a + bi \in \mathbb{Z}[i] \setminus \{0\}$ ist.

Restklassenkörper

Sei R Hauptidealring aber kein Körper. Der Restklassenring R/Rg ist ein Köper gdw. g irreduzibel ist, da $\forall a \notin Rg : a$ modulo g ist invertierbar.

Für $p \in \mathbb{P}$ ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ Körper mit p Elementen.

Ist p ungerade und $a \in \mathbb{F}_p^\times$ kein Quadrat, dann ist $X^2 - a \in \mathbb{F}_p[X]$ irreduzibel.

$\mathbb{F}_p[X]/(X^2 - a)$ ist Körper mit p^2 Elementen.

Maximale Ideale

Ein Ideal $I \subset R$ ist *maximales Ideal*, wenn $I \neq R$ und zwischen I und R kein weiteres Ideal liegt.
$I \subset R$ ist maximal gdw. R/I ein Körper ist.
Weiter $\forall a \in R \setminus I : (a + I) = R/I$ und ein zu $a + I$ inverses Element existiert.

Primideale

Ein Ideal $I \subset R$ ist *Primideal*, wenn:
$\forall x, y \in R : xy \in I \implies x \in I \vee y \in I$.

Ein Ideal I ist Primideal gdw. R/I integer ist, da dann jedes maximale Ideal auch ein Primideal ist.

In Hauptidealringen ist jedes Primideal ungleich (0) bereits maximal.

Körpererweiterungen

Sei K Körper und L Körper, der K umfasst. $K \subseteq L$ ist dann eine *Körpererweiterung*.

Algebraizität und Transzendenz

Element $\alpha \in L$ heißt *algebraisch* über K, wenn ein Polynom $f \in K[X]$ existiert s.d.: $f \not\equiv 0 \wedge f(\alpha) = 0$.

Element $\alpha \in L$ heißt *transzendent* über K, wenn es nicht algebraisch über K ist.

Körper L ist algebraisch über K, wenn alle Elemente von L über K algebraisch sind.

Sei $\alpha \in L$ algebraisch über K. Das Ideal $I(\alpha) := \{f \in K[X] | f(\alpha) = 0\}$ heißt *Verschwindungsideal* und ist nicht das Nullideal im Polynomring. Normierter Erzeuger von $I(\alpha)$ ist das *Minimalpolynom* von α.

Adjunktion

Der kleinste Teilkörper von L welcher K und geg. $\alpha \in L$ enthält, heißt $K(\alpha)$ d.h. *K adjungiert alpha*.
Für jede Teilmenge $A \subseteq L$ existiert ein kleinster Teilkörper welcher K und A enthält.

Algebraische Erweiterung

Sei $K \subseteq L$ Körpererweiterung. Dann gelten:

(a) $\alpha \in L$ ist algebraisch $\iff$ Dimension von $K(\alpha)$ als K-Vektorraum ist endlich.

(b) Menge aller über K algebraischen $\alpha \in L$ ist Teilkörper von L.

(c) $K \subseteq L$ und $L \subseteq M$ sind algebraische Körpererweiterungen $\implies K \subseteq M$ ist algebraische Körpererweiterung.

Grad der Körpererweiterung

Sei $K \subseteq L$ Körpererweiterung. Die Dimension von L als K-Vektorraum heißt *Grad von L über K*.
Geschrieben $[L : K]$.
$\alpha \in L$ ist algebraisch $\iff [K(\alpha) : K] < \infty$.

Sind $K \subseteq L \subseteq M$ endliche Körpererweiterungen so gilt: $[M : K] = [M : L] \cdot [L : K]$.

Algebraischer Abschluss

Ein Körper K ist *algebraisch abgeschlossen*, wenn er keinen echten algebraischen Erweiterungskörper besitzt. Äquivalent zerfallen alle normierten Polynome in $K[X]$ bereits in Linearfaktoren.

Eisensteinkriterium

Sei R kommutativer nullteilerfreier Ring, $P \subseteq R$ Primideal, $f = \sum_{i=0}^{d} r_i X^i \in R[X]$ nichtkonstantes Polynom mit $\forall i \in \{0, \cdots, d-1\} : r_i \in P$ und $r_d \notin P$ sowie r_0 sei kein Produkt zweier Elemente aus P.

Dann ist f kein Produkt zweier Faktoren in $R[X]$, die kleineren Grad als f haben.

Insb. für $R = \mathbb{Z}$: $X^n - p$ mit $p \in \mathbb{P}$ sind irreduzibel.

Inhalt

Sei R Hauptidealring. Der *Inhalt* $\mathrm{Inh}(f)$ von $f \in R[X]$ mit $f \not\equiv 0$ ist definiert als der Inhalt der Koeffizienten von f, d.h. der Erzeuger des von diesen erzeugten Ideals.

Ein normiertes Polynom in $R[X]$ hat Inhalt 1.

Lemma von Gauß

Sei R Hauptidealring mit Quotientenkörper K und $f, g \in K[X]$. Dann: $\mathrm{Inh}(fg) = \mathrm{Inh}(f) \cdot \mathrm{Inh}(g)$

Irreduzibilitätskriterium

Sei R Hauptidealring mit Quotientenkörper K und $f \in R[X]$ nichtkonstant sowie in $R[X]$ kein Produkt von Faktoren kleineren Grades.
Dann ist f in $K[X]$ irreduzibel.