Stuttgart, SoSe2011

Vorlesung Algebra

§1. Gruppen

1.1 Definition

Eine Gruppe $(G, *)$ ist eine Menge G mit einer Abbildung $* : G \times G \to G$, $(g, h) \mapsto g*h$, so dass gilt:
(1) $*$ ist assoziativ: $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3 \; \forall \; g_1, g_2, g_3 \in G$;
(2) $\exists \; e \in G : g * e = e * g = g \; \forall \; g \in G$;
(3) $\forall \; g \in G \; \exists \; g' : g * g' = g' * g = e$.

Die Abbildung $*$ wird oft als Multiplikation in der Gruppe G bezeichnet. e heißt neutrales Element (oder Einselement), g' heißt das inverse Element zu g und wird mit g^{-1} bezeichnet, $*$ wird of weggelassen: $gh := g * h$.

Seinen $(G, *_1)$ und $(H, *_2)$ Gruppen. Eine Abbildung $\varphi : G \to H$ ist ein Gruppenhomomorphismus, wenn gilt: $\varphi(g *_1 g') = \varphi(g) *_2 \varphi(g')$, $\forall \; g, g' \in G$.

Eine Gruppe $(G, *)$ heißt endlich, wenn die Menge G endlich ist; G heißt abelsch (oder kommutativ), wenn $g * h = h * g \; \forall \; g, h \in G$; heißt zyklisch, wenn $\exists g \in G : \{g^n | n \in \mathbb{Z}\} = G$.

Bemerkung: Das neutrales Element e ist eindeutig bestimmt, und zu g ist das inverse Element g^{-1} eindeutig bestimmt.

Beispiele:

(1) $G = \{e\}$, aber nicht $G = \emptyset$.
(2) $(\mathbb{Z}, +\}$ mit $e = 0$, aber nicht $(\mathbb{Z}, \cdot)$.
(3) Sei X eine Menge. Dann ist $S(X) = \{f : X \to X$ bijektive Abbildung$\}$ eine Gruppe mit Multiplikation $* = \circ$ die Komposition: $f * g = g \circ f : x \mapsto g(f(x))$. Ein spezieller Fall: $X = \{1, 2, \dots, n\}$ und $S(X)$ ist die symmetrische Gruppe (der Permutationen von n Elementen).
(4) Sei k ein Körper und V ein k-Vektorraum. Dann ist $GL(V) := \{f : V \to V$ bijektive lineare Abbildung$\}$ eine Gruppe, die allgemeine lineare Gruppe.

1.2 Definition

Sei $(G, *)$ eine Gruppe. Eine Teilmenge $H \subset G$ ist eine Untergruppe von $(G, *)$, wenn $(H, *)$ eine Gruppe ist. Das wird mit $H < G$ gezeichnet.

Es ist wichtig, dass H dieselbe Verknüpfung hat wie G. $H < G$ bedeutet $h_1 * h_2 \in H \; \forall \; h_1, h_2 \in H, \; e \in H, \; h^{-1} \in H \; \forall \; h \in H$.

Beispiel: $H = (n\mathbb{Z}, +) < G = (\mathbb{Z}, +)$. Ein Element $x \in G$ liegt in H genau dann, wenn $n|x$.

1.3 Definition
Sei $H < G$ und $x \in G$. Die Menge $xH = \{xh|h \in H\}$ heißt Linksnebenklasse von x. Entsprechend heißt $Hx = \{hx|h \in H\}$ Rechtsnebenklasse von x.

Zwei Linksnebenklassen xH und yH sind entweder gleich oder disjunkt. Also ist G eine disjunkte Vereinigung von Linksnebenklassen. Anderes gesagt, $x \sim_H y :\iff xH = yH$ definiert eine Äquivalenzrelation auf G. Im Beispiel $n\mathbb{Z} < \mathbb{Z}$: $x \sim y \iff x \equiv y \pmod n \iff x - y \in n\mathbb{Z}$.

1.4 Definition
Sei G eine Gruppe und H eine Untergruppe. H heißt normale Untergruppe (oder Normalteiler $H \lhd G$) $:\Leftrightarrow gH = Hg\ \forall g \in G \Leftrightarrow gHg^{-1} = H\ \forall g \in G \Leftrightarrow ghg^{-1} \in H\ \forall g \in G, h \in H$.
Hat G ausser $\{e\}$ und G keinen Normalteiler, so heißt G einfach.

1.5 Proposition

(1) Sei $N \lhd G$ ein Normalteiler und $G/N := \{gN|g \in G\}$ die Menge der Linksnebenklassen. Dann ist G/N eine Gruppe mit der Verknüpfung $(g_1N) * (g_2N) := (g_1g_2)N$. G/N heißt Faktorgruppe oder Quotientengruppe.
(2) Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und surjektiv. Sei $H :=\text{Kern}(\varphi) := \{g \in G|\varphi(g) = e_{G'}\}$. Dann gilt $H \lhd G$ (Normalteiler) und $G' \cong G/H$.

Beispiele:

(1) Sei G abelsch. Dann ist jede Untergruppe normal. Zum Beispiel $n\mathbb{Z} \lhd \mathbb{Z}$.
(2) Sei G beliebig und H eine Untergruppe mit je zwei Links- und Rechtsnebenklassen. Zum Beispiel, G endlich und H hat Ordnung $|H| = \frac{|G|}{2}$. Zum Beispiel $G = \Sigma_3$ und $H = \{(1), (123), (132)\}$. Die Gruppe H ist zyklisch.

Zkylische Gruppen sind immer abelsch und kommen häufig vor: sei G beliebig und $g \in G$. Dann ist $H := \{g^n|n \in \mathbb{Z}\}$ eine zyklische Untergruppe von G.

Nicht jede abelsche Gruppe ist zyklisch: zum Beispiel $Z/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Bis auf Isomorphie sind $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}$) alle zyklischen Gruppen.

1.6 Proposition
Sei $G =< g >$ eine zyklische Gruppe. Dann gilt:

(1) $|G| = \text{ord}(g) = n \in \mathbb{N} \cup \{\infty\}$ genau für $n = \min\{k \in \mathbb{N} : g^k = e\}$.
(2) Sei $n \in \mathbb{N}$: Für $s \in \mathbb{Z}$ gilt: $\text{ord}(g^s) = \frac{n}{\text{ggT}(n,s)}$.
(3) Jede Untergruppe $H < G$ ist zyklisch;

(4) Sei $n \in \mathbb{N}$: Für jedes $d|n$ gibt es genau eine Untergruppe H der Ordnung $|H| = d$; dies ist $H =< g^{\frac{n}{d}} >$. Jede Untergruppe ist von dieser Form.

1.7 Definition
Sei $H < G$. Die Anzahl $|G/H|$ der Linksnebenklassen von H in G heißt der Index von H in G und wird mit $[G : H]$ bezeichnet.

1.8 Proposition (Satz von Lagrange)
Sei $H < G$. Dann gilt: $|G| = |H| \cdot [G : H]$, also teilt die Ordnung einer Untergruppe die Ordnung der Gruppe. Inbesondere teilt die Ordnung eines Gruppenelements die Ordnung der Gruppe.

1.9 Proposition (Kleiner Satz von Fermat)
Sei $x \in \mathbb{Z}, p$ Primzahl, $p \nmid x \Rightarrow p \mid x^{p-1} - 1$, das heißt $x^{p-1} \equiv 1 (\mathrm{mod}\ p)$

1.10 Definition
Eine Operation einer Gruppe G auf einer Menge M ist eine Abbildung $G \times M \to M$, $(g, m) \mapsto gm$ (oder $g \cdot m$), für die gilt:

(1) $(g_1g_2)m = g_1(g_2m),\ \forall\ g_1, g_2 \in G, m \in M$;
(2) $em = m,\ \forall\ m \in M$.

Beispiele:

(1) $M = G$, $G \times G \to G$ durch Linksmultiplikation. Jedes Element $g \in G$ definiert eine Bijektion $G \to G$. Daher ist G eine Untergruppe der symmetrischen Gruppen $\Sigma_{|G|}$.
(2) $G = \Sigma_n$ operiert auf der Menge $M = \{1, 2 \ldots, n\}$.
(3) Die allgemeine lineare Gruppe $G = GL(n, \mathbb{C})$ operiert auf $\mathrm{Mat}(n, \mathbb{C})$ durch Konjugation $gm = gmg^{-1}$. In jeder Bahn $Gm = \{gm : g \in G\}$ liegt genau eine Jordansche Normalform.
(4) $G = GL(n, \mathbb{C}) \times GL(m, \mathbb{C})$ operiert auf $\mathrm{Mat}(n \times m, \mathbb{C})$ durch $(g, h)m = gmh^{-1}$.

1.11 Definition
Die Gruppe G operiere auf der Menge M. Für $m \in M$ heißt die Menge $Gm = \{gm : g \in G\}$ die Bahn von m unter der Operation von G. Ist M selbst eine Bahn (d.h. $\forall\ m_1, m_2 \in M$, $\exists\ g \in G$: $gm_1 = m_2$), so heißt die Operation von G transitiv.

Ist $M = G$ und G operiert durch Linksmultiplikation, so heißt die Operation die linksreguläre Permutationsdarstellung.

Ist $M = G$ und G operiert durch Konjugation: $gm = gmg^{-1}$, so heißen die Bahnen Konjugationsklassen (oder Konjugiertenklassen).

Ein $m \in M$ mit $Gm = \{m\}$ (das heißt $gm = m \; \forall \; g \in G$) heißt Fixpunkt. Die Menge der Fixpunkte wird mit M^G bezeichnet.

Für $m \in M$ ist $G_m := \{g \in G : gm = m\}$ der Stabilisator von m (wird auch mit $\mathrm{Stab}_G(m)$ bezeichnet) oder die Isotropiegruppe von m. (Also: m Fixpunkt $\Leftrightarrow G_m = G$).

Die Operation von G auf M heißt treu, wenn die Abbildung $G \to \Sigma_{|M|}$, $g \mapsto \overline{u_g} = (m \mapsto g(m))$ injektiv ist, d.h. wenn $gm = m$ für alle $m \in M$ nur für $g = e$ gilt.

Beispiel: Eine Untergruppe H von G operiert auf G durch Linksmultiplikation. Die Bahnen sind die Rechtsnebenklassen Hg. Für $H \neq \{e\}$ gibt es keine Fixpunkte, und alle Isotropiegruppen sind trivial.

1.12 Proposition
M sei eine G-Menge (das heißt G operiere auf M). Sei $m \in M$. Dann gibt es eine Bijektion $p : G/G_m \to Gm$ von der Menge der Linksnebenklassen von G_m auf die Bahn von m. Also gilt $|Gm| = [G : G_m]$.

Ist $M = G$ und operiert G durch Konjugation auf sich selbst, so gilt:

$$|G| = |Z(G)| + \sum_{g_i} [G : C_G(g_i)]$$

("Klassengleichung"), wobei $Z(G) = \{g \in G : gh = hg, \; \forall \; h \in G\}$, das Zentrum von G, $C_G(g_i) = \{h \in G : hg_i = g_i h\}$, der Zentralisator von g_i, und g_i Vertreter der Konjugationsklassen von G mit $g_i \notin Z(G)$.

Diese Gleichungen sind nützlich, um Strukturen von Gruppen zu bestimmen. Typische Fragen:

(1) $|G| = p$ (p Primzahl) $\Rightarrow G$ abelsch?
(2) $|G| = p^2$ (p Primzahl) $\Rightarrow G$ abelsch?
(3) $|G| = pq$ (p, q Primzhalen) $\Rightarrow G$ abelsch?
(4) $|G| = de$ ($d, e \in \mathbb{N}$) $\Rightarrow \exists \; H < G$: $|H| = d$?

1.13 Proposition
Sei p eine Primzahl und G eine Gruppe mit $|G| = p$ oder $|G| = p^2$. Dann ist G abelsch.

1.14 Definition
Sei G eine endliche Gruppe, p eine Primzahl. G heißt p-Gruppe $:\Leftrightarrow |G| = p^m$ für ein $m \in \mathbb{N}_0$.

Sei $G = p^m q$ mit $(p, q) = 1$. Eine Untergruppe $H < G$ heißt $p-$Sylow-Untergruppe, wenn $|H| = p^m$.

1.15 Theorem (Cauchy)
Sei G eine endliche Gruppe und p eine Primzahl mit $p|\ |G|$. Dann existiert ein $g \in G$ mit $\operatorname{ord}(g) = p$, also $|<g>| = p$.

1.16 Korollar
Sei G eine endliche Gruppe, p eine Primzahl.
G ist eine p-Gruppe $\Leftrightarrow\ \forall\, g \in G\ \exists\, n \in \mathbb{N} : \operatorname{ord}(g) = p^n$.

1.17 Proposition
Sei p eine Primzahl und G eine endliche p-Gruppe.

(1) Falls G auf einer endlichen Menge x operiert, dann gilt: $|X^G| \equiv |X| (\operatorname{mod} p)$.
(2) $G \neq \{e\} \Rightarrow Z(G) \neq \{e\}$.

1.18 Theorem (Sätze von Sylow)
Sei G eine endliche Gruppe, p eine Primzahl $|G| = p^m \cdot q$, wobei $(p, q) = 1$ (teilerfremd). Dann gilt:

(1) $\forall\, k : 1 \leq k \leq m\ \exists\, H < G, |H| = p^k$.
(2) $H < G$, H eine p-Gruppe, S eine $p-$Sylowuntergruppe von G. Dann existiert ein $g \in G$ mit $H \subseteq gSg^{-1}$.
(3) Sei s die Anzahl der p-Sylowuntergruppen von G. Dann gilt $s|q$ und $s \equiv 1 (\operatorname{mod} p)$.

1.19 Korollar
Alle p-Sylowuntergruppen sind zueinander konjugiert.

1.20 Korollar
Seien p, q Primzahlen, $p < q, p \nmid (q-1), |G| = p \cdot q \Rightarrow G \simeq \mathbb{Z}/pq\mathbb{Z}$, also ist G zyklisch und abelsch.

Falls $p \mid (q-1)$, z.B. $p = 2$ und $q = 3$, ist Σ_3 ein Gegenbeispiel.
Falls $p = q$, also $|G| = p^2$, nach 1.13 ist G abelsch, aber nicht eindeutig, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \not\simeq \mathbb{Z}/p^2\mathbb{Z}$.

§2. Ringe

2.1 Definition
Ein <u>Ring</u> $(R, +, \cdot)$ ist eine Menge R mit zwei Abbildungen $+ : R \times R \to R, (r, r') \mapsto r + r'$ ("Addition") und $\cdot : R \times R \to R, (r, r') \mapsto r \cdot r'$ ("Multiplikation"), so dass gilt

(1) $(R, +)$ ist eine abelsche Gruppe (bezeichne das neutrale Element mit 0, und das inverse zu a mit $-a$).

(2) Die Multiplikation ist assoziativ, und distributiv bezüglich $+ : (a+b)\cdot c = a\cdot c + b\cdot c$ und $a\cdot(b+c) = a\cdot b + a\cdot c \;\; \forall\, a,b,c \in R$, und $\exists$ neutrales Element $1 \in R$, d.h. $a \cdot 1 = 1 \cdot a = a, \quad \forall a \in R$.

Wir verlangen $0 \neq 1$.
R heißt <u>kommutativ</u>, wenn $\cdot$ kommutativ ist: $a\cdot b = b \cdot a,\ \forall\, a,b \in R$.

Seien R, S Ringe, Die Abbildung $\varphi : R \to S$ heißt <u>Ringhomomorphismus</u>, wenn φ ein Homomorphismus von Gruppen ist von $(R,+)$ nach $(S,+)$ und wenn gilt $\varphi(1_R) = \varphi(1_S)$ und $\varphi(a\cdot b) = \varphi(a)\varphi(b),\ \forall\, a,b \in R$.

Bemerkungen:

(1) Ohne $0 \neq 1$ wäre $R = \{0\}$ ein Ring.
(2) $0 = 0 + 0$ impliziert $0 \cdot a = a \cdot 0 = 0\ \forall\, a$, z.B. $0 \cdot 1 = 0 \neq 1$.

Beispiele:

(1) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$.
(2) $\mathrm{Mat}(n \times n, \mathbb{Q})$ mit $+$ und $\cdot$, oder $\mathbb{R}$ oder $\mathbb{C}$ oder $\mathbb{Z}$. Der ist nicht kommutativ für $n > 1$.
(3) $\mathbb{Q}[x]$, Polynomring in einer Variablen (oder in vielen).
(4) Sei $U \subset \mathbb{R}^n$ eine offene Teilmenge. Dann ist $R := \{f : U \to \mathbb{R} \text{ stetig}\}$ ein Ring mit Addition und Multiplikation im Bild: $(f+g)(x) := f(x) + g(x)$, $(f \cdot g)(x) := f(x) \cdot g(x)$.
(5) Sei G eine abelsche Gruppe. Dann ist $R :=\mathrm{Hom}_Z(G,G)$ ein Ring (der Gruppenhomomorphismen) mit $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$, $(\varphi \cdot \psi)(g) = \varphi(\psi(g))$ (oder $\psi(\varphi(g))$), $0 : g \mapsto 0$, und $1 : g \mapsto g$.
(6) $R = \{a, b\}$ mit $a + a = b$, $a + b = a = b + a$, $b + b = b$, $a \cdot a = a$, $a \cdot b = b = b \cdot a$ und $b \cdot b = b$ ist ein Ring mit $0 = b$ und $1 = a$. Das ist isomorph zu $(\mathbb{Z}/2\mathbb{Z},+,\cdot)$, entsteht aus $\mathbb{Z}$ durch Übergang zu Quotient.

2.2 Definition
Sei $(R,+,\cdot)$ ein Ring und $I \subset R$ eine Untergruppe von $(R,+)$.

(1) I heißt <u>Linksideal</u> von R, wenn gilt: $\forall\, x \in I, a \in R$ gilt: $ax \in I$.
(2) I heißt <u>Rechtsideal</u> von R, wenn gilt: $\forall\, x \in I, a \in R$ gilt: $xa \in I$.
(3) I heißt (zweiseitiges) <u>Ideal</u>, wenn I Links- und Rechtsideal ist.

Ein zweiseitiges Ideal wird mit $I \lhd R$ bezeichnet.

Beispiele: $I = 0$; $I = R$; $I = n\mathbb{Z} \lhd \mathbb{Z}$.

2.3 Proposition
Sei $I \subsetneqq R$ ein Ideal im Ring R. Dann ist die abelsche Faktorgruppe R/I ein Ring, der <u>Restklassenring</u>, mit Multiplikation $(x + I)(y + I) := xy + I$.

2.4 Definition
Sei R ein Ring, und $R^* := \{x \in R \,|\, x \text{ invertierbar bezüglich } \cdot\} = \{x \in R \,|\, \exists\ y \in R :$

$xy = yx = 1\}$. Die Elemente von R^* heißen Einheiten und R^* heißt die Einheitengruppe von R. Falls $R^* = R - \{0\}$, dann heißt R Schiefkörper (oder Divisionsring). Ein kommutativer Schiefkörper heißt Körper.

Beispiele:

(1) $\mathbb{Z}^* = \{\pm 1\}$.
(2) $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.
(3) $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{m} | m$ teilfremd zu $n\}$, $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - \{0\}$, $(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1}, \bar{5}\}$.
(4) $(k[x])^* = k^*$.

Voraussetzung ab sofort: R kommutativ.

2.5 Proposition
Sei R ein (kommutativer) Ring. Dann sind die folgenden Aussagen äquivalent:

(1) R ist ein Körper.
(2) Außer $\{0\}$ und R hat R keine Ideale.
(3) Für jeden Ring S und jeden Ringhomomorphismus $\varphi : R \to S$ gilt $\mathrm{Ker}(\varphi) = \{0\}$, also φ injektiv.

2.6 Definition
Sei R ein Ring, und $a \in R$. a heißt Nullteiler $:\Leftrightarrow \exists\ b \neq 0 : ab = 0$.
R heißt Integritätsbereich, falls 0 der einzige Nullteiler ist.

Beispiele:

(1) In $\mathbb{Z}/6\mathbb{Z}$ sind $2, 3, 4$ Nullteiler, 1 und 5 nicht (sondern sie sind Einheiten).
(2) $\mathbb{Z}$, ein Körper k, und $k[x]$ sind Integritätsbereiche.

2.7 Definition
Sei R ein kommutativer Ring, und I ein Ideal in R.
I heißt Hauptideal: $\Leftrightarrow \exists\ a \in R : I = Ra (= aR = RaR)$.
I in R heißt Primideal: $\Leftrightarrow I \neq R$ und $[\forall\ a, b \in R : a \cdot b \in I \Rightarrow a \in I$ oder $b \in I]$.
I in R heißt maximales Ideal: $\Leftrightarrow I \neq R$ und für jedes Ideal J in R gilt: $I \subset J \subset R \Rightarrow J = I$ oder $J = R$.
Ein Integritätsbereich R heißt Hauptidealring, falls jedes Ideal in R ein Hauptideal ist.

Beispiele und Bemerkungen:

(1) $I = \{0\} = R \cdot 0$ und $I = R = R \cdot 1$ sind Hauptideale.
(2) Jeder Körper ist ein Hauptidealring.
(3) Ein Ring R ist Körper $\Leftrightarrow I = \{0\}$ ist maximal (nach 2.5).
(4) Ein Ideal I ist maximal $\Leftrightarrow R/I$ ist ein Körper.
(5) Ein Ideal I ist Primideal $\Leftrightarrow R/I$ ist Integritätsbereich.
(6) Ein maximales Ideal ist immer Primideal. Die Umkehrung gilt nicht, z.B. $I = \{0\} \subset \mathbb{Z}$ ist Primideal, aber nicht maximal.

(7) $\mathbb{Z}$ ist ein Integritätsbereich. Alle Ideale von $\mathbb{Z}$ sind von der Form $n\mathbb{Z}$. Sie sind Hauptideale.
(8) $\mathbb{Z}/n\mathbb{Z}$ ist Integritätsbereich $\Leftrightarrow n = 0$ oder $n = p$ (Primzahl). Also $n\mathbb{Z} \subset \mathbb{Z}$ ist Primideal $\Leftrightarrow n = 0$ oder $n = p$ Primzahl. $n\mathbb{Z} \subset \mathbb{Z}$ ist maximal $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ ist Körper $\Leftrightarrow n = p$ Primzahl.
(9) $\mathbb{Z}[x]$ ist kein HIR: $< 2, x >$ ist kein Hauptideal.

2.8 Definition
Ein Integritätsbereich R heißt euklidisch, falls es eine Gradabbildung $\lambda : R - \{0\} \to \mathbb{N}$ gibt, so dass gilt:

$$\forall a, b \in R,\ b \neq 0\ \exists\ q, r \in R \text{ mit } a = qb + r \text{ und } [\ r = 0 \text{ oder } \lambda(r) < \lambda(b)\ ]$$

(Division mit Rest)

2.9 Theorem
R euklidisch $\Rightarrow R$ Hauptidealring.

Beispiel: $R = \mathbb{Z}$ mit $\lambda(x) = |x| \in \mathbb{N}_0$.

2.10 Proposition
Sei k ein Körper, dann ist $k[x]$ euklidisch, also insbesondere ein Hauptidealring.

$\mathbb{C} \supset \mathbb{Z}[i] := \{a + bi\ :\ a, b \in \mathbb{Z}\} \supset \mathbb{Z}$
$\mathbb{Z}[i]$ heißt der Ring der ganzen Gaußschen Zahlen.

2.11 Proposition
Der Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen ist euklidisch, also ein Hauptidealring.

2.12 Definition
Sei R ein Integritätsbereich und $p \neq 0$ ein nicht invertierbares Element.
p heißt irreduzibel: $\Leftrightarrow \forall\ x, y \in R : xy = p \Rightarrow x$ oder $b \in R^*$, sonst heißt p reduzibel.
p heißt prim oder Primelement: $\Leftrightarrow Rp$ Primideal $\Leftrightarrow \forall c, d \in R : p|cd \Rightarrow p|c$ oder $p|d$
($p|a$ heißt $\exists\ b : a = pb$).

Bemerkung: p prim $\Rightarrow p$ irreduzibel. Im Allgemeinen ist die Umkehrung falsch.

2.13 Proposition
Sei R ein Hauptidealring und $p \in R$, $p \neq 0$, $p \notin R^*$. Dann sind äquivalent:

(1) p ist irreduzibel.
(2) p ist prim.
(3) $< p > := Rp$ ist ein maximales Ideal.

2.14 Lemma
Sei R ein Hauptidealring. Dann ist R noethersch, d.h. $\forall$ Ketten von Idealen $< a_1 > \subset < a_2 > \subset \ldots \subset R$ gilt $\exists\, n \in \mathbb{N} :< a_n >=< a_{n+1} >= \ldots$.

2.15 Theorem
Sei R ein Hauptidealring und $a \in R$, $a \neq 0$, $a \notin R^*$. Dann ist a ein Produkt von Primelementen. Diese Zerlegung ist eindeutig bis auf Reihenfolge und Multiplikation mit Einheiten. Also ist R ein faktorieller Ring.

In faktoriellen Ringen gilt 'prim = irreduzibel', und das charakterisiert diese Ringe.

Beispiele:

(1) $p \in \mathbb{Z}$ ist prim $\Leftrightarrow p$ irreduzibel $\Leftrightarrow p = \pm$Primzahl.
(2) Irreduzible Polynome in $k[x]$ hängen von k ab: $x - \lambda$ ist immer irreduzibel, $x^2 + 1 \in \mathbb{R}[x]$ ist auch irreduzibel.
(3) $R = \mathbb{Z}[i]$: die Einheiten sind ± 1 und $\pm i$. $5 \in R$ ist kein Primelement, da $5 = (1 + 2i)(1 - 2i)$. Dies ist die Primfaktorzerlegung von 5 in R.
(4) $R = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, da $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$; beides sind Zerlegungen in Produkte irreduzibler Elemente. 2 ist irreduzibel aber nicht prim.

2.16 Theorem (Satz von Gauß)
Sei R faktoriell. Dann ist auch $R[x]$ faktoriell.

Insbesondere: $k[x_1, \ldots, x_n]$ für k Körper und $\mathbb{Z}[x_1, \ldots, x_n]$ sind faktoriell.

Sei R ein Integritätsbereich. Dann existiert ein Körper der Brüche $Q(R)$, der Quotientenkörper:

$$Q(R) := \{\frac{a}{b} : a, b \in R, b \neq 0\}/\sim$$

mit $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$. Addition und Multiplikation sind wie üblich bei Brüchen. R ist ein Teilring von $Q(R)$. Für R faktoriell, kann man a und b in Primfaktoren zerlegen: $a = \varepsilon p_1^{a_1} \cdots p_n^{a_n}$, $b = \varepsilon' p_1^{b_1} \cdots p_n^{b_n}$, wobei $\varepsilon, \varepsilon'$ Einheiten in R sind. Daher $\frac{a}{b} = \tilde{\varepsilon} p_1^{c_1} \cdots p_n^{c_n}$ mit $c_i = a_i - b_i \in \mathbb{Z}$. Das liefert eine eindeutige Darstellung (bis auf Wahl von ε)

$$\frac{a}{b} = \tilde{\varepsilon} \prod_{p \in \mathrm{Prim}(R)} p^{v_p} \qquad \text{mit } v_p = v_p(\frac{a}{b}) \in \mathbb{Z}.$$

Formal $v_p(0) = \infty$; für $f = \sum_i a_i x^i \in Q(R)[x]$, $v_p(f) := \min_i v_p(a_i)$. Also $f = 0 \Leftrightarrow v_p(f) = \infty$, und $f \in R[x] \Leftrightarrow v_p(f) \geq 0\ \forall\, p$ Prim.

2.17 Proposition (Lemma von Gauß)
Sei R faktoriell, $p \in R$ ein Primelement, und $f, g \in Q(R)[x]$. Dann gilt $v_p(fg) = v_p(f) + v_p(g)$.

Ein Polynom $f(x) = \sum_{i=0}^{n} a_i x^i$ heißt normiert, falls $a_n = 1$. Solche Polynome in $R[x]$ nennen wir primitiv. Für primitive Polynome stimmt die Zerlegung in $R[x]$ mit der Zerlegung in $Q(R)[x]$ überein.

2.18 Korollar
Sei R faktoriell, $h \in R[x]$ normiert, $h = f \cdot g$ mit f, g normiert und $f, g \in Q(R)[x]$. Dann gilt $f, g \in R[x]$.

§3. Körper

Polynomiale Gleichungen in $k[x]$ müssen in k nicht lösbar sein. Beispiel: $k = \mathbb{R}$, $x^2 + 1 - 0$; $k = \mathbb{Q}$, $x^2 - 2 = 0$. In beiden Fällen liegen Lösungen in größeren Körpern, zum Beispiel $\mathbb{C} = \mathbb{R}[i]$. Für $x^2 - 2$ reicht $\mathbb{Q}[\sqrt{2}\,] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

3.1 Definition
Sei L ein Körper. Ein Teilring $K \subset L$ heißt Teilkörper von L $:\Leftrightarrow \forall\ x \in K - \{0\}$: $x^{-1} \in K$ (also ist K ein Körper mit derselben Multiplikation und Addition). L heißt dann Erweiterungskörper von K. Die Inklusion $K \subset L$ heißt Körpererweiterung, Bezeichnung L/K. Ein Körper K' mit $K \subset K' \subset L$ heißt Zwischenkörper der Körpererweiterung L/K.

Sei $M \subset L$ eine Teilmenge. Dann heißt

$$T(M) \quad = \bigcap_{M \subset T,\ T \text{ Teilkörper von } L} T$$

der von M erzeugte Teilkörper von L.

Für $M \subset L$ und K Teilkörper, wird $T(K \cup M)$ mit $K(M)$ bezeichnet, und man sagt, dass $K(M)$ aus K durch Adjunktion von M entsteht.
Für $M = \{a_1, \cdots, a_n\}$ schreibt man $K(a_1, \cdots, a_n)$ statt $K(M)$.
L/K heißt endlich erzeugt (oder endlich erzeugbar): $\Leftrightarrow\ \exists\ a_1, \cdots, a_n \in L$ mit $L = K(a_1, \cdots, a_n)$.
L/K heißt einfach (einfache Erweiterung): $\Leftrightarrow \exists\ a \in L$ mit $L = K(a)$.

Bemerkung: Ein Erweiterungskörper L von K ist ein K-Vektorraum.

3.2 Definition
Sei L/K eine Körpererweiterung. Die Vektorraumdimension $\dim_K L$ heißt Grad von L über K oder Grad der Körpererweiterung L/K.
Bezeichnung: $[L : K] = \dim_K L$.
Die Erweiterung L/K heißt endlich, falls $[L : K] < \infty$.

Beispiel: $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$.

3.3 Lemma
Seien M/L und L/K Körpererweiterungen. Dann ist M/K eine Erweiterung vom Grad

$[M : K] = [M : L] \cdot [L : K]$

3.4 Proposition
Seien R, S kommutative Ringe, $\alpha : R \to S$ ein Ringhomomorphismus und $a \in S$. Dann gibt es genau einen Ringhomomorphismus $\varphi : R[x] \to S$ mit $\varphi|_R = \alpha$ und $\varphi(x) = a$. φ heißt Auswertungshomomorphismus.

Spezieller Fall: $a = 0$, $R[x] \to S$ mit $f(x) \mapsto f(0)$.

Beispiele: Sei L/K eine Körpererweiterung, und $\alpha : R = K \subset L = S$ die Inklusion.

(1) $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}\,]$, $a = \sqrt{2}$. Der Auswertungshomomorphismus $\varphi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$, $f(x) \mapsto f(\sqrt{2})$, ist surjektiv und hat den Kern $\langle x^2 - 2\rangle$. Daher ist $\mathbb{Q}[\sqrt{2}\,] \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle$.
(2) $\mathbb{R} \subset \mathbb{C}$, $a = i$: $\mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1\rangle$.
(3) $\mathbb{Q} \subset \mathbb{R}$, $a = \pi$: $\varphi : \mathbb{Q}[x] \to \mathbb{R}[\pi] \subset \mathbb{R}$ ist injektiv, aber nicht surjektiv, da π keine algebraische Gleichung erfüllt.

3.5 Definition
Sei L/K eine Körpererweiterung, $a \in L, \varphi : K[x] \to L$ mit $\varphi(x) = a$. Wenn φ injektiv ist, heißt a transzendent, sonst algebraisch (oder algebraisch abhängig über K).
Wenn a algebraisch ist und $f(x) \in K[x]\backslash\{0\}$ ein Polynom minimalen Grades mit $f(a) = 0$, dann heißt $f(x)$ Minimalpolynom $m_a = m_{a,K}$ von a über K.

Sei a algebraisch über $K, \varphi = \varphi_a : K[x] \to L$ mit $x \mapsto a$, und sei $f(x)$ Minimalpolynom von a über K, dann gilt: $\mathrm{Ker}(\varphi_a) = \langle f(x)\rangle$. Insbesondere existiert das Minimalpolynom und ist eindeutig bis auf skalare Vielfache.

Notation: Sei L/K eine Körpererweiterung, $a \in L$.
$K(a)$ = kleinster Teilkörper von L, der a enthält
$K[a] = \mathrm{Im}(\varphi_a) = \{\sum_{i=0}^{n} \lambda_i a^i : \lambda_i \in K, n \in \mathbb{N}\} \subset L$ („Polynome in a")

3.6 Proposition
Sei L/K eine Körpererweiterung, $a \in L$. Dann sind die folgenden Ausagen äquivalent:

(1) Das Element $a \in L$ ist algebraisch abhängig über K.
(2) Es gilt $K[a] = K(a)$.
(3) Es gilt $\dim_K K(a) < \infty$.

In diesem Fall gilt: $\lambda(m_a) = [K(a) : K]$. Diese Zahl heißt dann auch der Grad von a über K.

Das Minimalpolynom m_a eines algebraische Elements a ist irreduzibel. Das Ideal $\langle m_a\rangle$ ist maximal in $K[x]$ mit $K[a] \cong K[x]/\langle m_a\rangle$. Alle einfachen Körpererweiterungen von K sind von dieser Form.

3.7 Theorem (Kriterium von Eisenstein)
Sei R ein fatorieller Ring, K der Quotientenkörper von R,

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \text{ mit } n \geq 1,$$

und sei $p \in R$ eine Primzahl. Es gelte $p \nmid a_n$, aber $p | a_i$ für $i = 0, \cdots, n-1$ und $p^2 \nmid a_0$. Dann ist $f(x)$ irreduzibel in $K[x]$. Falls $a_n = 1$ oder allgemeiner $f(x)$ primitiv, dann ist $f(x)$ auch in $\mathbb{Q}[x]$ irreduzibel.

Beispiele:

(1) $f(x) = x^n - l$, $l \in \mathbb{Z} \backslash \{0\}$, ist irreduzibel.
(2) $g(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \ldots + x + 1$, für p Primzahl, ist irreduzibel.

3.8 Definition
Eine Körpererweiterung L/K heißt algebraisch: $\Leftrightarrow$ jedes $a \in L$ ist algebraisch abhängig über K.

3.9 Proposition
Seien L/K und M/L Körpererweiterungen. Dann gilt

(1) L/K endlich $\Rightarrow$ L/K algebraisch.
(2) L/K algebraisch und endlich erzeugt $\Rightarrow$ L/K endlich.
(3) L/K und M/L algebraisch $\Rightarrow$ M/K algebraisch.

3.10 Theorem (Kronecker)
Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Dann existiert eine algebraische (sogar einfache) Körpererweiterung L/K mit $[L : K] = \text{Grad } (f)$, so dass f in L eine Nullstelle hat.

3.11 Definition
Sei K ein Körper. Dann sind die folgenden Bedingungen äquivalent:

(a) $\forall\ f \in K[x] - K : f$ hat eine Nullstelle in K
(b) $\forall\ f \in K[x] - K : \exists f_1, \cdots, f_n \in K[x]$, alle vom Grad 1, $f = f_1 \cdot \ \ldots \ \cdot f_n$
(c) $\forall\ f \in K[x] : f$ irreduzibel und nomiert $\Rightarrow \exists\ a \in K : f(x) = x - a$
(d) L/K algebraisch $\Rightarrow L = K$

Wenn diese Bedingungen erfüllt sind, heißt K algebraisch abgeschlossen.
Bezeichnung: $K = \overline{K}$.

Analysis (Fundamentalsatz der Algebra): $\mathbb{C} = \overline{\mathbb{C}}$, $\mathbb{Q}$ und $\mathbb{R}$ sind nicht algebraisch abgeschlossen.

3.12 Definition
Sei K ein Körper, $\overline{K} \supset K$ eine algebraische Körpererweiterung mit $\overline{K}$ algebraisch abgeschlossen. Dann heißt $\overline{K}$ algebraischer Abschluss von K.

Frage: Existenz, Eindeutigkeit?

Auswahlaxiom (AC = axiom of choice)
Sei I eine Menge, $I \neq \emptyset$, und $\{M_i : i \in I\}$ eine Menge von Mengen, $M_i \neq \emptyset \ \forall i \in I$. Dann existiert eine Funktion

$$f : I \to \bigcup_{i \in I} M_i \quad \text{mit } f(i) \in M_i \ \forall \ i \in I.$$

f heißt Auswahlfunktion.

Sei M eine Menge und $\leq$ eine partielle Ordnung auf M, d.h. eine Relation in $M \times M$, so daß gilt: $x \leq x, \ \forall \ x$; $x \leq y, y \leq z \Rightarrow x \leq z$; $x \leq y, y \leq x \Rightarrow x = y$. Die Ordnung heißt total, wenn $\forall \ x, y \in M : x \leq y$ oder $y \leq x$. Sei $N \subseteq M$, $a \in M$ heißt obere Schranke für $N :\Leftrightarrow x \leq a, \ \forall \ x \in N$; $a \in M$ heißt maximales Element von M, wenn $a \leq x \Rightarrow a = x$. (Ein maximales Element muss nicht eindeutig sein; es muss kein größtes Element geben.)

Zorns Lemma
Sei $M \neq \emptyset$ durch $\leq$ partiell geordnet, so daß $\forall \ N \subseteq M : N$ total geordnet durch $\leq \Rightarrow$ $\exists$ obere Schranke $a \in M$ für N. Dann existiert ein maximales Element in M.

Das Auswahlaxiom anzunehmen macht die Welt größer, aber auch unübersichtlicher. Z.B. impliziert AC: Jeder Vektorraum hat eine Basis; es gibt nicht messbare Mengen; Produkte kompakter Mengen sind kompakt; es gilt das Banach-Tarski-Paradoxon.

3.13 Theorem
Sei R ein Ring mit $1 \neq 0$. Dann existiert ein maximales Ideal $I \lhd R$.

3.14 Theorem
Jeder Körper K hat einen algebraischen Abschluss.

3.15 Definition
Seien L_1/K und L_2/K Erweiterungen von K. Ein Ringhomomorphismus $\varphi : L_1 \to L_2$ heißt ein K-Homomorphismus, wenn φ ein Ringhomomorphismus ist und $\varphi(x) = x \ \forall \ x \in K$ gilt.
Falls φ bijektiv ist, heißt φ ein K-Isomorphismus und falls zusätzlich $L_1 = L_2$ gilt, heißt φ ein K-Automorphismus.

Beispiele:

(1) Komplexe Konjugation in $\mathbb{C}/\mathbb{R} : a + bi \mapsto a - bi$ ist ein $\mathbb{R}$-Automorphismus.
(2) $\mathbb{Q}[\sqrt{2}]/\mathbb{Q} : a + b\sqrt{2} \mapsto a - b\sqrt{2}$ ist ein $\mathbb{Q}$-Automorphismus.

In beiden Fällen werden die Wurzeln der Minimalpolynome permutiert.

Mit $\mathrm{Aut}_K(L)$ bezeichnen wir die Menge der K-Automorphismen von L. Das ist eine Gruppe unter Komposition.

3.16 Proposition
Seien K und K' Körper, $\sigma : K \to K'$ ein Isomorphismus, $\sigma^* : K[x] \to K'[x]$ der induzierte Isomorphismus mit $\sigma^*(\sum a_i x^i) = \sum \sigma(a_i)x^i$; seien L/K und L'/K' Körpererweiterungen.

(a) Für $a \in L, a' \in L'$ mit $m_{a',K'} = \sigma^*(m_{a,K})$ gibt es genau einen Isomorphismus $\varphi : K(a) \to K'(a')$ mit $\varphi|_K = \sigma$ und $\varphi(a) = a'$.

(b) Sei $a \in L$. Dann gilt:

$$\sharp\{\varphi : K(a) \to L' \text{ mit } \varphi|_K = \sigma\} = \sharp\{x \in L' : \sigma^*(m_{a,K})(x) = 0\}.$$

Beispiel: $K = K' = \mathbb{Q}$, $\sigma =$id, $m_{a,K} = x^3 - 2$ für $a = \sqrt[3]{2}(\in \mathbb{R})$, $L' = \mathbb{C}$. Dann gilt $\{x \in L' : \sigma^*(m_{a,K})(x) = 0\} = \{\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}, e^{\frac{4\pi i}{3}}\sqrt[3]{2}\}$. Deswegen ist $\sharp\{\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}\} = 3$.

3.17 Theorem
(a) Sei L/K eine algebraische Erweiterung, $M = \overline{M}$, $\sigma : K \to M$ ein Homomorphismus. Dann existiert ein Homomorphismus $\varphi : L \to M$ mit $\varphi|_K = \sigma$, das heißt φ setzt σ fort:

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, hook] \arrow[dr, phantom, "\circlearrowleft"] & M \arrow[d, phantom, "\parallel"] \\ L \arrow[r, "\varphi"] & \overline{M} \end{tikzcd}$$

(b) Sei $\sigma : K \xrightarrow{\sim} K'$, und sei $\overline{K}$ bzw. $\overline{K'}$ der algebraische Abschluss von K bzw. K'. Dann existiert ein Isomorphismus $\varphi : \overline{K} \to \overline{K'}$ mit $\varphi|_K = \sigma$, also

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, hook] \arrow[dr, phantom, "\circlearrowleft"] & K' \arrow[d, hook] \\ \overline{K} \arrow[r, "\varphi"] & \overline{K'} \end{tikzcd}$$

(c) Seien L_1, L_2 algebraische Abschlüsse von K, dann existiert ein K-Isomorphismus $L_1 \to L_2$, also

$$\begin{tikzcd} K \arrow[r, phantom, "="] \arrow[d, hook] \arrow[dr, phantom, "\circlearrowleft"] & K \arrow[d, hook] \\ L_1 \arrow[r, "\sim"] & L_2 \end{tikzcd}$$

Folglich ist der algebraische Abschluß eindeutig bis auf Isomorphie und alle algebraischen Gleichungen lassen sich darin lösen.

§4. Körpererweiterungen und Galoistheorie

4.1 Definition

Sei K ein Körper, $f(x) \in K[x]$ ein Polynom vom Grad $n \geq 1$, und sei L/K eine Körpererweiterung. Dann heißt L ein Zerfällungskörper von f über K $:\Leftrightarrow \exists a_1, \cdots, a_n \in L, c \in K$, so dass

(1) $f(x) = c \prod_{j=1}^{n}(x - a_j)$ in $L[x]$, d.h. f ist Produkt von Linearfaktoren;
(2) $L = K(a_1, \cdots, a_n)$, d.h. L ist erzeugt von den Nullstellen von f.

Bemerkung:

(1) Der durch den Satz von Kronecker konstruierte Körper ist im Allgemeinen kein Zerfällungskörper.
(2) Der Zerfällungskörper L von $f(x)$ existiert und ist eindeutig bis auf Isomorphie.
(3) Das Polynom $f(x)$, dessen Zerfällungskörper L ist, ist nicht eindeutig. Zum Beispiel ist $\mathbb{C} = L \supset K = \mathbb{R}$ Zerfällungskörper von $x^2 + 1$, von $(x^2 + 1)(x - 5)$ und von $(x - (1 + i))(x - (1 + i))$.

4.2 Definition

Sei L/K eine Körpererweiterung, Λ eine Menge von nichtkonstanten Polynomen in $K[x]$. Dann heißt L Zerfällungskörper von Λ über K, falls über L alle Polynome in Λ in Linearfaktoren zerfallen und es keinen Zwischenkörper L_0 mit $K \subset L_0 \subsetneqq L$ gibt, über dem auch schon alle Polynome aus Λ in Linearfaktoren zerfallen.
Eine Körpererweiterung L/K heißt normal, wenn es eine Menge Λ solcher Polynome gibt, so dass L Zerfällungskörper von Λ ist.

4.3 Proposition

Sei $K \subset L \subset \overline{K}$, dann sind äquivalent:

(1) $f \in K[x]$ irreduzibel mit Nullstelle in $L \Rightarrow f = \prod$ Linearfaktoren $\in L[x]$.
(2) L/K ist normal.
(3) $\varphi : L \to \overline{K}$ ein K-Homomorphismus $\Rightarrow \varphi(L) = L$.

4.4 Definition

(1) $K \subset L \subset \overline{K}$. Der Separabilitätsgrad $[L : K]_s$ ist definiert als Anzahl der verschiedenen K-Homomorphismen $L \to \overline{K}$.
(2) L/K endlich heißt separabel $:\Leftrightarrow [L : K]_s = [L : K]$.
(3) $a \in \overline{K}$ heißt separabel über K $:\Leftrightarrow m_{a,K}$ hat nur einfache Nullstellen über K.

Im Allgemeinen gilt $[L : K] \geq [L : K]_s$.

Für L/K normal gilt: $[L : K]_s = |\mathrm{Aut}_K(L)|$.

Sei a eine Nullstelle von $f(x)$. Dann a ist eine einfache Nullstelle $\Leftrightarrow f'(a) = 0$.

4.5 Lemma
Sei $a \in \overline{K}$. Dann gilt: a separabel über $K \Leftrightarrow m'_{a,K} \neq 0$.

4.6 Definition
Sei K ein Körper. Die Charakteristik $\mathrm{char}(K)$ ist $n \in \mathbb{N}_0$, wenn

$$\underbrace{1 + \cdots + 1}_{n} = 0$$

in K mit n minimal, oder 0 wenn kein solches n existiert.

Beispiele: $\mathrm{char}(\mathbb{F}_p) = p = \mathrm{char}(\overline{F_p})$, $\mathrm{char}(\mathbb{Q}) = 0 = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C})$.
Die Charakteristik muss Null oder eine Primzahl sein.

4.7 Proposition

(1) Sei L/K endlich. Dann gilt: L/K separabel $\Leftrightarrow$ jedes $a \in L$ separabel über K.
(2) Sei L/K endlich. Dann gilt: L/K separabel $\Leftrightarrow \exists\ a_1, \ldots, a_n \in L$, separabel über K mit $L = K(a_1, \ldots, a_n)$.
(3) $\mathrm{char}(K) = 0$, L/K endlich $\Rightarrow L/K$ separabel.
(4) $\mathrm{char}(K) = p \neq 0$, L/K endlich, $p \nmid [L : K] \Rightarrow L/K$ separabel.
(5) $K \subset M \subset L$. Dann gilt: L/K separabel $\Leftrightarrow L/M$ und M/K separabel.

Die obige Definition von separabel setzt L/K voraus. Proposition 4.7 erlaubt, separable Körpererweiterungen allgemeiner zu definieren. Im Folgenden werden jedoch nur endliche separable Erweiterungen betrachtet.

4.8 Theorem (Satz vom primitiven Element)
Sei L/K endlich und separabel. Dann existiert $a \in L$ mit $L = K(a)$, also L/K einfach.

4.9 Theorem

(1) Sei $n \in \mathbb{N}$, p Primzahl. Der Zerfällungskörper L des Polynoms $f(x) = x^{p^n} - x$ ist ein Erweiterungskörper von $\mathbb{F}_p$ mit $[L : \mathbb{F}_p] = n$. Also gilt $|L| = p^n$, $L = \{\text{Nullstellen von } f\}$ und $L/\mathbb{F}_p$ ist algebraisch, separabel und normal.
Bezeichnung $L = \mathbb{F}_q$ für $q = p^n$.
(2) $\mathbb{F}_q$ ist bis auf Isomorphie der einzige Körper mit q Elementen. Jeder endliche Körper ist isomorph zu einem $\mathbb{F}_q$.
(3) Die Gruppe $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ ist zyklisch von der Ordnung n, erzeugt vom Frobeniusautomorphismus $\mathrm{Fr} : x \mapsto x^p$.

4.10 Definition
Eine Körpererweiterung L/K heißt Galoiserweiterung (oder galoissche Erweiterung), wenn L/K separabel und normal ist. Die Gruppe $\mathrm{Aut}_K(L)$ heißt dann Galoisgruppe von L/K. Bezeichnung $\mathrm{Gal}(L/K)$ (oder $G(L/K)$).

Bemerkung: Wir betrachten nur endliche Galoiserweiterungen.
Wenn L/K galoissch ist, gilt $[L : K] = \mathrm{Aut}_K(L) = |\mathrm{Gal}(L/K)|$.

Beispiel: Sei L der Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$. Dann gilt $[L : \mathbb{Q}] = 6$ und $\mathrm{Gal}(L/K) \cong \Sigma_3$, Permutationen der drei Nullstellen $\{\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}}\}$.

4.11 Definition
Sei L ein Körper, $G \subset \mathrm{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L. Sei $L^G := \{a \in L : \varphi(a) = a, \ \forall \ \varphi \in G\}$; L^G ist ein Körper und heißt der Fixkörper von G.

4.12 Proposition
Sei L/K eine Galoiserweiterung mit $G = \mathrm{Gal}(L/K)$. Dann gilt $L^G = K$, d.h. K ist der Fixkörper der Galoisgruppe.

Eine beliebige Erweiterung L/K muss keine Galoiserweiterung sein, aber man kann Galoiserweiterungen daraus herstellen:

4.13 Proposition
Sei L ein Körper, $H \subset \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist L/L^H eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/L^H) = H$ und es gilt $[L : L^H] = |H|$.

4.14 Theorem (Hauptsatz der Galoistheorie)
Sei L/K eine (endliche) Galoiserweiterung, $\mathcal{U} := \{H < \mathrm{Gal}(L/K) : H \text{ Untergruppe}\}$, und $\mathcal{Z} := \{M : K \subset M \subset L, M \text{ Zwischenkörper}\}$. Dann gibt es zwei zueinander inverse Bijektionen α und β:

$$\alpha : \mathcal{Z} \to \mathcal{U}, \quad M \mapsto \mathrm{Gal}(L/M)$$

$$\beta : \mathcal{U} \to \mathcal{Z}, \quad H \mapsto L^H.$$

Insbesondere ist L/M Galoisch. Die Abbildungen α und β kehren Inklusionen um:

$$M \subset M' \Rightarrow \alpha(M) > \alpha(M')$$

$$H < H' \Rightarrow \beta(H) \supset \beta(H').$$

Für $H \in \mathcal{U}, \varphi \in \mathrm{Gal}(L/K)$ gilt: $\varphi(L^H) = L^{\varphi H \varphi^{-1}}$.
Für $M \in \mathcal{Z}$ ist die Erweiterung M/K normal $\Leftrightarrow$ $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$. In diesem Fall gibt es einen surjektiven Gruppenhomomorphismus

$$\gamma : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K), \quad \varphi \mapsto \varphi|_M$$

mit $\mathrm{Ker}(\gamma) = \mathrm{Gal}(L/M)$, und es gilt: $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Beispiel: Sei $L \subset \mathbb{C}$ der Zerfällungskörper von $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Die Nullstellen von $f(x)$ sind $\sqrt[4]{2}, \ -\sqrt[4]{2}, \ i\sqrt[4]{2}, \ -i\sqrt[4]{2}$. Daher ist $L = \mathbb{Q}(\sqrt[4]{2}, i)$ eine Galoiserweiterung über

$\mathbb{Q}$ von Grad 8. Die Galoisgruppe ist $G = \mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\circ\sigma, \tau\circ\sigma^2, \tau\circ\sigma^3\}$, wobei

$$\begin{aligned} \sigma &: \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \quad i \mapsto i, \\ \tau &: \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad i \mapsto -i. \end{aligned}$$

Diese Gruppe ist isomorph zur Diedergruppe D_4, der Gruppe der Symmetrien eines Quadrats (σ = Drehung und τ = Spiegelung). Das Untergruppendiagramm ist

$$\begin{tikzcd}[column sep=small]
 & & \mathrm{Gal}(L/\mathbb{Q}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & H_2 = \langle \sigma^2, \tau \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & H_1 = \langle \sigma \rangle \arrow[d, dash] & H_3 = \langle \sigma^2, \sigma\circ\tau \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
J_4 = \langle \sigma^2 \circ \tau \rangle \arrow[drr, dash] & J_2 = \langle \tau \rangle \arrow[dr, dash] & J_1 = \langle \sigma^2 \rangle \arrow[d, dash] & J_3 = \langle \sigma\circ\tau \rangle \arrow[dl, dash] & J_5 = \langle \sigma^3 \circ \tau \rangle \arrow[dll, dash] \\
 & & \{\mathrm{id}\} & &
\end{tikzcd}$$

Das Zwischenkörperdiagramm ist

$$\begin{tikzcd}[column sep=small]
 & & L^G = \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & L^{H_2} = \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & L^{H_1} = \mathbb{Q}(i) \arrow[d, dash] & L^{H_3} = \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L^{J_4} = \mathbb{Q}(i\sqrt[4]{2}) \arrow[drr, dash] & L^{J_2} = \mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash] & L^{J_1} = \mathbb{Q}(i, \sqrt{2}) \arrow[d, dash] & L^{J_3} = \mathbb{Q}((1+i)\sqrt[4]{2}) \arrow[dl, dash] & L^{J_5} = \mathbb{Q}((1-i)\sqrt[4]{2}) \arrow[dll, dash] \\
 & & L^{\{\mathrm{id}\}} = L & &
\end{tikzcd}$$

§5. Anwendungen

5.1 Definition

Sei $M \subset \mathbb{R}^2 = \mathbb{C}$. Ein Punkt $p = (x, y)$ heißt (aus M mit Zirkel und Lineal) <u>konstruierbar</u>: $\Leftrightarrow$ $\exists n \in \mathbb{N}$, Kette $M := M_0 \subset M_1 \subset \cdots \subset M_n \subset \mathbb{C} = \mathbb{R}^2$ so dass jedes M_i aus M_{i+1} in einem elementaren Konstruktionsschritt erhalten werden kann und $p \in M_n$.
$\mathrm{Kon}(M) := \{p \in \mathbb{R}^2 : p \text{ aus } M \text{ konstruierbar}\}$

5.2 Theorem

Sei $M \subset \mathbb{C}$, $0, 1 \in M$. Dann gilt:

(1) $\mathrm{Kon}(M)$ ist ein Teilkörper von $\mathbb{C}$;

(2) $\mathrm{Kon}(M) = \overline{\mathrm{Kon}(M)} := \{z \in \mathbb{C} : \overline{z} \in \mathrm{Kon}(M)\}$;
(3) $\mathbb{Q}(M \cup \overline{M})$ ist ein Teilkörper von $\mathrm{Kon}(M)$;
(4) Für $b \in \mathbb{C}$ gilt: $b^2 \in \mathrm{Kon}(M) \Rightarrow b \in \mathrm{Kon}(M)$ (d.h. $\mathrm{Kon}(M)$ ist quadratisch abgeschlossen, vgl Aufgabenblatt 8).

5.3 Theorem
Sei $M \subset \mathbb{C}$, $0, 1 \in M$. Dann gilt:
(1) $\mathrm{Kon}(M)/\mathbb{Q}(M \cup \overline{M})$ ist eine algebraische Körpererweiterung von unendlichem Grad;
(2) Für $z \in \mathbb{C}$ gilt: $z \in \mathrm{Kon}(M) \Leftrightarrow \exists$ Kette $\mathbb{Q}(M \cup \overline{M}) = L_0 \subset L_1 \subset \cdots \subset L_r$ von Körpererweiterungen mit $z \in L_r$ und $[L_j : L_{j-1}] \leq 2, \forall\, j$.

Falls $z \in \mathrm{Kon}(M)$, so gilt für $L_0 = \mathbb{Q}(M \cup \overline{M})$: $[L_0(z) : L_0]$ ist eine Potenz von 2; z ist algebraisch über L_0.

Anwendungen:
(1) Würfelverdoppelung (Delisches Problem): $M = \{0, 1\}$. Verdoppelung eines Würfels mit Volumen 1 heißt, man konstruiert einen Würfel mit Volumen 2, also mit Kantenlänge $\sqrt[3]{2}$. Aber $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist keine Potenz von 2. Daher ist $\sqrt[3]{2}$ nicht aus M konstruierbar.
(2) Winkeldreiteilung: Gegeben sei eine Einheitswurzel $z = e^{i\alpha}$. Wir wollen $\xi = e^{\frac{i\alpha}{3}}$ konstruieren. Im Fall $\alpha = \frac{2\pi}{3}$, $z = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, $\xi = e^{\frac{2\pi i}{9}}$ ist ξ nicht konstruierbar aus $M = \{0, 1, z\}$. Denn $L_0 = \mathbb{Q}(z)$, und $L_0(\xi) = \mathbb{Q}(z, \xi) = \mathbb{Q}(\xi)$ hat Grad 3 über L_0.
(3) Quadratur des Kreises: Ein Kreis vom Radius 1 hat die Fläche π, gesucht ist ein Quadrat mit derselben Fläche, also Seitenlänge $\sqrt{\pi}$. Aus $M = \{0, 1\}$ ist aber $\sqrt{\pi}$ nicht konstruierbar, denn π ist transzendent.
(4) Konstruierbarkeit von regelmäßigen n-Ecken, also n-ten Einheitswurzeln: Die primitive n-te Einheitswurzel $e^{\frac{2\pi i}{n}}$ ist konstruierbar genau dann, wenn $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$ eine Potenz von 2 ist. Das gilt genau dann wenn $n = 2^l p_1 \cdots p_r$, wobei $l \geq 1$, p_i sind paarweise verschiedene Fermatsche Primzahlen, das heißt von der Form $2^{2^a} + 1$ $(a \geq 0)$.

5.4 Definition
Sei K ein Körper, $n \in \mathbb{N}, a \in K, E \supset K$ eine Erweiterung, $b \in E$ eine Nullstelle von $x^n - a$ in E. Dann heißt b ein Radikal von a über K. Bezeichnung $b = \sqrt[n]{a}$ (eindeutig bis auf Multiplikation mit Einheitswurzeln).

Eine Körpererweiterung L/K heißt durch Radikale auflösbar :$\Leftrightarrow$ $\exists$ ein "Turm" von Körpererweiterungen $K_0 = K \subset K_1 \subset \cdots \subset K_l$ für ein $l \in \mathbb{N}$ mit $L \subset K_l$ und $\forall j : K_{j+1} = K_j(b_j)$ mit $b_j = \sqrt[n_j]{a_j}$ für $a_j \in K_j$.

Das Polynom $f(x) \in K[x]$ ist durch Radikale auflösbar :$\Leftrightarrow$ sein Zerfällungskörper L ist durch Radikale auflösbar.

5.5 Lemma
Es sei char$K = 0$, und K_n sei der Zerfällungskörper von $x^n - 1$ über K.
Es gibt einen injektiven Gruppenhomomorphismus Gal $(K_n/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ (multiplikative Gruppe), d.h. Gal(K_n/K) ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, also abelsch.

5.6 Lemma
Sei char$K = 0$, sei $e^{2\pi i/n} \in K, L := K(\sqrt[n]{a})$ für ein $a \in K$. Dann ist L/K eine Galoiserweiterung und Gal(L/K) ist zyklisch mit $[L:K]|n$.

Bemerkung: Es gilt auch die folgende Umkehrung: sei K wie oben, L/K eine endliche Galoiserweiterung mit $[L : K] = n$. Wenn Gal(L/K) zyklisch ist, ist L der Zerfällungskörper eines Polynoms $x^n - a$, $a \in K$. Also $L = K(\sqrt[n]{a})$.

5.7 Definition
Sei G eine Gruppe, $G_0 = \{1\} \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$ eine endliche Kette von Untergruppen mit $G_i \lhd G_{i+1}$ normal $\forall\ i = 0, \ldots, n-1$. Diese Kette heißt <u>Normalreihe</u>.
Die Normalreihe heißt <u>abelsch</u>:$\Leftrightarrow \forall\ i = 0, \cdots, n-1 : G_{i+1}/G_i$ ist abelsch.
Die Gruppe G heißt <u>auflösbar</u>: $\Leftrightarrow$ G hat eine abelsche Normalreihe.

Beispiele auflösbarer Gruppen.

1. abelsche Gruppen;
2. die symmetrische Gruppe Σ_3: $\{(1)\} \lhd \langle(123)\rangle \lhd \Sigma_3$ ist eine abelsche Normalreihe;
3. p-Gruppen (p eine Primzahl).

5.8 Definition
Sei G eine Gruppe, $a, b, \in G$, dann heißt $[a,b] := aba^{-1}b^{-1}$ der <u>Kommutator</u> von a und b. Die Untergruppe $D(G) := \langle [a,b] : a, b \in G \rangle$ heißt die <u>Kommutatoruntergruppe</u> (oder <u>derivierte Gruppe</u>) von G. Induktiv definiert man dann $D^{i+1}(G) := D(D^i(G))$.

Bemerkungen:

1. Die Menge $\{[a,b] : a, b \in G\}$ muss keine Gruppe sein.
2. $D(G) \lhd G$ ist normal.
3. G abelsch $\Leftrightarrow D(G) = \{1\}$.
4. $G/D(G)$ ist abelsch.

5.9 Proposition
Sei G eine Gruppe. Dann gilt: G auflösbar $\Leftrightarrow \exists n \in \mathbb{N}$: $D^n(G) = \{1\}$.

5.10 Proposition
Sei $n \geq 5$. Dann gilt $D(\Sigma_n) = D(A_n) = A_n (= \{\text{gerade Permutationen}\})$.
Also sind Σ_n und A_n nicht auflösbar.

5.11 Theorem
Sei L/K eine endliche Körpererweiterung und $\mathrm{char}K = 0$. Dann gilt (a) $\Rightarrow$ (b) mit:

(a) L/K ist durch Radikale auflösbar.
(b) Es existiert eine endliche Galoiserweiterung M/K mit $L \subset M$, so dass $\mathrm{Gal}(M/K)$ auflösbar ist.

Bemerkung: Die Umkehrung (b) $\Rightarrow$ (a) gilt auch. Der Beweis braucht die Umkehrung von 5.6.

5.12 Proposition
Sei $f(x) \in \mathbb{Q}[x]$ irreduzibel, $\deg f = 5$, so dass $f(x)$ in $\mathbb{C}$ genau drei reelle Nullstellen hat. Dann ist die Galoisgruppe von f, d.h. die Galoisgruppe des Zerfällungskörpers von f über $\mathbb{Q}$, isomorph zu Σ_5, also nicht auflösbar.

5.13 Theorem (Fundamentalsatz der Algebra)
Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.