Algebra SoSe 2010 Spickzettel

Aus Vorlesungs-Wiki

Dies ist der offizielle **Spickzettel** zur Vorlesung Algebra SoSe 2010. Alle sind herzlich eingeladen, an der Wiki-Seite mitzuarbeiten!

Für die Richtigkeit der hier gemachten Angaben wird keinerlei Verantwortung übernommen.

Konstruktion mit Zirkel und Lineal

Definition: Aus einer Menge von Punkten lässt sich ein anderer Punkt mit Z & L konstruieren, wenn er Schnittpunkt ist von zwei Geraden, zwei Kreisen, oder einem Kreis und einer Gerade.

Satz: Für $x \in \mathbb{R}$ ist äquivalent:

1. x lässt sich mit Z & L aus dem Teilkörper $K_0 \subset \mathbb{R}$ konstruieren
2. x liegt in einem Turm quadratischer Erweiterungen $K_0 \subset K_1 ... \subset K_n \ni x$ in $\mathbb{R}$, d.h. $K_{i+1} = K_i[\sqrt{c}]$

Beispiel: Das regelmäßige 9-Eck ist nicht konstruierbar

- Zuerst wird gezeigt: $\kappa = 2\cos(\frac{2\pi}{9})$ ist nicht rational. Beweis: κ erfüllt die Gleichung $P(\kappa) = \kappa^3 - 3\kappa + 1 = 0$ (Additionstheoreme). Das Polynom hat keine rationalen Nullstellen. Gegenannahme: $\exists$ NS $x = \frac{a}{b} \in \mathbb{Q}$ (gekürzter Bruch). Daraus folgt
$$a^3 + 3ab^2 - b^3 = 0$$
Man sieht $a|b$ und $b|a$ also $a = \pm 1, b = 1$. Aber $x = \pm 1$ ist keine Nullstelle, also existiert keine.
- Noch zu Zeigen: Wenn P eine NS hat in $K[\sqrt{c}]$, dann auch in K. Denn dann ist κ nicht durch einen Turm erreichbar.
Sei $x = a + b\sqrt{c} \in K[\sqrt{c}]$. Einsetzen, wenn $\sqrt{c} \notin K$:
$$a^3 + 3ab^2c - 3a + 1 = 0 \text{ und } 3a^2b + b^3c - 3b = 0$$
Zweite Gleichung nach c auflösen, in die erste einsetzen: $-8a^3 + 6a + 1 = 0$, also ist $-2a \in K$ Nullstelle von P.

Monoide und Gruppen

Grundstrukturen

Definitionen Axiome: 0: Kommutativität, 1: Assoziativität, 2: Neutrales Element, 3: Inverses Element

	abg. Verkn.	0	1	2	3	Beispiele
Magma	X					$(\mathbb{Z}, -)$
Halbgruppe	X		X			$(\mathbb{N}^*, +)$
Monoid	X		X	X		$(\mathbb{N}, +), (\mathbb{N}, \cdot), (End(X), \circ), \{e\}$
						$M^X = Abb(X, M)$, $M^{(X)}$: komp. Träger
Gruppe	X		X	X	X	$(\mathbb{Z}, +), (Aut(X) = End(X)^\times, \circ)$,
						$(\mathbb{Q}, +), (\mathbb{Q}^*, \cdot), \{e\}$
Abelsch	X	X				

Homomorphismen

Definition

- Magmen, Gruppen: $h: (M, \cdot) \to (N, *)$ muss erfüllen $h(a \cdot b) = h(a) * h(b)$
Bei Gruppen folgt $h(e_M) = e_N$ automatisch, weil
$$h(e_M) = h(e_M \cdot e_M) = h(e_M) * h(e_M) \quad | * h(e_M)^{-1}$$
Außerdem $e_N = h(e_M) = h(a \cdot a^{-1}) = h(a) * h(a^{-1})$, also $h(a^{-1}) = h(a)^{-1}$.
- Monoid: Magma + $h(e_M) = e_N$

Satz: Ein Gruppenhomomorphismus f ist injektiv dann, und nur dann, wenn $\ker(f) = \{e\}$ gilt. Denn: $f(a) = f(b) \Leftrightarrow f(a)f(b)^{-1} \Leftrightarrow f(ab^{-1}) = 1 \Leftrightarrow ab^{-1} \in \ker(f)$

Zyklische Gruppen: $\mathbb{Z}$ und $\mathbb{Z}/n$ sind zyklisch.

Ordnung: Die Ordnung einer Gruppe ist ihre Kardinalität: $ord(G) = |G|$
Die Ordnung von $a \in G$ ist die Ordnung von $<a>$

Satz von Cayley: Jede Gruppe $(G, *)$ ist isomorph zu einer Untergruppe von $Sym(X)$ für eine geeignete Menge X, wobei $X = G$ gewählt werden kann. Die λ_m sind hier immer bijektiv.

Kommutativität

Satz: Eine Gruppe G ist abelsch dann und nur dann wenn $x \mapsto x^n$ ein Endomorphismus ist. $x \mapsto x^{-1}$ ist dann sogar ein Automorphismus.

Satz: Sei A eine abelsche Gruppe. Dann gilt

- $(End(A), +)$ ist eine abelsche Gruppe
- $(End(A), \circ)$ ist ein Monoid

Quotientenstrukturen

Homomorphiesatz: Sei $(M, *)$ ein Magma, sei $\equiv$ eine Äquivalenzrelation auf M, die mit $*$ verträglich ist, und sei $\pi: M \to M/_\equiv$ der Quotientenhomom. Dann ist für einen Homom $f: M \to N$ äquivalent:

1. Für alle $a, b \in M$ mit $a \equiv b$ gilt $f(a) = f(b)$
2. Es existiert ein Homom $\bar{f}: M/_\equiv \to N$ sodass $f = \bar{f} \circ \pi$

Kanonische Faktorisierung: Jeder Homom $f: M \to N$ zwischen zwei Magmen M, N faktorisiert gemäß
$$f : M \xrightarrow{\pi} M/_{\ker(f)} \xrightarrow{\bar{f}} f(M) \xrightarrow{\iota} N$$
π: Projektion, ι: Inklusion, $\bar{f}$: Iso

Ringe und Körper

Grundstrukturen

Axiome: 0: Kommutativität, 1: Assoziativität, 2: Neutrales Element, 3: Inverses Element, D: Distributivität

	A0	A1	A2	A3	D	M0	M1	M2	M3	$1 \neq 0$	Beispiele
Ring	X	X	X	X	X		X	X			$\mathbb{Z}^{n \times n}, \{0\}$
Kommutativer Ring	X	X	X	X	X	X	X	X			$\mathbb{Z}$
Divisionsring /	X	X	X	X	X		X	X	X	X	$\mathbb{H}$
Schiefkörper											
Körper	X	X	X	X	X	X	X	X	X	X	$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
Halbring	X	X	X		X		X	X			$\mathbb{N}^{n \times n}$
Komm. Halbring	X	X	X		X	X	X	X			$\mathbb{N}$

Ringe

Satz von Cayley: Jeder Ring ist isomorph zu einem Unterring des Endomorphismenrings $(End(A), +, \circ)$ einer geeigneten abelschen Gruppe $(A, +) = (R, +)$ gewählt werden.

Bemerkung: $1 = 0$ kann nur im Nullring $\{0\}$ gelten da $a = 1a = 0a = 0$.

Invertierbare Elemente: werden Einheiten genannt (geschrieben $R^\times$)

- Ring: Gruppenhomomorphismus (+) und Monoidhomomorphismus (·)
- Körper: Def wie bei Ringen, jeder Körperhomomorphismus ist injektiv
- R-Moduln: Gruppenhomomorphismus + $f(ax) = af(x)$ für $a \in R$
- Endomorphismus: Homomorphismus in sich selbst, Auto: Iso in sich selbst

Beispiele

- $exp: (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ und $log: (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ sind inverse Gruppen- (also auch Monoid- und Magma-) isomorphismen

Kategorie

Kategorie ist sowas wie ein Monoid:

1. Für X ist id_X ein Homomorphismus
2. Sind f, g Homomorphismen (zwischen verschiedenen Objekten), so auch $g \circ f$
3. $\circ$ ist assoziativ

Magma

Untermagma: $U \subset M$ ist Untermagma, wenn $U * U \subset U$

Satz: Für einen Homomorphismus $f: M \to N$ gilt

1. Für $A \subset M$ Untermagma ist $f(A) \subset N$ Untermagma
Beweis: Sei $x, y \in f(A)$ also $x = f(u)$ und $y = f(v)$. Dann ist $x \cdot y = f(u * v) \in f(A)$
2. Für $B \subset N$ Untermagma ist $f^{-1}(B) \subset M$ Untermagma
Beweis: Sei $x, y \in f^{-1}(B)$ also $f(x), f(y) \in B$. Dann $f(x * y) = f(x) \cdot f(y) \in B$ also $x * y \in f^{-1}(B)$.

Monoid

Untermonoid: $U \subset M$ ist Untermonoid, wenn $U * U \subset U$ und $e_M \in U$

Erzeugtes Untermonoid: Sei $X \subset M$, dann ist $<X>^+$ das kleinste Untermonoid von M das X enthält. Es gilt:
$$< X >^+ = \{x_1^{e_1} \cdots x_n^{e_n}\}$$
Zum Beispiel: $<3,5>^+ = 3\mathbb{N} + 5\mathbb{N} = \{0, 3, 5, 6, 8, 9, 10, 11, 12, ...\}$

Zyklisches Monoid: bedeutet, das Monoid wird von einem Element erzeugt, zum Beispiel $(\mathbb{N}, +) = <1>^+$.

Satz von Cayley: Jedes Monoid $(M, *)$ ist isomorph zu einem Untermonoid von $Abb(X)$ für eine geeignete Menge X, wobei $X = M$ gewählt werden kann.
Beweis: Man kann jedem $m \in M$ das Element $\lambda_m \in Abb(M), \lambda_m(x) = m * x$ zuordnen. Zu zeigen: Die Zuordnung $m \mapsto \lambda_m$ ist ein Isomorphismus, d.h.

- $m * n \mapsto \lambda_m \circ \lambda_n$ bzw $\lambda_{m*n} = \lambda_m \circ \lambda_n$
- $e \mapsto id$
- Surjektiv nach Def., Injektiv: $\lambda_m \equiv 0 \Rightarrow m = 0$

Gruppe

Inverse Elemente Von einem Monoid M sind $M^\times$ die invertierbaren Elemente. Die Assoziativität garantiert die Eindeutigkeit des Inversen:
Angenommen, $a * b = e$ und $b' * a = e$ dann $b = (b' * a) * b = b' * (a * b) = b'$

Beispiel: Lineare Gruppen

- Allgemeine lin. Grp.: $GL_n(\mathbb{R}) = (\mathbb{R}^{n \times n})^\times$
- Spezielle lin. Grp.: $SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : \det(M) = 1\}$
- Orthogonale Grp.: $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : \det(M) = \pm 1, M \cdot M^t = E\}$
- Spezielle orthogonale Grp. / Drehgruppe: $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$

Untergruppe $U \subset G$ ist Untergruppe (geschrieben $U < G$), wenn $U * U \subset U$ und $e_G \in U$ und $U^{-1} \subset U$
Äquivalent: U nicht leer und $U * U^{-1} \subset U$
Beispiele: $\{e\}$ und G sind die trivialen Untergruppen, Bild und Kern von Homoms sind Untergruppen.

Beispiel: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q}^*$

Satz: R ist Divisionsring dann und nur dann wenn $R^\times = R^*$. Beweis:

- $R^* \subset R^\times$ genau dann wenn jedes Element $\neq 0$ invertierbar ist (M3)
- $R^\times \subset R^*$ genau dann wenn $1 \neq 0$
Hinrichtung: GA $1 = 0 \Rightarrow$ Nullring $\Rightarrow 0 \in R^\times$ (Widerspruch)
Rückrichtung: $0 \notin R^\times$

Nullteiler: Gilt $a \neq 0$, $b \neq 0$, aber $ab = 0$, dann ist a Linksnullteiler und b Rechtsnullteiler. Ist R kommutativ, sagt man einfach Nullteiler.

Beispiel: $2 \cdot 3 = 0$ in $\mathbb{Z}/6$

Nullteilerfrei Ein Ring ist nullteilerfrei, wenn gilt $R^* \cdot R^* \subset R^*$
Ein Ring mit $1 \neq 0$ ist genau dann nullteilerfrei, wenn R^* Untermonoid von $(R, \cdot)$ ist.

Beispiel: Jeder Körper oder Divisionsring ist nullteilerfrei.

Integritätsring ist ein kommutativer, nullteilerfreier Ring mit $1 \neq 0$.

Satz: In nullteilerfreien Ringen kann man kürzen

Satz: Jeder endliche Integritätsring ist ein Körper

Unterring: $S \subset (R, +, \cdot)$ ist Unterring wenn S Untergruppe von $(R, +)$ und Untermonoid von $(R, \cdot)$ ist.
Alternativ wenn $1 \in S$, $S - S \subset S$, $S \cdot S \subset S$

Beispiel: $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$.

Unterkörper: Ein Unterring ist ein Unterkörper, wenn er ein Körper ist.
Alternativ: Wenn R schon ein Körper ist, ist ein Unterring ein Körper wenn $a^{-1} \in S$.

Bruchkörper

Definition: Sei R ein Integritätsring. Ein Bruchkörper von R ist ein Körper K zusammen mit einem injektiven Ringhomomorphismus $\iota: R \to K$ sodass für $x \in K$ gilt $x = \iota(a) \cdot \iota(b)^{-1}$ mit $a \in R$, $b \in R^*$.

Universelle Eigenschaft: Ist $f: R \to L$ ein injektiver Ringhomomorphismus in einen Körper L, dann existiert genau ein Körperhomomorphismus $\bar{f}: K \to L$ mit $f = \bar{f} \circ \iota$.
$\bar{f}$ ist gegeben durch $\bar{f}(\frac{a}{b}) = \frac{f(a)}{f(b)}$

Satz: Je zwei Bruchkörper sind kanonisch isomorph. Siehe Bild ((REFERENCE: fig:bruch)).

Konstruktion: Auf der Menge $\bar{K} = R \times R^*$ definiert man $(a, b) + (c, d) = (ad + bc, bd)$ und $(a, b) \cdot (c, d) = (ac, bd)$ und die Äquivalenzrelation $(a, b) \equiv (c, d) \Leftrightarrow ad = bc$. Der Bruchkörper ist dann $K = \bar{K}/_\equiv$.

Ideal

Definition: $I \subset R$ heißt Ideal ($I \lhd R$) wenn gilt:

1. $0 \in I$, $I + I \subset I$
2. $RI \subset I$ und $IR \subset I$ Beispiele: $\{0\}$, R: triviale Ideale. Kerne von Ringhomomomorphismen.

Bemerkung: Divisionsringe haben nur die trivialen Ideale.

Satz: Ein kommutativer Ring ist genau dann ein Körper, wenn er nur die trivialen Ideale besitzt.

Satz: $I \lhd R$. R/I ist wieder ein Ring (eindeutige Struktur) und die Projektion ist ein Ringhomomorphismus.

Satz: $\mathbb{Z}/n$ ist ein Körper dann und nur dann wenn n eine Primzahl ist.
Falls n nicht prim, dann $n = pq$ also $\bar{p}\bar{q} = 0$. Falls n prim ist, ist $\mathbb{Z}/n$ nullteilerfrei, also ein endlicher Integritätsring, also ein Körper.

Homomorphiesatz: Sei $I \lhd R$ und π die Projektion auf R/I. Für jeden Ringhomomorphismus $f: R \to S$ sind äquivalent:

1. $I \subset \ker(f)$

2. $\exists$ Ringhomom $\bar{f}:R/_I \to S$ mit $f=\bar{f}\circ\pi$

Kanonische Faktorisierung: Jeder Ringhomom $f:R\to S$ faktorisiert gemäß

$$f : R \xrightarrow{\pi} R/_{\ker(f)} \xrightarrow{\bar{f}} f(R) \xrightarrow{\iota} S$$

Isomorphiesatz: Sei $f:R\to S$ surjektiver Ringhomom.

1. Das Bild eines Ideals $I \lhd R$ ist ein Ideal $f(I) \lhd S$.
2. Das Urbild eines Ideals $J \lhd S$ ist ein Ideal $f^{-1}(J) \lhd R$.
3. Das gibt eine Bijektion zwischen den Idealen $\ker(f) \lhd I \lhd R$ und den Idealen $J \lhd S$.
4. f induziert einen Ringhomomorphismus $R/_I \cong S/_{f(I)}$
5. Für jeden Quotientenring $S=R/_K$ und $K \subset I \lhd R$ gilt demnach $R/_I \cong (R/_K)/(I/_K)$

Charakteristik: Es existiert genau ein Ringhomomorphismus $\varphi:\mathbb{Z}\to R$.
Sei *(Anmerkung: Möglich, weil $\mathbb{Z}$ HIR ist)* $\ker(\varphi)=(n), n\in\mathbb{N}$. Die Charakteristik des Rings R ist $char(R)=n$.

Beispiel: $char(\mathbb{Z})=0$, $char(\mathbb{Z}/_n)=n$

Satz: Für jeden nullteilerfreien Ring gilt: Entweder $char(R)=0$ (R Körper $\Rightarrow$ Primkörper ist isomorph zu $\mathbb{Q}$) oder $char(R)$ ist eine Primzahl (R Körper $\Rightarrow$ Primkörper ist isomorph zu $\mathbb{Z}/_p$).

Frobenius-Homomorphismus: Sei R ein kommutativer Ring mit $char=p$ (Primzahl). Dann ist $f:R\to R, x\mapsto x^p$ ein Ringhomomorphismus. Wenn R ein endlicher Körper ist, ist f ein Automorphismus *(Anmerkung: Körperhomos sind injektiv)*.

Kleiner Satz von Fermat: Für alle $a\in\mathbb{Z}$ und Primzahlen p gilt $a^p \equiv a$ (mod p).

Teilerfremd: Zwei Ideale heißen Teilerfremd, wenn $I+J=R$ gilt.

Chinesischer Restsatz: Seien $I_1,\dots,I_n \lhd R$ paarweise teilerfremd, R kommutativ. Dann haben wir einen Ringisomorphismus:

$$R/_{I_1\cdots I_n} \longrightarrow R/_{I_1} \times \cdots \times R/_{I_n} \quad : \quad z+(I_1\cdots I_n) \mapsto (z+I_1,\dots,z+I_n)$$

Monoidring

Definition: Sei $(R,+,\cdot)$ ein kommutativer Ring und $(M,\cdot)$ ein Monoid. Wir nennen $(S,+,\cdot)$ Monoidring von M über R wenn gilt:

1. R ist Unterring im Zentrum von S
2. M ist Untermonoid von $(S,\cdot)$
3. Jedes $s\in S$ schreibt sich eindeutig als Linearkombination $s=\sum_{m\in M} r_m\cdot m$ wobei $r:M\to R, m\mapsto r_m$ endlichen Träger hat.

Universelle Eigenschaft: Sei S' ein Ring, $f:R\to S'$ ein Ringhomom in das Zentrum, $g:M\to S'$ ein Monoidhomom in $(S',\cdot)$. Dann $\exists! h:S\to S'$ Ringhomomorphismus, sodass $h|_R=f$ und $h|_M=g$.
Und zwar: $h(s)=\sum_{m\in M} f(r_m)\cdot g(m)$

Satz: Je zwei Monoidringe von M über R sind kanonisch isomorph. Denn: Pfeile umdrehen.

Konstruktion: Betrachte $S=R^{(M)}$ (Abbildungen $M\to R$, gleichbedeutend mit Koeffizienten r_m) mit den Verknüpfungen $(r+r')_m=r_m+r'_m$ und $(r\cdot r')_m=\sum_{a,b\in M, a\cdot b=m} r_a\cdot r'_b$

Satz: Es gilt $R[X_1\cdots X_{d-1}][X_d]=R[X_1\cdots X_d]$.

Polynomringe

Definition: Sei K ein kommutativer Ring. Ein kommutativer Ring R heißt Polynomring in der Variablen X über K wenn gilt:

- R enthält K als Unterring, $X\in R$
- Jedes $P\in R$ schreibt sich eindeutig als $a_0+a_1X+\dots+a_nX^n$ ($a_n\neq 0$) $a_n=lc(P)$ heißt Leitkoeffizient und $n=deg(P)$ heißt Grad des Polynoms P ($deg(0)=-\infty$)

$$5 = (-X^2+2X+1)(X^2+1) + (X-2)(X^3-2)$$

Gleichung in $\mathbb{Z}^2$ lösen

1. Ausklammern, evtl sieht man: keine Lösung
2. Erweiterter eukl. Algorithmus (ggf dann Gleichung erweitern) $\Rightarrow$ Partikulärlösung
3. Alle Lösungen = Homogene Lösungen + Partikulärlösung

Hauptidealringe

Definition: Ein Hauptideal in einem Ring R ist ein Ideal der Form $(a)=aR$ mit $a\in R$. Ein Integritätsring R heißt Hauptidealring wenn jedes Ideal in R ein Hauptideal ist.

Beispiel: $\mathbb{Z}$.

Satz: Jeder euklidische Ring ist ein HIR. Beweis: Teilen mit Rest

Faktorieller Ring

Irreduzible Elemente: Ein Element $a\in R$ (Integritätsring) heißt irreduzibel wenn gilt: Aus $a=bc$ folgt entweder $b\sim 1$ oder $c\sim 1$. (Invertierbare Elemente und 0 sind nicht irreduzibel)

Definition: Ein Integritätsring R heißt faktoriell, wenn jedes $a\in R^*$ eine eindeutige Zerlegung in irreduzible Faktoren erlaubt.

Beispiel: $\mathbb{Z}$, $K[X]$ (K: Körper)

Satz: Wenn man ein Element aus einem faktoriellen Ring in seine irreduziblen Faktoren zerlegt, sind die Teiler des Elements genau die Produkte der Faktoren.

Definition: Ein Element $a\in R\setminus R^\times$ heißt prim, wenn gilt: Aus $a|bc$ folgt $a|b$ oder $a|c$.

Beispiel: In einem Integritätsring ist 0 immer prim.

Satz: In einem Integritätsring ist jedes Primelement $\neq 0$ irreduzibel.

Satz (Lemma von Euklid): In einem HIR ist jedes irreduzible Element prim.

Satz: Sei in einem Integritätsring jedes irreduzible Element prim. Dann sind Zerlegungen in irreduzible Faktoren eindeutig.

Noethersche Ringe

Satz: Wenn $a_0\in R$ keine Zerlegung in irred. Faktoren erlaubt, dann gibt es eine unendliche aufsteigende Kette von Idealen $(a_0)\subsetneq(a_1)\subsetneq\dots$ in R.

Definition: Ein Ring R heißt noethersch wenn jede aufsteigende Kette von Idealen in R stationär ist.

Satz: Jeder HIR ist noethersch und damit auch faktoriell.

Teilerfremdheit und Invertierbarkeit

Definition: In einem Int.ring R heißen 2 Elemente teilerfremd wenn $ggT(a,b)=R^\times$.

Satz: Ist R ein HIR, dann ist $\bar{a}$ genau dann in $R/_{(b)}$ invertierbar, wenn a und b teilerfremd sind.

Beispiel: Invertieren Invertiere 5 in $\mathbb{Z}/_7$, d.h. suche u,v sodass $5u+7v=1$. Da $5,7$ teilerfremd sind, ist 1 der ggT und man findet u,v mit dem erweiterten euklidischen Algorithmus.

Primideal

Saftinition: Für $I \lhd R$ sind äquivalent:

1. Der Quotient $R/_I$ ist ein Integritätsring
2. Es gilt $I\neq R$ und aus $ab\in I$ folgt $a\in I$ oder $b\in I$ Dann heißt I Primideal von R.

Beispiel $(2)\lhd\mathbb{Z}$ ist Primideal. Denn: $\mathbb{Z}/_2$ ist Int.ring und aus $ab\in(2)$ folgt $a\in(2)$ oder $b\in(2)$.

Satz: $p\in R$ ist Primelement wenn $(p)\lhd R$ Primideal ist.

Universelle Eigenschaft: Sei $\varphi:K\to R$ ein Homomorphismus und $x\in R$. Dann existiert genau ein Ringhomomorphismus $\tilde{\varphi}:K[X]\to R$ mit $\tilde{\varphi}|_K=\varphi$ und $\tilde{\varphi}(X)=x$, nämlich:

$$\tilde{\varphi}(a_0+a_1X+\dots) = \varphi(a_0)+\varphi(a_1)\cdot x+\dots$$

Für $\varphi=id$ ist das das Einsetzen von x in P: $\tilde{id}(P)=P(x)\in K$

Eigenschaften vom Grad Der Grad $deg:K[X]\to\mathbb{N}\cup\{-\infty\}$ hat folgende Eigenschaften:

1. Für $P,Q\in K[X]$ gilt: $deg(P+Q)\leq\sup\{deg(P),deg(Q)\}$
   Gleichheit: $deg(P)\neq deg(Q)$ oder $lc(P)+lc(Q)\neq 0$
2. $deg(PQ)\leq deg(P)+deg(Q)$
   Gleichheit: $P=0$, $Q=0$ oder $lc(P)\cdot lc(Q)\neq 0$. Dann: $lc(PQ)=lc(P)\cdot lc(Q)$
   Zum Beispiel wenn K nullteilerfrei ist (genau dann wenn $K[X]$ nt-frei)

Satz: Für jeden Integritätsring K gilt $K[X]^\times=K^\times$

Beispiel: Polynomdivision mit Rest:

```
(5X^2+  X-  1) : (X+2) = 5X - 9   Rest: 17
-(5X^2+ 10X)
------------
       -9X-  1
     -(-9X- 18)
     ----------
              17
```

Satz: Sei $P\in K[X]$ Polynom von Grad n und $lc(P)\in K^\times$. Dann: $K[X]_{<n}\cong K[X]/_{(P)}$.

Satz: In einem Integritätsring ist für jedes Polynom $P\in K[X]^*$ die Zerlegung in Linearfaktoren eindeutig (bis auf Reihenfolge). D.h. ein Polynom von Grad n hat maximal n Nullstellen.

Satz: Ein Element $a\in K$ ist dann und nur dann mehrfache Nullstelle von P in $K[X]^*$ wenn a eine gemeinsame Nullstelle von P und der Ableitung P' ist.

Beispiel: X^p-X hat keine mehrfachen Nullstellen in $\mathbb{Z}/_p$.

Teilbarkeitstheorie in Integritätsringen

Assoziierte Elemente: $ab\in R$ heißen assoziert ($a\sim b$) wenn es $u\in R^\times$ gibt sodass $au=b$.
Es gilt $(a)=(b)$ genau dann wenn $a\sim b$.

Teilbarkeit: b teilt a (geschrieben $b|a$) wenn es $c\in R$ gibt mit $a=bc$
Es gilt $(a)\subset(b)$ genau dann wenn $b|a$.

GGT: Die Menge der gemeinsamen Teiler von $a_1,\dots,a_n\in R$ ist:

$$GT(a_1,\dots,a_n) = \{t\in R : t|a_1,\dots,t|a_n\}$$
$$GGT(a_1,\dots,a_n) = \{t\in GT(a_1,\dots,a_n) : \forall_{s\in GT} s|t\}$$

Wenn d ein ggT ist, dann auch alle Assoziierten von d. Wenn es 2 ggT gibt, sind sie assoziert.

Euklidische Ringe

Definition: Eine euklidische Division ("Division mit Rest") auf dem Ring R ist gegeben durch eine Funktion $\nu:R\to\mathbb{N}$ mit $\nu(0)=0$ und eine Abbildung $\delta:R\times R^*\to R\times R$ mit $(a,b)\mapsto(q,r)$ sodass $a=bq+r$ mit $\nu(r)<\nu(b)$. Ein euklidischer Ring besteht aus einem Integritätsring mit einer euklidischen Division.

Beispiel: $K[X]$, $\mathbb{N}$, $\mathbb{Z}[i]$

Bsp: Erweiterter Euklidischer Algorithmus ggT von X^2+1 und X^3-2 in $\mathbb{Q}[X]$:

- $X^3-2=X(X^2+1)+(-X-2)$
- $X^2+1=(-X+2)(-X-2)+5$
- $-X-2=5(-\frac{X}{5}-\frac{2}{5})+0$ Also ist der ggT 5 und: $5=(X^2+1)-(-X+2)(-X-2)$ und mit $(-X-2)=(X^3-2)-X(X^2+1)$:

Maximales Ideal

Saftinition: Für $I\lhd R$ sind äquivalent:

1. Der Quotient $R/_I$ ist ein Körper
2. Für jedes Ideal $J\lhd R$, $I\subset J\subset R$ gilt entweder $I=J$ oder $J=R$. Dann ist I maximales Ideal von R.

Satz: In einem HIR ist jedes Primideal maximal

Satz: Sei R ein HIR, $p\in R^*$. Dann ist $R/_{(p)}$ genau dann ein Körper, wenn p irred. ist.

Primfaktorzerlegung in Polynomringen

Man muss immer ein Repräsentantensystem irreduzibler Elemente $\mathcal{P}$ wählen.

Definition: Die Primfaktorzerlegung von einem Element hat die Form

$$x = u\cdot\prod_{p\in\mathcal{P}} p^{e_p} \quad , u\in R^\times$$

$u=lu(x)$ heißt Leiteinheit, $e_p(x)$ ist die Exponentenbewertung.
Ein Integritätsring ist genau dann faktoriell, wenn die Zuordnung von x zu $\{u,e_p\}$ bijektiv ist.

Satz: Sei R ein Integritätsring. Ist $R[X]$ faktoriell dann auch R.

Definition: $x\in R^*$ ist normiert bzgl $\mathcal{P}$ wenn $lu(x)=1$ ist.

Definition: Der Inhalt eines Polynoms $P=a_0+a_1X+\dots$ ist $cont(P)=ggT(a_0,a_1,\dots)$
$P\in R[X]^\times$ ist primitiv, wenn $cont(P)=1$ ist. $P/cont(P)$ ist immer primitiv.
$P\in R[X]$ ist normiert, wenn $lu(P):=lu(lc(P))=1$

Satz: Sind $P,Q\in R[X]^*$ primitiv, dann ist auch PQ primitiv.

Satz: Zu jedem Polynom $P\in R[X]^\times$ existiert genau ein $a\in R^*$ und $P_1\in R[X]$ sodass $P=aP_1$ gilt und P_1 normiert und primitiv ist. Es ist $a=lu(P)\cdot cont(P)$.

Beispiel: $P=-6X^3+15X+12 \Rightarrow P=(-1)\cdot 3\cdot(2X^3-5X-4)$

Satz: Zu jedem Polynom $P\in K[X]^\times$ (K ist der Bruchkörper) existiert genau ein $c\in K^*$ und $P_1\in R[X]$ sodass $P=cP_1$ gilt und P_1 normiert und primitiv ist. $c\in R^* \Leftrightarrow P\in R[X]^*$

Beispiel: $P=-\frac{3}{5}X^3+\frac{3}{2}X+\frac{6}{5} \Rightarrow 10P=-6X^3+15X+12 \Rightarrow P_1=(-\frac{10}{3})P$

Definition: $red(P)=P_1$, $scal(P)=c$

Satz: Seien $P,Q\in K[X]$ mit $lc(P)=lc(Q)=1$. Aus $PQ\in R[X]$ folgt $P,Q\in R[X]$.

Satz von Gauß: Ist R ein faktorieller Ring, so ist auch $R[X]$ faktoriell.

Beispiel: Berechnung des ggT in $\mathbb{Z}[X]$ $P=24X^3-81$, $Q=24X^2-72X+54$

1. $c=ggT(cont(P),cont(Q))=3$
2. P, Q reduzieren $\Rightarrow P'=8X^3-27$, $Q'=4X^2-12X+9$
3. Euklidscher Algorithmus $\Rightarrow ggT_{\mathbb{Q}[X]}(P',Q')=54X-81$
4. Reduzieren: $54X-81=27\cdot(2X-3)$
5. $ggT_{\mathbb{Z}[X]}(P,Q)=c\cdot red(ggT_{\mathbb{Q}[X]}(P',Q'))=3\cdot(2X-3)=6X-9$

Irreduzibilitätskriterien

Satz: Für $P\in R[X]$ über einem faktoriellen Ring R sind äquivalent:

1. P ist in $R[X]$ irreduzibel und $deg(P)\geq 1$
2. P ist in $K[X]$ irreduzibel und $cont(P)=1$

Satz: Sei $P\in K[X]$ ein Polynom vom Grad 2 oder 3. Dann ist P genau dann irreduzibel in $K[X]$ wenn P keine Nullstelle in K hat.

Beispiel: $P=X^2-2$ ist irred. über $\mathbb{Q}$, aber $P=(X-\sqrt{2})(X+\sqrt{2})$ über $\mathbb{R}$ zerlegbar
Wenn $x=\frac{a}{b}\in K$ eine Nullstelle von $P=c_0+\ldots+c_nX^n$ ist, dann gilt $a|c_0$ und $b|c_n$

Satz (Abbildungskriterium): Sei $\varphi:R\to S$ ein Homom zwischen Integritätsringen, fortgesetzt zu $\Phi:R[X]\to S[X]$. Sei $P\in R[X]$ primitiv und $\varphi(lcP)\neq 0$. Falls $\Phi(P)$ irred in $S[X]$, dann auch P irred in $R[X]$.

Beispiel: $P=3X^3+5X+7$ in $\mathbb{Z}[X]$ ist primitiv und Reduktion in $\mathbb{Z}/2$ ist X^3+X+1 ist irreduzibel. Also ist auch P irreduzibel.

Satz (Eisenstein): Sei R ein Integritätsring und $P\in R[X]$ mit Grad ≥ 1 mit

1. P ist primitiv
2. Es gibt $p\in R$ prim sodass $p|a_0,\ldots,p|a_{n-1}$ aber $p\nmid a_n$ sowie $p^2\nmid a_0$ (Eisenstein-Polynom) Dann ist P irreduzibel in $R[X]$. Beispiel: X^4-4X^3+6 mit $p=2$

Kreisteilungspolynome: $x^n-1=(x-1)(x-\alpha)\ldots(x-\alpha^{n-1})$, wobei $\alpha=e^{\frac{2\pi i}{n}}$. In Q: $(x^n-1)=(x-1)(x^{n-1}+\ldots+1)$, falls n prim Klammern irred.

Matrizenringe, Elementarteilersatz

Definition: Eine Matrix $D\in K^{m\times n}$ ist in Elementarteilerform, wenn gilt:

1. D ist diagonal, d.h. $d_{ij}=0$ für $i\neq j$
2. Auf der Diagonalen: $d_{11}|d_{22}|\ldots|d_{ll}$ mit $l=\min\{m,n\}$, die d_{ii} heißen Elementarteiler

Inverse einer 2×2-Matrix: Sei $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Dann folgt: $A^{-1}=\frac{1}{\det A}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$.

Algorithmus von Gauß-Bézout

Zeilenoperationen: Sei $d=ggT(x,y)=ux+vy$. Dann:

$$A=\begin{pmatrix}x & *\\ y & *\end{pmatrix},\ S=\begin{pmatrix}u & v\\ -y/d & x/d\end{pmatrix}\ \Rightarrow\ SA=\begin{pmatrix}d & *\\ 0 & *\end{pmatrix}$$

Spaltenoperationen: Sei $d=ggT(x,y)=ux+vy$. Dann:

$$A=\begin{pmatrix}x & y\\ * & \end{pmatrix},\ T=\begin{pmatrix}u & -y/d\\ v & x/d\end{pmatrix}\ \Rightarrow\ AT=\begin{pmatrix}d & 0\\ * & \end{pmatrix}$$

Diagonaloperationen: Sei $d=ggT(x,y)=ux+vy$. Dann:

$$A=\begin{pmatrix}x & 0\\ 0 & y\end{pmatrix},\ S=\begin{pmatrix}u & v\\ -y/d & x/d\end{pmatrix},\ T=\begin{pmatrix}1 & -vy/d\\ 1 & ux/d\end{pmatrix}\ \Rightarrow\ SAT=\begin{pmatrix}d & 0\\ 0 & xy/d\end{pmatrix}$$

Satz: Sei K ein HIR. Zu jeder Matrix $A\in K^{m\times n}$ existieren invertierbare Matrizen $S\in SL_m(K), T\in SL_n(K)$ sodass $D=SAT$ in Elementarteilerform ist. Die Elementarteiler sind eindeutig (bis auf Assoziierte).

Moduln

Definition (Modul): Sei $(R,+,\cdot)$ ein kommutativer Ring. Ein R-Modul $(M,+,*)$ besteht aus einer abelschen Gruppe $(M,+)$ mit einer Operation $*:R\times M\to M, (a,x)\mapsto a*x$ die folgenden Axiomen genügt:

1. $a*(x+y)=a*x+a*y$
2. $(a+b)*x=a*x+b*x$
3. $(a\cdot b)*x=a*(b*x)$
4. $1*x=x$ Falls R nicht kommutativ ist, Unterscheidung von Rechts- und Linksmoduln.

Falls R ein Körper ist, ist M ein Vektorraum.

- Für 5: $1=1$ d.h. $\mathbb{Z}/5$ Die Gruppen mit 360 Elementen sind alle Kombinationen dieser Möglichkeiten, also gibt es $3\cdot 2\cdot 1=6$ Möglichkeiten, z.B. $\mathbb{Z}/2\times\mathbb{Z}/4\times\mathbb{Z}/9\times\mathbb{Z}/5$

Zerlegung in unzerlegbare Moduln Nach dem chinesischen Restsatz ist z.B. $\mathbb{Z}/6\cong\mathbb{Z}/2\times\mathbb{Z}/3$. $\mathbb{Z}/2$ und $\mathbb{Z}/3$ sind unzerlegbar. Allgemeiner: $\mathbb{Z}/p^kq^l\cong\mathbb{Z}/p^k\times\mathbb{Z}/q^l$

Gruppentheorie

Satz: Für Gruppen $K<H<G$ gilt: $|G/K|=|G/H|\cdot|H/K|$
Spezialfall (S.v.Lagrange): Für jede Untergruppe $H<G$ gilt $|G|=|G/H|\cdot|H|$.
$|G/H|$ heißt auch Index $|G:H|$ von H in G

Satz: Sei G endliche Gruppe.

- Die Ordnung $|H|$ jeder Untergruppe $H<G$ teilt die Gruppenordnung $|G|$
- Die Ordnung $ord(x)$ von $x\in G$ teilt die Gruppenordnung $|G|$ Deshalb hat eine Gruppe von Primzahlordnung nur die trivialen Untergruppen und ist zyklisch.

Definition: Eine Untergruppe $K<G$ heißt normal, wenn $aKa^{-1}=K$ (d.h. $aK=Ka$, Rechtsnebenklassen = Linksnebenklassen) für alle $a\in G$ gilt. Geschrieben: $K\triangleleft G$.

Beispiel: Untergruppen von abelschen Gruppen sind normal. Kerne von Gruppenhom. sind normal.

Satz: Für jeden Gruppenhom $f:G\to H$ gilt: $|G|=|ker(f)|\cdot|im(f)|$

Satz: Homomorphiesatz und erster Isomorphiesatz gelten wie sonst immer

2. Isomorphiesatz: Sei G eine Gruppe und seien $H,K<G$ zwei Untergruppen.

1. Aus $H<G$ und $K\triangleleft G$ folgt $HK=KH$
2. Aus $HK=KH$ folgt $HK=KH=\langle H\cup K\rangle$

Satz: Sei G eine Gruppe, $H<G$ und $K\triangleleft G$. Dann gilt $H\cap K\triangleleft H$ und $H/(H\cap K)\cong HK/K$

3. Isomorphiesatz: Sei $K<U<G$ und ($K\triangleleft G$ oder $U\triangleleft G$), dann ist $(G/K)/(U/K)\cong G/U$

Kommutator

Definition: Der Kommutator von $a,b\in G$ ist $[a,b]=aba^{-1}b^{-1}$.
Die von allen Kommutatoren in G erzeugte Untegruppe $[G,G]=\langle[a,b]:a,b\in G\rangle$ heißt Kommutatorgruppe von G

Abelschmachung: $G/[G,G]$ ist abelsch

Lemma: Seien $H,K\leq G$ endliche Gruppen. Dann ist $|H|\cdot|K|=|HK|\cdot|H\cap K|$.

Direkte Produkte: G ist das innere direkte Produkt von H,K wenn $f:H\times K\to G, (a,b)\mapsto ab$ ein Isomorphismus ist. Dann identifizieren wir $H\times K\cong HK=G$

Satz: Für $H,K<G$ sind äquivalent

1. G ist das innere direkte Produkt von H und K
2. $HK=G$ und $H\cap G=\{1\}$ und $[H,K]=\{1\}$
3. $HK=G$ und $H\cap G=\{1\}$ und $H,K\triangleleft G$

Zyklische Gruppen

Satz: Die Gruppe G wird genau dann von $g\in G$ erzeugt, wenn der der Hom $\mathbb{Z}\to G, k\mapsto g^k$ surjektiv ist. (Additive Schreibweise: $k\mapsto k\cdot g$)

Satz: Jede Untergruppe $H<\mathbb{Z}$ ist zyklisch.
Jede zyklische Gruppe G ist isomorph zu $\mathbb{Z}/n$.
Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Die Untergruppen von $\mathbb{Z}/n$ sind genau $(m\mathbb{Z})/n$ für $m|n$

Satz: Jede zyklische Gruppe der Ordnung n hat für jeden Teiler m von n genau eine Untergruppe vom Index m

Restsatz: Falls $m,n\in\mathbb{Z}$ teilerfremd sind, existiert ein Gruppeniso $\mathbb{Z}/mn\cong\mathbb{Z}/m\times\mathbb{Z}/n$.

Beispiel: $(\mathbb{Z}/n,+)$ ist ein $\mathbb{Z}$-Modul. Der Polynomring $R[X]$ ist ein R-Modul. Jedes Linksideal ist ein Linksmodul.

Definition: Sei M ein R-Modul. $U\subset M$ heißt Untermodul über R falls U eine Untergruppe von $(M,+)$ ist und $RU=U$ gilt.

Beispiel: Jeder kommutative Ring ist Modul über sich selbst. Die Untermoduln sind genau die Ideale.

Torsion: Sei K ein Integritätsring und M ein K-Modul. $x\in M$ heißt Torsionselement wenn $\exists a\in K^*$ mit $ax=0$.

Beispiel: $1\in\mathbb{Z}/2$ ist ein Torsionselement im $\mathbb{Z}$-Modul $\mathbb{Z}/2$ da $2\cdot 1=0$.

Definition: Ein R-Modul M heißt einfach, wenn für jeden Untermodul U entweder $U=\{0\}$ oder $U=M$ gilt.

Beispiel: $\mathbb{Z}/n$ ist genau dann einfach, wenn n eine Primzahl ist. (Gilt allg in HIR)
Ein Modul heißt unzerlegbar, wenn für jede direkte Summe *(Anmerkung: $A+B=M$ und $A\cap B=\{0\}$)* $M=A\oplus B$ entweder $A=0$ oder $B=0$ gilt.

Beispiel: $\mathbb{Z}/p^k$ ist unzerlegbar für p prim, aber $\mathbb{Z}/ab=\mathbb{Z}/a\times\mathbb{Z}/b$ wenn $ggT(a,b)=1$ (Restsatz).

Satz: Homo- und Isomorphiesätze gelten wie in Ringen mit Idealen (da Untermodul = Ideal)

Freie Moduln

Definition: $X\subset M$ heißt Basis des R-Moduls M, wenn X ein Erzeugendensystem und linear unabhängig ist. Wenn M eine Basis hat, heißt M frei über R.

Beispiel: $\mathbb{Z}^n$ ist frei, $\mathbb{Z}/n$ ist nicht frei (als $\mathbb{Z}$-Modul), allgemein: R^n ist frei über R

Matrizen: Homomorphismen zwischen freien Moduln können als Matrix geschrieben werden.

Definition: Bei Moduln über Hauptidealringen sind alle Basen gleich groß, die Größe heißt Rang des Moduls (bei Vektorräumen: Dimension).

Satz: Sei K ein HIR. Jeder K-Untermodul $U<K^m$ ist frei und erfüllt $rang_K(U)\leq m$
Bei beliebigen Ringen gelten beide Eigenschaften nicht notwendigerweise.

Satz: Sei M ein endlich erzeugter K-Modul. Dann ist auch jeder Untermodul über K endlich erzeugt.

Elementarteilersatz: Sei K ein HIR und sei M ein freier K-Modul vom Rang m. Für jeden Untermodul $U\subset M$ existiert

1. eine Basis $b_1,\ldots,b_m$ von M
2. Elemente $a_1,\ldots,a_n\in K^*$ mit $a_1|\ldots|a_n$ sodass $a_1b_1,\ldots,a_nb_n$ eine Basis von U ist. Die a_i sind eindeutig durch U bestimmt und heißen Elementarteiler von U.

Das heißt auch, wenn U,U' zwei Untermoduln sind, existiert genau dann ein Automorphismus $f:M\to M$ mit $f|_U=U'$ wenn die Elementarteiler übereinstimmen.

Satz: Sei K ein HIR. Zu jedem endlich erzeugten K-Modul M existiert ein K-Isomorphismus

$$M\cong K/(a_1)\times\cdots\times K/(a_n)\times K^r$$

wobei $r\in\mathbb{N}$ (Rang des freien Anteils) und $a_1,\ldots,a_n\in K^*\backslash K^\times$ mit $a_1|\ldots|a_n$ (Elementarteiler) eindeutig.

Satz: Über einem HIR K zerlegt sich jeder endlich erzeugte K-Modul M gemäß $M=T\oplus F$ in den Torsionsmodul $T<M$ (eindeutig) und einen freien Modul $F<M$.

Endliche abelsche Gruppen

Um eine Liste der verschiedenen abelschen Gruppen der Ordnung n zu finden, zerlegt man n in Primfaktoren und betrachtet wie man die Exponenten als Summe schreiben kann.

Beispiel: abelsche Gruppen mit $360=2^3\cdot 3^2\cdot 5$ Elementen.

- Für 2: $3=1+1+1=1+2=3$ d.h. $\mathbb{Z}/2\times\mathbb{Z}/2\times\mathbb{Z}/2$ oder $\mathbb{Z}/2\times\mathbb{Z}/2^2$ oder $\mathbb{Z}/2^3$
- Für 3: $2=1+1=2$ d.h. $\mathbb{Z}/3\times\mathbb{Z}/3$ oder $\mathbb{Z}/3^2$

Satz: $\bar{a}$ erzeugt $\mathbb{Z}/n$ wenn $ggT(a,n)=1$ gilt

Beispiel: 3 erzeugt $\mathbb{Z}/4$ weil $3+3=2$, $3+3+3=1$, $3+3+3+3=0$ alle Elemente sind.

Satz: Wenn p eine Primzahl ist, hat $(\mathbb{Z}/p)^\times$ Ordnung $p-1$ und ist zyklisch.

Konjugation

Definition: Das Zentrum einer Gruppe G ist das was mit allem kommutiert:

$$Z(G)=\{z\in G: za=az\ \ \forall a\in G\}\triangleleft G$$

Der Zentralisator eines Elements a sind alle Elemente, die mit a kommutieren:

$$Z(G)<Z_G(a)=\{b\in G: ab=ba\}<G$$

Der Zentralisator existiert auch für Untergruppen (nicht nur einzelne Elemente)

Definition: Für $c\in G$ definieren wir die Linkskonjugation $\gamma_c:G\to G, g\mapsto cgc^{-1}=:{}^cg$ und Rechtskonjugation $\delta_c:G\to G, g\mapsto c^{-1}gc=:g^c$

Satz: Es gilt $\gamma_c\in Aut(G)$, $\gamma:c\mapsto\gamma_c$ ist ein Gruppenhom mit $ker(\gamma)=Z(G)$

Definition: $Inn(G)=\gamma(G)\triangleleft Aut(G)$, $Out(G)=Aut(G)/Inn(G)$

Definition: Der Normalisator einer Untergruppe $U<G$ ist das was U unter Konjugation invariant lässt:

$$U\triangleleft N_G(U)=\{g\in G: U^g=U\}$$

Bemerkung: $Z_G(U)<N_G(U)$

Definition: $U<G$ heißt charakteristisch, wenn für alle $\alpha\in Aut(G)$ gilt dass $\alpha(U)=U$.

Operation

Definition: Sei G eine Gruppe und X eine Menge. Eine Operation von G auf X ist eine Abbildung $(a,x)\mapsto a*x$ sodass

$$(a\cdot b)*x=a*(b*x)\ \text{und}\ 1*x=x$$

Es gibt auch Rechtsoperationen.

Definition: Die Bahn / der Orbit von $x\in X$ ist $Gx=\{gx:g\in G\}$
Die Standgruppe / der Stabilisator von x ist $G_x=\{g\in G:gx=x\}$
Die Fixpunkte der Operation sind $Fix(G)=\{x\in X:Gx=x\}$

Satz: (Bahnengleichung) Für jedes $x\in X$ ist $Gx=|G:G_x|$. Wenn $|G|<\infty$ dann gilt demnach $|G|=|Gx|\cdot|G_x|$, insbesondere $|Gx|$ teilt $|G|$.

Beispiel: G operiert auf sich selbst mit Konjugation, $(x,g)\mapsto g^{-1}xg$.
Die Bahn von x ist die Konjugationsklasse x^G und die Standgruppe ist der Zentralisator $Z_G(x)$.
Die Anzahl der zu x konjugierten Elemente ist $|x^G|=|G:Z_G(x)|$.

Satz (Bahnengleichung): Es gilt

$$X=Fix(G)\sqcup\bigsqcup_{k\in K}Gx_k$$

wobei die k die nicht trivialen Bahnen repräsentieren. Es folgt:

$$|X|=|Fix(G)|+\sum_{k\in K}|G:G_{x_k}|$$

Definition: Eine p-Gruppe ist eine Gruppe mit Ordnung p^e für ein $e\in\mathbb{N}$.

Satz: Jede nicht-triviale p-Gruppe hat nicht-triviales Zentrum.

Satz: Für jede Gruppe der Ordnung p^e existiert eine Kette

$$\{1\} = K_0 < \ldots < K_e = G$$

wobei $K_i \triangleleft G$ die Ordnung p^i hat, d.h. K_i/K_{i+1} ist zyklisch von Primzahlordnung.

Satz: Eine endliche Gruppe G ist genau dann eine p-Gruppe, wenn jedes $x \in G$ ein p-Element ist (d.h. $ord(x)=p^k$)

Symmetrische / Alternierende Gruppen

Definition: Die Fixpunkte einer Permutation $\sigma \in S_X$ sind $Fix(\sigma)=\{x \in X : \sigma(x)=x\}$. Der Träger ist $supp(\sigma)=\{x \in X : \sigma(x) \neq x\}$.
Permutationen heißen disjunkt, wenn $supp(\sigma) \cap supp(\tau)=\emptyset$, disjunkte Perm. kommutieren.

Schreibweise: Eine Permutation in S_n kann zum Beispiel so geschrieben werden:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 5 & 2 & 1 & 7 \end{bmatrix}$$

oder in Zykelschreibweise $\sigma=(1,4,3,8,7)(2,6)$ (disjunkte Zykel immer eindeutig möglich).

Definition: Eine Transposition ist ein 2er-Zykel (i,j).
Die symmetrische Gruppe wird von ihren Transpositionen erzeugt. Sogar schon von den Transpositionen benachbarter Elemente.

Satz: Für $n \geq 3$ hat S_n triviales Zentrum.

Satz: Für alle n gilt $|S_n|=n!$.

Zykel

Definition: Ein Zykel der Länge l ist eine Permutation $\sigma(i_1,\ldots,i_l)$ mit $\sigma(i_k)=i_{k+1}$ und alle anderen Elemente sind fix. Die Ordnung des Zykels ist l.

Satz: Jeder l-Zykel schreibt sich als Produkt von $l-1$ Transpositionen: $(i_1,\ldots,i_l)=(i_1,i_2)\cdots(i_{l-1},i_l)$

Definition: Sei σ ein Produkt disjunkter Zykel der Längen $l_1 \geq l_2 \geq \ldots \geq l_r \geq 2$. Dann ist $(l_1,\ldots,l_r) \in \mathbb{N}^r$ die Zykelstruktur von σ. Verlängert um die Fixpunkte $l_{r+1}=\ldots=l_s=1$ erhält man die Bahnenstruktur. Dies ist eine Partition von n: $\sum l_k = n$
Bemerkung: Die Ordnung von σ ist $ord(\sigma)=kgV(l_1,\ldots,l_r)$.

Satz: Für jeden Zykel $c=(i_1,\ldots,i_l) \in S_n$ und $\tau \in S_n$ gilt:

$$\tau \circ c \circ \tau^{-1} = (\tau(i_1), \ldots, \tau(i_l))$$

Daraus folgt: Zwei Permutationen sind genau dann konjugiert, wenn sie die selbe Zykelstruktur haben.

Satz: Sie $\sigma \in S_n$. In der Bahnenzerlegung von σ treten m_l Bahnen der Länge l auf. Dann hat der Zentralisator von σ die Ordnung:

$$|Z_{S_n}(\sigma)| = m_1! \cdot 1^{m_1} \cdot m_2! \cdot 2^{m_2} \cdot m_3! \cdots m_n! \cdots n^{m_n}$$

Die Konjugationsklasse von σ hat die Ordnung $|\sigma^{S_n}|=|S_n|/|Z_{S_n}|$.

Signatur

Definition:Für $n \geq 2$ existiert genau ein nicht-trivialer Gruppenhom $S_n \to \pm 1$. Diesen nennen wir die Signatur, geschrieben $sign: S_n \to \pm 1$.
Permutationen mit $sign=+1$ heißen gerade, die mit $sign=-1$ heißen ungerade.

Satz: Für einen l-Zykel ist $sign=(-1)^{l-1}$.

Alternierende Gruppe

Definition: Die Menge der geraden Permutationen ist die alternierende Gruppe $A_n = ker\, sign(S_n)$. Für $n=1$ ist A_n trivial, für $n \geq 2$ ist $A_n \triangleleft S_n$ vom Index 2, also $|A_n|=\frac{n!}{2}$.
A_n ist die Kommutatorgruppe von S_n.

Satz: Die alternierende Gruppe wird von ihren 3-Zykeln erzeugt.

Satz: Für jedes $\sigma \in A_n$ gilt

1. Wenn $Z_{S_n}(\sigma) \subset A_n$ dann gilt $Z_{S_n}(\sigma)=Z_{A_n}(\sigma)$ und $\sigma^{S_n}=\sigma^{A_n} \sqcup \sigma^{A_n}(1,2)$
2. Wenn $Z_{S_n}(\sigma) \not\subset A_n$ dann gilt $|Z_{S_n}(\sigma) : Z_{A_n}(\sigma)|=2$ und $\sigma^{A_n}=\sigma^{S_n}$.

Satz: Für $n \geq 5$ sind in A_n alle 3-Zykel konjugiert.

Einfache Gruppen

Definition: Eine Gruppe heißt einfach wenn sie nur die 2 trivialen normalen Untergruppen hat. Äquivalent: G ist einfach, wenn jeder Gruppenhom $f: G \to H$ trivial oder injektiv ist.

Beispiel: S_2

Satz: Jede Gruppe von Primzahlordnung ist einfach (isomorph zu $\mathbb{Z}/p$).
Eine abelsche Gruppe ist genau dann einfach, wenn sie von Primzahlordnung ist.

Satz: Für $n \geq 5$ ist A_n einfach. (außerdem für $n=3$, A_3 ist abelsch)

Satz: Jede einfache Gruppe G mit einer Untergruppe $H<G$ vom Index $n \geq 2$ kann in S_n eingebettet werden. Für $G \not\cong \mathbb{Z}/2$ gilt dann $|G| \leq \frac{n!}{2}$.

Satz: Für $n \geq 5$ enthält A_n keine Untergruppe vom Index $2,3,\ldots,n-1$.

Semidirektes Produkt

Definition: G ist das interne semidirekte Produkt von $K \triangleleft G$ und $H<G$ wenn $KH=G$ und $K \cap H=\{1\}$, geschrieben $G=K \rtimes H$

Beispiel: $S_n = A_n \rtimes \langle (1,2) \rangle$

Internes und externes Produkt: Wir wollen die Verknüpfung von (k_1,h_1) und (k_2,h_2) definieren. Sind $K,H<G$ dann geht das wie folgt durch Einfügen von $h_1^{-1}h_1$:

$$(k_1,h_1) \cdot (k_2,h_2) = (k_1 \underbrace{h_1 k_2 h_1^{-1}}_{\in K}, h_1 h_2)$$

Das heißt internes semidirektes Produkt. Steht die Operation durch Konjugation nicht zur Verfügung, weil nicht $K,H<G$ ist, kann man das ersetzen durch einen beliebigen Gruppenhomomorphismus $\alpha: H \to Aut(K)$ und definieren:

$$(k_1,h_1) \cdot (k_2,h_2) = (k_1 \alpha(h_1)(k_2))(h_1 h_2)$$

Das heißt dann externes semidirektes Produkt ${}_K \overset{\alpha}{\rtimes} H$. Das interne semidirekte Produkt ist also das externe mit der Operation $\tilde{\alpha}(h)(k)=hkh^{-1}$. Für $\alpha=id$ ergibt sich das direkte Produkt.

Beispiel: Die Diedergruppe $D_n = \mathbb{Z}/n \overset{\alpha}{\rtimes} \mathbb{Z}/2$ mit $\alpha: \mathbb{Z}/2 \to Aut(\mathbb{Z}/n), \bar{n} \mapsto (-1)^n$

Satz: Seien $p<q$ zwei Primzahlen. Wenn $p \not| (q-1)$ dann existiert nur ein semidirektes Produkt der Form $\mathbb{Z}/q \rtimes \mathbb{Z}/p$, nämlich das direkte Produkt $\mathbb{Z}/q \times \mathbb{Z}/p$.
Gilt hingegen $p|(q-1)$ dann existiert außerdem ein nicht-triviales semidirektes Produkt. Dieses ist bis auf Isomorphie eindeutig.

Sylow-Sätze

Satz (Cauchy): Teilt eine Primzahl p die Ordnung der Gruppe G dann existiert ein Element $x \in G$ der Ordnung p und damit eine Untergruppe $\langle x \rangle < G$ der Ordnung p.

Definition: Sei p prim. Sei G eine Gruppe der Ordnung $|G|=p^e \cdot a$ mit $e,a \in \mathbb{N}$ und $p \not| a$. Eine p-Sylow-Untergruppe von G ist eine Untergruppe $P<G$ der Ordnung $|P|=p^e$. Die Menge der p-Sylow-Untergruppen bezeichnen wir mit $Syl_p(G)$.

Satz (Sylow): Sei p prim und $|G|=p^e \cdot a$ wie oben. Dann gilt:

1. Jede p-Untergruppe von G liegt in einer p-Sylow-Untergruppe von G. D.h. es existiert mindestens eine p-Sylow-Untergruppe in G.
2. Je zwei p-Sylow-Untergruppen sind in G konjugiert.
3. Ihre Anzahl $m_p=|Syl_p(G)|$ erfüllt $m_p | a$ und $m_p = 1+kp$, $k \in \mathbb{N}$.

Satz: Eine p-Sylow-Gruppe $P \in Syl_p(G)$ ist einzig genau dann, wenn P normal ist in G.

Satz: Sei G eine endliche Gruppe und r die Anzahl der p-Sylowgruppen. Dann gibt es einen Homomorphismus $\varphi: G \to S_r$. (Konjugation *(Anmerkung: Ein $g \in G$ permutiert die Sylowgruppen durch Konjugation, φ ist die Abbildung von g auf diese Permutation)*)
Ist G einfach und φ nicht trivial (nicht $g \mapsto id$ für alle g), so ist φ sogar injektiv, also ist $|G|$ ein Teiler von $r!=|S_r|$.

Satz: Sind $K,H<G$ Untergruppen mit $ggT(|K|,|H|)=1$. Dann ist $K \cap H=\{1\}$. Gilt andererseits $|K|=|H|=p$, so ist entweder $K \cap H=\{1\}$ oder $K=H$.

Satz: Sind $K,H \triangleleft G$ Normalteiler mit $K \cap H=\{1\}$, dann ist $KH \cong K \times H$.

Satz: Wenn K < S_n eine Unterruppe von Index 2 ist, dann gilt K = A_n.

Satz: Wenn es nur eine p-Sylowgruppe in einer Gruppe H gibt, dann ist P ◁ G.

Satz: 1. Sei G eine endliche Gruppe und r die Anzahl der p-Sylowgruppen. Dann gibt es einen Homomorphismus phi:G nach S_r.

2. Ist G einfach und phi nicht trivial, so isr phi sogar injektiv, also |G| ein Teiler von r!=$|S_r|$.

Beispiel: Sei G eine einfache Gruppe der Ordnung $|G|=60$. Zeigen Sie, dass es in G genau zehn 3-Sylowgruppen gibt.
$60=3^1 \cdot 20$, es muss gelten: $m_3 | 20$ und $m_3 = 1+3k$. Daraus folgt $1,4,10$ kommen in Frage.
Zu 1: Dann wäre $P_3 \triangleleft G$, Widerspruch zu $|P_3|=3$ und G einfach
Zu 4: Da G einfach und φ nicht trivial (je 2 Sylowgruppen sind konjugiert) folgt $|G|=60|4!=24$ (Widerspruch)
Also gibt es 10 3-Sylowgruppen.

Auflösbare Gruppen

Definition: Eine endliche Gruppe heißt auflösbar, wenn es eine Folge $\{1\}=G_n \triangleleft \ldots \triangleleft G_1 \triangleleft G_0=G$ von Untergruppen gibt sodass jeweils $G_{i+1} \triangleleft G_i$ normal ist vom Primindex.

Beispiel: Jede zyklische Gruppe $\mathbb{Z}/n$ ist auflösbar: $\{0\}=p_1 \cdots p_r \mathbb{Z}/n \triangleleft \cdots \triangleleft p_1 \mathbb{Z}/n \triangleleft \mathbb{Z}/n$

Satz: Sei G eine endliche Gruppe.

1. Ist G auflösbar, dann sind auch alle Untergruppen $H<G$ und Quotienten G/K auflösbar.
2. Sind $K \triangleleft G$ und G/K auflösbar, ist auch G auflösbar.

Definition: Aus einer Gruppe G leiten wir die Kommutatorgruppe ab: $D(G)=[G,G]$.
Die abgeleiteten Gruppen sind $D^0(G)=G$ und $D^{k+1}(G)=D(D^k(G))$.

Satz: Für jede endliche Gruppe sind äquivalent:

1. G ist auflösbar
2. Es existiert eine Kette $\{1\}=G_n \triangleleft \ldots \triangleleft G_1 \triangleleft G_0=G$ mit G_i/G_{i+1} zyklisch
3. Es existiert eine Kette $\{1\}=G_n \triangleleft \ldots \triangleleft G_1 \triangleleft G_0=G$ mit G_i/G_{i+1} abelsch
4. Die Kette $G=D^0(G) > D^1(G) > \ldots$ endet mit $D^n(G)=\{1\}$

Körpererweiterungen

Beispiel: Zu jedem Körper K enthält der Polynomring $K[X]$ den Körper K als Unterkörper. Dies gilt auch für den Bruchkörper $K(X)=\{P/Q : P,Q \in K[X], Q \neq 0\}$ der rationalen Funktionen, also ist

dieser eine Körpererweiterung von K.

Notation: $\sigma \in Hom(E|K,F|K)$ ist eine Homomorphismus zwischen den Körpererweiterungen E,F von K sodass $\sigma|_K = id_K$ ist. (Geht auch zB mit $End(E|K)$ oder $Aut(E|K)$)

Definition: Die Dimension von E als K-Vektorraum $|E:K|=dim_K(E)$ heißt Grad der Erweiterung.

Beispiel: Ist $P \in K[X]$ irreduzibel (über K), dann ist $E=K[X]/(P)$ wieder ein Körper vom Grad $|E:K|=deg(P)$, zum Beispiel hat $\mathbb{Z}/2[X]/(X^2+X+1)$ Grad 2 über $\mathbb{Z}/2$ (Basis: $1,X$).

Satz (Gradformel): Für Körpererweiterungen $K<F<E$ gilt:

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

Algebraische Erweiterungen

Definition: $E|K$ heißt einfache Erweiterung, wenn es $a \in E$ gibt mit $E=K(a)$. Dann heißt a primitives Element der Körpererweiterung.

Definition: Sei $E|K$ Körpererweiterung. $a \in E$ heißt algebraisch über K wenn es ein Polynom $P \in K[X]^*$ gibt mit $P(a)=0$. Sonst heißt a transzendent über K.
Wenn jedes $a \in E$ algebraisch ist, heißt E algebraische Körpererweiterung.

Saftinition: Sei $E|K$ eine Körpererweiterung. Für jedes $a \in E$ sind äquivalent:

1. Das Element a ist algebraisch über K
2. Die Erweiterung $K(a)$ ist endlich über K
3. Der erzeugte Teilring $K[a]$ ist ein Körper: $K[a]=K(a)$ Dann existiert genau ein normiertes Polynom $P \in K[x]^*$ minimalen Grades mit $P(a)=0$. Dieses heißt Minimalpolynom von a: $Irr_K^{\times}(a)=P$.

Die Dimension von a über K ist $deg_K(a)=|K(a):K|$.

Satz: Jede endliche Erweiterung ist algebraisch.
Enthält $S \subset E$ nur algebraische Elemente über K, ist $K(S)$ algebraisch über K.

Zerfällungskörper

Satz (Kronecker): Sei K ein Körper. Zu jedem $P \in K[X]$ vom Grad $deg(P) \geq 1$ existiert ein algebraischer Erweiterungskörper $E|K$ in dem P eine Nullstelle hat.

Satz: Ein Körperhom $\sigma: E \to F$ über K (d.h. $Hom(E|K,F|K)$) bildet Nullstellen von $P \in K[X]$ in E auf Nullstellen von P in F ab.
Insbesondere: Körperautomorphismen permutieren Nullstellen.

Satz: Seien $K(a)$ und $K(a')$ einfache algebraische Erweiterungen. Genau dann existiert ein Körperiso $\sigma: K(a) \xrightarrow{\sim} K(a')$ mit $\sigma|_K = id_K$ und $\sigma(a)=a'$ wenn $Irr_K^{\times}(a)=Irr_K^{\times}(a')$ ist.

Definition: Sei $E|K$ eine Körpererweiterung und $P \in K[X]^*$. Wir sagen P zerfällt über E, wenn es $a_1,\ldots,a_n \in E$ gibt sodass $P=lc(P) \cdot (X-a_1) \cdots (X-a_n)$ gilt. Gilt zudem $E=K(a_1,\ldots,a_n)$ dann nennen wir E einen Zerfällungskörper von P über K (so wenig wie möglich und so viel wie nötig).

Satz: Zu jedem Polynom $P \in K[X]^*$ existiert ein Zerfällungskörper E über K. Je zwei Zerfällungskörper sind isomorph.
Allgemeiner: Sei $\varphi: K \to K'$ ein Körperiso. Sei $P \in K[X]$ und E Zerfällungskörper. Sei $P'=\varphi(P)$ das entsprechende Polynom in K' und E' der Zerfällungskörper davon. Dann existiert ein Körperiso $\sigma: E \xrightarrow{\sim} E'$ mit $\sigma|_K = \varphi$.

Algebraischer Abschluss

Definition: Ein Körper C heißt algebraisch abgeschlossen wenn jedes $P \in C[X]^*$ über C zerfällt.
$C|K$ heißt algebraischer Abschluss wenn $C|K$ algebraisch und C abgeschlossen

Satz: Für jeden Körper C sind äquivalent:

1. Jedes $P \in C[X]$ mit $deg(P) \geq 1$ hat eine Nullstelle in C
2. C ist alg. abg.
3. Jedes irred. Polynom in $C[X]$ hat Grad 1
4. Für jede algebraische Erweiterung $E|C$ gilt $E=C$

Satz: Sei $C|K$ algebraische Erweiterung. Dann sind äquivalent:

1. Jedes $P \in C[X]^*$ zerfällt über C
2. Jedes $P \in K[X]^*$ zerfällt über C

Satz: Zu jedem Körper K existiert ein algebraischer Abschluss $C|K$. Je zwei alg. Abschlüsse sind isomorph über K.

Satz: Sei $\varphi: K \to K'$ ein Körperiso. Sei $E|K$ eine algebraische Erweiterung und $C|K'$ ein alg. Abschluss. Dann ex. ein Körperhom $\sigma: E \to C$ mit $\sigma|_K = \varphi$.
Ist zudem E algebraisch abgeschlossen und $C|K'|$ algebraisch, dann ist jeder Körperhom $\sigma: E \to C$ über K ein Isomorphismus.

Endliche Körper

Klassifikation

Satz: Endliche Körper erlauben folgende Klassifikation:

1. Jeder endliche Körper hat p^n Elemente wobei $p = char(F)$ und $n \in \mathbb{N}_{\geq 1}$
   Denn: K enthält $\mathbb{Z}/_p$ als Primkörper und ist darüber ein VR, also isomorph zu $(\mathbb{Z}/_p)^n$
2. Zu jeder Primzahlpotenz p^n mit $n \in \mathbb{N}_{\geq 1}$ existieren Körper mit p^n Elementen
   Denn: Der Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{Z}/_p$ hat p^n Elemente.
3. Zwei endliche Körper mit gleicher Elementenzahl sind isomorph

Teilkörper: Sei F ein Körper der Ordnung p^n mit $p \in \mathbb{N}$ prim und $n \in \mathbb{N}_{\geq 1}$. Dann hat jeder Teilkörper $K < F$ Ordnung p^m mit $m|n$. Umgekehrt existiert für jeden Teiler $m|n$ in $\mathbb{N}$ genau ein Teilkörper $K < F$ der Ordnung p^m.

Automorphismen: Sei F ein Körper der Ordnung p^n mit $p \in \mathbb{N}$ prim und $n \in \mathbb{N}_{\geq 1}$. Dann ist $Aut(F) = \langle f_p \rangle$ eine zyklische Gruppe der Ordnung n. f_p ist der Frobenius-Homomorphismus.

Galois-Korrespondenz: Gilt hier genauso wie allgemeiner in Kapitel 14.

Galois-Theorie

Definition: Eine algebraische Körpererweiterung $E|K$ heißt galoissch wenn $Fix(Aut(E|K)) = K$. Trivialerweise gilt $K \subset Fix(Aut(E|K))$, die Bedingung besagt dass jedes Element aus $E \backslash K$ von einem Automorphismus bewegt wird.

Satz: Für jede endliche Körpererweiterung $E|K$ gilt $|Aut(E|K)| \leq |E:K|$ und $E|K$ ist genau dann galoissch wenn Gleichheit gilt.

Satz (Galois-Korrespondenz): Sei $E|K$ galoissch. Die Zwischenkörper der Erweiterung korrespondieren mit den Untergruppen von $Aut(E|K)$:

- Zu einem Zwischenkörper $K < F < E$ haben wir $G = Aut(E|F)$
- Zu einer Untergruppe $G < Aut(E|K)$ haben wir $F = Fix(G)$
- Es gilt $Fix(Aut(E|F)) = F$ und $Aut(E|Fix(G)) = G$
- Für zwei verschiedene Zwischenkörper F_1, F_2 gilt: $F_1 < F_2 \Leftrightarrow G_1 > G_2$ und Grad und Index entsprechen sich: $|F_2:F_1| = |G_1:G_2|$
- $F_2|F_1$ ist galoissch genau dann wenn $G_2 \lhd G_1$ ist, dann gilt $g(F_2) = F_2$ für $g \in Aut(E|F_1)$

Separable Erweiterungen

Definition: Sei K ein Körper und C ein alg. Abschluss. $P \in K[X]$ heißt separabel, wenn es in C lauter verschiedene Nullstellen hat. Gleichbedeutend mit $ggT(P,P') = 1$, irreduzible Polynome sind separabel genau dann wenn $P' \neq 0$.
Ein algebraisches Element $a \in E|K$ heißt separabel über K wenn sein Minimalpolynom $Irr_K^\times(a)$ separabel über K ist.
Eine algebraische Erweiterung heißt separabel wenn jedes $a \in E$ separabel über K ist.

Definition: Ein Körper heißt vollkommen, wenn jede alg. Erweiterung $E|K$ separabel ist.
Zum Beispiel ist jeder Körper mit Charakteristik 0 vollkommen (da $P' \neq 0$).

Satz: Ein Körper der Charakteristik $p > 0$ ist genau dann vollkommen, wenn der Frobenius-Homomorphismus ein Automorphismus ist.

Satz (Steinitz): Sei $E|K$ eine endliche Erweiterung. Genau dann existiert ein primitives Element $a \in E$ wenn $E|K$ nur endlich viele Zwischenkörper besitzt.

Satz: Ist $E|K$ endlich und separabel, dann existiert ein primitives Element $a \in E$.

Saftinition: Sei $E|K$ eine alg. Erweiterung und $C|K$ alg. Abschluss. Wir nennen $a \in E$ und $b \in C$ konjugiert über K wenn die folgenden äquivalenten Bedingungen gelten:

1. Es gibt einen Hom $\sigma: E \to C$ über K mit $\sigma(a) = b$
2. Es gibt einen Hom $\sigma: K(a) \to K(b)$ über K mit $\sigma(a) = b$
3. Für die Minimalpolynome über K gilt $Irr_K^\times(a) = Irr_K^\times(b)$

Normale Erweiterungen

Saftinition: Sei $C|K$ alg. Abschluss und $K < E < C$. Dann sind äquivalent:

1. Für jeden Hom $\sigma \in Hom(E|K, C|K)$ gilt $\sigma(E) = E$
2. Zu jedem Element $a \in E$ enthält E auch alle Konjugierten von a in C über K
3. Hat ein irred Polynom $P \in K[X]$ eine Nullstelle in E, so zerfällt es über E
4. E ist der Zerfällungskörper einer Menge $\mathcal{P} \subset K[X]$ von Polynomen über K Dann heißt $E|K$ normal.

Satz: Für jede algebraische Körpererweiterung $E|K$ gilt: $E|K$ ist galoissch genau dann wenn $E|K$ normal und separabel ist. Dann ist für jeden Zwischenkörper $K < F < E$ die Erweiterung $E|F$ auch galoissch.

Galois-Gruppe einer Gleichung

Definition: Sei $P \in K[X]$ separabel. Sei E der Zerfällungskörper von P über K. Die Galois-Gruppe $Aut(E|K)$ nennt man dann auch die Galois-Gruppe von P über K, geschrieben $Gal(P|K) = Aut(E|K)$.

Satz: Für jedes separable $P \in K[X]$ operiert seine Galois-Gruppe auf der Nullstellenmenge. Dadurch erhalten wir einen injektiven (nicht unbedingt bijektiven) Gruppenhomomorphismus $Gal(P|K) \to S_N$ wobei N die Nullstellenmenge von P ist. Insbesondere gilt für den Zerfällungskörper $E|K$ dass $|E:K| \leq n!$ mit $n = |N| = deg(P)$.

Beispiel: $Aut(\mathbb{C}|\mathbb{R}) = Gal(X^2+1|\mathbb{Q}) \cong S_{\pm i}$

Satz: Sei $P \in \mathbb{Q}[X]$ irreduzibel mit Grad $deg P = p$ prim, und mit $p-2$ reellen und zwei komplex konjugierten Nullstellen. Dann ist $Gal(P|\mathbb{Q}) \simeq S_p$ (Symmetrische Gruppe der NS von P)

Anwendungen der Galois-Theorie

Konstruktion mit Z & L

Definition: Das n-te Kreisteilungspolynom ist

$$\Phi_n = \prod_{\xi \in \mathbb{C}, ord(\xi) = n} (X - \xi)$$

Beispiel für $n = 6$: Sei $\zeta = e^{2\pi i/6}$. Dann ist $\Phi_6 = (X-\zeta)(X-\zeta^5) = X^2 - X + 1$ (alle anderen haben Ordnung < 6, ζ^k hat Ordnung n wenn $ggT(n,k) = 1$)
$deg\, \Phi_n = \varphi(n) = |(\mathbb{Z}/_n)^\times|$

Satz: Für jedes $n \in \mathbb{N}$ ist Φ_n irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$

Satz: Seien $z, z_1, ..., z_r \in \mathbb{C}$ komplexe Zahlen. Dann sind äquivalent:

1. Der Punkt z ist mit Zirkel und Lineal konstruierbar ausgehend von $1, z_1, ..., z_r$.
2. Ausgehend vom Grundkörper $K = Q(z_1, ..., z_r)$ gibt es einen Turm quadratischer Erweiterungen $K = E_0 < E_1 < ... < E_n$ mit $z \in E_n$.
3. Die Zahl z ist algebraisch über $K = Q(z_1, ..., z_r)$ und die normale Hülle *(Anmerkung: Die Erweiterung von K mit $S = \{b \in C : b \text{ ist zu einem } a \in E \text{ über K konjugiert}\}$ (C ist der alg. Abschluss))* E von $K(z)$ über K hat als Grad eine Zweierpotenz, also $|E:K| = 2^n$ für ein $n \in \mathbb{N}$.

Satz: Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^e \cdot p_1 \cdots p_t$ gilt mit $e \in \mathbb{N}$ und Fermat-Primzahlen *(Anmerkung: Primzahlen $2^{2^n} + 1$)* $p_1 < ... < p_t$.

Auflösbare Erweiterungen

Satz: Sei $p \in \mathbb{N}$ prim. Sei K Körper mit $char(K) = 0$, der eine primitive p-te Einheitswurzel enthält. Für $E|K$ sind äquivalent:

1. $\exists a \in E, a \notin K$ mit $E = K(a)$ und $a^p \in K$
2. Die Erweiterung $E|K$ ist galoissch vom Grad $|E:K| = p$

Definition: Eine endliche Erweiterung $E|K$ heißt Radikalerweiterung wenn es $a \in E$ gibt mit $E = K(a)$ und $a^n \in K$.
Eine Körpererweiterung $F|K$ heißt durch Radikale auflösbar wenn es eine Erweiterung $E|F$ und einen Turm von Radikalerweiterungen $K < ... < E$ gibt.

Satz: Sei P ein Polynom über einem Körper der Charakteristik 0. Dann ist P genau dann über K durch Radikale auflösbar, wenn die Galois-Gruppe $Gal(P|K)$ auflösbar ist.

Beispiel: Jedes Polynom mit Grad ≤ 4 ist durch Radikale auflösbar, weil sich die Galois-Gruppe in die S_4 einbetten lässt, die auflösbar ist.