Zusammenfassung Algebra

Diese Zusammenfassung basiert neben meiner Vorlesungsmitschrift auch auf dem Algebra-Skript von Prof. Dr. Helmut Schwichtenberg (Universität München).

Hinweis: Es gilt jeweils die letzte Festlegung für Bezeichnungen. Sie werden (insb. am Anfang von Lemmata und Sätzen) nicht notwendigerweise wiederholt.

1. Gruppen

1.1 Grundbegriffe

Definition: Gruppe: Assoziativität, Neutrales Element (genau eines), Inverse Elemente (eindeutig)
Abelsch, wenn kommutativ

Lemma: G nicht leere Menge und $\circ : G \times G \to G$ Abbildung. Dann:
G Gruppe $\Leftrightarrow$ (Assoziativität und $\forall \alpha, \beta \in G : \exists \gamma \in G : \alpha \circ \gamma = \beta$ und $\forall \alpha, \beta \in G : \exists \delta \in G : \delta \circ \alpha = \beta$)

Definition: Untergruppe: Abgeschlossenheit, Neutrales und inverse Elemente enthalten

Satz: (Untergruppenkriterium)

i) $U \subseteq G$ Teilmenge der Gruppe G. Dann:
U Untergruppe $\Leftrightarrow$ ($U \neq \emptyset$ und $\forall x, y \in U : xy^{-1} \in U$)

ii) U endl. Dann:
U Untergruppe $\Leftrightarrow$ ($U \neq \emptyset$ und $\forall x, y \in U : xy \in U$)

Definition: G, H Gruppen und $f : G \to H$ Abb. f heißt:

Homomorphismus: wenn $\forall x, y \in G : f(xy) = f(x)f(y)$

Mono-, Epi- bzw. Isomorphismus: wenn f Homomorphismus und injektiv, surjektiv bzw. bijektiv ist

Endo- bzw. Automorphismus: wenn $G = H$ und f Homo- bzw. Isomorphismus ist.

G und H heißen zueinander isomorph $G \cong H$, wenn es einen Isomorphismus $g : G \to H$ gibt.

Bemerkungen: $f : G \to H$ Homomorphismus. Dann:

i) $f(e) = e$ und $\forall x \in G : f(x^{-1}) = f(x)^{-1}$

ii) U Untergruppe von $G \Rightarrow f(U)$ Untergruppe von H. V Untergruppe von $H \Rightarrow f^{-1}(V)$ Untergruppe von G, insb. also auch $\mathrm{Kern}(f)$.

iii) $\mathrm{Kern}(f) = \{e\} \Leftrightarrow f$ injektiv

iv) f Isomorphismus $\Leftrightarrow \exists$ Homomorphismus $g : H \to G : g \circ f = \mathrm{id}_G$ und $f \circ g = \mathrm{id}_H$

Definition: G Gruppe, U Untergruppe. $x \in G$. Dann heißt $xU := \{xu \mid u \in U\}$ die von x erzeugte Linksnebenklasse bzgl. U (Rechtsnebenklasse analog).
$G/U := \{xU \mid x \in G\}$ („G modulo U“)
$|G/U|$ heißt Index und wird mir $[G : U]$ geschrieben.

Bemerkungen: $xU = yU \Leftrightarrow x^{-1}y \in U$ und $G = \bigcup_{i \in I} x_i U$, falls $(x_i)_{i \in I}$ alle Repräsentanten der Linksnebenklassen xU sind.

Satz: (Lagrange) $|G| = |U| \cdot [G : U]$

Folgerung: (Kleiner Fermat) G endl. $\Rightarrow \forall x \in G : x^{|G|} = e$

1.2 Zyklische Gruppen

Definition: Eine Gruppe $(G, \circ)$ heißt zyklisch, wenn $\exists a \in G : G = \{a^i \mid i \in \mathbb{Z}\} =: \langle a \rangle$.
Beispiele: $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$, $\mathbb{Z}_n := \{0, \ldots, n-1\}$

Lemma: Die Untergruppen von $\mathbb{Z}$ sind genau alle $n\mathbb{Z}$, $n \in \mathbb{N}$.

Lemma: G zyklisch $\Leftrightarrow$ ($G \cong \mathbb{Z}$ oder $G \cong \mathbb{Z}_n$, $n \in \mathbb{N}$)

Definition: $a \in G$. Dann heißt

$$\mathrm{ord}(a) := \begin{cases} \text{kleinstes } n > 0 \text{: } a^n = e & \text{falls ex.} \\ \infty & \text{sonst} \end{cases}$$

die Ordnung von a.

Satz: Sei G endliche Gruppe. Dann $\mathrm{ord}(a) \mid |G|$ (teilt). $|G|$ prim $\Rightarrow G$ zyklisch.

Satz: Jeder Untergruppe einer zyklischen Gruppe ist zyklisch. Jedes homomorphe Bild einer zyklischen Gruppe ist zyklisch.

1.3 Normalteiler

G, H Gruppen, $f : G \to H$ Homomorphismus und $N := \mathrm{Kern}(f)$. Es gilt dann $\forall x \in G : xN = Nx$.

Definition: $N \subseteq G$ Untergruppe. Dann heißt N Normalteiler (in G), wenn gilt $\forall x \in G : xN = Nx$.

Satz: Definiere kan : $G \to G/N$, $x \to xN$. Dann induziert die Verknüpfung in G (genau) eine Verknüpfung in G/N, so dass G/N Gruppe und kan Homomorphismus wird.

Folgerung: N Normalteiler $\Leftrightarrow \forall x \in G : xN \subseteq Nx$ $\Leftrightarrow N = \text{Kern}(f)$ für einen Gruppenhomomorphismus $f : G \to H$

Satz: $N \subseteq G$ Normalteiler, $N \subseteq \text{Kern}(f)$. Dann gibt es genau einen Homomorphismus $g : G/N \to H$ mit $g \circ \text{kan} = f$.

Satz: (Homomorphie) $f : G \to H$ Epimorphismus, $N = \text{Kern}(f)$. Dann: $G/N \cong H$

Satz: (1. Isomorphiesatz von Noether) $U \subseteq G$ Untergruppe, $N \subseteq G$ Normalteiler. Dann: $U \cap N$ Normalteiler in U, UN Untergruppe von G und $U/(U \cap N) \cong UN/N$

Satz: (2. Isomorphiesatz von Noether) $f : G \to H$ Epimorphismus, $M \subseteq H$ Normalteiler und $N := f^{-1}(M)$. Dann: $G/N \cong H/M$.

Definition: N maximaler Normalteiler $:\Leftrightarrow \forall M :$ ($N \subseteq M \subseteq G$ und M Normalteiler $\Rightarrow M = N$ oder $M = G$)
G einfach $:\Leftrightarrow G$ hat nur G und $\{e\}$ als Normalteiler („keine echten Normalteiler“).

Lemma: N maximaler Normalteiler $\Leftrightarrow G/N$ einfach.

1.4 Operationen einer Gruppe auf einer Menge

Definition: G Gruppe, p prim. G heißt p-Gruppe, wenn $|G| = p^n$, $n \in \mathbb{N}$. $Z_G := \{x \in G \mid xy = yx \ \forall x \in G\}$ heißt Zentrum von G.
Bemerkungen: Z_G ist Normalteiler in G.

Definition: S Menge, $m : G \times S \to S$ Abb. Abkürzung: $xs := m(x, s)$.

i) m heißt Operation von G auf S, wenn gilt: $\forall s \in S,\ x, y, \in G : (xy)s = x(ys)$ und $\forall s \in S : es = s$.
ii) m Operation von G auf S, $s \in S$:
$Gs := \{xs \mid x \in G\}$ heißt Bahn oder Orbit von s
$G_s := \{x \in G \mid xs = s\}$ heißt Stabilisator oder Isotopiegruppe von s

Bemerkungen: G_s ist Untergruppe von G.

Satz: S Menge, $m : G \times S \to S$ Operation. Dann:

i) $S = \dot{\bigcup}_{i \in I} G_{s_i}$ für eine Familie $(s_i)_{i \in I}$ in S.
ii) G endl. $\Rightarrow |Gs| = [G : G_s]$ für jedes $s \in S$

Folgerung: G endl. Gruppe, $C \subseteq S$, so dass $S = \dot{\bigcup}_{s \in C} G_s$. Dann:
$|S| = \sum_{s \in C} |Gs| = \sum_{s \in C} [G : G_s]$

Satz: (Klassengleichung) $C \subseteq G$, so dass $G = \dot{\bigcup}_{y \in C} Gy$. Dann:
$|G| = |Z_G| + \sum_{y \in C,\ [G:G_y] > 1} [G : G_y]$

Folgerung: ist G p-Gruppe, so gilt $|Z_G| \geq p$.

1.5 Auflösbare Gruppen

Definition: G Gruppe, $M \subseteq G$ Teilmenge. $\langle M \rangle := \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mid n \geq 0,\ x_1, \ldots, x_n \in M,\ \epsilon_1, \ldots, \epsilon_n = \pm 1\}$ heißt die von M erzeugte Untergruppe von G. Nach Definition ist $\langle M \rangle$ die kleinste Untergrupe von G, die M enthält.

Definition: $x, y \in G$. Das $k \in G$ mit $xy = kyx$ (also $k := xyx^{-1}y^{-1}$) heißt Kommutator von x und y. k misst die Abweichung vom kommutativen Gesetz.
$K_G := \{xyx^{-1}y^{-1} \mid x, y \in G\}$ heißt Kommutatormenge von G. Die Gruppe $G' := \langle K_G \rangle$ heißt Kommutatorgruppe von G oder erste Ableitung von G.
Bemerkungen:

i) G abelsch $\Leftrightarrow G' = \{e\}$
ii) $\langle K_G \rangle = \{k_1 \cdots k_n \mid n \geq 0 \text{ und } k_1, \ldots, k_n \in K_G\}$

Satz: $H \subset G$ Untergruppe. Dann: $G' \subseteq H \Leftrightarrow H$ ist Normalteiler mit abelscher Faktorgruppe G/H

Definition: Die n-te Ableitung $G^{(n)}$ von G wird rekursiv definiert durch: $G^{(0)} := G$, $G^{(n+1)} := (G^{(n)})'$. Eine endliche Familie von Untergruppen $G_i \subset G$, $i = 0, \ldots, n$, heißt Normalreihe in G, wenn gilt:

i) $G = G_0 \supseteq \cdots \supseteq G_n = \{e\}$
ii) G_{i-1} enthält G_i als Normalerteiler ($i = 1, \ldots, n$)

Die Gruppen G_{i-1}/G_i heißen Faktoren der Normalreihe.

Satz: Zu G gibt es Normalreihe mit abelschen Faktoren $\Leftrightarrow \exists n \in \mathbb{N}_0 : G^{(n)} = \{e\}$.

Definition: G heißt auflösbar, wenn eine der beiden letzten Eigenschaften (also beide) erfüllt.

Lemma:

i) $U \subseteq G$ Untergruppe $\Rightarrow U^{(n)} \subseteq G^{(n)}$
ii) H Gruppe, $f : G \to H$ Homomorphismus $\Rightarrow (f(G))^{(n)} = f(G^{(n)})$
iii) $N \subseteq G$ Normalteiler $\Rightarrow (G/N)^{(n)} = G^{(n)}N/N$

Satz: G auflösbare Gruppe. Dann

i) Jede Untergruppe von G ist auflösbar
ii) Jedes homomorphe Bild von G ist auflösbar

Satz: G Gruppe, $N \subseteq G$ Normalteiler. Dann: N und G/N auflösbar $\Rightarrow G$ auflösbar.

Folgerung: Jede p-Gruppe ist auflösbar.

Definition: $G_0 \supseteq \cdots \supseteq G_m$ Normalreihe. Eine Normalreihe $H_0 \supseteq \cdots \supseteq H_n$ heißt Verfeinerung von $G_0 \supseteq \cdots \supseteq G_m$, wenn es eine ordnungstreue injektive Abbildung $\pi : \{0, \ldots, m\} \to \{0, \ldots, n\}$ gibt, so dass $\forall i : G_i = H_{\pi(i)}$.

Lemma: $G = H_0 \supseteq \cdots \supseteq H_n = \{e\}$ Normalreihe mit abelschen Faktoren. Dann hat jede Verfeinerung dieser Normalreihe ebenfalls abelsche Faktoren.

Satz: Jede auflösbare Gruppe hat eine Normalreihe, deren Faktoren zyklische Gruppen von Primzahlordnungen sind.

Lemma: Sei $n \geq 5$, $U \subseteq S_n$ Untergruppe, $\overline{U} \subseteq U$ Normalteiler und $U/\overline{U}$ abelsch. Enthält U alle 3-Zykeln, so müssen sie schon in $\overline{U}$ liegen.

Satz: S_n ist für $n \geq 5$ nicht auflösbar.

2. Körper

2.1 Grundbegriffe

Definition: Körper K: Menge mit zwei Verknüpfungen ($+$ und $\cdot$). $(K, +)$ abelsche Gruppe, $(K^* := K \setminus \{0\}, \cdot)$ abelsche Gruppe. $\forall x, y, z \in K : x(y + z) = (xy) + (xz)$.

Definition: K Körper, $E \subseteq K$ Teilmenge. Dann heißt E Teilkörper oder Unterkörper von K und K heißt Körpererweiterung von E („K/E“), wenn E abgeschlossen und $(E, +, \cdot)$ Körper.

Bemerkungen: (Teilkörperkriterium) E Teilkörper $\Leftrightarrow \{0, 1\} \subseteq E$ und $\forall x, y \in E : x - y \in E$ und $\forall x, y \in E, y \neq 0 : x \cdot y^{-1} \in E$

Definition: $K \supseteq E$ Körpererweiterung. Dann kann K als E-Vektorraum aufgefasst werden. Dabei heißt $[K : E] := \dim_E(K)$ der Grad der Körpererweiterung $K \supseteq E$.

Bemerkungen: $[K : E] = 1 \Leftrightarrow 1(\in K)$ ist Basis des E-VRs $K \Leftrightarrow K = E$

Satz: (Gradsatz) L Zwischenkörper ($K \supseteq L \supseteq E$). Dann: $[K : E] = [K : L] \cdot [L : E]$

2.2 Monomorphismen zwischen Körpern

Definition: K, L Körper, $\varphi : K \to L$ Abb. φ heißt Körperhomomorphismus, wenn

i) $\forall x, y \in K : \varphi(x + y) = \varphi(x) + \varphi(y)$

ii) $\forall x, y \in K : \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

iii) $\varphi(1) = 1$

Bemerkungen: Es folgt $\forall x \in K^* : \varphi(x) \neq 0$, d. h. jeder Körperhomomorphismus ist injektiv.

Satz: $\varphi_1, \ldots, \varphi_n$ verschiedene Körperhomomorphismen $K \to L$. Dann sind $\varphi_1, \ldots, \varphi_n$ linear unabhängig über dem L-Vektorraum der Abbildungen $K \to L$.

Satz: $F := \{x \in K \mid \varphi_1(x) = \cdots = \varphi_n(x)\}$. Dann ist F Teilkörper von K und $[K : F] \geq n$.

Definition: Wenn $L = K$ und $\mathrm{id} \in \{\varphi_1, \ldots, \varphi_n\}$, nennt man F Fixkörper.
$\mathrm{Aut}(K)$ bezeichnet die Automorphismengruppe (Gruppe der Isomorphismen $K \to K$).

Definition: G endliche Untergruppe von $\mathrm{Aut}(K)$. Dann heißt die Abb. $\mathrm{sp}_G : K \to K$, $x \to \sum_{\varphi \in G} \varphi(x)$ die G-Spur in K.

Lemma: $F = \{x \in K \mid \varphi(x) = x \forall \phi \in G\} =: \mathrm{Fix}\, G$ Fixkörper von G. Dann: $\{0\} \neq \mathrm{sp}_G(K) \subseteq F$

Satz: $[K : F] = |G|$

2.3 Die Galoisgruppe, galoissche Erweiterungen

Definition: L/K Körpererweiterung. $\mathrm{Gal}(L/K) := \{\varphi \in \mathrm{Aut}(L) \mid \varphi(x) = x \ \forall x \in K\}$ heißt Galoisgruppe von L/K.
L/K heißt galoissch, falls $[L : k] < \infty$ und $\mathrm{Fix}\,\mathrm{Gal}(L/K) = K$

Satz: $|\mathrm{Gal}(L/K)| < \infty$ Dann: L/K galoissch $\Leftrightarrow [L : K] = |\mathrm{Gal}(L/K)|$

Lemma: $L/E/K$ Körpererweiterungen. Dann: L/K galoissch $\Rightarrow L/E$ galoissch

Satz: (Hauptsatz der Galois-Theorie) L/K galoissche Körpererweiterung.

i) Die Abbildungen $F \xrightarrow{\Phi} \mathrm{Gal}(L/F) \subseteq \mathrm{Gal}(L/K)$, F Zwischenkörper von L/K, und $\mathrm{Gal}(L/K) \supseteq U \xrightarrow{\Psi} \mathrm{Fix}\, U \subseteq L$, U Untergruppe, sind invers zueinander.

ii) Es gilt $[L : E] = |\mathrm{Gal}(L/E)|$ und $[E : K] = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)]$

iii) E/K galoissch $\Leftrightarrow \forall \varphi \in \mathrm{Gal}(L/K) : \varphi(E) = E$ $\Leftrightarrow \mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$ ist Normalteiler

Lemma: L/K galoissch, $\varphi : E \to L$ Homomorphismus mit $\varphi|_K = \mathrm{id}_K$. Dann $\exists \widetilde{\varphi} \in \mathrm{Gal}(L/K)$ mit $\widetilde{\varphi}|_E = \varphi$.

3. Ringe

3.1 Grundbegriffe

Definition: Ring A: Menge mit zwei Verknüpfungen ($+$ und $\cdot$). $(A,+)$ abelsche Gruppe, Assoziativität bei Multiplikation. $\forall x,y,z \in K : x(y+z) = (xy)+(xz)$ und $(x+y)z = (xz)+(yz)$. Im Folgenden werden nur kommutative Ringe mit 1 betrachtet.

Definition: A heißt nullteilerfrei, wenn $\forall x,y \in A$: $(xy = 0 \Rightarrow x = 0$ oder $y = 0)$.
Gilt im A Ring A zusätzlich zur Nullteilerfreiheit $1 \neq 0$, so heißt A Integritätsring.

Definition: A Ring und $U \subseteq A$ Teilmenge. U heißt Unterring von A, wenn $1 \in U$ und U abgeschlossen bzgl. $+$ und $\cdot$ und $(U,+)$ Untergruppe von $(A,+)$.

Definition: A, B Ringe. Eine Abb. $f : A \to B$ heißt Ringhomomorphismus, wenn

i) $\forall x,y \in A : \varphi(x+y) = \varphi(x) + \varphi(y)$
ii) $\forall x,y \in A : \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
iii) $\varphi(1) = 1$

Definition: A Ring. $\mathfrak{a} \subseteq A$ heißt Ideal, falls $\mathfrak{a}$ eine Untergruppe von $(A,+)$ ist, und $A\mathfrak{a} \subseteq \mathfrak{a}$.

Bemerkungen:

i) $f : A \to B$ Ringhomomorphismus. $B \supseteq \mathfrak{b}$ Ideal $\Rightarrow f^{-1}(\mathfrak{b})$ Ideal von A
$A \supseteq \mathfrak{a}$ Ideal und f surjektiv $\Rightarrow f(\mathfrak{a})$ Ideal von B
ii) A Körper $\Rightarrow \{0\}$ und A sind einzige Ideale von A

Satz: (Konstruktion des Restklassenrings) A Ring, $\mathfrak{a}$ Ideal. Definiere $A/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in A\}$ und kan $: A \to A/\mathfrak{a}$, $x \to x + \mathfrak{a}$. Dann existiert auf $A/\mathfrak{a}$ genau eine Struktur eines Ringes, so dass kan Ringhomomorphismus wird mit Kern(kan) $= \mathfrak{a}$.

Folgerung: $\mathfrak{a} \subseteq A$ Teilmenge. Dann $\mathfrak{a}$ Ideal $\Leftrightarrow \exists$ Ringhomomorphismus $f : A \to B$ mit Kern $f = \mathfrak{a}$

Satz: (Universelle Eigenschaft des Restklassenrings) $f : A \to B$ Ringhomomorphismus, $\mathfrak{a} \subseteq A$ Ideal mit $\mathfrak{a} = \text{Kern}\, f$. Dann ex. genau ein Ringhomomorphismus $g : A/\mathfrak{a} \to B$ mit $g \circ \text{kan} = f$.

Folgerung: (Homomorphiesatz) f surjektiv, $\mathfrak{a} :=$ Kern f. Dann: $A/\mathfrak{a} \cong B$

Definition: $\mathfrak{a}, \mathfrak{b} \subseteq A$ Ideale.

i) $\mathfrak{a} + \mathfrak{b} := \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$
ii) $M \subseteq A$ Teilmenge. $(M) := \{x_1a_1 + \cdots + x_na_n \mid n \geq 0,\ a_1,\ldots,a_n \in M,\ x_1,\ldots,x_n \in A\}$. Schreibe im Folgenden $(a_1,\ldots,a_n)$ statt $(\{a_1,\ldots,a_n\})$.

Bemerkungen: Die definierten Teilmengen sind Ideale in A. (M) ist das kleinste Ideal von A, das M enthält.

Definition: $u \in A$. u Einheit $:\Leftrightarrow \exists v \in A : uv = 1$.
$A^* := \{u \in A \mid u \text{ Einheit}\}$

Satz: A Integritätsring, $a, b \in A$. Dann: $(a) = (b) \Leftrightarrow \exists u \in A^* : a = ub$

Satz: (Konstruktion des Quotientenkörpers)

i) Auf $\{(x,y) \mid x,y \in A,\ y \neq 0\}$ wird durch $(x,y) \sim (x',y') :\Leftrightarrow xy' = x'y$ eine Äquivalenzrelation definiert.
ii) Bei Bezeichnung der Äquivalenzklasse (x,y) mit $\frac{x}{y}$ und der Menge aller Äquivalenzklassen mit $Q(A)$ werden eine Addition und Multiplikation durch $\frac{x}{y} + \frac{x'}{y'} = \frac{xy'+x'y}{yy'}$ und $\frac{x}{y} \cdot \frac{x'}{y'} = \frac{xx'}{yy'}$ (wohl-)definiert.
iii) $(Q(A),+,\cdot)$ ist Körper
iv) Die Abb. kan $: a \to Q(A)$, $x \to \frac{x}{1}$ ist injektiver Ringhomomorphismus.

Satz: (Universelle Eigenschaft des Quotentenkörpers) $f : A \to K$ Ringhomomorphismus, K Körper. Dann gibt es genau einen Körperhomomorphismus $g : Q(A) \to K$ mit $g \circ \text{kan} = f$.

3.2 Primideale und maximale Ideale

Definition: A Ring, $\mathfrak{a} \subsetneq A$ Ideal. $\mathfrak{a}$ heißt Primideal, falls $\forall x,y \in A : xy \in \mathfrak{a} \Rightarrow (x \in \mathfrak{a}$ oder $y \in \mathfrak{a})$.
$\mathfrak{a}$ heißt maximal, wenn $\forall \mathfrak{b} \in A, \mathfrak{b}$ Ideal: $(\mathfrak{a} \subseteq \mathfrak{b} \subseteq A \Rightarrow \mathfrak{a} = \mathfrak{b}$ oder $\mathfrak{b} = A)$.

Satz:

i) $A/\mathfrak{a}$ Integritätsring $\Leftrightarrow \mathfrak{a}$ Primideal
ii) $A/\mathfrak{a}$ Körper $\Leftrightarrow \mathfrak{a}$ max. Ideal

Bemerkungen: $\mathfrak{a}$ max. Ideal $\Rightarrow \mathfrak{a}$ Primideal

Definition: K Körper. $f : \mathbb{Z} \to K$, $n \to n \cdot 1$ Ringhomomorphismus. Wegen Kern(f) Ideal in $\mathbb{Z}$ gilt $\exists p \geq 0 :$ Kern$(f) = p\mathbb{Z}$. Dieses $p \in \mathbb{N}_0$ heißt Charakteristik von K. Es gilt stets $p \neq 1$, da $0 \neq 1$ in K.
Der kleinste Unterkörper von K, Durchschnitt aller Unterkörper von K, heißt Primkörper.

3.3 Hauptidealringe

Definition: A Ring. Ein Ideal $\mathfrak{a} \subseteq A$ heißt Hauptideal, wenn $\exists a \in A : \mathfrak{a} = (a)$. A heißt Hauptidealring, wenn A Integritätsring und jedes Ideal von A ein Hauptideal ist.

Definition: A Integritätsring. $x \in A$ heißt irreduzibel, wenn $x \neq 0$ und $x \notin A^*$ und $\forall a, b \in A : (x = ab \Rightarrow a \in A^* \text{ oder } b \in A^*)$.
Zwei Elemente $x, y \in A$ heißen assoziiert, $x \sim y :\Leftrightarrow \exists a \in A^* : x = ay$.

Definition: A heißt faktoriell, wenn jedes Element $x \in A \setminus \{0\}$ eine Darstellung $x = p_1 \dots p_n$, p_i irreduzibel, besitzt und für jede weitere Darstellung $x = q_1 \dots q_m$, q_i irreduzibel, gilt, dass $n = m$ und $p_i \sim q_{\sigma(i)}$ für eine Permutation $\sigma \in S_n$.

Satz: Jeder Hauptidealring ist faktoriell.

Folgerung: A Hauptidealring, $a \in A,\ a \neq 0,\ a \notin A^*$. Dann: (a) Primideal $\leftrightarrow$ (a) maximales Ideal $\Leftrightarrow a$ irreduzibel

3.4 Polynomringe

Satz: A Ring, $A[X]$ Menge aller Folgen $(a_0, a_1, \dots)$ von Elementen aus A, $a_k = 0$ für fast alle $k \in \mathbb{N}_0$.

i) Definiere $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$ und $(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots)$ mit $c_k := \sum_{i=0}^{k} a_i b_{k-i}$. Dann ist $A[X]$ ein Ring mit Nullelement $(0, 0, \dots)$ und Einselement $(1, 0, 0, \dots)$.
ii) Die Abbildung $\text{kan} : A \to A[X]$, $x \to (x, 0, 0, \dots)$, ist ein Ringhomomorphismus.
iii) Identifiziert man $X = (0, 1, 0, \dots)$, so hat jedes Element in $A[X] \setminus \{0\}$ eine eindeutige Darstellung $f = \sum_{i=0}^{n} a_i X^i$ mit $a \in A$ und $a_n \neq 0$.

Satz: A, B Ringe, $x \in B$ und $f : A \to B$ Ringhomomorphismus. Dann existiert genau ein Ringhomomorphismus $g : A[X] \to B$ mit $g(X) = x$ und $g \circ \text{kan} = f$.

Definition:
$A[X_1, \dots, X_{n+1}] := (A[X_1, \dots, X_n])[X_{n+1}]$.
Bemerkungen: Zu jedem $0 \neq f \in A[X_1, \dots, X_n]$ gibt es genau eine endliche Teilmenge $I \subseteq \mathbb{N}_0^n$ und eindeutig bestimmte $a_{i_1 \dots i_n} \in A \setminus \{0\}$, $(i_1, \dots, i_n) \in I$ mit

$$f = \sum_{(i_1,\dots,i_n) \in I} a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

Definition: Sei $f = \sum_{i=0}^{n} a_i X^i \in A[X]$, $a_n \neq 0$. Dann heißt $n = \deg g$ der Grad von f.

Satz: K Körper, $f, p \in K[X],\ p \neq 0$. Dann: $\exists q, r \in K[X] : f = q \cdot p + r$ und $\deg r < \deg p$

Folgerung: $K[X]$ ist Hauptidealring und daher faktoriell.

Definition: $f \in A[X]$ und $x \in A$. Dann heißt x Nullstelle von f, falls $f(x) = \sum_{i=0}^{n} a_i x^i = 0$

Satz: Sei $f \in K[X]$ mit $f \neq 0$, $\deg f = n$. Dann hat f höchstens n Nullstellen.

Lemma: G endliche abelsche Gruppe. Gibt es in G ein Element x maximaler Ordnung m, so gilt $\forall y \in G : y^m = e$.

Satz: Jede endliche Untergruppe von $(K^*, \cdot)$ ist zyklisch.

4. Algebraische Körpererweiterungen

4.1 Algebraische Elemente

Satz:

i) A, B Ringe, $A \subseteq B$, $a_1, \dots, a_n \in B$. Dann ist das Bild von

$$\begin{aligned}
&\widehat{(a_1, \dots, a_n)} : A[X_1, \dots, X_n] \to B,\\
&f = \sum_{(i_1,\dots,i_n) \in I} a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}\\
&\to \sum_{(i_1,\dots,i_n) \in I} a_{i_1 \dots i_n} a_1^{i_1} \cdots a_n^{i_n}\\
&=: f(a_1, \dots, a_n)
\end{aligned}$$

der kleinste Teilring von B, der $A \cup \{a_1, \dots, a_n\}$ enthält. Dieser Ring wird mit $A[a_1, \dots, a_n]$ bezeichnet. („Ringadjunktion“)
ii) L/K Körpererweiterung, $a_1, \dots, a_n \in L$. Dann ist

$$\begin{aligned}
&K(a_1, \dots, a_n)\\
&= \{\frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} \mid f, g \in K[X_1, \dots, X_n],\\
&\qquad g(a_1, \dots, a_n) \neq 0\} \subseteq L
\end{aligned}$$

der kleinste Teilkörper, der $K \cup \{a_1, \dots, a_n\}$ enthält. („Körperadjunktion“)

Bemerkungen: L/K Körpererweiterung, $a_1, \dots, a_n, b_1, \dots, b_n \in L$. Dann:
$L[a_1, \dots, a_n][b_1, \dots, b_m] = L[a_1, \dots, a_n, b_1, \dots, b_m]$, analog für Körperadjunktion.

Definition: L/K Körpererweiterung, $a \in L$

i) a heißt algebraisch über K, wenn $f(a) = 0$ für ein $f \in K[X] \setminus \{0\}$.
ii) a heißt transzendent über K, wenn $f(a) \neq 0$ für alle $f \in K[X] \setminus \{0\}$.
iii) L/K heißt algebraisch, wenn jedes $a \in L$ algebraisch über K ist.

Satz: $a \in L$ algebraisch. Dann:

i) $K[a] = K(a)$

ii) $0 \neq f \in K[X]$, $f(a) = 0$. Dann:
f hat minimalen Grad unter allen Polynomen $g \in K[X] \setminus \{0\}$ mit $g(a) = 0 \Leftrightarrow \mathrm{Kern}(\widehat{a}) = (f) \Leftrightarrow f$ irreduzibel
Es gibt genau ein solches diese Eigenschaften erfüllendes normiertes Polynom f, es heißt das Minimalpolynom. Es gilt: $K(a) \cong K[X]/(f)$ mit $a \to X + (f)$.

iii) $1 = a^0, a^1, \ldots, a^{n-1}$ mit $n := \deg(f)$ sind K-Basis für $K(a)$

Satz: $[L : K] < \infty \Leftrightarrow L$ algebraische Erweiterung von K der Form $L = K(a_1, \ldots, a_n)$

Satz: (Kronecker) $g \in K[X]$, $\deg g > 0$. Dann ex. eine Erweiterung $L/K : \exists x \in L : g(x) = 0$.

4.2 Zerfällungskörper

Lemma: A, A' Ringe, $\varphi : A \to A'$ Isomorphismus. Dann ist $\widehat{\varphi} : A[X] \to A'[X]$, $\sum_{i=0}^{n} a_i X^i \to \sum_{i=0}^{n} \varphi(a_i) X^i$ ein Isomorphismus.

Satz: L/K und L'/K' Körpererweiterungen, $a \in L$, $a' \in L'$, $p \in K[X]$, $p' \in K'[X]$ mit p, p' irreduzibel, $p(a) = 0 = p'(a')$, $\varphi : K \to K'$ Isomorphismus. Dann existiert ein Isomorphismus $\bar{\varphi} : K(a) \to K'(a')$ mit $\bar{\varphi}(a) = a'$ und $\bar{\varphi}|_K = \varphi$.

Folgerung: L/K Körpererweiterung, $p \in K[X]$ irred., $a, b \in L : p(a) = 0 = p(b)$. Dann gilt $K(a) \cong K(b)$.

Definition: $f \in K[X]$. Dann heißt L/K Zerfällungskörper von f über K, falls

i) $f = b(X - a_1) \cdots (X - a_n)$ mit $a_i \in L$, $b \in K$

ii) $L/E/K$ und f zerfällt über E in Linearfaktoren wie in i), dann ist $L = E$. (Minimalität von L)

Bemerkungen: L Zerfällungskörper von $f = b(X - a_1) \cdots (X - a_n)$. Dann: $L = K(a_1, \ldots, a_n)$

Satz: $\forall f \in K[X] : \exists$ Zerfällungskörper $L \supseteq K$ und $[L : K] < \infty$

Satz: K, K' Körper, $\varphi : K \to K'$ Isomorphismus, $f \in K[X]$, $f' \in K'[X]$ und $\widehat{\varphi}(f) = f'$. Seien L und L' Zerfällungskörper von f und f' über K und K', so existiert ein Isomorphismus $\bar{\varphi} : L \to L'$ und $\bar{\varphi}|_K = \varphi$ und $\bar{\varphi}(\{\text{Nullstellen von } f\}) = \{\text{Nullstellen von } f'\}$

Folgerung: Ein Zerfällungskörper von $f \in K[X]$ ist eindeutig bis auf Isomorphismus, der die Elemente in K festhält.

4.3 Separable Erweiterungen

Definition: K Körper, $f \in K[X]$, $L \supseteq K$ Zerfällungskörper von f. Für eine Nullstelle a von f heißt $\mu(f, a) = \max\{n \in \mathbb{N} \mid (x - a)^n \text{ teilt } f\}$ Vielfachheit. (Wohldefiniert wegen Eindeutigkeit des Zerfällungskörpers.)

Definition: L/K Körperweiterung.

i) $f \in K[X]$ heißt separabel, falls jeder irreduzible Faktor von f nur einfache Nullstellen besitzt.

ii) $a \in L$ heißt separabel, falls a Nullstelle eines separablen Polynoms ist.

iii) L/K heißt separabel, falls jedes $a \in L$ separabel ist.

Lemma: L/K galloisch, $a \in L$ und $a_1, \ldots, a_n$ die Bilder von a unter $\varphi \in \mathrm{Gal}(L/K)$. Dann:

i) $p = (X - a_1) \cdots (X - a_n) \in K[X]$

ii) p ist separabel.

iii) p ist Minimalpolynom von a.

Satz: L/K Körpererweiterung. Dann: L/K galoissch $\Leftrightarrow Z$ ist Zefällungskörper eines separablen Polynoms über K

Satz: $\mathrm{char}\, K = 0 \Rightarrow \forall f \in K[X] : f$ separabel

4.4 Normale Erweiterungen

Definition: L/K Körpererweiterung. L/K heißt normal, wenn L/K algebraisch und jedes irreduzible Polynom $f \in K[X]$, das in L eine Nullstelle hat, über L in Linearfaktoren erfällt.

Satz: L/K galoissch $\Leftrightarrow L/K$ endlich, normal und separabel $\Leftrightarrow L$ ist Zerfällungskörper eines separablen Polynoms

Satz: L/K endlich. Dann: L/K normal $\Leftrightarrow L$ ist Zerfällungskörer eines Polynoms $f \in K[X] \Leftrightarrow \forall L'/L$ Körpererweiterung, $\varphi : L \to L'$ Homomorphismus mit $\varphi|_K = \mathrm{id}_K : \varphi(L) \subseteq L$

Satz: K endlicher Körper. Dann ist $|K| = p^d$ mit p prim und $d \in \mathbb{N}$. Ferner: Sei $K_0 \cong \mathbb{Z}/p\mathbb{Z}$ der Primkörper von K, so ist K der Zerfällungskörper von $X^{p^d} - X$ über K_0. Insbesondere ist $x^{p^d} - X$ separabel und K/K_0 galoissch.

Bemerkungen: p prim, $d \in \mathbb{N}$. Dann hat der Zerfällungskörper von $X^{p^d} - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ genau p^d Elemente.

Satz: K^* ist zyklische Gruppe.

4.5 Teilbarkeit ganzzahliger Polynome

Lemma: (Gauß) $f, g \in \mathbb{Z}[X]$ nicht konstant. Dann: Sind die Koeffizienten von f und g jeweils teilerfremd, so auch die Koeffizienten von fg.

Satz: (Gauß) $f \in \mathbb{Z}[X]$ nicht konstant. Dann: f irreduzibel in $\mathbb{Z}[X] \Rightarrow f$ irreduzibel in $\mathbb{Q}[X]$

Satz: (Eisenstein'sches Irreduzibilitätskriterium) $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ mit teilerfremden Koeffizienten, $a_n \neq 0$, $n > 0$. Dann: $\exists p$ prim: $p|a_0, \ldots, p|a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_0 \Rightarrow f$ irreduzibel in $\mathbb{Z}[X]$.

5. Anwendungen der Galois-Theorie

5.1 Einheitswurzeln

K Körper, $n \in \mathbb{N}$ kein Vielfaches von $\operatorname{char} K$

Lemma: Die Nullstellen des Polynoms $X^n - 1$ heißen n-te Einheitswurzeln. $X^n - a$, $a \neq 0$, hat nur einfache Nullstellen.

Lemma: Die n-ten Einheitswurzeln in K bilden eine (abelsche endliche) multiplikative Gruppe.

Satz:

i) Die n-ten Einheitswurzeln bilden eine zyklische Gruppe. Die erzeugenden Elemente heißen primitive n-te Einheitswurzeln.

ii) ε primitive Einheitswurzel, $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ Gruppe der EWn. Dann: ε^i primitiv $\Leftrightarrow \operatorname{ggT}(i, n) = 1$
Insb. gibt es genau $\varphi(n)$ primitive n-te EWn, wobei mit φ die Euler'sche Funktion gemeint ist.

Satz: ε n-te EW, $Z = K(\varepsilon)$. Dann ist Z/K galoissch und $\operatorname{Gal}(Z/K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$.

Definition: $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ primitive n-te EWn. Dann heißt $f_n := (X - \varepsilon_1) \cdots (X - \varepsilon_{\varphi(n)})$ das Kreisteilungspolynom.

Satz: f_n ist ganzzahlig.

Satz: $f_n \in \mathbb{Q}[X]$ ist irreduzibel.

Satz: Z Zerfällungskörper von $X^n - \in \mathbb{Q}[X]$. Dann ist $Z/\mathbb{Q}$ galoissch mit $\operatorname{Gal}(Z/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

5.2 Reine Polynome

Definition: Ein Polynom der Form $X^n - a$ heißt rein.

Satz: L/K Körpererweiterung, $n \geq 2$, $\operatorname{char} K \nmid n$, K enthalte alle alle n-ten EWn. Dann:

i) L Zerfällungskörper eines reinen Polynoms $\Rightarrow$ L/K galoissch mit zyklischer Galoisgruppe

ii) L Zerfällungskörper eines irred. Polynoms $X^n - a \in K[X] \Leftrightarrow L/K$ galoissch mit zyklischer Galoisgruppe und $[L : K] = n$.

5.3 Auflösbarkeit von Polynomen durch Radikale

Definition: L/K Körpererweiterung, $f \in K[X]$.

i) L/K heißt Radikalerweiterung, wenn es einen Körperturm $K = K(a_0) \subseteq K(a_0, a_1) \subseteq \cdots \subseteq K(a_0, \ldots, a_r) = L$ und $n_1, \ldots, n_r \in \mathbb{N}$ gibt, so dass $\forall i \in \{1, \ldots, r\} : a_i^{n_i} \in K(a_0, \ldots, a_{i-1})$.

ii) f heißt auflösbar durch Radikale, wenn es eine Radikalerweiterung L/K gibt und f in L in Linearfaktoren zerfällt.

Satz: L/K Radikalerweiterung wie in der Definition (f zerfällt in L), $\operatorname{char} K \nmid n_i$, $1 \leq i \leq r$. Dann existiert eine Körpererweiterung L'/L, so dass L'/K eine Radikalerweiterung ist, zu der ein Körperturm $K = K(b_0) \subseteq \cdots \subseteq K(b_0, \ldots, b_s) = L'$ mit zugehörigen $m_1, \ldots, m_s \in \mathbb{N}$ existiert und es gilt:

i) L'/K galoissch, f zerfällt in L'

ii) $\{n_1, \ldots, n_r\} = \{m_1, \ldots, m_s\}$

iii) $K(b_0, b_1, \ldots, b_i)$ ist Zerfällungskörper des separablen Polynoms $X^{m_i} - b_i^{m_i}$ über $K(b_0, \ldots, b_{i-1})$ für $1 \leq i \leq s$

Satz: K Körper mit $\operatorname{char} K = 0$, $f \in K[X]$, f nicht konstant. Dann: f ist auflösbar durch Radikale $\Leftrightarrow$ $\operatorname{Gal}(Z_f/K)$ auflösbar, wobei Z_f der Zerfällungskörper von f ist

5.4 Die allgemeine Gleichung n-ten Grades

Definition: K Körper, $K(U_1, \ldots, U_n)$ Quotientenkörper des Integritätsrings $K[U_1, \ldots, U_n]$ (U_i sind Unbestimmte). Dann heißt $f = X^n - U_1 X^{n-1} + U_2 X^{n-2} - \cdots + (-1)^n U_n X^0 \in K(U_1, \ldots, U_n)[X]$ das allgemeine Polynom n-ten Gerades.

Satz: f ist separabel (bzgl. K) und die Galoisgruppe von f ist S_n.

Folgerung: (Abel) Die allg. Gleichung N-ten Grades ist auflösbar genau dann, wenn $n \leq 4$.

5.5 Konstruktion mit Zirkel und Lineal

Definition: $z_1, \dots, z_n \in \mathbb{C}$, $z_1 = 0$, $z_2 = 1$, $M_1 := \{z_1, \dots, z_n\}$ und $M_{r+1} := M_r \cup \{z \in \mathbb{C} \mid z$ ist

i) Schnittpunkt zweier Geraden, die verschiedene Punkte aus M_r verbinden,

ii) Schnittpunkt einer Geraden wie in i) und eines Kreises um einen Punkt aus M_r mit einem Radius gleich einem Abstand zweier Punkte aus M_r oder

iii) Schnittpunkt zweier Kreise wie in ii) $\}$.

Dann heißt $K(z_1, \dots, z_n) = \bigcup_{r=1}^{\infty} M_r$ die Menge der Elemente in $\mathbb{C}$, die mit Zirkel und Lineal konstruierbar sind.

Satz: $K(z_1, \dots, z_n)$ ist der kleinste Unterkörper von $\mathbb{C}$ mit:

i) $z_1, \dots, z_n \in K$

ii) $z^2 \in K \Rightarrow z \in K$ (Abschluss Wurzelziehung)

iii) $z \in K \Rightarrow \bar{z} \in K$ (Abschluss Konjugation)

Folgerung: $K = \mathbb{Q}(z_1, \dots, z_n, \bar{z}_1, \dots, \bar{z}_n)$. Dann: Ist $z \in \mathbb{C}$ aus $z_1, \dots, z_n$ mit Zirkel und Lineal konstruiertbar, so ist z algebraisch über K mit $[K(z) : K] = 2^s$ für ein $s \in \mathbb{N}_0$.