Algebra I

Werner Seiler

Bei diesem Skript handelt es sich um eine Zusammenfassung der Vorlesung Algebra I zusammen, die Herr Seiler im WS2004/05 an der Universität Heidelberg gehalten hat. Das Skript umfasst alle Definitionen und Sätze, allerdings ohne Beweise. Auch die Beispiele wurden weggelassen.

In LaTeXgesetzt wurde das Skript von Wolfgang Unger.
Korrekturhinweise bitte an uni@wolfgangunger.de

Inhaltsverzeichnis

1 Gruppentheorie

1.1 Grundstrukturen mit einer Verknüpfung

Definition 1. *Sei G Menge mit einer Verknüpfung*

$$\circ : G \times G \to G, (f, g) \mapsto f \circ g$$

(kurz geschrieben: $fg := f \circ g$).

1. *G heißt* Halbgruppe, *falls die Verknüpfung* assoziativ *ist, d.h.*

$$\forall f, g, h \in G : f(gh) = (fg)h$$

2. *G heißt* Monoid, *falls G eine Halbgruppe ist mit* neutralem Element, *d.h.*

$$\exists e \in G : eg = ge = g$$

3. *G heißt* Gruppe, *falls G ein Monoid ist und jedes Element ein* inverses Element *besitzt, d.h.*

$$\forall g \in G \, \exists g^{-1} \in G : g^{-1}g = gg^{-1} = e$$

4. *G ist abelsch falls die Verknüpfung* kommutativ *ist, d.h.*

$$\forall f, g \in G : fg = gf$$

5. *Die Anzahl der Elemente von G heißt* Ordnung *von G, geschrieben $|G|$*

Definition 4. *Sei $(G, \circ)$ eine Gruppe (Halbgruppe, Monoid). Dann heißt eine Teilmenge $U \subseteq G$* Untergruppe *(Unterhalbgruppe, Untermonoid), geschrieben $U \leq G$, falls $(U, \circ)$ eine Gruppe (Halbgruppe, Monoid) ist.*

Definition 6. *Sei $M \subseteq G$ Teilmenge einer Gruppe G, dann heißt*

$$\langle M \rangle := \bigcap_{M \leq U \leq G} U$$

die von M erzeugte Gruppe. G heißt zyklisch, *, wenn*

$$\exists g \in G : \langle g \rangle = G$$

Satz 8. *Sei G eine Gruppe. $U \subset G$ ist genau dann eine Untergruppe, $U \leq G$, wenn mit $f, g \in U$ auch $fg^{-1} \in U$ ist.*

Lemma 9. *Sei G eine Gruppe, $U \leq G$ Untergruppe. Dann wird durch $f \sim g \Leftrightarrow fg^{-1} \in U$ eine Äquivalenzrelation definiert, dessen Äquivalenzklassen* Rechtsnebenklassen *von U genannt werden, geschrieben $[g] = Ug = \{ug | u \in U\}$. Ebenso wird durch $f \sim g \Leftrightarrow f^{-1}g \in U$ eine Äquivalenzrelation definiert, dessen Äquivalenzklassen* Linksnebenklassen *von U genannt werden, geschrieben $[g] = gU = \{gu | u \in U\}$.*

Definition 10. *Die Menge aller Rechtsnebenklassen von U wird mit $U\backslash G$ bezeichnet, die Menge aller Linksnebenklassen von U mit G/U. Die Zahl $|G\backslash U| = |G/U|$ heißt* Index *der Untergruppe $U \leq G$, geschrieben $(G : U)$.*

Satz 11. Kürzungsregel: *Es seien $U \leq V \leq G$ Untergruppen. Dann gilt:*

$$(G : U) = (G : V)(V : U)$$

Korollar 12. Satz von Lagrange: *Sei $H \leq G$. Dann gilt:*

$$|G| = (G : H)|H|$$

Definition 13. *Sei G Gruppe, $g \in G$. Dann heißt $o(g) := |\langle g \rangle|$ die* Ordnung *von g.*

Korollar 14. Kleiner Fermat: *Sei G eine endliche Gruppe. Dann gilt:*

$$\forall g \in G : g^{|G|} = e$$

Definition 15. *Eine Untergruppe $N \leq G$ heißt* Normalteiler, *falls:*

$$\forall g \in G : gN = Ng$$

Man schreibt hierfür $N \trianglelefteq G$. Eine Gruppe heißt einfach, *wenn sie nur die trivialen Normalteiler $E := \{e\}$ und G besitzt.*

Lemma 17. *Sei G eine Gruppe, $N \trianglelefteq G$ Normalteiler, $U \leq G$ Untergruppe. Dann gilt:*

1. $N \trianglelefteq NU = \langle N, U \rangle \leq G$
2. $|N|, |U| < \infty \Rightarrow |NU| = \frac{|N||U|}{|N \cap U|}$

Definition 18. *Sei G eine Gruppe. Eine Äquivalenzrelation $\equiv$ auf G heißt Kongruenzrelation, wenn*

$$\forall f, \bar{f}, g, \bar{g} \in G : f \equiv \bar{f} \wedge g \equiv \bar{g} \Rightarrow fg \equiv \bar{f}\bar{g}$$

Lemma 19. *Sei $\equiv$ eine Kongruenzrelation auf Gruppe G. Dann ist die Menge der Äquivalenzklassen $\overline{G} := G/\equiv$ wieder eine Gruppe, die sogenannte* Faktorgruppe .

Satz 20. *Sei G eine Gruppe.*

1. *Für $N \trianglelefteq G$ ist $f \equiv g :\Leftrightarrow fg^{-1} \in N$ eine Kongruenzrelation.*
2. *Ist $\equiv$ eine Kongruenzrelation auf G, so gilt $[e] \trianglelefteq G$.*

1.2 Homomorphismen

Definition 1. *Seien G, H Gruppen. Eine Abbildung $\phi : G \to H$ heißt* Gruppenhomomorphismus, *falls*

$$\forall f, g \in G : \phi(fg) = \phi(f)\phi(g)$$

Falls $G = H$, heißt ϕ Endomorphismus, *ein bijektiver Homomorphismus heißt* Isomorphismus, *ein bijektiver Endomorphismus heißt* Automorphismus. *Die Menge $\ker \phi := \{g \in G | \phi(g) = e_H\}$ heißt* Kern *von ϕ*

Lemma 2.

$$\phi \in \mathrm{Hom}(G, H) \Rightarrow \mathrm{im}\, \phi \leq H, \ker \phi \trianglelefteq G$$

Satz 5. Homomorphiesatz: *Seien G, H Halbgruppen, $\phi : G \to H$ ein Halbgruppenhomomorphismus. Dann gilt:*

$$\mathrm{im}\, \phi \cong G/_{\overset{\phi}{\equiv}}$$

Sind G und H Gruppen, so gilt:

$$G/_{\overset{\phi}{\equiv}} = G/\ker \phi$$

Definition 6. *Seien $G_i, i \in \mathbb{Z}$ Gruppen und $\phi_i : G_i \to G_{i+1}$ Homomorphismen. Die Sequenz*

$$.. \to G_{i-1} \xrightarrow{\phi_{i-1}} G_i \xrightarrow{\phi_i} ..$$

heißt EXAKT, *wenn*

$$\forall i \in \mathbb{Z} : \operatorname{im} \phi_{i-1} = \ker \phi_i$$

Satz 7. 1. ISOMORPHIESATZ: *Sei G eine Gruppe, $U \leq G$, $N \trianglelefteq G$. Dann gilt:*

$$N \trianglelefteq NU \leq G \text{ und } U \cap N \trianglelefteq U \text{ sowie } NU/N \cong U/U \cap N$$

Satz 8. 2. ISOMORPHIESATZ: *Sei G eine Gruppe, $N \trianglelefteq G$. Für eine Untergruppe $U \leq G$ sei $\bar{U} := U/N$. Ferner sei*

$$\mathcal{U}_N := \{U | N \leq U \leq G\} \text{ und } \overline{\mathcal{U}} := \{\overline{U} | \overline{U} \leq G/N\}$$

Dann gilt für ein $U \in \mathcal{U}_N$:

$$U \trianglelefteq G \Leftrightarrow U/N \trianglelefteq \overline{G} \text{ und } G/U \cong \overline{G}/\overline{U}$$

Lemma 9. *$E \neq U \lneq (\mathbb{Z}, +)$. Dann existiert ein $m \in \mathbb{Z}$ mit $U = m\mathbb{Z}$.*

Korollar 10. *Sei G zyklische Gruppe. Dann gilt:* $G \cong \begin{cases} \mathbb{Z} & \text{für } |G| = \infty \\ \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} & \text{für } |G| = m \end{cases}$

1.3 Normalreihen und Kompositionsreihen

Definition 1. *Sei G eine Gruppe. Eine endliche absteigende Reihe von Normalteilern*

$$G = N_0 \rhd N_1 \rhd .. \rhd N_r = E$$

heißt NORMALREIHE *der Länge r. Die Faktorgruppen $N_i := N_i/N_{i+1}$ heißen* NORMALFAKTOREN. *Zwei Normalreihen $(N_1, ..N_r), (M_1, ..M_r)$ der gleichen Länge heißen* ÄQUIVALENT, *wenn es Permutationen $\pi \in \mathfrak{S}_r$ gibt, so dass $\forall i \in \{1, ..r\} : \bar{N}_i \cong \bar{M}_{\pi(i)}$. Eine Normalreihe heißt* KOMPOSITIONSREIHE, *wenn alle Normalfaktoren einfach sind.*

Bemerkung 3. *Nicht jede Gruppe besitzt eine Kompositionsreihe, etwa $G = (\mathbb{Z}, +)$ besitzt keine.*

Satz 4. *Jede endliche Gruppe besitzt eine Kompositionsreihe*

Satz 5. JORDAN-HÖLDER: *Sei G eine endliche Gruppe. Dann haben alle Kompositionsreihen die selbe Länge und sind einander äquivalent.*

Definition 6. *Sei G eine Gruppe. Für $f, g \in G$ heißt $[f, g] := fgf^{-1}g^{-1}$ der* KOMMUTATOR *von f, g. $G' = \langle [f, g] | f, g \in G \rangle$ heißt die* KOMMUTATORGRUPPE *von G. Es gilt: $[f, g]^{-1} = [g, f]$*

Lemma 7. *Sei G eine Gruppe mit Kommutatorgruppe G'. Dann gilt: $G' \trianglelefteq G$ und G/G' abelsch. Für $N \leq G$ gilt: $N \trianglelefteq G \wedge G/N$ abelsch $\Leftrightarrow G' \leq N$.*

Definition 8. *Sei G eine Gruppe. G heißt* AUFLÖSBAR, *falls $\exists r \in \mathbb{N} : G^{(r)} = E$.*

Satz 9. *Eine endliche Gruppe G ist genau dann auflösbar, wenn sie eine Normalreihe mit abelschen Normalfaktoren besitzt.*

Satz 10. *Sei $N \trianglelefteq G$ ein Normalteiler. G ist genau dann auflösbar, wenn N und G/N auflösbar ist.*

1.4 Transformationsgruppen

Definition 1. *Sei M eine Menge und G eine Gruppe. G ist eine* Transformationsgruppe *auf M (G operiert auf M), wenn es eine Abbildung*

$$\phi : G \times M \to M, (g, x) \mapsto gx$$

gibt mit

1. $\forall x \in M : ex = x$
2. $\forall f, g \in G, x \in M : (fg)x = f(gx)$

Bemerkung 2. *Sei $g \in G$ fest. Dann ist $\phi_g : M \to M, x \mapsto gx$, und $\phi_g \in S(M)$. Die Abbildung $\pi : G \to S(M), g \mapsto \phi_g$ ist ein Gruppenhomomorphismus und wird* Permutationsdarstellung *genannt. Ist π injektiv, dann sagt man, G operiere* treu *auf M.*

Definition 4. *Es sei $\phi : G \times M \to M$ eine Operation. Für $x \in M$ heißt*

$$Gx := \{gx | g \in G\} \subseteq M$$

der Orbit *von x unter G. Falls Gx=$\{x\}$, so sagt man, x ist* Fixpunkt .

$$G_x := \{g \in G | gx = x\} \leq G$$

heißt Fixgruppe *(auch Stabilisator, Isotropiegruppe) von x.*

Bemerkung 5. *M besitzt disjunkte Zerlegungen in Orbits. Falls $\exists x \in M : Gx = M$, so operiert G* transitiv *auf M. M heißt dann homogener Raum, es gibt dann eine Bijektion $M \leftrightarrow G/G_x$. Eine Teilmenge $\{x_i | i \in I\} \subseteq M$ heißt* Vertretersystem der Orbits *von M, falls $M = \dot{\bigcup}_{i \in I} Gx_i$*

Satz 6. Bahnbilanzgleichung: *Die Gruppe G operiere auf M.*

1. $\forall x \in M : |Gx| = (G : G_x)$
2. *Sei$\{x_i | i \in I\}$ Vertretersystem der Orbits von M. Dann gilt:*

$$|M| = \sum_{i \in I} |Gx_i| = \sum_{x \in I} (G : G_{x_i})$$

Definition 8. *Die Orbits zur Konjugationsoperation von G auf sich selbst*

$$G \times G \to G, (g, h) \mapsto ghg^{-1}$$

heißen Konjugationsklassen

$$G_g := \{f \in G | \exists h \in G : f = hgh^{-1}\}$$

$f \in G_g$ heißt zu g konjugiert. *Die Anzahl der Konjugationsklassen heißt* Klassenzahl *von G. Die Fixgruppe $Z_g = \{h \in G | hgh^{-1} = g\} \leq G$ heißt* Zentralisator *von g. Allgemeiner führt man für jede Teilmenge $S \leq G$ den Zentralisator*

$$Z_S = \{h \in G | \forall s \in S : hsh^{-1} = s\}$$

ein. Z_G ist das Zentrum *von G.*

Lemma 9. *Es gilt:*

1. *$Z_G \trianglelefteq G$ abelsch*
2. *Die Gruppe der inneren Automorphismen ist isomorph zu G/Z_G.*
3. *Wenn G/Z_G zyklisch, so ist G abelsch*

4. *Es gilt:* $|G_g| = (G : Z_g)$. *Insbesondere ist für jede endliche Gruppe* $|G_g|$ *immer ein Teiler der Gruppenordnung.*

5. KLASSENGLEICHUNG: *Sei* $\{g_i | i \in I\}$ *ein Vertretersystem der Konjugationsklassen. Dann gilt:* $|G| = \sum_{i \in I} (G : Z_{g_i})$

Definition 10. *Sei* $\Gamma = \{U | U \leq G\}$ *die Menge aller Untergruppen in* G. *Dann operiert* G *auf* Γ *durch Konjugation* $(g, U) \mapsto gUg^{-1}$. *Der Orbit von* $U \in \Gamma$,

$$^G U = \{V \leq G | \exists g \in G : V = gUg^{-1}\}$$

heißt Klasse der zu U *konjugierten Untergruppen. Die Fixgruppe von* U *ist der* NORMALISATOR $N_U = \{g \in G | gUg^{-1} = U\}$

Lemma 11. *Es gilt:*

1. $|^G U| = (G : N_U)$, *insbesondere ist für jede endliche Gruppe* $|^G U|$ *ein Teiler von* $|G|$.

2. $U \leq G \Rightarrow U \trianglelefteq N_U$

3. $U \trianglelefteq V \leq G \Rightarrow V \leq N_U$

Korollar 12. *Sei* p *eine Primzahl und* $|G| = p^n$ *für ein* $n \geq 1$. *Ferner sei* $E \neq N \trianglelefteq G$ *ein Normalteiler. Dann gilt* $p \mid |N \cap Z_G|$, *insbesondere also* $N \cap Z_G \neq E$.

1.5 Die Sylowsätze

Definition 1. *Sei* G *eine endliche Gruppe,* p *eine Primzahl.*

1. G *heißt* p-GRUPPE, *falls* $|G| = p^n$ *für ein* $n \in \mathbb{N}$.

2. *Eine Untergruppe* $U \leq G$ *heißt* p-SYLOWGRUPPE, *falls* U *eine* p*-Gruppe ist und* $p \nmid (G : U)$, *d.h.* $|U| = p^n$, $|G| = p^n m$ *mit* $p \nmid m$

Lemma 2. SATZ VON CAUCHY: *Sei* G *eine endliche abelsche Gruppe und* p *ein Primteiler von* $|G|$. *Dann existiert ein* $g \in G$ *mit* $o(g) = p$.

Satz 3. 1. SYLOW-SATZ: *Sei* G *eine endliche Gruppe und* p *eine Primzahl, so dass* $p^k \mid |G|$ *für ein* $k \geq 0$. *Dann existiert eine Untergruppe* $U \leq G$ *mit* $|U| = p^k$.

Lemma 4. *Sei* $P \leq G$ *eine* p*-Sylow-Gruppe und* $U \leq N_P \leq G$ *eine* p*-Untergruppe des Normalisators von* P. *Dann gilt:* $U \leq P$

Satz 5. 2. SYLOW-SATZ: *Es bezeichne* n_p *die Anzahl der* p*-Sylowgruppen in* G. *Dann gilt:*

1. *Für festes* p *sind alle* p*-Sylow-Gruppen in* G *zueinander konjugiert.*

2. *Es gilt:* $n_p \mid |G|$ *und* $n_p \equiv 1 \bmod p$.

3. *Jede* p*-Untergruppe von* G *liegt in einer* p*-Sylow-Gruppe.*

Satz 6. *Sei* G *eine endliche Gruppe,* $U \leq G$ *eine* p*-Gruppe aber keine* p*-Sylow-Gruppe. Dann gilt:* $U \subsetneqq N_U$.

Korollar 7. *Sei* G *eine* p*-Gruppe und* $U \subsetneqq G$ *eine maximale Untergruppe. Dann ist* $U \trianglelefteq G$.

Korollar 8. *Jede* p*-Gruppe ist auflösbar.*

Satz 9. *Es gibt keine einfache Gruppe der Ordnung 24.*

1.6 Freie Monoide und freie Gruppen

Definition 1. *Sei I eine nichtleere Menge. Ein* FREIES MONOID *über I ist ein Paar (M_I, ε) bestehend aus einem Monoid M_I und einer Abbildung $\varepsilon : I \to M_I$, welche folgende universelle Abbildungseigenschaft besitzt: Sei (M, ϕ) ein weiteres Monoid mit einer Abbildung $\phi : I \to M$, so existiert ein eindeutig bestimmter Homomorphismus $\psi : M_I \to M$ mit $\phi = \psi \circ \varepsilon$.*

Satz 2. *Zu jeder nichtleeren Menge I existiert ein freies Monoid M_I über I und dieses ist bis auf Isomorphie eindeutig bestimmt.*

Bemerkung 3. *Wenn I, J gleichmächtige Mengen sind, gilt: $M_I \cong M_J$.*

Definition 4. *Sei I eine nichtleere Menge. Eine* FREIE GRUPPE *über I ist ein Paar (G_I, ε) bestehend aus einer Gruppe G_I und einer Abbildung $\varepsilon : I \to G_I$, das die universelle Abbildungseigenschaft besitzt.*

Satz 5. *Zu jeder nichtleeren Menge I existiert eine freie Gruppe G über I und diese ist bis auf Isomorphie eindeutig bestimmt.*

Bemerkung 6. *Es gilt:*

1. *Für gleichmächtige Mengen I, J gilt: $G_I \cong G_J$*
2. *Wenn (G_I, ε) eine freie Gruppe ist, dann ist ε injektiv.*

Satz 8. *Jede Gruppe ist isomorph zu einer Faktorgruppe einer freien Gruppe.*

Definition 9. $R_I = \ker \Phi$ *heißt die* RELATIONENGRUPPE *von G bzgl. des Erzeugendensystems $\{g_i | i \in I\}$. Wenn $\{r_j | j \in J\}$ ein Erzeugendensystem von R_I ist, nennen wir*

$$G = \langle g_i, i \in I | r_j = e, j \in J \rangle$$

eine DARSTELLUNG *von G durch* ERZEUGER *und* RELATIONEN.

1.7 Die Symmetrischen und Alternierenden Gruppen

Satz 1. *Sei $n \geq 2$.*

1. *Wenn π_1, π_2 fremde Zyklen sind, gilt: $\pi_1 \pi_2 = \pi_2 \pi_1$.*
2. *Jede Permutation $\pi \in \mathfrak{S}_n$ lässt sich bis auf die Reihenfolge eindeutig als Produkt paarweise fremder Zyklen schreiben.*
3. *Jede Permutation $\pi \in \mathfrak{S}_n$ lässt sich als Produkt von Transpositionen schreiben.*

Definition 2. *Sei $\pi = (i_{11}..i_{1r_1})(i_{21}..i_{2r_2})..(i_{s1}..i_{sr_s})$ die Zerlegung von π in fremde Zyklen. Dann heißt* $\mathrm{Typ}(\pi) := (r_1..r_s)$ *der* PERMUTATIONSTYP *von $\pi \in \mathfrak{S}_n$.*

Lemma 3. *Zwei Permutationen $\pi, \rho \in \mathfrak{S}_n$ sind genau dann konjugiert, wenn* $\mathrm{Typ}\,\pi = \mathrm{Typ}\,\rho$.

Lemma 4. *Es gilt:*

1. $\mathrm{sgn}(\pi\rho) = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\rho)$
2. *Für ein r-Zyklus gilt:* $\mathrm{sgn}\,\pi = (-1)^{r-1}$
3. *Die Operation von $\langle \pi \rangle$ zerlege $\{1, ..n\}$ in m Orbits. Dann gilt:* $\mathrm{sgn}\,\pi = (-1)^{nm}$

Lemma 5.
1. *Für $n \geq 3$ gilt $\mathfrak{A}_n = \langle (ijk) | 1 \leq i, j, k \leq n \wedge i, j, k$ paarweise verschieden $\rangle$*
2. *Für $n \geq 5$ gilt $\mathfrak{A}_n = \langle (ij)(kl) | 1 \leq i, j, k, l \leq n \wedge i, j, k, l$ paarweise verschieden $\rangle$*

Lemma 6. *Es gilt:*

1. $\mathfrak{S}_n' = \mathfrak{A}_n$ *für $n \geq 2$.*
2. $\mathfrak{A}_n' = \mathfrak{A}_n$ *für $n \geq 5$.*

Satz 7. *Die Symmetrische Gruppe $\mathfrak{S}_n$ ist nur für $n = 2, 3, 4$ auflösbar.*

Bemerkung 8. *Für $n \geq 5$ ist $\mathfrak{A}_n$ der einzige nichttriviale Normalteiler der $\mathfrak{S}_n$*

Satz 9. *Für $n \geq 5$ ist $\mathfrak{A}_n$ einfach.*

2 Ringtheorie

2.1 Grundstrukturen mit zwei Verknüpfungen

Definition 1. *Eine Menge R mit zwei Verknüpfungen $+, \cdot : R \times R \to R$ heißt* Halbring *(Ring ohne Eins), wenn*

1. *$(R, +)$ eine abelsche Gruppe mit neutralem Element 0 ist,*
2. *$(R, \cdot)$ eine Halbgruppe ist, und*
3. *die* Distributivgesetze
$$\forall r, s, t \in R : r(s + t) = rs + rt$$
$$\forall r, s, t \in R : (r + s)t = rt + st$$
gelten. Ein Halbring heißt Ring *(Ring mit Eins), wenn $(R \setminus \{0\})$ ein Monoid mit neutralem Element ist. Ein Halbring R heißt kommutativ, wenn $\forall r, s \in R : rs = sr$*

Bemerkung 2. *In jedem Halbring gilt: $\forall r \in R : 0r = r0 = 0$.*

Definition 3. *Sei R ein Halbring. Ein Element $r \in R \setminus \{0\}$ heißt* Nullteiler, *falls $\exists s \in R \setminus \{0\} : rs = 0$. Ein kommutativer Ring ohne Nullteiler heißt* Integritätsring.

Lemma 5. *Es gilt:*

1. *Sei R ein Halbring und $S \subseteq R$ die Menge der Nichtnullteiler. Dann ist $(S, \cdot)$ eine Halbgruppe (Monoid, wenn R Ring).*
2. *Sei R ein Ring und $R^\times = \{r \in R | \exists s \in R : rs = sr = 1\}$. Dann ist $(R^\times, \cdot)$ eine Gruppe und es gilt $R^\times \subseteq S$.*

Definition 6. *Die Elemente von $R^\times := \{r \in R | \exists s \in R : rs = sr = 1\}$ heißen* Einheiten, *$R^\times$ ist die Einheitengruppe. Ein Ring R ist ein* Schiefkörper, *wenn $R^\times = R \setminus \{0\}$. Ein kommutativer Schiefkörper ist ein* Körper .

Satz 7. *Jeder endliche Schiefkörper ist ein Körper*

Definition 9. *Sei R ein (Halb-)Ring.*

1. *$S \subseteq R$ heißt Unter(halb-)ring, geschrieben $S \leq R$, falls $(S, +, \cdot)$ (Halb-)Ring (mit $1_S = 1R$)*
2. *$I \subseteq R$ heißt (zweiseitiges)* Ideal , *geschrieben $I \trianglelefteq R$, falls $(I, +, \cdot)$ ein (Halb-)ring ist und gilt: $RI \subseteq I$ und $IR \subseteq I$*

Bemerkung 10. *Sei R ein Ring. Das Einheitsideal $I = R$ ist das einzige Ideal mit $1 \in I$. Ist R ein Schiefkörper, so sind das Nullideal $0 = \{0\}$ und das Einheitsideal die einzigen Ideale.*

Lemma 11. *Sei R ein Ring, $I, J \trianglelefteq R$ Ideale. Dann ergeben die folgenden Operationen wieder ein Ideal:*

1. *$I \cap J \trianglelefteq R$*
2. *$I + J := \{r + s | r \in I, s \in J\} \trianglelefteq R$*
3. *$IJ := \{\sum_{i=1}^{n} r_i s_i | n \in \mathbb{N}, r_i \in I, s_i \in J\} \trianglelefteq R$*

Definition 12. *Sei R ein kommutativer Ring und $r_1, ..r_k \in R$. Dann heißt $I = \langle r_1, ..r_k \rangle = Rr_1 + .. + Rr_2$ das von $r_1, ..r_k$* erzeugte Ideal. *Ein Ideal $I \trianglelefteq R$ heißt* Hauptideal , *wenn $\exists r \in I : I = \langle r \rangle$. Wenn R ein Integritätsring und jedes $I \trianglelefteq R$ ein Hauptideal ist, heißt R* Hauptidealring.

Satz 13. *$\mathbb{Z}$ ist ein Hauptidealring.*

Definition 14. *Sei R ein Halbring. Eine Äquivalenzrelation $\equiv$ auf R heißt* Kongruenzrelation, *wenn*
$$\forall r, \bar{r}, s, \bar{s} \in R : r \equiv \bar{r}, s \equiv \bar{s} \Rightarrow rs \equiv \bar{r}\bar{s} \wedge r + s \equiv \bar{r} + \bar{s}$$

Lemma 15. *Sei $\equiv$ eine Kongruenzrelation auf dem (Halb-)Ring R. Dann ist die Menge der Äquivalenzklassen $R/\equiv$ wieder ein (Halb-)Ring, der* Faktor(halb-)Ring.

Satz 16. *Sei $\equiv$ eine Kongruenzrelation auf dem Halbring R. Dann ist $I = [0]$ ein Ideal in R und es gilt: $r \equiv s \Leftrightarrow (r-s) \in I$. Sei umgekehrt $I \trianglelefteq R$ ein Ideal. Dann definiert $r \equiv s \Leftrightarrow (r-s) \in I$ eine Kongruenzrelation auf R.*

Definition 17. *Sei R ein kommutativer Ring. Ein Ideal $M \triangleleft R$ heißt* maximal, *wenn $M \subsetneqq I \trianglelefteq R \Rightarrow I = R$. Bei einem* Primideal *$P \trianglelefteq R$ folgt aus $rs \in P$ daß entweder $r \in P$ oder $s \in P$.*

Bemerkung 18. *Jedes maximale Ideal ist prim.*

Bemerkung 19. *Für $R = \mathbb{Z}$ gilt: $0 \neq P \trianglelefteq \mathbb{Z}$ Primideal $\Leftrightarrow P = \langle p \rangle$ mit p Primzahl $\Leftrightarrow P \trianglelefteq \mathbb{Z}$ maximales Ideal*

Satz 20. *Sei R ein kommutativer Ring.*

1. *$P \trianglelefteq R$ ist genau dann ein Primideal, wenn R/P ein Integritätsring ist.*
2. *$M \triangleleft R$ ist genau dann maximales Ideal, wenn R/M ein Körper ist.*

Korollar 21. *Sei R ein kommutativer Ring mit den einzigen Idealen $0, R$. Dann ist R ein Körper.*

2.2 Homomorphismen

Definition 1. *Seien R, S Halbringe. Eine Abbildung $\phi : R \to S$ heißt* Halbringhomomorphismus, *wenn*

$$\forall r_1, r_2 \in R : \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \wedge \phi(r_1 r_2) = \phi(r_1)\phi(r_2)$$

Sind R, S Ringe, so ist $\phi : R \to S$ Ringhomomorphismus, *wenn zusätzlich $\phi(1_R) = 1_S$.*

Satz 3. Homomorphiesatz: *Seien R, S (Halb-) Ringe und $\phi : R \to S$ (Halb-) Ringhomomorphismus. Dann gilt:*

1. *$\operatorname{im}\phi \leq S$ ist ein Unter (Halb-) Ring,*
2. *$\ker\phi \trianglelefteq R$ ist ein Ideal und*
3. *$R/\ker\phi \cong \operatorname{im}\phi$*

Bemerkung 4. *Wenn R, S Körper, dann ist jeder Homomorphismus $\phi : R \to S$ injektiv.*

Lemma 5. *Sei R ein Integritätsring. Dann gibt es genau einen Ringhomomorphismus $\phi : \mathbb{Z} \to R$ und für diesen ist $\ker\phi$ ein Primideal.*

Definition 6. *Sei R ein Ring ohne Nullteiler und $\phi : \mathbb{Z} \to R$ obiger eindeutige Homomorphismus. Dann heißt $p \in \mathbb{P} \cup \{0\}$ mit $\ker\phi = \langle p \rangle$ die* Charakteristik *von R, geschrieben $\operatorname{char} R$*

Satz 8. Chinesischer Restsatz: *Sei R ein Ring und $I_1, ..I_n \trianglelefteq R$ Ideale mit $I_k + I_l = R$ für alle $1 \leq k, l \leq n$. Dann existiert ein Isomorphismus*

$$\phi : R/\bigcap_{k=1}^{n} I_k \to R/I_1 \times .. \times R/I_n$$

2.3 Halbgruppenringe und Polynome

Definition 1. *Ein Monoid $(S, \cdot)$ heißt* Monoid mit Endlichkeitsbedingung, *wenn gilt:*

$$\forall s \in S : |\{(r,t) \in S \times S | rt = s\}| < \infty$$

Sei R ein kommutativer Ring und S ein Monoid mit Endlichkeitsbedingung. Eine Abbildung $f \in R^S$ heißt finit, *falls die Menge $S_f = \{s \in S | f(s) \neq 0\}$ endlich ist. Wir schreiben: $R[S] \subseteq R^S$ für die Menge der finiten Abbildungen.*

Satz 2. *Die Menge $R[S]$ mit den Verknüpfungen*

$$+ : R[S] \times R[S] \to R[S], (f+g)(s) = f(s) + g(s)$$

und

$$\cdot : R[S] \times R[S] \to R[S], (f \cdot g)(s) = \sum_{rt=s} f(r) \cdot g(t)$$

ist ein Ring.

Bemerkung 3. *Es gilt:*

1. *Ist S kommutativ, so auch $R[S]$*
2. *Für $s \in S$ setzen wir*
$$e_s(r) := \begin{cases} 1_R & \text{für } r = s \\ 0_R & \text{für } r \neq s \end{cases}$$
Dann gilt: $\sigma : S \to R[S], s \mapsto e_s$ ist ein injektiver Monoidhomomorphismus.
3. *$\rho : R \to R[S], r \mapsto re$ ist ein injektiver Ringhomomorphismus.*

Definition 4. *Der Ring $(R[S], +, \cdot)$ heißt* Halbgruppenring *(bzw.* Gruppenring, *falls S eine Gruppe).*

Bemerkung 6. *$R[S]$ enthält nur finite Abbildungen. Ohne diese Einschränkung erhält man den Ring $R[[S]]$. Speziell für $S \in \mathbb{N}^n$ ist dies der Ring der formalen Potenzreihen.*

Satz 7. Universelle Abbildungseigenschaft für Halbgruppenringe: *Sei R ein kommutativer Ring und S ein Monoid. Weiter sei $R[S]$ der zugehörige Halbgruppenring mit obigen Einbettungen $\sigma : S \to R[S], \rho : R \to R[S]$. Dann gibt es zu jedem kommutativen Ring R' mit einem Ringhomomorphismus $\phi : R \to R'$ sowie einen Monoidhomomorphismus $\psi : S \to R'$ genau einen Ringhomomorphismus $\Psi : R[S] \to R'$ mit $\psi = \Psi \circ \sigma$ und $\phi = \Psi \circ \rho$.*

Korollar 8. *Seien R, R', ϕ, ρ wie oben, ferner sei $S = (\mathbb{N}, t)$ so dass $R[S] = R[X]$ der univariante Polynomring ist. Dann existiert zu jedem $r' \in R'$ genau ein Ringhomomorphismus $\Phi : R[x] \to R'$ mit $\phi = \Phi\rho$ und $\Phi(x) = r'$*

Definition 9. *Sei R ein Ring, $R \subseteq R'$.*

1. *Ein Element $r' \in R'$ heißt* Nullstelle *des Polynom $f \in R[x]$ falls $f(r') = 0$*
2. *Sei $f = \sum_{i \geq 0} a_i x^i \in R[X] \setminus \{0\}$. Dann heißt die Zahl $\deg(f) = max\{i \in \mathbb{N} | a_i \neq 0\}$ der* Grad *von f. Für das Nullpolynom setzen wir $\deg(0) = -\infty$.*

Lemma 10. *Seien $f, g \in R[X]$. Dann gilt*

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(fg) \leq \deg(f) + \deg(g)$

Bemerkung 11. *Ist R Integritätsring, so gilt $\deg(fg) = \deg(f) + \deg(g)$, somit ist auch $R[X]$ Integritätsring.*

Satz 12. Division mit Rest: *Seien $f = \sum_{i=1}^{n} a_i x^i, g = \sum_{j=0}^{m} b_j x^j \in R[X]$ zwei Polynome mit $b_m \in R^\times$. Dann gibt es zwei eindeutig bestimmte Polynome $q, r \in R[X]$ so dass*

1. *$f = qg + r$ und*
2. $\deg(r) < \deg(g)$

Korollar 13. *Sei $s \in R$ eine Nullstelle von $f \in R[X]$. Dann gilt: $(x - s) | f$*

Korollar 14. *Sei R ein Integritätsbreich und $f \in R[X]$ ein Polynom mit $\deg(f) = n > 0$. Dann besitzt f in R höchstens n Nullstellen.*

2.4 Zerlegung in Primfaktoren

Es sei in diesem Abschnitt R ein Integritätsring.

Definition 1. *Seien $r, s \in R$. Wir sagen r teilt s, geschrieben $r|s$, falls $\exists t \in R : s = rt$, d.h. $\langle r \rangle \supseteq \langle s \rangle$. Wir sagen r ist* ASSOZIIERT *zu s, geschrieben $r \simeq s$, falls $\exists t \in R^\times$: s=rt (dann gilt $r|s$) und $s|r$, d.h. $\langle r \rangle = \langle s \rangle$. r ist ein* TRIVIALER TEILER *von s, falls $r \simeq s$ oder $r \simeq 1$. Ein Element $u \in R \backslash R^\times$ heißt* IRREDUZIBEL *(unzerlegbar), wenn en nur triviale Teiler besitzt. $p \in R \backslash R^\times$ ist ein* PRIMELEMENT, *wenn*

$$\forall r, s \in R : p|rs \Rightarrow p|r \vee p|s$$

Bemerkung 2. *Es gilt:*

1. *$r \simeq s$ definiert eine Äquivalenzklasse*
2. *$R^\times = \{r \in R | r \simeq 1\}$*

Satz 3. *Es gilt:*

1. *$u \in R$ ist genau dann irreduzibel, wenn $\langle u \rangle$ maximal unter allen nichttrivialen Hauptidealen in R ist.*
2. *$p \in R$ ist genau dann prim, wenn $\langle p \rangle$ ein Primideal ist.*

Bemerkung 4. *Sei R ein Hauptidealring, dann gilt: u irreduzibel $\Leftrightarrow \langle u \rangle$ maximal*

Satz 5. *Jedes Primideal ist irreduzibel.*

Satz 7. *Sei R ein Hauptidealring. Dann ist ein Element $p \in R \setminus \{0\}$ genau dann irreduzibel, wenn p prim ist.*

Definition 8. *Seien $r_1, ..r_n \in R$. Ein Element $d \in R$ heißt* GRÖSSTER GEMEINSAMER TEILER *von $r_1, ..r_n$, geschrieben $d = \mathrm{ggT}(r_1, ..r_n)$, wenn d jedes r_i teilt und jedes andere $t \in R$ mit dieser Eigenschaft ein Teiler von d ist. Entsprechend heißt $v \in R$* KLEINSTES GEMEINSAMES VIELFACHE, *geschrieben $v \in \mathrm{kgV}(r_1, ..r_n)$, wenn jedes r_i v teilt und v ein Teiler von $t \in R$ mit dieser Eigenschaft ist.*

Bemerkung 9. ggT *und* kgV *sind nur bis auf assoziierte eindeutige bestimmt.*

Satz 10. *Sei R ein Hauptidealring und $r_1, ..r_n \in R$ derart, dass $\mathrm{ggT}(r_1, ..r_n) \neq 0$. Dann gibt es zu jedem $d \in \mathrm{ggT}(r_1, ..r_n)$ Elemente $s_1, ..s_n \in R$ mit $d = \sum_{i=1}^n s_i r_i$*

Definition 11. *Ein Integritätsring R heißt* EUKLIDISCHER RING, *wenn es eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ gibt so dass*

$$\forall f \in R, g \in R \setminus \{0\} \exists q, r \in R : f = qg + r \wedge (r = 0 \vee \delta(r) < \delta(g))$$

Satz 13. *Jeder euklidische Ring ist ein Hauptidealring.*

Korollar 14. *Wenn K ein Körper, ist $K[X]$ ein Hauptidealring*

Definition 16. *Ein kommutativer Ring R heißt* NOETHERSCH, *wenn jede aufsteigende Kette von Idealen $I_1 \leq I_2 \leq .. \leq R$ stationär wird, d.h.*

$$\exists n \in \mathbb{N} \forall m > n : I_m = I_n$$

Satz 17. *Jeder Hauptidealring ist noethersch.*

Satz 18. *Wenn in dem Integritätsring R jede aufsteigende Kette von Hauptidealen stationär wird, dann läßt sich jede Nichteinheit $0 \neq r \in R \backslash R^\times$ als Produkt endlich vieler irreduzibler Elemente schreiben.*

Definition 19. *Ein Integritätsring R heißt* FAKTORIELLER RING, *wenn sich jede Nichteinheit $0 \neq r \in R \backslash R^\times$ als endliches Produkt irreduzibler Elemente schreiben läßt und die Faktoren dieser Darstellung bis auf die Reihenfolge und Einheiten eindeutig sind.*

Satz 20. *Ein Integritätsring ist genau dann faktoriell, wenn*

1. *jede aufsteigende Kette von Hauptidealen stationär wird und*
2. *jedes unzerlegbare Element von R auch prim ist.*

Korollar 21. *Jeder Hauptidealring ist faktoriell*

Bemerkung 22. *Wenn $\mathbb{P}_R$ ein Vertretersystem der assoziierten Primelemente in einem faktoriellen Ring R, dann läßt sich jedes Element $0 \neq r \in R \backslash R^\times$ eindeutig in der Form*

$$r = \epsilon \prod_{p \in \mathbb{P}_R} p^{ord_p(r)}$$

zerlegen.

2.5 Quotientenringe

Lemma 1. *Sei R ein kommutativer Ring, $S \leq R \setminus \{0\}$ ein Untermonoid von $(R, \cdot)$. Dann wird durch*

$$(r_1, s_1) \sim (r_2, s_2) :\Leftrightarrow \exists s \in S : s(s_2 r_1 - s_1 r_2) = 0$$

eine Äquivalenzrelation definiert auf $R \times S$.

Satz 2. *Unter den Voraussetzungen von Lemma 1 ist $S^{-1}R$ mit den Verknüpfungen*

$$+ : S^{-1}R \times S^{-1}R, (r_1/s_1, r_2/s_2) \mapsto (r_1 s_2 + s_1 r_2)/s_1 s_2$$

$$\cdot : S^{-1}R \times S^{-1}R, (r_1/s_1, r_2/s_2) \mapsto r_1 r_2 / s_1 s_2$$

ein kommutativer Ring. Darüber hinaus ist

$$\lambda_S : R \to S^{-1}R, r \mapsto r/1$$

ein Ringhomomorphismus mit $\lambda_S(S) \leq (S^{-1}R)^\times$

Bemerkung 3. *λ_S ist injektiv falls S keine Nullteiler von R enthält.*

Satz 4. UNIVERSELLE ABBILDUNGSEIGENSCHAFT FÜR QUOTIENTENRINGE: *Sei R ein kommutativer Ring, $S \leq R \backslash \{0\}$ ein Untermonoid. Wenn T ein weiterer kommutativer Ring mit einem Ringhomomorphismus $\phi : R \to T$ mit $\phi(S) \subseteq T^\times$ ist, dann existiert genau ein Ringhomomorphismus $\Psi : S^{-1}R \to T$ mit $\Psi \circ \lambda(S) = \phi$*

Lemma 5. *Sei R ein Integritätsring und $S = R \backslash \{0\}$. Dann ist $S^{-1}R$ ein Körper.*

Definition 6. *Der Ring $S^{-1}R$ mit $\lambda(S) : R \to S^{-1}R$ heißt* QUOTIENTENRING *von R bzgl. S. Wenn R ein Integriätsbereich und $S = R \backslash \{0\}$ ist, erhält man den* QUOTIENTENKÖRPER *von R, geschrieben* $\mathrm{Quot}(R)$

Lemma 8. *Sei R ein kommutativer Ring, $I \trianglelefteq R$ ein Ideal und $S \leq R \backslash \{0\}$ ein Untermonoid. Dann ist*

$$S^{-1}I = \{r/s | r \in I, s \in S\}$$

ein Ideal im Quotientenring.

Satz 9. *Sei R ein kommutativer Ring und $P \trianglelefteq R$ ein Primideal. Dann besitzt für $S = R \backslash P$ der Quotientenring $S^{-1}R$ nur ein maximales Ideal, nämlich $S^{-1}R \backslash (S^{-1}R)^\times$*

Definition 10. *Ein kommutativer Ring mit einem einzigen maximalen Ideal heißt* LOKALER RING. *Wenn $P \trianglelefteq R$ ein Primideal ist und $S = R \backslash P$, dann heißt $R_P = S^{-1}R$ die Lokalisierung von R bei P (mit maximalem Ideal $M_P = S^{-1}P$)*

Satz 11. *Sei R ein kommutativer Ring und $P \trianglelefteq R$ Primideal. Dann gilt:* $\mathrm{Quot}(R/P) \cong R_P / M_P$

2.6 Teilbarkeit in Polynomringen

Definition 1. *Sei R ein fakorieller Ring und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. Dann heißt $c(f) \in \mathrm{ggT}(a_0, ..a_n)$* Inhalt *von f. Das Polynom f heißt* primitiv, *wenn $c(f) \simeq 1$, d.h. $c(f) \in R^\times$.*

Lemma 2. Gausssches Lemma: *Sei R ein faktorieller Ring. Dann gilt für $f, g \in R[x]$, daß $c(fg) \simeq c(f)c(g)$.*

Satz 3. *Sei R ein faktorieller Ring, $K = \mathrm{Quot}(R)$ der zugehörige Quotientenkörper. Dann sind für ein primitives Polynom $f \in R[x]$ die folgenden Aussagen äquivalent:*

1. *f ist irreduzibel in $R[x]$*
2. *f ist irreduzibel in $K[x]$*
3. *f ist Primelement in $K[x]$*
4. *f ist Primelement in $R[x]$*

Lemma 4. *Sei R ein Integritätsring. $p \in R$ ist genau dann prim, wenn p auch ein Primelement von $R[x]$ ist.*

Satz 5. Satz von Gauss: *$R[x]$ ist genau dann faktoriell, wenn R faktoriell ist.*

Bemerkung 6. *$\mathbb{Z}[x]$ ist faktoriell, aber $\mathbb{Z}[x]$ ist kein Hauptidealring, da $\langle 2, x\rangle$ Ideal.*

Satz 7. Kronecker-Verfahren zur Primzerlegung: *Sei R ein faktorieller Ring mit endlicher Einheitengruppe, in dem Primzerlegung in endlich vielen Schritten möglich ist. Dann kann auch in $R[x]$ eine Primzerlegung in endlich vielen Schritten berechnet werden.*

Bemerkung 8. *Durch vollständige Induktion kann der vorstehende Satz auch auf $R[x_1, ...x_n]$ erweitert werden.*

Lemma 10. *Seien R, $\overline{R}$ Integritätsringe, $\phi : R \to \overline{R}, r \mapsto \overline{r} := \phi(r)$ ein Ringhomomorphismus, der durch $\overline{\phi}(x) = x$ zu einem Homomorphismus $\overline{\phi} : R[x] \to \overline{R}[x]$ fortgesetzt wird. Weiter sei $f = \sum_{i=0}^{n} a_i r^i \in R[x]$ ein primitives Polynom mit $\overline{a}_n \neq 0$. Wenn $\overline{f} = \overline{\phi}(f) \in \overline{R}[x]$ irreduzibel ist, dann ist auch $f \in R[x]$ irreduzibel.*

Satz 11. Eisenstein-Kriterium: *Sei R ein Integritätsring, $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ ein primitives Polynom. Wenn es ein Primelement $p \in \mathbb{P}_R$ gibt mit*

1. *$p \nmid a_n$*
2. *$p | a_i, 0 \leq i \leq n$*
3. *$p^2 \nmid a_0$*

dann ist f irreduzibel in $R[x]$

Korollar 12. *Sei $p \in \mathbb{P}$ Primzahl. Dann ist $f = x^{p-1} + .. + x + 1 \in \mathbb{Z}[x]$ irreduzibel.*

3 Körpertheorie

3.1 Der Aufbau eines Körpers

Definition 1. *Sei K ein Körper. Ein* Teilkörper *ist ein Unterring $T \leq K$ der selbst wieder ein Körper ist. K wird dann auch Oberkörper oder* Erweiterungskörper *von T genannt. Da der Durchschnitt zweier Teilkörper wieder ein Körper ist, enthält K einen eindeutig bestimmten Teilkörper, den* Primkörper *$P = \bigcap_{T \ Teilkörper} T$*

Satz 2. *Sei K ein Körper mit Primkörper P. Dann gilt:*

1. $\mathrm{char}\, K = p > 0 \Leftrightarrow P \cong \mathbb{F}_p = (\mathbb{Z}_p, +, *)$
2. $\mathrm{char}\, K = 0 \Leftrightarrow P \cong \mathbb{Q}$

Lemma 3. *Es gilt:*

1. Φ *injektiv* $\Rightarrow K[X] \cong K[\theta] \wedge K(\theta) = \mathrm{Quot}(K[\theta]) \cong K(x)$
2. Φ *nicht injektiv* $\Rightarrow \exists 0 \neq f_\theta \in K[X] : \ker \Phi = \langle f_\theta \rangle \wedge K(\theta) \cong K[x]/\langle f_\theta \rangle$

Definition 4. *Seien $K \leq L$ Körper. Ein Element θ heißt* TRANSZENDENT *über K, wenn $K(x) \cong K(\theta)$. L/K ist eine* TRANSZENDENTE KÖRPERERWEITERUNG, *wenn $\exists \theta \in L : \theta$ transzendent. Ein Element $\theta \in L$ heißt algebraisch, wenn*

$$\exists 0 \neq f \in K[x] : K(\theta) \cong K[x]/\langle f_\theta \rangle$$

Das eindeutig bestimmte normierte Polynom mit dieser Eigenschaft ist das MINIMALPOLYNOM *von θ. L/K ist eine* ALGEBRAISCHE KÖRPERERWEITERUNG, *wenn alle $\theta \in L$ algebraisch sind.*

Definition 6. *Seien $K \leq L$ Körper. Elemente $\theta_1, ..\theta_n \in L$ heißen* ALGEBRAISCH UNABHÄNGIG *über K, wenn*

$$\forall f \in K[x_1, ..x_n] : f(\theta_1, ..\theta_n) = 0 \Rightarrow f = 0$$

Andernfalls sind $\theta_1, ..\theta_n$ algebraisch abhängig. Eine Teilmenge $S \subseteq L$ ist algebraisch unabhängig über K wenn jede endliche Teilmenge S es ist. Eine algebraisch unabhängige Teilmenge $B \leq L$ ist eine TRANSZENDENZBASIS *von L/K, wenn $L/K(B)$ algebraisch ist. L/K ist eine* TRANSZENDENTE KÖRPERERWEITERUNG, *wenn eine Tranzendenzbasis existiert, so dass $L = K(B)$.*

Lemma 7. ZORNSCHES LEMMA: *Sei $M \neq \emptyset$ eine partiell geordnete Menge. Wenn für jede total gerordnete Teilmenge von M eine obere Schranke in M existiert, dann besitzt M ein maximales Element.*

Lemma 8. SATZ VON SCHRÖDER-BERNSTEIN: *Zu den Mengen M, N gebe es zwei injektive Abbildungen $\alpha : M \to N, \beta : N \to M$. Dann sind M, N gleichmächtig.*

Lemma 9. *Es gilt:* $\mathrm{card}\, M \leq N \wedge \mathrm{card}\, N \leq M \Rightarrow \mathrm{card}\, N = \mathrm{card}\, M$

Lemma 10. *Jede unendliche Menge ist disjunkte Vereinigung abzählbar vieler Mengen*

Satz 11. *Sei L/K Körpererweiterung.*

1. *Es existiert eine Transzendenzbasis von L/K*
2. *Jede über K algebraisch unabhängige Menge $B' \subset L$ läßt sich zu einer Transzendenzbasis B von L/K erweitern.*
3. *Alle Tranzendenzbasen von L/K sind gleichmächtig*

3.2 Algebraische Erweiterungen

Bemerkung 1. *Sei L/K Körpererweiterung. Dann ist L ein K-Vektorraum.*

Definition 2. *$[L : K] = dim_K L$ heißt* GRAD DER KÖRPERERWEITERUNG *L/K. Für $[L : K] < \infty$ spricht man von einer endlichen Körpererweiterung.*

Satz 3. *Es gilt:*

1. *Jede endliche Körpererweiterung ist algebraisch.*
2. *Sei $\theta \in L$ algebraisch über K mit Minimalpolynom f_θ. Dann gilt:*

$$[K(\theta) : K] = \deg f_\theta$$

Satz 4. *Seien $K \leq L \leq M$ Körper. M/K ist genau dann endlich, wenn M/L und L/K endlich ist. Es gilt dann*

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

Korollar 5. *Sei M/K endlich und $\theta \in M$ mit Minimalpolynom f_θ. Dann gilt: $g_\theta = f_\theta^{[M:K(\theta)]}$.*

Definition 6. *$g_\theta \in K[x]$ heißt* HAUPTPOLYNOM *von θ und hängt nur von θ und M ab.*

Definition 7. *Eine Körpererweiterung L/K heißt* EINFACH *, wenn*

$$\exists \theta \in L : L = K(\theta)$$

L/K ist ENDLICH ERZEUGT, *wenn*

$$\exists n \in \mathbb{N}, \theta_1, ..\theta_n \in L : L = K(\theta_1, ..\theta_n)$$

Satz 8. *L/K ist genau dann eine endliche Erweiterung, wenn*

$$\exists n \in \mathbb{N}, \theta_1, ..\theta_n \in L : L = K(\theta_1, ..\theta_n) \wedge \theta_1, ..\theta_n \text{ algebraisch über } K$$

Bemerkung 9. *Seien $K \leq L \leq M$ Körper und L/K algebraisch. Ist $\theta \in M$ algebraisch über L, dann ist θ algebraisch über K.*

Korollar 10. *Seien $K \leq L$ Körper. Dann ist $\tilde{K} := \{\theta \in L | \theta \text{ algebraisch über } K\}$ ein Körper.*

Definition 11. *$\tilde{K}$ heißt der* ALGEBRAISCHE ABSCHLUSS *von K in L*

3.3 Der algebraische Abschluß

Definition 1. *Ein Körper K heißt* ALGEBRAISCH ABGESCHLOSSEN, *wenn jedes nichtkonstante Polynom $f \in K[x]$ eine Nullstelle in K besitzt (d.h. jedes solche Polynom zerfällt über K in Linearfaktoren).*

Definition 3. *Seien $K \leq L$ und $K \leq M$ Körpererweiterungen. Ein Körperhomomorphismus $\phi : L \to M$ heißt* K-HOMOMORPHISMUS, *wenn $\phi \mid_K = id_K$. Wir schreiben $\mathrm{End}(L/K)$ für die Menge aller K-Endomorphismen und $\mathrm{Aut}(L/K)$ für die Menge aller K-Automorphismen.*

Satz 4. SATZ VON KRONECKER: *Sei K ein Körper und $f \in K[x]$ ein normiertes, irreduzibles Polynom. Dann existiert eine endliche Körpererweiterung L/K vom Grad n mit einem $\theta \in L$, so dass $f(\theta) = 0$ und $L = K(\theta)$. L ist durch diese Bedingung bis auf K-Isomorphie eindeutig bestimmt.*

Satz 5. *Seien K, K' Körper mit einem Isomorphismus $\phi : K \to K'$, $a \mapsto a'$, sowie den induzierten Isomorphismus $\phi' : K[x] \to K'[x]$, $f \mapsto f'$. Sei $f \in K[x]$ prim und $L = K(\theta)$ mit $f(\theta) = 0$ sowie $L' = K'(\theta^*)$ mit $f'(\theta^*) = 0$. Dann existiert ein eindeutig bestimmter Isomorphismus $\Phi : L \to L'$ mit $\Phi(\theta) = \theta^*$ und $\Phi \mid_K = \phi$.*

Definition 6. *Ein Körper L mit der Eigenschaft des Satzes von Kronecker heißt* STAMMKÖRPER *des Polynoms $f \in K[x]$*

Lemma 7. *Sei $I \subsetneq R$ ein Ideal in einem Ring $R \neq 0$. Dann besitzt R ein maximales Ideal M mit $I \leq M$.*

Satz 8. *Zu jedem Körper K existiert ein algebraisch abgeschlossener Erweiterungskörper L*

Korollar 10. *Zu jedem Körper K existiert ein algebraisch abgeschlossener Erweiterungskörper $\bar{K}/K$, die algebraisch ist.*

Definition 11. *$\bar{K}$ nennt man einen algebraischen Abschluss von K.*

Satz 12. *Sei L/K eine algebraische Erweiterung und $\phi : K \to M$ ein Körperhomomorphismus in einem algebraisch abgeschlossenen Körper M. Dann existiert eine Fortsetzung $\Phi : L \to M$ mit $\Phi \mid_K = \phi$. Wenn L ebenfalls algebraisch abgeschlossen und $M/\operatorname{im}\phi$ algebraisch ist, dann ist jede Fortsetzung ein Isomorphismus.*

Korollar 13. *Seien $\bar{K}_1$,$\bar{K}_2$ zwei algebraische Abschlüsse von K. Dann existiert ein K-Isomorphismus $\bar{K}_1 \to \bar{K}_2$.*

3.4 Normale Körpererweiterungen

Definition 1. *Sei $F = \{f|i \in I\} \subseteq K[x]$ eine Menge nichtkonstanter Polynome über Körper K. Ein Erweiterungskörper heißt* ZERFÄLLUNGSKÖRPER *von F, wenn*

1. *jedes Polynom $f_i \in F$ über L vollständig in Linearfaktoren zerfällt, und*
2. *die Erweiterung L/K von den Nullstellen der f_i erzeugt wird.*

Definition 3. *Eine algebraische Körpererweiterung N/K heißt* NORMAL, *wenn jedes irreduzible Polynom $f \in K[x]$, das eine Nullstelle in N besitzt, über N vollständig in Linearfaktoren zerfällt.*

Satz 5. *Sei K ein Körper, $\bar{K}$ ein algebraischer Abschluss von K. Ferner sei N/K eine algebraische Erweiterung. Dann sind folgende Aussagen äquivalent:*

1. *N/K ist normal*
2. *N ist ein Zerfällungskörper einer Menge von irreduziblen Polynomen*
3. *Jeder K-Homomorphismus $\phi : N \to \bar{N}$ liegt in $Aut(N/K)$*

Bemerkung 6. *Folgende Aussagen sind äquivalent:*

1. *N/K normal und endlich*
2. *N Zerfällungskörper eines Polynoms.*

Bemerkung 7. *Seien $K \leq L \leq M$ algebraische Körpererweiterungen. Wenn M/K normal ist, dann auch M/L.*

Definition 9. *Sei L/K eine algebraische Erweiterung. Eine algebraische Erweiterung N/L heißt* NORMALE HÜLLE *von L/K, wenn N/K normal ist aber kein echter Teilkörper $K \leq N' \leq N$ normal über K ist.*

Satz 10. *Sei L/K eine algebraische Erweiterung. Dann existiert eine bis auf L-Isomorphie eindeutig bestimmte normale Hülle N/L.*

Lemma 11. *Sei $\mathbb{F}$ ein endlicher Körper. Dann gilt $p = \operatorname{char} \mathbb{F} > 0$ so dass der Primkörper von $\mathbb{F}$ isomorph zu $\mathbb{F}_p$ ist. Außerdem gilt: $|\mathbb{F}| = p^n$ mit $n = [\mathbb{F} : \mathbb{F}_p]$ und $\mathbb{F}$ ist ein Zerfällungskörper zu $x^q - x \in \mathbb{F}_p[x]$ (also $\mathbb{F}/\mathbb{F}_p$ normal).*

Lemma 12. *Sei $f \in K[x]$ und $\theta \in L/K$ eine Nullstelle. θ ist genau dann eine mehrfache Nullstelle, wenn $f'(\theta) = 0$*

Satz 13. *Zu jedem $p \in \mathbb{P}$, $n \in N$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit $|\mathbb{F}_q| = q = p^n$, nämlich den Zerfällungskörper von $x^q - x$ über $\mathbb{F}_q$.*

Lemma 14. *Sei G eine abelsche Gruppe. Wenn G zwei Elemente endlicher Ordnung m bzw. n enthält, dann gibt es in G auch ein Element der Ordnung $\operatorname{kgV}(m, n)$.*

Satz 15. *Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist U zyklisch. Ist also insbesondere K ein endlicher Körper $\mathbb{F}_q$, so ist $\mathbb{F}_q^\times$ eine zyklische Gruppe der Ordnung $q - 1$.*

3.5 Separable Körpererweiterungen

Definition 1. *Sei K ein Körper. Ein Polynom $f \in K[x]$ heißt* SEPARABEL, *wenn f in $\bar{K}$ keine mehrfachen Nullstellen hat. Sei L/K eine algebraische Erweiterung. Ein Element $\theta \in L$ heißt separabel über K, falls sein Minimalpolynom $f_\theta \in K[x]$ separabel ist. Die Erweiterung L/K heißt separabel, wenn alle $\theta \in L$ separabel sind.*

Lemma 2. *Sei K ein Körper und $f \in K[x]$ ein Polynom mit $\deg f \geq 1$*

1. *Die mehrfachen Nullstellen von f in einem algebraischen Abschluss $\bar{K}$ sind gerade die Nullstellen von $\operatorname{ggT}(f, f')$.*

2. *Ein irreduzibles Polynom f besitzt genau dann mehrfache Nullstellen, wenn $f' = 0$.*

Satz 3. *Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom.*

1. *Wenn $\operatorname{char} K = 0$, dann ist f separabel.*
2. *Für $\operatorname{char} K > 0$ ist f genau dann inseparabel wenn ein Polynom $g \in K[x]$ existiert mit $f(x) = g(x^p)$.*

Definition 5. *Ein Körper K heißt* VOLLKOMMEN, *wenn alle irreduziblen Polynome $f \in K[x]$ separabel sind.*

Definition 7. *Sei L/K eine endliche Körpererweiterung und $\bar{K}$ ein algebraischer Abschluss. Wir setzen $Hom_K(L, \bar{K}) = \{\phi : L \to \bar{K} | \phi$ K-Homomorphismus$\}$. Dann ist der* SEPARABILITÄTSGRAD *$[L : K]_S = |Hom_K(L, \bar{K})|$. Da alle algebraischen Abschlüsse isomorph sind, ist diese Definition unabhängig von $\bar{K}$.*

Lemma 8. *Sei K ein Körper und $L \geq K$ der Stammkörper zu dem irreduziblen Polynom $f \in K[x]$. Dann gilt:*

1. *$[L : K]_S \leq [L : K]$*
2. *$[L : K]_S = [L : K]$ genau dann wenn f separabel.*

Satz 9. *Seien $M \geq L \geq K$ endliche Körpererweiterungen. Dann gilt:*

$$[M : K]_S = [M : L]_S [L : K]_S$$

Satz 10. *Sei L/K eine endliche Körpererweiterung.*

1. *Wenn $\operatorname{char} K = 0$, so ist $[L : K] = [L : K]_S$*
2. *Für $\operatorname{char} K = p > 0$ existiert ein $r \in \mathbb{N}$ mit $[L : K] = p^r [L : K]_S$*

Satz 11. *Sei L/K eine endliche Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*

1. *L/K ist separabel*
2. *$\exists \theta_1, ..\theta_n \in L : \theta_1, ..\theta_n separabel \wedge L = K(\theta_1, ..\theta_n)$*
3. *$[L : K] = [L : K]_S$*

Korollar 12. *Seien $K \leq L \leq M$ algebraische Körpererweiterungen. M/K ist genau dann separabel, wenn M/L und L/K separabel sind.*

Satz 13. SATZ VOM PRIMITIVEN ELEMENT: *Sei L/K eine endliche (separable) Körpererweiterung. Dann existiert ein primitives Element $\theta \in L$ mit $L = K(\theta)$.*

Definition 14. *Sei K ein Körper. Ein Polynom $f \in K[x]$ heißt* REIN INSEPARABEL, *wenn es in einem algebraischen Abschluss $\bar{K}$ genau eine Nullstelle besitzt. Sei L/K eine algebraische Erweiterung. Ein Element $\theta \in L$ heißt rein inseparabel, wenn sein Minimalpolynom $f_\theta \in K[x]$ rein inseparabel ist. Die Erweiterung L/K ist rein inseparabel, wenn jedes $\theta \in L$ rein inseparabel ist.*

Bemerkung 15. *Es gilt:*

1. *Ist $\operatorname{char} K = 0$, dann ist jedes irreduzible Polynom separabel.*
2. *Ist $\operatorname{char} K = p > 0$ und $f \in K[x]$ rein inseparabel mit Nullstelle θ, dann ist $f = c f_\theta^n$ mit $c \in K$.*

Bemerkung 16. *Rein inseparable Erweiterungen sind immer normal.*

Satz 18. *Sei L/K eine algebraische Körpererweiterung. Die folgenden Aussagen sind äquivalent:*

1. *L/K rein inseparabel*

2. *Es existiert eine Menge* $B = \{\theta_i \in L | i \in I\}$ *rein inseparabler Elemente, so dass* $L = K(B)$.

3. $[L : K]_S = 1$

4. *Zu jedem* $\theta \in L$ *existiert ein* $n \in \mathbb{N}$, *so dass* $\theta^{(p^n)} \in K$

Satz 19. *Sei* L/K *eine algebraische Körpererweiterung. Dann exisitiert ein eindeutiger Zwischenkörper* $K \leq K_S \leq L$, *so dass* K_S/K *separabel und* L/K_S *rein inseparabel ist.* K_S *ist die* SEPARABLE HÜLLE *von* K *in* L, *d.h.* $K_S = \{\theta \in L | \theta$ *separabel über* $K\}$. *Ferner gilt:* $[L : K]_S = [K_S : K]$.

4 Galoistheorie

4.1 Die Galois-Korrespondenz

Definition 1. *Eine algebraische Erweiterung* L/K *heißt* GALOISCH, *wenn sie normal und separabel ist. In diesem Fall nennt man* $\mathrm{Gal}(L/K) = Aut(L/K)$ *die* GALOIS-GRUPPE .

Lemma 3. *Sei* N/K *eine endliche normale Körpererweiterung. Dann gilt:*

$$|Aut(N/K)| = [N : K]_S \leq [N : K]$$

Offensichtlich ist N/K *genau dann galoisch, wenn* $|Aut(N/K)| = [N : K]$.

Lemma 4. *Seien* $K \leq L \leq M$ *Körpererweiterungen mit* M/K *galoisch.*

1. M/L *ist ebenfalls galoisch und* $\mathrm{Gal}(M/L) \leq \mathrm{Gal}(M/K)$.

2. *Wenn auch* L/K *galoisch ist, so ist*

$$\rho : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K), \sigma \mapsto \sigma|_L$$

ein surjektiver Gruppenhomomorphismus.

Satz 5. SATZ VON ARTIN: *Sei* L *ein Körper und* $G \leq Aut(L)$ *eine Untergruppe.*

1. $K = L^G := \{\theta \in L | \sigma(\theta) = \theta \forall \sigma \in G\}$ *ist ein Körper, der* FIXKÖRPER *von* G.

2. *Für eine endliche Untergruppe* G *ist* L/K *eine endliche Galois-Erweiterung mit* $[L : K] = |G| - 1$ *und* $\mathrm{Gal}(L/K) = G$.

3. *Falls* G *unendlich ist und* L/K *algebraisch, so ist* L/K *eine unendliche Galois-Erweiterung und es gilt* $G \leq \mathrm{Gal}(L/K)$ *(sogar* $G = \mathrm{Gal}(L/K)$*).*

Korollar 6. *Sei* L/K *eine normale algebraische Körpererweiterung und* $G = Aut_K(L)$

1. L/L^G *ist galoisch mit Galois-Gruppe* G.

2. *Ist* L/K *galoisch, so gilt* $L^G = K$.

3. *Ist* L/K *inseparabel, so gilt* L^G/K *rein inseparabel.*

Satz 7. HAUPTSATZ DER GALOIS-THEORIE: *Sei* L/K *eine galoische Erweiterung mit Galois-Gruppe* $G = \mathrm{Gal}(L/K)$. *Wir definieren mit* $\mathcal{U} = \{U | U \leq G\}$ *und* $\mathcal{E} = \{E | K \leq E \leq L\}$ *die Abbildungen*

$$\Phi : \mathcal{U} \to \mathcal{E}, U \mapsto L^U$$

$$\Psi : \mathcal{E} \to \mathcal{U}, E \mapsto \mathrm{Gal}(L/E)$$

und es gilt:

1. $\Phi \circ \Psi = id$, *d.h. insbesondere ist* Φ *surjektiv und* Ψ *injektiv. Wenn* L/K *endlich ist, so gilt auch* $\Psi \circ \Phi = id$, *d.h.* Ψ, Φ *sind zueinander invers.*

2. *Sei $U \leq G$ eine Untergruppe mit $(\Psi \circ \Phi)(U) = U$. Der Fixkörper L^U ist genau dann galoisch über K, wenn U ein Normalteiler von G ist. In diesem Fall gilt für den surjektiven Gruppenhomomorphismus*

$$\rho : G \to \mathrm{Gal}(L^U/K), \sigma \mapsto \sigma|_{L^U}$$

dass $\ker \rho = U$ und ρ induziert einen Isomorphismus $G/U \to \mathrm{Gal}(L^U/K)$.

Definition 8. *Seien $T_1, T_2 \leq K$ zwei Teilkörper. Das* Kompositum *$T_1 \cdot T_2$ ist der kleinste Teilkörper von K der T_1 und T_2 enthält. Offensichtlich gilt: $T_1 \cdot T_2 = T_1(T_2) = T_2(T_1)$.*

Korollar 9. *Sei L/K endliche galoische Erweiterung und E_1, E_2 zwei Zwischenkörper mit Galois-Gruppen $U_1, U_2 \leq G = \mathrm{Gal}(L/K)$. Dann gilt:*

1. $E_1 \leq E_2 \Leftrightarrow U_1 \geq U_2$
2. $E_1 \cdot E_2 = L^{U_1 \cap U_2}$
3. $E_1 \cap E_2 = L^{\langle U_1, U_2 \rangle}$

Bemerkung 10. *Nach Satz 7 haben wir für endliche Galois-Erweiterungen L/K Bijektionen. Nach Korollar 9 drehen sich die Inklusionen um. So etwas nennt man auch* Korrespondenz .

Definition 11. *Eine galoische Erweiterung L/K heißt* abelsch *(bzw.* zyklisch, *) wenn $\mathrm{Gal}(L/K)$ abelsch (bzw. zyklisch) ist.*

Korollar 12. *Sei L/K endliche abelsche (bzw. zyklische) Erweiterung. Dann ist für jeden Zwischenkörper E auch E/K abelsch (bzw. zyklisch).*

Satz 13. Translationssatz: *Sei L/K eine Körpererweiterung mit Zwischenkörper E_1, E_2, die endliche galoische Erweiterungen von K sind. Dann gilt:*

1. *$E_1 \cdot E_2/K$ ist wieder endlich und galoisch.*
2. *Der Homomorphismus $\phi : \mathrm{Gal}(E_1 \cdot E_2/E_1) \to \mathrm{Gal}(E_2/E_1 \cap E_2), \sigma \mapsto \sigma|_{E_2}$ ist bijektiv.*
3. *Der Homomorphismus $\psi : \mathrm{Gal}(E_1 \cdot E_2/K) \to \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K), \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$ ist injektiv und für $E_1 \cap E_2 = K$ sogar bijektiv.*

4.2 Die Galois-Gruppe eines Polynoms

Definition 1. *Sei K ein Körper, $f \in K[x]$ ein nichtkonstantes separables Polynom, und N/K ein Zerfällungskörper von f. Dann heißt $\mathrm{Gal}(f) := \mathrm{Gal}(N/K)$ die* Galois-Gruppe des Polynoms *f.*

Satz 2. *Sei $f \in K[x]$ ein separables Polynom mit $\deg f = n > 0$ und $\theta_1, ..\theta_n \in N$ die Nullstellen von f in einem Zerfällungskörper N/K. Die Abbildung*

$$\rho : \mathrm{Gal}(f) \to S(\{\theta_1, ..\theta_n\}) \cong \mathfrak{S}_n, \sigma \mapsto \sigma|_{\{\theta_1, ..\theta_n\}}$$

definiert eine treue Permutationsdarstellung von $\mathrm{Gal}\, f$, d.h. einen injektiven Gruppenhomomorphismus. Das Polynom f ist genau dann irreduzibel, wenn es transitiv auf $\{\theta_1, ..\theta_n\}$ operiert.

Bemerkung 3. *Sei L/K eine endliche galoische Erweiterung mit $[L : K] = n$. Dann kann $\mathrm{Gal}(L/K)$ als Untergruppe von $\mathfrak{S}_n$ betrachtet werden.*

Definition 6. *Seien k ein Körper und $T_1, ..T_n$ über k algebraisch unabhängig. Wir setzen $L = k(T_1, ..T_n)$ und lassen $\mathfrak{S}_n$ auf L durch Permutation operieren, d.h.*

$$\sigma(f(T_1, ..T_n)) = f(T_{\sigma(1)}, ..T_{\sigma(n)})$$

Dann heißt der zugehörige Fixkörper $K = L^{\mathfrak{S}_n}$ der Körper der symmetrischen rationalen Funktionen . *Das Polynom $f = x^n + T_1 x^{n-1} + .. + T_n$ heißt* allgemeines Polynom vom Grad n.

Bemerkung 7. *$L/L^{\mathfrak{S}_n}$ ist galoische Erweiterung mit $[L:K]=n!$. L ist Zerfällungskörper von*

$$g=\prod_{i=1}^{n}(x-T_i)\in L[x]$$

über K. Man definiert das j-te ELEMENTARSYMMETRISCHE POLYNOM *durch $s_j := T_1 \cdot .. \cdot T_j$.*

Satz 8. *Die elementarsymmetrischen Polynome sind algebraisch unabhängig über k und es gilt $K = k(s_1, ..s_n)$.*

Satz 9. *Das allgemeine Polynom vom Grad n, $f \in k(s_1, ..s_n)$ ist separabel und irreduzibel. Es gilt:* $\mathrm{Gal}(f) = \mathfrak{S}_n$

4.3 Kreisteilungskörper und Einheitswurzeln

Lemma 1. *Sei K ein Körper und N/K ein Zerfällungskörper des Polynoms $f_n = x^n - 1 \in K[x]$ für ein $n \in \mathbb{N}$. Es gilt:*

1. *N/K ist galoisch*
2. *Wenn* $\mathrm{char}\, K \nmid n$, *dann ist $W_n := \{\zeta \in N | f_n(\zeta) = 0\}$ eine zu $(\mathbb{Z}_n, +)$ isomorphe zyklische Untergruppe von $N^\times$*
3. *Falls* $\mathrm{char}\, K = p$ *und $n = p^k m$ mit* $\mathrm{ggT}(p, m) = 1$, *dann ist $W_n \cong (\mathbb{Z}_n, +)$.*

Definition 2. *$\zeta \in W_n$ heißt n-te* EINHEITSWURZEL. *Falls $W_n = \langle\zeta\rangle$, spricht man von einer* PRIMITIVEN EINHEITSWURZEL.

Definition 4. *Die Eulersche φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ ist definiert durch $\varphi(n) = |\mathbb{Z}_n^\times|$*

Lemma 5. *Es gilt:*

1. *$\varphi(n) = |\{0 \le m \le n | ggT(n, m) = 1\}|$*
2. *Ist* $\mathrm{ggT}(n, m) = 1$, *dann ist $\varphi(nm) = \varphi(n)\varphi(m)$.*
3. *Sei $n = p_1^{r_1} \cdot .. \cdot p_k^{r_k}$ die Primfaktorzerlegung von n, dann gilt: $\varphi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1)$*

Satz 6. *Sei $m \in \mathbb{Z}, n \in \mathbb{N}$. $\langle[m]\rangle = (\mathbb{Z}_n, +) \Leftrightarrow [m] \in \mathbb{Z}_n^\times$.*

Korollar 7. *Sei K ein Körper, $n \in \mathbb{N}$, so dass* $\mathrm{char}\, K \nmid n$. *Dann gibt es genau $\varphi(n)$ primitive n-te Einheitswurzeln. Sei $\zeta \in W_n$ primitiv und $r \in \mathbb{Z}$. ζ^r ist genau dann primitiv, wenn $[r] \in \mathbb{Z}_n^\times$.*

Definition 8. *Seien* $\mathrm{char}\, K \nmid n$ *und $\zeta_1, ..\zeta_{\phi(n)}$ die primitiven n-ten Einheitswurzeln. Dann heißt $\Phi_n := \prod_{i=1}^{\phi(n)}(x - \zeta_i)$ das n-te* KREISTEILUNGSPOLYNOM, *und ein Zerfällungskörper $K^{(n)}$ von Φ_n n-ter* KREISTEILUNGSKÖRPER.

Satz 9. *$\mathbb{Q}^{(n)}/\mathbb{Q}$ ist eine endliche galoische Erweiterung mit $[\mathbb{Q}^{(n)} : \mathbb{Q}] = \varphi(n)$.*

Satz 10. *Sei K ein Körper und $n \in \mathbb{N}$ mit* $\mathrm{char}\, K \nmid n$. *Ferner sei $\zeta \in W_n$ primitiv und $K^{(n)} = K(\zeta)$.*

1. *$K^{(n)}/K$ ist eine endliche abelsche galoische Erweiterung mit $[K^{(n)} : K] \le \varphi(n)$.*
2. *Zu jedem $\sigma \in \mathrm{Gal}(K^{(n)}/K)$ existiert ein $r_\sigma \in \mathbb{N}$ mit $\sigma(\zeta) = \zeta^{r_\sigma}$. Dabei ist $[r_\sigma] \in \mathbb{Z}_n^\times$ unabhängig von ζ eindeutig durch σ bestimmt. Die Abbildung*

$$\Psi : \mathrm{Gal}(K^{(n)}/K) \to \mathbb{Z}_n^\times, \sigma \mapsto [r_\sigma]$$

ist ein injektiver Gruppenhomomorphismus, der für $K = \mathbb{Q}$ sogar bijektiv ist.

Satz 11. *Es gilt:*

1. *$\Phi_n \in K[x]$ ist normiert und separabel,* $\deg \Phi_n = \varphi(n)$

2. *Für $K = \mathbb{Q}$ gilt $\Phi_n \in \mathbb{Z}[x]$ und Φ_n ist irreduzibel.*

3. $x^n - 1 = \prod_{d|n, d>0} \Phi_d$

4. *Sei* $\operatorname{char} K \nmid n$ *Anwenden des kanonischen Homomorphismus $\mathbb{Z} \to K$ transformiert das n-te Kreisteilungspolynom Φ_n über $\mathbb{Q}$ in das entsprechende Polynom $\tilde{\Phi}_n$ über K.*

Satz 12. Satz von Kronecker-Weber: *Sei $L/\mathbb{Q}$ mit $L \leq \mathbb{C}$ eine endliche abelsche galoische Erweiterung. Dann existiert ein $n \in \mathbb{N}$ mit $L \leq \mathbb{Q}^{(n)}$.*

4.4 Lineare Galoistheorie und zyklische Erweiterungen

Definition 1. *Sei G eine Gruppe und K ein Körper. Ein Gruppenhomomorphismus $\chi : G \to K^\times$ heißt* K-wertiger Charakter *von G.*

Bemerkung 2. *Es gilt:*

1. $\chi : G \to K^\times, g \mapsto 1$ *ist trivialer Charakter*

2. *K-wertige Charaktere bilden eine Gruppe unter der Verknüpfung $(\chi_1 \circ \chi_2)(g) = \chi_1(g)\chi_2(g)$*

3. *Die Charaktere sind Teilmengen des K-Vektorraums $Abb(G, K)$.*

Satz 3. Satz von Artin: *Seien $\chi_1, ..\chi_n$ verschiedene K-wertige Charaktere der Gruppe G. Dann sind $\chi_1, ..\chi_n$ linear unabhängig als Elemente von $Abb(G, K)$*

Korollar 4. *Sei L/K eine endliche separable Erweiterung und $\{\theta_1, ..\theta_n\}$ eine K-Basis von L. Für $\operatorname{Hom}_K(L, \bar{K}) = \{\sigma_1, ..\sigma_n\}$ sind dann die Vektoren $\zeta_i = (\sigma_i(\theta_1), ..\sigma_i(\theta_n)) \in \bar{K}^n$ mit $1 \leq i \leq n$ linear unabhängig.*

Bemerkung 5. *Erinnerung an die Lineare Algebra: wir verwenden im Folgenden die Begriffe Determinante, Spur, charakteristisches Polynom.*

Definition 6. *Sei L/K eine endliche Körpererweiterung. Für $\theta \in L$ betrachte man die Linksmultiplikation $x \mapsto \theta x$ als K-Vektorraumendomorphismus $\phi_\theta : L \to L$. Dann heißt $\operatorname{tr}_{L/K}(\theta)$ die* Spur *und $N_{L/K}(\theta) = \det \phi_\theta$ die* Norm *von θ bezüglich der Erweiterung L/K.*

Lemma 7. *Sei L/K eine endliche Körpererweiterung und $\theta \in L$. Mit $s = [L : K(\theta)]$ gilt dann:*

$$\operatorname{tr}_{L/K}(\theta) = s \operatorname{tr}_{K(\theta)/K}(\theta) \wedge N_{L/K}(\theta) = (N_{K(\theta)/K}(\theta))^s$$

Satz 9. *Sei L/K eine endliche Körpererweiterung. Dann gilt:*

1. *Es sei $[L : K] = rs$ mit $s = [L : K]_s$ und $\operatorname{Hom}_K(L, \bar{K}) = \{\theta_1, ..\theta_s\}$. Dann gilt für jedes $\theta \in L$, dass $\operatorname{tr}_{L/K}(\theta) = r \sum_{i=1}^s \sigma_i(\theta)$ und $N_{L/K}(\theta) = \prod_{i=1}^s \sigma_i(\theta))^r$*

2. *Sei M/L eine weitere endliche Erweiterung. Dann gilt: $\operatorname{tr}_{M/K} = \operatorname{tr}_{L/K} \circ \operatorname{tr}_{M/L}$ und $N_{M/K} = N_{L/K} \circ N_{M/L}$*

Korollar 10. *Sei L/K eine endliche Erweiterung. Dann bleiben Spur und Norm invariant unter Galois-Automorphismen, d.h.*

$$\forall \theta \in L, \sigma \in \operatorname{Gal}(L/K) : \operatorname{tr}_{L/K}(\sigma(\theta)) = tr_{L/K}(\theta) \wedge N_{L/K}(\sigma(\theta)) = N_{L/K}(\theta)$$

Korollar 11. *Eine endliche Körpererweiterung L/K ist genau dann separabel, wenn $\operatorname{tr}_{L/K} : L \to K$ nicht die triviale Abbildung ist, also $\operatorname{tr}_{L/K}$ surjektiv ist.*

Satz 12. Hilbert 90: *Sei L/K eine endliche zyklische galoische Erweiterung mit $\operatorname{Gal}(L/K) = \langle\sigma\rangle$ und $\theta \in L$. Dann gilt:*

1. $N_{L/K}(\theta) = 1 \Leftrightarrow \exists \tilde{\theta} \in L^\times : \theta = \tilde{\theta}\sigma(\tilde{\theta})^{-1}$

2. $\mathrm{tr}_{L/K}(\theta) = 0 \Leftrightarrow \exists \tilde{\theta} \in L : \theta = \tilde{\theta} - \sigma(\tilde{\theta})$

Satz 13. *Sei L/K eine Körpererweiterung und $n \in \mathbb{N}$, so daß $\mathrm{char}\, K \nmid n$ und K eine primitive n-te Einheitswurzel enthält.*

1. *Wenn L/K eine zyklische galoische Erweiterung mit $[L : K] = n$ ist, dann gilt: $L = K(\theta)$ für ein $\theta \in L$, dessen Minimalpolynom von der Form $x^n - c$ mit $c \in K$ ist.*
2. *Sei $\theta \in L$ die Nullstellen eines Polynoms $x^n - c \in K[x]$ und $L = K(\theta)$. Dann ist L/K eine zyklische Galoische Erweiterung, $d = [L : K] \mid n$ und $\theta^d \in K$ (d.h. $x^d - \theta^d \in K[x]$ ist das Minimalpolynom von θ).*

Satz 14. ARTIN-SCHREIER: *Sei L/K eine Körpererweiterung mit $\mathrm{char}\, K = p > 0$.*

1. *Wenn L/K eine zyklische galoische Erweiterung mit $[L : K] = p$ ist, dann ist $L = K(\theta)$ für ein $\theta \in L$, dessen Minimalpolynom $f_\theta \in K[x]$ von der Form $x^p - x - c$ mit $c \in K$ ist.*
2. *Sei $\theta \in L$ eine Nullstelle dieses Polynoms $x^p - x - c \in K[x]$ und $L = K(\theta)$. Dann ist L/K eine zyklische galoische Erweiterung. Entweder zerfällt das Polynom $x^p - x - c$ über K vollständig in Linearfaktoren, oder aber es ist irreduzibel und es gilt $[L : K] = p$*

4.5 Auflösbarkeit durch Radikale

Definition 1. *Eine endliche separable Erweiterung L/K heißt durch Radikale auflösbar, wenn es eine endliche Erweiterung E/L und einen Körperturm $K = E_0 \leq E_1 \leq .. \leq E_n = E$ gibt, wobei $E_{i+1} = E_i(\theta_{i+1})$ mit*

1. *θ_{i+1} ist eine Einheitswurzel*
2. *θ_{i+1} ist Nullstelle eines Polynoms $x^n - c \in E_i[x]$, falls $\mathrm{char}\, K \nmid n$ bzw. $x^p - x - c$, falls $\mathrm{char}\, K = p$*

Bemerkung 2. *Im Fall (2) kann o.B.d.A. $n \in \mathbb{P}$ angenommen werden.*

Definition 3. *Eine endliche Körpererweiterung L/K heißt* AUFLÖSBAR, *wenn es eine endliche Erweiterung E/L gibt, so dass E/K galoisch ist und die Gruppe $\mathrm{Gal}(E/K)$ auflösbar ist.*

Lemma 4. *Sei G eine endliche auflösbare Gruppe. Dann besitzt G eine Normalreihe, deren Faktoren zyklisch von Primzahlordnung sind.*

Satz 5. *Die endliche Erweiterung L/K ist genau dann durch Radikale auflösbar, wenn L/K auflösbar.*

Korollar 6. *Sei K ein Körper und $f \in K[x]$ ein irreduzibles Polynom. Die Nullstellen von f lassen sich genau dann in eine geschlossene algebraische Formel mit Radikalen einschieben, wenn die Galois-Gruppe des Zerfällungskörpers von f auflösbar ist.*

Korollar 7. SATZ VON ABEL: *Die allgemeine Gleichung n-ten Grades ist für $n = 1, 2, 3, 4$ durch Radikale auflösbar, aber nicht für $n \geq 5$*

4.6 Konstruktionen mit Zirkel und Lineal

Bemerkung 1. *Der Übergang $z \mapsto \bar{z}$ entspricht der Spiegelung an der reellen Achse. Dies Konjugation ist mittels Zirkel und Lineal konstruierbar.*

Lemma 2. *Für $\{0, 1\} \subseteq M$ ist $\lhd(M)$ ein Körper, der insbesondere $\mathbb{Q}(i)$ enthält.*

Satz 3. *Sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ und $z \in \mathbb{C}$ Dann sind folgende Aussagen äquivalent:*

1. *$z \in \lhd(M)$*
2. *Es existiert ein Körperturm $K = \mathbb{Q}(M \cup \bar{M}) = L_0 < L_1, .., L_n \leq \mathbb{C}$ mit $z \in L_n$ und $[L_i : L_{i-1}] = 2$ für $1 \leq i \leq n$*
3. *Es existiert eine galoische Erweiterung N/K mit $z \in N$ und $[N : K] = 2^m$ für ein $m \in \mathbb{N}$*

Korollar 4. *Die Verdopplung eines Würfels mit Zirkel und Lineal ist nicht möglich.*

Korollar 5. *Für alle Winkel $0 \leq \varphi < 2\pi$ für die $e^{i\phi}$ transzendent über $\mathbb{Q}$ ist, ist die Dreiteilung mit Lineal und Zirkel nicht möglich.*

Korollar 7. *Die Quadratur des Kreises ist mit Zirkel und Lineal unmöglich.*

Korollar 8. *Sei $3 \leq n \in \mathbb{N}$. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n) = 2^m$ für ein $m \in \mathbb{N}$.*

Bemerkung 9. *Für $n \leq 17$ sind nur das 7-Eck, das 9-Eck und das 13-Eck nicht konstruierbar.*

Definition 10. *Für $k \in \mathbb{N}$ heißt $F_k := 2^{(2^k)} + 1$ die k-te* Fermatsche Zahl. *Falls F_k prim, so spricht man von einer* fermatschen Primzahl.

Lemma 12. *Sei $n \geq 2$. $\varphi(n)$ ist genau dann eine Potenz von 2, wenn es paarweise verschiedene Fermatsche Primzahlen $p_1, ..p_n$ gibt sowie eine Zahl $n \in \mathbb{N}$ mit $n = 2^n p_1 \cdot .. \cdot p_r$.*

Index