Protokoll zur Vorlesung Algebra (gymnasiales Lehramt)

W. Bley

9. Februar 2016

1 Gruppentheorie

1.1 Grundlegende Definitionen

Definition 1.1.1 Eine Halbgruppe ist eine nicht-leere Menge G zusammen mit einer binären Operation $G \times G \to G, (a, b) \mapsto ab$, so daß gilt:

$$(i) \qquad a(bc) = (ab)c, \forall a, b, c \in G \quad \text{(Assoziativität)}$$

Ein Monoid ist eine Halbgruppe G, die ein Element e enthält, so daß gilt:

$$(ii) \qquad ae = ea = a, \forall a \in G \quad \text{(Existenz der Identität)}$$

Eine Gruppe ist ein Monoid G, so daß es zu jedem $a \in G$ ein Inverses $a^{-1} \in G$ gibt mit

$$(iii) \qquad aa^{-1} = a^{-1}a = e.$$

Eine Halbgruppe heißt abelsch oder kommutativ, falls für all $a, b \in G$ gilt: $ab = ba$.

Wichtige Beispiele:
1) Die Diedergruppe $D_4 = \{\sigma^i\tau^j \mid 0 \leq i \leq 3, 0 \leq j \leq 1, \tau\sigma = \sigma^3\tau\}$. Dies ist die Gruppe der Symmetrien eines regelmäßigen Vierecks. σ kann man sich als die Drehung um 90 Grad vorstellen; τ ist etwa die Spiegelung an der x-Achse.
2) Die symmetrischen Gruppen S_n der Permutationen von n Symbolen. Es gilt: $|S_n| = n!$.

An dieser Stelle sei an die Definition einer Äquivalenzrelation erinnert. Konsultieren Sie dazu zum Beispiel das Buch von S. Bosch, Lineare Algebra, Kapitel 2.2.

Satz 1.1.2 *Sei $\sim$ eine Äquivalenzrelation auf dem Monoid G, so daß für alle $a, b, c, d \in G$ gilt: $a \sim b, c \sim d \implies ac \sim bd$. Dann ist die Menge $\bar{G} := G/\sim$ der Äquivalenzklassen ein Monoid unter der binären Operation $\bar{a}\bar{b} := \overline{ab}$, wobei für $a \in G$ die Äquivalenzklasse $\{b \in G \mid a \sim b\}$ mit $\bar{a}$ bezeichnet wird.*
Falls G eine Gruppe ist, so auch $\bar{G}$. Ebenso vererbt sich die Eigenschaft abelsch.

Wichtiges Beispiel: Sei $G = \mathbb{Z}$ bezüglich $+$ oder $\cdot$ und m eine natürliche Zahl. Dann definiert man: $a \sim b :\iff m \mid a - b$. Wir schreiben dafür: $a \equiv b (\text{mod } m)$ und $\mathbb{Z}/m\mathbb{Z} := \bar{G}$. Bezüglich $+$ ist $\mathbb{Z}/m\mathbb{Z}$ eine abelsche Gruppe, bezüglich $\cdot$ ein Monoid.

Definition 1.1.3 Sei G eine Gruppe und $n \in \mathbb{Z}$. Dann setzt man:

$$a^n := \begin{cases} a \cdots a \quad (n \text{ Faktoren}), & \text{if } n > 0, \\ a^{-1} \cdots a^{-1} \quad (-n \text{ Faktoren}), & \text{if } n < 0, \\ e, & \text{if } n = 0. \end{cases}$$

Es gelten dann die üblichen Rechenregeln:

$$a^m b^n = a^{m+n}, \quad (a^n)^m = a^{mn}, \quad a \in G, m, n \in \mathbb{Z}.$$

1.2 Homomorphismen und Untergruppen

Definition 1.2.1 Seien G, H Gruppen. Eine Abbildung $f : G \to H$ heißt Homomorphismus (von Gruppen), falls für alle $a, b \in G$ gilt $f(ab) = f(a)f(b)$. Man benützt die üblichen, aus der linearen Algebra bekannten Bezeichnungen Monomorphismus, Epimorphismus und Isomorphismus.

Bemerkungen
1) Das Kompositum von zwei (oder mehreren) Homomorphismen ist stets wieder ein Homomorphismus.
2) Es gilt: $f(e_G) = e_H$ und $f(a^{-1}) = f(a)^{-1}, \forall a \in G$.

Definition 1.2.2 Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann heißt

$$\ker(f) := \{g \in G \mid f(g) = e_H\}$$

der Kern von f, $f(G)$ heißt das Bild von f und $f^{-1}(B)$ das Urbild der Teilmenge $B \subseteq H$ unter f.

Kern und Bild sind stets wieder Gruppen. Falls $B \subseteq H$ eine Untergruppe von H ist, so ist das Urbild eine Untergruppe von G.

Satz 1.2.3 *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*
(i) f ist ein Monomorphismus $\iff \ker(f) = \{e_G\}$.
(ii) f ist ein Isomorphismus $\iff \exists$Homomorphismus $f^{-1} : H \to G$ mit $f \circ f^{-1} = id_H, f^{-1} \circ f = id_G$.

Definition 1.2.4 Sei H eine nicht-leere Teilmenge der Gruppe G, die abgeschlossen unter der Gruppenoperation ist. Fall H selbst eine Gruppe ist, so heißt H Untergruppe von G (in Zeichen: $H \leq G$).

Bemerkung: $\{e\}$ bezeichnen wir als die triviale Untergruppe. Für ein Homomorphismus $f : G \to H$ ist $\ker(f)$ stets eine Untergruppe von G.

Satz 1.2.5 *Sei H eine nicht-leere Teilmenge einer Gruppe G. Dann gilt:*

$$H \leq G \iff ab^{-1} \in H, \forall a, b \in H.$$

1.3 Zyklische Untergruppen

Definition 1.3.1 a) Sei G eine Gruppe und $a \in G$. Dann heißt $< a >:= \{a^k \mid k \in \mathbb{Z}\}$ die von a erzeugte zyklische Untergruppe von G. Die Zahl $\text{ord}(a) := | < a > |$ heißt die Ordnung von a.
b) Die Gruppe G heißt zyklisch, falls es ein $a \in G$ gibt, so dass $G =< a >$ gilt.

Satz 1.3.2 *Sei G eine Gruppe und $a \in G$. Falls a unendliche Ordnung hat, so gilt:*

(i) $a^k = e \iff k = 0$.

(ii) $a^k = a^l \iff k = l$.

Falls a endliche Ordnung $m \in \mathbb{N}$ hat, so gilt:

(iii) *m ist die kleinste positive ganze Zahl mit $a^m = e$.*

(iv) $a^k = e \iff m \mid k$.

(v) $a^k = a^l \iff k \equiv l (\text{mod } m)$.

(vi) $< a >= \{a^0, a^1, \ldots, a^{m-1}\}$.

(vii) $ord(a^k) = m/k$, *falls* $k \mid m$.

Folgerung 1.3.3 *Jede unendliche zyklische Gruppe ist isomorph zu* $\mathbb{Z}$. *Jede endliche zyklische Gruppe der Ordnung* m *ist isomorph zu* $\mathbb{Z}/m\mathbb{Z}$.

Satz 1.3.4 *Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer: Ist* H *Untergruppe von* $G =< a >$, *so gilt:*

$$H =< a^k > \text{ mit } k := \min\{s \in \mathbb{N} \mid a^s \in H\}.$$

Satz 1.3.5 *Sei* $G =< a >$ *eine zyklische Gruppe. Falls* $ord(a) = \infty$, *so sind* a *und* $-a$ *die einzigen Erzeuger von* G. *Falls* $ord(a) = m < \infty$, *so gilt:*

$$< a >=< a^k > \iff \text{ggT}(m, k) = 1.$$

Genauer gilt: $ord(a^k) = m/\text{ggT}(k, m)$.

1.4 Nebenklassen und Untergruppen

Definition 1.4.1 Sei H eine Untergruppe von G und $a, b \in G$. Dann heißt a (rechts-)kongruent zu b, in Zeichen $a \equiv_r b (\text{mod } H)$, falls $ab^{-1} \in H$.

Bemerkung: Für $G = \mathbb{Z}, H = m\mathbb{Z}$ ist dies die bereits bekannte Kongruenz.

Satz 1.4.2 *(i)* $\equiv_r$ *ist eine Äquivalenzrelation auf* G.
(ii) Die Äquivalenzklasse von $a \in G$ *ist gerade die sogenannte Rechtsnebenklasse*

$$Ha = \{ha \mid h \in H\}.$$

(iii) Alle Nebenklassen haben diesselbe Kardinalität, nämlich $|H|$.

Definition 1.4.3 Sei $H \leq G$. Dann heißt die Anzahl der Rechtsnebenklassen der Index von H in G. In Zeichen: $[G : H]$.

Bemerkung: Sei $H \leq G$. Dann schreibt man $H \setminus G$ für die Menge der Rechtsnebenklassen. Völlig analog definiert man G/H für die Menge der Linksnebenklassen. Hier liegt dann die Definition

$$a \equiv_l b (\text{mod } H) : \iff a^{-1}b \in H$$

zugrunde. Es gilt: Die Anzahl der Linksnebenklassen ist gleich der Anzahl der Rechtsnebenklassen. Der Index kann also auch als die Anzahl der Linksnebenklassen definiert werden

Satz 1.4.4 *Seien* $K \leq H \leq G$ *Gruppen. Dann verhält sich der Index multiplikativ, d.h.* $[G : K] = [G : H][H : K]$. *Falls zwei dieser Indizes endlich sind, so auch der dritte.*

Satz 1.4.5 *(Lagrange) Falls* $H \leq G$, *so gilt:* $|G| = [G : H]|H|$. *Falls also* $|G| < \infty$, *so teilt* $|H|$ *stets* $|G|$.

Folgerung 1.4.6 *Sei* G *eine Gruppe der Ordnung* $m < \infty$. *Dann gilt für alle* $a \in G$:

$$ord(a) \mid m \text{ und } a^m = e.$$

Satz 1.4.7 *Seien* H, K *endliche Untergruppen eine Gruppe* G. *Dann gilt:*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Hierbei ist $HK := \{ab \mid a \in H, b \in K\}$.

Achtung: HK ist im allgemeinen keine Gruppe.

In diesem Abschnitt wurde großer Wert darauf gelegt, zu zeigen, daß im Allgemeinen

- Rechtsnebenklassen nicht mit Linksnebenklassen übereinstimmen.
- die natürlich definierte binäre Struktur auf der Menge der Rechtsnebenklassen (bzw. Linksnebenklassen) nicht wohldefiniert ist.

Dies führt uns zum Studium von Untergruppen mit einer zusätzlichen Eigenschaft, den sogenannten Normalteilern, wo dann obige "Defizite" nicht mehr auftreten.

1.5 Normale Untergruppen und Quotienten

ZIEL: Studium derjenigen Untergruppen $N \leq G$ für die gilt: $aN = Na$ (oder gleichbedeutend: für die $\equiv_r$ und $\equiv_l$ übereinstimmen).

Satz 1.5.1 *Für eine Untergruppe $N \leq G$ sind folgende Eigenschaften äquivalent:*

a) $aN = Na, \forall a \in G.$

b) $aNa^{-1} \subseteq N, \forall a \in G.$

c) $aNa^{-1} = N, \forall a \in G.$

Definition 1.5.2 Eine Untergruppe N von G, die diesen äquivalenten Eigenschaften genügt, heißt Normalteiler von G. In Zeichen: $N \lhd G$.

Bemerkungen:
1) $\equiv_r$ und $\equiv_l$ stimmen überein, falls N normal in G ist. Wir schreiben daher kurz: $\equiv$.
2) Für eine Normalteiler N erfüllt $\equiv$ die zusätzliche Eigenschaft aus Satz 1.2. Also ist $\bar{G} = G/N = N \setminus G$ eine Gruppe.

Satz 1.5.3 *Seien K, N, G Gruppen mit $K \leq G, N \lhd G$. Dann gilt:*

(i) $N \cap K$ *ist normal in* K.

(ii) $NK = KN$ *ist eine Untergruppe von* G.

(iii) Falls ebenfalls $K \lhd G$ *und* $K \cap N = \{e\}$, *so folgt:* $nk = kn, \forall n \in N, k \in K$.

Satz 1.5.4 *Sei $N \lhd G$. Dann ist G/N eine Gruppe der Ordnung $[G : N]$ unter der binären Operation $aN \cdot bN = abN, a, b \in G$.*

Die Gruppe G/N heißt Quotientengruppe oder Faktorgruppe von G modulo N.

Satz 1.5.5 *Sei $f : G \to H$ ein Homomorphismus. Dann gilt:*
(i) $\ker(f) \lhd G$.
(ii) Jeder Normalteiler N ist Kern eines Homomorphismus, nämlich von der sogenannten kanonischen Projektion

$$\pi : G \longrightarrow G/N, \quad g \mapsto gN.$$

Satz 1.5.6 *Sei $f : G \to H$ ein Homomorphismus und $N \lhd G$ mit $N \subseteq \ker(f)$. Dann ist die kanonische Abbildung*

$$\bar{f} : G/N \longrightarrow H, \quad gN \mapsto f(g)$$

ein wohldefinierter Homomorphismus und es gilt: $\ker(\bar{f}) = \ker(f)/N,\ im(\bar{f}) = im(f)$. *Der Homomorphismus $\bar{f}$ ist also genau dann injektiv, wenn $N = \ker(f)$.*

Folgerung 1.5.7 *(1. Isomorphiesatz) Sei $f : G \to H$ ein Homomorphismus. Dann induziert f einen Isomorphismus*

$$\bar{f} : G/\ker(f) \xrightarrow{\simeq} im(f), \quad g\ker(f) \mapsto f(g).$$

Folgerung 1.5.8 *Sei $f : G \to H$ ein Homomorphismus und $N \lhd G, M \lhd H$ mit $f(N) \leq M$. Dann induziert f einen Homomorphismus*

$$\bar{f} : G/N \longrightarrow H/M, \quad gN \mapsto f(g)M.$$

Es gilt:
(a) $\bar{f}$ ist surjektiv $\iff im(f)M = H$.
(b) $\bar{f}$ ist injektiv $\iff f^{-1}(M) \subseteq N$.

Folgerung 1.5.9 *(2. Isomorphiesatz) Seien $K, N \leq G, N \lhd G$. Dann ist $(K \cap N) \lhd K$ und die Abbildung*

$$K/(K \cap N) \longrightarrow KN/N, \quad k(K \cap N) \mapsto kN$$

ist ein Isomorphismus.

Folgerung 1.5.10 *(3. Isomorphiesatz) Seien $H, N \lhd G$ mit $N \leq H$. Dann ist $H/N \lhd G/N$ und die Abbildung*

$$G/H \longrightarrow \frac{G/N}{H/N}, \quad gH \mapsto gN \cdot (H/N)$$

ist ein Isomorphismus.

Satz 1.5.11 *Sei $f : G \to H$ ein Epimorphismus. Dann ist die Zuordnung $U \mapsto f(U)$ eine Bijektion zwischen der Menge der Untergruppen U von G mit $\ker(f) \subseteq U$ und der Menge der Untergruppen V von H. Dabei entsprechen normale Untergruppen wieder normalen Untergruppen.*
Ferner gilt: Falls $\ker(f) \leq U_2 \lhd U_1 \leq G$ so ist $f(U_2) \lhd f(U_1)$ und

$$U_1/U_2 \simeq f(U_1)/f(U_2), \quad uU_2 \mapsto f(u)f(U_2).$$

1.6 Normalreihen und Auflösbarkeit

Definition 1.6.1 (a) Sei G eine Gruppe. Eine Kette

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r = \{e\}$$

von Untergruppen G_i von G mit $G_i \lhd G_{i-1}$ heißt Normalreihe von G. Die Gruppen G_{i-1}/G_i heißen die Faktoren der Normalreihe.
(b) G heißt auflösbar, falls G eine Normalreihe mit abelschen Faktoren besitzt.

Zum Beispiel sind alle abelschen Gruppen auflösbar.

Satz 1.6.2 *Sei G eine Gruppe. Dann gilt:*
a) G auflösbar, $H \leq G \implies H$ auflösbar.
b) G auflösbar, $N \lhd G \implies G/N$ auflösbar.
c) Sei $N \lhd G$. Dann gilt:

$$G \text{ auflösbar} \iff G/N \text{ und } N \text{ auflösbar.}$$

d) Sei G eine endliche p-Gruppe (p Primzahl). Dann ist G auflösbar.

Der Beweis von d) ist eine direkte Konsequenz von Satz 1.6.4. Dazu folgende Begriffsbildung.

Definition 1.6.3 Sei G eine Gruppe. Dann heißt

$$Z(G) := \{g \in G \mid gh = hg, \forall h \in G\}$$

das Zentrum von G.

Offensichtlich ist $Z(G)$ ein Normalteiler von G.

Satz 1.6.4 *Sei G eine nicht-triviale endliche p-Gruppe. Dann hat G ein nicht-triviales Zentrum.*

In der Literatur wird Auflösbarkeit oft durch die Existenz einer Normalreihe mit zyklischen Faktoren definiert. Der nächste Satz zeigt die Äquivalenz zu unserer Definition.

Satz 1.6.5 *Sei G endlich und auflösbar. Dann besitzt G eine Normalreihe mit zyklischen Faktoren.*

Wir schließen den Abschnitt mit einer wichtigen Definition.

Definition 1.6.6 Eine nicht-triviale Gruppe G heißt einfach, falls G keine Normalteiler außer $\{e\}$ und G besitzt.

Im nächsten Abschnitt wollen wir einsehen, dass die symmetrische Gruppe S_n für $n \geq 5$ nicht auflösbar ist. Diese Tatsache wird Anwendungen für die Auflösbarkeit von allgemeinen Gleichungen vom Grad n haben. Den Zusammenhang wird die sogenannte Galoistheorie herstellen. Dass die S_n nicht auflösbar ist, ist eine direkte Konsequenz aus dem Resultat, dass die alternierende Gruppe A_n für $n \geq 5$ einfach ist. Genaueres dazu im folgenden Abschnitt.

1.7 Die symmetrischen Gruppen S_n

In diesem Abschnitt werden wir zeigen, daß für $n \geq 5$ die alternierende Gruppe A_n (wird noch definiert) einfach ist. Hieraus folgt insbesondere, daß $S_n, n \geq 5$, nicht auflösbar ist.

Definition 1.7.1 Sei $X_n = \{1, 2, \ldots, n\}$ und seien $a_1, \ldots a_s, s \leq n$, paarweise verschiedene Elemente aus X_n. Dann bezeichnet $(a_1, a_2, \ldots, a_s)$ diejenige Permutation für die gilt:

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_{s-1} \mapsto a_s, a_s \mapsto a_1,$$
$$a \mapsto a, \forall a \in X_n \setminus \{a_1, a_2, \ldots, a_s\}.$$

$(a_1, a_2, \ldots, a_s)$ heißt Zyklus der Länge s oder s-Zyklus; ein 2-Zyklus heißt Transposition.

Beobachtung Zwei disjunkte Zyklen vertauschen.

Satz 1.7.2 *Jede nicht-triviale Permutation ist eindeutig (bis auf Vertauschung) als Produkt von disjunkten Zyklen darstellbar.*

Folgerung 1.7.3 *Die Ordnung einer Permutation $\sigma \in S_n$ ist gleich dem kleinsten gemeinsamen Vielfachen der Längen der disjunkten Zyklen in der eindeutigen Produktdarstellung.*

Satz 1.7.4 *Jedes $\sigma \in S_n$ kann als Produkt von Transpositionen geschrieben werden. Diese Darstellung ist nicht eindeutig, jedoch ist die Parität der Anzahl der Transpositionen unabhängig von der Darstellung.*

Zum Beweis haben wir die Signatur

$$sgn : S_n \to \{\pm 1\}$$

definiert durch

$$sgn(\sigma) = \det(e_{\sigma(e_1)} \cdots e_{\sigma(e_n)}),$$

wobei $e_1, \ldots, e_n$ die Standardbasis des $\mathbb{R}^n$ bezeichnet. Die Signatur $sgn : S_n \to \{\pm 1\}$ ist ein surjektiver Gruppenhomomrphismus.
Sei weiter $\sigma \in S_n$ und $\sigma = \tau_1 \cdots \tau_s$, wobei sämtliche τ_i Transpositionen sind. Dann gilt

$$sgn(\sigma) = (-1)^s.$$

Definition 1.7.5 Der Normalteiler $A_n := \ker(sgn)$ heißt die alternierende Gruppe.

Satz 1.7.6 *A_n ist der einzige Normalteiler der S_n vom Index 2.*

Satz 1.7.7 *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Als direkte Konsequenz hieraus erhalten wir

Folgerung 1.7.8 *Für $n \geq 5$ ist die symmetrische Gruppe S_n nicht auflösbar.*

Wesenliche Schritte im Beweis von Satz 1.7.7 sind:
a) Die A_n wird erzeugt von den Dreierzyklen. Genauer sogar: Dreierzyklen der Form $(1\ 2\ k), k = 3, \ldots, n$ erzeugen A_n.
b) Für einen Normalteiler $N \neq \{e\}$ der A_n, der einen Dreierzyklus enthält folgt: $N = A_n$. Den Beweis hierzu haben wir nur sehr grob angedeutet.

1.8 Gruppenoperationen

Definition 1.8.1 Sei M eine Menge und G eine Gruppe. Dann operiert G auf M, falls es eine Abbildung $G \times M \to M, (g, s) \mapsto gs$ gibt, so daß gilt

$$(g_1 g_2)m = g_1(g_2 m) \text{ und } em = m, \forall g_1, g_2 \in G, m \in M.$$

Man sagt dann auch: M ist eine G-Menge.

Zwei wichtige Beispiele erhält man für $M = G$:
a) G wirkt durch Konjugation auf G, d.h. $G \times G \longrightarrow G, (g, s) \mapsto gsg^{-1}$.
b) G wirkt durch Translation auf G, d.h. $G \times G \longrightarrow G, (g, s) \mapsto gs$.

Bezeichnung: Für eine Menge M bezeichne $S(M)$ die Gruppe der Permutationen von M.

Falls M eine G-Menge ist, so wird für jedes $g \in G$ durch die Setzung $T_g(m) := gm$ ein Element $T_g \in S(M)$ definiert.

Lemma 1.8.2 *Sei M eine G-Menge. Dann ist die Abbildung $T\colon G \longrightarrow S(M), g \mapsto T_g$, ein Gruppenhomomorphismus.*

Läßt man eine Gruppe durch Translation auf sich selbst wirken, so liefert dies den

Satz 1.8.3 *(Cayley) Jede Gruppe der Ordnung n ist isomorph zu einer Untergruppe der S_n.*

Definition 1.8.4
a) Sei M eine G-Menge und $x \in M$. Dann heißt $Gx := \{gx \mid g \in G\}$ die Bahn oder der Orbit von x unter G.
b) Man sagt G operiert transitiv auf M, falls M nur aus einem einzigen Orbit besteht.

Durch $m_1 \sim m_2 : \Longleftrightarrow \exists g \in G : gm_1 = m_2$ ist eine Äquivalenzrelation auf M definiert, wobei die Äquivalenzklassen genau die Bahnen sind. Man erhält daher

Satz 1.8.5 *Sei M eine G-Menge.*
a) M ist die disjunkte Vereinigung über die verschiedenen G-Bahnen.
b) Falls $|M| < \infty$, so gilt: $|M| = \sum_C |C|$, wobei über die verschiedenen Bahnen summiert wird.

Definition 1.8.6 Sei M eine G-Menge und $x \in M$. Dann heißt

$$G_x = Stab_G(x) := \{g \in G \mid gx = x\}$$

der Stabilisator von x in G. Weitere Bezeichnung: Standunterruppe.

Die Bijektion $G/Stab_G(x) \to Gx, gStab_G(x) \mapsto gx$ liefert

Satz 1.8.7 *(Bahnengleichung) Sei M eine endliche G-Menge und sei $x_1, \ldots, x_s$ ein vollständiges Vertretersystem der verschiedenen G-Bahnen. Dann gilt:*

$$|M| = \sum_{i=1}^{s} [G : Stab_G(x_i)].$$

1.9 Die Sylowsätze und Anwendungen

Definition 1.9.1 Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Es gelte: $p^r \mid |G|, p^{r+1} \nmid |G|$. Dann nennt man jede Untergruppe $U \leq G$ mit $|U| = p^r$ eine p-Sylowuntergruppe von G.

Satz 1.9.2 *Sei G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Dann existiert eine p-Sylowuntergruppe.*

Der Beweis dazu erfolgt über Induktion nach der Gruppenordnung. Benötigt wird dazu

Lemma 1.9.3 *Sei G eine endliche abelsche Gruppe und $p \mid |G|$, p Primzahl. Dann hat G eine Untegruppe der Ordnung p.*

Satz 1.9.4 *(Sylowsätze) Sei G eine endliche Gruppe und P eine p-Sylowuntergruppe.*
(i) Sei H eine p-Untergruppe von G. Dann ist H in einer p-Sylowuntergruppe enthalten. Genauer: es gibt $x \in G$ mit $H \leq x^{-1}Px$.
(ii) Alle p-Sylowuntergruppe sind konjugiert.
(iii) Sei n_p die Anzahl der verschiedenen p-Sylowuntergruppen. Dann gilt:

$$n_p \equiv 1 (\mathrm{mod}\ p) \text{ und } n_p = |G/N_G(P)|.$$

Hierzu ist folgende Definition nachzutragen:

Definition 1.9.5 Sei $H \leq G$. Dann heißt $N_G(H) := \{g \in G \mid gHg^{-1} \subseteq H\}$ der Normalisator von H in G.

Offensichtlich ist $N_G(H)$ eine Untergruppe von G, die H enthält. Zusammen mit (iii) impliziert dies:

$$n_p \mid m \text{ falls } |G| = p^r m, p \nmid m.$$

Als Anwendung der Sylowsätze klassifizieren wir die Gruppen der Ordnung pq, $p > q$ Primzahlen.

Satz 1.9.6 *Seien p, q Primzahlen mit $p > q$.*
a) Falls $q \nmid (p-1)$, so ist jede Gruppe der Ordnung pq zyklisch.
b) Falls $q \mid (p-1)$, so gibt es bis auf Isomorphie genau zwei Gruppen der Ordnung pq, nämlich C_{pq} und

$$< a, b \mid a^p = e = b^q, ba = a^s b >, \text{ wobei } s \not\equiv 1 (\text{mod } p), s^q \equiv 1 (\text{mod } p).$$

Zusatz: Gruppen der Ordnung pq, $p \neq q$, sind stets auflösbar.

Beim Beweis geht ein, daß für die zyklische Gruppe C_n gilt: $\text{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Ferner haben wir benutzt: $(\mathbb{Z}/p\mathbb{Z})^\times, p$ Primzahl, ist zyklisch. Dies werden wir später in der Ringtheorie beweisen.

Folgerung 1.9.7 *Sei $p > 2$ eine Primzahl und $|G| = 2p$. Dann ist G zyklisch oder isomorph zur Diedergruppe der Ordnung $2p$.*

Definition 1.9.8 Seien G und H Gruppen und $\varphi : H \to \text{Aut}(G)$ ein Homomorphismus. Dann wird das kartesische Produkt $G \times H$ mit der binären Operation

$$(g, h)(g', h') := (g\varphi(h)(g'), hh'), \quad g, g' \in G, h, h' \in H,$$

zu einer Gruppe. Diese heißt das semi-direkte Produkt von G und H. Man schreibt: $G \rtimes H$ oder $G \times_\varphi H$.

Beobachtung: G ist ein Normalteiler in $G \rtimes H$.

Remark 1.9.9 Mit Hilfe semi-direkter Produkte kann man nicht-abelsche Gruppen der Ordnung p^3, p eine Primzahl, konstruieren

1.10 Abelsche Gruppen

Wir werden abelsche Gruppen stets additiv notieren. Falls $A_1, \ldots, A_n$ abelsche Gruppen sind, so schreiben wir $A_1 \oplus \ldots \oplus A_n$ für das kartesische Produkt. Die binäre Struktur hierauf wird komponentenweise definiert.
In diesem Zusammenhang sei auch an die folgende Definition (etwa aus der Theorie der Vektorräume) erinnert: Sei A eine abelsche Gruppe und $A_1, A_2 \leq A$. Dann schreibt man $A = A_1 \oplus A_2$, falls $A = A_1 + A_2$ und $A_1 \cap A_2 = \{0\}$. Äquivalent dazu: Für alle $a_1, a_1' \in A_1, a_2, a_2' \in A_2$ gilt: $a_1 + a_2 = a_1' + a_2' \iff a_1 = a_1'$ und $a_2 = a_2'$.

Definition 1.10.1 Eine abelsche Gruppe F heißt frei vom Rang n, $n \in \mathbb{N}$, falls $F \simeq \mathbb{Z}^n$.

Lemma 1.10.2 *(a) Sei $F = \oplus_{i=1}^n \mathbb{Z}e_i$ eine freie abelsche Gruppe und A eine abelsche Gruppe. Seien $a_1, \ldots, a_n \in A$ gegeben. Dann gibt es genau einen Gruppenhomomorphismus $f\colon F \longrightarrow A$ mit $f(e_i) = a_i, i = 1, \ldots, n$.*
(b) Seien F und A wie in (a) und $f\colon A \longrightarrow F$ ein Epimorphismus. Dann gibt es eine Untergruppe $B \leq A$ mit

$$A = \ker(f) \oplus B \text{ und } B \simeq F.$$

Definition 1.10.3 Sei A eine abelsche Gruppe.
(a) Ein Element $a \in A$ heißt Torsionselement, falls es ein $m \in \mathbb{Z}, m \neq 0$, gibt, so daß $ma = 0$.
(b) Die Menge

$$T(A) := \{a \in A \mid a \text{ ist Torsionselement } \}$$

heißt Torsionsuntergruppe von A.
(c) A heißt torsionsfrei, falls $T(A) = \{0\}$.

Man beachte, daß $T(A)$ tatsächlich eine Untergruppe von A ist.

Satz 1.10.4 *Sei F eine freie abelsche Gruppe vom Rang n und $A \leq F$ eine Untergruppe. Dann ist A frei vom Rang $\leq n$.*

Definition 1.10.5 Eine abelsche Gruppe heißt endliche erzeugt, falls es $a_1, \ldots, a_n \in A$ gibt, $n \in \mathbb{N}$, mit $A = \langle a_1, \ldots, a_n \rangle_{\mathbb{Z}}$.

Für eine endlich erzeugte abelsche Gruppe $A = \langle a_1, \ldots, a_n \rangle_{\mathbb{Z}}$ betrachten wir den Epimorphismus

$$\pi \colon \mathbb{Z}^n \longrightarrow A, \quad \sum_{i=1}^{n} n_i e_i \mapsto \sum_{i=1}^{n} n_i a_i,$$

Sei $F := \mathbb{Z}^n$ und $N := \ker(\pi)$. Dann ist nach dem Isomorphiesatz $A \simeq F/N$. Die Struktur von F/N wird durch den folgenden Satz eindeutig bestimmt.

Satz 1.10.6 *Sei F eine freie abelsche Gruppe vom Rang n und N eine Untergruppe von F. Dann gibt es "$\mathbb{Z}$-Basen" $u_1, \ldots, u_n$ von F und $v_1, \ldots, v_m$ von N mit $m \leq n$ und*

$$v_i = \epsilon_i u_i, \quad i = 1, \ldots, m, \epsilon_i \in \mathbb{N},$$
$$\epsilon_1 \mid \epsilon_2 \mid \ldots \mid \epsilon_m.$$

Der Beweis ist algorithmisch und kann als Verallgemeinerung des Gaußschen Algorithmus aufgefasst werden. Sei zunächst eine beliebige Basis $u_1, \ldots, u_n$ von F gegeben und beliebige Erzeugende $v_1, \ldots, v_k$ von N. Schreibe

$$v_k = \sum_{i=1}^{n} \alpha_{ik} u_i \text{ mit } \alpha_{ik} \in \mathbb{Z}.$$

Sei $A = (\alpha_{ik}) \in \mathbb{Z}^{n \times k}$. Wir werden die Matrix A durch schrittweises Abändern der Basis $u_1, \ldots, u_n$ und des Erzeugendensystems $v_1, \ldots, v_k$ in die Form

$$\left(\begin{array}{ccc|c} \epsilon_1 & & & \\ & \ddots & & 0 \\ & & \epsilon_m & \\ \hline & 0 & & 0 \end{array}\right)$$

transfromieren. Erlaubte Abänderungen sind dabei:
(1) Vertauschung zweier u oder v. Dies entspricht der Vertauschung zweier Zeilen oder Spalten.
(2) Ersetzung eines u_i durch $u_i + \lambda u_j, \lambda \in \mathbb{Z}, i \neq j$. Wegen

$$v_k = \sum_{l=1}^{n} \alpha_{lk} u_l = \sum_{l=1, l \neq i,j}^{n} \alpha_{lk} u_l + \alpha_{ik}(u_i + \lambda u_j) + (\alpha_{jk} - \alpha_{ik}\lambda) u_j$$

entspricht dies der Ersetzung der j-ten Zeile durch j-te Zeile minus λ mal i-te Zeile.
(3) Ersetzung eines v_i durch $v_i - \lambda v_j, \lambda \in \mathbb{Z}, i \neq j$. Dies entspricht der Ersetzung der i-ten Spalte durch i-te Spalte minus λ mal j-te Spalte.

Wir wenden nun den folgenden Algorithmus auf die Matrix A an:
Schritt 1: Durch Vertauschen von Zeilen und Spalten bringe man das Element ungleich Null von kleinstem Betrag an die Stelle $(1, 1)$.
Schritt 2: Durch Subtraktion geeigneter Vielfacher der ersten Zeile, kann man erreichen, dass A von der Form

$$A = \begin{pmatrix} \alpha_{11} & * & \ldots & * \\ \gamma_2 & & & \\ \vdots & & * & \\ \gamma_n & & & \end{pmatrix}$$

ist, wobei jedes γ_i entweder gleich Null ist oder $|\gamma_i| < |\alpha_{11}|$ gilt. Falls alle γ_i gleich Null sind, so gehe zu Schritt 3. Andernfalls gehe zu Schritt 1.
Schritt 3: Durch Subtraktion geeigneter Vielfacher der ersten Spalte, kann man sodann erreichen, dass A von der Form

$$A = \left(\begin{array}{c|ccc} \alpha_{11} & \gamma_1 & \dots & \gamma_k \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

ist, wobei jedes γ_i entweder gleich Null ist oder $|\gamma_i| < |\alpha_{11}|$ gilt. Falls alle γ_i gleich Null sind, so gehe zu Schritt 4. Andernfalls gehe zu Schritt 1.
Schritt 4: Falls $A' = 0$ so beende den Algorithmus.
Schritt 5: Falls alle Einträge von A' durch α_{11} teilbar sind, so gehe mit A' in Schritt 1.
Schritt 6: Sei α_{ik} ein Koeffizient in A', der nicht durch α_{11} teilbar ist. Teile mit Rest,

$$\alpha_{ik} = \alpha_{11}\beta + \gamma, \gamma \neq 0, |\gamma| < |\alpha_{11}|.$$

Addiere nun die erste Zeile zur i-ten Zeile und subtrahiere dann β mal 1. Spalte von der k-ten Spalte. Dann kommt an der Stelle (i,k) gerade γ zu stehen. Gehe mit A in Schritt 1.

Der Algorithmus endet nach endlich vielen Schritten, da in den Schritten 2,3 und 5 der minimale Betrag der Elemente ungleich 0 von A verringert wird.
Als Folgerung hieraus (bis auf die Eindeutigkeit) erhalten wir den

Satz 1.10.7 *(Hauptsatz über endlich erzeugte abelsche Gruppen) Sei A eine endlich erzeugte abeslche Gruppe. Dann gibt es eindeutig bestimmte $\epsilon_1, \dots, \epsilon_s \in \mathbb{N}$, $\epsilon_i > 1$, mit $\epsilon_1 \mid \epsilon_2 \mid \dots \mid \epsilon_s$, so dass*

$$A \simeq \oplus_{i=1}^{s} \mathbb{Z}/\epsilon_i\mathbb{Z} \oplus \mathbb{Z}^r, \quad r = Rang(A/T(A)).$$

Definition 1.10.8 $\epsilon_1, \dots, \epsilon_s$ nennt man die Invariantenteiler von A. Falls

$$\epsilon_i = \prod_{j=1}^{t} p_j^{e_{ij}}, \quad e_{ij} \in \mathbb{N}_0,$$

die eindeutige Primzahlzerlegung der ϵ_i ist, so nennt man die $p_j^{e_{ij}}$ die Elementarteiler von A.

Remarks 1.10.9 1) Nach dem Chinesischen Restsatz folgt

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s}\bigoplus_{j=1}^{t} \mathbb{Z}/p_j^{e_{ij}}\mathbb{Z} \simeq \mathbb{Z}^r \oplus \bigoplus_{j=1}^{t}\bigoplus_{i=1}^{s} \mathbb{Z}/p_j^{e_{ij}}\mathbb{Z}.$$

Es gilt:

$$T_{p_j}(A) \simeq \bigoplus_{i=1}^{s} \mathbb{Z}/p_j^{e_{ij}}\mathbb{Z},$$

wobei wir für eine Primzahl p definieren:

$$T_p(A) := \{a \in A \mid \text{ es gibt } k \in \mathbb{N} \text{ mit } p^k a = 0\}.$$

2) Invariantenteiler und Elementarteiler entsprechen sich eineindeutig.

2 Körpertheorie

2.1 Konstruierbarkeit mit Zirkel und Lineal

Gegeben sei eine Menge $M \subseteq \mathbb{R}^2$. Kosntruierbar sind

(i) Geraden durch zwei Punkte aus M.

(ii) Kreise um $m \in M$ durch $c \in M$.

(iii) Schnittpunkte zwischen diesen Kreisen und Geraden.

Es sei $\mathcal{K}_M$ die Menge der Punkte, die man durch wiederholte Anwendung von (i)-(iii) aus M konstruieren kann.
Wir identifizieren den $\mathbb{R}^2$ mit den komplexen Zahlen $\mathbb{C}$. Durch elementare geometrische Konstruktionen zeigt man

Satz 2.1.1 *Sei $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$. Dann ist $\mathcal{K}_M$ ein Teilkörper von $\mathbb{C}$ und es gilt $\mathbb{Q}(i) \subseteq \mathcal{K}_M$.*

Satz 2.1.2 *Sei $M \subseteq \mathbb{C}$ mit $\{0,1\} \subseteq M$. Dann ist $\mathcal{K}_M$ quadratisch abgeschlossen, d.h., falls $z \in \mathcal{K}_M$, so auch $\sqrt{z} \in \mathcal{K}_M$.*

Definition 2.1.3 Sei E ein Körper und $k \subseteq E$ ein Teilkörper. Sei $A \subseteq E$. Dann heißt der kleinste Teilkörper von E, der k und A enthält, der aus k durch Adjunktion von A entstehende Teilkörper von E.
Bezeichnung: $k(A)$ "k adjungiert A"
Falls $A = \{\alpha_1, \ldots, \alpha_s\}$ endlich ist, so schreibt man auch $k(A) = k(\alpha_1, \ldots, \alpha_s)$.

Für den Körper $K := \mathbb{Q}(M \cup \bar{M})$ gilt $\mathcal{K}_M = \mathcal{K}_K$, so daß wir ab jetzt voraussetzen, daß $M = K$ ein Körper ist mit $K = \bar{K}$.

Lemma 2.1.4 *Sei $K \subseteq \mathbb{C}$ ein Teilkörper mit $K = \bar{K}$. Dann gilt:*
a) Ist z der Schnittpunkt zweier aus K konstuierbarer Geraden, so ist $z \in K$.
b) Ist z Schnittpunkt eines Kreises und einer Geraden, bzw. von zwei Geraden (alle Geraden und Kreise aus M konstruierbar), so gibt es ein $w \in \mathbb{C}$ mit $w^2 \in K$ und $z \in K(w)$.

Definition 2.1.5 Sei E/K eine Körpererweiterung. Dann entsteht E aus K durch Adjunktion einer Quadratwurzel, falls es ein $w \in E$ mit $w^2 \in K$ und $E = K(w)$ gibt. Man sagt, E ensteht aus K durch sukzessive Adjunktion einer Quadratwurzel, falls es eine Kette

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = E$$

gibt, so daß K_{i+1} aus K_i durch Adjunktion einer Quadratwurzel entsteht.

Hiermit können wir eine erste Version des Hauptsatzes hinsichtlich Fragen der Konstruierbarkeit formulieren.

Satz 2.1.6 *Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $K = \mathbb{Q}(M \cup \bar{M})$. Dann sind folgende Aussagen äquivalent:*
a) $z \in \mathcal{K}_M$
b) z liegt in einem Teilkörper E von $\mathbb{C}$, der aus K durch sukzessive Adjunktion von Quadratwurzeln entsteht.

2.2 Die Gradformel

Falls E/K eine Körpererweiterung ist, so kann man E in natürlicher Weise als K-Vektorraum auffassen.

Definition 2.2.1 Sei E/K eine Körpererweiterung. Dann heißt die Dimension $[E : K] := \dim_K(E)$ der Grad von E über K.

Remark 2.2.2 Falls E ein endlicher Körper der Charakteristik p ist, so gilt: $|E| = p^d$ mit $d = [E : \mathbf{F}_p]$.

Körpererweiterungen vom Grad 2 lassen sich leicht charakterisieren.

Lemma 2.2.3 *Sei K ein Körper mit Charakteristik $\neq 2$ und E/K. Dann sind folgende Aussagen äquivalent:*
a) $[E : K] = 2$
b) $E = K(\alpha), \alpha \notin K, \alpha^2 \in K$.

Damit erhalten wir eine neue Formulierung des Hauptsatzes.

Satz 2.2.4 *Sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ und $K = \mathbb{Q}(M \cup \bar{M})$. Dann sind folgende Aussagen äquivalent:*
a) $z \in \mathcal{K}_M$
b) Es gibt eine Kette $K = K_0 \subseteq \ldots \subseteq K_n = E$ mit $[K_{i+1} : K_i] = 2$ und $z \in E$

Satz 2.2.5 *(Gradfromel) Sei $E/F/K$ ein Körperturm. Dann gilt:*

$$[E : K] = [E : F][F : K]$$

Zusammen mit unserem Hauptsatz erhalten wir

Folgerung 2.2.6 *a) Falls E aus K, char$(K) \neq 2$, durch sukzessive Adjunktion von Quadratwurzeln hervorgeht, so gilt: $[E : K] = 2^m, m \in \mathbb{N}$.*
b) Insbesondere gilt für Körper $K \subseteq \mathbb{C}$ mit $K = \bar{K}$:

$$z \in \mathcal{K}_K \implies [K(z) : K] = 2^m, m \in \mathbb{N}_0$$

Remark 2.2.7 a) Die Umkehrung der Folgerung ist im Allgemeinen falsch.
b) Die Verdoppelung des Würfels (dies entspricht der Konstruktion von $\sqrt[3]{2}$) und die Quadratur des Kreises (dies entspricht der Konstruktion von π) sind nicht möglich. Ebenso ist die Konstruktion eines regelmäßigen n-Ecks im Allgemeinen nicht möglich. Wie wir später beweisen werden:

$$\omega = e^{2\pi i/n} \text{ konstruierbar} \iff \varphi(n) = 2^m, m \in \mathbb{N}_0.$$

Hierbei ist φ die Eulersche φ-Funktion.
Letztlich ist auch die Dreiteilung des Winkels im Allgemeinen nicht möglich.

2.3 Algebraische Körpererweiterungen

Definition 2.3.1 Sei E/K eine Körpererweiterung. Ein Element $\alpha \in E$ heißt algebraisch über K, falls es ein Polynom $f(x) \neq 0$ in $K[x]$ gibt, so daß $f(\alpha) = 0$.
Falls α nicht algebraisch ist, so heißt α transzendent über K.

Der Begriff "algebraisch" läßt sich folgendermaßen charakterisieren.

Satz 2.3.2 *Sei E/K eine Körpererweiterung und $\alpha \in E$. Dann gilt:*

$$\alpha \text{ ist algebraisch}/K \iff [K(\alpha) : K] < \infty.$$

Eine wesentliche Rolle im Beweis spielt das sogenannte Minimalpolynom.

Definition 2.3.3 Sei E/K eine Körpererweiterung und $\alpha \in E$ algebraisch über K. Dann heißt das normierte Polynom $m(x) \in K[x]$ kleinsten Grades mit der Eigenschaft $m(\alpha) = 0$ das Minimalpolynom von α über K.

Remark 2.3.4 1) Für jedes Polynom $f(x) \in K[x]$ mit $f(\alpha) = 0$ gilt $m(x) \mid f(x)$. Insbesondere, falls $f(x) \in K[x]$ normiert und irreduzibel ist und $f(\alpha) = 0$ gilt, so ist f das Minimalpolynom von α.
2) Das Minimalpolynom $m(x)$ ist irreduzibel.
3) $[K(\alpha) : K] = \deg(m(x))$.
4) Faßt man die Multiplikation mit α als Endomorphismus des K-Vektorraums E auf, so ist $m(x)$ ein Teiler des charakteristischen Polynoms.

Definition 2.3.5 Eine Körpererweiterung E/K heißt algebraisch, falls jedes Element $\beta \in E$ algebraisch über K ist. Andernfalls heißt E transzendent.

Satz 2.3.6 *1) Jede endliche Körpererweiterung E/K (d.h. $[E : K] < \infty$) ist algebraisch.*
2) Es gilt: $\alpha \in E$ ist algebraisch über $K \iff K(\alpha)/K$ ist algebraisch.
3) Sei $\alpha \in E$ algebraisch über K mit Minimalpolynom $m(x)$. Dann gilt: $\deg(m(x)) \mid [E : K]$.

Man beachte, daß die Umkehrung von 1) falsch ist. Jedoch gilt

Satz 2.3.7

$$E = K(\alpha_1, \ldots, \alpha_m), \alpha_1, \ldots, \alpha_m \text{ alg. } /K \iff [E : K] < \infty.$$

Definition 2.3.8 Sei E/K eine Körpererweiterung. Dann heißt

$$\{\alpha \in E \mid \alpha \text{ ist algebraisch über } K\}$$

der algebraische Abschluß von K in E.

Satz 2.3.9 *Sei E/K eine Körpererweiterung. Dann ist der algebraische Abschluß von K in E ein Teilkörper von E.*

Der folgende Satz besagt, daß der Begriff "algebraisch" transitiv ist.

Satz 2.3.10 *Sei $E/L/K$ ein Körperturm. Dann gilt:*

$$E/K \text{ ist algebraisch} \iff E/L \text{ und } L/K \text{ sind algebraisch.}$$

Definition 2.3.11 Sei E/K eine Körpererweiterung und $K \subseteq L_1, L_2 \subseteq E$ seien Zwischenkörper. Dann heißt $L_1L_2 := L_1(L_2) = L_2(L_1)$ das Kompositum von L_1 und L_2. Also ist L_1L_2 der kleinste Teilkörper von E, der L_1 und L_2 enthält.

Satz 2.3.12 *Sei $K \subseteq L_1, L_2 \subseteq E$. Dann gilt:*
a) L_1/K algebraisch $\implies L_1L_2/L_2$ algebraisch.
b) L_1/K endlich $\implies L_1L_2/L_2$ endlich, genauer: $[L_1L_2 : L_2] \leq [L_1 : K]$.
c) $L_1/K, L_2/K$ algebraisch $\implies L_1L_2/K$ algebraisch.
d) $L_1/K, L_2/K$ endlich $\implies L_1L_2/K$ endlich, genauer: $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$. Falls zusätzlich $ggT([L_1 : K], [L_2 : K]) = 1$, so gilt in der Ungleichung sogar Gleichheit.

2.4 Einfache Körpererweiterungen

Definition 2.4.1 Eine Körpererweiterung L/K heißt einfach, falls $\alpha \in L$ existiert, so daß $L = K(\alpha)$. Jedes solche α heißt primitives Element.

Es sei nun L/K eine Körpererweiterung und $\alpha \in L$. Dann definieren wir

$$K[\alpha] := \{g(\alpha) \mid g \in K[X]\}.$$

Lemma 2.4.2 *Es gilt:*

$$\alpha \text{ ist algebraisch}/K \iff K(\alpha) = K[\alpha] \iff K[\alpha] \text{ ist ein Körper.}$$

Im Gegensatz hierzu gilt:

Lemma 2.4.3 *Folgende Aussagen sind äquivalent:*
(i) α ist transzendent.
(ii) Die Abbildung $\varphi : K[X] \longrightarrow K[\alpha], g(X) \mapsto g(\alpha)$ ist ein Isomorphismus.
(iii) $K[\alpha]$ ist kein Körper.

Definition 2.4.4 Der Körper $K(X) := Quot(K[X])$ heißt der rationale Funktionenkörper. Es gilt:

$$K(X) = \left\{ \frac{f(X)}{g(X)} \mid f, g \in K[X], g \neq 0 \right\}.$$

Satz 2.4.5 *Sei L/K eine Körpererweiterung und $\alpha \in L$ sei transzendent. Dann ist $K(\alpha)$ isomorph zu $K(X)$.*

Wir erinnern nochmals an einfache Konsequenzen aus der Definition des Minimalpolynoms.

Lemma 2.4.6 *Sei L/K eine Körpererweiterung und $\alpha \in L$ algebraisch. Dann gilt:*
a) Mipo_α *ist irreduzibel.*
b) Sei $f \in K[X]$ irreduzibel und normiert und es gelte $f(\alpha) = 0$. Dann ist $f = \mathrm{Mipo}_\alpha$.

Satz 2.4.7 *Sei L/K eine einfache algebraische Erweiterung und $\alpha \in L$ ein primitives Element, d.h. $L = K(\alpha)$. Dann gilt:*

$$K[X]/\left(\mathrm{Mipo}_\alpha(X)\right) \xrightarrow{\simeq} K(\alpha) = K[\alpha]$$

Umgekehrt gilt

Satz 2.4.8 *Sei $f \in K[X]$ irreduzibel. Dann is $K[X]/(f(X))$ eine algebraische Körpererweiterung vom Grad* $\deg(f)$.

2.5 Zerfällungskörper von Polynomen

Definition 2.5.1 Seien E_1, E_2 Erweiterungskörper von K. Dann nennt man einen Körperhomomorphismus $\sigma : E_1 \longrightarrow E_2$ mit $\sigma|_K = id$ einen K-Homomorphismus von E_1 in E_2. Man schreibt dann auch $\sigma : E_1/K \longrightarrow E_2/K$.

K-Homomorphismen sind stets injektiv. Sei $E_1 = K(\alpha)$ mit $f = \mathrm{Mipo}_\alpha$. Sei $\sigma : E_1/K \longrightarrow E_2/K$ und es sei $\sigma(\alpha) = \beta$. Dann ist β ebenfalls eine Nullstelle von f.

Lemma 2.5.2 *Seien E/K und E'/K' Körpererweiterungen und $\sigma : K \longrightarrow K'$ ein Homomorphismus von Körpern.*
a) σ induziert einen Ringhomomorphismus

$$\begin{aligned} \sigma : K[X] &\longrightarrow K'[X], \\ f = \sum a_i X^i &\mapsto f^\sigma = \sigma f := \sum \sigma(a_i) X^i. \end{aligned}$$

b) Jeder Homomorphismus $\tau : E \longrightarrow E'$, der σ fortsetzt (d.h. $\tau|_K = \sigma$), führt Nullstellen von f in Nullstellen von σf über.
c) Sei $\sigma : K \longrightarrow K'$ ein Isomorphismus. Sei $\alpha \in E$ algebraisch und $f = \mathrm{Mipo}_\alpha$. Sei $\alpha' \in E'$ eine Nullstelle von σf. Dann gibt es genau eine Fortsetzung $\tau : K(\alpha) \longrightarrow K(\alpha')$ von σ mit $\tau(\alpha) = \alpha'$.

Definition 2.5.3 Ein Körper C heißt algebraisch abgeschlossen, falls jedes nicht-konstante Polynom $f \in C[X]$ eine Nullstelle in C besitzt.

Satz 2.5.4 *Folgende Aussagen sind äquivalent:*
(i) C ist algebraisch abgeschlossen.
(ii) Jedes irreduzible Polynom in $C[X]$ ist linear.
(iii) Jedes Polynom $f \in C[X]$ vom Grad ≥ 1 zerfällt vollständig in Linearfaktoren.
(iv) Ist E/C eine algebraische Körpererweiterung, so gilt $E = C$.

Satz 2.5.5 *Sei K ein beliebiger Körper. Dann gibt es einen Erweiterungskörper C/K mit folgenden Eigenschaften:*

(i) C ist algebraisch abgeschlossen.

(ii) C/K ist algebraisch.

Der Körper C ist bis auf K-Isomorphie eindeutig bestimmt.

Definition 2.5.6 Der Körper C aus vorigem Satz heißt der algebraische Abschluß von K. Oft schreibt man $C = \bar{K}$.

Die Existenz eines algebraischen Abschluß ist im allgemeinen nicht ganz einfach zu beweisen. Falls $K \subseteq \mathbb{C}$, so können wir einfach

$$C := \{\alpha \in \mathbb{C} | \alpha \text{ ist algebraisch über } K\}$$

wählen.

Satz 2.5.7 *Sei E/K algebraisch und C ein algebraischer Abschluss von E (und damit auch von K). Sei $\tau\colon E \longrightarrow C$ ein K-Homomorphismus.*
a) Sei $\alpha \in C$. Dann gibt es eine Fortsetzung

$$\hat{\tau}\colon E(\alpha) \longrightarrow C$$

von τ. Genauer: Sei $f \in E[x]$ das Minimalpolynom von α und $\beta \in C$ eine Nullstelle von τf. Sei $E' := \tau(E)$. Dann ist

$$\begin{aligned} \hat{\tau}\colon E(\alpha) &\longrightarrow E'(\beta), \\ \alpha &\mapsto \beta, \\ a &\mapsto \tau(a) \text{ für alle } a \in E, \end{aligned}$$

ein K-Isomorphismus.
b) Sei L/E eine endliche Körpererweiterung. Dann gibt es eine Fortsetzung $\hat{\tau}\colon L \longrightarrow C$ von τ.

Satz 2.5.8 *Sei E/K algebraisch und C ein algebraischer Abschluss von E. Sei $\tau\colon E \longrightarrow C$ ein K-Homomorphismus und C' ein Körper mit $E \subseteq C' \subseteq C$. Dann gibt es eine Fortsetzung $\hat{\tau}\colon C' \longrightarrow C$ von τ.*

Definition 2.5.9 Sei $f \in K[X]$ ein nicht-konstantes Polynom. Sei C ein algebraischer Abschluß von K und $\{\alpha_1, \ldots, \alpha_n\}$ die Menge der Nullstellen von f in C. Dann heißt $E := K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von f.

Unsere Definition ist abhängig von der Wahl eines algebraischen Abschluß C. Der Zerfällungskörper von f ist jedoch eindeutig bis auf K-Isomorphie.

Definition 2.5.10 Eine Körpererweiterung E/K heißt normal, falls für jedes irreduzible Polynom $f \in K[X]$ gilt: Hat f eine Nullstelle in E, so liegen sämtliche Nullstellen (die a priori in einem algebraischen Abschluß C von E liegen) im Körper E.

Der folgende Satz charakterisisiert den wichtigen Begriff "normal".

Satz 2.5.11 *Sei E/K algebraisch und C ein algebraischer Abschluß von E (und damit auch von K). Dann sind folgende Aussagen äquivalent:*

(i) *E/K ist normal.*

(ii) *Für jeden K-Homomorphismus $\sigma : E \longrightarrow C$ gilt $\sigma(E) \subseteq E$.*

(iii) *Für jeden K-Homomorphismus $\sigma : C \longrightarrow C$ gilt $\sigma(E) \subseteq E$.*

(iv) *Es gibt eine Menge von Polynomen $M \subseteq K[X]$, so daß $E = K(N)$, wobei $N = \{\alpha \in C \mid \alpha$ ist Nullstelle eines $f \in M\}$ die Gesamtheit der Nullstellen in C der Polynome in M bezeichnet.*

Remark 2.5.12 Insbesondere ist also der Zerfällungskörper eines Polynoms $f \in K[X]$ stets normal über K.

Remark 2.5.13 In (ii) und (iii) kann man jeweils $\sigma(E) \subseteq E$ ersetzen durch $\sigma(E) = E$. Dies folgt aus der folgenden allgemeinen Beobachung: Sei E/K algebraisch und $\sigma\colon E/K \longrightarrow E/K$ eine K-Homomorphismus. Dann ist σ ein Isomorphismus.

Satz 2.5.14 *Sei E/K algebraisch.*
a) Es gibt einen Erweiterungskörper E'/E mit den folgenden Eigenschaften:

(i) *E'/K ist normal.*
(ii) *Falls $E'/L/K$ und L/K normal ist, so ist $E' = L$.*

b) Sind E' und E'' zwei solche Körper, so gibt es einen K-Isomorphismus

$$\sigma\colon E'/K \longrightarrow E''/K.$$

c) Ist $[E : K] < \infty$, so auch $[E' : K] < \infty$

Definition 2.5.15 Den Körper E' aus Satz 2.5.14 nennt man die normale Hülle von E/K.

2.6 Separabilität

Definition 2.6.1 Sei K ein Körper und C ein algebraischer Abschluß von K. Zwei Elemente $\alpha, \beta \in C$ heißen zueinander konjugiert über K, falls es einen Homomorphismus $\tau : C/K \longrightarrow C/K$ mit $\tau(\alpha) = \beta$ gibt.

Lemma 2.6.2 *Folgende Aussagen sind äquivalent:*
(i) α und β sind zueinander konjugiert über K.
(ii) β ist eine Nullstelle von Mipo_α.
(iii) Es gibt einen Isomorphismus $\tau : K(\alpha)/K \longrightarrow K(\beta)/K$ mit $\tau(\alpha) = \beta$.
(iv) $\mathrm{Mipo}_\alpha = \mathrm{Mipo}_\beta$.

Als Konsequenz aus dem Lemma ergibt sich

Folgerung 2.6.3 *Jedes $\alpha \in C$ hat höchstens* $\deg(\mathrm{Mipo}_\alpha) = [K(\alpha) : K]$ *viele verschiedene Konjugierte über K.*

Definition 2.6.4 Sei $\alpha \in C$ und $f = \mathrm{Mipo}_\alpha$. Dann heißt die Anzahl der verschiedenen Nullstellen von f in C der Separabilitätsgrad von α (in Zeichen: $[K(\alpha) : K]_s$). Ein Element α heißt separabel über K, falls gilt: $[K(\alpha) : K]_s = [K(\alpha) : K]$. Andernfalls heißt α inseparabel.

Definition 2.6.5 Sei E/K algebraisch. Dann heißt E/K separabel, falls jedes Element $\alpha \in E$ über K separabel ist. Sonst heißt E/K inseparabel.

Die folgenden Bemerkungen sind offensichtlich.

Remark 2.6.6 1) α ist separabel $\iff$ Mipo_α hat nur einfache Nullstellen in C.
2) $[K(\alpha) : K]_s \leq [K(\alpha) : K]$.
3) $\alpha \in K$ ist stets separabel über K.

Definition 2.6.7 1) Seien E_1 und E_2 zwei Körpererweiterungen von K. Dann bezeichnet $G(E_1/K, E_2/K)$ die Menge der K-Homomorphismen von E_1 in E_2. Falls $E_1 = E_2 = E$, so schreiben wir kürzer $G(E/K) = G(E_1/K, E_2/K)$.
2) Falls E/K algebraisch ist, so nennt man $G(E/K)$ auch die Automorphismengruppe von E/K.

Der folgende Satz ist grundlegend.

Satz 2.6.8 *Sei $[E : K] = n < \infty$ und C ein algebraischer Abschluß von E. Dann gilt:*
i) $|G(E/K, C/K)| \leq n$.
ii) $|G(E/K, C/K)| = n \iff E/K$ ist separabel.

Folgerung 2.6.9 *Sei $\alpha \in C$. Dann gilt:*

$$\alpha \text{ ist separabel über } K \iff K(\alpha)/K \text{ ist separabel.}$$

Der Begriff der Separabilität ist transitiv.

Satz 2.6.10 *Sei E/K algebraisch und $K \subseteq L \subseteq E$. Dann gilt:*

$$E/K \text{ ist separabel} \iff E/L \text{ und } L/K \text{ sind separabel.}$$

Satz 2.6.11 *Sei E/K eine Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:*
i) E/K ist endlich und separabel.
ii) Es gibt separable algebraische Elemente $\alpha_1, \ldots, \alpha_n \in E$, so daß $E = K(\alpha_1, \ldots, \alpha_n)$.

In der Zahlentheorie wurde im Abschnitt über Polynomringe gezeigt, daß für irreduzible Polynome $f \in K[X]$ folgende Äquivalenz gilt:

$$f \text{ separabel} \iff f' \neq 0. \tag{1}$$

Dies impliziert:

Satz 2.6.12 *Sei $char(K) = 0$. Dann ist jedes irreduzible Polynom $f \in k[X]$ separabel. Insbesondere ist jede algebraische Erweiterung von K separabel.*

Eine weitere Konsequenz aus (1) ist das folgende Resultat.

Folgerung 2.6.13 *Sei $char(K) = p > 0$. Sei $f \in K[x]$ irreduzibel. Dann gilt:*

$$f \textit{ ist separabel} \iff f \notin K[x^p].$$

Definition 2.6.14 Ein Körper K heißt vollkommen oder perfekt, falls jede algebraischen Erweiterung E/K separabel ist.

Körper K der Charakteristik 0 sind also vollkommen. Wir wollen im Weiteren zeigen, dass auch alle endlichen Körper K vollkommen sind.

Satz 2.6.15 *Sei $char(K) = p > 0$. Sei $K^p := \{\alpha^p \mid \alpha \in K\}$. Dann gilt:*

$$K \textit{ ist vollkommen} \iff K^p = K$$

Für eine Körper K der Charakteristik $p > 0$ betrachten wir den sogenannten Frobenius-Homomorphismus

$$\sigma_p \colon K \longrightarrow K, \quad \alpha \mapsto \alpha^p.$$

Falls K endlich ist, so ist σ_p ein Automorphismus und wir erhalten das folgende Korollar.

Folgerung 2.6.16 *Sei $|K| < \infty$. Dann ist K vollkommen.*

3 Galoistheorie

3.1 Der Hauptsatz der Galoistheorie

Definition 3.1.1 Sei E/K eine Galoiserweiterung und $G \leq G(E/K)$. Dann nennt man

$$E^G := \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

den Fixkörper von E unter G.

Definition 3.1.2 Eine algebraische Erweiterung heißt galoissch, falls $E^{G(E/K)} = K$ gilt.

Der nächste Satz liefert eine äquivalente definierende Eigenschaft.

Satz 3.1.3 *Sei E/K algebraisch. Dann gilt:*

$$E/K \textit{ ist galoissch} \iff E/K \textit{ ist separabel und normal.}$$

Folgerung 3.1.4 *Sei $f \in K[X]$ separabel und E der Zerfällungskörper von f. Dann ist E/K eine endliche galoissche Erweiterung.*

Sei nun E/K galoissch und F ein Zwischenkörper. Es ist leicht zu beweisen, daß dann E/F ebenfalls galoissch ist. Ferner ist die Zuordung

$$\begin{array}{rccc} \psi\colon \text{ Menge der Zwischenkörper von } E/K & \longrightarrow & \text{Menge der Untergruppen von } G(E/K), \\ F & \mapsto & G(E/F) \end{array}$$

injektiv.

Remark 3.1.5 Falls E/K eine endliche Erweiterung ist, so ist $G(E/K)$ eine endliche Gruppe. Wegen der Injektivität von ψ folgt, dass es nur endlich viele Zwischenkörper von E/K gibt.

Man beacht, daß F/K im allgemeinen nicht galoissch ist. Hier gilt:

Satz 3.1.6 *Sei E/K galoissch und F ein Zwischenkörper. Sei $\sigma \in G(E/K)$. Dann gilt:*

$$G(E/\sigma(F)) = \sigma G(E/F)\sigma^{-1}.$$

Ferner sind die folgenden Aussagen äquivalent:
(i) F/K ist galoissch.
(ii) $\sigma(F) = F, \forall \sigma \in G(E/K)$.
(iii) $G(E/F) \lhd G(E/K)$.
In diesem Fall induziert die Restriktion eine Isomorphie von Gruppen

$$G(E/K)/G(E/F) \xrightarrow{\simeq} G(F/K).$$

Ein wichtiger Schritt auf dem Weg zum Hauptsatz der Galoistheorie ist der sogenannte Satz vom primitiven Element, der auch für sich allein von Bedeutung ist.

Satz 3.1.7 *(Satz vom primitiven Element) Sei E/K endlich und separabel. Dann gibt es ein Element $\alpha \in E$, so daß $E = K(\alpha)$. Man sagt dann auch, die Erweiterung E/K ist einfach.*

Der folgende Satz faßt im wesentlichen unsere bisherigen Resultate dieses Abschnitts zusammen. Neu hinzu kommt nur die Aussage zur Surjektivität im ersten Teil des Satzes.

Satz 3.1.8 *(Hauptsatz der Galoistheorie) Sei E/K eine endliche galoissche Erweiterung. Dann ist die Abbildung*

$$F \mapsto G(E/F)$$

eine Bijektion zwischen der Menge der Zwischenkörper F von E/K und der Menge der Untergruppen U von $G(E/K)$. Ferner gilt:
(i) E/F ist galoissch und $|G(E/F)| = [E : F]$.
(ii) $F_1 \subseteq F_2 \iff G(E/F_2) \leq G(E/F_1)$.
(iii) F/K ist galoissch $\iff G(E/F) \lhd G(E/K)$.
(iv) Falls F/K galoissch ist, so induziert die Restriktion einen Isomorphismus

$$G(E/K)/G(E/F) \xrightarrow{\simeq} G(F/K).$$

Remark 3.1.9 Sei E/K eine endliche Erweiterung. Dann gilt:

$$E/K \text{ ist galoissch} \iff |G(E/K)| = [E : K].$$

Wir haben in der Vorlesung nur die Hinrichtung gezeigt. Die Rückrichtung folgt aus den Sätzen 2.6.8 und 2.5.11.
Der Satz vom primitiven Element impliziert

Folgerung 3.1.10 *Die endlichen galoisschen Erweiterungen E/K sind genau die Zerfällungskörper von separablen Polynomen $f \in K[X]$.*

Definition 3.1.11 Sei $f \in K[X]$ separabel und E/K der Zerfällungskörper von f. Dann nennt man die Galoisgruppe $G(E/K)$ auch die Galoisgruppe von f über K.

Wichtige Beispiele für Galoiserweiterungen sind die Kreisteilungskörper $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ und die endlichen Erweiterungen E/K mit endlichen Körpern K, die im Rahmen der Vorlesung zur Zahlentheorie besprochen wurden.

3.2 Konstruierbarkeit

Wir kommen zurück zu Fragen der Konsruierbarkeit. Insbesondere wollen wir entscheiden, welche regelmäßigen n-Ecke mit Zirkel und Lineal konstruierbar sind.

Satz 3.2.1 *Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $K := \mathbb{Q}(M \cup \bar{M})$. Dann sind für $z \in \mathbb{C}$ die folgenden zwei Aussagen äquivaelent:*
(i) z ist konstruierbar, d.h. $z \in \mathcal{K}_M = \mathcal{K}_K$.
(ii) z ist algebraisch über K und für die normale Hülle E von $K(z)/K$ gilt:

$$[E : K] \text{ ist eine 2-Potenz.}$$

Als Konsequenz hieraus erhalten wir eine einfache Charakterisierung der Konstruierbarkeit von regelmäßigen n-Eccken.

Satz 3.2.2 *Das regelmäßigen n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn*

$$n = 2^e p_1 \cdots p_r$$

mit paarweise verschiedenen ungeraden Primzahlen von der Form $p_i = 1 + 2^{m_i}$. (Hier ist $r = 0$ erlaubt.)

Man zeigt leicht, daß folgendes gilt:

$$1 + 2^m \text{ ist eine Primzahl } \implies m \text{ ist eine 2-Potenz.} \tag{2}$$

Dies führt zu folgender Definition.

Definition 3.2.3 $F_k := 1 + 2^{2^k}$ heißt k-te Fermatzahl.

Die Umkehrung von (2) ist im Allgemeinen falsch, z.B. $F_5 = 641 \cdot 6700417$.

3.3 Ergänzungen zur Galoistheorie

Satz 3.3.1 *(Translationssatz) Sei C ein algebraischer Abschluß von K und $E, K' \subseteq C$. Sei E/K galoissch. Dann gilt:*
a) EK'/K' ist galoisch.
b) Die Restriktionsabbildung

$$G(EK'/K') \longrightarrow G(E/E \cap K'), \quad \sigma \mapsto \sigma|_E,$$

ist ein Isomorphismus.
c) Falls E/K endlich ist, so ist auch EK'/K' endlich und es gilt

$$[EK' : K'] \mid [E : K].$$

Satz 3.3.2 *(Kompositonssatz) Sei C ein algebraischer Abschluß von K und E_1/K und E_2/K galoissche Teilkörper von C/K. Dann gilt:*
a) E_1E_2/K ist galoissch.
b) Der Gruppenhomomorphismus

$$\begin{aligned} G(E_1E_2/K) &\longrightarrow G(E_1/K) \times G(E_2/K), \\ \gamma &\mapsto (\gamma|_{E_1}, \gamma|_{E_2}), \end{aligned}$$

ist injektiv. Das Bild ist gegeben durch

$$\Delta := \{(\sigma, \tau) \in G(E_1/K) \times G(E_2/K) \mid \sigma|_{E_1 \cap E_2} = \tau|_{E_1 \cap E_2}\}.$$

3.4 Auflösbarkeit von Gleichnungen

Definition 3.4.1 i) Sei F/K eine Körpererweiterung. Dann entsteht F aus K durch sukzessive Adjunktion von Radikalen, falls es einen Körperturm

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_r = F$$

gibt, so dass K_i aus K_{i-1} durch Adjunktion einer n_i-ten Wurzel (= Radikal vom Exponenten n_i) entsteht. F/K heißt dann auch Radikalerweiterung.
(ii) Eine Körpererweiterung E/K heißt durch Radikale auflösbar, falls es eine Radikalerweiterung F/K gibt mit $E \subseteq F$.
(iii) Ein Polynom $f \in K[x]$ heißt durch Radikale auflösbar, falls der Zerfällungskörper E von f durch Radikale auflösbar ist.

Remarks 3.4.2 a) Jede Radikalerweiterung entsteht durch sukzessive Adjunktion von Radikalen von Primzahlexponenten.
b) Falls F_1/K eine Radikalerweiterung und F_2/K eine beliebige Körpererweiterung ist, so ist F_1F_2/F_2 ebenfalls eine Radikalerweiterung. Falls F_2/F_1 und F_1/K Radikalerweiterungen sind, so ist auch F_2/K eine Radikalerweiterung. Falls F_1/K und F_2/K Radikalerweiterungen sind, so ist auch F_1F_2/K eine Radikalerweiterung.
c) Falls F/K eine Radikalerweiterung und E die normale Hülle von F/K ist, so ist auch E/K eine Radikalerweiterung.
d) Sei $f \in K[x]$ irreduzibel und E/K durch Radikale auflösbar. Sei $\alpha \in E$ eine Nullstelle von f. Dann ist f durch Radikale auflösbar.

Satz 3.4.3 *Sei E/K durch Radikale auflösbar und E'/K die normale Hülle von E. Dann ist die Gruppe $G(E'/K)$ auflösbar.*

Examples 3.4.4 1) Sei $E = \mathbb{Q}(\sqrt[4]{2})$ und $K = \mathbb{Q}$. Dann ist der normale Abschluss gegeben durch $E' = \mathbb{Q}(\sqrt[4]{2}, i)$. Die Erweiterung $E'/\mathbb{Q}$ ist galoissch mit Gruppe $G(E'/\mathbb{Q}) \simeq D_4$. Offensichtlich ist E/K eine Radikalerweiterung, so dass der Satz impliziert, dass $G(E'/\mathbb{Q})$ auflösbar ist. Für die D_4 ist das natürlich längst bekannt.
2) Sei $E/\mathbb{Q}$ vom Grad 5 und $E'/\mathbb{Q}$ die normale Hülle. Falls dann $G(E'/\mathbb{Q}) \simeq S_5$ gilt, so ist $E/\mathbb{Q}$ nicht durch Radikale auflösbar, da die S_5 nicht auflösbar ist.
3) Sei $f \in K[x]$ irreduzibel vom Grad ≥ 5. Sei E'/K der Zerfällungskörper von f. Es gelte: $G(E'/K) \simeq S_n$. Dann ist f nicht durch Radikale auflösbar.
4) Hier ist ein explizites Beispiel: Sei $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Nach Eisenstein für $p = 2$ ist f irreduzibel in $\mathbb{Q}[x]$. Eine einfache Kurvendiskussion zeigt, dass f genau ein Paar komplexer Nullstellen und drei reelle Nullstellen hat. Sei $E'/\mathbb{Q}$ der Zerfällungskörper von f. Dann induziert die komplexe Konjugation einen 2-Zyklus $\tau \in G := G(E'/\mathbb{Q})$. Wegen $5 \mid [E' : \mathbb{Q}] = |G|$ hat G eine nicht-triviale 5-Sylowuntergruppe. Diese hat ein nicht-triviales Zentrum Z. In endlichen abelschen Gruppen gibt es zu jedem Teiler d der Gruppenordnung eine Untergruppe U mit $|U| = d$ (Grund:

Elementarteilersatz). Also gibt es in Z eine Untergruppe U der Ordnung 5. Also enthält G einen 5-Zyklus.
Man zeigt relativ leicht, dass eine Untergruppe H der S_5, die einen 2-Zyklus und einen 5-Zyklus enthält, gleich der S_5 ist. Da die S_5 nicht auflösbar ist, ist f nicht durch Radikale auflösbar.

Es gilt auch die Umkehrung von obigem Satz. Der Einfachheit halber setzen wir $\mathrm{char}(K) = 0$ voraus.

Satz 3.4.5 *Sei* $\mathrm{char}(K) = 0$ *und* $f \in K[x]$. *Sei* G *die Gruppe von* f, *d.h.* $G = G(E'/K)$, *wobei* E'/K *den Zerfällungskörper von* f *bezeichnet. Dann gilt:*

$$f \text{ ist durch Radikale auflösbar} \iff G \text{ ist auflösbar.}$$