Algebra 2

Mitschrift von www.kuertz.name

Hinweis: Dies ist **kein offizielles Script**, sondern nur eine private Mitschrift. Die Mitschriften sind teweilse **unvollständig, falsch oder inaktuell**, da sie aus dem Zeitraum 2001–2005 stammen. Falls jemand einen Fehler entdeckt, so freue ich mich dennoch über einen kurzen Hinweis per E-Mail – vielen Dank!

Mihhail Aizatulin (avatar@hot.ee)

Inhaltsverzeichnis

1 Gruppen

1.0 Vorkenntnisse

Sei $G = (G, \cdot)$ eine Gruppe, $|G|$ die Ordnung von G (Anzahl der Elemente von G).

1.0.1 Untergruppen

Sei $H \subseteq G$.

DEFINITIONEN:

1. $H \leq G \Leftrightarrow (H, \cdot|_{H\times H})$ Gruppe $\Leftrightarrow H \neq \emptyset$ und für $x, y \in H$ gilt $xy^{-1} \in H$.
2. $H_i \leq G\ (i \in I) \Rightarrow \bigcap_{i\in I} H_i \leq G$.
3. $\langle H\rangle := \bigcap \{U \mid H \subseteq U \leq G\} = \{a_1 \dots a_n \mid a_i \in H \cup H^{-1}, n \in \mathbb{N}\}$, heißt das *Erzeugnis* von H.
4. $\mathfrak{V}(G) := \{U \mid U \leq G\}$ heißt der *Untergruppenverband* von G (mit Inklusion $\subseteq$ als teilweise Ordnung)

1.0.2 Zyklische Gruppen

G heißt *zyklisch* genau dann, wenn $g \in G$ existiert mit $G = \langle g\rangle$.

1. LEMMA: $\langle g\rangle = \{g^m \mid m \in \mathbb{Z}\}$.
2. SATZ: Für jedes $n \in \mathbb{N} \cup \{\infty\}$ gibt es (bis auf Isomorphie) genau eine zyklische Gruppe der Ordnung n, nämlich $(\mathbb{Z}, +)$ (für $n = \infty$) bzw. $(\mathbb{Z}/n\mathbb{Z}, +)$ $(n \in \mathbb{N})$.
3. SATZ: Zu jedem Teiler d von n existiert in der zyklischen Gruppe $\langle g\rangle$ der Ordnung n genau eine Untergruppe der Ordnung d und zwar $\left\langle g^{\frac{n}{d}}\right\rangle$.

1.0.3 Restklassen, Index, Satz von Lagrange

Sei $H \leq G, x \in G$.

DEFINITION: $Hx = \{hx \mid h \in H\}$, $xH = \{xh \mid h \in H\}$ *Rechts- bzw. Linksrestklassen*. *Index* $|G : H|$ sei die Anzahl der Rechtsrestklassen.

1. SATZ: $G = \bigcup_{x\in G} Hx$ und $Hx = Hy \Leftrightarrow Hx \cap Hy \neq \emptyset \Leftrightarrow xy^{-1} \in H$.
2. SATZ VON LAGRANGE Ist G endlich und $H \leq G$, so ist $|G| = |H| \cdot |G : H|$.

1.0.4 Elementordnung

Sei $g \in G$.

DEFINITION: $o(g) := |\langle g \rangle|$ (kleinstes $n \in \mathbb{N}$ mit $g^n = 1$ bzw. ∞).

EIGENSCHAFTEN:

1. $o(g)$ teilt $|G|$, falls $|G| < \infty$.
2. Sind $a, b \in G$ mit $ab = ba$ und $(o(a), o(b)) = 1$, so ist $o(ab) = o(a) \cdot o(b)$.

1.0.5 Komplexprodukte

Seien $X, Y \subseteq G$.

DEFINITION: $XY = \{ xy \mid x \in X, y \in Y \}$.

1.0.6 Konjugation, Normalteiler, Faktorgruppe

Seien $x, y, g \in G$ und $X \subseteq G$.

DEFINITION: $x^g = g^{-1}xg$ das zu x unter g *konjugierte* Element. $X^g = \{ x^g \mid x \in X \}$.

EIGENSCHAFTEN:

1. $(xy)^g = x^g y^g$
2. $x^{gh} = (x^g)^h$. Genauso für $X \subseteq G$.
3. $\sigma_g : G \to G;\ x \mapsto x^g$ ist ein Automorphismus von G, der von g bewirkte *innere Automorphismus*.
4. SATZ: Folgende Eigenschaften der Untergruppe N von G sind äquivalent:

   (1) $N \trianglelefteq G$ (d.h. $N^g = N$ für alle $g \in G$)

   (2) $Ng = gN$ für alle $g \in G$.

   (3) $G/N = \{ Ng \mid g \in G \}$ bildet mit der Komplexmultiplikation $(Ng) \circ (Nh) = NgNh$ eine Gruppe. Ist $N \trianglelefteq G$, so heißt $(G/N, \circ)$ die *Faktorgruppe* von G nach N.

   Ein $N \leq G$ mit diesen Eigenschaften heißt *Normalteiler* von G.

1.0.7 Homomorphiesatz

Seien G und H Gruppen.

1. Ist $N \trianglelefteq G$, so ist die Abbildung $\rho : G \to G/N;\ g \mapsto Ng$ ein Epimorphismus, der *natürliche Homomorphismus* von G auf G/N.

2. Ist $\sigma : G \to H$ ein Homomorphismus, so ist $N := \operatorname{Kern}\sigma \trianglelefteq G$ und $\sigma = \rho \cdot \tau$ mit $\rho : G \to G/N$, dem natürlichem Homomorphismus und dem Monomorphismus $\tau : G/N \to H;\ Ng \mapsto g^\sigma$. Insbesondere ist $G^\sigma \simeq G/\operatorname{Kern}\sigma$.

1.0.8 Beispiele

1. Ω Menge, $\mathrm{Sym}(\Omega)$ - Menge aller Permutationen ($g : \Omega \to \Omega$ bijektiv) auf Ω, mit Hintereinanderausführung als Verknüpfung.

2. $\Omega = \{1, \ldots, n\},\ S_n := \mathrm{Sym}(\Omega),\ |S_n| = n!$. Sei

$$\mathrm{sgn}(g) = \begin{cases} +1, & \text{falls } g \text{ Produkt gerader Anzahl der Transpositionen} \\ -1, & \text{falls } g \text{ Produkt ungerader Anzahl der Transpositionen} \end{cases}$$

   Somit ist $\mathrm{sgn} : S_n \to \{+1, -1\}$ ein Homomorphismus.

3. Für $n \geq 2$ ist $A_n := \operatorname{Kern}\mathrm{sgn} = \{\, g \in S_n \mid \mathrm{sgn}(g) = 1\}$ ein Normalteiler vom Index 2 in S_n - die *alternierende Gruppe vom Grad n*.

4. V Vektorraum über Körper K. $\mathrm{GL}(V)$ - Menge aller nichtsingulären linearen Abbildungen von V nach V ist Gruppe mit Hintereinanderausführung als Verknüpfung, die *volle lineare Gruppe auf V*. Ist $\dim V = n$, so ist $\mathrm{GL}(V)$ isomorph zu $\mathrm{GL}(n, K)$ - Gruppe der nichtsingulären $n \times n$ - Matrizen über K (mit Matrizenmultiplikation) [1]. Ist $K = \mathrm{GF}(q)$ mit $q = p^f (p \in \mathbb{P},\ f \in \mathbb{N})$, so erhalten wir endliche Gruppen (siehe 5).

5. $\mathrm{GL}(n, q) = \mathrm{GL}(n, GF(q)) \simeq \mathrm{GL}(\mathrm{GF}(q)^n))$. Es gilt $|\mathrm{GL}(n, q)| = (q^n - 1)(q^n - q)(q^n - q^2)\ldots(q^n - q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i)$ - Anzahl der Basen eines n-dimensionalen Vektorraums.

6. $\det : GL(V) \to K^*$. Sei $\mathrm{SL}(V) := \operatorname{Kern}\det = \{\, g \in \mathrm{GL}(V) \mid \det g = 1\}$, die *spezielle lineare Gruppe*. Sei $SL(n, q) := \{\, g \in \mathrm{GL}(n, q) \mid \det g = 1\}$. Für $q = p^f$ ist

$$\mathrm{GL}(V)/\mathrm{SL}(V) \overset{(1.0.7)}{\simeq} K^* \Rightarrow |\mathrm{SL}(n, q)| = \frac{\mathrm{GL}(n, q)}{q - 1}$$

[1] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 4.1.3, 4.2.2

1.0.9 Direktes Produkt

Seien $G_1, \ldots, G_n$ Gruppen. Dann ist $G_1 \times \ldots \times G_n = \{(x_1, \ldots, x_n) \mid x_i \in G_i\}$ mit $(x_1, \ldots, x_n) \circ (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$ eine Gruppe, das *direkte Produkt* der G_i.

BEWEIS: $(1, \ldots, 1)$ ist Einselement, $(x_1^{-1}, \ldots, x_n^{-1})$ ist das Inverse zu $(x_1, \ldots, x_n)$.
BEISPIEL: $n = 2,\ G_1 = \{1, a\},\ G_2 = \{1', b\} \Rightarrow G_1 \times G_2 =: V_4$ Vierergruppe mit Elementen $(1, , 1'), (1, b), (a, 1'), (a, b)$.

1.1 Operationen von Gruppen (auf Mengen)

1.1.1 G-Menge

Sei G eine Gruppe und Ω eine Menge.

DEFINITION: Wir nennen Ω eine *G-Menge*, wenn eine Verknüpfung $(\Omega, G) \to \Omega;\ (\alpha, g) \mapsto \alpha^g$ definiert ist mit

1. $\alpha^1 = \alpha$ für alle $\alpha \in \Omega$.
2. $\alpha^{gh} = (\alpha^g)^h$ für alle $\alpha \in \Omega, g, h \in G$.

Wir sagen „G *operiert auf* Ω“, wenn Ω eine G-Menge ist.

BEMERKUNG: Ist Ω eine G-Menge und $H \leq G$, so ist Ω auch eine H-Menge.

BEISPIEL: Sei $\Omega = \{1, \ldots, n\}$ und $G \leq S_n$ und für $\alpha \in \Omega, g \in G$ sei α^g der Punkt aus Ω, auf den die Permutation g den Punkt α abbildet. Das ist eine G-Menge: Verknüpfung ist klar. $1 = \mathrm{id}$, also ist (1) erfüllt, (2) gilt nach Definition des Produktes zweier Permutationen.

SATZ:

1. Sei Ω eine G-Menge. Für $g \in G$ sei $\sigma_g : \Omega \to \Omega, \alpha \to \alpha^g$. Dann ist σ_g eine Permutation auf Ω und die Abbildung $\sigma : G \to \mathrm{Sym}\Omega,\ g \to \sigma_g$ ist ein Homomorphismus mit $\mathrm{Kern}\,\sigma = \{g \in G \mid \alpha^g = \alpha \text{ für alle } \alpha \in \Omega\} =: \mathrm{Kern}(\Omega, G)$
2. Sei umgekehrt Ω eine Menge und $\sigma : G \to \mathrm{Sym}\,\Omega$ ein Homomorphismus. Dann ist Ω mit der Verknüpfung $(\Omega, G) \to \Omega,\ (\alpha, g) \mapsto \alpha^{g^\sigma}$ eine G-Menge.

BEMERKUNG: $\mathrm{Kern}(\Omega, G)$ heißt *Kern* der G-Menge und der Homomorphiesatz (1.0.7) besagt: $\mathrm{Kern}(\Omega, G) \trianglelefteq G$ und $G/\mathrm{Kern}(\Omega, G) \simeq G^\sigma \leq \mathrm{Sym}\,\Omega$.

BEWEIS: Triviale Rechnung.

1. $\sigma_g : \Omega \to \Omega$ ist offenbar wohldefiniert. Zur Injektivität:

$$\begin{aligned} \alpha^{\sigma_g} = \beta^{\sigma_g} &\overset{Def.\sigma_g}{\Rightarrow} \alpha^g = \beta^g \\ &\Rightarrow \quad \alpha \overset{(1)}{=} \alpha^1 = \alpha^{gg^{-1}} \overset{(2)}{=} (\alpha^g)^{g^{-1}} = (\beta^g)^{g^{-1}} = \beta \end{aligned}$$

   Zur Surjektivität: Sei $\beta \in \Omega$. Sei $\alpha := \beta^{g^{-1}} \in \Omega$. Dann ist $\alpha^{\sigma_g} = \alpha^g = (\beta^{g^{-1}})^g = \beta$. Also $\sigma_g \in \operatorname{Sym}\Omega$. Somit $\sigma : G \to \operatorname{Sym}\Omega$ wohldefiniert. Seien $g, h \in G, \alpha \in \Omega$.

$$\begin{aligned} \alpha^{\sigma_{gh}} &= \alpha^{gh} \overset{(2)}{=} (\alpha^g)^h = (\alpha^{\sigma_g})^{\sigma_h} \overset{\circ \text{ in Sym}}{=} \alpha^{\sigma_g \cdot \sigma_h} \\ &\Rightarrow \quad \sigma_{gh} = \sigma_g \cdot \sigma_h \end{aligned}$$

   Also σ Homomorphismus. Weiter gilt:

$$g \in \operatorname{Kern}\sigma \Leftrightarrow \sigma_g = \mathrm{id} \Leftrightarrow \alpha = \alpha^{\sigma_g} = \alpha^g \text{ für alle } \alpha \in \Omega$$

2. Die Verknüpfung ist klar. Beweis der Eigenschaften:

   (a) $\alpha^1 = \alpha^{1^\sigma} \overset{\sigma Hom.}{=} \alpha^{\mathrm{id}} = \alpha$

   (b) $\alpha^{gh} = \alpha^{(gh)^\sigma} \overset{\sigma Hom.}{=} \alpha^{g^\sigma h^\sigma} = \left(\alpha^{g^\sigma}\right)^{h^\sigma} = (\alpha^g)^h$

1.1.2 Beispiel: Galoisgruppe

Seien $K \leq L$ Körper und $G = \mathrm{Gal}(L/K)$.

1. $\Omega = L$. Für $\alpha \in \Omega, g \in G$ sei α^g das Bild von α unter dem Automorphismus $g \in G$. Das ist eine G-Menge, da Multiplikation von Automorphismen Hintereinanderausführung ist.

2. $f \in K[x]$, $\Omega = \{\alpha \in L \mid f(\alpha) = 0\}$, Verknüpfung [2] wie oben ist auch eine G-Menge.

1.1.3 Beispiel: Konjugation

Sei G eine Gruppe.

1. $\Omega = G$ mit $(\alpha, g) \mapsto \alpha^g := g^{-1}\alpha g$ (Konjugierte von α) ist G-Menge. *Beweis:* Verknüpfung ist klar, $\alpha^1 = 1^{-1}\alpha 1 = \alpha$, $\alpha^{gh} = (\alpha^g)^h$ laut (1.0.6).

2. $\Omega = \mathfrak{V}(G)$, $(U, g) \mapsto U^g = \{x^g \mid x \in U\} \leq G$ (da $\sigma_g : G \to G, x \mapsto x^g$ Automorphismus) ist G-Menge, d.h. G operiert auf $\mathfrak{V}(G)$ durch Konjugation.

3. $H \leq G$, $\Omega = \{H^x \mid x \in G\}$, $(H^x, g) \mapsto (H^x)^g = H^{xg}$.

[2] Verknüpfung ist wohldefiniert wegen (I.7.3(c)) - siehe Script Algebra 1 WS 2002/03.

1.1.4 Beispiel: Rechtsmultiplikation

Sei G eine Gruppe.

1. $\Omega = G,\ (\alpha, g) \mapsto \alpha \cdot g$ ist eine G-Menge, d.h. G operiert auf sich durch Rechtsmultiplikation.

   Beweis: Verknüpfung ist trivial, $\alpha^1 = \alpha,\ \alpha(gh) = (\alpha g)h$ - Assoziativgesetz.

2. Sei $H \leq G$, dann ist $\Omega = \{\, Hx \mid x \in G\}\,,\ (V, g) \mapsto Vg$ eine G-Menge.

   Beweis: $V = Hx \Rightarrow Vg = (Hx)g \overset{(1.0.5)}{=} H(xg) \in \Omega$. Weiter ist $(Hx)(gh) \overset{(1.0.5)}{=} ((Hx)g)h$.

   Bemerkung: (1) ist Spezialfall $H = 1$ von (2).

Bemerkung: Linksmultiplikation statt Rechtsmultiplikation geht nicht.

1.1.5 Stabilisator und Bahn

Sei Ω eine G-Menge und $\alpha \in \Omega$.

Definitionen:

1. $G_\alpha := \{\, g \in G \mid \alpha^g = \alpha\}$, *Stabilisator* von α in G.
2. $\alpha^G := \{\, \alpha^g \mid g \in G\}$, *Bahn* von α unter G.

Lemma:

1. $G_\alpha \leq G$
2. $\mathrm{Kern}(\Omega, G) = \bigcap_{\alpha \in \Omega} G_\alpha \trianglelefteq G$

Beweis:

1. $1 \in G_\alpha$ nach (1). Für $g, h \in G_\alpha$ ist $\alpha^g = \alpha = \alpha^h$, damit

   $$\alpha^{gh} \overset{(2)}{=} (\alpha^g)^h = \alpha^h = \alpha \Rightarrow gh \in G_\alpha; \quad \alpha^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha \Rightarrow g^{-1} \in G_\alpha$$

2. Gleichheit folgt aus den Definitionen. Für $x \in \mathrm{Kern}, g \in G, \alpha \in \Omega$ ist

   $$\alpha^{g^{-1}xg} \overset{(2)}{=} \left(\left(\alpha^{g^{-1}}\right)^x\right)^g \overset{x \in \mathrm{Kern}}{=} \left(\alpha^{g^{-1}}\right)^g = \alpha \Rightarrow g^{-1}xg \in \mathrm{Kern} \Rightarrow \mathrm{Kern} \trianglelefteq G$$

1.1.6 Hauptsatz über G-Mengen

Sei Ω eine G-Menge.

1. Die Bahnen von G auf Ω bilden eine Partition von Ω, d.h. jedes $\alpha \in \Omega$ liegt in genau einer Bahn von G auf Ω.

2. Sei $\alpha \in \Omega$ und $\mathfrak{R}_\alpha$ die Menge der Rechtsrestklassen von G_α in G. Die Abbildung $\varphi_\alpha : \alpha^G \to \mathfrak{R}_\alpha,\ \alpha^g \mapsto G_\alpha \cdot g$ ist bijektiv. Somit $\left|\alpha^G\right| = |G : G_\alpha|$. Ist G endlich, so folgt: $|G| = |G_\alpha| \cdot \left|\alpha^G\right|$.

3. Ist Ω endlich und sind $\Delta_1, \ldots, \Delta_r$ die Bahnen von G auf Ω und sind $\alpha_i \in \Delta_i,\ (i = 1, \ldots, r)$, d.h. $\Delta_i = \alpha_i^G$, so gilt

$$|\Omega| = \sum_{i=1}^{r} |\Delta_i| = \sum_{i=1}^{r} |G : G_{\alpha_i}|$$

BEWEIS:

1. $\alpha \in \alpha^G$ (wegen (1) aus (1.1.1)), daraus folgt: $\Omega = \bigcup_{\alpha\in\Omega} \alpha^G$. Zu zeigen: falls $\gamma \in \alpha^G \cap \beta^G$ so ist $\alpha^G = \beta^G$. *Beweis:* Da $\gamma \in \alpha^G \cap \beta^G$, existieren $x, y \in G$ mit $\gamma = \alpha^x = \beta^y$. Also $\beta^{yx^{-1}} = (\beta^y)^{x^{-1}} = (\alpha^x)^{x^{-1}} = \alpha$. Ist $\delta \in \alpha^G$, so existiert $g \in G$ mit $\delta = \alpha^g$, also $\delta = \alpha^g = (\beta^{yx^{-1}})^g = \beta^{yx^{-1}g} \in \beta^G \Rightarrow \alpha^G \subseteq \beta^G$. Genauso $\beta^G \subseteq \alpha^G$, also $\alpha^G = \beta^G$.

   Andere Beweismöglichkeit: definiere

$$\alpha \sim \beta \Leftrightarrow \exists g \in G \text{ mit } \alpha^g = \beta$$

   Zeige: $\sim$ ist Äquivalenzrelation und zugehörige Klassen sind die Bahnen.

2. Für $\alpha \in \Omega$ und $g, h \in G$ gilt:

$$\begin{aligned} \alpha^g = \alpha^h \quad &\Longleftrightarrow \quad \alpha^{gh^{-1}} = (\alpha^g)^{h^{-1}} = (\alpha^h)^{h^{-1}} = \alpha^{hh^{-1}} = \alpha \\ &\overset{Def.(1.1.5)}{\Longleftrightarrow} \quad gh^{-1} \in G_\alpha \\ &\overset{Def.(1.0.3)}{\Longleftrightarrow} \quad G_\alpha \cdot g = G_\alpha \cdot h \end{aligned}$$

   Von links nach rechts gelesen: φ_α ist wohldefiniert, von rechts nach links: φ_α ist injektiv. Offensichtlich ist φ_α surjektiv (da $(G_\alpha \cdot g) = (\alpha^g)^{\varphi_\alpha}$). Der Satz von Lagrange besagt:

$$|G| = |G_\alpha| \cdot |G : G_\alpha| = |G_\alpha| \cdot |\alpha^G|$$

3. Folgt aus (a) und (b), wenn man beachtet, dass für $\alpha_i \in \Delta_i = \beta^G$ gilt: $\alpha_i \in \alpha_i^G \cap \beta^G$, also $\alpha_i^G = \beta^G = \Delta_i$ (siehe Beweis zu (a)).

BEISPIELE:

1. Für $\Omega = \{1, \ldots, n\},\ G = S_n,\ \alpha = n$ ist $G_\alpha = \{g \in S_n \mid n^g = n\} \simeq S_{n-1}$ und $\alpha^G = \Omega$, d.h.

$$n = |\alpha^G| = |G : G_\alpha| = |S_n : S_{n-1}|$$

   Daraus ergibt sich insbesondere die Formel $|S_n| = n!$.

2. Sei $K \leq L, G = \mathrm{Gal}(L, K)$.

   (a) Für $\Omega = L, \alpha \in L$ ist $G_\alpha = \{\alpha\}\mathfrak{G} \leq G$.

   (b) Für $f \in K[x], \Omega = \{\alpha \in L \mid f(\alpha) = 0\}$ ist $\mathrm{Kern}(\Omega, G) = \Omega\mathfrak{G} \trianglelefteq G$ [3]

1.1.7 Zentralisator, Normalisator, Zentrum, Klassengleichung

Sei G eine Gruppe.

1 Betrachte Beispiel (1.1.3(a)): Sei $\Omega = G$ mit $(x, g) \mapsto x^g = g^{-1}xg$.

DEFINITIONEN:

(a) $G_x = \{g \in G \mid g^{-1}xg = x\} = \{g \in G \mid xg = gx\} = C_G(x) \leq G$ heißt *Zentralisator* von x in G.

(b) $x^G = \{x^g \mid g \in G\}$ heißt *Konjugiertenklasse* von x in G.

(c) $\mathrm{Kern}(\Omega, G) = \{g \in G \mid x^g = x \text{ für alle } x \in G\} = \bigcap_{x \in G} C_G(x) = Z(G) \trianglelefteq G$ heißt *Zentrum* von G.

BEMERKUNG: Nach (1.1.6) ist $|x^G| = |G : C_G(x)|$.

SATZ: Sei G eine endliche Gruppe. Sind $K_1, \ldots, K_n$ die Konjugiertenklassen von G und ist $x_i \in K_i$, so ist $|K_i| = |G : C_G(x_i)|$ und

$$|G| = \sum_{i=1}^{r} |K_i| = |Z(G)| + \sum_{\substack{i=1 \\ x_i \notin Z(G)}}^{r} |G : C_G(x_i)| \quad \text{(Klassengleichung)}$$

[3] Vergleiche I, 10.9: $K(\Omega)$ ist normal über K, also $\Omega\mathfrak{G} = K(\Omega)\mathfrak{G} \trianglelefteq G$. Hier allerdings haben wir nicht vorausgesetzt, dass L galoissch über K ist.

BEWEIS: Es gilt

$$\begin{aligned} K_i = \{x_i\} &\Leftrightarrow 1 = |K_i| = |G_i : C_G(x_i)| \Leftrightarrow C_G(x_i) = G \\ &\Leftrightarrow x_i g = g x_i \text{ für alle } g \in G \Leftrightarrow x_i \in Z(G) \end{aligned}$$

2 Betrachte Beispiel (1.1.3(b)): Sei $\Omega = \mathfrak{V}(G)$ mit $(U, g) \mapsto U^g$.

DEFINITIONEN:

(a) $G_U = \{g \in G \mid U^g = U\} := N_G(U)$ heißt *Normalisator* von U in G. $N_G(U)$ ist nach (1.1.5) eine Untergruppe von G, die U enthält.

(b) $U^G = \{U^g \mid g \in G\}$ heißt *Konjugiertenklasse* von U unter G.

(c) $\text{Kern}(\Omega, G) = \{g \in G \mid U^g = U \text{ für alle } U \leq G\} = \bigcap_{U \leq G} N_G(U)$ heißt *Kern* oder *Norm* von G.

BEMERKUNG: Nach (1.1.6) ist $|\{U^g \mid g \in G\}| = |G : N_G(U)|$.

1.1.8 Anwendung auf p-Gruppen

Sei p eine Primzahl.

DEFINITION: G heißt *p-Gruppe* genau dann, wenn $|G| = p^n$ für $n \in \mathbb{N}_0$.

LEMMA: Sei G eine p-Gruppe. Ist Ω eine G-Menge und $\Omega_0 := \{\alpha \in \Omega \mid \alpha^g = \alpha \text{ für alle } g \in G\}$ Menge der Fixpunkte unter G, so ist $|\Omega| \equiv |\Omega_0| \mod p$ (d.h. $p \mid |\Omega| - |\Omega_0|$). Ist insbesondere $p \nmid |\Omega|$, so ist $\Omega_0 \neq \emptyset$.

BEWEIS: Nach Hauptsatz (1.1.6) ist $|\Omega| = \sum_{i=1}^{r} |G : G_{\alpha_i}|$ mit gewissen $\alpha_i \in \Omega$. Offenbar gilt:

$$|G : G_{\alpha_i}| = 1 \Leftrightarrow G_{\alpha_i} = G \Leftrightarrow \alpha_i \in \Omega_0$$

also

$$|\Omega| = |\Omega_0| + \sum_{\substack{i=1 \\ G_{\alpha_i} < G}}^{r} |G : G_{\alpha_i}|$$

Nach Lagrange ist $p \mid |G : G_{\alpha_i}|$, falls $G_{\alpha_i} < G$, also $p \mid \sum \ldots = |\Omega| - |\Omega_0|$. Insbesondere falls $p \nmid |\Omega|$, so ist

$$|\Omega| = |\Omega_0| + (|\Omega| - |\Omega_0|) \Rightarrow p \nmid |\Omega_0|$$

SATZ: Ist G eine p-Gruppe und $N \trianglelefteq G$ mit $N \neq 1$, so ist $N \cap Z(G) > 1$ [4]. Insbesondere, ist G eine p-Gruppe und $G \neq 1$, so ist $Z(G) \neq 1$.

BEWEIS: Sei $\Omega = N \setminus \{1\}$ mit $(\Omega, G) \to \Omega, x \mapsto x^g = g^{-1}xg$. Da $N \trianglelefteq G$, ist $N^g = N$ und $1^g = 1$, also ist Ω eine G-Menge. Es gilt $|N| = p^s$ für $s \geq 1$, daraus folgt $|\Omega| = p^s - 1$, also $p \nmid |\Omega|$. Nach Lemma existiert $x \in \Omega_0$, d.h. $x \in Z(G) \cap N$ mit $x \neq 1$. Setzt man $N = G$, so folgt: $Z(G) \neq 1$.

BEMERKUNG: $Z(G) \neq 1$ folgt auch sofort aus der Klassengleichung: $p \mid |Z(G)|$, wegen $1 \in Z(G)$ folgt $|Z(G)| \geq p$.

FOLGERUNG:

1. Ist $|G| = p$, so ist G zyklisch.
2. Ist $|G| = p^2$, so ist G abelsch.

BEWEIS:

1. Sei $1 \neq a \in G$, dann ist $1 \neq \langle a \rangle \leq G$, daraus folgt mit Lagrange: $|\langle a \rangle| = p$, d.h. $G = \langle a \rangle$.
2. Nach Satz ist $1 < Z(G) \leq G$, daraus folgt: $|Z(G)|$ teilt $|G| = p^2$. Ist $|Z(G)| = p^2$, so ist $G = Z(G)$, also G abelsch. Angenommen $|Z(G)| = p$. Sei dann $a \in G \setminus Z(G)$. Betrachte $C_G(a) \leq G$. Es gilt $Z(G) \leq C_G(a)$ und $a \in C_G(a)$. Also $Z(G) < C_G(a) \leq G$, mit $|G| = p^2$ folgt: $C_G(a) = G$, somit $a \in Z(G)$, Widerspruch.

1.1.9 Anwendung der Rechtsmultiplikation

Sei $H \leq G$, $\Omega = \{ Hx \mid x \in G \}$ mit $(Hx, g) \mapsto Hxg$.

LEMMA:

1. Der Stabilisator von Hx in G ist H^x.
2. Die Bahn von Hx ist Ω.

BEWEIS:

1. Es gilt

$$g \in G_{Hx} \Leftrightarrow Hx = Hxg \overset{(1.0.3)}{\Leftrightarrow} xgx^{-1} \in H \Leftrightarrow g \in H^x$$

2. Für $Hy \in \Omega$ ist $Hx(x^{-1}y) = Hy$.

DEFINITION: $\operatorname{Kern}(\Omega, G) = \bigcap_{x \in G} H^x = H_G \trianglelefteq G$ heißt das *Herz* von H in G.

SATZ: Ist $H \leq G$ mit $|G : H| = n \in \mathbb{N}$, so ist G/H_G isomorph zu einer Untergruppe der symmetrischen Gruppe S_n. Insbesondere ist $|G/H_G|$ ein Teiler von $n!$

BEWEIS: Betrachte die G-Menge $\Omega = \{Hx \mid x \in G\}$ mit Rechtsmultiplikation. Dann ist $|\Omega| = n$. Satz (1.1.1) besagt: $\sigma : G \to \operatorname{Sym} \Omega$ ist Homomorphismus mit $\operatorname{Kern} \sigma = \operatorname{Kern}(\Omega, G) = H_G$. Homomorphiesatz liefert: $G/H_G = G/\operatorname{Kern} \sigma \simeq G^\sigma \leq \operatorname{Sym} \Omega \simeq S_n$.

FOLGERUNG:

1. Ist $H \leq G$ mit $|G : H| < \infty$, so existiert ein in H enthaltener Normalteiler von endlichem Index in G (nämlich H_G)

2. Ist G endlich und $H \leq G$ mit $|G : H| = p$, wobei p der kleinste Primteiler von $|G|$ ist, so ist $H \trianglelefteq G$.

BEWEIS von (2): Ist $V \leq U \leq G$, so ist

$$|G : V| \cdot |V| = |G| = |G : U| \cdot |U| = |G : U| \cdot |U : V| \cdot |V|$$

Also $|G : V| = |G : U| \cdot |U : V|$. Somit $|G : H_G| = |G : H| \cdot |H : H_G| = p \cdot |H : H_G|$ teilt $p!$ (nach Satz), also $|H : H_G|$ teilt $(p-1)!$. Jeder Primteiler q von $|H : H_G|$ teilt $|G|$, ist also größer gleich p, kann also $(p-1)!$ nicht teilen. Also existiert kein solches q, d.h. $|H : H_G| = 1$. Damit ist $H = H_G \trianglelefteq G$.

1.1.10 Satz von CAYLEY

Jede Gruppe G ist isomorph zu einer Untergruppe von $\operatorname{Sym} G$. Falls $|G| = n$, so ist $G \simeq S \leq S_n$. Insbesondere ist G isomorph zu einer Untergruppe von $\operatorname{Sym} \mathbb{N}$.

BEWEIS: Setze $H = 1$ im Satz (1.1.9) (für endliche Gruppen). Für unendliche Gruppen betrachte $\Omega = G$ mit Rechtsmultiplikation. Offenbar $\operatorname{Kern}(\Omega, G) = 1$. Satz (1.1.1) liefert: $G/\operatorname{Kern}(\Omega, G) \simeq S \leq \operatorname{Sym} \Omega = \operatorname{Sym} G$.

1.2 Die Sylowschen Sätze

1.2.1 Untergruppen der Ordnung p^α

SATZ: Sei $|G| = p^\alpha \cdot n$, wobei p Primzahl, $\alpha \in \mathbb{N}_0$ und $n \in \mathbb{N}$ (p und n nicht notwendig teilerfremd) und sei $A_G(p^\alpha)$ die Anzahl der Untergruppen der Ordnung p^α von G. Dann gilt: $A_G(p^\alpha) \equiv 1 \mod p$, insbesondere $A_G(p^\alpha) \neq 0$.

BEWEIS: (von Wielandt 1959).

1. Sei $\Omega = \{M \subseteq G \mid |M| = p^\alpha\}$ mit $(M, g) \mapsto Mg$. Dies ist eine G-Menge, da aus $|M| = p^\alpha$ folgt $|Mg| = |\{mg \mid m \in M\}| = p^\alpha$, d.h. Rechtsmultiplikation ist Verknüpfung auf Ω. Es gilt $|\Omega| = \binom{p^\alpha n}{p^\alpha} =: N(p^\alpha, n)$.

2. Sei Δ eine Bahn von G auf Ω, $M \in \Delta$ und $U = G_M$ der Stabilisator von M in G. Dann ist $U = \{g \in G \mid Mg = M\}$, d.h. für alle $m \in M$ und $u \in U$ ist $m \cdot u \in M$, also $mU \subseteq M$. Somit ist M Vereinigung von Linksnebenklassen von U. Da Linksnebenklassen (zur Gruppe U) disjunkt sind, so existiert $k \in \mathbb{N}$ mit $M = \bigcup_{i=1}^{k} m_i U$ und $|M| = k \cdot |U|$. Insbesondere ist $|U|$ ein Teiler von $|M| = p^\alpha$.

3. Es gilt
$$|\Delta| \overset{(1.1.6b)}{=} |G : U| = \frac{|G|}{|U|} = \frac{p^\alpha n}{|U|}$$
Somit ist $|U| = p^\alpha$ genau dann, wenn $|\Delta| = n$. Weiter ist $U < p^\alpha$ genau dann, wenn $|\Delta| \equiv 0 \mod pn$.

4. *Behauptung:* Die Bahnen der Länge n sind genau die Mengen $\{Vg \mid g \in G\}$ für $V \leq G$ mit $|V| = p^\alpha$.

   Beweis: Ist $|V| = p^\alpha$, so ist $B := \{Vg \mid g \in G\} \subseteq \Omega$ und B ist natürlich eine Bahn von G auf Ω. Ferner
$$|B| \overset{Def.1.0.3}{=} |G : V| = \frac{|G|}{|V|} = \frac{p^\alpha n}{p^\alpha} = n$$
   Sei umgekehrt Δ eine Bahn der Länge n und seien M und $U = G_m$ wie in (2). Es ist $|U| = p^\alpha$, somit ist in (2) $k = 1$, d.h. $M = mU$ mit $m \in M$. Mit M liegt auch $Mm^{-1} = mUm^{-1} = U^{m^{-1}} := V$ in Δ. Ferner ist $Vg \in \Delta$ für alle $g \in G$. Damit $B := \{Vg \mid g \in G\} \subseteq \Delta$. Da $|B| = |G : V| = n$, so ist $B = \Delta$.

5. Die Anzahl der Bahnen der Länge n ist laut (4) $A_G(p^\alpha)$ (jede Bahn enthält genau eine Untergruppe der Ordnung p^α und jede Untergruppe liefert genau eine Bahn). Hauptsatz (1.1.6) besagt: Seien $\Delta_1, \ldots, \Delta_r$ die Bahnen von G auf Ω, dann ist

$$N(p^\alpha, n) = |\Omega| = \sum_{i=1}^{r} |\Delta_i| = \sum_{|\Delta_i|=n} |\Delta_i| + \sum_{|\Delta_i|\neq n} |\Delta_i| \overset{(3)}{\equiv} A_G(p^\alpha) \cdot n \mod pn$$

6. Wende (5) auf die zyklische Gruppe G der Ordnung $p^\alpha n$ an. Dann folgt $N(p^\alpha, n) \equiv 1 \cdot n \mod pn$. Nun setze (7) in (6) (für unsere beliebige Gruppe) ein:

$$n \equiv N(p^\alpha, n) \equiv A_G(p^\alpha) n \mod pn$$

also $pn \mid n(A_G(p^\alpha) - 1)$, daraus folgt: $A_G(p^\alpha) \equiv 1 \mod p$.

1.2.2 p-Sylowuntergruppen

Sei $p \in \mathbb{P}$, G eine endliche Gruppe, $|G| = p^\alpha n$ mit $(p, n) = 1$.

DEFINITION: Eine *p-Sylowuntergruppe* von G ist eine Untergruppe der Ordnung p^α von G. Die Menge aller p-Sylowuntergruppen wird mit $\mathrm{Syl}_p(G)$ bezeichnet.

SATZ: Ist P eine p-Untergruppe und S eine p-Sylowuntergruppe von G, so existiert ein $x \in G$ mit $P \leq S^x$ (oder $P^{x^{-1}} \leq S$)

BEWEIS: $\Omega = \{ Sx \mid x \in G \}$ mit Rechtsmultiplikation ist nach (1.1.4) eine G-Menge, also auch eine P-Menge (nach Bemerkung (1.1.1)). Es gilt

$$|\Omega| \overset{Def.}{=} |G : S| = \frac{|G|}{|S|} = \frac{p^\alpha n}{p^\alpha} = n \not\equiv 0 \mod p$$

Mit Lemma (1.1.8) folgt daraus: es existiert ein Fixpunkt Sx von P auf Ω, also $P \leq G_{Sx} \overset{1.1.9(1)}{=} S^x$.

1.2.3 Hauptsatz

Sei G eine endliche Gruppe und p eine Primzahl.

SATZ VON SYLOW (1872):

1. Zu jeder p-Untergruppe P von G existiert eine p-Sylowuntergruppe S von G mit $P \leq S$. Insbesondere (mit $P = 1$) existieren p-Sylowuntergruppen.
2. Je zwei p-Sylowgruppen sind konjugiert.
3. $|\mathrm{Syl}_p(G)| = |G : N_G(S)| \equiv 1 \mod p$ für $S \in \mathrm{Syl}_p(G)$.

BEWEIS:

1. Nach Satz (1.2.1) existiert eine p-Sylowgruppe T. Nach Satz (1.2.2) existiert $x \in G$ mit $P \leq S = T^x$ und $S \in \mathrm{Syl}_p(G)$, da $|S| = |T|$.
2. Seien $S, T \in \mathrm{Syl}_p(G)$. Satz (1.2.2) mit $T = P$ liefert: es existiert $x \in G$ mit $T \leq S^x$. Da $|T| = |S| = |S^x|$, folgt: $T = S^x$.
3. Nach (2) ist

$$|\mathrm{Syl}_p(G)| = |\{S^x \mid x \in G\}| \overset{1.1.7(2)}{=} |G : N_G(S)|$$

Nach (1.2.1) ist

$$|\mathrm{Syl}_p(G)| = |A_G(p^\alpha)| \equiv 1 \mod p$$

1.2.4 Gruppen der Ordnung pq

SATZ: Ist $|G| = pq$ für Primzahlen p, q mit $p > q$, so hat G eine normale p-Sylowgruppe. Ist G nicht zyklisch, so ist $q \mid p - 1$ und G hat genau p q-Sylowgruppen.

BEWEIS: Sei $P \in \mathrm{Syl}_p(G)$. Dann ist $|P| = p$ und nach (3) aus (1.2.3) gilt: $|\mathrm{Syl}_p(G)|$ teilt $|G : P| = q$, also ist $|\mathrm{Syl}_p(G)| = 1$ oder q. Da $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$, folgt: $|\mathrm{Syl}_p(G)| = 1$. Also ist P die einzige p-Sylowgruppe, damit $P \trianglelefteq G$.

Hat G nur eine q-Sylowgruppe Q, so sind nach Lagrange $1, P, Q, G$ die einzigen Untergruppen von G. Da $P \cup Q$ nur $p = q - 1 < pq$ Elemente enthält, existiert $g \in G$ mit $g \notin P \cup Q$, also ist $\langle g \rangle = G$, d.h. G ist zyklisch. Ist also G nicht zyklisch, so enthält G mehr als eine q-Sylowgruppe, also (da $|G : Q| = p$) gibt es p q-Sylowuntergruppen. Nach (3) aus (1.2.3) ist $p \equiv 1 \mod q$.

FOLGERUNGEN:

1. Der Untergruppenverband von G besteht aus $1, P, Q, G$ oder aus $1, P$, p Untergruppen der Ordnung q und G.

2. Die Untergruppen der Ordnung $15, 33, 35, \ldots$ (mit $q \nmid p-1$) sind immer zyklisch.

3. Die einzigen Gruppen der Ordnung 6 sind Z_6 und S_3.

   Beweis: ist $|G| = 6$, G nicht zyklisch, so ist $|\mathrm{Syl}_2(G)| = 3$, also $\Omega = \mathrm{Syl}_2(G)$ mit Konjugation ist eine G-Menge. Es gilt nach Satz (1.1.9): $G = G/Q_G \simeq G_0 \leq S_3$ für $Q \in \mathrm{Syl}_2(G)$. Da $|G| = |G_0| = 6 = |S_3|$, folgt $G \simeq S_3$.

BEMERKUNG: (ohne Beweis) Für $q \mid p-1$ gibt es (bis auf Isomorphie) genau eine nichtzyklische Gruppe der Ordnung pq.

1.2.5 Beispiele: A_4 und S_4

SATZ:

1. Die S_4 hat 4 3-Sylowuntergruppen und 3 2-Sylowuntergruppen.

2. $G = A_4$ enthält die 4 3-Sylowgruppen aus der S_4, eine 2-Sylowgruppe und keine Untergruppe der Ordnung 6.

BEWEIS:

1. $|S_4| = 24 = 2^3 \cdot 3$. Ist $S \in \mathrm{Syl}_3(G)$ so ist $|S| = 3$ und $|G : S| = 8$. Mit (1.2.3(3)) folgt: $|\mathrm{Syl}_3(G)| \in \{1, 2, 4, 8\}$. Da $|\mathrm{Syl}_3(G)| \equiv 1 \mod 3$ sein muss, können wir 2 und 8 ausschließen. Es gibt also 4 solche Untergruppen, nämlich 1, $\langle(123)\rangle, \langle(124)\rangle$ und $\langle(234)\rangle$.

   Ist nun $T \in \mathrm{Syl}_2(G)$, so ist $|T| = 8$ und $|G : T| = 3$. Daraus folgt: $|\mathrm{Syl}_2(G)| = 1$ oder 3. Alle 12 Transpositionen können nicht in einer 2-Sylowgruppe der Ordnung 8 liegen, also gibt es 3 solche Sylowgruppen.

2. $G = A_4$ enthält die 4 3-Sylowgruppen aus der S_4. Diese 4 Untergruppen der Ordnung 3 enthalten $4 \cdot (3-1) = 8$ Elemente ungleich 1. Es bleiben 4 Elemente in G, die dann nach (1.2.3(1)) die 2-Sylowuntergruppe von G bilden. Das sind die Elemente $\{1, (12)(34), (13)(24), (14)(23)\}$. Diese Elemente bilden die sog. *Kleinsche Vierergruppe*. Gäbe es eine Untergruppe $H \leq A_4$ mit $|H| = 6$, so folgte $H \trianglelefteq A_4$ und H enthielte eine und nach (1.2.3(2)) alle 4 3-Sylowuntergruppen der A_4. Damit enthielte H 8 Elemente, Widerspruch.

SATZ: Ist $|G| = 12$ und hat G mehr als eine 3-Sylowgruppe, so ist $G \simeq A_4$.

BEWEIS: Für $S \in \mathrm{Syl}_2(G)$ ist $|G : S| = 4$. Da es mehrere 3-Sylowgruppen gibt, ist nach Satz (1.1.9) $G = G/S_G$. Weiter ist nach Satz (1.1.9) G/S_G isomorph zu einer Untergruppe von S_4. Da S_4 nur eine Untergruppe der Ordnung 12 hat, folgt: $G \simeq A_4$.

Zur Eindeutigkeit von A_4: ist $A_4 \neq H \leq S_4$ mit $|H| = 12$, so ist nach Aufgabe 1 $A_4 H = S_4$. Nach Aufgabe 2 folgt:

$$24 = \frac{|A_4| \cdot |H|}{|A_4 \cap H|} = \frac{12 \cdot 12}{|A_4 \cap H|} \Rightarrow |A_4 \cap H| = 6$$

Wie oben gesehen, gibt es aber keine Untergruppe der Ordnung 6 in A_4.

1.2.6 Normaleigenschaften der Sylowgruppen

SATZ: Sei G eine Gruppe und $S \leq \mathrm{Syl}_p(G)$. Dann sind äquivalent:

1. $S \trianglelefteq G$.
2. S ist die einzige p-Sylowgruppe von G.
3. Jede p-Untergruppe von G ist in S enthalten

BEWEIS:

(a) $\Rightarrow$ (b) Ist $T \in \mathrm{Syl}_p(G)$, so existiert nach (1.2.3(2)) $x \in G$ mit $T = S^x = S$.

(b) $\Rightarrow$ (c) Ist P eine p-Untergruppe von G, so folgt mit (1.2.3(1)): $P \leq S$.

(c) $\Rightarrow$ (a) Sei $x \in G$. Dann ist $|S^x| = |S|$, also S^x eine p-Untergruppe von G. Mit Voraussetzung gilt $S^x \leq S$, somit $S^x = S$, d.h. $S \trianglelefteq G$.

1.2.7 Gruppe der Ordnung p^3q

SATZ: Sei $|G| = p^3q$ mit Primzahlen p und q. Hat G mehr als eine p-Sylowgruppe und mehr als eine q-Sylowgruppe, so ist $p = 2, q = 3$, also $|G| = 24$ und $G \simeq S_4$.

BEWEIS: Es folgt sofort $p \neq q$. Ist $P \in \mathrm{Syl}_p(G)$, so ist $|G : P| = q$, also hat G eine oder q p-Sylowgruppen, mit Voraussetzung q. Somit $q = |\mathrm{Syl}_p(G)| \equiv 1 \mod p$. Daraus folgt: $p < q$.

Sei $Q \in \mathrm{Syl}_q(G)$, dann ist $|Q| = q$ und $|\mathrm{Syl}_q(G)| \in \{1, p, p^2, p^3\}$. 1 geht

nach Voraussetzung nicht. Da $|\mathrm{Syl}_q(G)| \equiv 1 \mod q$ und $p < q$, so folgt: $|\mathrm{Syl}_q(G)| \neq p$. Angenommen $|\mathrm{Syl}_q(G)| = p^3$. Die p^3 q-Sylowgruppen enthalten $p^3(q-1) = p^3q - p^3 = |G| - p^3$ q-Elemente ungleich 1. Die übrigen p^3 Elemente bilden dann die einzige p-Sylowgruppe von G, Widerspruch. Also $|\mathrm{Syl}_q(G)| = p^2 \equiv 1 \mod q$, also $q \mid p^2 - 1 = (p+1)(p-1)$. Da $q > p$, folgt: $q = p + 1$. Dann ist $p = 2$ und $q = 3$, also $|G| = 24$.

Sei $\Omega = \mathrm{Syl}_3(G)$. Dann ist $|\Omega| = 4$. G operiert durch Konjugation auf Ω. Sei $K = \mathrm{Kern}(\Omega, G) = \bigcap_{Q \in \Omega} N_G(Q)$. Da $|G : N_G(Q)| \overset{(1.1.6)}{=} |Q^G| \overset{(1.2.3(2))}{=} |\Omega| = 4$, so ist $|N_G(Q)| = 6$ und $|K| \leq 6$. Nach Satz (1.1.1) ist $G/K \lesssim \mathrm{Sym}\,\Omega = S_4$. Ist also $K = 1$, so folgt: $G \simeq S_4$. Wäre $|K| = 3$ oder 6, so enthielte K eine 3-Sylowgruppe, also alle 3-Sylowgruppen, Widerspruch zu Satz (1.2.4). Wäre $|K| = 2$, so wäre $|G/K| = 12$ und somit $G/K \simeq A_4$. Sei S/K die Kleinsche Vierergruppe in G/K, dann folgt mit Aufgabe 5: $S \trianglelefteq G$ und $|S| = 8$, daraus folgt: S ist die einzige 2-Sylowgruppe von G, Widerspruch.

1.2.8 Normalteiler von p-Gruppen

SATZ: Ist $|G| = p^n$ und $N \trianglelefteq G$ sowie $k \in \mathbb{N}$ mit $p^k \mid |N|$, so existiert ein in N enthaltener Normalteiler der Ordnung p^k.

KOROLLAR: Es existiert eine Kette $1 = N_0 < N_1 < \ldots < N_n = G$ von Normalteilern N_k von G mit $|N_k| = p^k$.

BEWEIS des Satzes: Sei $\Omega = \left\{ U \leq N \mid |U| = p^k \right\}$. Nach Satz (1.2.1) angewandt auf N ist $|\Omega| \equiv 1 \mod p$. Ω ist G-Menge per Konjugation: für $U \in \Omega$ ist $U^g \leq N^g = N$ und $|U^G| = p^k$, also $U^g \in \Omega$. Nach Lemma (1.1.8) existiert ein Fixpunkt $M \in \Omega$, d.h. $M^g = M$ für alle $g \in G$, also $M \trianglelefteq G$.

Mit Induktion folgt das Korollar.

1.2.9 Normalisatoren in p-Gruppen

SATZ: Ist G eine p-Gruppe und $H < G$, so ist $H < N_G(H)$.

BEWEIS: Induktion nach $|G|$. Ist $Z(G) \not\leq H$, so ist $N_G(H) \geq \langle Z(G), H \rangle > H$. Sei also $Z = Z(G) \leq H$. Nach Satz (1.1.8) ist $Z \neq 1$ und somit $|G/Z| < |G|$. Da $|H/Z| < |G/Z|$, folgt mit Induktionsannahme: $N_{G/Z}(H/Z) > H/Z$. Sei $xZ \in N_{G/Z}(H/Z) \setminus H/Z$. Dann ist $x \notin H$ und

$$H/Z = (H/Z)^{xZ} = (xZ)^{-1}(H/Z)(xZ) = (x^{-1}HxZ)/Z = (H^xZ)/Z = H^x/Z$$

Mit Aufgabe 5 folgt: $H = H^x$.

1.2.10 Maximale Untergruppen von p-Gruppen

DEFINITION: Sei G eine Gruppe. M ist *maximale Untergruppe* von G genau dann, wenn $M < G$ und aus $M < H \leq G$ folgt $H = G$.

SATZ: Jede maximale Untergruppe einer p-Gruppe G ist normal in G und hat Index p in G.

BEWEIS: Nach Satz (1.2.9) ist für maximale Untergruppe M von G offenbar $M < N_G(M) \leq G$, also $N_G(M) = G$. Damit ist $M \trianglelefteq G$.

Sei $x \in G \setminus M$ mit $o(x)$ minimal. Dann ist $o(x^p) < o(x)$, also $x^p \in M$. Nach Aufgabe 1 ist $M < M\langle x\rangle \leq G$ (da $M \trianglelefteq G$), also $M\langle x\rangle = G$. Es gilt

$$|G| = |M\langle x\rangle| \overset{\text{Aufg2}}{=} \frac{|M| \cdot |\langle x\rangle|}{|M \cap \langle x\rangle|} = \frac{|M| \cdot |\langle x\rangle|}{|\langle x^p\rangle|} = |M| \cdot p$$

also $|G : M| = p$.

1.3 Auflösbare Gruppen

1.3.1 Die Kommutatorgruppe

Sei G eine Gruppe und seien $a, b \in G$.

DEFINITIONEN:

1. $[a, b] = a^{-1}b^{-1}ab = a^{-1}a^b$ heißt *Kommutator* von a und b.
2. $G' = \langle \{ [x, y] \mid x, y \in G\} \rangle$ heißt *Kommutatorgruppe* von G.

BEMERKUNGEN:

1. $ba[a, b] = baa^{-1}b^{-1}ab = ab$. Offenbar ist $ab = ba$ genau dann, wenn $[a, b] = 1$.
2. Offenbar ist G abelsch genau dann, wenn $G' = 1$.
3. $\{ [x, y] \mid x, y \in G\}$ ist im Allgemeinen keine Untergruppe.

SATZ: Sei $H \leq G$. Genau dann gilt $H \trianglelefteq G$ und G/H abelsch, wenn $G' \leq H$. Die Kommutatorgruppe ist also der kleinste Normalteiler mit abelscher Faktorgruppe.

BEWEIS: Sei $G' \leq H$. Für alle $g \in H, h \in H$ gilt: $h^{-1}h^g = [h, g] \in H$, also $h^g \in H$. Somit $H \trianglelefteq G$. Weiter gilt für $H \trianglelefteq G$:

$$\begin{aligned} G/H \text{ abelsch} &\Leftrightarrow \forall x, y \in G : Hxy = HxHy = HyHx = Hyx \\ &\Leftrightarrow \forall x, y \in G : x^{-1}y^{-1}xy = (yx)^{-1}xy \in H \\ &\Leftrightarrow G' \leq H \end{aligned}$$

BEISPIELE: Für $G = S_3$ ist $G' = A_3$, für $G = A_4$ ist $G' = V_4$, für $G = S_4$ ist $G' = A_4$.

1.3.2 Vererbungseigenschaften

Seien $G, \bar{G}$ Gruppen.

LEMMA:

1. $H \leq G \Rightarrow H' \leq G'$
2. Ist $\sigma : G \to \bar{G}$ ein Homomorphismus, so ist $(G^\sigma)' = (G')^\sigma$. Insbesondere (für $\sigma : G \to G/N$ natürlicher Homomorphismus): Ist $N \trianglelefteq G$, so ist $(G/N)' = G'N/N$.

BEWEIS:

1. Trivial.
2. Für $a, b \in G$ ist

$$[a, b]^\sigma = (a^{-1}b^{-1}ab)^\sigma = (a^\sigma)^{-1}(b^\sigma)^{-1}a^\sigma b^\sigma = [a^\sigma, b^\sigma] \in (G^\sigma)' \qquad (\star)$$

   Weiter gilt: ist $x \in G'$, so gilt nach Lemma (1.0.1)(3): es existieren Kommutatoren oder Inverse der Kommutatoren $x_1, \ldots, x_n$ mit $x = x_1 \ldots x_n$. Dann ist nach $(\star)$ $x^\sigma = x_1^\sigma \ldots x_n^\sigma \in (G^\sigma)'$, also $(G')^\sigma \leq (G^\sigma)'$.

   Für $u, v \in G^\sigma$ existieren $a, b \in G$ mit $u = a^\sigma, v = b^\sigma$, mit $(\star)$ folgt: $[u, v] = [a^\sigma, b^\sigma] = [a, b]^\sigma \in (G')^\sigma$, d.h. $(G^\sigma)' \leq (G')^\sigma$.

   Für $\sigma : G \to G/N$ mit $g \mapsto gN$ gilt: $(G/N)' = (G^\sigma)' = (G')^\sigma = G'N/N$.

1.3.3 Höhere Kommutatorgruppen

Sei G eine Gruppe.

DEFINITION: $G^{(0)} = G$, $G^{(k+1)} = \left(G^{(k)}\right)'$ für $k \in \mathbb{N}_0$. $G^{(k)}$ heißt die k-*te*

Kommutatorgruppe von G. $G^{(2)}$ und $G^{(3)}$ werden oft mit G'' und G''' bezeichnet.

LEMMA: Seien G und $\bar{G}$ Gruppen und sei $k \in \mathbb{N}_0$.

1. $H \leq G \Rightarrow H^{(k)} \leq G^{(k)}$
2. Ist $\sigma : G \to \bar{G}$ ein Homomorphismus, so ist $\left(G^{(k)}\right)^\sigma = (G^\sigma)^{(k)}$, insbesondere aus $N \trianglelefteq G$ folgt: $(G/N)^{(k)} = G^{(k)}N/N$
3. $G^{(k)} \trianglelefteq G$

BEWEIS:

2. Induktion nach k. Für $k = 0$ ist $\left(G^{(0)}\right)^\sigma = G^\sigma = (G^\sigma)^{(0)}$. Die Aussage gelte für k, dann gilt

$$(G^{(k+1)})^\sigma \overset{Def.}{=} ((G^{(k)})')^\sigma \overset{(1.3.2)}{=} ((G^{(k)})^\sigma)' \overset{Vor.}{=} ((G^\sigma)^{(k)})' \overset{Def.}{=} (G^\sigma)^{(k+1)}$$

3. Für $g \in G$ wenden wir (b) an auf $\sigma_g : G \to G : x \mapsto x^g$ und erhalten

$$(G^{(k)})^g = (G^{(k)})^{\sigma_g} \overset{(b)}{=} (G^{\sigma_g})^{(k)} \overset{\sigma_g Auto.}{=} G^{(k)}$$

also $G^{(k)} \trianglelefteq G$.

1.3.4 Auflösbare Gruppen

SATZ: Die folgenden Eigenschaften der Gruppe G sind äquivalent:

1. Es existiert ein $n \in \mathbb{N}$ mit $G^{(n)} = 1$.
2. Es gibt eine Kette von Normalteilern N_i von G mit $G = N_0 \geq N_1 \geq \ldots \geq N_r = 1$ und N_i/N_{i+1} abelsch für alle i.
3. Es gibt eine Kette von Untergruppen M_i von G mit $G = M_0 \geq M_1 \geq \ldots \geq M_s = 1$ und $M_{i+1} \trianglelefteq M_i$ und M_i/M_{i+1} abelsch für alle i.

DEFINITION: Die Gruppe G heißt *auflösbar*, wenn sie eine (und damit alle) dieser 3 Eigenschaften hat.

BEWEIS:

(1)⇒(2) Setze $N_i = G^{(i)}$. Dann folgt mit (1.3.3)(c): $N_i \trianglelefteq G$ und $N_{i+1} = N_i'$ also N/N_{i+1} abelsch nach Satz (1.3.1).

(2)⇒(3) Trivial, setze $M_i = N_i$.

(3)⇒(1) Induktion nach s. In M_1 existiere Kette der Länge $s-1$. Nach Induktionsannahme existiert $m \in \mathbb{N}$ mit $(M_1)^{(m)} = 1$. Da $M_1 \trianglelefteq G$ mit G/M abelsch, folgt mit (1.3.1): $G' \leq M_1$. Somit $G^{(m+1)} = (G')^{(m)} \overset{1.3.3(a)}{\leq} (M_1)^{(m)} = 1$

BEISPIELE:

1. Abelsche Gruppen sind auflösbar: $n = 1$ erfüllt (a) des Satzes.
2. p-Gruppen sind auflösbar. Mit Korollar (1.2.8) folgt: (b) ist erfüllt.
3. S_n ist auflösbar für $n \leq 4$. In S_3 ist die Kette $S_3, A_3, 1$. In S_4 ist die Kette $S_4, A_4, V_4, 1$.

1.3.5 Vererbungseigenschaften für auflösbare Gruppen

Sei G eine Gruppe.

SATZ:

1. Ist G auflösbar und $H \leq G$, so ist H auflösbar.
2. Ist G auflösbar und $\sigma : G \to G^\sigma$ ein Homomorphismus, so ist G^σ auflösbar. Insbesondere falls $N \trianglelefteq G$ und G auflösbar, so ist G/N auflösbar.
3. Ist $N \trianglelefteq G$ und sind N und G/N auflösbar, so ist G auflösbar.

BEWEIS:

1. Ist G auflösbar, so existiert $n \in \mathbb{N}$ mit $G^{(n)} = 1$, dann folgt mit (1.3.3)(a): $H^{(n)} \leq G^{(n)} = 1$, also ist H auflösbar.
2. Ist G auflösbar, so existiert $n \in \mathbb{N}$ mit $G^{(n)} = 1$, dann folgt $(G^\sigma)^{(n)} \overset{1.3.3(b)}{=} (G^{(n)})^\sigma = 1^\sigma = 1$, damit ist G^σ auflösbar.
3. Sind N und G/N auflösbar, so existieren $r, s \in \mathbb{N}$ mit $N^{(r)} = 1$ und $1 = (G/N)^{(s)} = G^{(s)}N/N$. Also $G^{(s)} \leq N$. Somit $G^{(r+s)} = (G^{(s)})^{(r)} \leq N^{(r)} = 1$.

1.3.6 Gruppen der Ordnung $p^\alpha q$

SATZ: Gruppen der Ordnung $p^\alpha q$ mit $\alpha \in \mathbb{N}$ und Primzahlen p, q sind auflösbar.

BEWEIS: Induktion nach $|G|$. Sei $|G| = p^\alpha q$. Wir zeigen:

($\star$) Es existiert ein Normalteiler N von G mit $1 < N < G$.

Dann sind wir fertig: N und G/N sind entweder p-Gruppen oder haben Ordnung $p^\beta q$ (oder q) mit $\beta < \alpha$. Nach Induktionsannahme bzw. Bsp (1.3.5)(a) sind also N und G/N auflösbar. Nach (1.3.5)(c) ist also G auflösbar.

Beweis von ($\star$): Sei $p \neq q$ und $q = |\mathrm{Syl}_p(G)|$ (sonst gilt ($\star$)).

Fall 1. $S \cap T = 1$ für alle $S, T \in \mathrm{Syl}_p(G)$ mit $S \neq T$. Dann enthalten diese p-Sylowgruppen $q(p^\alpha - 1) = qp^\alpha - q = |G| - q$ p-Elemente. Die übrigen Elemente bilden die normale q-Sylowgruppe.

Fall 2. Es existieren $S, T \in \mathrm{Syl}_p(G)$ mit $S \neq T$ und $D := S \cap T \neq 1$. Wähle S und T so, dass D möglichst groß ist. Sei $M = N_G(D)$. Nach Satz (1.2.9) ist $D < N_S(D) = N_G(D) \cap S = M \cap S$. Genauso $M \cap T = N_T(D) > D$. Wäre M eine p-Gruppe, so gäbe es nach nach (1.2.3(1)) $P \in \mathrm{Syl}_p(G)$ mit $M \leq P$. Dann gilt $S \cap P \geq S \cap M = N_S(D) > D$. Mit Wahl von D folgt: $S = P$, genauso $T = P$, also $S = T$, Widerspruch. Somit $q \mid |M|$ und nach Sylow (1.2.3) existiert $Q \leq M$ mit $|Q| = q$. Dann ist

$$|SQ| \overset{Aufg.2}{=} \frac{|S| \cdot |Q|}{|S \cap Q|} = \frac{p^\alpha q}{1} = |G| \Rightarrow SQ = G$$

Für jedes $g \in G$ existieren also $x \in S, y \in Q$ mit $g = xy$. Somit

$$S^g = S^{xy} = (S^x)^y \overset{x \in S}{=} S^y \geq D^y = D$$

da $y \in Q \leq M = N_G(D)$. Daraus folgt: $1 < D \leq \bigcap_{g \in G} S^g = S_G \trianglelefteq G$. Also $N = S_G$ erfüllt ($\star$).

1.3.7 Gruppen S_n für $n \geq 5$

SATZ: Für $n \geq 5$ ist S_n nicht auflösbar.

BEWEIS: Wir zeigen mit Induktion nach k, dass $S_n^{(k)}$ alle 3-Zyklen enthält. Für $k = 0$ ist $S_n^{(0)} = S_n$, die Aussage gilt. Sei die Aussage für k richtig. Sei (a, b, c) ein 3-Zyklus. Da $n \geq 5$, existieren 2 weitere Elemente in $\Omega = \{1, \ldots, n\}$, etwa d, e. Sei $\alpha = (c, d, a)$ und $\beta = (a, b, e)$. Nach Induktionsvoraussetzung ist $\alpha, \beta \in S_n^{(k)}$ und somit $[\alpha, \beta] \in S_n^{(k+1)}$. Also

$$[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta = (a, d, c)(e, b, a)(c, d, a)(a, b, e) = (a, b, c) \in S_n^{(k+1)}$$

1.3.8 Einfache Gruppen

DEFINITION: Die Gruppe G heißt *einfach*, wenn G genau zwei Normalteiler besitzt (also $G \neq 1$ und G außer 1 und G keine weiteren Normalteiler hat)

BEMERKUNG: Sei G eine Gruppe, M_1 maximaler Normalteiler von G, M_2 maximaler Normalteiler von M_1 usw. Dann sind G/M_1 und M_i/M_{i+1} für alle i einfach.

FRAGEN:

1. Welches sind die einfachen Gruppen?
2. Wie setzen sie sich zusammen (Erweiterungstheorie)?

LEMMA: Sei G eine auflösbare Gruppe. Dann gilt: G ist genau dann einfach, wenn G zyklisch von Primzahlordnung ist.

BEWEIS:

„$\Leftarrow$“ Trivial

„$\Rightarrow$“ Sei G einfach und auflösbar, also $G \neq 1$. Da $G^{(n)} = 1$ für ein $n \in \mathbb{N}$, ist $G > G'$. Da nach (1.3.1) oder (1.3.3) $G' \trianglelefteq G$, folgt $G' = 1$ (da G einfach). Also G abelsch nach (1.3.1). Sei $1 \neq x \in G$. Dann ist $1 \neq \langle x \rangle \trianglelefteq G$. Da G einfach, folgt: $G = \langle x \rangle$. Ist $p \in \mathbb{P}$ (mit $p \mid o(x)$ falls $o(x) < \infty$), so ist $\langle x^p \rangle < \langle x \rangle = G$, also $\langle x^p \rangle = 1$, d.h. $|G| = p$.

1.3.9 Einfache Gruppen der Ordnung 60

SATZ: Die alternierende Gruppe A_5 (der Ordnung $\frac{5!}{2} = 60$) ist die kleinste nichtabelsche einfache Gruppe, das soll heißen:

1. Gruppen der Ordnung kleiner 60 sind auflösbar.
2. A_5 ist einfach.
3. Jede einfache Gruppe der Ordnung 60 ist isomorph zu A_5.

BEWEIS:

1. $60 = 2^2 \cdot 3 \cdot 5$. Wir wissen: Gruppen der Ordnung $p^\alpha, p^\alpha q, pqr$[5] sind auflösbar. Die einzige Zahl kleiner 60, die nicht von dieser Form ist, ist $2^2 \cdot 3^2 = 36$. Ist $|G| = 36$, so existiert $P \in \mathrm{Syl}_3(G)$ mit $|P| = 9$,

[5]Die Auflösbarkeit für pqr folgt mit Aufgabe 6(b).

also $|G : P| = 4$. Mit dem Satz (1.1.9) folgt: $|G/P_G|$ teilt $4! = 24$. Wie bereits gesehen, ist dann G/P_G auflösbar, ferner nach Beispiel (1.3.4) ist P_G auflösbar. Nach (1.3.5)(3) ist G auflösbar.

2. Angenommen es existiert $N \trianglelefteq A_5$ mit $1 < N < A_5$. Dann sind $|N|$ und $|G/N|$ kleiner 60, also auflösbar nach (1). Nach (1.3.5)(3) ist dann A_5 selber auflösbar. Da $|S_5/A_5| = 2$, folgt mit (1.3.5)(3): S_5 ist auflösbar, Widerspruch zu Satz (1.3.7)

3. Sei G einfach mit $|G| = 60$. Wir zeigen:

   ($\star$) G hat eine Untergruppe H der Ordnung 12.

   Dann sind wir fertig, denn nach (1.1.9) ist $G/H_G \simeq U \leq S_5$. Da G einfach, ist $H_G = 1$, also $G \simeq U$. Also $|U| = 60$. Wäre $U \neq A_5$, so wäre $120 \geq |UA_5| = \frac{|U|\cdot|A_5|}{|U\cap A_5|} = \frac{60\cdot 60}{|U\cap A_5|}$. Daraus folgt: $|U \cap A_5| \geq 30$. Aber A_5 hat nach (2) keine Untergruppe der Ordnung 30. Somit $U = A_5$, d.h. $G \simeq A_5$.

   Beweis von ($\star$): Sei $S \in \mathrm{Syl}_2(G)$ (also $|S| = 4$) und sei $H = N_G(S)$. Angenommen G hat keine Untergruppe der Ordnung 12.

   (i) *Behauptung:* Ist $U \leq G$ mit $|G : U| \leq 4$, so ist $U = G$.

   Beweis: Nach Satz (1.1.9) wäre $G/U_G \lesssim S_4, S_3$ oder S_2 wenn $|G : U| = 4, 3$ oder 2 wäre. Da G einfach, folgt: $U_G = 1$, also G auflösbar, Widerspruch zu Lemma.

   Es gilt $|G : N_G(S)| = 3, 5$ oder 15. Wegen (i) und Annahme, folgt: $|G : N_G(S)| = 15$.

   (ii) *Behauptung:* G hat 15 2-Sylowgruppen.

   Beweis: Seien $S_1, S_2 \in \mathrm{Syl}_2(G)$ mit $S_1 \neq S_2$ und sei $D = S_1 \cap S_2$. Es folgt: $D < S_1 < \langle S_1, S_2\rangle \leq C_G(D)$[6] (da die Gruppen der Ordnung 4 abelsch sind). Falls $|C_G(D)| = 4 \cdot 3$, so erhalten wir einen Widerspruch zur Annahme, falls $|C_G(D)| = 4 \cdot 5$, erhalten wir einen Widerspruch zu (i). Es folgt $|C_G(D)| = 4 \cdot 15$, d.h. $C_G(D) = G$. Somit $D \trianglelefteq G$, also $D = 1$. Somit enthalten die 2-Sylowgruppen von G $15(4-1) = 45$ verschiedene Elemente. Bleiben 15 übrig. Gäbe es 4 5-Sylowgruppen, so hätten wir $4(5-1) = 16$ Elemente der Ordnung 5, Widerspruch. Es folgt also $|\mathrm{Syl}_5(G)| \leq 3$, mit (1.2.3(3)) folgt: $|\mathrm{Syl}_5(G)| = 1$, d.h. die 5-Sylowgruppe ist ein Normalteiler von G, Widerspruch, da G einfach.

[6] Mit $C_G(D) = \{\, x \in G \mid\ a^x = a \text{ für alle } a \in D\}$

1.3.10 Gruppen A_n für $n \geq 5$

SATZ: Für alle $n \geq 5$ ist die alternierende Gruppe A_n einfach. Ferner sind $1, A_n$ und S_n die einzigen Normalteiler der S_n.

BEWEIS:

1. $A_n = \langle (ab)(cd) \mid a, b, c, d \in \Omega \rangle$, wobei $\Omega = \{1, \ldots, n\}$.
2. Sind $a, b, c, d \in \Omega$ paarweise verschieden, so ist
$$\begin{aligned} (ab)(cd) &= (abc)(cad) \\ (ab)(ad) &= (abd) \\ (ab)(ab) &= 1 \end{aligned}$$
3. Aus (1) und (2) folgt: $A_n = \langle (a, b, c) \mid a, b, c \in \Omega \rangle$
4. $(a_1, \ldots, a_k)^\sigma = (b_1, \ldots, b_k)$ falls
$$\sigma = \begin{pmatrix} a_1 & \ldots & a_k & \ldots \\ b_1 & \ldots & b_k & \ldots \end{pmatrix}$$
Beweis:
$$b_i^{\sigma^{-1}(a_1,\ldots,a_k)\sigma} = a_i^{(a_1,\ldots,a_k)\sigma} = a_{i+1 \bmod k}^{\sigma} = b_{i+1 \bmod k}$$
Folgerung: Je zwei Zyklen der Länge k sind in S_n konjugiert (allgemeiner: je zwei Elemente gleichen „Typs“ sind konjugiert) Konjugierte eines Zyklus der Länge k ist wieder ein Zyklus der Länge k.
5. Aus (4) folgt: Die Zyklen der Länge k bilden eine Konjugiertenklasse in S_n.
6. Aus $1 \neq N \trianglelefteq S_n$ folgt: $A_n \leq N$.
Beweis: Sei $1 \neq \sigma \in N$ und $i \in \Omega$ mit $i^\sigma \neq i$. Da $n \geq 5$, existiert $j \in \Omega$ mit $i \neq j \neq i^\sigma$. Sei $\tau = (ij) \in S_n$. Dann gilt $i^{\tau\sigma} = j^\sigma \neq i^\sigma \overset{i^\sigma \neq i,j}{=} i^{\sigma\tau}$. Damit ist $\tau\sigma \neq \sigma\tau$, also
$$1 \neq [\sigma, \tau] = \sigma^{-1}\sigma^\tau \in N \quad (\text{da } \sigma \in N \trianglelefteq S_n)$$
Es gilt $\tau^{-1} = \tau$, also $[\sigma, \tau] = \sigma^{-1}\tau\sigma\tau = \tau^\sigma\tau \in N$, dies ist nach (4) Produkt zweier Transpositionen. Da $[\tau, \sigma] \neq 1$, ist $\tau^\sigma \neq \tau$. Nach (2) ist also $\tau^\sigma\tau = (abc)$ oder $\tau^\sigma\tau = (ab)(cd)$ mit a, b, c, d paarweise verschieden. Da $n \geq 5$, existiert ein weiterer Punkt $e \in \Omega$. Nach (4) ist $(ab)(ce) \in N$ (da $N \trianglelefteq G$). Somit $(ab)(cd)(ab)(ce) = (cde) \in N$. In jedem Falle enthält N einen 3-Zyklus, nach (5) also alle, nach (3) folgt: $A_n \leq N$.

7. A_n ist einfach.

   Beweis: Angenommen es existiert $N \trianglelefteq A_n$ mit $1 < N < A_n$. Sei τ irgendeine Transposition in S_n. Dann ist $\tau \notin A_n$, also $S_n = \langle A_n, \tau \rangle$. Es gilt $N^\tau \trianglelefteq A_n$, also auch $NN^\tau \trianglelefteq A_n$ und $N \cap N^\tau \trianglelefteq A_n$. Ferner gilt

   $$(NN^\tau)^\tau = N^\tau N^{\tau^2} \overset{\tau^2=1}{=} N^\tau N = NN^\tau, \text{ d.h. } N_{S_n}(NN^\tau) \geq \langle A_n, \tau \rangle = S_n$$

   Also $NN^\tau \trianglelefteq S_n$. Nach (6) ist dann $NN^\tau = A_n$. Genauso $(N \cap N^\tau)^\tau = N^\tau \cap N$, also $N \cap N^\tau \trianglelefteq S_n$ nach (6) ist dann $N \cap N^\tau = 1$. Es gilt

   $$\frac{n!}{2} = |A_n| = |NN^\tau| \overset{\text{Aufg. 2}}{=} |N| \cdot |N^\tau| = |N|^2$$

   Hieraus folgt: $|N|$ ist gerade. Nach (1.2.1) existiert $\sigma \in N$ mit $o(\sigma) = 2$, also $\sigma = (ab)(cd)\ldots$, die Zyklenzerlegung enthält nur Zyklen der Länge 2. Sei jetzt $\tau = (ab)$, dann ist $\sigma = \sigma^\tau$, also $\sigma \in N \cap N^\tau = 1$, Widerspruch.

2 Anwendungen der Galoistheorie

2.4 Einheitswurzeln und Kreisteilungskörper

Sei K ein Körper, $n \in \mathbb{N}$ mit $\operatorname{char} K \nmid n$, $L = K(x^n - 1)$.

2.4.1 Einheitswurzel

DEFINITION: ε heißt *n-te Einheitswurzel* über K, genau dann, wenn ε Nullstelle von $x^n - 1$ ist.

SATZ: $E_n = \{\varepsilon \in L \mid \varepsilon^n = 1\}$ ist eine zyklische Gruppe von L^* der Ordnung n.

2.4.2 Primitive Einheitswurzeln und Eulersche φ-Funktion

DEFINITIONEN:

1. ε heißt *primitive* n-te Einheitswurzel genau dann, wenn $E_n = \langle \varepsilon \rangle$.
2. $\varphi(n)$ sei die Anzahl der primitiven n-ten Einheitswurzeln über K.

LEMMA:

$$\begin{aligned}\varphi(n) &= \text{Anzahl der primitiven } n\text{-ten Einheitswurzeln von } E_n \\ &= \text{Anzahl der Erzeugenden einer zyklischen Gruppe der Ordnung } n \\ &= \text{Anzahl der zu } n \text{ teilerfremden natürlichen Zahlen kleiner } n \\ &= |E(\mathbb{Z}/n\mathbb{Z})| \text{ Ordnung der Einheitengruppe von } \mathbb{Z}/n\mathbb{Z}\end{aligned}$$

SATZ:

1. φ ist multiplikativ, d.h. $\varphi(rs) = \varphi(r)\varphi(s)$ falls $\mathrm{ggT}(r,s) = 1$.
2. $\varphi(p^t) = p^t - p^{t-1} = p^t\left(1 - \frac{1}{p}\right)$
3. $\varphi(n) = n \cdot \prod_{p\in\mathbb{P}, p|n}\left(1 - \frac{1}{p}\right)$

2.4.3 Kreisteilungspolynome

DEFINITION: Das *n-te Kreisteilungspolynom* sei

$$\phi_{n,K} = \prod_{\substack{\varepsilon\in E_n \\ \text{primitiv}}} (x - \varepsilon)$$

Sei zudem $\phi_n := \phi_{n,\mathbb{Q}}$ und $\phi_{n,p} = \phi_{n,GF(p)}$

BEISPIELE:

$$\phi_1 = x - 1, \quad \phi_4 = x^2 + 1, \quad \phi_6 = x^2 - x + 1, \quad \phi_{12} = x^4 - x^2 + 1$$

Für $p \in \mathbb{P}$ ist

$$\phi_p = 1 + x + \ldots + x^{p-1}$$

LEMMA: Es gilt

$$x^n - 1 = \prod_{d|n} \phi_{d,K}$$

SATZ: Die Koeffizienten von $\phi_{n,K}$ liegen im Primkörper; ist $\mathrm{char}\, K = 0$, so sind sie ganzzahlig, d.h. $\phi_n \in \mathbb{Z}[x]$.

2.4.4 Anwendung - Lemma über Teilbarkeit

LEMMA: Seien $q, d, n \in \mathbb{N}$ und $q > 1$.

1. $q^d - 1 \mid q^n - 1 \iff d \mid n$
2. $d \mid n,\ d \neq n \Longrightarrow \phi_n(q) \mid \frac{q^n-1}{q^d-1}$
3. $n > 1 \Longrightarrow |\phi_n(q)| > q - 1$ (insbesondere $\phi_n(q) \nmid q - 1$)

BEWEIS:

(2), (1 „⇐“) Sei $d \mid n$. Nach Lemma (2.4.3) ist

$$x^n - 1 = \prod_{t|n} \phi_t = \prod_{t|d} \phi_t \cdot \prod_{s|n, s \nmid d} \phi_s \overset{(2.4.3)}{=} (x^d - 1) \cdot \prod_{s|n, s \nmid d} \phi_s$$

Also $q^d - 1 \mid q^n - 1$. Für $d \neq n$ ist

$$\frac{q^n - 1}{q^d - 1} = \prod_{s|n, s \nmid d} \phi_s(q)$$

Dieses Produkt wird offenbar von $\phi_n(q)$ geteilt.

(1 „⇒“) Sei $q^d - 1 \mid q^n - 1$ und $n = de + r$ mit $0 \leq r < d$. Dann folgt

$$q^d - 1 \mid q^n - 1 = q^{de+r} - 1 = q^r(q^{de} - 1) + q^r - 1$$

Da $q^d - 1 \mid q^{de} - 1$ nach (1 „⇐“), folgt: $q^d - 1 \mid q^r - 1$. Mit $r < d$ folgt: $r = 0$, also $d \mid n$.

(3) Sei $q \in \mathbb{R}, q \geq 2$. Ist ε primitive n-te Einheitswurzel, so folgt: ε liegt auf dem Einheitskreis und $\varepsilon \neq 1$. Geometrisch klar: $q - 1 < |q - \varepsilon|$, daraus folgt

$$|\phi_n(q)| = \left| \prod_{\substack{\varepsilon \in E_n \\ \text{primitiv}}} (q - \varepsilon) \right| = \prod_{\substack{\varepsilon \in E_n \\ \text{primitiv}}} |q - \varepsilon| > (q-1)^{\varphi(n)} \overset{q \geq 2}{\geq} q - 1$$

2.4.5 Endliche Schiefkörper - Satz von WEDDERBURN

DEFINITION: Ein *Schiefkörper* ist eine Menge K mit zwei Verknüpfungen $+, \cdot$ mit [7]

[7] Anders ausgedruckt: Schiefkörper ist ein Körper, bei dem die Kommutativität der multiplikativen Gruppe nicht verlangt wird.

1. $(K, +)$ ist eine abelsche Gruppe. Sei 0 das neutrale Element.
2. $(K \setminus \{0\}, \cdot)$ ist eine Gruppe.
3. $(a + b)c = ac + bc$ und $a(b + c) = ab + ac$ für alle $a, b, c \in K$.

BEISPIELE:

1. Jeder Körper ist ein Schiefkörper.
2. $\mathbb{H} = \{(a, b, c, d) \mid a, b, c, d \in \mathbb{R}\}$ mit komponentenweise Addition und

$$\begin{aligned}(a_0, a_1, a_2, a_3) \circ (b_0, b_1, b_2, b_3) \quad = \quad & (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3, \\ & a_0b_1 + b_0a_1 + a_2b_3 - a_3b_2, \\ & a_0b_2 + b_0a_2 + a_1b_3 - a_3b_1, \\ & a_0b_3 + b_2a_3 + a_1b_2 - a_2b_1)\end{aligned}$$

heißt *Quaternionenschiefkörper* . Ist

$$e = (1, 0, 0, 0), i = (0, 1, 0, 0), j = (0, 0, 1, 0), k = (0, 0, 0, 1)$$

so ist e das Einselement und

$$i^2 = j^2 = k^2 = -e,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j$$

Es gilt[8]

$$Q = \{e, -e, i, -i, j, -j, k, -k\} \leq \mathbb{H}^*$$

SATZ: (WEDDERBURN 1905) Jeder endliche Schiefkörper ist ein Körper, d.h. kommutativ.

BEWEIS: (Witt 1931) Sei K ein endlicher nichtkommutativer Schiefkörper. Für $a \in K$ sei $C(a) := \{x \in K \mid ax = xa\}$ und sei $Z(K) = \{x \in K \mid xy = yx$ für alle $y \in K\}$.

1. $Z(K) \leq C(a) \leq K$ (Teilschiefkörper) für alle $a \in K$ und natürlich ist $Z(K)$ ein Körper.

   Beweis: Für $b, c \in C(a)$ ist

$$\begin{aligned}a(b \pm c) = ab \pm ac = ba \pm ca = (b \pm c)a \quad &\Rightarrow \quad b \pm c \in C(a) \\ a(bc) = (ab)c = (ba)c = (bc)a \quad &\Rightarrow \quad b \cdot c \in C(a)\end{aligned}$$

[8] Vergleiche Aufgabe 4: $i^4 = e,\ i^2 = j^2,\ i^j = (-j)ij = -jk = -i = i^{-1}$. Damit ist $Q \simeq Q_8$, der Quaternionengruppe.

2. Ist $Z(K) \leq R \leq K$, so ist R ein $Z(K)$-Vektorraum. Sei $q = |Z(K)|$. Da $Z(K)$ ein Körper ist, ist $q > 1$. Ist $\dim_{Z(K)}(K) = n$, so ist $|K| = q^n$. Für $a \in K$ sei $\dim_{Z(K)} C(a) = n_a$, also $|C(a)| = q^{n_a}$. Sei $G = K^*$. Offenbar ist G eine endliche nichtkommutative Gruppe mit $|G| = q^n - 1$. Weiter ist $Z(G) = Z(K) \setminus \{0\}$, also $|Z(G)| = q - 1$, genauso gilt für alle $0 \neq a \in K$: $C_G(a) = C(a) \setminus \{0\}$, also $|C_G(a)| = q^{n_a} - 1$. Nach Lagrange ist $|C_G(a)|$ ein Teiler von $|G|$. Mit Lemma (2.4.4)(a) folgt daraus: $n_a \mid n$ für alle $0 \neq a \in K$. Sei $R \subseteq G$ ein Repräsentantensystem für die Konjugiertenklassen der Länge größer 1 in G. Die Klassengleichung (Satz (1.1.7)) besagt:

$$q^n - 1 = |G| = |Z(G)| + \sum_{a \in R} |G : C_G(a_i)| = q - 1 + \sum_{a \in R} \frac{q^n - 1}{q^{n_a} - 1}$$

Es gilt nach (2.4.4): $\phi_n(q) \mid q^n - 1$ und $\phi_n(q)$ teilt die Summe rechts, daraus folgt: $\phi_n(q) \mid q - 1$, Widerspruch zu (2.4.4).

2.4.6 Satz von Dirichlet

SATZ: (DIRICHLET 1837) Zu je zwei teilerfremden natürlichen Zahlen n, m existieren unendlich viele Primzahlen p mit $p \equiv m \mod n$, d.h. von der Form $m, m + n, m + 2n, \ldots$

Wir beweisen den Spezialfall $m = 1$.

LEMMA: Seien $n, m \in \mathbb{N}$ mit $m > 1$ und p ein Primteiler von $\phi_n(m)$. Dann ist $p \nmid m$. Ist zusätzlich $p \nmid n$, so gilt $p \equiv 1 \mod n$.

BEWEIS: Nach (2.4.3) ist ϕ_n ein Teiler von $x^n - 1$ in $\mathbb{Z}[x]$, also $p \mid \phi_n(m) \mid m^n - 1$. Wäre also $p \mid m$, so $p \mid m^n$ und somit $p \mid 1$, Widerspruch.

Da $p \nmid m$, ist $m + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$. Sei d die Ordnung von $m + p\mathbb{Z}$ in dieser Gruppe. Es gilt:

$$(m + p\mathbb{Z})^n = m^n + p\mathbb{Z} \overset{p \mid m^n - 1}{=} 1 + p\mathbb{Z} = 1$$

Nach (3) aus 8.3 (Algebra 1) folgt $d \mid n$. Angenommen $d < n$, also $n = de$ mit $e > 1$. Nach (2.4.4)(2) ist

$$p \mid \phi_n(m) \mid \frac{m^n - 1}{m^d - 1} = \frac{(m^d)^e - 1}{m^d - 1} = 1 + m^d + (m^d)^2 + \ldots + (m^d)^{e-1}$$

Da $1 + p\mathbb{Z} = (m + p\mathbb{Z})^d = m^d + p\mathbb{Z}$, folgt:

$$0 \equiv \underbrace{1 + 1 + \ldots + 1}_{e} = e \mod p$$

Somit $p \mid e$, also $p \mid de = n$, Widerspruch zur Voraussetzung. Somit $d = n$ ist Ordnung von $m + p\mathbb{Z}$ in der Gruppe $\mathbb{Z}/p\mathbb{Z}$ der Ordnung $p - 1$, nach Lagrange folgt $d = n \mid p - 1$, d.h. $p \equiv 1 \mod n$.

KOROLLAR: Ist $n \in \mathbb{N}, n > 1$ und p ein Primteiler von $\phi_n(n)$, so ist $p \equiv 1 \mod n$.

BEWEIS: Setze $n = m$ im Lemma.

SATZ: Zu jeder natürlichen Zahl n existieren unendlich viele Primzahlen p mit $p \equiv 1 \mod n$.

BEWEIS: Für jedes $k \in \mathbb{N}$ mit $k \geq 2$ betrachte $\phi_{nk}(nk)$. Nach (2.4.4)(c) ist $|\phi_{nk}(nk)| > nk - 1$, enthält also einen Primteiler p_k. Nach Korollar ist $p_k \equiv 1 \mod nk$, insbesondere $p_k \equiv 1 \mod n$. Für alle k gilt $p_k > nk$. Daraus folgt $\lim\limits_{k \to \infty} p_k = \infty$, es gibt also unendlich viele solche Primzahlen.

2.4.7 Kreisteilungskörper

Sei $n \in \mathbb{N}$.

DEFINITION: $\mathbb{Q}_n := \mathbb{Q}(x^n - 1) = \mathbb{Q}(\phi_n) = \mathbb{Q}(\varepsilon)$ mit $\varepsilon \in E_n$ primitiv heißt *n-ter Kreisteilungskörper*.

LEMMA: (Gauß) ϕ_n ist irreduzibel über $\mathbb{Q}$ und somit $[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n)$.

SATZ: $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq E(\mathbb{Z}/n\mathbb{Z})$, insbesondere ist $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ abelsch und somit sind alle Zwischenkörper normal

KOROLLAR: Ist $n = p \in \mathbb{P}$, so ist $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ zyklisch der Ordnung $p - 1$.

BEMERKUNG: Allgemein für $\mathrm{char}\, K \nmid n$ und $L = K(x^n - 1)$ ist $\mathrm{Gal}(L/K) \lesssim E(\mathbb{Z}/n\mathbb{Z})$, insbesondere abelsch und jeder Zwischenkörper normal.

2.4.8 Fixkörper eines Kreisteilungskörpers

SATZ: Sei p eine Primzahl, ε eine primitive p-te Einheitswurzel, $\mathbb{Q}_p = \mathbb{Q}(\varepsilon)$ der p-te Kreisteilungskörper und $G = \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$. Sei $H \leq G$, $f = |G : H|$ und sei R ein Repräsentantensystem für die Restklassen von H in G. Sei $\delta = \sum_{\tau \in H} \varepsilon^\tau$ und für $\rho \in R$ sei $\delta_\rho = \sum_{\tau \in H} \varepsilon^{\rho\tau}$. Dann gilt:

1. $\{\, \delta_\rho \mid \rho \in R\}$ ist eine Basis von $H\mathfrak{F}$ als $\mathbb{Q}$-Vektorraum.
2. $H\mathfrak{F} = \mathbb{Q}(\delta_\rho)$ für alle $\rho \in R$, insbesondere $H\mathfrak{F} = \mathbb{Q}(\delta)$.

BEWEIS:

1. Für $\sigma \in H$ ist

$$(\delta_\rho)^\sigma = \left(\sum_{\tau \in H} \varepsilon^{\rho\tau}\right)^\sigma \overset{\sigma \text{Auto.}}{=} \sum_{\tau \in H} \varepsilon^{\rho(\tau\sigma)} = \delta_\rho$$

   denn mit τ durchläuft auch $\tau\sigma$ alle Elemente aus H. Somit ist $\delta_\rho \in H\mathfrak{F}$, also sind δ_ρ f Elemente in $H\mathfrak{F}$. Es bleibt zu zeigen: δ_ρ sind linear unabhängig.

   Angenommen es existieren $a_\rho \in \mathbb{Q}$ mit

$$0 = \sum_{\rho \in R} a_\rho \delta_\rho = \sum_{\rho \in R} a_\rho \sum_{\tau \in H} \varepsilon^{\rho\tau} = \sum_{\rho \in R} \sum_{\tau \in H} a_\rho \varepsilon^{\rho\tau}$$

   Die $\rho\tau$ durchlaufen alle Elemente von G. Die $\varepsilon^{\rho\tau}$ sind dann genau die $p-1$ primitiven p-ten Einheitswurzeln, also $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$. Multiplikation mit ε^{-1} liefert die Gleichung $0 = \sum a_\rho \varepsilon^i$ mit $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-2}$. Diese Potenzen sind nach 4.4 (Algebra 1) linear unabhängig über $\mathbb{Q}$, also sind alle $a_\rho = 0$ und damit sind die δ_ρ linear unabhängig.

2. Für $\rho \in R$ gilt

$$\delta^\rho = \left(\sum_{\tau \in H} \varepsilon^\tau\right)^\rho = \sum_{\tau \in H} \varepsilon^{\tau\rho} \overset{G \text{ abelsch}}{=} \sum_{\tau \in H} \varepsilon^{\rho\tau} = \delta_\rho$$

   d.h. alle δ_ρ sind unter G konjugiert. Wäre für ein $\rho \in R$ $\mathbb{Q}(\delta_\rho) < H\mathfrak{F}$, so wären alle δ_μ ($\mu \in R$) in diesem normalen (nach Satz (2.4.7)) Zwischenkörper enthalten, Widerspruch zu (1). Somit $\mathbb{Q}(\delta_\rho) = H\mathfrak{F}$.

2.4.9 Die p-ten Einheitswurzeln

1. Für $p = 2$ sind $1, -1$ die Einheitswurzeln.

2. Sei $p = 3$. Es gilt $0 = \varepsilon^3 - 1 = (\varepsilon - 1)(\varepsilon^2 + \varepsilon + 1)$. Da ε primitiv, folgt: $\varepsilon^2 + \varepsilon + 1 = 0$, daraus folgt: $\varepsilon_{1,2} = -\frac{1}{2} \pm \sqrt{\frac{1}{4} - 1} = \frac{1}{2}(-1 \pm i\sqrt{3})$.

3. Sei $p = 5$. Sei $G = \mathrm{Gal}(\mathbb{Q}_5/\mathbb{Q})$, dann ist $|G| = 4$. Für $\sigma : \varepsilon \mapsto \varepsilon^2$ gilt $\sigma^2 : \varepsilon \mapsto \varepsilon^4 = \varepsilon^{-1}$, also $\sigma^2 \neq 1$, damit ist $G = \langle\sigma\rangle$. Sei $H = \langle\sigma^2\rangle$ und $K = H\mathfrak{F}$. Es gilt $G = H \cup H\sigma = \{1, \sigma^2\} \cup \{\sigma, \sigma^3\}$, sei also $R = \{1, \sigma\}$ (siehe (2.4.8)). Dann ist

$$\begin{aligned} \delta &= \delta_1 = \varepsilon^1 + \varepsilon^{\sigma^2} = \varepsilon + \varepsilon^4 = \varepsilon + \varepsilon^{-1} \\ \delta_\sigma &= \varepsilon^\sigma + \varepsilon^{\sigma^3} = \varepsilon^2 + \varepsilon^3 \end{aligned}$$

Es gilt $(x - \delta)(x - \delta_\sigma) = x^2 - (\delta + \delta_\sigma)x + \delta\delta_\sigma$. Die Koeffizienten sind

$$\begin{aligned} \delta + \delta_\sigma &= \varepsilon + \varepsilon^4 + \varepsilon^2 + \varepsilon^3 = \sum_{i=0}^{4} \varepsilon^i - \varepsilon^0 = -1 \\ \delta\delta_\sigma &= (\varepsilon + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 = \varepsilon^3 + \varepsilon^4 + \varepsilon + \varepsilon^2 = -1 \end{aligned}$$

Damit ist

$$\delta_{1,\sigma} = \frac{1}{2}\left(\pm\sqrt{5} - 1\right) \qquad (*)$$

Multipliziere $\delta = \varepsilon + \varepsilon^4$ mit ε, dann folgt $\varepsilon\delta = \varepsilon^2 + 1$, also $\varepsilon^2 - \delta\varepsilon + 1 = 0$, d.h. ε ist Nullstelle des Polynoms $x^2 - \delta x + 1 \in K[x]$. Daraus folgt

$$\varepsilon_{1,2} = \frac{\delta}{2} \pm \sqrt{\frac{\delta^2}{4} - 1}$$

Da $\delta^2 + \delta - 1 = 0$, ist $\delta^2 = 1 - \delta$, daraus folgt

$$\varepsilon_{1,2} = \frac{1}{2}\left(\delta \pm \sqrt{\delta^2 - 4}\right) = \frac{1}{2}\left(\delta \pm \sqrt{-3 - \delta}\right) = \frac{1}{2}\left(\delta \pm i\sqrt{3 + \delta}\right)$$

Die letzte Gleichheit gilt, weil aus (*) folgt: $|\delta| < 3$. Damit ist

$$\varepsilon_{1,2,3,4} = \frac{1}{2}\left(\delta \pm i\sqrt{3 + \delta}\right) \text{ mit } \delta = \frac{1}{2}\left(\pm\sqrt{5} - 1\right)$$

ε liegt im 1 Quadranten, falls beide Male positives Vorzeichen genommen wird. Es folgt

$$\begin{aligned} \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} &= \frac{1}{4}\left(\sqrt{5} - 1\right) + i\frac{1}{2}\sqrt{3 + \frac{1}{2}\left(\sqrt{5} - 1\right)} \\ &= \frac{1}{4}\left(\sqrt{5} - 1\right) + i\frac{1}{4}\sqrt{2\sqrt{5} + 10} \end{aligned}$$

Also

$$\cos\frac{2\pi}{5} = \frac{1}{4}(\sqrt{5}-1); \qquad \sin\frac{2\pi}{5} = \frac{1}{4}\sqrt{2\sqrt{5}+10}$$

Dies ergibt die Vorschrift für die Konstruktion des regelmäßigen 5-Ecks.

4. Sei $p = 17$, dann ist $|G| = 16$. Es gilt[9]

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2\left(1-\sqrt{17}\right)\sqrt{34-2\sqrt{17}}}\right)$$

2.5 Reine Gleichungen und zyklische Körpererweiterungen

2.5.1 n-te Radikale

Sei K ein Körper, $n \in \mathbb{N}$.

DEFINITION: Die Nullstellen der Polynome $x^n - a$ mit $0 \neq a \in K$ heißen *n-te Radikale* über K.

SATZ: Sei K ein Körper mit $\operatorname{char} K \nmid n$, der die n-ten Einheitswurzeln enthält. Ist $L = K(\alpha)$ mit einem n-ten Radikal α über K, so ist L galoissch über K und $\mathrm{Gal}(L/K)$ zyklisch von n teilender Ordnung.

BEWEIS: Sei $\alpha^n - a = 0$ mit $0 \neq a \in K$. Sei ε eine primitive n-te Einheitswurzel. Dann gilt $(\varepsilon^i\alpha)^n = \varepsilon^{in}\alpha^n = \alpha^n = a$ für alle $i = 0, \ldots, n-1$, d.h. $\varepsilon^i\alpha$ sind Nullstellen von $x^n - a$ (siehe 12.2, Algebra 1). Das sind n verschiedene Nullstellen, d.h. $x^n - a$ ist separabel und $L = K(\alpha) = K(x^n - a)$, d.h. L ist galoissch über K.

Für $\sigma \in G = \mathrm{Gal}(L/K)$ ist $(\alpha^\sigma)^n = (\alpha^n)^\sigma = a^\sigma = a$, also $\alpha^\sigma = \varepsilon^i\alpha$ für ein $i \in \{0, \ldots, n-1\}$. Sei E_n die Gruppe der n-ten Einheitswurzeln. Dann erhalten wir eine Abbildung $\rho : G \to E_n$ mit $\sigma \mapsto \varepsilon^i = \frac{\alpha^\sigma}{\alpha}$. *Behauptung:* ρ ist ein Monomorphismus.

Beweis: Seien $\sigma, \tau \in G$ und $\alpha^\sigma = \varepsilon^i\alpha$ und $\alpha^\tau = \varepsilon^j\alpha$.

$$\alpha^{\sigma\tau} = (\varepsilon^i\alpha)^\tau = (\varepsilon^i)^\tau\alpha^\tau \overset{\varepsilon^i \in K}{=} \varepsilon^i\varepsilon^j\alpha$$

Somit $(\sigma\tau)^\rho = \varepsilon^i\varepsilon^j = \sigma^\rho\tau^\rho$, d.h. ρ ist ein Homomorphismus.

Ist $\sigma \in \operatorname{Kern}\rho$, so gilt $\sigma^\rho = \frac{\alpha^\sigma}{\alpha} = 1$, daraus folgt $\alpha^\sigma = \alpha$. Da $L = K(\alpha)$, folgt: $\sigma = \mathrm{id}$. Mit Homomorphiesatz folgt: $G \simeq G/\operatorname{Kern}\rho \simeq G^\rho \leq E_n$, d.h. G ist

[9] Siehe v.d. Waerden S. 180-181, Hornfeck S. 223-225, Stewart S. 186-188.

zyklisch von n teilender Ordnung (siehe Satz (2.4.1))

KOROLLAR: Ist $n = p \in \mathbb{P}$, so ist entweder $L = K$ oder $[L : K] = n$ (d.h. das Polynom $x^n - a$ ist irreduzibel)

BEWEIS: $|\mathrm{Gal}(L/K)| \mid p$, daraus folgt: $|\mathrm{Gal}(L/K)| = [L : K] = 1$ oder p. Ist $[K(\alpha) : K] = p$, so folgt: das definierende Polynom von α hat Grad p, also ist $x^p - a$ das definierende Polynom.

BEMERKUNG: Die Voraussetzungen des Satzes sind notwendig:

1. $\mathrm{char}\, K \nmid n$. Ist $\mathrm{char}\, K = p = n$, so $x^p - a = (x - \alpha)^p$, damit ist dieses Polynom inseparabel, falls irreduzibel, die Erweiterung ist also nicht galoissch.

2. K enthält die n-ten Einheitswurzeln. $\mathbb{Q}$ enthält i und $-i$ nicht. Nach 10.7, Beispiel 5 (Algebra 1) hat $\mathbb{Q}(x^4 - 5)$ als Galoisgruppe D_8, die nicht zyklisch ist.

2.5.2 Spur und Norm

Sei L galoissch über K und $G = \mathrm{Gal}(L/K)$, sei $\alpha \in L$.

DEFINITIONEN:

1. $S_{L/K}(\alpha) = \sum_{\sigma \in G} \alpha^\sigma$ heißt *Spur* von α.

2. $N_{L/K}(\alpha) = \prod_{\sigma \in G} \alpha^\sigma$ heißt *Norm* von α.

SATZ:

1. $S = S_{L/K} : L \to K$ ist eine K-lineare Abbildung von L in K, d.h. es gilt für alle $\alpha, \beta \in L$ und $a \in K$:
   (a) $S(\alpha) \in K$
   (b) $S(\alpha + \beta) = S(\alpha) + S(\beta)$
   (c) $S(a\alpha) = aS(\alpha)$
2. $N = N_{L/K} : L \to K$ ist multiplikativ und homogen vom Grad $n = [L : K]$, d.h.
   (a) $N(\alpha) \in K$
   (b) $N(\alpha\beta) = N(\alpha)N(\beta)$
   (c) $N(a\alpha) = a^n N(\alpha)$

   Ferner ist $N^* = N|_{L^*} : L^* \to K^*$ ein Gruppenhomomorphismus.

BEWEIS: Für $\tau \in G$ ist

$$S(\alpha)^\tau = \left(\sum_{\sigma\in G} \alpha^\sigma\right)^\tau = \sum_{\sigma\in G} \alpha^{\sigma\tau} = S(\alpha)$$

Da mit σ auch $\sigma\tau$ alle Gruppenelemente durchläuft. Somit $S(\alpha) \in F\mathfrak{F} = K$, da L/K galoissch ist. Genauso

$$N(\alpha)^\tau = \left(\prod_{\sigma\in G} \alpha^\sigma\right)^\tau = \prod_{\sigma\in G} \alpha^{\sigma\tau} = N(\alpha)$$

also $N(\alpha) \in K$. Weiter gilt

$$\begin{aligned}
S(\alpha+\beta) &= \sum_{\sigma\in G}(\alpha+\beta)^\sigma = \sum_{\sigma\in G}\alpha^\sigma + \sum_{\sigma\in G}\beta^\sigma = S(\alpha) + S(\beta)\\
S(a\alpha) &= \sum_{\sigma\in G}(a\alpha)^\sigma = \sum_{\sigma\in G} a^\sigma\alpha^\sigma = \sum_{\sigma\in G} a\alpha^\sigma = a\sum_{\sigma\in G}\alpha^\sigma = aS(\alpha)\\
N(\alpha\beta) &= \prod_{\sigma\in G}(\alpha\beta)^\sigma = \prod_{\sigma\in G}\alpha^\sigma\beta^\sigma = \prod_{\sigma\in G}\alpha^\sigma \prod_{\sigma\in G}\beta^\sigma = N(\alpha)N(\beta)\\
N(a\alpha) &= \prod_{\sigma\in G}(a\alpha)^\sigma = \prod_{\sigma\in G} a^\sigma\alpha^\sigma = \prod_{\sigma\in G} a\alpha^\sigma = a^{|G|}\prod_{\sigma\in G}\alpha^\sigma = a^n N(\alpha)
\end{aligned}$$

BEISPIELE:

1. $K = \mathbb{R}, L = \mathbb{C}, G = \{1, \sigma\}$ mit $\sigma : a + ib \mapsto a - ib$. Ist $\alpha = a + ib$, so gilt

$$\begin{aligned} S(\alpha) &= (a+ib) + (a-ib) = 2a = 2\Re(\alpha) \\ N(\alpha) &= (a+ib)(a-ib) = a^2 + b^2 = |\alpha|^2 \\ \operatorname{Kern} S &= \{ib \mid b \in \mathbb{R}\} \\ \operatorname{Bild} S &= \mathbb{R} \\ \operatorname{Kern} N^* &= \{\alpha \in \mathbb{C} \mid |\alpha| = 1\} = \text{ Einheitskreis} \\ \operatorname{Bild} N^* &= \mathbb{R}_{>0} \end{aligned}$$

2. Sei $0 \neq n \in \mathbb{Z}$ kein Quadrat und $s \in \mathbb{C}$ mit $s^2 = n$. Sei $K = \mathbb{Q}, L = \mathbb{Q}(s) = \{a + bs \mid a, b \in \mathbb{Q}\}$. Es ist $G = \{1, \sigma\}$ mit $\sigma : a + bs \to a - bs$. Es gilt $S(\alpha) = 2a$ mit Kern und Bild wie in (1).

$$\begin{aligned} N(\alpha) &= (a+bs)(a-bs) = a^2 - nb^2 \\ \operatorname{Kern} N^* &= \left\{a + bs \mid a^2 - nb^2 = 1\right\} \\ \operatorname{Bild} N^* &= \left\{c \in \mathbb{Q} \mid \exists a, b \in \mathbb{Q} \text{ mit } a^2 - nb^2 = c\right\} \end{aligned}$$

   Für den Kern sind gesucht die rationalen Punkte auf der Hyperbel (oder Ellipse) $x^2 - ny^2 = 1$. Für das Bild sind c gesucht, für die die Gleichung $x^2 - ny^2 = c$ rationale Lösungen hat.

3. Sei $K = \mathrm{GF}(q)$ $(q = p^f, p \in \mathbb{P}), L = \mathrm{GF}(q^n)$. Sei $\sigma : \alpha \to \alpha^q$, dann gilt $\sigma \in G = \mathrm{Gal}(L/K)$ und $G = \langle\sigma\rangle = \{\sigma^i \mid i = 1, \ldots, n\}$, wobei $\sigma^i : \alpha \to \alpha^{q^i}$. Es gilt

$$\begin{aligned} S(\alpha) &= \sum_{i=0}^{n-1} \alpha^{\sigma^i} = \sum_{i=0}^{n-1} \alpha^{q^i} = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}} \\ N(\alpha) &= \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{1+q+q^2+\ldots+q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}} \end{aligned}$$

   Behauptung: Spur und Norm sind für endliche Körper surjektiv.

   Beweis: Ist $S(\alpha) = 0$, so ist α Nullstelle des Polynoms $x + x^q + \ldots + x^{q^{n-1}}$. Dieses Polynom hat höchstens q^{n-1} Nullstellen. Da $|L| = q^n > q^{n-1}$, existiert $\alpha \in L$ mit $S(\alpha) \neq 0$. Somit ist $S(L)$ ein Teilraum ungleich $\{0\}$ von K. Daraus folgt: $S(L) = K$.

   Es gilt $|\operatorname{Kern} N^*| \leq \frac{q^n-1}{q-1}$, da $\alpha \in \operatorname{Kern} N^* \Leftrightarrow \alpha^{\frac{q^n-1}{q-1}} = 1$. Daraus folgt

$$|\operatorname{Bild} N^*| \overset{(1.0.7)}{=} \frac{|L^*|}{|\operatorname{Kern} N^*|} \geq \frac{q^n - 1}{\frac{q^n-1}{q-1}} = q - 1$$

   Da $|K^*| = q - 1$, folgt: $\operatorname{Bild} N^* = K^*$.

2.5.3 Dedekinds Lemma

DEFINITION: Eine *Halbgruppe* ist eine nichtleere Menge H mit einer assoziativen Verknüpfung.

SATZ: Sei $(H, \cdot)$ eine Halbgruppe, K ein Körper und seien $\sigma_1, \ldots, \sigma_n$ verschiedene Homomorphismen von H in K^*. Dann sind $\sigma_1, \ldots, \sigma_n$ linear unabhängig im K-Vektorraum $\mathrm{Abb}(H, K)$, d.h. sind $c_1, \ldots, c_n \in K$, so dass

$$c_1 h^{\sigma_1} + c_2 h^{\sigma_2} + \ldots + c_n h^{\sigma_n} = 0 \qquad (*)$$

für alle $h \in H$, so ist $c_1 = \ldots = c_n = 0$.[10]

BEWEIS: Induktion nach n. Sei $n = 1$. Sei $c_1 \in K$ mit $c_1 h^{\sigma_1} = 0$ für alle $h \in H$. Da $h^{\sigma_1} \in K^*$, ist $h^{\sigma_1} \neq 0$, also $c_1 = 0$.

Sei $n > 1$ und die Aussage für $n-1$ richtig. Seien $c_1, \ldots, c_n \in K$ mit (*) für alle $h \in H$. Angenommen nicht alle $c_i = 0$. Sei o.B.d.A. $c_2 \neq 0$. Da $\sigma_1 \neq \sigma_2$, existiert $a \in H$ mit $a^{\sigma_1} \neq a^{\sigma_2}$. Setze ah in (*) ein:

$$0 = c_1 (ah)^{\sigma_1} + \ldots + c_n (ah)^{\sigma_n} = c_1 a^{\sigma_1} h^{\sigma_1} + \ldots + c_n a^{\sigma_n} h^{\sigma_n}$$

Nun multipliziere (*) mit a^{σ_1}:

$$0 = a^{\sigma_1} c_1 h^{\sigma_1} + \ldots + a^{\sigma_1} c_n h^{\sigma_n} = c_1 a^{\sigma_1} h^{\sigma_1} + \ldots + c_n a^{\sigma_1} h^{\sigma_n}$$

Subtraktion liefert

$$0 = c_2 (a^{\sigma_2} - a^{\sigma_1}) h^{\sigma_2} + \ldots + c_n (a^{\sigma_n} - a^{\sigma_1}) h^{\sigma_n} = \sum_{i=2}^{n} c_i' h^{\sigma_i} \text{ mit } c_i' = c_i (a^{\sigma_i} - a^{\sigma_1})$$

Nach Induktionsannahme sind alle $c_i' = 0$, insbesondere gilt $0 = c_2' = c_2 (a^{\sigma_2} - a^{\sigma_1})$, dies ist ein Widerspruch, da $c_2 \neq 0$ und $a^{\sigma_2} \neq a^{\sigma_1}$.

FOLGERUNGEN:

1. Seien K_1 und K_2 Körper und seien $\sigma_1, \ldots, \sigma_n$ Monomorphismen von K_1 in K_2. Dann sind $\sigma_1, \ldots, \sigma_n$ über K_2 linear unabhängig.

2. Paarweise verschiedene Automorphismen eines Körpers sind linear unabhängig. Also sind $\sigma_1, \ldots, \sigma_n$ paarweise verschiedene Automorphismen von L und sind $c_1, \ldots, c_n \in L$ mit $c_1 \alpha^{\sigma_1} + \ldots + c_n \alpha^{\sigma_n} = 0$ für alle $\alpha \in L$, so sind alle $c_i = 0$.

BEWEIS:

1. Betrachte $\sigma_i|_{K_1^*} : K_1^* \to K_2^*$ (möglich, da σ_i Monomorphismus). Wende nun den Satz an.

[10] Beachte dafür, dass die Summe gleich $h^{\sum c_i \sigma_i}$ ist.

2.5.4 Surjektivität der Spur

SATZ: Ist L galoissch über K, so ist $S_{L/K}(L) = K$.

BEWEIS: Nach Folgerung (2.5.3)(2) existiert $\alpha \in L$ mit $S_{L/K}(\alpha) \neq 0$; denn wäre $0 = S_{L/K}(\alpha) = \sum_{\sigma \in G} 1 \cdot \alpha^\sigma$ für alle $\alpha \in L$, so folgte aus (2.5.3)(2): $1 = 0$. Daraus folgt: $\dim \operatorname{Bild} S_{L/K} \geq 1$, also $\operatorname{Bild} S_{L/K} = K$.

FOLGERUNG: Sei L galoissch über K, $G = \operatorname{Gal}(L/K)$ und $H \leq G$. Ist $L = \langle \alpha_1, \ldots, \alpha_m \rangle$ als K-Vektorraum, so ist $H\mathfrak{F} = \langle \beta_1, \ldots, \beta_m \rangle$ als K-Vektorraum mit

$$\beta_i = S_{L/H\mathfrak{F}}(\alpha_i) = \sum_{\sigma \in H} \alpha_i^\sigma \text{ für } i = 1, \ldots, m \qquad (*)$$

BEWEIS: Sei $R = H\mathfrak{F}$. Nach 10.6 (Algebra 1) ist $\operatorname{Gal}(L/R) = H$ und somit für $\alpha \in L$ gilt $S_{L/R}(\alpha) = \sum_{\sigma \in H} \alpha^\sigma$. Also gilt die Gleichheit (*) und $\beta_i \in R$ nach Satz (2.5.2)(1). Nach Satz existiert zu jedem $r \in R$ ein $\alpha \in L$ mit $r = S_{L/R}(\alpha)$. Da $L = \langle \alpha_1, \ldots, \alpha_m \rangle$, existieren $c_i \in K$ mit $\alpha = \sum_{i=1}^m c_i \alpha_i$, also

$$r = S_{L/R}(\alpha) = S_{L/R}\left(\sum_{i=1}^m c_i \alpha_i\right) \overset{2.5.2(1)}{=} \sum_{i=1}^m c_i S_{L/R}(\alpha_i) = \sum_{i=1}^m c_i \beta_i$$

2.5.5 Die Lagrangeschen Resolventen

Sei $n \in \mathbb{N}$ und K ein Körper mit $\operatorname{char} K \nmid n$, der die n-ten Einheitswurzeln enthält. Sei L galoissch über K vom Grad n mit zyklischer Galoisgruppe $G = \operatorname{Gal}(L/K) = \langle \sigma \rangle$ der Ordnung n.

DEFINITION: Für $\alpha \in L$ und $\varepsilon \in E_n$ nennen wir $(\varepsilon, \alpha) = \sum_{i=0}^{n-1} \varepsilon^i \alpha^{\sigma^i}$ eine *Lagrangesche Resolvente*.

SATZ:

1. $(\varepsilon, \alpha)^\sigma = \varepsilon^{-1}(\varepsilon, \alpha)$.
2. $(\varepsilon, \alpha)^n \in K$ (d.h. $(\varepsilon, \alpha) = 0$ oder n-tes Radikal)
3. $\alpha = \frac{1}{n} \sum_{\varepsilon \in E_n} (\varepsilon, \alpha)$.
4. Ist ε eine primitive n-te Einheitswurzel, so gilt $(\varepsilon, \alpha) = 0$ oder $L = K((\varepsilon, \alpha))$.

BEWEIS:

1. Es gilt

$$\begin{aligned}(\varepsilon,\alpha)^\sigma &= \left(\sum_{i=0}^{n-1}\varepsilon^i\alpha^{\sigma^i}\right)^\sigma = \sum_{i=0}^{n-1}(\varepsilon^\sigma)^i\alpha^{\sigma^{i+1}} \overset{\varepsilon\in K}{=} \sum_{i=0}^{n-1}\varepsilon^i\alpha^{\sigma^{i+1}}\\ &= \sum_{i=0}^{n-1}\varepsilon^{-1}\varepsilon^{i+1}\alpha^{\sigma^{i+1}} = \varepsilon^{-1}\sum_{i=0}^{n-1}\varepsilon^{i+1}\alpha^{\sigma^{i+1}} = \varepsilon^{-1}(\varepsilon,\alpha)\end{aligned}$$

   Die letzte Gleichheit gilt, weil $\varepsilon^n\alpha^{\sigma^n} = \alpha$, da $\varepsilon \in E_n$ und $\sigma^n = \mathrm{id}$.

2. Es gilt

$$((\varepsilon,\alpha)^n)^\sigma = ((\varepsilon,\alpha)^\sigma)^n \overset{(1)}{=} (\varepsilon^{-1}(\varepsilon,\alpha))^n = \varepsilon^{-n}(\varepsilon,\alpha)^n = (\varepsilon,\alpha)^n$$

   Also $(\varepsilon,\alpha)^n \in \langle\sigma\rangle\,\mathfrak{F} = K$.

3. Sei $E_n = \langle\varepsilon\rangle$. Für alle $i = 0,\ldots,n-1$ gilt dann

$$(\varepsilon^i,\alpha) = \alpha + \varepsilon^i\alpha^\sigma + \varepsilon^{2i}\alpha^{\sigma^2} + \ldots + \varepsilon^{(n-1)i}\alpha^{\sigma^{n-1}}$$

   Die Summe über alle Gruppenelemente ist

$$\sum_{i=0}^{n-1}(\varepsilon^i,\alpha) = n\alpha + \ldots + \alpha^{\sigma^j}\left(\sum_{i=0}^{n-1}(\varepsilon^j)^i\right) + \ldots + \alpha^{\sigma^{n-1}}\left(\sum_{i=0}^{n-1}(\varepsilon^{n-1})^i\right)$$

   Für $j = 1,\ldots,n-1$ gilt

$$\sum_{i=0}^{n-1}(\varepsilon^j)^i = \frac{(\varepsilon^j)^n - 1}{\varepsilon^j - 1} = 0$$

   Alle Summanden außer dem ersten sind also 0, es folgt: $\alpha = \frac{1}{n}\sum_{\delta\in E_n}(\delta,\alpha)$.

4. Sei $0 \neq \beta = (\varepsilon,\alpha)$. Dann folgt: $\beta^\sigma = \varepsilon^{-1}\beta$. Daraus folgt: $\beta^{\sigma^i} = \varepsilon^{-i}\beta$.

   Beweis: Induktion liefert

$$\beta^{\sigma^{i+1}} = (\beta^{\sigma^i})^\sigma = (\varepsilon^{-i}\beta)^\sigma = (\varepsilon^{-i})^\sigma\varepsilon^{-1}\beta \overset{\varepsilon\in K}{=} \varepsilon^{-(i+1)}\beta$$

   Es ist $G = \{1,\sigma,\sigma^2,\ldots,\sigma^{n-1}\}$. Es gilt $\beta^{\sigma^i} = \varepsilon^{-i}\beta \neq \beta$ für alle $i = 1,\ldots,n-1$. Wäre $K(\beta) \neq L$, so wäre $K(\beta) = (K(\beta)\mathfrak{G})\mathfrak{F}$ mit $1 \neq K(\beta)\mathfrak{G}$. Für $\sigma^i \in K(\beta)\mathfrak{G}$ wäre $\beta^{\sigma^i} = \beta$, Widerspruch.

Beispiele:

1. $K = \mathbb{R}, L = \mathbb{C}, n = 2, G = \langle\sigma\rangle$ für $\sigma : a + ib \to a - ib$. Die n-ten Einheitswurzel sind $1, -1$. Für $\alpha = a + ib$ gilt

$$\begin{aligned}(1, \alpha) &= a + ib + 1 \cdot (a - ib) = 2a \\ (-1, \alpha) &= a + ib - (a - ib) = 2ib\end{aligned}$$

   Es gilt $(-1, \alpha)^2 = -2b^2 \in K$, somit ist (2) erfüllt. Weiter gilt (3):

$$\alpha = \frac{1}{2}(2a + 2ib)$$

   Es gilt $\mathbb{C} = \mathbb{R}(2ib)$, somit ist (4) erfüllt.

2. Sei K mit $\operatorname{char} K \neq 2, f = x^2 + px + q \in K[x]$ irreduzibel und separabel, $L = K(f)$. Seien α, β Nullstellen von f, dann ist $\alpha^\sigma = \beta$ und $\beta^\sigma = \alpha$. Es gilt

$$x^2 + px + q = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$$

   Also $p = -(\alpha + \beta), q = \alpha\beta$. Weiter gilt

$$\begin{aligned}(1, \alpha) &= \alpha + \alpha^\sigma = \alpha + \beta = -p \\ (-1, \alpha) &= \alpha - \alpha^\sigma = \alpha - \beta \\ (-1, \alpha)^2 &= (\alpha - \beta)^2 = \alpha^2 - 2\alpha\beta + \beta^2 = (\alpha + \beta)^2 - 4\alpha\beta = p^2 - 4q\end{aligned}$$

   Es folgt: $(-1, \alpha) = \pm\sqrt{p^2 - 4q}$. (3) des Satzes liefert:

$$\alpha = \frac{1}{2}((1, \alpha) + (-1, \alpha)) = \frac{1}{2}\left(-p \pm \sqrt{p^2 - 4q}\right)$$

2.5.6 Kriterium für Radikalerweiterung

SATZ: Sei $n \in \mathbb{N}$ und K ein Körper mit $\operatorname{char} K \nmid n$, der die n-ten Einheitswurzeln enthält. Ist L eine galoissche Erweiterung vom Grad n von K mit zyklischer Galoisgruppe, so ist $L = K(\beta)$ mit einem n-ten Radikal β über K.

BEWEIS: Sei ε eine primitive n-te Einheitswurzel in K. Sei $\operatorname{Gal}(L/K) = \langle\sigma\rangle$. Dann existiert $\alpha \in L$ mit $(\varepsilon, \alpha) = \sum_{i=0}^{n-1} \varepsilon^i \alpha^{\sigma^i} \neq 0$, denn $1, \sigma, \ldots, \sigma^{n-1}$ sind paarweise verschiedene Automorphismen von L und $c_i = \varepsilon^i \in L$ müssten alle 0 sein, nach (2.5.3)(2), wenn $\sum_{i=0}^{n-1} \varepsilon^i \alpha^{\sigma^i} = 0$ wäre für alle $\alpha \in L$. Dann ist $\beta = (\varepsilon, \alpha)$ nach (2.5.5)(2) ein n-tes Radikal über K und $L = K(\beta)$ nach (2.5.5)(4).

2.5.7 Ultraradikale

Sei $\operatorname{char} K = p$ und $K \leq L$.

DEFINITION: $\alpha \in L$ heißt *Ultraradikal* über K genau dann, wenn $\alpha^p - \alpha \in K$, also α Nullstelle von $x^p - x - a$ für $a \in K$.

SATZ: Sei $\operatorname{char} K = p > 0, a \in K$ und α eine Nullstelle von $x^p - x - a$. Dann sind $\alpha, \alpha + 1, \ldots, \alpha + p - 1$ die sämtlichen Nullstellen dieses Polynoms und somit ist $L = K(\alpha)$ galoissch über K und $\operatorname{Gal}(L/K)$ zyklisch der Ordnung 1 oder p.

BEWEIS: Sei $k \in GF(p) \leq K$. Dann gilt

$$(\alpha+k)^p - (\alpha+k) - a = \alpha^p + k^p - \alpha - k - a \overset{\alpha \text{ Nullstelle}}{=} k^p - k \overset{k \in GF(p)}{=} k - k = 0$$

Also ist $\alpha + k$ Nullstelle von $f = x^p - x - a$. Das sind p verschiedene, also alle Nullstellen von f und somit ist f separabel über K. Nach Def. 10.5 (Algebra 1) ist $K(f) = K(\alpha)$ galoissch über K.

Für $\sigma \in G = \operatorname{Gal}(L/K)$ ist $\alpha^\sigma = \alpha + k$ mit $k \in \operatorname{GF}(p)$, da α^σ Nullstelle von $f^{\bar{\sigma}} = f$ ist. Sei $\rho : G \to (\operatorname{GF}(p), +)$ mit $\sigma \mapsto k = \alpha^\sigma - \alpha$. Ist $\sigma^\rho = k$ und $\tau^\rho = l$, so folgt:

$$\alpha^{\sigma\tau} = (\alpha^\sigma)^\tau = (\alpha + k)^\tau = \alpha^\tau + k^\tau = \alpha + l + k$$

Also ist $(\sigma\tau)^\rho = l + k = \sigma^\rho + \tau^\rho$, d.h. ρ ist Homomorphismus. Ist $\sigma \in \operatorname{Kern} \rho$, so ist $\sigma^\rho = 0$, d.h. $\alpha^\sigma = \alpha$, also $\sigma = \mathrm{id}$ (da $L = K(\alpha)$). Somit ist ρ Monomorphismus und $G \lesssim (\operatorname{GF}(p), +)$.

2.5.8 Kriterium für Ultraradikalerweiterung

SATZ: Sei $\operatorname{char} K = p > 0$ und L galoissch über K mit $[L : K] = p$. Dann existiert ein $\alpha \in L$ mit $\alpha^p - \alpha \in K$ und $L = K(\alpha)$.

BEWEIS: Sei $G = \operatorname{Gal}(L/K)$, dann ist $|G| = [L : K] = p$, d.h. G zyklisch. Sei $G = \langle \sigma \rangle$. Nach (2.5.4) ist $S_{L/K}(L) = K$, d.h. es existiert $\beta \in L$ mit $S_{L/K}(\beta) = 1$. Sei

$$\alpha = \sum_{i=1}^{p-1} i\beta^{\sigma^i} = \beta^\sigma + 2\beta^{\sigma^2} + \ldots + (p-1)\beta^{\sigma^{p-1}}$$

Es gilt

$$\alpha^\sigma = \beta^{\sigma^2} + 2\beta^{\sigma^3} + \ldots + (p-1)\beta^{\sigma^p}$$

wobei $(p-1)\beta^{\sigma^p} = -\beta^{\mathrm{id}} = -\beta$. Subtraktion liefert:

$$\alpha - \alpha^\sigma = \beta^\sigma + \beta^{\sigma^2} + \ldots \beta^{\sigma^{p-1}} + \beta = S_{L/K}(\beta) = 1$$

Also $\alpha^\sigma = \alpha - 1 \neq \alpha$, somit $\alpha \notin K$, d.h. $L = K(\alpha)$ (da $[L:K] = p$). Somit ist $\operatorname{grad} p_\alpha = p$, sei etwa

$$p_\alpha = x^p + a_k x^k + a_{k-1}x^{k-1} + \ldots + a_0 \in K[x] \text{ mit } a_k \neq 0$$

Da x^p nicht irreduzibel und $x^p - a$ nicht separabel ist, ist $k \geq 1$. Mit α ist auch α^σ Nullstelle von $p_\alpha \in K[x]$. Somit ist

$$\begin{aligned} 0 &= p_\alpha(\alpha) = \alpha^p + a_k\alpha^k + a_{k-1}\alpha^{k-1} + \ldots + a_0 \\ 0 &= p_\alpha(\alpha - 1) = \alpha^p - 1 + a_k\alpha^k - ka_k\alpha^{k-1} + \text{ Terme vom Grade } \leq k-2 \\ &\quad + a_{k-1}\alpha^{k-1} + \text{ Terme vom Grade } \leq k-2 \end{aligned}$$

Subtraktion liefert

$$0 = 1 + ka_k\alpha^{k-1} + \text{ Terme vom Grade } \leq k-2$$

Somit ist $0 = f(\alpha)$ mit $f \in K[x]$ vom Grade $\leq k-1$. Nach 4.4 (Algebra 1) gilt $p_\alpha \mid f$, wobei

$$f = ka_k x^{k-1} + 1 + \text{ Terme vom Grade } \leq k-2$$

Daraus folgt: f ist Nullpolynom. Daraus folgt: $ka_k x^{k-1} + 1 = 0$, also $k = 1$ und $a_k = -1$. Somit gilt $p_\alpha = x^p - x + a_0$, d.h. α ist ein Ultraradikal.

2.6 Auflösbarkeit von Gleichungen durch Radikale

2.6.1 Hauptsatz

Sei K ein Körper.

DEFINITION:

1. L heißt *Radikalerweiterung* von K, wenn $L = K(\alpha_1, \ldots, \alpha_r)$ mit $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1}) = K_{i-1}$ und $\operatorname{char} K \nmid n_i$ für $i = 1, \ldots, r$ (also α_i ist n-tes Radikal über K_{i-1})

2. $f \in K[x]$ heißt *durch Radikale auflösbar*, wenn $K(f)$ in einer Radikalerweiterung von K enthalten ist.

   BEMERKUNGEN:

   (a) $K(f)$ braucht selbst keine Radikalerweiterung zu sein. Zum Beispiel hat die Gleichung $x^3 = 20x + 25$ die Lösung $x_1 = 5$, die in der Cardano-Formel mit Hilfe von komplexen Zahlen dargestellt wird.

   (b) Alle Nullstellen sollen durch Radikale ausdrückbar sein.

SATZ: Sei $\operatorname{char} K = 0$ und L galoissch über K. Genau dann ist L in einer Radikalerweiterung von K enthalten, wenn $\mathrm{Gal}(L/K)$ auflösbar ist.

KOROLLAR: Sei $\operatorname{char} K = 0$. Das Polynom $f \in K[x]$ ist genau dann durch Radikale auflösbar, wenn $\mathrm{Gal}(K(f)/K)$ auflösbar ist.

2.6.2 Der Isomorphiesatz

SATZ: Sei M eine Erweiterung des Körpers K, seien L und S Zwischenkörper und sei $T = \langle L, S\rangle$. Ist L galoissch über K, so ist T galoissch über S und $\mathrm{Gal}(T/S) \simeq \mathrm{Gal}(L/L \cap S) \leq \mathrm{Gal}(L/K)$. Insbesondere ist $[T : S] = [L : L \cap S]$.

BEWEIS: Nach Definition I.10.5 ist $L = K(f)$ mit einem separablen Polynom $f \in K[x]$, $L = K(\alpha_1, \ldots, \alpha_n)$ und $f = (x - \alpha_1) \ldots (x - \alpha_n)$. Somit $T = \langle L, S\rangle = \langle K, \alpha_1, \ldots, \alpha_n, S\rangle = S(\alpha_1, \ldots, \alpha_n)$, also $T = S(f)$ und f ist nach Lemma I.9.1 separabel über S. Nach Definition I.10.5 ist T galoissch über S.

Sei $\rho : \mathrm{Gal}(T/S) \to \mathrm{Gal}(L/L \cap S);\ \sigma \mapsto \sigma|_L$ Für $\sigma \in \mathrm{Gal}(T/S)$ ist $k^\sigma = k$ für alle $k \in K$ und σ permutiert die Nullstellen $\{\alpha_1, \ldots, \alpha_n\}$ von f. Daraus folgt: $L^\sigma = L$, somit ist ρ wohldefiniert. Es gilt

$$(\sigma\tau)^\rho = (\sigma\tau)|_L = \sigma|_L \tau|_L = \sigma^\rho \tau^\rho$$

Damit ist ρ ein Homomorphismus. Weiter gilt

$$\begin{aligned} \sigma \in \operatorname{Kern} \rho \Longrightarrow \sigma|_L = \mathrm{id} &\implies \alpha_i^\sigma = \alpha_i \text{ für alle } i \\ &\implies \sigma = \mathrm{id} \text{ auf } S(\alpha_1, \ldots, \alpha_n) = T \end{aligned}$$

Somit ist ρ injektiv.

Sei nun $U := \operatorname{Bild} \rho \leq \mathrm{Gal}(L/L \cap S)$. *Behauptung:* $U^{\mathfrak{F}} = L \cap S$. *Beweis:* Trivialerweise $L \cap S \leq U^{\mathfrak{F}}$. Sei $\beta \in U^{\mathfrak{F}}$. Für $\sigma \in \mathrm{Gal}(T/S)$ ist dann $\beta^\sigma =$

$\beta^{\sigma|_L} = \beta^{\sigma^\rho} = \beta$, d.h. $\beta \in \mathrm{Gal}(T/S)\mathfrak{F} = S$, also $\beta \in L \cap S$. Es gilt somit nach I.10.6

$$U = U\mathfrak{F}\mathfrak{G} = (L \cap S)\mathfrak{G} = \mathrm{Gal}(L/L \cap S)$$

Damit ist ρ ein Isomorphismus. Mit I.10.5 folgt

$$[T : S] = |\mathrm{Gal}(T/S)| = |\mathrm{Gal}(L/L \cap S)| = [L : L \cap S]$$

2.6.3 Sukzessive abelsche Erweiterungen

SATZ: Seien $K = K_0 \leq \ldots \leq K_r = M$ Körper, K_i galoissch über K_{i-1} mit abelscher Galoisgruppe $\mathrm{Gal}(K_i/K_{i-1})$ für $i = 1, \ldots, r$ und sei $K \leq L \leq M$ mit L galoissch über K. Dann ist $\mathrm{Gal}(L/K)$ auflösbar.

BEWEIS: Induktion nach r. Für $r = 0$ ist $K = M = L$ und $\mathrm{Gal}(L/K) = 1$ auflösbar. Sei also $r \geq 1$ und die Aussage für $r - 1$ richtig. Nach (2.6.2) ist $T = \langle L, K_1 \rangle$ galoissch über K_1. In (K_1, M) sind dieselben Voraussetzungen mit $r-1$ statt r erfüllt. Nach Induktionsannahme ist also $\mathrm{Gal}(T/K_1)$ auflösbar. Sei $R = L \cap K_1$. Mit dem Isomorphiesatz (2.6.2) folgt:

(i) $\mathrm{Gal}(L/R)$ ist auflösbar.

Im Folgenden zeigen wir auch:

(ii) R ist normal über K und $\mathrm{Gal}(R/K)$ ist abelsch.

Betrachte die galoisschen Erweiterungen (K, K_1) und (K, L). Seien $\widetilde{\mathfrak{F}}, \widetilde{\mathfrak{G}}$ in $\mathrm{Gal}(K_1/K) = \widetilde{G}$ und $\mathfrak{F}, \mathfrak{G}$ in $\mathrm{Gal}(L/K) = G$ die zugehörigen Korrespondenzen.

Für (K, K_1) gilt: $R\widetilde{\mathfrak{G}} \trianglelefteq \widetilde{G}$ (da $\widetilde{G}$ abelsch). Mit I.10.9 folgt: R ist normal über K. Nach Satz I.10.11 ist $\mathrm{Gal}(R/K) \simeq \widetilde{G}/R\widetilde{\mathfrak{G}}$, also ist abelsch.

Für (K, L) gilt: Da R normal über K, folgt mit I.10.9: $R\mathfrak{G} \trianglelefteq G$ und I.10.11 sagt $G/R\mathfrak{G} \simeq \mathrm{Gal}(R/K)$. Nach (i) ist $R\mathfrak{G} = \mathrm{Gal}(L/R)$ auflösbar. Nach Satz (1.3.5)(3) ist dann G auflösbar.

2.6.4 Beweis des Hauptsatzes

LEMMA: Sei L galoissch über K mit $[L : K] = n = |\mathrm{Gal}(L/K)|$ und K enthalte die n-ten Einheitswurzeln. Ist $G = \mathrm{Gal}(L/K)$ auflösbar, so ist L eine Radikalerweiterung.

BEWEIS: Induktion nach n. Ist $n = 1$, so ist $L = K$ triviale Radikalerweiterung. Sei also $n > 1$ und Aussage für kleinere Grade richtig.

Fall 1. Es existiert R mit $K < R < L$ und R normal über K. Dann ist R galoissch über K und $\mathrm{Gal}(R/K) \overset{\text{I.10.11}}{\simeq} G/R\mathfrak{G}$ auflösbar (nach (1.3.5)(2)) von n echt teilender Ordnung. Nach Induktionsvoraussetzung ist $R = K(\alpha_1, \ldots, \alpha_r)$ eine Radikalerweiterung von K.

Offenbar ist L galoissch über R und $\mathrm{Gal}(L/R) = R\mathfrak{G} < G$ auflösbar nach (1.3.5)(1) von n echt teilender Ordnung. Nach Induktionsvoraussetzung ist $L = R(\beta_1, \ldots, \beta_s) = K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$ eine Radikalerweiterung.

Fall 2. Es existiert kein solches R, d.h. nach I.10.9 G ist einfach. Nach Lemma (1.3.8) ist dann G zyklisch von Primzahlordnung n. Nach Satz (2.5.6) ist dann $L = K(\alpha)$ mit n-tem Radikal α über K.

Beweis des Satzes:

„$\Rightarrow$“ Sei L enthalten in einer Radikalerweiterung von K, also $L \leq K(\alpha_1, \ldots, \alpha_r)$ mit $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ für $i = 1, \ldots, r$. Sei $n = \mathrm{kgV}\{n_i \mid i = 1, \ldots, r\}$ und sei $M = K_r(x^n - 1)$. Sei ε eine primitive n-te Einheitswurzel. Sei $M_0 = K, M_1 = K(\varepsilon)$ und $M_{i+1} = M_i(\alpha_i)$ für $i = 1, \ldots, r$. *Behauptung:* Voraussetzungen von (2.6.3) sind erfüllt für (K, L) und M_i statt K_i. Nach Satz (2.4.7) ist M_1 galoissch über M_0 mit abelscher Galoisgruppe. $M_{i+1} = M_i(\alpha_i)$ mit n_i-tem Radikal und $M_i \geq M_1$ enthält n_i-te Einheitswurzeln. Nach (2.5.1) ist die Erweiterung galoissch und $\mathrm{Gal}(M_{i+1}/M_i)$ zyklisch.

„$\Leftarrow$“ Sei $G = \mathrm{Gal}(L/K)$ auflösbar und $|G| = n$. Sei $\widetilde{L} = L(x^n - 1)$ und $\widetilde{K} = K(\varepsilon)$ mit primitiver n-ter Einheitswurzel $\varepsilon \in \widetilde{L}$. Offenbar ist $\widetilde{L}$ galoissch über K (denn aus $L = K(f)$ folgt: $\widetilde{L} = K(f(x^n - 1))$) und $\widetilde{L} = \left\langle L, \widetilde{K} \right\rangle$ (da $\widetilde{L} = L(\varepsilon)$). Nach (2.6.2) ist $\widetilde{L}$ galoissch über $\widetilde{K}$ und $\mathrm{Gal}(\widetilde{L}/\widetilde{K}) \simeq \mathrm{Gal}(L/L \cap \widetilde{K}) \leq \mathrm{Gal}(L/K)$ auflösbar von n teilender Ordnung. Mit Lemma ist $\widetilde{L}$ Radikalerweiterung von $\widetilde{K} = K(\varepsilon)$, also von K.

2.6.5 Der Hauptsatz für $\mathrm{char}\, K > 0$

Seien $K \leq L$ Körper, $\mathrm{char}\, K = p > 0$.

Definition: L heißt eine *Ultraradikalerweiterung* von K, wenn $L = K(\alpha_1, \ldots, \alpha_r)$, wobei entweder $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ und $p \nmid n_i$ (also α_i ist n_i-tes Radikal über $K(\alpha_1, \ldots, \alpha_{i-1})$) oder $\alpha_i^p - \alpha_i \in K(\alpha_1, \ldots, \alpha_{i-1})$ (also α_i Ultraradikal über $K(\alpha_1, \ldots, \alpha_{i-1})$) für $i = 1, \ldots, r$.

SATZ: Sei $\operatorname{char} K = p > 0$ und L galoissch über K. Genau dann ist L in einer Ultraradikalerweiterung von K enthalten, wenn $\mathrm{Gal}(L/K)$ auflösbar ist.

BEWEIS: In der Übung.

2.7 Die allgemeine Gleichung n-ten Grades.

2.7.1 Hauptsatz

DEFINITION: Sei K ein Körper (beliebiger Charakteristik) und $L = K(a_1, \ldots, a_n)$ der Körper der rationalen Funktionen in den unbestimmten $a_1, \ldots, a_n$ über K. Das Polynom

$$f = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \ldots + (-1)^n a_n \in L[x]$$

heißt *allgemeine Gleichung n-ten Grades* über K.

BEMERKUNGEN:

1. Man beachte: $f \in L[x]$, nicht $f \in K[x]$.
2. Das alternierende Vorzeichen hat technische Gründe.
3. Gesucht ist Lösung dieses Polynoms durch Radikale über L.

SATZ: Seien K, L, f wie oben. Dann ist $L(f)$ galoissch über L und $\mathrm{Gal}(L(f)/L) \simeq S_n$ die symmetrische Gruppe auf n Symbolen.

KOROLLAR: (ABEL 1826) Die allgemeine Gleichung n-ten Grades ist bei Charakteristik 0 für $n \geq 5$ nicht auflösbar durch Radikale.[11]

BEWEIS DES KOROLLARS: Nach (2.6.1) ist f auflösbar durch Radikale genau dann, wenn $\mathrm{Gal}(L(f)/L)$ auflösbar ist. Nach dem Hauptsatz ist $\mathrm{Gal}(L(f)/L) \simeq S_n$. Nach (1.3.7) ist S_n für $n \geq 5$ nicht auflösbar.

2.7.2 Symmetrische Funktionen

Seien K, L, f wie in (2.7.1). Weiter sei

$$g = (x - a_1) \ldots (x - a_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n$$

[11] Für $n = 3, 4$ ist die allgemeine Gleichung auflösbar. Tartaglia hat die Formeln für $n = 3$ gefunden und sie Cardano erzählt, der sie 1545 veröffentlicht hat.

LEMMA: (VIETASCHER WURZELSATZ) Es gilt

$$\begin{aligned} s_1 &= a_1 + \ldots + a_n = \sum_{i=1}^{n} a_i \\ s_2 &= a_1a_2 + \ldots + a_1a_n + a_2a_3 + \ldots + a_2a_n + \ldots + a_{n-1}a_n = \sum_{i<j} a_ia_j \\ s_k &= \sum_{i_1<i_2<\ldots<i_k} a_{i_1}a_{i_2}\ldots a_{i_k} \\ s_n &= a_1 \ldots a_n \end{aligned}$$

s_i heißen *elementarsymmetrische Funktionen* in den $a_1, \ldots, a_n$.

BEWEIS: Wie erhält man $s_k x^{n-k}$? Durch k Faktoren der Form $(-a_i)$ und $n-k$ Mal x.

SATZ: Sei $M = K(s_1, \ldots, s_n)$ (also $K \leq M \leq L$). Dann ist $L = M(g)$ galoissch über M und $\mathrm{Gal}(L/M) \simeq S_n$.

BEWEIS: Es gilt $g \in M[x]$ und $L = K(a_1, \ldots, a_n) = M(a_1, \ldots, a_n) = M(g)$. Da die Nullstellen von g paarweise verschieden sind, ist g separabel. Also ist L galoissch über M.

$G = \mathrm{Gal}(L/M)$ operiert nach Beispiel (1.1.2) auf $\Omega = \{a_1, \ldots, a_n\}$ (Menge der Nullstellen von g) Für $\sigma \in \mathrm{Sym}\,\Omega = G_0$ sei σ^ρ der Automorphismus von $L = K(a_1, \ldots, a_n)$, der die a_i wie σ permutiert und die Elemente aus K fest lässt (existiert, da $a_1, \ldots, a_n$ gleichwertig sind). Offenbar bleiben alle s_i fest unter σ^ρ. Somit $\sigma^\rho \in \mathrm{Gal}(L/M)$. Also $\rho : \mathrm{Sym}\,\Omega \to \mathrm{Gal}(L/M)$ mit $\sigma \mapsto \sigma^\rho$ ist wohldefiniert.

Behauptung: ρ ist ein Isomorphismus. *Beweis:*

$$\begin{aligned} a_i^{(\sigma\tau)^\rho} &= a_i^{\sigma\tau} = (a_i^\sigma)^\tau = (a_i^{\sigma^\rho})^{\tau^\rho} = a_i^{\sigma^\rho\tau^\rho} \Rightarrow (\sigma\tau)^\rho = \sigma^\rho\tau^\rho \\ \sigma \in \mathrm{Kern}\,\rho &\Rightarrow \sigma^\rho = \mathrm{id} \text{ auf } L \Rightarrow a_i = a_i^{\sigma^\rho} = a_i^\sigma \text{ für alle } i \\ &\Rightarrow \sigma = \mathrm{id} \end{aligned}$$

Somit ist ρ ein Monomorphismus. Ist $\omega \in \mathrm{Gal}(L/M)$, so permutiert ω die Nullstellen von g, d.h. induziert eine Permutation μ auf Ω. Dann ist $\omega = \mu^\rho$, d.h. ρ ist surjektiv.

KOROLLAR: Ist $h \in K(a_1, \ldots, a_n)$ symmetrisch (d.h. in invariant unter Permutationen der a_i), so ist $h \in K(s_1, \ldots, s_n) = M$, lässt sich also rational in den elementarsymmetrischen Funktionen $s_1, \ldots, s_n$ ausdrücken.[12]

BEWEIS: $h \in \mathrm{Gal}(L/M)\mathfrak{F} = M$.

BEISPIEL: Sei $n = 2$. Sei $h = a_1^2 + a_2^2$, dann gilt

$$h = a_1^2 + a_2^2 = (a_1 + a_2)^2 - 2a_1a_2 = s_1^2 - 2s_2$$

2.7.3 Beweis des Hauptsatzes

Seien K, L, f, M, g wie in (2.7.1) und (2.7.2).

IDEE: Konstruiere Isomorphismus $\varphi : L \to M$ mit $f^{\bar{\varphi}} = g$. Dann wende I.7.4 an.

BEWEIS: Sei $\varphi : L \to M$ mit $h = \frac{u}{v} \mapsto h(s_1, \ldots, s_n) = \frac{u(s_1,\ldots,s_n)}{v(s_1,\ldots,s_n)}$. Dieses ist ein Homomorphismus, falls wohldefiniert. Zu zeigen ist also zunächst:

($\star$) Ist $v \in K[a_1, \ldots, a_n]$ mit $v(s_1, \ldots, s_n) = 0$, so ist $v = 0$.

Beweis: Es gilt

$$0 = v(s_1, \ldots, s_n) = v\left(\sum a_i, \sum_{i<j} a_ia_j, \ldots\right) \in K[a_1, \ldots, a_n]$$

Setzen wir in dieses Polynom die Nullstellen $x_1, \ldots, x_n$ von f (aus $L(f)$) ein, so erhalten wir mit Lemma (2.7.2) angewandt auf f:

$$0 = v\left(\sum x_i, \sum_{i<j} x_ix_j, \ldots\right) = v(a_1, \ldots, a_n) = v$$

Zur Injektivität von φ:

$$0 = h^{\varphi} = \frac{u(s_1, \ldots, s_n)}{v(s_1, \ldots, s_n)} \Rightarrow u(s_1, \ldots, s_n) = 0 \overset{(\star)}{\Rightarrow} u = 0, \text{ d.h. } h = 0$$

Somit ist $\mathrm{Kern}\,\varphi = 0$. Setzt man $s_1, \ldots, s_n$ in die rationale Funktion $h = a_i$ ein, so erhält man $h^{\varphi} = s_i \in \mathrm{Bild}\,\varphi$. Setzt man $s_1, \ldots, s_n$ in die konstante Funktion $h = k \in K$ ein, so erhält man $h^{\varphi} = k \in \mathrm{Bild}\,\varphi$. Somit $\mathrm{Bild}\,\varphi \supseteq K(s_1, \ldots, s_n) = M$.

Nun gilt

$$f^{\bar{\varphi}} = x^n - s_1x^{n-1} + s_2x^{n-2} - \ldots + (-1)^n s_n = g$$

[12] Der allgemeine Satz gilt für Polynome $h \in K(a_1, \ldots, a_n)[x]$ und besagt, dass h in $M[x]$ liegt - siehe v.d.Waerden, S. 100.

Nach I.7.4 existiert Fortsetzung von φ zu Isomorphismus $\psi : L(f) \to M(g)$. Sei $\lambda : \mathrm{Gal}(L(f)/L) \to \mathrm{Gal}(M(g)/M)$ mit $\sigma \mapsto \psi^{-1}\sigma\psi$. Offenbar ist $\psi^{-1}\sigma\psi$ ein Automorphismus von $M(g)$ und für $a \in M$ gilt: $a^{\psi^{-1}} = a^{\varphi^{-1}} \in L$, somit

$$a^{\psi^{-1}\sigma\psi} = ((a^{\psi^{-1}})^{\sigma})^{\psi} = a^{\psi^{-1}\psi} = a$$

Also $\psi^{-1}\sigma\psi \in \mathrm{Gal}(M(g)/M)$, d.h. λ ist wohldefiniert. Zur Injektivität:

$$\sigma^{\lambda} = \tau^{\lambda} \Rightarrow \psi^{-1}\sigma\psi = \psi^{-1}\tau\psi \Rightarrow \sigma = \psi(\psi^{-1}\sigma\psi)\psi^{-1} = \psi(\psi^{-1}\tau\psi)\psi^{-1} = \tau$$

Zur Surjektivität: Für $\mu \in \mathrm{Gal}(M(g)/M)$ ist $\mu = \psi^{-1}(\psi\mu\psi^{-1})\psi = (\psi\mu\psi^{-1})^{\lambda}$. Weiter ist

$$(\sigma\tau)^{\lambda} = \psi^{-1}(\sigma\tau)\psi = (\psi^{-1}\sigma\psi)(\psi^{-1}\tau\psi) = \sigma^{\lambda}\tau^{\lambda}$$

2.7.4 Erweiterungen mit vorgegebener Galoisgruppe

SATZ: Sei G eine endliche Gruppe und p eine Primzahl oder 0. Dann existieren Körper $K \leq L$ der Charakteristik p mit L galoissch über K und $\mathrm{Gal}(L/K) \simeq G$.

BEWEIS: Nach Satz von Cayley (1.1.10) ist $G \simeq G_1 \leq S_n$ mit $n = |G|$. Sei F ein Körper der Charakteristik p, $K_0 = F(a_1, \ldots, a_n)$ Körper der rationalen Funktionen in $a_1, \ldots, a_n$ über F und $L = K_0(f)$ mit f wie in (2.7.1). Nach dem Hauptsatz ist L galoissch über K_0 mit $\mathrm{Gal}(L/K_0) \simeq S_n$. Sei $K = G_1\mathfrak{F}$, dann ist $\mathrm{Gal}(L/K) = K\mathfrak{G} = G_1\mathfrak{F}\mathfrak{G} = G_1$. [13]

2.7.5 Umkehrproblem der Galoistheorie

FRAGE: Kann in (2.7.4) $K = \mathbb{Q}$ gewählt werden?

SATZ: Ist A eine endliche abelsche Gruppe, so existiert ein galoisscher Erweiterungskörper L von $\mathbb{Q}$ mit $\mathrm{Gal}(L/\mathbb{Q}) \simeq A$

BEWEISSKIZZE: Nach dem Hauptsatz über endliche abelsche Gruppen gilt: $A = A_1 \times \ldots \times A_r$ mit A_i zyklisch der Ordnung n_i.[14] Nach dem Satz von Dirichlet (2.4.6) existieren Primzahlen $p_1, \ldots, p_r$ mit $p_i = 1 \mod n_i$ und $p_i \neq p_j$ für $i \neq j$. Sei $n = p_1 \ldots p_r$, $L = \mathbb{Q}_n$ und $G = \mathrm{Gal}(L/\mathbb{Q})$. Dann gilt $G \simeq E(\mathbb{Z}/n\mathbb{Z}) \simeq U_1 \times \ldots \times U_r$ mit $U_i \simeq E(\mathbb{Z}/p_i\mathbb{Z})$ zyklisch der Ordnung $p_i - 1$.

[13] Es ist bis heute nicht bekannt, ob man als K immer $\mathbb{Q}$ nehmen kann.

[14] Siehe z.B. *Kowalsky, Michler.*

Mit (1.0.2) folgt: es existieren $V_i \leq U_i$ mit $|U_i : V_i| = n_i$. Sei $H = V_1 \times \ldots \times V_r$, dann gilt

$$G/H \simeq U_1/V_1 \times \ldots \times U_r/V_r \simeq A_1 \times \ldots \times A_r = A$$

Sei nun $K = H\mathfrak{F}$, dann ist K normal über $\mathbb{Q}$ und $\mathrm{Gal}(K/\mathbb{Q}) \simeq G/K\mathfrak{G} = G/H \simeq A$.

2.7.6 Nichtauflösbare Gleichungen über $\mathbb{Q}$

LEMMA: Sei p eine Primzahl. Ist $G \leq S_p$ und enthält G eine Transposition und ein Element der Ordnung p, so ist $G = S_p$.

BEWEIS: S_p wird durch die Transpositionen erzeugt:

$$(a_1 \ldots a_r) = (a_1 a_2)(a_1 a_3) \ldots (a_1 a_r)$$

Sei $\tau = (ij) \in G$. Das Element $g \in G$ mit $o(g) = p$ muss wegen $|\Omega| = p$ ein Zyklus der Länge p sein, also $g = (\ldots i \ldots j \ldots)$. Dann ist $g^k = (\ldots ij \ldots)$ für geeignetes $k \in \mathbb{N}$. O.B.d.A. enthält G $\tau = (12)$ und $g = (123 \ldots p)$, dann gilt $\tau^g = (1^g 2^g) = (23)$, $(23)^g = (34)$ usw., d.h. G enthält alle Transpositionen der Form $(i, i+1)$. Für $r < s$ ist

$$(rs) = (r\ r+1) \ldots (s-1\ s)(s-2\ s-1) \ldots (r\ r+1) \in G$$

SATZ: Sei f ein irreduzibles Polynom aus $\mathbb{Q}[x]$ mit $\operatorname{grad} f = p \in \mathbb{P}$. Besitzt f genau $p-2$ reelle Nullstellen, so ist $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) \simeq S_p$.

BEWEIS: O.B.d.A. sei $\mathbb{Q}(f) \leq \mathbb{C}$. Sei $\Omega = \{\alpha \in \mathbb{Q}(f) \mid f(\alpha) = 0\}$. Da f separabel ist, sind alle Nullstellen von f verschieden, also $|\Omega| = p$. Sei $G = \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$. Nach (1.1.2) operiert G auf Ω mit $\mathrm{Kern}(\Omega, G) = 1$ (da aus $\alpha^\sigma = \alpha$ für alle $\alpha \in \Omega$ folgt: $\sigma = \mathrm{id}$ auf $\mathbb{Q}(\alpha_1, \ldots, \alpha_p) = \mathbb{Q}(f)$). Nach Satz (1.1.1) ist $G \simeq G_1 \leq \operatorname{Sym} \Omega = S_p$.

Da f irreduzibel, ist $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \operatorname{grad} f = p$ für $\alpha_i \in \Omega$. Also nach dem Gradsatz $p \mid [\mathbb{Q}(f) : \mathbb{Q}] \overset{\text{I.10.6}}{=} |G| = |G_1|$. Mit dem Satz von Sylow (1.2.1) folgt: G_1 enthält ein Element der Ordnung p.

Sei $\sigma : \mathbb{C} \to \mathbb{C}$ mit $a + ib \mapsto a - ib$. Dann ist $f^\sigma = f$ (da f reell), also $\mathbb{Q}(f)^\sigma = \mathbb{Q}(f)$. Sei $\tau : \mathbb{Q}(f) \to \mathbb{Q}(f)$ mit $\alpha \mapsto \alpha^\sigma$, also $\tau = \sigma|_{\mathbb{Q}(f)}$. Offenbar gilt $\tau \in G$.

Da σ jede nichtreelle Zahl $z \in \mathbb{C}$ bewegt, muss τ die beiden nichtreellen Nullstellen α, β von f vertauschen, d.h. $\tau = (\alpha\beta)$ bewirkt Transposition auf

Ω. Nach Lemma ist $G_1 = S_p$, also $G \simeq S_p$.

SATZ: Für jede ungerade Zahl $r \geq 3$ gibt es ein irreduzibles Polynom $f \in \mathbb{Q}[x]$ mit genau $r-2$ reellen Nullstellen, wobei $\operatorname{grad} f = r$. Für alle Primzahlen $p \geq 5$ existieren somit Polynome $f \in \mathbb{Q}[x]$ vom Grad p mit $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) \simeq S_p$, d.h. die nicht durch Radikale auflösbar sind.

BEWEIS: (R.BRAUER) Für $r = 3$ erfüllt $x^3 - 2$ die Behauptung. Sei also $r \geq 5$. Sei m eine gerade natürliche Zahl und seien $n_1 < n_2 < \ldots < n_{r-2}$ gerade Zahlen. Sei

$$g = (x^2 + m)(x - n_1) \ldots (x - n_{r-2})$$

Offenbar ist $\operatorname{grad} g = r$ und g hat die $r-2$ Nullstellen $n_1, \ldots, n_{r-2}$. Für $s \in \mathbb{Z}$ ungerade ist $|g(s)| > 2$, da $|g(s)| = |s^2 + m||s - n_1| \ldots |s - n_{r-2}|$, wobei alle Faktoren ≥ 1 und ein $|s - n_j| \geq 3$ sind.

Sei $f(x) = g(x) - 2$. Zwischen n_1 und n_{r-2} hat die Funktion g mindestens $\frac{r-3}{2}$ Maxima, die Funktion f hat dann $r-3$ Nullstellen (für jedes Maximum 2 auf dem entsprechenden Intervall) Ferner ist $f(n_{r-2}) = g(n_{r-2}) - 2 = -2$ und $\lim_{x\to\infty} f(x) = +\infty$, da f den höchsten Term x^r hat. Also existieren weitere Nullstellen $> n_{r-2}$ von f, somit hat f $r-2$ reelle Nullstellen.

Seien $\alpha_1, \ldots, \alpha_r$ sämtliche Nullstellen von f, dann ist

$$\prod_{i=1}^{r}(x - \alpha_i) = f(x) = g(x) - 2 = (x^2 + m)\prod_{i=1}^{r-2}(x - n_i) - 2$$

Mit (2.7.2) gilt:

$$\begin{aligned} \text{Koeffizient von } x^{r-1} &= -\sum_{i=1}^{r}\alpha_i = -\sum_{i=1}^{r-2} n_i \\ \text{Koeffizient von } x^{r-2} &= \sum_{i<j}^{r}\alpha_i\alpha_j = m + \sum_{i<j}^{r-2} n_i n_j \end{aligned}$$

Weiter gilt

$$\begin{aligned} \sum_{i=1}^{r}\alpha_i^2 &\overset{\text{Binom.}}{=} \left(\sum_{i=1}^{r}\alpha_i\right)^2 - 2\sum_{i<j}^{r}\alpha_i\alpha_j \\ &= \left(\sum_{i=1}^{r-2} n_i\right)^2 - 2\sum_{i<j}^{r-2} n_i n_j - 2m = \sum_{i=1}^{r-2} n_i^2 - 2m \end{aligned}$$

Wähle m so groß, das $\sum_{i=1}^{r-2} n_i^2 - 2m \leq 0$ wird. Dann ist $\sum_{i=1}^{r} \alpha_i^2 \leq 0$ und somit mindestens ein α_i nicht reell. Dann ist auch die Nullstelle $\bar{\alpha}_i$ nicht reell, somit hat f genau $r-2$ reelle Nullstellen.

Nach Eisenstein ist f irreduzibel: 2 teilt alle Koeffizienten in g, also auch in f, bis auf den von x^r und 4 teilt nicht das absolute Glied von f, da 4 das absolute Glied von g teilt.

BEISPIEL: Für $r = 5$ wähle $n_1 = -2, n_2 = 0, n_3 = 2$, dann ist $\sum_{i=1}^{3} n_i^2 = 4 + 0 + 4 = 8$. Also reicht $m = 4$, dann ist

$$f = (x^2+4)(x+2)x(x-2) - 2 = x(x^4 - 16) - 2 = x^5 - 16x - 2$$

Cardanosche Formel für $n = 2$

Sei K Körper mit $\operatorname{char} K \neq 2$, $f = x^2 + px + q$, $K(x_1, x_2) = K(f)$. Es gilt

$$f = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1 x_2$$

Daraus folgt: $(x_1 + x_2) = -p$ und $x_1 x_2 = q$. Weiter gilt:

$$(x_1 - x_2)^2 = p^2 - 4q, \quad \text{also } x_1 - x_2 = \sqrt{p^2 - 4q}$$

Daraus folgt:

$$\begin{aligned} x_1 &= \frac{1}{2}((x_1 + x_2) + (x_1 - x_2)) = \frac{1}{2}(-p + \sqrt{p^2 - 4q}) \\ x_2 &= \frac{1}{2}((x_1 + x_2) - (x_1 - x_2)) = \frac{1}{2}(-p - \sqrt{p^2 - 4q}) \end{aligned}$$

2.7.7 Die Cardanoschen Formeln für $n = 3$

Sei K_0 ein Körper, $\operatorname{char} K_0 \neq 2, 3$ und sei $K = K_0(\varepsilon)$ mit $\varepsilon = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ (dann gilt $\varepsilon^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$ und $\varepsilon^3 = 1$). Dabei ist $\sqrt{-3}$ irgendein Element α von K mit $\alpha^2 = -3$ (für $K_0 = \mathbb{Q}$ etwa $\sqrt{-3} = i\sqrt{3}$, wobei $\sqrt{3}$ die positive reelle Wurzel ist). Betrachte $L = K(a_1, a_2, a_3)$ und $f_0 = z^3 - a_1 z^2 + a_2 z - a_3 \in L[z]$, die allgemeine Gleichung 3. Grades über K.

(a) Substituiere $z = x + \frac{1}{3}a_1$ und betrachte $f = f_0\left(x + \frac{1}{3}a_1\right)$. Dann ist $L(f_0) = L(f)$ und somit $\operatorname{Gal}(L(f)/L) = \operatorname{Gal}(L(f_0)/L) \overset{2.7.1}{\simeq} S_3$. Es gilt

$$\begin{aligned} f_0\left(x + \frac{1}{3}a_1\right) &= x^3 + a_1 x^2 + \frac{1}{3}a_1^2 x + \frac{1}{27}a_1^3 - a_1 x^2 - \frac{2}{3}a_1^2 x - \frac{1}{9}a_1^3 + a_2 x + \frac{1}{3}a_1 a_2 - a_3 \\ &= x^3 + px + q \end{aligned}$$

mit

$$p = a_2 - \frac{1}{3}a_1^2 \quad \text{und} \quad q = \frac{1}{3}a_1 a_2 - \frac{2}{27}a_1^3 - a_3$$

(b) Wir betrachten also $f = x^3 + px + q$. Seien x_1, x_2, x_3 die Nullstellen von f in $L(f)$. Sei

$$d = \prod_{i<j}(x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)^{15}$$

BEHAUPTUNG: $d^2 = -4p^3 - 27q^2$.

BEWEIS: Es gilt

$$f = x^3 + px + q = (x - x_1)(x - x_2)(x - x_3) \tag{1}$$

Mit dem Vietaschen Satz (2.7.2) ergibt sich

$$\left.\begin{array}{rcl} 0 & = & x_1 + x_2 + x_3 \\ p & = & x_1x_2 + x_1x_3 + x_2x_3 \\ q & = & -x_1x_2x_3 \end{array}\right\} \tag{2}$$

Es gilt

$$f' = 3x^2 + p \overset{\text{I.8.6}}{=} (x - x_1)(x - x_2) + (x - x_1)(x - x_3) + (x - x_2)(x - x_3)$$

Setze x_1, x_2, x_3 ein:

$$\begin{array}{rcl} 3x_1^2 + p & = & (x_1 - x_2)(x_1 - x_3) \\ 3x_2^2 + p & = & (x_2 - x_1)(x_2 - x_3) \\ 3x_3^2 + p & = & (x_3 - x_1)(x_3 - x_2) \end{array}$$

Multipliziert man alle drei Gleichungen, so ergibt sich auf der rechten Seite $(-1)^3 \cdot d^2 = -d^2$, somit gilt

$$d^2 = -(3x_1^2 + p)(3x_2^2 + p)(3x_3^2 + p)$$

Ausmultiplizieren ergibt

$$d^2 = -27x_1^2x_2^2x_3^2 - 9p(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) - 3p^2(x_1^2 + x_2^2 + x_3^2) - p^3 \tag{3}$$

In dieser Formel stehen symmetrische Funktionen, die nach Korollar (2.7.2) durch elementarsymmetrische Funktionen ausgedruckt werden können.

[15] Mit dieser Wahl von d erhalten wir $L(d) = A_3\mathfrak{F}$. Der nächste Schritt wird darin bestehen, $L(f)$ ausgehend von $A_3\mathfrak{F}$ zu bestimmen.

Es gilt nach (2)

$$\begin{aligned} p^2 &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2x_1^2x_2x_3 + 2x_2^2x_1x_3 + 2x_3^2x_1x_2 \\ &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 2x_1x_2x_3 \underbrace{(x_1 + x_2 + x_3)}_{=0 \text{nach (2)}} \end{aligned}$$

Also gilt

$$p^2 = x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 \tag{4}$$

Mit (2) folgt weiter

$$0 = (x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + \underbrace{2x_1x_2 + 2x_1x_3 + 2x_2x_3}_{=2p}$$

Also

$$-2p = x_1^2 + x_2^2 + x_3^2 \tag{5}$$

Eingesetzt in (3) ergibt sich

$$d^2 = -27q^2 - 9p^3 + 6p^3 - p^3 = -4p^3 - 27q^2$$

Also

$$d = \sqrt{-4p^3 - 27q^2} \tag{6}$$

(c) Es ist $[L(f) : A_3\mathfrak{F}] = 3$ und nach (2.5.5) gilt dann $\mathrm{Gal}(L(f)/A_3\mathfrak{F}) = A_3 = \langle\sigma\rangle$ wobei $x_1^\sigma = x_2,\ x_2^\sigma = x_3,\ x_3^\sigma = x_1$. Daraus folgt

$$\begin{aligned} (1, x_1) &= x_1 + x_2 + x_3 = 0 \\ (\varepsilon, x_1) &= x_1 + \varepsilon x_2 + \varepsilon^2 x_3 \\ (\varepsilon^2, x_1) &= x_1 + \varepsilon^2 x_2 + \varepsilon x_3 \end{aligned}$$

Es gilt nach (2.5.5)(3):

$$x_1 = \frac{1}{3}((\varepsilon, x_1) + (\varepsilon^2, x_1))$$

Behauptung:

$$\begin{aligned} x_2 &= \frac{1}{3}(\varepsilon^2(\varepsilon, x_1) + \varepsilon(\varepsilon^2, x_1)) \\ x_3 &= \frac{1}{3}(\varepsilon(\varepsilon, x_1) + \varepsilon^2(\varepsilon^2, x_1)) \end{aligned}$$

Beweis: Es gilt

$$\begin{aligned} 0 &= x_1 + x_2 + x_3 \\ \varepsilon^2(\varepsilon, x_1) &= \varepsilon^2 x_1 + x_2 + \varepsilon x_3 \\ \varepsilon(\varepsilon^2, x_1) &= \varepsilon x_1 + x_2 + \varepsilon^2 x_3 \end{aligned}$$

Mit Addition ergibt sich

$$\varepsilon^2(\varepsilon, x_1) + \varepsilon(\varepsilon^2, x_1) = 0 + 3x_2 + 0 \tag{7}$$

Die andere Formel folgt genauso.

(d) BEHAUPTUNG:

$$\left.\begin{array}{rcl} (\varepsilon, x_1) & = & \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3d^2}} = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{12p^3 + 81q^2}} \\ (\varepsilon^2, x_1) & = & \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3d^2}} = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{12p^3 + 81q^2}} \end{array}\right\} \tag{8}$$

wobei dieselbe Wurzel $\sqrt{12p^2 + 81q^2}$ in beiden Formeln genommen werden muss und die 3-ten Wurzeln so zu wählen sind, dass gilt

$$(\varepsilon, x_1)(\varepsilon^2, x_1) = -3p \tag{9}$$

(7), (8) und (9) sind die Cardanoschen Formeln (veröffentlicht 1545).

BEWEIS:

$$\left.\begin{array}{rcl} d & = & (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\ & = & (x_1 - x_2)(x_1x_2 - x_2x_3 - x_1x_3 + x_3^2) \\ & = & x_1^2x_2 + x_1x_3^2 + x_2^2x_3 + x_1x_2x_3 - x_1x_2x_3 - x_1^2x_3 - x_2^2x_1 - x_2x_3^2 \end{array}\right\} \tag{10}$$

Es gilt

$$(a+b+c)^3 = a^3 + b^3 + c^3 + 3ab^2 + 3ac^2 + 3ba^2 + 3bc^2 + 3ca^2 + 3cb^2 + 6abc$$

Somit ist

$$\begin{array}{rcl} (\varepsilon, x_1)^3 & = & (x_1 + \varepsilon x_2 + \varepsilon^2 x_3)^3 \\ & = & x_1^3 + \varepsilon^3 x_2^3 + \varepsilon^6 x_3^3 + 3\varepsilon(x_1^2x_2 + x_2^2x_3 + x_1x_3^2) \\ & & +3\varepsilon^2(x_1^2x_3 + x_2^2x_1 + x_3^2x_2) + 6\varepsilon^3 x_1x_2x_3 \\ & = & x_1^3 + x_2^3 + x_3^3 - \frac{3}{2}(x_1^2x_2 + x_2^2x_3 + x_1x_3^2 + x_1^2x_3 + x_2^2x_1 + x_3^2x_2) \\ & & +\frac{3}{2}\sqrt{-3}\underbrace{(x_1^2x_2 + x_2^2x_3 + x_1x_3^2 - x_1^2x_3 - x_2^2x_1 - x_3^2x_2)}_{= d \text{ nach (10)}} + 6x_1x_2x_3 \end{array}$$

Die letzte Gleichheit gilt, da

$$\varepsilon = -\frac{1}{2} + \frac{1}{2}\sqrt{-3} \quad \text{und} \quad \varepsilon = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$$

Die Terme sind symmetrisch und können somit wieder durch elementarsymmetrische Funktionen ausgedruckt werden. Nach (2) gilt

$$\begin{aligned} 0 &= (x_1+x_2+x_3)^3 \\ &= x_1^3+x_2^3+x_3^3+3x_1x_2^2+3x_1x_3^2+3x_2x_1^2+3x_2x_3^2+3x_3x_1^2+3x_3x_2^2+6x_1x_2x_3 \\ 0 &= (x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) \\ &= x_1^2x_2+x_1^2x_3+x_2^2x_1+x_2^2x_3+x_3^2x_1+x_3^2x_2+3x_1x_2x_3 \\ q &= -x_1x_2x_3 \end{aligned}$$

Die erste Formel mit 1, die zweite mit $-\frac{9}{2}$ und die dritte mit $-\frac{27}{2}$ multipliziert und alles aufaddiert ergibt

$$-\frac{27}{2}q = x_1^3+x_2^3+x_3^3-\frac{3}{2}(x_1x_2^2+x_1x_3^2+x_2x_1^2+x_2x_3^2+x_3x_1^2+x_3x_2^2)+6x_1x_2x_3$$

Also gilt

$$(\varepsilon, x_1)^3 = -\frac{27}{2}q+\frac{3\sqrt{-3}}{2}d \overset{(6)}{=} -\frac{27}{2}q+\frac{3}{2}\sqrt{12p^3+81q^2}$$

Dieselbe Rechnung mit (ε^2, x_1) liefert ε und ε^2 vertauscht und das negative Vorzeichen.

Seien $a, \varepsilon a, \varepsilon^2 a$ die Lösungen der ersten Gleichung in (8) und $b, \varepsilon b, \varepsilon^2 b$ die Lösungen der zweiten Gleichung. *Frage:* in welcher Kombination sollen die Lösungen genommen werden? Betrachte

$$\begin{aligned} (\varepsilon, x_1)(\varepsilon^2, x_1) &= (x_1+\varepsilon x_2+\varepsilon^2 x_3)(x_1+\varepsilon^2 x_2+\varepsilon x_3) \\ &= x_1^2+\varepsilon^3 x_2+\varepsilon^3 x_3+(\varepsilon+\varepsilon^2)(x_1x_2+x_1x_3+x_2x_3) \\ &= x_1^2+x_2+x_3-(x_1x_2+x_1x_3+x_2x_3) \\ &\overset{(2),(5)}{=} -2p-p=-3p \end{aligned}$$

Beachte $\varepsilon^2+\varepsilon+1=0$, also $\varepsilon+\varepsilon^2=-1$.

Bemerkungen:

1. Das sind Formeln für beliebige Koeffizienten aus K_0.
2. Direkte Herleitung der Formel: Wir betrachten wieder $f=x^3+px+q$. Sei α eine Nullstelle dieser Gleichung und ω eine Nullstelle der Gleichung $x^2-3\alpha x-3p$. Dann ist also $\omega^2-3\alpha\omega-3p=0$, also

$$\alpha = \frac{\omega}{3}-\frac{p}{\omega} \qquad (\star)$$

Setze α aus $\star$ in f ein:

$$\begin{aligned} 0 = f(\alpha) &= \left(\frac{\omega}{3} - \frac{p}{\omega}\right)^3 + p\left(\frac{\omega}{3} - \frac{p}{\omega}\right) + q \\ &= \frac{\omega^3}{27} - \frac{p^3}{\omega^3} - 3\frac{\omega}{3}\cdot\frac{p}{\omega}\left(\frac{\omega}{3} - \frac{p}{\omega}\right) + p\left(\frac{\omega}{3} - \frac{p}{\omega}\right) + q \\ &= \frac{\omega^3}{27} - \frac{p^3}{\omega^3} + q \end{aligned}$$

Also ist ω^3 Nullstelle der Gleichung

$$0 = \frac{x}{27} - \frac{p^3}{x} + q \quad \text{oder} \quad 0 = x^2 - 27p^3 + 27qx$$

Die pq-Formel liefert:

$$x_{1,2} = -\frac{27}{2}q \pm \frac{1}{2}\sqrt{(27q)^2 + 4\cdot 27p^3} = -\frac{27}{2}q \pm \frac{3}{2}\sqrt{81q^2 + 12p^3}$$

3. Sei $K_0 \leq \mathbb{R}$. Es gibt zwei Möglichkeiten:

   - f hat eine reelle und zwei konjugiertkomplexe Lösungen, also $x_1,\ x_2 = a + ib,\ x_3 = a - ib$. Dann ist

     $$\begin{aligned} d &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = (x_1 - a - ib)(x_1 - a + ib)2ib \\ &= |x_1 - a - ib|2ib \end{aligned}$$

     Somit ist $d^2 \leq 0$. Also ist $-3d^2 \geq 0$, somit $-\frac{27}{2}q + \frac{3}{2}\sqrt{-3d^2} \in \mathbb{R}$, d.h. (ε, x_1) und (ε^2, x_1) sind reelle Radikale, also x_1 Summe reeller Radikale.

   - f hat drei reelle Lösungen x_1, x_2, x_3. Dann ist

     $$d = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in \mathbb{R}$$

     Somit ist $d^2 \geq 0$. Betrachte zwei Fälle:

     - $d = 0$, dann ist $(\varepsilon, x_1) = \sqrt[3]{-\frac{27}{2}q}$ in $\mathbb{R}$ wählbar, also x_1 durch reelle Radikale dargestellt. Man kann dann $(x - x_1)$ aus f ausklammern und weiter mit der pq-Formel reelle Darstellung von x_2, x_3 erhalten.
     - $d^2 > 0$. Dann sind alle Lösungen durch komplexe Radikale dargestellt. Dies kann nicht behoben werden, wie (2.7.8) zeigt.

2.7.8 Der „Casus irreducibilis“

SATZ: Ist $K \leq \mathbb{R}$ und $f \in K[x]$ irreduzibel vom Grad 3 mit 3 verschiedenen reellen Nullstellen, so ist f nicht durch reelle Radikale auflösbar, d.h. es existiert keine Radikalerweiterung L von K mit $K(f) \leq L \leq \mathbb{R}$.

LEMMA: Ist $K \leq \mathbb{R}$ und $\alpha \in \mathbb{R}$ ein p-tes Radikal über K für ein $p \in \mathbb{P}$, so ist $[K(\alpha) : K] = p$ oder 1.

BEWEIS: α ist Nullstelle von $x^p - a$. Sei $\alpha \notin K$. Zu zeigen ist: $x^p - a$ ist irreduzibel über K (dann folgt mit I.5.1: $[K(\alpha) : K] = p$). Sei $\varepsilon \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Dann folgt:

$$x^p - a = (x - \alpha)(x - \varepsilon\alpha) \dots (x - \varepsilon^{p-1}\alpha) \qquad (\star)$$

(da die $\varepsilon^i\alpha$ genau die Nullstellen von $x^p - a$ sind). Angenommen $x^p - a = gh$ mit $g, h \in K[x]$, wobei $1 < \operatorname{grad} g < p$. Dann ist g Produkt einiger der linearen Faktoren in $(\star)$ und somit ist das konstante Glied b von g von der Form $\varepsilon^k\alpha^m$ mit $1 < m < p$. Dann ist

$$b^p = \varepsilon^{kp}\alpha^{mp} = \alpha^{mp} = (\alpha^p)^m = a^m$$

Da $(m, p) = 1$, existieren $i, j \in \mathbb{Z}$ mit $1 = im + jp$, also

$$a = a^{im}a^{jp} = b^{ip}a^{jp} = (b^i a^j)^p$$

Somit ist $b^i a^j \in K$ eine, also die reelle Nullstelle von $x^p - a$, also $b^i a^j = \alpha$ (siehe $(\star)$). Dies ist ein Widerspruch, somit ist $x^p - a$ irreduzibel.

BEWEIS DES SATZES: Sei $f = x^3 + px + q$. Angenommen $K \leq K(f) \leq L = K(\alpha_1, \dots, \alpha_r) \leq \mathbb{R}$ mit $\alpha_i^{n_i} \in K_{i-1} = K(\alpha_1, \dots, \alpha_{i-1})$. O.B.d.A. sind alle n_i Primzahlen, denn für $\alpha_i^{pq} = a_i \in K_{i-1}$ ist α_i^p Nullstelle von $x^q - a_i$ und α_i Nullstelle von $x^p - \alpha_i^p$, man betrachte also eine Zwischenerweiterung mit α_i^p.

Sei $\alpha_0 = d = \prod_{i<j}(x_i < x_j)$. Dann ist $d^2 = -4p^3 - 27q^2 \in K$. Somit ist $K(\alpha_0, \dots, \alpha_r)$ eine Radikalerweiterung von K und immer noch in $\mathbb{R}$, da alle $x_i \in \mathbb{R}$.

K enthält keine Nullstelle von f (da f irreduzibel), $K(\alpha_0, \alpha_1, \dots, \alpha_r)$ enthält alle Nullstellen. Also existiert $s \geq 0$ so, dass $R = K(\alpha_0, \dots, \alpha_{s-1})$ keine Nullstelle enthält, aber $R(\alpha_s)$ enthält eine Nullstelle x_1. Da R keine Nullstelle enthält, ist f irreduzibel über R, also $[R(x_1) : R] = \operatorname{grad} f = 3$. Ist α_s ein p-tes Radikal mit $p \in \mathbb{P}$, so folgt nach Lemma: $[R(\alpha_s) : R] = p$. Daraus folgt mit dem Gradsatz: $R(x_1) = R(\alpha_s)$ und $p = 3$. Da $[K(\alpha_0) : K] = 2$, folgt: $s > 0$, d.h. $d = \alpha_0 \in R$.

Fall 1. $R(x_1) = R(f) = R(\alpha_s)$. Es gilt $\alpha_s^3 = a \in R$. Da $R(\alpha_s)$ ein Zerfällungskörper, also normal ist, enthält $R(\alpha_s)$ alle Nullstellen des über R irreduziblen Polynoms $x^3 - a$, also $\alpha_s, \varepsilon\alpha_s, \varepsilon^2\alpha_s$ mit ε primitive 3-te Einheitswurzel. Somit ist $\frac{\varepsilon\alpha^s}{\alpha^s} = \varepsilon \in R(\alpha_s) \leq \mathbb{R}$.

Fall 2. $R(x_1) < R(f)$. Daraus folgt: $[R(f) : R] = 6$ und $\mathrm{Gal}(R(f)/R) \simeq S_3$, d.h. es existiert $\sigma \in G$ mit $x_1^\sigma = x_2,\ x_2^\sigma = x,\ x_3^\sigma = x_3$. Es gilt

$$d^\sigma = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -d \neq d$$

Dies ist ein Widerspruch, da $d \in R$ und $\sigma \in \mathrm{Gal}(R(f)/R)$.

Beispiel: Sei $K = \mathbb{Q}$, sei $f = x^3 - 4x + 2$ irreduzibel nach Eisenstein. Es gilt $\lim_{x\to-\infty} f(x) = -\infty$, $f(0) = 2$, $f(1) = -1$ und $\lim_{x\to\infty} f(x) = \infty$, somit hat f laut dem Zwischenwertsatz drei Nullstellen.

2.7.9 Die Cardanoschen Formeln für $n = 4$

Sei K_0 ein Körper mit $\mathrm{char}\, K_0 \neq 2, 3$, sei $K = K_0(\varepsilon)$ mit primitiver 3-ter Einheitswurzel ε. Sei

$$f_0 = z_4 - a_1 z^3 + a_2 z^2 - a_3 z + a_4$$

(a) Die Substitution $z = x + \frac{1}{4}a$ liefert:

$$f = x^4 + px^2 + qx + r$$

mit $p, q, r \in L = K(a_1, \ldots, a_r)$. Es gilt nämlich

$$p = a_2 - \frac{3}{8}a_1^2; \quad q = \frac{1}{2}a_1a_2 - \frac{1}{8}a_1^3 - a_3; \quad r = a_4 + \frac{1}{16}a_1^2a_2 - \frac{1}{4}a_1a_3 - \frac{3}{256}a_1^4$$

(b) Es gilt $V_4 < A_4 < S_3$, wobei $V_4 = \{(12)(34), (13)(24), (14)(23), 1\}$. Seien

$$\left.\begin{array}{rcl} \delta_1 &=& (x_1 + x_2)(x_3 + x_4) \\ \delta_2 &=& (x_1 + x_3)(x_2 + x_4) \\ \delta_3 &=& (x_1 + x_4)(x_2 + x_3) \end{array}\right\} \tag{1}$$

Dann ist δ_1 invariant unter V_4 und (12) (also im Fixkörper einer 8-Sylowgruppe), δ_2 invariant unter V_4 und (13) und δ_3 invariant unter V_4 und (14). Somit liegen δ_i in den drei Fixkörpern der 8-Sylowgruppen. Sei

$$g = (x - \delta_1)(x - \delta_2)(x - \delta_3) = x^3 - t_1x^2 + t_2x - t_3$$

wobei t_i elementarsymmetrische Funktionen von δ_i und symmetrische Funktionen von x_i sind. Es gilt

$$g = x^3 - 2px^2 + (p^2 - 4r)x + q^2 \tag{2}$$

Diese Gleichung heißt *kubische Resolvente* der Gleichung 4 Grades. (2) kann man mit Hilfe der Cardanoschen Formel lösen und erhält Radikale in p, q, r. Das liefert $L(\delta_1, \delta_2, \delta_3) = V_4\mathfrak{F}$.

(c) $V_4\mathfrak{F}$ liegt in 3 Körpern vom Grad 2 unter $L(f)$, die invariant unter den Involutionen der V_4 (aber nicht der ganzen V_4) sind. Seien

$$\alpha_1 = x_1 + x_2, \quad \alpha_2 = x_1 + x_3, \quad \alpha_3 = x_1 + x_4$$

Dann gilt wegen $\delta_1 = (x_1 + x_2)(x_3 + x_4)$ und $x_1 + x_2 + x_3 + x_4 = 0$ (Vieta):

$$\delta_1 = (x_1 + x_2)(-(x_1 + x_2)) = -\alpha_1^2$$

Analog für α_2 und α_3. Es gilt also:

$$\alpha_1 = \sqrt{-\delta_1}; \quad \alpha_2 = \sqrt{-\delta_2}; \quad \alpha_3 = \sqrt{-\delta_3} \tag{3}$$

Ferner gilt

$$\alpha_1 + \alpha_2 + \alpha_3 = 2x_1 + x_1 + x_2 + x_3 + x_4 = 2x_1$$

also

$$x_1 = \frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3) = \frac{1}{2}\left(\sqrt{-\delta_1} + \sqrt{-\delta_2} + \sqrt{-\delta_3}\right)$$

Genauso

$$\alpha_1 - \alpha_2 - \alpha_3 = x_1 + x_2 + x_2 + x_4 + x_2 + x_3 = 2x_2$$

also $x_2 = \frac{1}{2}(\alpha_1 - \alpha_2 - \alpha_3)$. Insgesamt ergibt sich

$$\left.\begin{aligned} x_1 &= \frac{1}{2}\left(\sqrt{-\delta_1} + \sqrt{-\delta_2} + \sqrt{-\delta_3}\right) \\ x_2 &= \frac{1}{2}\left(\sqrt{-\delta_1} - \sqrt{-\delta_2} - \sqrt{-\delta_3}\right) \\ x_3 &= \frac{1}{2}\left(-\sqrt{-\delta_1} + \sqrt{-\delta_2} - \sqrt{-\delta_3}\right) \\ x_4 &= \frac{1}{2}\left(-\sqrt{-\delta_1} - \sqrt{-\delta_2} + \sqrt{-\delta_3}\right) \end{aligned}\right\} \tag{4}$$

Es gilt

$$\left.\begin{aligned} \alpha_1\alpha_2\alpha_3 &= (x_1+x_2)(x_1+x_3)(x_1+x_4) \\ &= \underbrace{x_1^3+x_1^2(x_2+x_3+x_4)}_{=0} + x_1\left(\prod_{i<j} x_i x_j\right) + x_2x_3x_4 \\ &= -q \end{aligned}\right\} \quad (5)$$

Somit sind zwei Vorzeichen in (3) wählbar, das dritte muss so gewählt werden, dass (5) erfüllt ist.

3 Geordnete Körper

Eines der Ergebnisse der Theorie ist der folgende Satz:

SATZ VON ARTIN-SCHREIER (1927): Sei A ein algebraisch abgeschlossener Körper. Ist K ein echter Teilkörper von A und $[A : K] < \infty$, so ist $[A : K] = 2$ und $A = K(i)$ mit $i^2 = -1$. Die Menge S der Quadrate ungleich 0 in K ist abgeschlossen unter Addition und $K = S \dot\cup \{0\} \dot\cup -S$.

FOLGERUNGEN:

1. $\operatorname{char} A = 0$ (denn aus $\operatorname{char} K = p$ folgt mit $1 = 1^2 \in S$, dass $0 = p \cdot 1 \in S$)
2. $\operatorname{Aut} A$ hat höchstens nur endliche Untergruppen der Ordnung 1 oder 2:

$$U \leq \operatorname{Aut} A \text{ und } |U| < \infty \overset{\text{I.10,4}}{\Longrightarrow} [A : U\mathfrak{F}] = |U|$$

3.8 Geordnete Gruppen, Ringe und Körper

3.8.1 Geordnete Gruppen

Sei $(G, +)$ eine abelsche Gruppe.

DEFINITION: $P \subseteq G$ heißt *Positivbereich* von G, wenn gilt:

1. $P + P \subseteq P$
2. $0 \notin P$
3. $G = P \cup \{0\} \cup -P$

Ist P ein Positivbereich von G, so heißt G *geordnet* durch P. Die Elemente aus P heißen *positiv*, die aus $-P$ *negativ*.

BEISPIELE:

1. $(\mathbb{Z}, +)$ mit $P = \mathbb{N}$
2. $(\mathbb{Q}, +)$ mit $P = \{a \in \mathbb{Q} \mid a > 0\}$
3. $(\{a \in \mathbb{Q} \mid a > 0\}, \cdot)$ mit $P = \{a \in \mathbb{Q} \mid a > 1\}$

BEMERKUNGEN:

1. $P \cap -P = \emptyset$ (deshalb sind die Namen „positiv“ und „negativ“ sinnvoll): Wäre $a \in P \cap -P$, so wäre $-a \in P$, also $0 = a + (-a) \in P$, Widerspruch.

2. Mit P ist auch $-P$ ein Positivbereich: Für $a, b \in P$ ist $(-a) + (-b) = -(a + b) \in -P$.

3.8.2 Geordnete Ringe (und Körper)

Sei R ein (nicht notwendig kommutativer) Ring.

DEFINITION: $P \subseteq R$ heißt *Positivbereich*, wenn gilt:

1 - 3 Wie in (3.8.1), d.h. P ist ein Positivbereich der additiven Gruppe $(R, +)$.

4 $P \cdot P \subseteq P$

Weiter wie in Definition (3.8.1).

BEMERKUNG: Hier ist $-P$ kein Positivbereich, wenn P einer ist, denn für $a \in P$ ist $(-a)(-a) = a^2 \in P$, also $(-a)(-a) \notin P$.

SATZ: Ist P ein Positivbereich des Ringes R und definieren wir für $a, b \in R$

$$a < b :\Leftrightarrow b - a \in P \ (\Leftrightarrow: b > a)$$

so gilt für alle $a, b, c \in R$:

(1') $a < b,\ b < c \Rightarrow a < c$

(2') $a \not< a$

(3') $a < b$ oder $a = b$ oder $a > b$

(4') $a < b \Rightarrow a + c < b + c$ (Monotonie)

(5') $a < b,\ 0 < c \Rightarrow ac < bc$

Mit (1') - (3') ist $(R, <)$ vollständig geordnet, also eine Kette.

Ist Umgekehrt $<$ eine Relation auf R mit (1') - (5'), so ist $P = \{a \in R \mid 0 < a\}$ ein Positivbereich von R.

BEWEIS:

(1') Ist $a < b,\ b < c$, so gilt: $(c-a) = \underbrace{(c-b)}_{\in P} + \underbrace{(b-a)}_{\in P} \in P \Rightarrow a < c$

(2') $a - a = 0 \notin P \Rightarrow a \not< a$

(3') Aus $a \neq b$ folgt mit (3): entweder $a - b \in P$ (also $a < b$) oder $b - a \in P$ (also $a - b \in P$, somit $a > b$)

(4') $(b + c) - (a + c) = (b - a) \in P$, also $b + c > a + c$

(5') Ist $(b - a) \in P,\ c \in P$, so ist $(b - a)c = bc - ac \in P$, also $bc > ac$.

Beweis der Umkehrung:

1. $P + P \subseteq P$:

$$a, b \in P \Rightarrow 0 < a = a + 0 < a + b \Rightarrow 0 < a + b \Rightarrow a + b \in P$$

2. Nach (2') ist $0 \not< 0$, also $0 \notin P$

3. Für $a \in R$ ist $a = 0$ oder $0 < a$ oder $a < 0$. Mit (4') ist im letzten Fall $a + (-a) < 0 + (-a)$, also $0 < -a$, d.h. $-a \in P$.

4. Für $0 < a, 0 < b$ ist $0 = 0 \cdot b < ab$, also $ab \in P$.

BEISPIELE:

1 - 3 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind geordnet durch die natürlichen positiven Zahlen.

4 $\mathbb{C}$ besitzt keinen Positivbereich. *Beweis:* Angenommen P wäre einer. Dann ist $i \in P$ oder $i \in -P$, also $-1 = i^2 = (-i)^2 \in P$. Auch $1 \in P$ oder $1 \in -P$, also $1 = 1^2 = (-1)^2 \in P$, somit ist $0 = 1 - 1 \in P$, Widerspruch.

3.8.3 Polynomringe

SATZ: Ist P ein Positivbereich des Integritätsbereiches R, so ist

$$\tilde{P} = \left\{ f \in R[x] \;\middle|\; f = \sum_{i=0}^{n} a_i x^i \text{ und } a_n \in P \right\}$$

ein Positivbereich von $R[x]$.

BEWEIS: Seien $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} a_j x^j \in \tilde{P}$ und etwa $a_n, b_m \in P$, so ist a_n, b_m oder $a_n + b_m$ höchster Koeffizient von $f + g$, also $f + g \in \tilde{P}$; ferner

$a_n b_m \in P$ der von fg, d.h. $fg \in \tilde{P}$. Somit gelten (1) und (4). Da $0 \notin \tilde{P}$, so gilt (2). Ist $f \in R[x]$, so ist entweder $a_n \in P$ (also $f \in \tilde{P}$) oder $a_n = 0$ (also $f = 0$) oder $a_n \in -P$ (also $-f \in \tilde{P}$). Somit gilt (3).

BEMERKUNG: Das ist im allgemeinen keineswegs die einzige Anordnung von $R[x]$ (siehe nächstes Beispiel).

BEISPIEL:

5 Sei $\tau \in \mathbb{R}$ transzendent über $\mathbb{Q}$. Dann ist $P_\tau = \{ f \in \mathbb{Q}[x] \mid f(\tau) > 0\}$ ein Positivbereich von $\mathbb{Q}[x]$. Für $\tau_1 \neq \tau_2$ ist $P_{\tau_1} \neq P_{\tau_2}$, d.h. $\mathbb{Q}[x]$ besitzt überabzählbar viele verschiedene Anordnungen.

Beweis: Sind $f, g \in P_\tau$, so ist $(f+g)(\tau) = f(\tau) + g(\tau) > 0$, also $f + g \in P_\tau$, genauso mit fg statt $f + g$. Somit gelten (1) und (4). Trivialerweise ist $0 \notin P_\tau$, denn $0(\tau) = 0$. Sei nun $f \in \mathbb{Q}[x], f \neq 0$. Da τ transzendent, folgt: $f(\tau) \neq 0$, also $f \in P$ oder $-f \in P$. Somit gilt (3).

Sind nun $\tau_1 \neq \tau_2$, etwa $\tau_1 < \tau_2$, dann existiert $r \in \mathbb{Q}$ mit $\tau_1 < r < \tau_2$. Sei $f = x - r \in \mathbb{Q}[x]$, dann ist $f(\tau_2) > 0$, also $f \in P_{\tau_2}$ und $f(\tau_1) < 0$, also $f \neq P_{\tau_1}$.

3.8.4 Grundeigenschaften geordneter Gruppen, Ringe und Körper

SATZ: Jede geordnete Gruppe ist *torsionsfrei* , d.h. hat außer der 0 keine Elemente endlicher Ordnung. Jeder geordnete Ring ist nullteilerfrei. Jeder geordnete Körper hat Charakteristik 0.

BEWEIS: Sei P ein Positivbereich der Gruppe G bzw. des Ringes R bzw. des Körpers K.

1. Angenommen $0 \neq a \in G$ hat endliche Ordnung. Dann existiert $n \in \mathbb{N}$ mit $na = 0$ und $n(-a) = 0$. Sei o.B.d.A $a \in P$. Dann ist $0 = na \in P$, Widerspruch.

2. Angenommen $ab = 0$ mit $a \neq 0 \neq b$. Dann folgt: $(-a)(-b) = (-a)b = a(-b) = 0$. Somit existieren solche a, b mit $a, b \in P$. Dann ist aber $0 = ab \in P$, Widerspruch.

3. Ist $\operatorname{char} K = p > 0$, so ist p die Ordnung von 1 in $(K, +)$. Mit (1) ergibt sich ein Widerspruch.

3.8.5 Eigenschaften geordneter Körper

Sei P ein Positivbereich des Ringes (oder Körpers) R.

DEFINITION: Für $a \in R$ sei $|a| = a$ falls $a \in P$ und $|a| = -a$ sonst.

LEMMA: Für $a, b, c \in R$ und $a_i \in R$ gilt:

(a) Ist $a \neq 0$, so ist $a^2 \in P$, ferner $\sum a_i^2 \in P$, falls eines der $a_i \neq 0$.

(b) $a < b \Rightarrow -a > -b$

(c) $0 < a < b \Rightarrow 0 < a^2 < b^2$ und $0 < \frac{1}{b} < \frac{1}{a}$, falls Inverse existieren

(d) $1 < a \Rightarrow a < a^2$ und $0 < a < 1 \Rightarrow a^2 < a$

(e) $a < b,\ c < d \Rightarrow a + c < b + d$

(f) $|ab| = |a| \cdot |b|$

(g) $|a + b| \leq |a| + |b|$

BEWEIS:

(a) Ist $a \neq 0$, so ist $a \in P$ oder $-a \in P$. Daraus folgt: $a^2 = (-a)^2 \in P$.

3.8.6 Eindeutigkeit der Anordnung von $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

SATZ: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ besitzen jeweils nur einen Positivbereich (als Ringe), sind also nur auf eine Weise anordbar.

LEMMA: Sind P_1, P_2 Positivbereiche mit $P_1 \subseteq P_2$, so ist $P_1 = P_2$.

BEWEIS: Angenommen $P_1 \neq P_2$. Dann existiert $a \in P_2 \setminus P_1$. Dann ist $a \neq 0$ und somit $a \in -P_1$ nach (3). Daraus folgt: $-a \in P_1 \subseteq P_2$, also $0 = a - a \in P_2$.

BEWEIS DES SATZES: Sei P ein Positivbereich von $\mathbb{Z}$ bzw. $\mathbb{Q}, \mathbb{R}$.

1. Für $\mathbb{Z}$: Es gilt $1 = 1 \cdot 1 \in P$ nach (3.8.5)(a). Mit trivialer Induktion folgt: $n \cdot 1 \in P$, also $\mathbb{N} \subseteq P$. Mit dem Lemma folgt: $\mathbb{N} = P$.

2. Für $\mathbb{Q}$: Genauso wie oben folgt: $\mathbb{N} \subseteq P$. Nach (3.8.5)(c) gilt: $\frac{1}{m} \in P$ für alle $m \in \mathbb{N}$, also mit (4): $\frac{n}{m} = n \cdot \frac{1}{m} \in P$ für alle $n, m \in \mathbb{N}$.

3. Für alle $a \in \mathbb{R}$ mit $a > 0$ existiert $b \in P$ mit $a = b^2$, also $a \in P$. Somit gilt $\{a \in \mathbb{R} \mid a > 0\} \subseteq P$. Wende nun das Lemma an.

3.8.7 Einschränkung und Fortsetzung von Anordnungen

Sei P ein Positivbereich des Ringes R.

LEMMA: Ist $T \leq R$, so ist $P \cap T$ ein Positivbereich des Ringes T.

BEWEIS: (1), (2), (4) sind trivial. Zu (3): Sei $a \in T$, dann gibt es drei Fälle: $a \in P$ (also $a \in P \cap T$) oder $a = 0$ oder $a \in -P$ (also $-a \in P \cap T$, d.h. $a \in -(P \cap T)$). Somit gilt: $P \cap T$ erfüllt (3).

DEFINITION: Seien P und P' Positivbereiche der Ringe R bzw. R' und sei $R \leq R'$. Die Anordnung P' auf R' *setzt* die Anordnung P von R *fort* , wenn $P' \cap R = P$, d.h. wenn für alle $a, b \in R$ gilt:

$$a < b \Leftrightarrow b - a \in P \Leftrightarrow b - a \in P' \Leftrightarrow a <' b$$

BEISPIELE:

(a) Die Anordnung auf $\mathbb{R}$ setzt die Anordnungen von $\mathbb{Q}$ und $\mathbb{Z}$ fort.

(b) Ist R durch P geordnet, so setzt $\tilde{P}$ aus (3.8.3) P auf $R[x]$ fort. *Beweis:* $\tilde{P} \cap R = P$, da ein konstantes Polynom $a_0 \in R$ genau dann in $\tilde{P}$ liegt, wenn sein höchster Koeffizient a_0 in P liegt.

(c) Betrachte $\mathbb{Q}[x], \tau \in \mathbb{R}$ transzendent über $\mathbb{Q}$ und $P_\tau = \{ f \in \mathbb{Q}[x] \mid f(\tau) > 0\}$ (vergleiche (3.8.3)). Dann setzt P_τ die Anordnung von $\mathbb{Q}$ fort, denn es gilt $a_0(\tau) = a_0$.

SATZ: Jede Anordnung eines Integritätsbereichens R lässt sich auf genau eine Weise zu einer Anordnung des Quotientenkörpers Q von R fortsetzen, nämlich durch $rs^{-1} \in P^* \Leftrightarrow rs \in P$.

BEMERKUNG: Diese Definition ist wohldefiniert: Ist $rs^{-1} = uv^{-1}$, so ist $rv = us$, also $rsv^2 = uvs^2$ und wegen (3.8.5)(a) folgt: $rs \in P \Leftrightarrow uv \in P$.

BEWEIS: *Eindeutigkeit:* Angenommen P^* ist ein Positivbereich von Q, der P fortsetzt. Sei $a \in Q$, etwa $a = \frac{r}{s}$ mit $r, s \in R, s \neq 0$. Dann gilt:

$$a = \frac{r}{s} \in P^* \overset{(3.8.5a)}{\Longleftrightarrow} \frac{r}{s} \cdot s^2 = rs \in P^* \overset{P=P^* \cap R}{\Longleftrightarrow} rs \in P$$

Somit ist $a \in P^*$ genau dann, wenn $r, s \in R$ existieren mit $a = \frac{r}{s}$ und $rs \in P$.

Existenz: Sei $P^* = \left\{ a \in \mathbb{Q} \mid \exists r, s \in R \text{ mit } a = \frac{r}{s} \text{ und } rs \in P \right\}$. Zu (1) und

(4): Sei $a, b \in P^*$, also $a = \frac{r}{s}, b = \frac{u}{v}$ mit $r, s, u, v \in R$ und $rs, uv \in P$. Dann gilt

$$\begin{aligned} a+b &= \frac{rv+us}{sv} \text{ und } (rv+us)sv = rsv^2 + uvs^2 \in P \text{ nach (3.8.5)(a)} \\ &\Rightarrow a+b \in P^* \\ ab &= \frac{ru}{sv} \text{ und } (ru)(sv) = (rs)(uv) \in P \Rightarrow ab \in P^* \end{aligned}$$

Zu (2): Ist $0 = \frac{r}{s}$, so ist $r = 0$, also $rs \notin P$, also gilt $0 \notin P^*$.

Zu (3): Sei $a = \frac{r}{s} \in Q$ für $r, s \in R$. Dann gibt es drei Fälle: $rs \in P$ (also $a \in P^*$) oder $rs = 0$ (also $a = 0$) oder $rs \in -P$ (also $-rs \in P$, d.h. $-a = \frac{-r}{s} \in P^*$).

KOROLLAR: Ist K ein durch P geordneter Körper, so ist

$$\tilde{P}^* = \left\{ \frac{f}{g} \;\middle|\; f = \sum_{i=0}^{n} a_i x^i,\ g = \sum_{j=0}^{m} b_j x^j \in K[x] \text{ und } a_n b_m \in P \right\}$$

ein Positivbereich des Körpers der rationalen Funktionen $K(x)$ über K.

BEWEIS: Es ist nach (3.8.3)

$$\tilde{P} = \left\{ f \in K[x] \;\middle|\; f = \sum_{i=0}^{n} a_i x^i \text{ und } a_n \in P \right\}$$

Sei $g = \sum_{j=0}^{m} b_j x^j$, dann gilt

$$\frac{f}{g} \in \tilde{P}^* \Leftrightarrow fg \in \tilde{P} \Leftrightarrow a_n b_m \in P$$

BEMERKUNG: P_τ^* lässt sich beschreiben als $P_\tau^* = \{\varphi \in \mathbb{Q}(x) \mid \varphi(\tau) > 0\}$

3.8.8 Isomorphismen und Anordnung

LEMMA: Ist P ein Positivbereich des Ringes R und $\sigma : R \to S$ ein Ringisomorphismus, so ist P^σ ein Positivbereich von S.

BEWEIS: Sind $a, b \in P^\sigma$, so ist $a = u^\sigma$ und $b = v^\sigma$ mit $u, v \in P$. Dann gilt $a \dot{+} b = u^\sigma \dot{+} v^\sigma = (u \dot{+} v)^\sigma$. Somit gelten (1) und (4). Zu (2): $0 \notin P^\sigma$, da $0 \notin P$ und σ injektiv. Zu (3): Ist $a \in S$, so existiert $u \in R$ mit $u^\sigma = a$. Es gibt dann drei Fälle: $u \in P$ (also $a \in P^\sigma$) oder $u = 0$ (also $a = 0$) oder $u \in -P$ (also $a = -(-u)^\sigma \in -P^\sigma$).

BEMERKUNG: Ist $f \in Q[x]$ und $\alpha \in \mathbb{R}$ mit $f(\alpha) = 0$, so ist $\mathbb{Q}(\alpha) \leq \mathbb{R}$ geordnet nach Lemma (3.8.7). Ist $f(\beta) = 0$, so existiert nach I.4.4 ein Isomorphismus $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. Lemma (3.8.8) liefert Anordnung auf $\mathbb{Q}(\beta)$.

BEISPIEL:

6. Sei $f = x^4 - 2$. Sei $\alpha = \sqrt[4]{2} \in \mathbb{R}$ positiv. Sei $\beta = i\alpha$, dann erhält $\mathbb{Q}(\beta)$ Ordnung über $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ mit $\alpha \mapsto \beta$. Es gilt z.B.

$$\begin{aligned} \beta - \beta^2 &= i\sqrt[4]{2} + \sqrt{2} < 0, \text{ da } (\beta - \beta^2)^{\sigma^{-1}} = \alpha - \alpha^2 = \sqrt[4]{2} - \sqrt{2} < 0 \text{ in } \mathbb{R} \\ \beta + \beta^2 &= i\sqrt[4]{2} - \sqrt{2} > 0, \text{ da } \alpha + \alpha^2 > 0 \end{aligned}$$

DEFINITION: Seien P und P' Positivbereiche der Ringe R bzw. R'. Die Abbildung $\sigma : R \to R'$ heißt *Ordnungsisomorphismus* (bezüglich P und P'), wenn σ ein Isomorphismus des Ringes R auf den Ring R' ist und $P^\sigma \subseteq P'$ gilt (nach Lemma (3.8.6) also $P^\sigma = P'$), also $a < b \Leftrightarrow a^\sigma <' b^\sigma$ für alle $a, b \in R$.

BEISPIELE:

7. $\mathbb{Q}(\sqrt{2})$ hat genau zwei (isomorphe) verschiedene Anordnungen. Betrachte $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ mit $a+b\sqrt{2} \mapsto a-b\sqrt{2}$. Sei P der Positivbereich, der zu von $\mathbb{R}$ induzierten Anordnung gehört. Dann gilt: $\sqrt{2} \in P$, also $-\sqrt{2} \in P^\sigma$, d.h. $\sqrt{2} \notin P^\sigma$. Somit sind P und P^σ verschiedene Anordnungen von $\mathbb{Q}(\sqrt{2})$ und σ ist Ordnungsisomorphismus zwischen den beiden.

- $\mathbb{Q}[x]$ mit P_τ^* ist isomorph zu $Q(x)$ mit P_σ^* genau dann, wenn $\mathbb{Q}(\tau) = \mathbb{Q}(\sigma)$. *Beweis:* in der Übung.

3.8.9 Anordnung transzendenter Erweiterungen

SATZ: Ist K ein durch P geordneter Körper und α transzendent über K, so ist

$$\tilde{P}^* = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f = \sum_{i=0}^{n} a_i x^i,\ g = \sum_{j=0}^{m} b_j x^j \in K[x] \text{ und } a_n b_m \in P \right\}$$

ein Positivbereich von $K(\alpha)$

BEWEIS: Korollar (3.8.7) + Lemma (3.8.8) + I.4.3.

3.9 Archimedische Anordnungen

3.9.1 Archimedisch geordnete Gruppen (und Körper)

DEFINITIONEN:

1. Eine geordnete Gruppe $(G, <)$ heißt *archimedisch geordnet* , wenn es für alle $a, b \in G$ mit $a, b > 0$ ein $n \in \mathbb{N}$ gibt mit $b < na$.

2. Ein geordneter Ring (Körper) R heißt *archimedisch geordnet*, wenn seine additive Gruppe $(R, +)$ archimedisch geordnet ist.

BEISPIELE:

1. Jede Untergruppe und jeder Teilkörper von $\mathbb{R}$ ist archimedisch geordnet, da $(\mathbb{R}, +)$ die Eigenschaft (1) hat.

2. Die Anordnung aus (3.8.9) für $\mathbb{Q}(\alpha)$ mit α transzendent über $\mathbb{Q}$ ist nicht archimedisch: Sei $b = \alpha, a = 1 \in \tilde{P}^*$. Es gilt $\alpha - na \in \tilde{P}^*$ für alle $n \in \mathbb{N}$, da höchster Koeffizient gleich 1 ist. Somit ist $\alpha > n$ für alle $n \in \mathbb{N}$. Ist $\alpha \in \mathbb{R}$, so hat $\mathbb{Q}(\alpha)$ nach (1) auch eine archimedische Anordnung.

3.9.2 Ganzzahlig einschließbare Elemente, Dichtheit

Sei K ein geordneter Schiefkörper. Dann ist $\mathbb{Z} \leq \mathbb{Q} \leq Z(K) \leq K$.

DEFINITIONEN:

1. Ein Element $a \in K$ heißt *ganzzahlig einschließbar*, wenn es $n \in \mathbb{N}$ gibt mit $-n < a < n$.

   BEMERKUNG: Elemente, die nicht ganzzahlig einschließbar sind, nennt man *unendlich groß* und ihre multiplikativen inversen *unendlich klein*. Z.B. x in $(K(x), \tilde{P}^*)$ ist unendlich groß und $\frac{1}{x}$ ist unendlich klein.

2. $\mathbb{Q}$ ist *dicht* in K genau dann, wenn für alle $a, b \in K$ mit $a < b$ ein $q \in \mathbb{Q}$ existiert mit $a < q < b$.

SATZ: Sei K ein geordneter Schiefkörper. Dann sind äquivalent:

1. K ist archimedisch geordnet.
2. Jedes Element aus K ist ganzzahlig einschließbar.
3. $\mathbb{Q}$ ist dicht in K.

BEWEIS:

(1) $\Rightarrow$ (2) Sei $b \in K$. Ist $b > 0$, so existiert nach Definition (3.9.1) ein $n \in \mathbb{N}$ mit $b < n \cdot 1 = n$. Also $-n < 0 < b < n$. Ist $b < 0$, so ist $-b > 0$, also existiert $n \in \mathbb{N}$ mit $-n < -b < n$, also nach (3.8.5)(b) $-n < b < n$.

(2) $\Rightarrow$ (3) Seien $a, b \in K$ mit $a < b$. Dann ist $b - a > 0$. Nach (3.8.5)(c) ist dann $(b-a)^{-1} > 0$ und nach Voraussetzung existiert $n \in \mathbb{N}$ mit $(b-a)^{-1} < n$, also $0 < \frac{1}{n} < b - a$. Nach Voraussetzung existiert $k \in \mathbb{Z}$ mit $-k < na < k$. Somit existiert die kleinste ganze Zahl m mit $na < m$, also $m - 1 \leq na < m$. Somit gilt

$$a < \frac{m}{m} = \frac{m-1}{n} + \frac{1}{n} < a + (b-a) = b$$

Also $q = \frac{m}{n}$ tut das Verlangte.

(2) $\Rightarrow$ (3) Seien $a, b \in K$ mit $0 < a, b$. Nach Voraussetzung existiert $r \in \mathbb{Q}$ mit $0 < r < a$ und $s \in \mathbb{Q}$ mit $b < s \ (< b + b)$. Da $\mathbb{Q}$ archimedisch geordnet ist, existiert $n \in \mathbb{N}$ mit $nr > s$, also $b < s < nr < na$.

3.9.3 Satz von HILBERT

SATZ: Ein archimedisch geordneter Schiefkörper ist ein Körper.

BEWEIS: Sei S ein nichtkommutativer archimedisch geordneter Schiefkörper. Dann existieren $a, b \in S$ mit $ab \neq ba$, also etwa $ab < ba$. Offenbar ist $(-a)(-b) = ab < ba = (-b)(-a)$. Wir können also $a > 0$ annehmen. Nach Satz (3.9.2) existiert $r \in \mathbb{Q}$ mit $ab < r < ba$. Multiplikation mit $a > 0$ und Benutzung von (5') aus (3.8.2) für Multiplikation von rechts und links ergibt $aba < ra$ und $ra < aba$. Da $\mathbb{Q} \leq Z(S)$, ist $ar = ra$, also $aba < ra = ar < aba$, Widerspruch.

3.9.4 Nullstellen von Polynomen

LEMMA: Sei K ein geordneter Körper und $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$, sei $M = \max\{1, |a_0| + \ldots + |a_{n-1}|\}$. Dann ist $f(s) > 0$ für $M < s \in K$ und $(-1)^n f(s) > 0$ für $-M > s \in K$. Somit liegen die Nullstellen von f im Intervall $[-M, M]$.

BEWEIS: Es gilt

$$f = x^n \left(1 + \frac{a_{n-1}}{x} + \ldots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n}\right)$$

Für $1 \leq M < |s|$ ist $\frac{1}{|s|} < \frac{1}{M} \leq 1$, also $\frac{1}{|s^i|} < \frac{1}{M}$. Daraus folgt:

$$\begin{aligned} \left|\frac{a_{n-1}}{s} + \ldots + \frac{a_1}{s^{n-1}} + \frac{a_0}{s^n}\right| &\leq \frac{|a_{n-1}|}{|s|} + \ldots + \frac{|a_1|}{|s^{n-1}|} + \frac{|a_0|}{|s^n|} \\ &< \frac{1}{M}(|a_{n-1}| + \ldots + |a_0|) \leq \frac{M}{M} = 1 \end{aligned}$$

Für $M < s$ ist $s > 0$, also $f(s) = s^n(1 + \ldots) > 0$, da beide Faktoren größer 0 sind. Ist $-M > s$, so ist $|s| > M$, also $f(s) = (-1)^n(-s)^n(1 + \ldots)$. Da $(-s) > 0$ ist, folgt: $(-1)^n f(s) > 0$.

3.9.5 Algebraische Erweiterungen

SATZ: Jede Fortsetzung einer archimedischen Anordnung eines Körpers auf einen algebraischen Erweiterungskörper ist archimedisch.

BEWEIS: Sei K archimedisch geordnet, L eine algebraische Erweiterung von K geordnet und diese Anordnung Fortsetzung der Anordnung von K. Wir zeigen: jedes $b \in L$ ist ganzzahlig einschließbar. Da b algebraisch über K ist, existiert $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K[x]$ mit $f(b) = 0$. Offenbar $f \in L[x]$. Sei $M = \max\{1, |a_{n-1}| + \ldots + |a_0|\}$. Nach Lemma ist $-M < b < M$ (in L). Offenbar ist $M \in K$ und somit (da K archimedisch geordnet) nach Satz (3.9.2) ganzzahlig einschließbar, d.h. es existiert $n \in \mathbb{N}$ mit $-n < M < n$ (in K). Dies gilt auch in L, also $-n < -M < b < M < n$. Somit ist b ganzzahlig einschließbar. Nach Satz (3.9.2) ist L archimedisch geordnet.

KOROLLAR: Ist K *absolut algebraisch* (d.h. algebraisch über $\mathbb{Q}$), so besitzt K höchstens archimedische Anordnungen.

3.9.6 Hauptsatz

SATZ: Jeder archimedisch geordneter Körper ist ordnungsisomorph zu einem Teilkörper von $\mathbb{R}$.

BEWEIS: Sei K ein archimedisch geordneter Körper. Für $a \in K$ sei $L(a) = \{r \in \mathbb{Q} \mid r < a\}$. Nach Satz (3.9.2) existiert $n \in \mathbb{N}$ mit $-n < a < n$, somit ist $L(a) \neq \emptyset$ (da $-n \in L(a)$) und n ist eine obere Schranke von $L(a)$. Somit ist $L(a) \subseteq \mathbb{R}$ nicht leer und nach oben beschränkt, d.h. es existiert $\sup L(a) \in \mathbb{R}$. Dann ist $\sigma : K \to \mathbb{R}$ mit $a \mapsto \sup L(a)$ eine wohldefinierte Abbildung. Wir zeigen: σ ist ein Ordnungsisomorphismus auf $K^\sigma \leq \mathbb{R}$.

1. *Behauptung:* $L(a+b) = \{r + s \mid r \in L(a), s \in L(b)\}$.

   Beweis: Für $r \in L(a)$ und $s \in L(b)$ ist $r + s < r + b < a + b$, also $r + s \in L(a + b)$.

   Sei $t \in L(a + b)$, d.h. $t < a + b$, dann ist $t - b < a$. Nach Satz (3.9.2) existiert $r \in \mathbb{Q}$ mit $t - b < r < a$. Sei $s = t - r$. Dann ist $r + s = t$ und $r \in L(a)$ und $s = t - r < b$, also $s \in L(b)$.

2. *Behauptung:* $(a + b)^\sigma = \sup L(a + b) \overset{!}{=} \sup L(a) + \sup L(b) = a^\sigma + b^\sigma$.

   Beweis: Ist $t \in L(a+b)$, so existieren $r \in L(a)$ und $s \in L(b)$ mit $t = r+s \leq \sup L(a) + \sup L(b)$. Daraus folgt: $\sup L(a + b) \leq \sup L(a) + \sup L(b)$.

   Angenommen $\sup L(A) + \sup L(b) - \sup L(a + b) = \varepsilon > 0$. Nach Definition von sup existieren $r \in L(a)$ und $s \in L(b)$ mit $\sup L(a) - r < \frac{\varepsilon}{2}$ und $\sup L(b) - s < \frac{\varepsilon}{2}$. Es gilt also

   $$\sup L(a) + \sup L(b) - (r + s) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

   Daraus folgt: $\sup L(a + b) < r + s \in L(a + b)$, Widerspruch.

3. Ist $a \in K$ mit $0 < a$, so existiert $r \in \mathbb{Q}$ mit $0 < r < a$. Somit enthält $L(a)$ positive rationale Zahlen, also ist $\sup L(a) = a^\sigma > 0$ in $\mathbb{R}$. Somit ist σ ein Ordnungsisomorphismus, falls Isomorphismus und σ ist injektiv: Nach (2) ist σ ein additiver Homomorphismus. Sei $a \in \operatorname{Kern} \sigma$. Ist $a > 0$, so ist $a^\sigma > 0$, ist $a < 0$, so ist $-a > 0$, also $0 < (-a)^\sigma = -a^\sigma$. Somit folgt: $\operatorname{Kern} \sigma = \{0\}$.

4. Zu zeigen ist: $(ab)^\sigma = a^\sigma b^\sigma$. *Behauptung:* Gilt dieses für $a, b > 0$, so gilt es allgemein.

   Beweis: (hier nur ein Fall, die anderen analog) Sei $a < 0$, $b > 0$, dann gilt:

   $$(ab)^\sigma = (-(-a)b)^\sigma = -((-a)b)^\sigma = -(-a)^\sigma b^\sigma = -(-a^\sigma)b^\sigma = a^\sigma b^\sigma$$

5. Ist $a > 0$, so existieren nach (3.9.2) $r \in \mathbb{Q}$ mit $0 < r < a$ also $r \in L(a)$ für $r > 0$. Sei $L^+(a) = \{r \in \mathbb{Q} \mid 0 < r < a\}$. Dann ist also $L^+(a) \neq \emptyset$ und $\sup L^+(a) = \sup L(a)$.

6. *Behauptung:* $L^+(ab) = \{rs \mid r \in L^+(a), s \in L^+(b)\}$, falls $a, b > 0$.

   Beweis: Ist $r \in L^+(a)$ und $s \in L^+(b)$, so ist $0 < r < a$ und $0 < s < b$, also mit $r < a$ und $0 < s$ folgt: $rs < as < ab$. Daraus folgt: $rs \in L^+(ab)$.

   Sei nun $t \in L^+(ab)$, also $0 < t < ab$. Dann folgt: $0 < \frac{t}{b} < a$. Nach (3.9.2) existiert $r \in \mathbb{Q}$ mit $\frac{t}{b} < r < a$. Setze $s = \frac{t}{r} > 0$. Dann ist $r \in L^+(a)$ und $t = rs$. Aus $\frac{t}{b} < r$ folgt: $s = \frac{t}{r} < b$, also $s \in L^+(b)$.

7. *Behauptung:* $(ab)^\sigma = \sup L^+(ab) \stackrel{!}{=} \sup L^+(a) \cdot \sup L^+(b) = a^\sigma b^\sigma$.

   Beweis: Ist $t \in L^+(ab)$, so existieren $r \in L^+(a)$ und $s \in L^+(b)$ mit $t = rs \leq \sup L^+(a) \sup L^+(b)$. Somit gilt: $\sup L^+(ab) \leq \sup L^+(a) \sup L^+(b)$.

   Wäre nun $\sup L^+(a) \sup L^+(b) - \sup L^+(ab) = \varepsilon > 0$ und ist $r + \varepsilon_1 = \sup L^+(a)$ und $s + \varepsilon_2 = \sup L^+(b)$ für $r \in L^+(a)$ und $s \in L^+(b)$, so gilt:

   $$\sup L^+(a) \sup L^+(b) = (r + \varepsilon_1)(s + \varepsilon_2) = rs + \varepsilon_1 s + r\varepsilon_2 + \varepsilon_1\varepsilon_2$$

   Für geeignete $\varepsilon_1, \varepsilon_2$ ist $\varepsilon_1 s + r\varepsilon_2 + \varepsilon_1\varepsilon_2 < \varepsilon$. Somit folgt: $\sup L^+(ab) < rs$, Widerspruch.

3.9.7 Automorphismen

SATZ: Jeder Ordnungsisomorphismus σ eines archimedisch geordneten Körpers K ist die Identität.

BEWEIS: Angenommen $\sigma \neq \mathrm{id}$. Dann existiert $a \in K$ mit $a^\sigma \neq a$, also etwa $a^\sigma > a$. Nach Satz (3.9.2) existiert $r \in \mathbb{Q}$ mit $a < r < a^\sigma$. Da Automorphismen nach (I.10.1) trivial auf Primkörpern sind, ist $r^\sigma = r$. Da σ die Ordnung erhält, folgt aus $a < r$, dass $a^\sigma < r^\sigma = r < a^\sigma$, Widerspruch.

KOROLLAR: $\mathbb{R}$ hat nur den trivialen Automorphismus ($\mathrm{Aut}\,\mathbb{R} = 1$).

BEWEIS: Für $a \in \mathbb{R}$ ist $a > 0$ genau dann, wenn $a \neq 0$ und ein $b \in \mathbb{R}$ existiert mit $b \neq 0$ und $b^2 = a$. Somit $a^\sigma = (b^2)^\sigma = (b^\sigma)^2$, also $a^\sigma > 0$, d.h. jeder Automorphismus von $\mathbb{R}$ ist ein Ordnungsisomorphismus.

3.10 Erweiterungen geordneter Körper

3.10.1 Formal-reelle Körper

DEFINITION: Der Körper K heißt *formal-reell*, wenn -1 nicht Summe von Quadraten in K ist.

BEMERKUNGEN:

1. K ist genau dann formal-reell, wenn gilt:

$$\sum_{i=1}^{n} a_i^2 = 0 \text{ für } a_i \in K \Longrightarrow a_i = 0 \text{ für alle } i$$

„⇒“ Angenommen $\sum_{i=1}^{n} a_i^2 = 0$ und o.B.d.A. $a_1 \neq 0$. Dann gilt:

$$0 = \frac{1}{a_1^2} \sum_{i=1}^{n} a_i^2 = 1 + \sum_{i=2}^{n} \left(\frac{a_i}{a_1}\right)^2$$

„⇐“ Angenommen $-1 = \sum_{i=1}^{n} a_i^2$. Dann gilt: $0 = 1^2 + \sum_{i=1}^{n} a_i^2$.

2. Ist K formal-reell, so ist $\operatorname{char} K = 0$ (da $p \cdot 1^2 \neq 0$ für alle $p \in \mathbb{N}$).

3. Ist K geordnet, so sind alle $a_i^2 \in P$ für $a_i \neq 0$, also -1 nicht Summe von Quadraten. Somit gilt: K geordnet $\Rightarrow$ K formal-reell.

SATZ: (ARTIN-SCHREIER 1926) Ein Körper K ist genau dann anordbar, wenn er formal-reell ist.

BEWEISIDEE: Sei $Q = \{\sum a_i^2 \mid 0 \neq a_i \in K\}$. Dann erfüllt Q die Eigenschaften (1), (2), (4) eines Positivbereiches. Mit dem Lemma von Zorn wollen wir Q so erweitern, dass auch (3) erfüllt ist.

3.10.2 Q-Bereiche

Sei K ein Körper.

DEFINITION: Eine Teilmenge M von K heißt *Q-Bereich*, wenn gilt:

1. $M + M \subseteq M$
2. $0 \notin M$
3’ $Q := \{\sum a_i^2 \mid 0 \neq a_i \in K\} \subseteq M$.
4. $M \cdot M \subseteq M$

BEMERKUNGEN:

1. Ist K nicht formal-reell, so existiert kein Q-Bereich. *Beweis:* Ist K nicht formal-reell, so ist $0 \in Q \subseteq M$, ein Widerspruch zu (2).

2. Ist K formal-reell, so ist $M = Q$ ein Q-Bereich. *Beweis:*

   (1) $(\sum a_i^2) + \left(\sum b_j^2\right) \in Q$

   (2) Gilt nach Bemerkung (3.10.1)(1).

   (3') $Q \subseteq Q$

   (4) $(\sum a_i^2)\left(\sum b_j^2\right) = \sum_{i,j}(a_i b_j)^2 \in Q$

3. Jeder Positivbereich ist ein Q-Bereich (nach Definition (3.8.2) und (3.8.5)(a)).

LEMMA: Sei M ein Q-Bereich des Körpers K und $t \in K$ mit $t \notin -M \cup \{0\} \cup M$. Dann existiert ein Q-Bereich M' mit $M \subseteq M'$ und $t \in M'$.

BEWEIS: Sei $M' = \{a + bt \mid a \in M,\ b \in M_0 = M \cup \{0\}\}$. Dann gilt für $a, c \in M$ und $b, d \in M_0$:

(1) $(a + bt) + (c + dt) = \underbrace{(a + c)}_{\in M} + \underbrace{(b + d)}_{\in M_0} t \in M'$.

(4) $(a + bt)(c + dt) = \underbrace{ac}_{\in M} + \underbrace{bd}_{\in M_0}\underbrace{t^2}_{\in M} + \underbrace{(ad + bc)}_{\in M_0} t \in M'$

(3') $Q \subseteq M \subseteq M'$: man wähle $b = 0$.

(2) Angenommen $0 \in M'$, d.h. $0 = a + bt$ mit $a \in M$ und $b \in M_0$. Nach (2) ist $a \neq 0$, also auch $b \neq 0$. Dann gilt: $t = -\frac{a}{b} = -ab\frac{1}{b^2} \in -M$, da $ab \in M$ und $\frac{1}{b^2} \in M$.

Zu zeigen ist noch: $t \in M'$. Setze $a = b = 1$, dann folgt: $1 + t \in M'$. Nach (2) gilt: $1 + t \neq 0$. Damit

$$M' \ni \left(\frac{2t}{t+1}\right)^2 + \left(\frac{t-1}{t+1}\right)^2 t = t \cdot \frac{4t + t^2 - 2t + 1}{(t+1)^2} = t \cdot \frac{(t+1)^2}{(t+1)^2} = t$$

SATZ: (ARTIN-SCHREIER 1926) Jeder Q-Bereich eines (formal-reellen) Körpers lässt sich zu einem Positivbereich erweitern.

FOLGERUNG: Satz (3.10.1). *Beweis:* Sei K formal-reell. Dann ist nach Bemerkung (2) Q ein Q-Bereich, also laut dem Satz existiert ein Positivbereich

von K.

BEWEIS: Sei M ein Q-Bereich von K. Sei $\mathfrak{M} = \{ M' \mid M \subseteq M',\ M'\, Q - \text{Bereich}\}$. $\mathfrak{M}$ ist durch Inklusion teilweise geordnet. Weiter ist $M \in \mathfrak{M}$, also $\mathfrak{M}$ ist nicht leer. Sei $\mathfrak{T} \subseteq M$ eine Kette in $\mathfrak{M}$ und $S = \bigcup_{T \in \mathfrak{T}} T$. Wir zeigen: S ist ein Q-Bereich.

(1), (4) Seien $a, b \in S$. Dann existieren $T_1, T_2 \in \mathfrak{T}$ mit $a \in T_1$ und $b \in T_2$. Da $\mathfrak{T}$ eine Kette ist, gilt etwa $T_1 \subseteq T_2$, also $a, b \in T_2$. Da T_2 ein Q-Bereich ist, folgt: $a + b \in T_2 \subseteq S$ und $ab \in T_2 \subseteq S$.

(2) $0 \notin T$ für alle $T \in \mathfrak{T}$, also $0 \notin \bigcup_{T \in \mathfrak{T}} T = S$.

(3') $Q \subseteq T \subseteq S$ für alle $T \in \mathfrak{T}$.

Somit ist S ein Q-Bereich und $M \subseteq T \subseteq S$ für alle $T \in \mathfrak{T}$, also ist $S \in \mathfrak{M}$ obere Schranke von $\mathfrak{T}$. Mit dem Lemma von Zorn folgt: ex existiert ein maximales Element $P \in \mathfrak{M}$.

Behauptung: P ist ein Positivbereich. *Beweis:* Da $P \in \mathfrak{M}$ ein Q-Bereich ist, sind (1), (2), (4) von Definition (3.8.2) erfüllt. Zu (3): angenommen $K \neq -P \cup \{0\} \cup P$, dann existiert $t \in K \setminus (-P \cup \{0\} \cup P)$. Mit dem Lemma folgt: es existiert ein Q-Bereich P' mit $P \subseteq P'$ und $t \in P'$. Dann ist $M \subseteq P \subseteq P'$, also $P' \in \mathfrak{M}$ und $P \neq P'$, ein Widerspruch zur Maximalität von P.

3.10.3 Fortsetzungen der Anordnung

SATZ: Seien $K \leq L$ Körper und sei K durch P geordnet. Genau dann lässt sich P zu einem Positivbereich P^* von L fortsetzen, wenn gilt:

$$\sum a_i t_i^2 \neq -1 \text{ für alle } a_i \in P \text{ und } t_i \in L \qquad (\star)$$

Äquivalent dazu ist:

$$\sum a_i t_i^2 = 0 \text{ für } a_i \in P,\ t_i \in L \Longrightarrow t_i = 0 \text{ für alle } i \qquad (\star\star)$$

BEWEIS:

„⇒“ Sei P^* ein Positivbereich von L mit $P \subseteq P^*$. Da $a_i \in P \subseteq P^*$ und (nach (3.8.5)) $t_i^2 \in P^* \cup \{0\}$, folgt: $\sum a_i t_i^2 \in P^* \cup \{0\}$.

„⇐“ Sei $M = \{ \sum a_i t_i^2 \mid a_i \in P,\ 0 \neq t_i \in L\}$. Wir zeigen: M ist ein Q-Bereich.

(1) Offensichtlich $\sum a_i t_i^2 + \sum b_j s_j^2 \in M$.

(4) $\left(\sum a_i t_i^2\right)\left(\sum b_j s_j^2\right) = \sum_{i,j} a_i b_j (t_i s_j)^2 \in M$.

(2) Mit $(\star\star)$ folgt: $0 \notin M$.

(3') Setzt man $a_i = 1$, so ist $\sum t_i^2 \in M$, also $Q \subseteq M$.

Nach Satz (3.10.1) existiert ein Positivbereich $P^* \supseteq M \supseteq P$ (da es gilt $a_i = a_i 1^2 \in M$).

$(\star) \Rightarrow (\star\star)$ Angenommen $\sum_{i=1}^n a_i t_i^2 = 0$ und o.B.d.A. $t_1 \neq 0$. Dann gilt:

$$0 = \frac{1}{a_1 t_1^2} \sum_{i=1}^n a_i t_i^2 = 1 + \sum_{i=2}^n \frac{a_i}{a_1} \left(\frac{t_i}{t_1}\right)^2$$

$(\star\star) \Rightarrow (\star)$ Angenommen $\sum a_i t_i^2 = -1$, dann gilt: $0 = 1 \cdot 1^2 + \sum a_i t_i^2$.

3.10.4 Einfache algebraische Erweiterungen

Sei K ein geordneter Körper.

DEFINITION: Wir sagen, dass das Polynom $f \in K[x]$ auf K *das Vorzeichen wechselt*, wenn es $a, b \in K$ gibt mit $f(a)f(b) < 0$. Man sagt auch: f wechselt zwischen a und b das Vorzeichen.

Achtung: Hat nichts mit einer Nullstelle zwischen a und b zu tun!

SATZ: Sei K ein durch P geordneter Körper und f ein irreduzibles Polynom aus $K[x]$, das auf K das Vorzeichen wechselt. Sei $L = K(\alpha)$ mit einer Nullstelle α von f. Dann lässt sich die Anordnung P auf L fortsetzen:

$$M_f = \left\{ \sum a_i t_i^2 \;\middle|\; a_i \in P,\, 0 \neq t_i \in L \right\}$$

ist ein Q-Bereich von L.

BEWEIS: Wir zeigen mittels Induktion nach $n := \operatorname{grad} f = [K(\alpha) : K]$, dass $(\star\star)$ in $K(\alpha)$ gilt. Für $n = 1$ ist $K(\alpha) = K$ und die Aussage gilt nach (3.8.5)(1). Sei nun die Aussage für Polynome kleineren Grades richtig. Angenommen $(\star\star)$ und somit auch $(\star)$ ist falsch, dann existieren $0 \neq t_i \in K(\alpha)$, $a_i \in P$ mit $\sum a_i t_i^2 = -1$, also

$$1 + \sum_{i=1}^k a_i t_i^2 = 0$$

Nach (I.4.4) existieren $f_i \in K[x]$ mit $t_i = f_i(\alpha)$ und $\operatorname{grad} f_i < n$. Somit ist $1 + \sum_{i=1}^{k} a_i f_i^2 \in K[x]$ mit

$$\left(1 + \sum_{i=1}^{k} a_i f_i^2\right)(\alpha) = 1 + \sum_{i=1}^{k} a_i f_i^2(\alpha) = 1 + \sum_{i=1}^{k} a_i t_i^2 = 0$$

Nach (I.4.4) teilt f dieses Polynom in $K[x]$ (da $f = p_\alpha$ bis evtl. auf den ersten Koeffizienten), d.h. es existiert $h \in K[x]$ mit

$$1 + \sum_{i=1}^{k} a_i f_i^2 = fh \tag{1}$$

Für alle $c \in K$ ist $f(c)h(c) = 1 + \sum_{i=1}^{k} a_i f_i^2(c) > 0$, also insbesondere für $c = a$ und $c = b$ mit $f(a)f(b) < 0$. Somit $0 < f(a)h(a)f(b)h(b)$. Da $f(a)f(b) < 0$, folgt: $h(a)h(b) < 0$.

Sei $h = g_1 \dots g_r$ mit irreduziblen $g_i \in K[x]$. Wäre $g_i(a)g_i(b) > 0$ für alle i, so wäre auch $h(a)h(b) = \prod g_i(a)g_i(b) > 0$. Somit existiert ein irreduzibler Teiler g von h mit $g(a)g(b) < 0$.

Da $\operatorname{grad}\left(1 + \sum_{i=1}^{k} a_i f_i^2\right) \leq 2n-2$ und $\operatorname{grad} f = n$, folgt: $\operatorname{grad} h \leq n-2$, also $\operatorname{grad} g \leq n-2 < n$. Nach Induktionsvoraussetzung gilt $(\star\star)$ in $K(\gamma)$, wobei γ eine Nullstelle von g ist. Da g ein Teiler von h ist, ist $h(\gamma) = 0$. Setze γ in (1) ein:

$$0 = h(\gamma)f(\gamma) = 1 + \sum_{i=1}^{k} a_i f_i^2(\gamma), \text{ also } -1 = \sum_{i=1}^{k} a_i f_i^2(\gamma)$$

Dies ist ein Widerspruch zu $(\star)$ in $K(\gamma)$.

KOROLLAR:

1. Für jedes $a \in P$ lässt sich P auf $K(\sqrt{a})$ fortsetzen.
2. Ist $[L : K]$ ungerade, so lässt sich P auf L fortsetzen.

BEWEIS:

1. $f = x^2 - a$ ist das definierende Polynom von $\sqrt{a}$, falls $\sqrt{a} \notin K$. Es gilt $f(0) = -a < 0$ und $f(s) > 0$ für $s > M = \max\{1, |a|\}$ nach (3.9.4).
2. Nach (I.9.6) (Satz vom primitiven Element) ist $L = K(\alpha)$ mit $\alpha \in L$. Ferner für $f = p_\alpha$ ist $n = \operatorname{grad} f = [L : K]$ ungerade. Nach (3.9.4) existiert $M \in K$ mit $f(s) > 0$ für $s > M$ und $(-1)^n f(s) > 0$ (also $f(s) < 0$) für $s < -M$.

3.10.5 Ordnungs- bzw. reell-abgeschlossene Körper

Seien K, L geordnete Körper.

DEFINITIONEN:

1. L heißt *Ordnungserweiterung* von K, wenn $K \leq L$ und die Ordnung von L die von K fortsetzt (siehe (3.8.7)).
2. L heißt *ordnungsabgeschlossen*, wenn jede algebraische Ordnungserweiterung von L gleich L ist.
3. L heißt *Ordnungsabschluß* von K, wenn L eine algebraische Ordnungserweiterung von K ist und L ordnungsabgeschlossen ist.
4. Der Körper F heißt *reell-abgeschlossen* , wenn F formal-reell ist und keine echte algebraische Erweiterung formal-reell ist.

BEMERKUNGEN:

1. $\mathbb{R}$ ist ordnungsabgeschlossen und reell-abgeschlossen. *Beweis:* Eine echte algebraische Erweiterung von $\mathbb{R}$ müsste im zu $\mathbb{C}$ isomorphen algebraischen Abschluß liegen, wegen $[\mathbb{C} : \mathbb{R}] = 2$ also selbst isomorph zu $\mathbb{C}$ sein.
2. Ist F reell-abgeschlossen, so ist nach (3.10.1) F anordbar und jede Ordnungserweiterung ist formal-reell. Somit ist F ordnungsabgeschlossen in jeder Anordnung.

SATZ: Der algebraische Abschluß A eines geordneten Körpers K enthält einen Ordnungsabschluß von K.

BEWEIS: Sei $\mathfrak{M} = \{(L, P_L) \mid K \leq L \leq A,\ P_K \subseteq P_L\}$. Für $L, M \in \mathfrak{M}$ sei

$$(L, P_L) < (M, P_M) \Leftrightarrow L \leq M,\ P_L \subseteq P_M$$

$\mathfrak{M}$ ist nicht leer, da $(K, P_K) \in \mathfrak{M}$. Ist $\mathfrak{T} \subseteq \mathfrak{M}$ eine Kette, so sei $S = \bigcup_{(T,P_T)\in\mathfrak{T}} T$ und $P_S = \bigcup_{(T,P_T)\in\mathfrak{T}} P_T$.

Behauptung: $(S, P_S) \in \mathfrak{M}$. *Beweis:* Da S Vereinigung einer Kette von Körpern ist, so ist S selbst ein Körper. Noch zu zeigen: P_S ist ein Positivbereich. Seien $a, b \in P_S$, dann ist $a \in P_{T_1}$ und $b \in P_{T_2}$, wobei etwa $P_{T_1} \subseteq P_{T_2}$, also ist $a, b \in P_{T_2}$. Somit folgt: $a + b,\ ab \in P_{T_2} \subseteq P_S$. Trivialerweise ist $0 \notin P_S$. Ist $a \in S$, so existiert ein Körper T mit $a \in T$. Es gibt folgende Fälle:

$a \in P_T \subseteq P_S$ oder $a = 0$ oder $a \in -P_T \subseteq -P_S$.

Somit ist S eine obere Schranke von $\mathfrak{M}$. Mit dem Lemma von Zorn folgt: $\mathfrak{M}$ hat ein maximales Element (L, P_L). *Behauptung:* (L, P_L) ist ordnungsabgeschlossen (somit nach Definition (L, P_L) ein Ordnungsabschluß von K).

Beweis: Sei $(R, \tilde{P})$ eine algebraische Ordnungserweiterung von (L, P_L). Sei B ein algebraischer Abschluß von R. Da R algebraisch über L ist, ist B algebraisch über L, also ein algebraischer Abschluß von L. Da A algebraisch über L ist, ist A ein algebraischer Abschluß von L. Nach (I.7.12) existiert $\sigma : B \to A$, ein Isomorphismus über L. Nach Lemma (3.8.8) ist dann $(R^\sigma, \tilde{P}^\sigma)$ geordnet und $P_K \subseteq P_L = P_L^\sigma \subseteq \tilde{P}^\sigma$ (da $P_L \subseteq \tilde{P}$). Somit ist $(R^\sigma, \tilde{P}^\sigma) \in \mathfrak{M}$. Da $L \leq R^\sigma$ und $P_L \subseteq \tilde{P}^\sigma$, folgt: $(L, P_L) < (R^\sigma, \tilde{P}^\sigma)$. Aus der Maximalität von L folgt: $L = R^\sigma$, also $L = R$.

3.10.6 Zwischenwertsatz

SATZ: Sei K ein ordnungsabgeschlossener Körper, seien $a, b \in K$ und $f \in K[x]$ mit $f(a)f(b) < 0$. Dann besitzt f eine Nullstelle $c \in K$ zwischen a und b.

BEWEIS: Wie im Beweis vom Satz (3.10.4) existiert ein irreduzibler Faktor h von f mit $h(a)h(b) < 0$. Nach Satz (3.10.4) lässt sich die Anordnung von K auf $K(\alpha)$ fortsetzen, wobei α eine Nullstelle von h ist. Da K ordnungsabgeschlossen ist, folgt: $K(\alpha) = K$. Somit hat h eine Nullstelle in K, also $\operatorname{grad} h = 1$, d.h. $h = x - \alpha$. Dann ist $f(\alpha) = 0$. Sei o.B.d.A $a < b$. Da $h(a)h(b) < 0$, folgt:

$$(a - \alpha)(b - \alpha) < 0 \Rightarrow a - \alpha < 0 < b - \alpha \Rightarrow a < \alpha < b$$

KOROLLAR: Ist $f(a) < u < f(b)$, so existiert c zwischen a und b mit $f(c) = u$.

BEWEIS: Setze $g = f - u$, dann ist $g(a) = f(a) - u < 0$ und $g(b) = f(b) - u > 0$, also $g(a)g(b) < 0$. Mit dem Satz folgt: es existiert c zwischen a und b mit $g(c) = 0 = f(c) - u$.

3.10.7 Hauptsatz über ordnungsabgeschlossene Körper

SATZ: (EULER 1749, LAGRANGE 1772) Die folgenden Eigenschaften sind für den geordneten Körper K äquivalent:

1. K ist ordnungsabgeschlossen.
2. Jedes Polynom ungeraden Grades in $K[x]$ hat eine Nullstelle in K und jedes positive Element von K ist ein Quadrat, d.h. $K = (K^*)^2 \cup \{0\} \cup -(K^*)^2$.
3. $K(i)$ ist algebraisch abgeschlossen.

BEWEIS:

(1) $\Rightarrow$ (2) Ist $f \in K[x]$ mit Grad von f ungerade, dann folgt mit (3.9.4): f wechselt Vorzeichen auf K (siehe Beweis zu Korollar (3.10.4)). Mit (3.10.6) folgt daraus: f hat eine Nullstelle in K.

Sei $0 < a \in K$. Dann gilt: $f = x^2 - a \in K[x]$ wechselt Vorzeichen auf K (siehe Beweis zu Korollar (3.10.4)). Mit (3.10.6) folgt daraus: es existiert $\beta \in K$ mit $0 = f(\beta) = \beta^2 - a$.

(2) $\Rightarrow$ (3) Siehe (I.11.3). Aus (2) folgen die Voraussetzungen (1) und (2) von (I.11.3). Die Voraussetzung (3) gilt, da in $L = K(i)$ jedes Element ein Quadrat ist: für $a + ib \in L$ sei

$$u = \frac{\sqrt{a + \sqrt{a^2 + b^2}}}{2} \quad v = \operatorname{sgn} b \frac{\sqrt{-a + \sqrt{a^2 + b^2}}}{2}$$

Dann gilt: $(u + iv)^2 = a + ib$. Mit (I.11.3) folgt: L ist algebraisch abgeschlossen.

(3) $\Rightarrow$ (1) Sei $K < L$ eine algebraische Ordnungserweiterung. Laut (3) gilt dann: $[L : K] = 2$ und $L = K(i)$ mit $i^2 = -1$. Dann ist aber L nicht geordnet, Widerspruch.

KOROLLAR: Ein ordnungsabgeschlossener Körper hat nur eine Anordnung. Jeder Isomorphismus zwischen zwei ordnungsabgeschlossenen Körpern ist ein Ordnungsisomorphismus.

BEWEIS: Ist K ordnungsabgeschlossen, so ist nach Satz $P = (K^*)^2$. Quadrate werden von Isomorphismen auf Quadrate abgebildet, somit folgt der zweite Teil der Aussage.

BEMERKUNG: Reell-abgeschlossen ist dasselbe wie ordnungsabgeschlossen, da ein ordnungsabgeschlossener Körper nur eine Anordnung hat.

3.10.8 Sturmsche Ketten

Sei K ein geordneter Körper, $f \in K[x]$ und $a < b$ aus K.

FRAGE: Wieviele Nullstellen hat f zwischen a und b?

DEFINITIONEN:

Wir setzen $f_0 = f$ und $f_1 = f'$. Dann wenden wir den Euklidischen Algorithmus an:

$$\begin{aligned} f_0 &= q_1 f_1 - f_2 \quad (\text{wobei } f_2 = 0 \text{ oder } \operatorname{grad} f_2 < \operatorname{grad} f_1) \\ f_1 &= q_2 f_2 - f_3 \\ &\vdots \\ f_{r-1} &= q_r f_r \end{aligned}$$

Die Polynomfolge $(f_0, \ldots, f_r)$ heißt die *Sturmsche Kette* von f.

(a) Seien $0 \neq a_i \in K$. Die Anzahl der Vorzeichenwechsel der Folge $(a_0, \ldots, a_n)$ ist die Anzahl der $i \in \{0, \ldots, n-1\}$ mit $a_i a_{i+1} < 0$.

(b) Seien $b_i \in K$. Dann sei die Anzahl der Vorzeichenwechsel der Folge $(b_0, \ldots, b_m)$ definiert als die Anzahl der Vorzeichenwechsel der Folge, die man erhält, wenn man alle Nullen weglässt.

BEISPIEL: Die folgende Folge hat 3 Vorzeichenwechsel:

$$(-1,\ 7,\ 0,\ 0,\ 3,\ -2,\ 0,\ 1,\ 5) \Longrightarrow (-1,\ 7,\ 3,\ -2,\ 1,\ 5)$$

SATZ: (JACQUES CHARLES FRANCOIS STURM 1807-1855) Sei K ein ordnungsabgeschlossener Körper, $f \in K[x]$ mit $\operatorname{grad} f \geq 1$ und $a, b \in K$ mit $a < b$ und $f(a) \neq 0 \neq f(b)$. Für $c \in K$ sei $v(c)$ die Anzahl der Vorzeichenwechsel in der Folge $(f_0(c), \ldots, f_r(c))$, wobei $(f_0, \ldots, f_r)$ die Sturmsche Kette von f ist. Dann ist die Anzahl der Nullstellen von f in (a, b) gleich $v(a) - v(b)$.

BEISPIEL: Sei $f = f_0 = x^2 - 1,\ f_1 = f' = 2x$. Dann ist $x^2 - 1 = \frac{1}{2}x \cdot 2x - 1$,

also $f_2 = 1$. Die Vorzeichen in der Sturmschen Kette sehen wie folgt aus:

t	$f_0(t)$	$f_1(t)$	$f_2(t)$	$v(t)$
$t < -1$	$+$	$-$	$+$	2
$t = -1$	0	$-$	$+$	1
$-1 \leq t \leq 0$	$-$	$-$	$+$	1
$t = 0$	$-$	0	$+$	1
$0 < t < 1$	$-$	$+$	$+$	1
$t = 1$	0	$+$	$+$	0
$t > 1$	$+$	$+$	$+$	0

BEWEIS: $f_0, \ldots, f_r$ sind Polynome ungleich 0, haben zusammen also nur endlich viele Nullstellen. Somit ist $D = \{d \in K \mid \exists i \text{ mit } f_i(d) = 0\}$ endlich. Sei $D \cap (a, b) = \{d_1, \ldots, d_n\}$, wähle $d_i < d_{i+1}$ für alle i. Seien

$$s_0 = \frac{a + d_1}{2}; \quad s_i = \frac{d_i + d_{i+1}}{2} \text{ für } i = 1, \ldots, n-1; \quad s_n = \frac{d_n + b}{2}$$

Es gilt dann: $d_i < s_i < d_{i+1}$. Wir zeigen:

(i) $v(a) = v(s_0)$ und $v(b) = v(s_n)$

(ii) $v(s_i) = v(s_{i-1})$ falls $f(d_i) \neq 0$.

(iii) $v(s_i) = v(s_{i-1}) - 1$ falls $f(d_i) = 0$.

Seien $s, t \in K$ mit $s < t$. Wir betrachten drei Fälle.

1. *Behauptung:* Ist $[s, t] \cap D = \emptyset$, so ist $v(s) = v(t)$.

   Beweis: Wäre $f_i(s) f_i(t) < 0$ für ein i, so folgte nach (3.10.6): es existiert eine Nullstelle von f in $[s, t]$, Widerspruch, da $[s, t] \cap D = \emptyset$. Also sind die Vorzeichen der Folgen $(f_0(s), \ldots, f_r(s))$ und $(f_0(t), \ldots, f_r(t))$ gleich, also $v(s) = v(t)$.

2. *Behauptung:* Ist $[s, t] \cap D = \{d\}$ und $f(d) \neq 0$, so ist $v(s) = v(t)$. (Somit sind (i) und (ii) bewiesen)

   Beweis: Zu betrachten ist nur die Situation $t = d$ (sonst wende man diese und die entsprechende $s = t$ auf die Teilintervalle $[s, d]$ und $[d, t]$ an). Ist $f_i(d) \neq 0$, so hat f_i in $[s, d]$ keine Nullstelle und nach (3.10.6) ist $f_i(s) f_i(d) > 0$, d.h. beide Folgen haben an i-ter Stelle dasselbe Vorzeichen. Insbesondere gilt das für $i = 0$.

   Sei nun $i \in \{1, \ldots, r\}$ mit $f_i(d) = 0$. Zunächst gilt: $i \neq r$, d.h. $f_r(d) \neq 0$. Denn $f_r = \mathrm{ggT}(f_0, f_1)$, wäre $f_r(d) = 0$, so auch $f(d) = 0$, Widerspruch zur

Voraussetzung.

Betrachte nun die i-te Zeile. Es gilt

$$f_{i-1}(d) = q_i(d)f_i(d) - f_{i+1}(d) = -f_{i+1}(d) \neq 0$$

Denn sonst wäre:

$$f_i(d) = 0 = f_{i-1}(d) \Longrightarrow f_{i-2}(d) = 0 \Longrightarrow \ldots \Longrightarrow f_0(d) = 0$$

Für die Vorzeichen der Polynome im Intervall $[s, d]$ gibt es somit folgende vier Möglichkeiten:

$$(\ldots \overset{i-1}{+} \overset{i}{\pm} \overset{i+1}{-} \ldots),\ (\ldots \overset{i-1}{-} \overset{i}{\pm} \overset{i+1}{+} \ldots),\ (\ldots \overset{i-1}{+} \overset{i}{0} \overset{i+1}{-} \ldots),\ (\ldots \overset{i-1}{-} \overset{i}{0} \overset{i+1}{+} \ldots)$$

Zwischen $i-1$ und $i+1$ liegt also in allen 4 Folgen *genau ein* Vorzeichenwechsel.

3. *Behauptung:* Ist $[s,t] \cap D = \{d\} \subseteq (s,t)$ und $f(d) = 0$, so ist $v(t) = v(s) - 1$.

   Beweis: Sei d eine m-fache Nullstelle, also $f = (x-d)^m g$ mit $g(d) \neq 0$. Dann gilt:

$$f' = m(x-d)^{m-1}g + (x-d)^m g' = (x-d)^{m-1}(\underbrace{mg + (x-d)g'}_{h_0 \text{ mit } h_0(d) \neq 0})$$

   Daraus folgt: $f_r = \mathrm{ggT}(f, f') = (x-d)^{m-1}h$ mit $h(d) \neq 0$. Definiere

$$f_i^* = \frac{f_i}{(x-d)^{m-1}} \in K[x]$$

   Betrachte $(f_0^*, \ldots, f_r^*)$. Sei $w(c)$ die Anzahl der Vorzeichenwechsel in der Kette $(f_0^*(c), \ldots, f_r^*(c))$. Da $(s-d)^{m-1} \neq 0$, ist $w(s) = v(s)$, genauso $w(t) = v(t)$. Zu zeigen ist also: $w(t) = w(s) - 1$. Für die Polynome f_i^* gilt:

   (a) $f_r^*(d) = h(d) \neq 0$.

   (b) $f_{i-1}^* = q_i f_i^* - f_{i+1}^*$, da in der definierenden Gleichung für f_{i+1} alle f_j durch $(x-d)^{m-1}$ dividiert werden.

   Für ein Polynom f_i^* betrachten wir folgende Fälle:

   (b1) Ist $f_i^*(d) \neq 0$, so haben $f_i^*(s)$ und $f_i^*(t)$ dasselbe Vorzeichen nach (3.10.6).

(b2) Sei $f_i^*(d) = 0$ und $i > 0$. Nach (a) ist $i \neq r$, daraus folgt mit (b): $f_{i-1}^*(d) = -f_{i+1}^*(d) \neq 0$ (siehe Beweis zu (2)). Genauso wie in (2) folgt: die Kette hat auf dem Intervall $[s,t]$ *genau ein* Vorzeichenwechsel zwischen $i-1$ und $i+1$.

(b3) Es gilt: $f_1^*(d) = mg(d)$ hat dasselbe Vorzeichen wie $g(d)$. Nach (3.10.6) haben $f_1^*(s)$ und $f_1^*(t)$ dasselbe Vorzeichen wie $f_1^*(d)$, also wie $g(d)$. Weiter gilt: $f_0^*(s) = (s-d)g(s)$ hat das andere Vorzeichen, da $g(s)$ dasselbe Vorzeichen wie $g(d)$ hat (es liegt keine Nullstelle von g dazwischen). Anderseits hat $f_0^*(t) = (t-d)g(t)$ dasselbe Vorzeichen wie $g(d)$, da $t-d > 0$. Es gilt also: $f_0^*(s) \cdot f_1^*(s) < 0$ und $f_0^*(t) \cdot f_1^*(t) > 0$, somit hat die Kette bei t ein Vorzeichenwechsel weniger.

BEMERKUNGEN:

1. Ist $f = \sum_{i=0}^{n} a_i x^i$ mit $a_n = 1$, so liegen nach (3.9.4) alle Nullstellen in K zwischen $-M$ und M, wobei $M = \max\left\{1, \sum_{i=0}^{n-1} |a_i|\right\}$. Somit ist die Anzahl der Nullstellen in K, falls K ordnungsabgeschlossen ist, gleich $v(-M) - v(M)$.

2. Mit dem Sturmschen Satz kann man durch Halbieren des Intervalls Nullstellen beliebig genau bestimmen. *Aufgabe:* wie viele Nullstellen hat das Polynom $f = x^3 - 5x^2 + 8x - 9$ in $\mathbb{R}$. Wo liegen sie?

3. Die ganzen Rechnungen finden in $\mathbb{Q}(a_0, \ldots, a_n)$ statt. Somit hat das Polynom in jedem ordnungsabgeschlossenen Körper, der $\mathbb{Q}(a_0, \ldots, a_n)$ enthält, genauso viele Nullstellen wie in $\mathbb{R}$.

3.10.9 Eindeutigkeit des Ordnungsabschlusses

SATZ: Sei σ ein Ordnungsisomorphismus des geordneten Körpers K auf den geordneten Körper K^σ und seien R bzw. S Ordnungsabschlüsse von K bzw. K^σ. Dann existiert genau eine Fortsetzung σ^* von σ zu einem Isomorphismus von R auf S. Nach Korollar (3.10.7) ist σ^* ein Ordnungsisomorphismus.

KOROLLAR:

1. Je zwei Ordnungsabschlüsse von K sind über K ordnungsisomorph.

2. Ist R ein Ordnungsabschluß von K, so ist $\mathrm{Gal}(R/K) = 1$, da id_R die einzige Fortsetzung von id_K ist.

BEWEIS:

1. *Behauptung:* $f \in K[x]$ hat in R genauso viele Nullstellen, wie $f^{\bar\sigma}$ in S.

   Beweis: Nach Bemerkung (3.10.8) ist die Anzahl der Nullstellen von f in R gleich $v(-M) - v(M)$, wobei $f = \sum_{i=0}^{n} a_i x^i$ mit $a_n = 1$, $M = \max\left\{1, \sum_{i=0}^{n-1} |a_i|\right\}$ und v wie im Satz (3.10.8). Alles, was dabei eingeht, findet in K statt (siehe Bemerkung (3.10.8)(3)) und wird von σ auf die entsprechenden Terme für f^σ in K^σ abgebildet:

   (a) *Behauptung:* $f_i^{\bar\sigma} = (f^{\bar\sigma})_i$ für $i = 1, \ldots, r$.

   Beweis: Induktion. Es gilt $f_0^{\bar\sigma} = f^{\bar\sigma} = (f^{\bar\sigma})_0$. Weiter gilt

$$\begin{aligned} & f_1 = \sum i a_i x^{i-1} \\ \Longrightarrow \quad & f_1^{\bar\sigma} = \sum i a_i^\sigma x^{i-1} = \left(\sum a_i^\sigma x^i\right)' = (f^{\bar\sigma})' = (f^{\bar\sigma})_1 \end{aligned}$$

   Sei die Aussage für $i-1, i$ richtig. Dann gilt

$$\begin{aligned} f_{i-1}^{\bar\sigma} &= q_i^{\bar\sigma} f_i^{\bar\sigma} - f_{i+1}^{\bar\sigma} \quad \text{mit } \operatorname{grad} f_{i+1}^{\bar\sigma} < \operatorname{grad} f_i^{\bar\sigma} \\ (f^{\bar\sigma})_{i-1} &= q_i'(f^{\bar\sigma})_i - (f^{\bar\sigma})_{i+1} \end{aligned}$$

   Mit Eindeutigkeit des Euklidischen Algorithmus folgt: $f_{i+1}^{\bar\sigma} = (f^{\bar\sigma})_{i+1}$.

   (b) $M^\sigma = \max\{1, |a_0^\sigma| + \ldots + |a_{m-1}^\sigma|\}$ ist das „M“ für $f^{\bar\sigma}$, da σ ein Ordnungsisomorphismus ist.

   (c) Es gilt:

$$(f_i)^{\bar\sigma}(M^\sigma) = (f_i(M))^{\bar\sigma}, \quad \text{da} \quad \left(\sum b_j M^j\right)^\sigma = \sum b_j^\sigma (M^\sigma)^j$$

   Daraus folgt: die Sturmschen Ketten von f an der Stelle M und von $f^{\bar\sigma}$ an der Stelle M^σ haben dieselben Vorzeichen an jedem i. Somit ist $v(-M) - v(M) = v^*(-M^\sigma) - v^*(M^\sigma)$, wobei v^* die Anzahl der Vorzeichen für die Kette von $f^{\bar\sigma}$ sei.

2. Definition von $\sigma^* : R \to S$ und Eindeutigkeit. Sei $\alpha \in R$. Nach Definition (3.10.5) ist α algebraisch über K, sei $p_\alpha \in K[x]$ das definierende Polynom. Dieses habe in R die Nullstellen $\alpha_1, \ldots, \alpha_n$ mit $\alpha_1 < \ldots < \alpha_n$, sei etwa $\alpha = \alpha_k$. Nach (1) hat $p_\alpha^{\bar\sigma}$ genau n Nullstellen $\beta_1 < \ldots < \beta_n$ in S. Setze $\alpha^{\sigma^*} = \beta_k$.

   Das ist offensichtlich wohldefiniert und einzige Möglichkeit σ zu Isomorphismus $\tau : R \to S$ fortzusetzen: Wie immer muss τ Nullstellen des Polynoms p_α in R abbilden auf Nullstellen des Polynoms $p_\alpha^{\bar\tau} = p_\alpha^{\bar\sigma}$ (da $p_\alpha \in K[x]$). Nach Korollar (3.10.7) ist τ ein Ordnungsisomorphismus, d.h. die Ordnung der Nullstellen bleibt erhalten: $\alpha^\tau = \alpha_k^\tau = \beta_k = \alpha^{\sigma^*}$.

3. *Behauptung:* σ^* ist bijektiv. *Beweis:* Definiere Umkehrabbildung ρ in derselben Weise: Für $\beta \in S$ sei $p \in K^\sigma[x]$ das definierende Polynom, seien $\beta_1 < \ldots < \beta_m$ Nullstellen davon in S und $\alpha_1 < \ldots < \alpha_m$ Nullstellen von $p^{\bar{\sigma}^{-1}}$ in R. Ist $\beta = \beta_l$, so sei $\beta^\rho = \alpha_l$. Nach Satz (I.4.6) ist $p^{\bar{\sigma}^{-1}}$ irreduzibel in $K[x]$ und somit $\alpha_l^{\sigma^*} = \beta_l = \beta$. Somit ist $\rho\sigma^* = \mathrm{id}_S$, genauso $\sigma^*\rho = \mathrm{id}_R$.

4. *Behauptung:* Ist $E = \{\alpha_1, \ldots, \alpha_n\}$ eine endliche Teilmenge von R, wobei $\alpha_1 < \ldots < \alpha_n$, so existiert ein Monomorphismus $\sigma_E : K(E) \to S$ mit $\alpha_1^{\sigma_E} < \ldots < \alpha_n^{\sigma_E}$.

   Beweis: Es gilt: $\alpha_{i+1} - \alpha_i > 0$. Nach (3.10.7) existiert $\beta_i \in R$ mit $\beta_i^2 = \alpha_{i+1} - \alpha_i$. Sei f ein Polynom aus $K[x]$, das sämtliche α_i und β_i zu Nullstellen hat. Sei N die Menge der Nullstellen von f in R und $L = K(N)$. Nach dem Satz vom primitiven Element (I.9.6) existiert $\alpha \in L$ mit $L = K(\alpha)$. Sei $p_\alpha \in K[x]$ das definierende Polynom von α. Nach (1) existiert $\beta \in S$ mit $p_\alpha^{\bar{\sigma}}(\beta) = 0$. Der Satz (I.4.6) liefert: ex existiert $\tau : K(\alpha) = L \to K^\sigma(\beta)$ mit $\tau|_K = \sigma$.

   Es gilt: $K(E) \leq K(N) = L$. Sei $\sigma_E = \tau|_{K(E)}$, dann gilt:

   $$\alpha_{i+1}^\tau - \alpha_i^\tau = (\alpha_{i+1} - \alpha_i)^\tau = (\beta_i^2)^\tau = (\beta_i^\tau)^2 > 0$$

   also ist $\alpha_i^\tau < \alpha_{i+1}^\tau$ für alle i.

5. *Behauptung:* $(\alpha + \beta)^{\sigma^*} = \alpha^{\sigma^*} + \beta^{\sigma^*}$ und $(\alpha \cdot \beta)^{\sigma^*} = \alpha^{\sigma^*} \cdot \beta^{\sigma^*}$.

   Beweis: Sei E die Menge aller Nullstellen der definierenden Polynome von $\alpha, \beta, \alpha + \beta$ und $\alpha - \beta$. Betrachte σ_E aus (4). Für $\gamma \in E$ ist dann $\gamma^{\sigma_E} = \gamma^{\sigma^*}$: Betrachte dazu p_γ mit Nullstellen $\gamma_1 < \ldots < \gamma_n$ und $\gamma = \gamma_k$. Nach Definition von σ^* ist γ^{σ^*} die k-te Nullstelle von $p_\gamma^{\bar{\sigma}}$. Anderseits folgt aus $\gamma_1, \ldots, \gamma_n \in E$ mit (4), dass $\gamma_1^{\sigma_E} < \ldots < \gamma_n^{\sigma_E}$, also $\gamma_k^{\sigma_E}$ ist die k-te Nullstelle von $p_\gamma^{\bar{\sigma}_E} = p_\gamma^{\bar{\sigma}}$. Nun gilt

   $$(\alpha + \beta)^{\sigma^*} = (\alpha + \beta)^{\sigma_E} = \alpha^{\sigma_E} + \beta^{\sigma_E} = \alpha^{\sigma^*} + \beta^{\sigma^*}$$

   Genauso für die Multiplikation.

3.10.10 Der Ordnungsabschluß von $\mathbb{Q}$

LEMMA: Seien $K \leq L$ Körper und sei $A = \mathfrak{A}(K, L) = \{\alpha \in L \mid \alpha$ algebraisch über $K\}$. Dann gilt:

1. Ist L algebraisch abgeschlossen, so ist A ein algebraischer Abschluss von K.
2. Ist L ordnungsabgeschlossen, so ist A ein Ordnungsabschluß von K.

BEWEIS:

1. Nach (I.5.7) ist A ein Körper und natürlich algebraisch über K. Sei $f \in A[x]$. Da L algebraisch abgeschlossen ist, gilt:

   $$f = c(x - \alpha_1) \dots (x - \alpha_n) \text{ mit } \alpha_i \in L$$

   Mit (I.5.6) folgt: α_i sind algebraisch über A, also auch über K. Daraus folgt: $\alpha_i \in A$, also A ist algebraisch abgeschlossen.

2. Offensichtlich ist A algebraisch über K. Zu zeigen bleibt: A ist ordnungsabgeschlossen. Wir weisen (2) aus (3.10.7) nach. Sei $f \in A[x]$ mit $\operatorname{grad} f$ ungerade. Mit (3.10.7) existiert $\alpha \in L$ mit $f(\alpha) = 0$. Genauso wie oben folgt: $\alpha \in A$.

   Sei nun $a \in A$ mit $a > 0$. Nach (3.10.7) existiert $\beta \in L$ mit $\beta^2 = a$, also β Nullstelle von $x^2 - a \in A[x]$. Daraus folgt: $\beta \in A$. Mit Satz (3.10.7) folgt nun: A ist ordnungsabgeschlossen.

SATZ: Sei $\mathbb{A} = \mathfrak{A}(\mathbb{Q}, \mathbb{C}) = \{\alpha \in \mathbb{C} \mid \alpha$ algebraisch über $\mathbb{Q}\}$. Dann gilt:

1. $\mathbb{A}$ ist ein algebraischer Abschluss von $\mathbb{Q}$.
2. $\mathbb{A} \cap \mathbb{R}$ ist ein Ordnungsabschluss von $\mathbb{Q}$.
3. $\mathbb{A}$ enthält unendlich viele verschiedene Ordnungsabschlüsse von $\mathbb{Q}$.

BEWEIS: (1) und (2) folgen aus Lemma mit $K = \mathbb{Q}$ und $L = \mathbb{C}$ bzw. $L = \mathbb{R}$. Zum Beweis von (3) zeigen wir: Für jedes $n \in \mathbb{N}$ existieren $2n+1$ verschiedene Ordnungasbschlüsse von $\mathbb{Q}$ in $\mathbb{A}$.

Beweis: Sei $r = 2n+1$ und $f = x^r - 2 \in \mathbb{Q}[x]$. f ist irreduzibel nach Eisenstein, $\left\{ \varepsilon \sqrt[r]{2} \;\middle|\; \varepsilon \text{ } r\text{-te Einheitswurzel} \right\}$ ist die Menge der Nullstellen von f in $\mathbb{C}$. Für jedes solche ε existiert ein Isomorphismus von $\mathbb{R} \geq \mathbb{Q}(\sqrt[r]{2}) \to \mathbb{Q}(\varepsilon \sqrt[r]{2})$.

Nach Lemma (3.8.8) existiert Anordnung auf $\mathbb{Q}(\varepsilon\sqrt[r]{2})$. Nach Satz (3.10.5) existiert ein Ordnungsabschluß R_ε von $\mathbb{Q}(\varepsilon\sqrt[r]{2})$ im algebraischen Abschluss von $\mathbb{Q}(\varepsilon\sqrt[r]{2})$, also in $\mathbb{A}$. Nach Definition vom Ordnungsabschluß sind alle R_ε Ordnungsabschlüsse von Q.

Zu zeigen bleibt: alle R_ε sind verschieden. Wäre $R_{\varepsilon_1} = R_{\varepsilon_2} =: R$, so enthielte R sowohl $\varepsilon_1\sqrt[r]{2}$ als auch $\varepsilon_2\sqrt[r]{2}$. Wir zeigen: Ist R geordnet, so enthält R höchstens eine Nullstelle von $x^r - a$ für r ungerade, $a \in R$.

Beweis: Angenommen α_1, α_2 sind Nullstellen mit etwa $\alpha_1 < \alpha_2$. Es folgt: $\alpha_1^r = \alpha^{2n+1}$ hat dasselbe Vorzeichen wie α_1. Weiter ist $\alpha_2^r = \alpha_1^r = a$, somit entweder $0 < \alpha_1 < \alpha_2$ oder $\alpha_1 < \alpha_2 < 0$. Im ersten Fall gilt (Induktion nach m):

$$\alpha_1^m < \alpha_2^m \Rightarrow \alpha_1^{m+1} = \alpha_1\alpha_1^m < \alpha_1\alpha_2^m < \alpha_2\alpha_2^m = \alpha_2^{m+1}$$

Also $\alpha_1^r < \alpha_2^r$. Im zweiten Fall gilt:

$$0 < -\alpha_2 < -\alpha_1 \Rightarrow -\alpha_2^r = (-\alpha_2)^r < (-\alpha_1)^r = -\alpha_1^r$$

KOROLLAR:

1. $\mathrm{Aut}(\mathbb{A} \cap \mathbb{R}) = 1$ (Korollar (3.10.9))
2. Sei Ω die Menge der in $\mathbb{A}$ enthaltenen Ordnungsabschlüsse von $\mathbb{Q}$. Für $R \in \Omega$ sei $\sigma_R : \mathbb{A} \to \mathbb{A}$ mit $a + bi \mapsto a - bi$, wobei $a, b \in R$. Dann ist $\{\sigma_R \mid R \in \Omega\}$ eine unendliche Konjugiertenklasse von Elementen der Ordnung 2 in $\mathrm{Aut}\,\mathbb{A}$.

BEWEIS:

2. Nach (3.10.7) ist $R(i) \subseteq \mathbb{A}$ algebraisch abgeschlossen, also $R(i) = \mathbb{A}$. Trivialerweise ist $\sigma_R \in \mathrm{Aut}(\mathbb{A})$, weiter ist $\sigma_R^2 = \mathrm{id}$ und $\langle\sigma_R\rangle\,\mathfrak{F} = R$. Nach (3.10.9) existiert ein Isomorphismus $\tau_0 : R \to S$. Der lässt sich nach Satz I.4.6 fortsetzen zu $\tau : \mathbb{A} \to \mathbb{A}$, wobei $i \mapsto i$ und somit $\sigma_R^\tau = \sigma_S$.

3.11 Der Satz von ARTIN-SCHREIER

SATZ: Sei A algebraisch abgeschlossen und $K < A$ mit $[A : K] < \infty$. Dann ist $[A : K] = 2$, $A = K(i)$ mit $i^2 = -1$ und K ist reell-abgeschlossen.

3.11.1 Kriterium für reell-abgeschlossen

LEMMA: Ist K ein Köper (beliebiger Charakteristik), so dass $i = \sqrt{-1} \notin K$ und $K(i)$ algebraisch abgeschlossen, so ist K formal-reell (also reell-abgeschlossen nach (3.10.1) und (3.10.7)).

BEWEIS: Wir zeigen, dass jede Summe von Quadraten ein Quadrat ist. Dann folgt aus $i \notin K$, dass -1 keine solche Summe ist. Dazu genügt zu zeigen: sind $a, b \in K$ mit $b \neq 0$, so ist $a^2 + b^2$ ein Quadrat.

Sei $A = K(i)$ und $g \in A(x)$ definiert durch

$$\begin{aligned} g &= (x - \sqrt{a+bi})(x + \sqrt{a+bi})(x - \sqrt{a-bi})(x + \sqrt{a-bi}) \\ &= (x^2 - (a+bi))(x^2 - (a-bi)) \\ &= ((x^2 - a) + bi)((x^2 - a) - bi) \\ &= (x^2 - a)^2 + b^2 \in K[x] \end{aligned}$$

Ist $f \in K[x]$ irreduzibel, so ist $K(f) \leq A = K(i)$, also $[K(f) : K] \leq 2$, d.h. $\operatorname{grad} f \leq 2$. Somit folgt: g ist reduzibel. Hätte g in K eine Nullstelle, so wäre $\sqrt{a \pm bi} \in K$, also $i \in K$, da $b \neq 0$, Widerspruch. Somit ist $g = fh$ mit irreduziblen Polynomen $f, g \in K[x]$ vom Grad 2. Sei o.B.d.A. $x - \sqrt{a+bi} \mid f$ in $A[x]$. Aus der Eindeutigkeit der Primfaktorzerlegung ergeben sich für f folgende drei Möglichkeiten:

$$f = (x - \sqrt{a+bi})(x + \sqrt{a+bi}) = x^2 - (a+bi)$$

Dies ist ein Widerspruch, da $a + bi \notin K$. Die anderen Möglichkeiten sind

$$\begin{aligned} f &= (x - \sqrt{a+bi})(x - \sqrt{a-bi}) = x^2 + (\ldots)x + \sqrt{a^2+b^2} \in K[x] \\ f &= (x - \sqrt{a+bi})(x + \sqrt{a-bi}) = x^2 + (\ldots)x - \sqrt{a^2+b^2} \in K[x] \end{aligned}$$

3.11.2 Inseparable Körper

Für den Beweis des Satzes müssen wir $P\mathfrak{F} \leq A$ betrachten mit $P \leq \operatorname{Gal}(A/K)$. Es gibt drei Fälle:

1. Der gute Fall: $\operatorname{char} K \neq p$.
2. Weniger gut: $\operatorname{char} K = p$, separabel.
3. Schlechter Fall: $\operatorname{char} K = p$, inseparabel.

Im folgenden Lemma zeigen wir: Fall 3 tritt nicht auf.

LEMMA: Sei K ein Körper, $\operatorname{char} K = p > 0$. Ist K nicht vollkommen, so existiert zu jedem $n \in \mathbb{N}$ ein irreduzibles Polynom vom Grade p^n in $K[x]$. Genauer: ist $a \in K$ keine p-te Potenz (Satz I.9.5), so ist $f_n = x^{p^n} - a \in K[x]$ irreduzibel.

BEWEIS: Sie a wie im Lemma, $f = x^{p^n} - a$ und sei $\alpha \in L = K(f)$ Nullstelle von f. Dann gilt wegen $\operatorname{char} L = p$:

$$0 = \alpha^{p^n} - a \Longrightarrow \alpha^{p^n} = a \Longrightarrow f = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$$

Sei $f = g_1 \dots g_m$ Zerlegung in irreduzible Polynome $g_i \in K[x]$. In $L[x]$ ist $g_i = (x - \alpha)^{r_i}$, d.h. $g_i(\alpha) = 0$. Somit mit (I.4.4) gilt: $p_\alpha \mid g_i$, wobei p_α das definierende Polynom von α über K ist. Da p_α und g_i irreduzibel sind, folgt: $p_\alpha = g_i$, also $(x - \alpha)^{p^n} = f = p_\alpha^m$. Es folgt: $p^n = \operatorname{grad} f = m \cdot \operatorname{grad} p_\alpha$, d.h. m ist eine p-Potenz. Es gilt nun:

$$-a = f(0) = p_\alpha(0)^m \Rightarrow (-p_\alpha(0))^m = -p_\alpha(0)^m = a$$

Wäre $m = p^r$ mit $r \geq 1$, so wäre[16]

$$(-p_\alpha(0)^{p^{r-1}})^p = -p_\alpha(0)^{p^r} = a$$

Dies ist ein Widerspruch zur Voraussetzung. Also folgt: $m = p^0 = 1$, d.h. f ist irreduzibel.

3.11.3 Separable Körper mit Charakteristik p

LEMMA: Seien $K \leq L$ Körper, L galoissch über K und $[L : K] = p = \operatorname{char} K$. Dann existiert $\alpha \in L$ so, dass $f = x^p - x - \alpha \in L[x]$ irreduzibel in $L[x]$ ist.

BEWEIS: Nach Satz (2.5.8) ist $L = K(\beta)$ mit einem Ultraradikal β über K, d.h. $b := \beta^p - \beta \in K$. Somit ist $p_\beta = x^p - x - b$, da $[K(\beta) : K] = p$. Sei $\alpha = b\beta^{p-1} \in L$ und $f = x^p - x - \alpha \in L[x]$. Wir zeigen:

($\star$) f hat keine Nullstelle in L.

Beweis: Angenommen es existiert $\gamma \in L$ mit $f(\gamma) = 0$. Nach (I.4.4)

[16] Man beachte, dass dies auch im Falle $p = 2$ richtig ist, weil dann $-1 = +1$ gilt.

existiert $g \in K[x]$ mit $\operatorname{grad} g \leq p-1$ so, dass $\gamma = g(\beta)$. Sei $g = \sum_{i=0}^{p-1} a_i x^i$ und $h = \sum_{i=0}^{p-1} a_i^p x^i \in K[x]$, dann gilt

$$\begin{aligned} g^p &\overset{\operatorname{char} K = p}{=} \sum_{i=0}^{p-1} a_i^p (x^p)^i = h(x^p) \\ b\beta^{p-1} &= \alpha = \gamma^p - \gamma = g(\beta)^p - g(\beta) = h(\beta^p) - g(\beta) \\ &= h(b+\beta) - g(\beta) = \sum_{i=0}^{p-1} a_i^p (b+\beta)^i - \sum_{i=0}^{p-1} a_i \beta^i \end{aligned}$$

Da $1, \beta, \ldots, \beta^{p-1}$ eine K-Basis von L ist, müssen die Koeffizienten von β^{p-1} links und rechts gleich sein, also $b = a_{p-1}^p - a_{p-1}$. Somit ist $a_{p-1} \in K$ Nullstelle von $x^p - x - b = p_\beta$, Widerspruch, da p_β irreduzibel ist.

Aus $(\star)$ folgt: f ist irreduzibel. Denn ist δ Nullstelle von f in $L(f)$, so ist nach Satz (2.5.7) $[L(\delta) : L] = p$ oder 1, also p nach $(\star)$. Somit ist $f = x^p - x - \alpha = p_\delta$ das definierende Polynom von δ über L, also irreduzibel.

3.11.4 Separable Körper mit Charakteristik ungleich p

LEMMA: Seien $K \leq L$ Körper, L galoissch über K und $[L : K] = p \neq \operatorname{char} K$ für $p \in \mathbb{P}$. Ferner enthalte K die p-ten Einheitswurzeln und für $p = 2$ sei -1 ein Quadrat in K. Dann existiert $\alpha \in L$ so, dass $x^p - \alpha$ irreduzibel in $L[x]$ ist.

BEWEIS: Sei $G = \operatorname{Gal}(L/K)$, dann ist $|G| = p$, also $G = \langle \sigma \rangle$. Nach Satz (2.5.6) existiert $\alpha \in L$ mit $L = K(\alpha)$ und $\alpha^p \in K$. Sei $f = x^p - \alpha \in L[x]$. Wir zeigen:

$(\star)$ f hat keine Nullstelle in L.

Beweis: Angenommen es existiert $\beta \in L$ mit $f(\beta) = 0$, also $\beta^p = \alpha$. Dann ist $\beta^{p^2} = \alpha^p \in K = \langle \sigma \rangle \mathfrak{F}$ und somit

$$(\beta^\sigma)^{p^2} = (\beta^{p^2})^\sigma = \beta^{p^2} \Longrightarrow \left(\frac{\beta^\sigma}{\beta}\right)^{p^2} = 1 \tag{1}$$

Sei $\delta = \frac{\beta^\sigma}{\beta}$, also $\delta^{p^2} = (\delta^p)^p = 1$. Dann ist also δ^p eine p-te Einheitswurzel, also $\delta^p \in K$. Daraus folgt:

$$(\delta^\sigma)^p = (\delta^p)^\sigma = \delta^p \Longrightarrow \left(\frac{\delta^\sigma}{\delta}\right)^p = 1 \tag{2}$$

Sei $\varepsilon = \frac{\delta^\sigma}{\delta}$. Dann gilt: $\beta^\sigma = \beta\delta$ und $\delta^\sigma = \varepsilon\delta$. Weiter gilt:

$$\beta^{\sigma^i} = \beta\delta^i\varepsilon^{\frac{i(i-1)}{2}} \text{ für } i = 1, \ldots, p \tag{3}$$

Beweis von (3): Induktion nach i. Der Fall $i = 1$ ist klar. Sei die Aussage für i richtig, dann gilt:

$$\begin{aligned} \beta^{\sigma^{i+1}} &= (\beta^{\sigma^i})^\sigma = \left(\beta\delta^i\varepsilon^{\frac{i(i-1)}{2}}\right)^\sigma = \beta^\sigma(\delta^\sigma)^i(\varepsilon^\sigma)^{\frac{i(i-1)}{2}} \\ &\overset{(2)}{=} \beta\delta(\varepsilon\delta)^i\varepsilon^{\frac{i(i-1)}{2}} = \beta\delta^{i+1}\varepsilon^{\frac{i(i+1)}{2}} \end{aligned}$$

Da $|G| = p$, folgt: $\sigma^p = \mathrm{id}$, also

$$\beta = \beta^{\sigma^p} \overset{(3)}{=} \beta\delta^p\varepsilon^{\frac{p(p-1)}{2}} \Longrightarrow 1 = \delta^p\varepsilon^{\frac{p(p-1)}{2}}$$

Ist $p \neq 2$, so ist $\frac{(p-1)}{2} \in \mathbb{Z}$, also $\varepsilon^{\frac{p(p-1)}{2}} = 1$ nach (2), daraus folgt: $1 = \delta^p$. Sei $p = 2$, dann folgt mit (1):

$$1 = \delta^{p^2} = \delta^4 \overset{Vor.}{\Longrightarrow} \delta = \sqrt{\pm 1} \in K \Longrightarrow \varepsilon\delta \overset{(3)}{=} \delta^\sigma \overset{\delta\in K}{=} \delta \Longrightarrow \varepsilon = 1$$

Mit obiger Rechnung folgt: $1 = \delta^p\varepsilon^{\frac{p(p-1)}{2}} = \delta^p$ (4)

Daraus ergibt sich:

$$\begin{aligned} \alpha^\sigma &\overset{Def.}{=} (\beta^p)^\sigma = (\beta^\sigma)^p \overset{(3)}{=} (\beta\delta)^p = \beta^p\delta^p \overset{(4)}{=} \beta^p = \alpha \\ &\Longrightarrow \alpha \in \langle\sigma\rangle\,\mathfrak{F} = K \end{aligned}$$

Dies ist ein Widerspruch zu $L = K(\alpha)$, somit folgt $(\star)$.

Sei nun ω eine Nullstelle von f in $L(f)$. Mit (2.5.1) folgt: $[L(\omega) : L] = p$ oder 1. Mit $(\star)$ folgt daraus: $[L(\omega) : L] = p$, somit ist $x^p - \alpha = p_\omega$ das definierende Polynom von ω über L, also irreduzibel.

3.11.5 Hauptsatz (Artin-Schreier, 1927)

Satz: Sei A ein algebraisch abgeschlossener Körper. Ist K ein echter Teilkörper von A und $[A : K] < \infty$, so ist K reell-abgeschlossen und $A = K(\sqrt{-1})$. Insbesondere ist $[A : K] = 2$, die Menge S der Quadrate ungleich 0 in K abgeschlossen unter Addition und $K = S \cup \{0\} \cup -S$

KOROLLAR:

1. Ist A algebraisch abgeschlossen, $\operatorname{char} A = p > 0$ und $K < A$, so ist $[A : K] = \infty$.
2. Ist L ordnungsabgeschlossen und $K < L$, so ist $[L : K] = \infty$.

BEWEIS: Wir zeigen (mit $i = \sqrt{-1}$):

($\star$) Ist $K < A$ mit $[A : K] < \infty$, so ist $i \notin K$.

Dann sind wir fertig: Wende ($\star$) an auf $K(i)$. Wäre $K(i) < A$ so folgte mit ($\star$): $i \notin K(i)$, es gilt also: $K(i) = A$. Nach (3.11.1) ist K formal-reell, nach (3.10.1) anordbar, also ordnungsabgeschlossen nach (3.10.7), also reell-abgeschlossen nach Bemerkung (3.10.7). „Insbesondere“ folgt aus (3.10.7).

Beweis von ($\star$):

1. *Behauptung:* A ist galoissch über K.

   Beweis: Sonst wäre A inseparabel über K, also K nicht vollkommen. Nach (3.11.2) folgt: $[A : K] = \infty$ (Zerfällungskörper von irreduziblen Polynomen beliebig großen Grades liegen in A), Widerspruch.

2. *Behauptung:* Wir können annehmen: $[A : K] = p$ für eine Primzahl p.

   Beweis: $\operatorname{Gal}(A/K)$ hat eine Untergruppe H von Primzahlordnung p. Mit dem Hauptsatz der Galoistheorie folgt: $[A : H\mathfrak{F}] = |H| = p$. Zeigen wir $i \notin H\mathfrak{F}$, so gilt auch $i \notin K$. Somit sei o.B.d.A. $K = H\mathfrak{F}$.

3. *Behauptung:* $\operatorname{char} K \neq p$.

   Beweis: Sonst wäre A nicht algebraisch abgeschlossen nach (3.11.3).

4. *Behauptung:* $i \notin K$.

   Beweis: Da A algebraisch abgeschlossen ist, existiert eine primitive p-te Einheitswurzel $\varepsilon \in A$. Dann ist mit (2.4.3) $[K(\varepsilon) : K] \leq p-1$, anderseits teilt $[K(\varepsilon) : K]$ den Grad $[A : K] = p$, somit folgt: $K(\varepsilon) = K$. Wäre $i \in K$, so folgte aus (3.11.4), dass A nicht algebraisch abgeschlossen ist, Widerspruch.

BEWEIS DES KOROLLARS:

1. Trivial.
2. Sei L ordnungsabgeschlossen und $[L : K] < \infty$. Mit (3.10.7) folgt: $L(i)$ ist algebraisch abgeschlossen. Mit dem Satz folgt: $[L(i) : K] = 2$, also $K = L$.

3.11.6 Automorphismen von $\mathbb{C}$

SATZ: Jede endliche Untergruppe $H \neq 1$ von $\operatorname{Aut}\mathbb{C}$ hat die Ordnung 2 und ist von der Form $H = \langle \sigma_R \rangle$, $\sigma_R : \mathbb{C} \to \mathbb{C}$ mit $a + bi \mapsto a - bi$ für $a, b \in R$, wobei $R \leq \mathbb{C}$ ordnungsabgeschlossen und $\mathbb{C} = R(i)$ ist.

BEWEIS: Nach dem Satz von Artin (I.10.4) folgt: $[\mathbb{C} : H\mathfrak{F}] = |H|$, also $|H| = 2$ und $\mathbb{C} = H\mathfrak{F}(i)$.

FRAGE: Gibt es solche $R \neq \mathbb{R}$?

ANTWORT: Ja! Überabzählbar viele und nichtarchimedisch geordnete.

Index