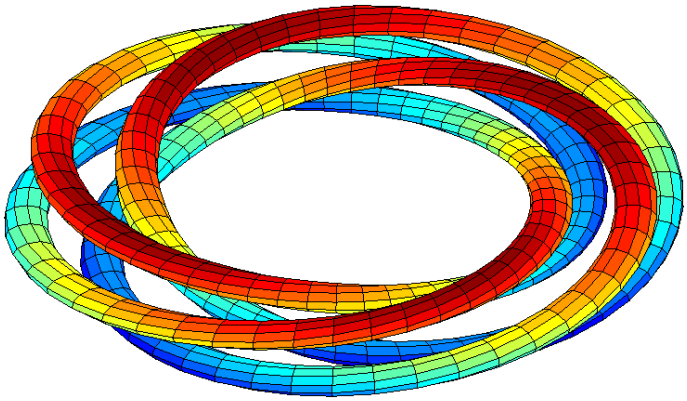
Skript zur Vorlesung

Algebra

Private Mitschrift



Gruppen, Ringe, Körper

gelesen von

Prof. Dr. Alexander Prestel

Martin Gubisch

Konstanz, Wintersemester 2006/2007

Inhaltsverzeichnis

Problemstellungen der Algebra

Mathematische Vorgehensweise zur Problemlösung.

1. Problemstellung (in -g en Unbestimmten (explizite Beschreibung der gesuchten Größen)
2. Berechnung (durch Eins-g en Unbestimmten (explizite Beschreibung der gesuchten Größen)
3. Berechnung (durch Eins Form einer "Textaufgabe")
4. Modellierung (implizite mathematische Beschreibung mit Hilfe von Unbestimmten)
5. Auflösung nach d - -g en Unbestimmten (explizite Beschreibung der gesuchten Größen)
6. Berechnung (durch Einsg etzen gegebener Werte)

Dazu: Sätze über die Lösbarkeit (Existenz und Eindeutigkeit) und Lösungsverfahren (zur konkreten Berechnung).

Beschreibung: Sehr oft durch Gleichungssysteme, zum Beispiel:

1. Lineare Systeme über $\mathbb{R}$ oder $\mathbb{C}$: **Lineare Algebra**
2. Differenzialgleichungen: **Analysis, Theorie und Numerik für Differenzialgleichungen**
3. Algebraische Gleichung in einer Unbestimmten z.B. über $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{F}_p$: **Algebra**
4. Algebraische Gleichungen in n Unbestimmten über $\mathbb{C}$: **Algebraische Geometrie**

Delisches Problem. Es ist unmöglich, einen Würfel mit Volumen 2 nur mit Zirkel und Lineal zu konstruieren.

Zusammenhang mit nichtlinearen Gleichungen: Die Seitenlänge x des Würfels löst

$$X^3 - 2 = 0,$$

ist also Nullstelle eines Polynoms dritten Grades.

Dreiteilung von Winkeln. Es ist unmöglich, den 60°-Winkel $\alpha = \frac{\pi}{3}$ mit Zirkel und Lineal dreizuteilen.

Für α gilt wegen $(e^{i\frac{\alpha}{3}})^3 = e^{i\alpha}$ der Zusammenhang

$$\frac{1}{2} = \mathrm{Re}\left(\cos\frac{\alpha}{3} + i\sin\frac{\alpha}{3}\right)^3 = \cos^3\frac{\alpha}{3} + 3\cos\frac{\alpha}{3}\left(-\sin^2\frac{\alpha}{3}\right) = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3},$$

d.h. der exakte Wert $\alpha = \cos\frac{\alpha}{3}$ ist gegeben als Lösung der kubischen Gleichung

$$x^3 - \frac{3}{4}x - \frac{1}{8} = 0.$$

Quadratur des Kreises. Unmöglichkeit der Konstruktion eines Quadrates mit Flächeninhalt π mit Zirkel und Lineal.

Die Seitenlängen a des Quadrats lösen

$$x^2 - \pi = 0.$$

Da π "transzendent über $\mathbb{Q}$" ist, d.h. Nullstelle keinen Polynoms mit rationalen Koeffizienten, ist die Konstruktion nicht möglich.

Konstruktion eines regelmäßigen p-Ecks. Es ist nicht möglich, mit Zirkel und Lineal ein regelmäßiges 7-Eck zu konstruieren.

Ein $(\frac{360}{7})°$-Winkel $\alpha = e^{\frac{2\pi i}{7}}$ ist nämlich Nullstelle des Polynoms

$$X^7 - 1 = (X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1).$$

Da $7-1$ keine Zweierpotenz ist, ist die Konstruktion nicht möglich. Selbiges Argument funktioniert auch für 11-Ecke, 13-Ecke u.s.w..

Auflösung in Wurzeln. Für polynomiale Gleichungen bis zum Grad vier existieren explizite Lösungsformeln:

1. Für quadratische Gleichungen:

$$x^2 + ax + b = 0 \qquad \Longrightarrow \qquad x_{1,2} = \frac{1}{2}(-a \pm \sqrt{D})$$

mit Diskriminante

$$D = a^2 - 4b.$$

2. Für kubische Gleichungen: Betrachte

$$x^3 + a_2x^2 + a_1x + a_0 = 0.$$

Substitutionsansatz: Ersetze x durch $x - \frac{1}{3}a_2$, dann ist

$$x^3 + ax + b = 0.$$

Setze

$$D := -(4a^3 + 27b^2); \qquad A := \sqrt[3]{-\frac{27}{2}b + \frac{3}{2}\sqrt{-3D}}; \qquad B := \sqrt[3]{-\frac{27}{2}b - \frac{3}{2}\sqrt{-3D}}$$

und $\rho := -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ (d.h. $\rho^3 = 1$). Dann liefern die Cardanische Formeln:

$$x_1 = \frac{1}{3}(A + B); \qquad x_2 = \frac{1}{3}(\rho^2 A + \rho B); \qquad x_3 = \frac{1}{3}(\rho A + \rho^2 B).$$

3. Auflösung von Gleichungen vierten Grades: Formel von Ferrari (16. Jh.).
4. Nichtauflösbarkeit von Gleichungen fünften Grades bewiesen durch Abel 1826.
5. 1831: Endgültige Lösung des Auflösbarkeitsproblems durch Galois.

1 Gruppen

1.1 Grundbegriffe

1.1. Wiederholung

1. Seien G eine Menge und $\circ : G \times G \to G$ eine Abbildung. $(G, \circ)$ heißt Gruppe, falls gelten:

   a) $\circ$ ist assoziativ, d.h. $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$.
   b) G besitzt ein neutrales Element, d.h. $\exists e \in G : \forall x \in G : x \circ e = e \circ x = x$.
   c) Jedes Element in G besitzt ein Inverses, d.h. $\forall x \in G : \exists x^{-1} \in G : x \circ x^{-1} = x^{-1} \circ x = e$.

   $(G, \circ)$ heißt abelsch (kommutativ), falls für alle $x, y \in G$ gilt: $x \circ y = y \circ x$.

2. $H \subseteq G$ heißt Untergruppe von G (in Zeichen: $H < G$), falls gelten:

   a) $\forall x, y \in H : x \circ y \in H$.
   b) $e \in H$.
   c) $\forall x \in H : x^{-1} \in H$.

3. H heißt Normalteiler von G (in Zeichen: $H \lhd G$), falls $xHx^{-1} = H$ bzw. $xH = Hx$ für alle $x \in G$.

   xH heißt Linksnebenklasse und Hx Rechtsnebenklasse von H. Es gilt: $Hx \cap Hy \neq \emptyset \Rightarrow Hx = Hy$.

4. Sind H eine Untergruppe von G und G ist disjunkte Vereinigung $G = Hx_1 \cup ... \cup Hx_n$ für gewisse $x_1, ..., x_n \in G$, dann gilt: $|G| = n|H|$.

   $|G : H| := \frac{|G|}{|H|}$ heißt der Index von H in G.

5. Ist H Normalteiler in G, so definiert $(xH)(yH) := xyH$ eine Multiplikation auf den Nebenklassen. $G/H := \{xH \mid x \in G\}$ wird dadurch zu einer Gruppe, der Quotientengruppe von G nach H.
6. $f : G \to H$ heißt Gruppenhomomorphismus (in Zeichen: $f \in \mathrm{Hom}(G, H)$), falls für alle $x, y \in G$ gilt: $f(xy) = f(x)f(y)$. Ist f zusätzlich bijektiv, dann heißt f Isomorphismus (in Zeichen: $G \cong H$). Ein surjektiver Homomorphismus heißt Epimorphismus, ein injektiver Homomorphismus Monomorphismus.

   $\mathrm{Kern}(f) := \{x \in G \mid f(x) = e\}$ ist ein Normalteiler von G und G/N ist isomorph zu $\mathrm{Bild}(f) := f(G)$ via $gN \mapsto f(g)$ (Homomorphiesatz). ◊

1.2. BEISPIEL

Die folgenden Abbildungen sind Gruppenhomomorphismen:

1. $\exp : (\mathbb{R}, +) \to (\mathbb{R}, \cdot),\ x \mapsto e^x$, denn es gilt $e^{x+y} = e^x \cdot e^y$.
2. Sei $l : V \to W$ eine lineare Abbildung zwischen Vektorräumen, dann ist $l(v + w) = l(v) + l(w)$.
3. Sei $N \lhd G$, dann definiert der kanonischer Epimorphismus $\sigma(g) := gN$ einen Homomorphismus zwischen G und G/N, denn $(xN)(yN) = (xy)N$. ◊

1.3. SATZ (Erster Isomorphiesatz)

Seien $U < G$ und $N \lhd G$. Dann gelten:

1. $UN < G$.
2. $(U \cap N) \lhd U$.
3. $N \lhd UN$.
4. $U/(U \cap N) \cong (UN)/N$.

BEWEIS.

1. a) $1 \in UN$: $1 = 1 \cdot 1 \in UN$.

   b) $a, b \in UN \Rightarrow ab \in UN$:

   Seien $a, b \in UN$. Wähle $g, g' \in U$ und $h, h' \in N$ mit $a = gh$ und $b = g'h'$. Dann gilt:

   $$g'^{-1}hg' \in N \Rightarrow ab = ghg'h' = gg'(g'^{-1}hg')h' \in UN.$$

   c) $a \in UN \Rightarrow a^{-1} \in UN$:

   Sei $a \in UN$. Wähle $g \in U,\ h \in N$ mit $a = gh$. Dann gilt:

   $$gh^{-1}g^{-1} \in N \Rightarrow a^{-1} = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}(gh^{-1}g^{-1}) \in UN.$$

2. Zu zeigen: $g \in U,\ h \in U \cap N \Rightarrow g^{-1}hg \in U \cap N$.

   Es gelten $g^{-1}hg \in N$, da $N \lhd G$, und $g^{-1}hg \in U$, da $U < G$, also $g^{-1}hg \in U \cap N$.

3. Trivial.

4. Betrachte die kanonische Einbettung ι und den kanonischen Epimorphismus π, gegeben durch

   $$\iota : U \to UN,\ \iota(g) := g \cdot 1 \qquad \text{und} \qquad \pi : UN \to (UN)/N,\ \pi(g) := [g]_N.$$

   Definiere $\varphi := \pi \circ \iota : U \to (UN)/N, \varphi(g) := [g]_N$, dann ist φ ein Homomorphismus als Verkettung von Homomorphismen.

   a) $U \cap N = \mathrm{Kern}(\varphi)$:

   Trivial.

   b) φ ist surjektiv:

   Sei $a \in (UN)/N$. Wähle $g \in U,\ h \in N$ mit $a = [gh]_N$. Dann

   $$\varphi(g) = [g]_N = [g]_N[h]_N = [gh]_N = a,$$

   d.h. zu jedem $a \in (UN)/N$ findet man ein $g \in U$ mit $\varphi(g) = a$.

Mit dem Homomorphiesatz folgt: $U/(U \cap N) \cong (UN)/N$. □

1.4. Satz (Zweiter Isomorphiesatz)
Seien G Gruppe, $U \lhd G,\ N \lhd G,\ U < N$. Dann gelten:
1. $N/U \lhd G/U$.
2. $(G/U)/(U/N) \cong G/N$.

Beweis.
1. Offensichtlich ist N/U eine Untergruppe von G/U. Noch zu zeigen:

$$\forall a \in G/U : \forall b \in N/U : a^{-1}ba \in N/U.$$

äquivalente Formulierung mit Vertretern:

$$\forall g \in G : \forall h \in N : [g]_U^{-1}[h]_U[g]_U = [g^{-1}hg]_U \in N/U.$$

Seien $g \in G$ und $h \in N$. Dann gilt $g^{-1}hg \in N$, da N Normalteiler von G. Insbesondere gilt dann

$$[g^{-1}hg]_U \in N/U.$$

2. Der Normalteiler U von G ist im Kern des kanonischen Epimorphismus

$$G \to G/N, \qquad g \mapsto gN$$

enthalten, da $U \subseteq N$.
Der Homomorphiesatz liefert also den Epimorphismus

$$\varphi : G/U \to G/N, \qquad [g]_U \mapsto [g]_N.$$

Wiederum nach Homomorphiesatz ist nur zu zeigen: $\mathrm{Kern}(\varphi) = N/U$.

$\subseteq$: Ist $g \in G$ mit $[g]_U \in \mathrm{Kern}(\varphi)$, dann $[g]_N = \varphi([g]_U) = 1$, also $g \in N$.

$\supseteq$: Sei $b \in N/U$. Wähle $h \in N$ mit $b = [h]_U$. Dann gilt:

$$\varphi(b) = \varphi([h]_U) = [h]_N = [1]_N = 1,$$

da $h \in N$. Also $b \in \mathrm{Kern}(\varphi)$.

Damit ist

$$(G/U)/(N/U) \to G/N, \qquad [[g]_U]_{N/U} \to [g]_N$$

ein Isomorphismus. □

1.5. Wiederholung
1. Seien $A \subseteq G$ und G Gruppe.

$$\langle A \rangle := \bigcap_{\substack{A \subseteq H \\ H < G}} H$$

heißt die von A in G erzeugte Gruppe.

2. Es gilt

$$\langle A \rangle = \{a_1, ..., a_m \mid m \in \mathbb{N},\ a_i \in A \text{ oder } a_i^{-1} \in A \text{ oder } a_i = e\}.$$

3. Sei $A = \{a\}$. Dann heißt

$$\langle a \rangle = a^{\mathbb{Z}} = \{a^n \mid n \in \mathbb{Z}\}$$

die von a in G erzeugte Gruppe.

4. Durch
$$\varphi : \mathbb{Z} \to a^{\mathbb{Z}} \subseteq G, \qquad n \mapsto a^n$$
ist ein Epimorphismus gegeben, denn $a^{n+m} = a^n \cdot a^m$. Zwei Fälle sind möglich:
   a) $\mathrm{Kern}(\varphi) = \{0\}$, dann ist $\mathbb{Z} \cong a^{\mathbb{Z}}$ via φ. $\langle a \rangle$ heißt dann unendliche zyklische Gruppe.
   b) $\mathrm{Kern}(\varphi) = n\mathbb{Z}$. Dann ist $\mathbb{Z}/(n\mathbb{Z}) \cong \{0, 1, ..., n-1\}$. $\langle a \rangle = \{a^0, ..., a^{n-1}\}$ heißt dann zyklische Gruppe der n. ◊

1.6. DEFINITION

Seien X eine Menge und $(G, \cdot)$ eine Gruppe.
$$f : G \times X \to X, \qquad (g, x) \mapsto gx$$
heißt Operation von G auf X, falls gelten:
$$(gh) \cdot x = g \cdot (h \cdot x) \qquad \text{und} \qquad e \cdot x = x.$$
Sei $x \in X$.
$$G \cdot x = \{g \cdot x \mid g \in G\}$$
heißt Bahn von x unter G.
$V \subseteq X$ heißt vollständiges Vertretersystem, falls für alle $x \in X$ gilt:
$$|(G \cdot x) \cap V| = 1.$$
f heißt transitiv, falls es nur eine Bahn in X gibt.
$$G_x := \{g \in G \mid g \cdot x = x\}$$
heißt Stabilitätsgruppe oder Isotropiegruppe oder Fixgruppe von $x \in X$.

1.7. BEMERKUNG

1. Sei $g \cdot x_1 = h \cdot x_2$. Dann gilt:
$$x_1 = e \cdot x_1 = g^{-1}g \cdot x_1 = g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (h \cdot x_2) = (g^{-1}h) \cdot x_2,$$
   d.h. $x_1 \in G \cdot x_2$ und damit $G \cdot x_1 = G \cdot x_2$.
2. G_x ist eine Untergruppe von G.
3. Seien X endlich und $G \times X \to X$ transitiv, so gilt für jedes $x \in X$:
$$|X| = |G : G_x|.$$ ◊

   Allgemeiner erhalten wir:

1.8. SATZ (Bahnengleichung)

Seien G eine Gruppe, X eine endlich Menge und $V \subseteq X$ ein vollständiges Vertretersystem. Dann gilt:
$$|X| = \sum_{x \in V} |G : G_x|.$$

BEWEIS.

Es ist $|X| = \sum\limits_{x \in V} |Gx|$. Wir zeigen: $|Gx| = |G : G_x|$ für festes x. Sei hierfür
$$G \to \{x_1, ..., x_m\} = Gx \subseteq X, \qquad g \mapsto gx,$$

Œ $x = x_1$. Dann lässt G sich schreiben als disjunkte Vereinigung

$$G = \{g \mid gx = x_1\} \cup \cdots \cup \{g \mid gx = x_m\}.$$

Sei $g_1 x = x_1$. Dann ist

$$hx = x_1 \Leftrightarrow hx = g_1 x \Leftrightarrow (g_1^{-1}h)x = x \Leftrightarrow g_1^{-1}h \in G_x \Leftrightarrow h \in g_1 G_x.$$

Also $G = g_1 G_x \cup \cdots \cup g_m G_x$, d.h.

$$m = |Gx| = |G : G_x|. \qquad \square$$

1.9. Definition

Seien G eine Gruppe und $H < G$.

$$\mathrm{Nor}(H) := \{g \in G \mid gHg^{-1} = H\}$$

heißt Normalisator von H in G.

1.10. Bemerkung

1. $\mathrm{Nor}(H)$ ist eine Untergruppe von G.
2. $H \lhd \mathrm{Nor}(H)$.
3. Ist $K < G$ mit $H \lhd K$, dann ist $K \subseteq \mathrm{Nor}(H)$, d.h. $\mathrm{Nor}(H)$ ist die größte Untergruppe von G, in der H Normalteiler ist:

$$k \in K \quad \Longrightarrow \quad kHk^{-1} = H \quad \Longrightarrow \quad k \in \mathrm{Nor}(H). \qquad \lozenge$$

1.2 Sylow-Gruppen

1.11. Definition

Seien G eine Gruppe und p eine Primzahl.

G heißt p-Gruppe, falls es zu jedem $g \in G$ ein $k \in \mathbb{N}$ gibt mit $g^{(p^k)} = e$.

Eine Untergruppe H von G heißt p-Untergruppe von G, falls H eine p-Gruppe ist.

H heißt p-Sylowgruppe von G, falls H eine maximale p-Untergruppe von G ist.

1.12. Bemerkung

Seien G eine endliche Gruppe und d ein Teiler von $|G|$. Wir wollen im Folgenden Aussagen darüber treffen, ob G Untergruppen der Ordnung d enthält oder ob es ein Element der Ordnung d in G gibt. $\lozenge$

1.13. Behauptung

Seien p prim und $n = p^r m$ mit $p \nmid m$. Dann ist p^{r-s+1} für kein $s \in \{1, ..., r\}$ Teiler von $\binom{n}{p^s}$.

Beweis.

Es gilt

$$\binom{n}{p^s} = \frac{n(n-1)\cdots(n-(p^s-1))}{p^s(p^s-1)\cdots 1} = p^{r-s}m\xi \qquad \text{mit} \qquad \xi := \prod_{i=1}^{p^s-1} \frac{p^r m - i}{p^s - i}.$$

Zu zeigen: $p \nmid \xi$.

$$i = p^{l_i}t_i,\ p \nmid t_i \& 0 \le l_i \le s \qquad \Longrightarrow \qquad \xi = \prod_i \frac{p^{r-l_i}m - t_i}{p^{s-l_i} - t_i} \overset{\cdot \frac{p^{l_i}}{p^{l_i}}}{=} \frac{\lambda p + a}{\mu p + a} \quad \text{mit} \quad a = \prod_i (-t_i).$$

Also folgt

$$a\xi - a = \lambda p - \mu p\xi = p(\lambda - \mu\xi) \qquad \Longrightarrow \qquad p \mid a(\xi - 1).$$

Wegen $p \nmid a$ gilt dann $p \mid (\xi - 1)$ und damit $p \nmid \xi$. □

1.14. Lemma

Seien G endliche Gruppe, p eine Primzahl und $|G| = p^k m$ mit $p \nmid m$.

Dann gibt es zu jedem $l \leq k$ eine Untergruppe H von G mit $|H| = p^l$.

Beweis.

Sei X die Menge aller Teilmengen von G der Mächtigkeit p^l. Ist $|G| = n$, dann $|X| = \left(\begin{array}{c} n \\ p^l \end{array} \right)$.

$$G \times X \to X, \qquad (g, U) \mapsto gU = \{gu \mid u \in U\}$$

definiert einen Monomorphismus, da $\sigma_g : U \to gU,\ u \mapsto gu$ injektiv ist. Mit Behauptung 1.13 gilt:

$$p^{k-l+1} \nmid \left(\begin{array}{c} n \\ p^l \end{array} \right) = |X|.$$

Sei $G_U := \{g \in G \mid gU = U\}$. Nach der Bahnengleichung 1.8 gibt es $U \in X$ mit

$$p^{k-l+1} \nmid |G : G_U| \qquad \Longrightarrow \qquad s \leq k - l.$$

Es gibt v, w, so dass $|G_U| = p^r v$ mit $p \nmid v$ und $|G : G_U| = p^s w$ mit $p \nmid w$, also

$$|G| = |G : G_U||G_U| \qquad \Longrightarrow \qquad k = r + s \leq r + k - l \qquad \Longrightarrow l \leq r,$$

also $p^l \mid |G_U|$. Fixiere ein $u \in U$ und betrachte $\sigma_u : G_U \to U,\ h \mapsto hu$. Da σ_u ein Monomorphismus ist, folgt

$$|G_U| \leq |U| = p^l \qquad \Longrightarrow \qquad |G_U| = p^l.$$ □

1.15. Korollar

Sei G eine endliche Gruppe. Dann gelten:

1. Ist p ein Teiler von $|G|$, so es gibt ein $g \in G$ mit $\mathrm{Ord}(g) = p$.
2. Ist G eine p-Gruppe, so gilt $|G| = p^k$ für ein $k \in \mathbb{N}$.
3. Ist $|G| = p^k m$ mit $p \nmid m$, dann ist jedes $H < G$ mit $|H| = p^k$ eine p-Sylowgruppe in G.

Beweis.

1. Gelte $|G| = p^k m$ mit $p \nmid m,\ k \geq 1$. Nach Lemma 1.14 gibt es ein $H < G$ mit $|H| = p$ und da p prim, ist $H = g^{\mathbb{Z}}$ für ein $g \in \mathbb{Z}$ und für dieses g gilt: $\mathrm{Ord}(g) = p$.
2. $\Rightarrow$ Sei q prim mit $q \mid |G|$ und $q \neq p$. Nach Lemma 1.14 gibt es dann ein $g \in G$ mit $g^q = 1$ und G kann somit keine p-Gruppe sein.

   $\Leftarrow$ Ist $|G| = p^k$, dann gilt für alle $g \in G$, dass $\mathrm{Ord}(g) \mid p^k$.
3. Sei $S < G$ mit $|S| = p^k,\ S \subseteq H$ und H eine p-Gruppe. Dann ist $|H| = p^l$, d.h. $k \leq l$, und $|H|$ teilt $|G|$, d.h. $l \leq k$, also $k = l$ und damit $S = H$. □

1.16. Hilfssatz

Seien G eine endliche Gruppe, p prim, H eine p-Untergruppe von G, S eine p-Sylowgruppe in G und $H \subseteq \mathrm{Nor}(S)$.

Dann gilt $H \subseteq S$.

Beweis.

Da $S \lhd \mathrm{Nor}(S)$, gilt nach dem ersten Isomorphiesatz: $(HS)/S \cong H/(H \cap S)$. Wegen $|H| = |H \cap S|H/(H \cap S)|$ ist $(HS)/S$ eine p-Gruppe unf wegen $|HS| = |S||(HS)/S$ ist HS eine p-Gruppe. Da $S \subseteq SH$, folgt mit Korollar 1.15: $S = SH$, also $H \subseteq S$. □

1.17. Hilfssatz

Seien G eine endliche Gruppe, p prim und $|G| = p^k m$ mit $p \nmid m$.

Ist S_0 eine Untergruppe von G mit $|S_0| = p^k$, so gibt es zu jeder p-Untergruppe H von G ein $b \in G$ mit $H \subseteq bS_0b^{-1}$.

Beweis.

Sei $X = \{gS_0g^{-1} \mid g \in G\}$. Durch $G \times X \to X,\ (g, S) \mapsto gSg^{-1}$ ist eine transitive Operation von G auf X gegeben. $X = GS_0$ ist die Bahn von S_0, also $|X| = |G : S_{S_0}|$, d.h. $|G| = |X||G_{S_0}|$.

Wegen $S_0 < G_{S_0} = \{g \in G \mid gS_0g^{-1} = S_0\}$ ist $p \nmid |X|$. Betrachte $H \times X \to X$, definiert durch $(h, S) \mapsto hSh^{-1}$ (muss nicht mehr transitiv sein). Nach der Bahnengleichung gilt für ein vollständiges Vertretersystem V: $|X| = \sum\{|H : H_s| \mid s \in V\}$.

Da H eine p-Gruppe ist, folgt $|H : H_S| = 1$ oder durch p teilbar. Da $p \nmid |X|$, gibt es ein $S \in X$ mit $H = H_S$, d.h. $hSh^{-1} = S$ für alle $h \in H$ und somit $H \subseteq \mathrm{Nor}(S)$. Da außerdem S_0 eine p-Sylowgruppe in G ist und $S = aS_0a^{-1}$ gilt, folgt, dass S eine p-Sylowgruppe ist, also $H \subseteq S$ nach Hilfssatz 1.16. □

1.18. Satz (Sylowsatz)

Seien G eine endliche Gruppe und p prim, so dass $|G| = p^k m$ mit $p \nmid m$. Dann gelten:

1. Eine Untergruppe S von G ist genau dann eine p-Sylowgruppe in G, wenn $|S| = p^k$ gilt.
2. Zu jeder p-Untergruppe H von G gibt es eine p-Sylowgruppe S in G mit $H \subseteq S$.
3. Mit S ist auch gSg^{-1} eine p-Sylowgruppe in G.

   Je zwei p-Sylowgruppen S_1, S_2 in G sind zueinander konjugiert in G, d.h. es gibt ein $g \in G$ mit $S_1 = gS_2g^{-1}$.
4. Ist s die Anzahl der p-Sylowgruppen in G, dann wird $|G|$ von s geteilt und $s \equiv 1 \bmod p$.

Beweis.

1. $\Rightarrow$ Seien S und S_0 zwei p-Sylowgruppen, dann liefert Hilfssatz 1.17, dass $S \subseteq gS_0g^{-1}$ für ein $g \in G$. Da S maximal, folgt $S = gS_0g^{-1}$, d.h. $|S| = |S_0| = p^k$.

   $\Leftarrow$ Dies besagt bereits Korollar 1.15.

2. vgl. Hilfssatz 1.17.

3. Schon gezeigt: Da S p-Sylowgruppe, ist auch gSg^{-1} eine p-Sylowgruppe. Seien S_0 und S_1 zwei p-Sylowgruppen, dann $S_1 \subseteq gS_0g^{-1}$ und aus der Maximalität folgt $S_1 = gS_0g^{-1}$.

4. Sei $X := \{gSg^{-1} \mid g \in G\}$. Setze $s := |X|$. $G \times X \to X,\ (g, S) \mapsto gSg^{-1}$ ist eine transitive Operation von G auf X, d.h. es gibt nur eine Bahn. Wähle einen Vertreter S_0 aus dieser Bahn. Nach der Bahnengleichung ist $|X| = |G : G_{S_0}|$ (wobei $G_{S_0} = \{g \in G \mid gS_0 = S_0\}$), also $gS_0g^{-1} = S_0$. Weiter gilt $|G : G_{S_0}| \mid |G|$.

   Betrachte $S_0 \times X \to X,\ (a, S) \mapsto aSa^{-1}$ (muss nicht transitiv sein). Sei V vollständiges Vertretersystem, dann $|X| = \sum\{|S_0 : S_0s| \mid s \in V\}$. Œ sei $S_0 \in V$, dann $|S_0 : S_0s_0| = |S_0 : S_0| = 1$. Wegen $S \neq S_0$ ist $(S_0)s \neq S_0$, sonst $S_0 \subseteq \mathrm{Nor}(S) = \{a \mid aSa^{-1} = S\}$ und mit Hilfssatz 1.17 würde folgen $S_0 = S$. Damit

$$|S_0 : (S_0)s| > 1 \quad \Longrightarrow \quad p \mid |S_0 : (S_0)s| \quad \Longrightarrow \quad s \equiv 1 \bmod p \quad \Longrightarrow \quad s = 1 + pl. \qquad \square$$

1.19. Wiederholung

1. Ist $|G| = p$ prim, dann ist $G = a^{\mathbb{Z}}$ für ein $a \in G\backslash\{e\}$ und es ist $G \cong \mathbb{Z}/(p\mathbb{Z})$.
2. Sei $\sigma : (\mathbb{Z}, +) \to (G, \cdot),\ n \mapsto a^n$, dann ist $\mathrm{Kern}(\sigma) = p\mathbb{Z}$.
3. Seien G_1 und G_2 zwei Gruppen. Definiere $G_1 \times G_2 := \{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}$. Dann ist $|G_1 \times G_2| = |G_1||G_2|$.

   $$(G_1 \times G_2) \times (G_1 \times G_2) \to (G_1 \times G_2), \qquad (a_1, a_2)(b_1, b_2) := (a_1b_1, a_2b_2)$$

   macht $G_1 \times G_2$ zu einer Gruppe. $G_1 \times G_2$ heißt direktes Produkt von G_1 mit G_2. Neutrales Element ist (e_1, e_2); zu $(a, b) \in G_1 \times G_2$ ist das Inverse gegeben durch $(a, b)^{-1} = (a^{-1}, b^{-1})$.

   Es gelten $G_1 \cong G_1 \times \{e_2\}$ und $G_2 \cong \{e_1\} \times G_2$ via $a \mapsto (a, e_2),\ b \mapsto (e_1, b)$. ◊

1.20. Behauptung

Sei $|G_1| = p \neq q = |G_2|$ mit p, q prim, dann ist $G_1 \times G_2$ zyklisch.

Beweis.

Seien $G_1 = a_1^{\mathbb{Z}}$ und $G_2 = a_2^{\mathbb{Z}}$ mit $a_1^p = e_1$ und $a_2^q = e_2$. Es gilt $\mathrm{Ord}((a_1, a_2)) = pq$, denn $\mathrm{Ord}(a_1, a_2)$ liegt in $\{1, p, q, pq\}$ und $(a_1, a_2)^p = (a_1^p, a_2^p) = (e_1, a_2^p) \neq (e_1, e_2)$ ... analog können die anderen Fälle ausgeschlossen werden, also $\mathrm{Ord}(a_1, a_2) = pq$. □

1.21. Behauptung

Seien G eine Gruppe und N_1, N_2 zwei Normalteiler von G mit $N_1 \cap N_2 = \{1\}$.

Dann gilt für alle $(a, b) \in N_1 \times N_2$: $ab = ba$.

Beweis.

Wir zeigen: Gibt es ein $(a, b) \in N_1 \times N_2$ mit $ab \neq ba$, dann ist $N_1 \cap N_2 \neq \{1\}$.

Sei $ab \neq ba$, dann $a \neq 1,\ b \neq 1$. Wegen $N_1 \lhd G,\ N_2 \lhd G$ sind $bab^{-1} \in N_1$ und $aba^{-1} \in N_2$, d.h. $aba^{-1}b^{-1} \in N_2$ und $bab^{-1}a^{-1} \in N_1$. Es folgt: $1 \neq bab^{-1}a^{-1} = (aba^{-1}b^{-1})^{-1} \in N_2 \Rightarrow N_1 \cap N_2 \neq \{1\}$. □

1.22. Satz

Es seien p, q Primzahlen mit $p < q$ und $p \nmid q - 1$. Dann ist jede Gruppe der Ordnung pq zyklisch.

Beweis.

Sei $|G| = pq$ mit s Anzahl der p-Sylowgruppen in G. Dann $s \equiv 1 \bmod p$, also $s = 1 + kp$, und $s|pq$, d.h. $s = 1$ oder $s = q$. Es gilt $s \neq q$, sonst $q - 1 = kp$, Widerspruch zur Voraussetzung. Also ist $s = 1$, d.h. es gibt nur eine p-Sylowgruppe in G. Bezeichne S' die Anzahl der q-Sylowgruppen in G, $s' = 1 + lp$ und $s'|pq$. Analoge Argumentation ergibt: $s' = 1$. Seien S_1 eine p-Sylowgruppe mit $|S_1| = p$ und S_2 eine q-Sylowgruppe mit $|S_2| = q$, insbesondere sind S_1 und S_2 zyklisch.

$\varphi : S_1 \times S_2 \to G,\ (a_1, a_2) \mapsto a_1a_2$ ist ein Gruppenhomomorphismus, denn da S_1 die einzige p-Sylowgruppe und S_2 die einzige q-Sylowgruppe ist, gelten $S_1 \lhd G$ und $S_2 \lhd G$, außerdem ist $S_1 \cap S_2 = \{1\}$. Mit Behauptung 1.21 folgt:

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2) \mapsto a_1b_1a_2b_2 = (a_1a_2)(b_1b_2).$$

Weiter ist φ injektiv, denn

$$(a_1, a_2) \in \mathrm{Kern}(\varphi) \quad \Longrightarrow \quad a_1a_2 = 1 \quad \Longrightarrow \quad a_1, a_2 \in S_1 \cap S_2 \quad \Longrightarrow \quad a_1 = 1 = a_2.$$

Mit dem Homomorphiesatz folgt $G \cong (S_1 \times S_2)/\mathrm{Kern}(\varphi)$. Aus $G \cong S_1 \times S_2$ mit $|S_1| = p \neq q = |S_2|$ folgt dann nach Behauptung 1.20: $S_1 \times S_2$ ist zyklisch. □

1.23. Bemerkung

1. $\mathbb{Z}/(n\mathbb{Z})$ ist zyklisch, da von 1 erzeugt.
2. $\mathbb{Z}/(n\mathbb{Z}) \times \mathbb{Z}/(n\mathbb{Z})$ dagegen ist nicht zyklisch, denn für jedes Element $(a,b) \in \mathbb{Z}/(n\mathbb{Z}) \times \mathbb{Z}/(n\mathbb{Z})$ gilt: $n(a,b) = (na, nb) = (0,0)$, d.h. $\mathrm{Ord}(a,b) \mid n$, d.h. es gibt kein Element der Ordnung n^2, also auch kein Element, das die ganze Gruppe erzeugt. ◊

1.24. Behauptung

Seien G endliche Gruppe, p die kleinste Primzahl mit $p \mid |G|$, $H < G$ und $X := \{gH \mid g \in G\}$ die Menge der Linksnebenklassen von H.

Ist dann $|X| = p$, so ist H ein Normalteiler von G.

Beweis.

Sei $x \in X$ beliebig. Dann ist $|Hx| = |H : H_x|$, insbesondere $|Hx| \mid |H| \mid |G|$. Wegen $|Hx| \leq |X| = p$ und p kleinster Primteiler von G, folgt $|Hx| = p$ oder $|Hx| = 1$. Wäre nun $|Hx| = p$, dann $Hx = X$, d.h. es gibt nur eine Bahn $Hx = Hx_0$, etwa $x_0 = H$. Sei $g \in G$ beliebig. Dann $gH \in X$, d.h. es gibt $h \in H$ mit $gH = hx_0$, also $g \in hH \subseteq H$. Damit $G \subseteq H$, also $G = H$ und damit $|X| = 1$, Widerspruch. Also sind die Bahnen der Gruppenwirkung von H auf X alle einelementig. Setzt man $\varphi : G \to S_X,\ g \mapsto (x \mapsto gx)$, so ist H gerade der Kern von φ, also $H \lhd G$. □

1.25. Satz

Seien G eine Gruppe und p prim mit $|G| = p^2$. Dann ist $G \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Beweis.

1. Ist G zyklisch, dann $G \cong \mathbb{Z}/p^2\mathbb{Z}$.
2. Ist G dagegen nicht zyklisch, dann $g^p = 1$ für alle $g \in G$, denn wegen $\mathrm{Ord}(g) \mid p$ folgt $\mathrm{Ord}(g) \in \{1, p, p^2\}$ und im Falle $\mathrm{Ord}(g) = p^2$ wäre $\langle g \rangle = G$, d.h. G zyklisch.

   Es gibt nach Lemma 1.14 $H < G$ mit $|H| = p$, insbesondere ist H zyklisch, also $H = \langle a \rangle = a^{\mathbb{Z}}$ für ein $a \in G$. Sei $b \in G \backslash H$, dann $\mathrm{Ord}(b) \in \{1, p, p^2\}$. Setze $H' := \langle b \rangle$. Dann gilt:

$$b \notin H \cap H' \implies H \cap H' \subsetneq H' \implies |H \cap H'| \mid p \implies |H \cap H'| = 1 \implies H \cap H' = \{1\}.$$

   Es ist $|G : H| = |G : H'| = \frac{p^2}{p} = p$, d.h. $H, H' \lhd G$. Wie oben ist $\varphi : H \times H' \to G,\ (a,b) \mapsto ab$ ein Gruppenhomomorphismus. Für $(a,b) \in \mathrm{Kern}(\varphi)$ gilt $a, b \in H \cap H' = \{1\}$, also $H \times H' \cong G$, d.h. $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, da $H \cong \mathbb{Z}/p\mathbb{Z}$ und $H' \cong \mathbb{Z}/p\mathbb{Z}$. □

1.3 Semidirekte Produkte

1.26. Satz

Seien G eine Gruppe und $H_1,\ H_2$ Untergruppen von G. Dann ist $\varphi : H_1 \times H_2 \to G,\ (a,b) \mapsto ab$ genau dann ein Isomorphismus, wenn gelten:

1. $ab = ba$ für alle $a \in H_1,\ b \in H_2$, d.h. H_1 und H_2 kommutieren,
2. $G = H_1H_2 = \{ab \mid a \in H_1,\ b \in H_2\}$ und
3. $H_1 \cap H_2 = \{e\}$.

Beweis.

⇒ 1. $abab = \varphi(a,b)\varphi(a,b) = \varphi((a,b)(a,b)) = \varphi(a^2, b^2) = a^2b^2$, d.h. $ba = ab$.

2. Klar, da φ surjektiv.

3. Sei $a \in H_1 \cap H_2$, dann $\varphi(a,e) = ae = ea = \varphi(e,a)$. Da φ injektiv, folgt $\Rightarrow a = e$.

$\Leftarrow$ 1. $\Rightarrow \varphi$ Homomorphismus, denn $(aa', bb') = (a,b)(a',b') \mapsto (a,b)(a',b') = aa'bb'$.

2. $\Rightarrow$ Surjektivität.

3. $\Rightarrow$ Injektivität, denn $ab = e \Rightarrow b = a^{-1} \Rightarrow b \in H_1 \cap H_2 \Rightarrow a = b = e$, d.h. $\mathrm{Kern}(\varphi) = \{e\}$. □

1.27. Bemerkung

Bedingung 1. kann ersetzt werden durch $H_1 \lhd G,\ H_2 \lhd G$, denn:

$\Rightarrow$ $H_1 \lhd G,\ H_2 \lhd G$ und $H_1 \cap H_2 = \{e\}$, d.h. $ab = ba$ für alle $a \in H_1,\ b \in H_2$.

$\Leftarrow$ Sei $G = H_1 \times H_2$. Dann gilt: $(a,b)(c,e)(a,b)^{-1} = (aca^{-1}, beb^{-1}) = (aca^{-1}, e) \in H_1$, d.h. $H_1 \lhd G$. Analog $H_2 \lhd G$. ◊

1.28. Bemerkung

1. Seien G eine Gruppe und $b \in G$, dann ist die Konjugation mit b, $\rho_b : G \to G,\ a \mapsto bab^{-1}$, ein Automorphismus von G, d.h. ein Isomorphismus von G in sich.

2. Seien ab jetzt $H_1 \lhd G,\ H_2 < G$ und $\varphi : H_1 \times H_2 \to G,\ (a,b) \mapsto ab$ die Einschränkung der Gruppenoperation auf $H_1 \times H_2$, dann

$$\forall (a,b),(a',b') \in H_1 \times H_2 : \varphi(a,b)\varphi(a',b') = (ab)(a'b') = a(ba'b^{-1})bb' = a\rho_b(a')bb'.$$

   Da $H_1 \lhd G$, ost $\rho_b : H_1 \to H_1$ nach 1.27 weiter ein Automorphismus von H_1.

3. $\mathrm{Aut}(H_1)$ bezeichne die Automorphismengruppe von H_1 mit neutralem Element id. Beachte: Es gilt $\rho, \rho' \in \mathrm{Aut}(H_1) \Rightarrow \rho' \circ \rho \in \mathrm{Aut}(H_1)$.

4. Definiere $\Phi : H_2 \to \mathrm{Aut}(H_1)$ via $\Phi(b) := \rho_b$, dann ist $\Phi_{b_1 b_2} = \Phi_{b_1} \circ \Phi_{b_2}$, d.h. $\Phi \in \mathrm{Hom}(H_2, \mathrm{Aut}(H_1))$.◊

1.29. Definition

Sei $\Phi \in \mathrm{Hom}(H_2, \mathrm{Aut}(H_1))$. Wir definieren eine neue Multiplikation auf $H_1 \times H_2$ durch

$$\circ_\Phi : (H_1 \times H_2) \times (H_1 \times H_2) \to (H_1 \times H_2), \qquad (a,b) \circ_\Phi (a',b') := (a\Phi_b(a'), bb').$$

$H_1 \times_\Phi H_2 := (H_1 \times H_2, \circ_\Phi)$ heißt semidirektes Produkt von H_1 und H_2

1.30. Behauptung

1. $\circ_\Phi$ definiert eine Gruppenoperation auf $H_1 \times H_2$:

   a) Assoziativität: Seien $a, a', a'' \in H_1$ und $b, b', b'' \in H_2$, dann gilt:

$$\begin{aligned}((a,b)(a',b'))(a'',b'') &= (a\Phi_b(a'), bb')(a'',b'') \\ &= (a\Phi_b(a')\Phi_{bb'}(a''), bb'b'') \\ &= (a\Phi_b(a')\Phi_b(\Phi_{b'}(a'')), bb'b'') \\ &= (a\Phi_b(a')\Phi_{bb'}(a''), bb'b'') \\ &= (a,b)((a',b')(a'',b''))\end{aligned}$$

   b) Neutrales Element: Seien $a \in H_1$ und $b \in H_2$, dann

$$\begin{aligned}(a,b)(e_1,e_2) &= (a\Phi_b(e_1)be_2) \\ &= (ae_1, be_2) \\ &= (e_1 a, e_2 b) \\ &= (e_1\Phi_{e_2}(a), e_2 b) \\ &= (e_1,e_2)(a,b)\end{aligned}$$

c) Inverse Elemente: Seien $a \in H_1$ und $b \in H_2$, dann ist $(a,b)^{-1} = (\Phi_{b^{-1}}(a^{-1}), b^{-1})$:

$$\begin{aligned}(a,b)(\Phi_{b^{-1}}(a^{-1}), b^{-1}) &= (a\Phi_b(\Phi_{b^{-1}}(a^{-1}))bb^{-1}) \\ &= (a\Phi_{bb^{-1}}(a^{-1}), e_2) \\ &= (aa^{-1}, e_2) \\ &= (e_1, e_2) \\ &= (\Phi_{b^{-1}}(e_1), e_2) \\ &= (\Phi_{b^{-1}}(a^{-1})\Phi_{b^{-1}}(a), b^{-1}b) \\ &= (\Phi_{b^{-1}}(a^{-1}), b^{-1})(a,b).\end{aligned}$$

2. Ist $\Phi : H_2 \to \mathrm{Aut}(H_1)$ gegeben durch $\Phi_b = \mathrm{id}_{H_1}$, so ist $H_1 \times_\Phi H_2 = H_1 \times H_2$ das direkte Produkt.
3. $H_1 \cong \{(a, e_2) \mid a \in H_1\}$ via $a \mapsto (a, e_2)$. Beachte dabei: $(a,e_2)(a',e_2) = (a\Phi_{e_2}(a'), e_2e_2) = (aa', e_2)$. ◊

1.31. Satz

Seien G eine Gruppe, $H_1 \lhd G$ und $H_2 < G$. Dann liefert die Abbildung

$$\varphi : H_1 \times_\rho H_2 \to G, \qquad (a,b) \mapsto ab$$

einen Isomorphismus, falls $H_1 \cap H_2 = \{e\}$ und $G = H_1H_2$.

Beweis.

1. Homomorphie: $\varphi(a,b)\varphi(a',b') = (ab)(a'b') = a(ba'b^{-1})bb' = a\rho_b(a')bb' = \varphi(a\rho_b(a'), bb')$.
2. Surjektivität ist klar. Injektivität: $(a,b) \in \mathrm{Kern}(\varphi) \Rightarrow ab = e \Rightarrow a, b \in H_1 \cap H_2 = \{e\}$. □

1.32. Bemerkung

Falls auch $H_2 \lhd G$, so kommutieren H_1 und H_2. Also gilt $\rho_b(a) = bab^{-1} = a$, d.h. $\rho_b = \mathrm{id}$. ◊

1.33. Beispiel

Seien G eine Gruppe und H_1 eine Untergruppe von G zum Index 2 (d.h. $H_1 \lhd G$). Dann ist G disjunkte Vereinugung $G = eH_1 \cup bH_1$ für ein $b \notin H_1$. Damit ist $G = H_1H_2$. Weiter seien $b^2 = e$, d.h. $b = b^{-1}$, und $H_2 := \{e, b\} = \langle b \rangle$ und $H_1 \cap H_2 = \{e\}$. Dann ist $G \cong H_1 \times_\rho H_2$ mit $\rho : H_2 \to \mathrm{Aut}(H_1)$, gegeben durch $b \mapsto \rho_b$. ◊

1.34. Definition

Ist $\rho_b(a) = bab^{-1} = a^{-1}$ für alle $a \in G$, so heißt G eine Diedergruppe.

1.35. Bemerkung

Diedergruppen sind stets abelsch:

$$xy = (y^{-1}x^{-1})^{-1} = \rho_b(y^{-1}x^{-1}) = \rho_b(y^{-1})\rho_b(x^{-1}) = yx.$$ ◊

1.36. Beispiel

Seien $\sigma, \tau \in S_n$, der Permutationsgruppe von $\{1, ..., n\}$, gegeben durch

$$\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}, \qquad \tau := \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}.$$

Dann gelten $\tau^2 = \mathrm{id}$ und $\sigma^n = \mathrm{id}$. $D_n := \langle \sigma, \tau \rangle$ ist eine Diedergruppe.

Sei nun etwa $n = 7$. Dann ist D_n die Gruppe der „Bewegungen“ des Siebenecks in der Ebene. τ Spiegelung am Durchmesser von S_7 durch eine fixierte Ecke (der Eins) und σ der Drehung um den Winkel $\frac{360}{7}^\circ$.

Es gilt $D_n = \{\mathrm{id},\ \sigma,\ ...,\ \sigma^{n-1},\ \tau,\ \sigma\tau,\ ...,\ \sigma^{n-1}\tau\}$, d.h. $|D_n| = 2n$ für beliebiges $n \geq 3$. Weiter sind $\tau\sigma^m = \sigma^{-m}\tau$ für alle m. ◊

1.37. Satz

Jede Gruppe der Ordnung $2p$ mit $p \neq 2$ prim ist zyklisch oder die Diedergruppe D_p.

Beweis.

Seien H_1 und H_2 Untergruppen von G mit $|H_1| = p$, also $H_1 = \langle a\rangle \cong \mathbb{Z}/p\mathbb{Z}$, und $|H_2| = 2$, also $H_2 = \langle b\rangle$, $b^2 = e$, d.h. $b = b^{-1}$. Wegen $[G : H_1] = 2$ sind (vgl. Beispiel 1.33) $H_1 \lhd G$ und $G = H_1 \cup H_1 b$ disjunkt, also $G \cong H_1 \times_\rho H_2$ mit

$$H_1 \times_\rho H_2 \to G, \qquad (a, b) \mapsto ab \qquad \text{und} \qquad \rho : H_2 \to \mathrm{Aut}(H_1), \qquad b \mapsto \rho_b,$$

insbesondere $e \mapsto \rho_e = \mathrm{id} = \rho_{b^2} = \rho_b \circ \rho_b = (\rho_b)^2$. Da ρ_b Automorphismus, gilt$\rho_b(a) = a^m$ für ein $m \in \{1, ..., p-1\}$. Dann sind $\rho_b(a^n) = (a^m)^n = a^{mn}$ und $\rho_b \circ \rho_b(a^n) = a^{m^2 n} = a^n = \mathrm{id}(a^n)$, d.h. $m^2 n \equiv n \bmod p$, also $p \mid n(m^2 - 1)$. Speziell für $n = 1$ folgt $p \mid m^2 - 1 = (m+1)(m-1)$; da p prim, also $p \mid (m+1)$ oder $p \mid (m-1)$, d.h. $m = \pm 1 \bmod p$, also $a^m = a$ oder $a^m = a^{-1}$.

Im Fall $\rho_b(a) = a$ ist $\rho = \mathrm{id}$, also $G \cong H_1 \times_\rho H_2 = H_1 \times H_2$ und damit G zyklisch. Falls dagegen $\rho_b(a) = a^{-1}$, ist G die Diedergruppe D_p. □

1.4 Die Symmetrische Gruppe

1.38. Notation

Sei $\sigma \in S_n$ eine Permutationen von $\{1, ..., n\}$, dann schreiben wir

$$\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Speziell setzen wir $\sigma := \begin{pmatrix} x_1 & \cdots & x_m \end{pmatrix}$ für den m-Zykel

$$\sigma(x_i) = x_{i+1} \text{ für alle } 1 \leq i \leq m-1, \qquad \sigma(x_m) = x_1, \qquad \sigma(x) = x \text{ und } x \notin \{x_1, ..., x_m\}.$$

Ein $\tau = \begin{pmatrix} x_1 & x_2 \end{pmatrix}$ heißt Transposition ein $\sigma = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}$ heißt 3er-Zykel. ◊

1.39. Bemerkung

1. Jedes $\sigma \in S_n$ ist ein Produkt von Transpositionen.
2. Je zwei Transpositionen sind konjugiert zueinander, d.h. $\forall \tau_1, \tau_2 \in S_n : \exists \sigma \in S_n : \tau_1 = \sigma\tau_2\sigma^{-1}$. ◊

1.40. Definition

(i, j) heißt Fehlstand von $\sigma \in S_n$, falls $i < j$ und $\sigma(i) > \sigma(j)$.

Ist n die Anzahl der Fehlstände von σ, so ist das Signum von σ definiert als $\mathrm{sgn}(\sigma) := (-1)^n$.

1.41. Bemerkung

1. $\mathrm{sgn} : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus und $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$: $\mathrm{sgn}(\sigma \circ \sigma') = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma')$.
2. $A_n := \mathrm{Kern}(\mathrm{sgn}) = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$ heißt alternierende Gruppe auf $\{1, ..., n\}$.
3. Nach dem Homomorphiesatz gilt $S_n/A_n \cong \{\pm 1\}$, d.h. $[S_n : A_n] = 2$, also $A_n \lhd S_n$ und $S_n = A_n \cup A_n\sigma$ disjunkt mit beliebigem $\mathrm{sgn}(\sigma) = -1$.
4. Jeder 3er-Zykel liegt in A_n, denn $\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix}$.
5. Die Determinante einer Matrix $A \in \mathbb{R}^{n\times n}$ lässt sich berechnen als

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)}.$$ ◊

1.42. Lemma

Für $n \geq 3$ ist A_n die Menge aller Produkte von 3er-Zyklen.

Beweis.

Klar: Mit den 3er-Zyklen liegen auch alle Produkte von 3er-Zyklen liegen in A_n. Dann liegen auch alle Produkte von Transpositionen in A_n: Seien x_1, x_2, x_3, x_4 paarweise verschieden, dann gelten:

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \circ \begin{pmatrix} x_3 & x_4 \end{pmatrix} = \begin{pmatrix} x_3 & x_2 & x_1 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_3 & x_4 \end{pmatrix} \in A_n.$$
$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \circ \begin{pmatrix} x_2 & x_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \in A_n.$$
$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix} = \mathrm{id} \in A_n.$$

Also liegt auch jedes beliebige $\sigma = \tau_1 \circ \cdots \circ \tau_{2m}$ in A_n. □

1.5 Auflösbare Gruppen

1.43. Definition

Seien G eine Gruppe und $a, b \in G$. $[a, b] := aba^{-1}b^{-1}$ heißt Kommutator von a und b.

Die von $\{[a, b] \mid a, b \in G\}$ erzeugte Untergruppe in G heißt die Kommutatorgruppe $K(G)$ von G.

1.44. Bemerkung

1. Ist G abelsch, dann ist $K(G) = \{e\}$.
2. Es gilt $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ für alle $a, b \in G$.
3. $K(G) = \{[a_1, b_1] \cdots [a_m, b_m] \mid m \in \mathbb{N},\ a_i, b_i \in G\}$. ◊

1.45. Lemma

1. $K(G)$ ist ein Normalteiler von G.
2. Sei N ein Normalteiler von G. Dann gilt: G/N ist abelsch $\Leftrightarrow$ $K(G)$ ist eine Untergruppe von N.

Speziell ist $G/K(G)$ stets abelsch und es gilt $[a, b] = e \Rightarrow ab = ba$.

Beweis.

1. Seien $x, a, b \in G$ beliebig. Dann liegt $x[a_n, b_n]x^{-1}$ in $K(G)$:

$$\begin{aligned} x[a, b]x^{-1} &= x(aba^{-1}b^{-1})x^{-1} \\ &= (xax^{-1})(xb^{x}-1)(xa^{-1}x^{-1})(xb^{-1}x^{-1}) \\ &= [xax^{-1}, xbx^{-1}]. \end{aligned}$$

   Allgemeiner ist

$$x[a_1, b_1][a_2, b_2] \cdots [a_n, b_n]x^{-1} = x[a_1, b_1]x^{-1}x[a_2, b_2]x^{-1} \cdots x[a_n, b_n]x^{-1}$$

   ein Kommutator.

2. Betrachte $\rho : G \to G/N,\ g \mapsto gN$, insbesondere $N = \mathrm{Kern}(\rho)$. Dann gilt:

$$G/N \text{ abelsch} \iff \rho([a, b]) = \rho(a)\rho(b)\rho(a^{-1})\rho(b^{-1}) = N \iff K(G) \subseteq \mathrm{Kern}(\rho) = N.$$ □

1.46. Behauptung

1. $K(S_n) = A_n$ für $n \geq 2$.
2. $K(A_n) = A_n$ für $n \geq 5$.
3. $K(A_n) = \{\mathrm{id}\}$ für $n \in \{1, 2, 3\}$.
4. $K(A_4) = K_4 := \{\mathrm{id}, (1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}$, die Kleinsche Vierergruppe.

Beweis.

Beachte: S_n/A_n ist abelsch, da $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, also $K(S_n) < A_n$.

1. Ist $n = 2$, dann $A_n = \{\mathrm{id}\}$, also ist A_n abelsch, d.h. $A_n = K(S_n)$. Ist dagegen $n \geq 3$, dann ist jedes Element aus A_n Produkt aus 3er-Zyklen und für paarweise verschiedene i, j, k ist
$$(i\ j\ k) = (i\ k)(j\ k)(i\ k)^{-1}(j\ k)^{-1}$$
ein Kommutator. Also gilt: $A_n = K(S_n)$.
2. Zu zeigen: Jeder 3er-Zyklus ist Kommutator von 3er-Zyklen. Seien $\alpha := (i\ j\ k)$ und l, m so gewählt, dass $|\{i, j, k, l, m\}| = 5$. Setze $\pi := (i\ j\ l)$ und $\sigma := (i\ k\ m)$, dann $\pi \circ \sigma \circ \pi^{-1} \circ \sigma^{-1} = \alpha$
3. Für $n \in \{1, 2, 3\}$ ist A_n abelsch, d.h. $K(A_n) = \{\mathrm{id}\}$.
4. a) $K(A_4) \subseteq K_4$: Es gilt $K(A_4) \lhd A_4$ und $A_4/K(A_4)$ ist abelsch. Weiter ist K_4 die einzige 2-Sylowuntergruppe von A_4 der Ordnung 4, denn in A_4 liegen alle 8 3-Zykel von S_4; diese haben die Ordnung 3, können also in keiner Gruppe der Ordnung 4 liegen. Damit ist $K_4 \lhd A_4$ und $|A_4/K(A_4)| = \frac{|A_4|}{|K_4|} = \frac{12}{4} = 3$ ist prim. Also ist $A_4/K(A_4)$ zyklisch und damit abelsch, d.h. $K(A_4) < K_4$.

   b) $K(A_4) \supseteq K_4$: Jedes von id verschiedene Element der K_4 lässt sich in das Produkt von vier 3-Zyklen der Gestalt $\sigma_1 \circ \sigma_2 \circ \sigma_1^{-1} \circ \sigma_2^{-1}$ zerlegen:
$$\begin{aligned}(1\ 2)(3\ 4) &= (1\ 2\ 3)(1\ 2\ 4)(3\ 2\ 1)(4\ 2\ 1);\\ (1\ 3)(2\ 4) &= (1\ 3\ 2)(1\ 3\ 4)(2\ 3\ 1)(4\ 3\ 1);\\ (1\ 4)(2\ 3) &= (1\ 4\ 2)(1\ 4\ 3)(2\ 4\ 1)(3\ 4\ 1).\end{aligned}$$
   Also liegt jedes Element aus K_4 im Kommutator von A_4. □

1.47. Bemerkung

Setzt man $K^0(G) := G$ und $K^{n+1}(G) := K(K^n(G))$, so erhält man mit
$$G = K^0(G) \supseteq K^1(G) \supseteq K^2(G) \supseteq \cdots \supseteq K^n(G) \supseteq K^{n+1}(G) \supseteq \cdots$$
eine Kette von Untergruppen von G derart, dass für alle $n \in \mathbb{N}$ gelten:
$$K^{n+1}(G) \lhd K^n(G) \qquad \text{und} \qquad K^n(G)/K^{n+1}(G) \text{ ist abelsch.}$$ ◊

1.48. Definition

Sei G eine Gruppe. Dann heißt $G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$ eine Normalreihe. Die Quotientengruppen G_i/G_{i+1} heißen Faktoren dieser Normalreihe.

G heißt auflösbar, falls es ein $n \in \mathbb{N}$ gibt mit $K^n(G) = \{e\}$.

1.49. Satz (Auflösbarkeit von Gruppen)

Sei G eine Gruppe. Dann gilt: G ist auflösbar $\Leftrightarrow$ G besitzt eine Normalreihe mit abelschen Faktoren.

Beweis.

$\Rightarrow$ $G = K^0(G) \rhd K^1(G) \rhd K^2(G) \rhd \cdots \rhd K^n(G) = \{e\}$ ist eine Normalreihe von G aus abelschen Faktoren.

$\Leftarrow$ Wir zeigen per endlicher Induktion über i, dass $K^i(G) \subseteq G_i$, dann ist insbesondere $K^n(G) = \{e\}$. Im Fall $i = 0$ ist offenbar $K^0(G) = G = G_0$. Gelte die Behauptung also für ein i, dann ist G_i/G_{i+1} abelsch, d.h. $K(G_i) \subseteq G_{i+1}$. Mit der Induktionsvoraussetzung folgt: $K^i(G) \subseteq G_i$ und wir erhalten $K^{i+1}(G) \subseteq K(G_i) \subseteq G_{i+1}$, d.h. die Behauptung gilt auch für $i + 1$. □

1.50. Beispiele

1. Ist G abelsch, dann ist G auflösbar, da $K(G) = \{e\}$.

2. A_n und S_n sind für $n \geq 5$ nicht auflösbar, denn es gelten $K(S_n) = A_n$ und $K(A_n) = A_n$, also $K^{i+1}(S_n) = K^i(A_n) = A_n \neq \{e\}$.

3. S_3 ist auflösbar: $K(S_3) = A_3$ und $K(A_3) = \{e\}$, da $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ zyklisch, also abelsch.

4. S_4 ist auflösbar, denn $K(S_4) = A_4$ ujd $K(A_4) = K_4$ abelsch, d.h. $K^3(S_4) = \{e\}$. ◊

1.51. Satz

Zu jeder endlichen auflösbaren Gruppe gibt es eine Normalreihe, deren Faktoren zyklisch von Primzahlordnung sind.

Beweis.

Seien $G = G_0 \rhd \cdots \rhd G_n = \{e\}$ eine Normalreihe mit abelschen Faktoren und $\rho : G_i \to G_i/G_{i+1}$ der kanonische Homomorphismus. Wähle $U < G_i/G_{i+1}$ mit $|U| = p$ prim und setze $N_1 := \rho^{-1}(U) < U$. Dann ist $U \lhd G_i/G_{i+1}$, da G_i/G_{i+1} abelsch. Damit $N_1 \lhd G$ und wegen $U \cong N_1/G_{i+1}$ gilt

$$G_i/N_1 \cong (G_i/G_{i+1})/(N_1/G_{i+1}) \cong (G_i/G_{i+1})/U.$$

$(G_i/G_{i+1})/U$ ist abelsch und $|G_i/N_1| = |G_i/G_{i+1}|\frac{1}{p} < |G_i/G_{i+1}|$ und $N_1/G_{i+1} = U$ hat Ordnung p. Per Induktion finden wir $G_i \rhd N_m \rhd \cdots \rhd N_1 \rhd G_{i+1}$, wobei alle Quotienten Primzahlordnung haben. □

1.52. Lemma

Seien G, G' Gruppen, $\varphi : G \to G'$ ein Homomorphismus und H eine Untergruppe von G. Dann gelten:

1. $\varphi(K(H)) = K(\varphi(H))$.
2. $\varphi(K^n(G)) \subseteq K^n(G')$ für alle $n \in \mathbb{N}$. Ist φ surjektiv, dann gilt sogar Gleichheit.

Beweis.

1. Folgt aus
$$\varphi([a,b]) = \varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a^{-1})\varphi(b^{-1}) = [\varphi(a), \varphi(b)].$$

2. Per Induktion über n: Im Fall $n = 0$ ist
$$\varphi(K^0(G)) = \varphi(G) \subseteq G' = K^0(G')$$
und Gleichheit gilt, falls φ surjektiv ist. Gelte die Behauptung also für ein n, dann ist
$$\varphi(K^{n+1}(G)) = K(\varphi(K^n(G))) \subseteq K(K^n(G')) = K^{n+1}(G'),$$
wobei wiederum für surjektives φ Gleichheit erfüllt ist. Also gilt die Behauptung auch für $n+1$. □

1.53. Satz

1. Jede Untergruppe H einer auflösbaren Gruppe G ist auflösbar.
2. Sei $N \lhd G$. Dann gilt: G ist auflösbar $\Leftrightarrow$ G/N und N sind auflösbar.

Beweis.

1. Ab gewissem n gilt $K^n(H) \subseteq K^n(G) = \{e\}$, d.h. $K^n(H) = \{e\}$.

2. $\Rightarrow$ Da G auflösbar ist, folgt mit 1., dass N auflösbar ist. Betrachte den kanonischen Homomorphismus $\varphi : G \to G/N$. Wegen $K^n(G) = \{e\}$ gilt $K^n(G/N) = \varphi(K^n(G)) = \varphi(\{e\}) = \{e\}$.

   $\Leftarrow$ Seien $K^n(N) = \{e\}$ und $K^m(G/N) = \{N\}$. Dann ist $\varphi(K^m(G)) = K^m(G/N) = \{N\}$, also $K^m(G) \subseteq N$. Aus $K^n(N) = \{e\}$ folgt $K^{n+m}(G) = K^n(K^m(G)) = \{e\}$. □

1.54. Definition

Seien G eine Gruppe und X eine Teilmenge von G.

$\mathrm{Cen}(X) := \{g \in G \mid gx = xg \text{ für alle } x \in X\}$ heißt der Zentralisator von X in G.

$\mathrm{Z}(G) := \mathrm{Cen}(G)$ heißt das Zentrum von G.

1.55. Bemerkung

1. Es gilt $\mathrm{Cen}(X) < G$, denn falls $ax = xa$ und $bx = xb$, dann auch $xab = axb = abx$ und $xa^{-1} = a^{-1}x$.
2. $\mathrm{Z}(G) < \mathrm{Cen}(X)$.
3. Für $x \in X$ gilt: $\mathrm{Cen}(x) := \mathrm{Cen}(\{x\}) = G$ genau dann, wenn $x \in \mathrm{Z}(G)$.
4. $\mathrm{Z}(G)$ ist abelsch und $\mathrm{Z}(G) \lhd G$.

   Für den Monomorphismus $\rho : G/\mathrm{Aut}(G),\ g \mapsto \rho_g := g(\cdot)g^{-1}$ gilt

   $$\mathrm{Kern}(\rho) = \{g \in G \mid gxg^{-1} = x \text{ für alle } x \in G\} = \mathrm{Z}(G) \lhd G.$$

   $\mathrm{Bild}(\rho) \cong G/\mathrm{Z}(G)$ ist die Gruppe der inneren Automorphismen von G.
5. Ist $G/\mathrm{Z}(G)$ zyklisch, dann ist G abelsch: Sei $x \in \mathrm{Z}(G)$ ein erzeugendes Element von $G/\mathrm{Z}(G)$, d.h. $G/\mathrm{Z}(G) = \langle x\mathrm{Z}(G)\rangle$. Dann gilt für alle $a, b \in G$, dass $a = x^n z_1$ und $b = x^m z_2$ für gewisse $n, m \in \mathbb{Z}$ und $z_1, z_2 \in \mathrm{Z}(G)$, also

   $$ab = x^n z_1 x^m z_2 = x^{n+m} z_1 z_2 = x^{m+n} z_2 z_1 = x^m z_2 x^n z_1 = ba. \qquad \lozenge$$

1.56. Satz (Klassengleichung)

Seien G eine endliche Gruppe und V eine Teilmenge von G, so dass jedes Element von $G \backslash \mathrm{Z}(G)$ zu genau einem Element aus V konjugiert ist. Dann gilt:

$$|G| = |\mathrm{Z}(G)| + \sum_{x \in V} |G : \mathrm{Cen}(x)|.$$

Beweis.

$G \times G \to G,\ (g, x) \mapsto gxg^{-1}$ operiert auf G mit Fixgruppe $G_x = \{g \in G \mid gxg^{-1} = x\} = \mathrm{Cen}(x)$. Für $x \in \mathrm{Z}(G)$ gilt $\mathrm{Cen}(x) = G$, also ist $V' := V \cup \mathrm{Z}(G)$ ein vollständiges Vertretersystem und mit der Bahnengleichung folgt:

$$|G| = \sum_{x \in V'} |G : G_x| = \sum_{x \in \mathrm{Z}(G)} |G : G| + \sum_{x \in V} |G : \mathrm{Cen}(x)|. \qquad \square$$

1.57. Behauptung

Seien G eine Gruppe und p prim mit $|G| = p^k$. Dann gilt $p \mid |\mathrm{Z}(G)|$ und insbesondere $|\mathrm{Z}(G)| > 1$.

Beweis.

Sei $x \notin \mathrm{Z}(G)$. Dann ist $|G : \mathrm{Cen}(x)| > 1$, sonst wäre $G = \mathrm{Cen}(x)$, d.h. G abelsch und damit $G \backslash \mathrm{Z}(G) = \emptyset$. Damit $p \mid |G : \mathrm{Cen}(x)|$ und die Klassengleichung liefert $p \mid |\mathrm{Z}(G)|$. $\square$

1.58. Satz (Auflösbarkeit von p-Gruppen)

Sei p prim. Dann ist jede endliche p-Gruppe auflösbar.

Beweis.

Sei G eine Gruppe mit $|G| = p^k$. Wir führen eine Induktion über k: Im Falle $k = 0$ ist $G = \{e\}$ auflösbar.

Gelte die Behauptung also für alle $l < k$ und sei $|G| = p^l$ mit $l < k$, dann ist G auflösbar und $\mathrm{Z}(G)$ ist abelsch, d.h. $\mathrm{Z}(G)$ ist auflösbar ($\mathrm{Z}(G) \lhd G$). Weiter ist $|\mathrm{Z}(G)| > 1$, d.h. $|G/\mathrm{Z}(G)| = p^l$, und wegen $l < k$ ist $G/\mathrm{Z}(G)$ auflösbar. Also ist auch G auflösbar. □

1.59. Satz (Feit-Thomson)

Jede endliche Gruppe ungerader Ordnung ist auflösbar (ohne Beweis).

2 Ringe

2.1 Grundbegriffe

2.1. Wiederholung

1. $(A,+,\cdot)$ ist ein Ring, falls

   a) $(A,+)$ eine abelsche Gruppe ist,
   b) $(A,\cdot)$ assoziativ ist und
   c) $(A,+,\cdot)$ distributiv ist, d.h. $\forall a,b,c\in A: (a+b)c = ac+bc \;\&\; a(b+c) = ab+ac$.

2. $(A,+,\cdot)$ ist kommutativ, falls $\forall a,b\in A: ab = ba$.

3. $1\in A$ heißt Einselement, falls $\forall a\in A: 1a = a1 = a$.

4. $(A,+,\cdot)$ ist ein Schiefkörper, falls $(A\backslash\{0\},\cdot)$ eine Gruppe ist.

5. Sei A ein Ring mit Eins. $A^\times := \{a\in A \mid \exists b\in A: ab = ba = 1\}$ ist die Einheitengruppe von A. Beispiele sind $\mathbb{Z}^\times = \{\pm 1\}$ und $K^\times = K\backslash\{0\}$.

6. $a\in A$ heißt Nullteiler, falls $a\neq 0$ und es ein $b\neq 0$ gibt mit $ab = 0$ oder $ba = 0$.

   $(A,+,\cdot)$ heißt Integritätsbereich, falls A kommutativ mit Eins und nullteilerfrei ist. Beispiele sind $\mathbb{Z}$ und $K[X]$.

7. $f: A\to B$ heißt Ringhomomorphismus, falls $f(1) = 1$, $f(a+b) = f(a)+f(b)$ und $f(ab) = f(a)f(b)$ für alle $a,b\in A$ gelten. $\mathrm{Kern}(f) := f^{-1}\{0\}$ ist genau dann trivial (d.h. $\mathrm{Kern}(f) = \{0\}$), wenn f injektiv ist. Es gilt der Homomorphiesatz: $f(A)\cong A/\mathrm{Kern}(f)$.

8. $I\subseteq A$ heißt Ideal, wenn $I+I\subseteq I$ und $AI, IA\subseteq I$ gelten. Beispiele sind $\mathrm{Kern}(f)$ und $\{0\}$.

   $A/I := \{a+I \mid a\in A\}$ heißt Quotientenring oder Restklassenring mit additiv Neutralem $I = 0+I$, wobei $a+I := \{a+b \mid b\in I\}$. Die Operationen auf A/I sind gegeben durch $(a+I)+(b+I) := (a+b)+I$ und $(a+I)(b+I) := (ab)+I$. Es gilt: $a+I = b+I \Leftrightarrow a-b\in I$.

2.2. Beispiel

In $A = \mathbb{Z}$ ist jedes $I = n\mathbb{Z}$ ein Ideal. Es gilt:

$$a+I = b+I \iff a-b\in I \iff n\mid(a-b) \iff a\equiv b \bmod n.$$

A/I lässt sich schreiben als $\mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}\cup(1+n\mathbb{Z})\cup\cdots\cup((n-1)+n\mathbb{Z}) = \{0,1,...,n-1\}$.

Für $n\geq 1$ gilt: $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper $\Leftrightarrow$ n ist eine Primzahl. ◊

2.3. Satz (Chinesischer Restsatz)

Seien R ein kommutativer Ring mit 1 und $I_1,...,I_n$ Ideale in R mit $I_i+I_j = R$ für $i\neq j$.

Dann gibt es zu $x_1,...,x_n\in R$ ein $x\in R$ mit $x\equiv x_i \bmod I_i$ für alle $i\leq n$.

Beweis.

Per Induktion über n.

1. $n = 2$: Seien $a_1\in I_1$ und $a_2\in I_2$ mit $a_1+a_2 = 1$. Setze $x := x_1a_2 + x_2a_1$, dann gelten

$$x\equiv x_1a_2 = (1-a_1)x_1 = x_1 - a_1x_1\equiv x_1 \bmod I_1,$$
$$x\equiv x_2a_1 = (1-a_2)x_2 = x_2 - a_2x_2\equiv x_2 \bmod I_2.$$

2. $n > 2$: Für $i\geq 2$ gibt es $a_i\in I_1$ und $b_i\in I_i$ mit $a_i+b_i = 1$. Dann ist

$$1 = \prod_{i\geq 2}(a_i+b_i) = \prod_{i\geq 2}a_i + \cdots + \prod_{i\geq 2}b_i,$$

wobei alle Faktoren bis auf den letzten in I_1 liegen und der letzte in $\bigcap_{i\geq 2} I_i =: I$, d.h. $I_1 + I = R$.

Nach Induktionsvoraussetzung gibt es $y_1 \in R$ mit $y_1 \equiv 1 \bmod I_1$ und $y_1 \equiv 0 \bmod I$. Analog gibt es $y_j \in R$ mit $y_j \equiv 1 \bmod I_j$ und $y_j \equiv 0 \bmod \bigcap_{j\neq i} I_i$.

Setze $x := x_1y_1 + \cdots + x_ny_n$, dann $x \equiv x_jy_j$ (da $x_i \in I_j$ für alle $i \neq j$) und $x_jy_j \equiv x_j1 = 1 \bmod I_j$.□

2.4. Bemerkung

Seien R kommutativer Ring mit Eins, und I, J Ideale in R. Dann sind auch

$$I \cap J, \qquad I + J := \{i + j \mid i \in I,\ j \in J\}, \qquad I \cdot J := \left\{ \sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N},\ i_k \in I,\ j_k \in J \right\}$$

Ideale in R. Seien $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ Ideale in R. Dann ist auch $\bigcup_{i=1}^{\infty} I_i$ ein R-Ideal. ◊

2.5. Definition

Zu $M \subseteq R$ heißt

$$(M) := \bigcup_{\substack{M\subseteq I \\ I \text{Ideal}}} I = \left\{ \sum_{k=1}^{n} i_k m_k \mid n \in \mathbb{N},\ i_k \in R,\ m_k \in M \right\}$$

das von M erzeugte Ideal in R.

Für endliches $M = \{b_1, ..., b_n\}$ schreiben wir auch $(b_1, ..., b_n) := (\{b_1, ..., b_n\}) = Rb_1 + \cdots + Rb_n$. R heißt Noethersch, falls jedes Ideal I von R endlich erzeugt ist.

2.6. Wiederholung

1. Seien R ein kommutativer Ring und $a \in R$, dann heißt $Ra := \{ba \mid b \in R\}$ ein Hauptideal von R.
2. R heißt ein Hauptidealring, falls jedes R-Ideal ein Hauptideal ist.
3. $w : R\backslash\{0\} \to \mathbb{N}$ heißt euklidische Wertefunktion, falls für alle $a, b \in R\backslash\{0\}$ gelten:

   a) Falls $a \mid b$, dann $w(a) \leq w(b)$ und
   b) Es gibt $q, r \in R$ mit $r = 0$ oder $w(r) < w(b)$, so dass $a = bq + r$.

   R heißt euklidisch, falls auf R eine euklidische Wertefunktion existiert. Beispiele sind $\mathbb{Z}$ mit $w(m) := |m|$ und $K[X]$ mit $w(p) := \deg(p)$.
4. Jeder euklidische Integritätsbereich ist ein Hauptidealring. Insbesondere ist $K[X]$ ein Integritätsbereich, falls K ein Körper ist.
5. Ingeritätsbereiche, die Hauptidealringe sind, besitzen keine unendlichen Teilerketten. ◊

2.7. Satz

Für kommutative Ringe mit Eins sind äquivalent:

1. R ist Noethersch.
2. Jede aufsteigende Kette von Idealen bricht ab.
3. Jede nichtleere Menge von Idealen besitzt ein maximales Element.

Beweis.

1. (1) ⇒ (2): Sei $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots \subseteq I := \bigcup I_n$. Dann ist $I = (a_1, ..., a_m)$, d.h. es gibt ein $n \in \mathbb{N}$ mit $a_1, ..., a_m \in I_n$, also $I \subseteq I_n$, also $I = I_n$, d.h. es gilt $I = I_j$ für alle $j \geq n$.
2. (2) ⇒ (3): Sei $M \neq \emptyset$ eine Menge von Idealen. Dann ist $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n$ mit I_n maximal.
3. (3) ⇒ (1): Seien I ein Ideal und M die Menge aller endlich erzeugten Teilideale von I. Dann ist $M \neq \emptyset$, da zu $a \in I$ auch $(a) \subseteq I$, also $(a) \in M$. Sei $(a_1, ..., a_n) \subseteq I$ maximal, dann $I = (a_1, ..., a_n)$, denn sonst gäbe es ein $a \in I\backslash\{a_1, ..., a_n\}$ und damit $(a_1, ..., a_n) \subsetneq (a_1, ..., a_n, a)$. Also ist I endlich erzeugt. □

2.8. Korollar

Seien R, R' Ringe, R Noethersch und $\varphi : R \to R'$ ein Epimorphismus, dann ist auch R' Noethersch.

Beweis.

Sei $I'_1 \subseteq I'_2 \subseteq \cdots$ eine Idealkette in R'. Setze $I_i := \varphi^{-1}(I'_i)$. Dies definiert eine Idealkette in R. Dann gibt es $n \in \mathbb{N}$ mit $I_n = I_m$ für alle $m \geq n$, also auch $I'_n = I'_m$ für $m \geq n$. Also bricht die Kette I'_i ab. □

2.2 Polynomringe

2.9. Wiederholung

1. Sei R ein kommutativer Ring mit Eins. Dann heißt

$$R[X] := \{f = a_0 + a_1X + \cdots + a_nX^n \mid a_1, ..., a_n \in R,\ n \in \mathbb{N}\}$$

   der Ring der Polynome in der Unbestimmten X mit Koeffizienten aus R.

2. Es gilt: $a_0 + a_1X + \cdots + a_nX^n = 0 \Leftrightarrow a_0 = 0, ..., a_n = 0$.

3. Ist $a_n \neq 0$, dann heißt $\deg(f) := n$ der Grad von f. Setze $\deg(0) := -\infty$.

   Es gilt $\deg(fg) \leq \deg f + \deg g$; Gleichheit gilt in Integritätsbereichen. ◊

2.10. Satz (Division mit Rest)

Seien R kommut. Ring mit Eins, $f, g \in R[X]\backslash\{0\}$ und $n = \deg g,\ m \geq \deg f,\ k = \max\{0, m-n+1\}$.

Ist $g = bX^n + \cdots$, so gibt es $q, r \in R[X]$ mit $b^k f = qg + r$ und $\deg r < \deg g$.

Ist b kein Nullteiler, so sind q und r eindeutig bestimmt.

Beweis.

1. Eindeutigkeit: Sei $qg+r = q'g+r'$, dann $(q-q')g = r'-r$. Wäre $q \neq q'$, dann $\deg(q-q')g \geq \deg g = n$, da b kein Nullteiler ist, und $\deg g > r - r'$, was nicht möglich ist, da $\deg(r-r') = \deg(q-q')g$. Analog würde aus $r \neq r'$ folgen $\deg(r-r') < \deg g \leq \deg(q-q')g$, ein Widerspruch. Also gelten $q = q'$ und $r = r'$.

2. Existenz: Per Induktion über m.

   a) Sei $m = 0$. Falls auch $n = 0$, dann gelten $b^1 f = fg + 0$ und $\deg r = -\infty < \deg f = 0$. Ist dagegen $n > 0$, so gelten $b^0 f = 0g + f$ und $\deg f = 0 < n = \deg g$.

   b) Sei nun $m > 0$ und die Behauptung gelte für alle $l < m$. Falls $n > m$, so gelten $b^0 f = 0g + f$ und $\deg f \leq m < n = \deg g$. Für $m \geq n$ sei $f = aX^m + \cdots$. Es gilt $\deg(bf - aX^{m-n}g) \leq m-1$. Mit der Induktionsvoraussetzung folgt: Es gibt $q', r' \in R[X]$ mit $q'g + r' = b^l(bf - aX^{m-n}g)$ mit $l = \max\{0, m-1-n+1\}$ und $\deg r' < n$. Dann $b^{l+1}f = (b^l aX^{m-n}q')g + r',\ \deg r' < n = \deg g$ und $l+1 = \max\{0, m-n+1\}$. □

2.11. Satz (Hilbertscher Basissatz)

Ist R ein kommutativer Noetherscher Ring mit Eins, so ist auch $R[X]$ Noethersch.

Beweis.

Wir nehmen an, es gibt ein nicht endlich erzeugtes Ideal I in $R[X]$. Da $I \neq \{0\}$, gibt es $f_1 \in I\backslash\{0\}$ mit minimalem Grad, $f_2 \in I\backslash(f_1)$ mit minimalem Grad, $f_3 \in I\backslash(f_1, f_2) = I\backslash(R[X]f_1 + R[X]f_2)$ mit minimalem Grad u.s.w.. Diese Kette bricht nicht ab und die Folge der Grade von f_i ist monoton wachsend.

Sei $f_k = a_kX^{m_k} + \cdots$ mit $a_k \neq 0$. Es folgt $m_k \leq m_{k+1}$ und $(a_1, ..., a_k) = Ra_1 + ... + Ra_k \subseteq (a_1, ..., a_{k+1})$. Weiter gilt: $(a_1, ..., a_k) \neq (a_1, ..., a_{k+1})$, sonst $a_{k+1} = \sum\{r_i a_i \mid i = 1, ..., k\}$ mit $r_i \in R$.

Definiere $g := \sum\{r_i X^{m_{k+1}-m_i} f_i \mid i = 1, ..., k\}$. Dann gelten für $h := f_{k+1} - g$, dass $\deg h < m_{k+1}$ und $h \in I \backslash (f_1, ..., f_k)$, Widerspruch. Gleichzeitig kann nicht gelten $(a_1, ..., a_k) \subsetneq (a_1, ..., a_{k+1})$, da R Noethersch. Also gibt es in $R[X]$ nur endlich erzeugte Ideale. □

2.12. Definition

$R[X_1, ..., X_n] := R[X_1, ..., x_{n-1}][X_n]$ heißt Polynomring mehrerer Unbestimmter.

Elemente aus $R[X_1, ..., X_n]$ sind Polynome der Gestalt $f = a_0 + a_1 X_n^1 + \cdots + a_d X_n^d$ mit $a_i \in R[X_1, ..., X_{n-1}]$.

Beachte: $R[X_1, ..., X_n] = R[X_{\sigma(1)}, ..., X_{\sigma(n)}]$ für beliebige Permutation $\sigma \in S_n$.

2.13. Beispiel

Sei

$$f = f[X, Y] = 1 + 3X + 7Y - X^2 Y + YX \in R[X, YY],$$

dann gelten

$$\begin{array}{rclcrcl} \deg_Y(f) & = & \deg_y((1+3X) + (7 + X - X^2)Y) & = & 1 \text{ in } R[X][Y] & \text{und} \\ \deg_X(f) & = & \deg_X((1+7Y) + (3+Y)X - YX^2) & = & 2 \text{ in } R[Y][X]. & \end{array}$$ ◊

2.14. Definition

Ein Monom ist ein Polynom der Gestalt $f = aX_1^{\nu_1} \cdots X_n^{\nu_n}$. f heißt primitiv, falls $a = 1$.

$\deg_{\text{tot}}(f) := \nu_1 + \cdots + \nu_n$ heißt der totale Grad von f.

Der Grad $\deg f(X_1, ..., X_n) := \deg_X f(X, ..., X)$ eines Polynoms $f \in R[X_1, ..., X_n]$ ist das Maximum der totalen Grade der Monome in f.

$f \in R[X_1, ..., X_n]$ heißt homogen, falls alle Monome in f den gleichen totalen Grad haben.

2.15. Beispiel

1. $f = X^3 - 3Y^2 + XY \in R[X, Y]$ hat den Grad 2 und ist nicht homogen.
2. $g = aX + bY \in R[X, Y]$ hat den Grad 1 und ist homogen. ◊

2.16. Bemerkung

Jedes $f \in R[X_1, ..., X_n]$ hat eine eindeutige Darstellung

$$f = \sum_{(\nu_1, ..., \nu_n) \in \mathbb{N}_0^n} a_{\nu_1, ..., \nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n}.$$ ◊

2.17. Behauptung

Sei K ein Körper, dann ist $K[X_1, ..., X_n]$ Noethersch.

Beweis.

$K[X_1]$ ist ein Hauptidealring, insbesondere Noethersch. Nach dem Hilbertschen Basisatz ist dann auch $K[X_1, ..., X_n]$ Noethersch. □

2.18. Behauptung

$K[X, Y]$ ist kein Hauptidealring.

BEWEIS.

Wäre (X,Y) ein Hauptideal in $R = K[X,Y]$, d.h. $RX + RY = Rf = (f)$ für ein $f = f(X,Y) \in R$, dann sind $f = gX + hY$ und $f \mid X$, $f \mid Y$. Aus $f \mid X$ folgt $\deg_Y f = 0$, also $f = f(X) \in K[X]\backslash\{0\}$; gleichzeitig folgt aus $f \mid Y$, dass auch $\deg_X f = 0$, d.h. $f = a \in K\backslash\{0\}$. Einsetzung der Null ergibt: $a = g(0,0)0 + h(0,0)0 = 0$, ein Widerspruch. □

2.19. WIEDERHOLUNG

1. Seien $R \subseteq R'$ Ringe und $a_1, ..., a_n \in R'$. Dann ist $R[X_1, ..., X_n] \to R'$, $f \mapsto f(a_1, ..., a_n)$ ein Homomorphismus, der Einsetzungshomomorphismus von f an der Stelle $(a_1, ..., a_n)$
2. $(a_1, ..., a_n) \in R'$ heißt Nullstelle von f, falls $f(a_1, ..., a_n) = 0$. ◊

2.20. LEMMA (Faktorisierung)

$a \in R$ ist eine Nullstelle von $f \in R[X] \Leftrightarrow f = (X - a)g$ für ein $g \in R[X]$.

BEWEIS.

$\Rightarrow$ Sei $f \neq 0$. Dann gibt es $g, r \in R[X]$ mit $f = (X - a)g + r$ und $\deg r < 1$, d.h. $r \in R$. Wegen $f(a) = 0$ folgt $r = 0$, also $f = (X - a)g$.

$\Leftarrow$ Trivial. □

2.21. SATZ

Ist R ein Integritätsbereich, dann besitzt $f \in R[X]\backslash\{0\}$ höchstens $\deg f$ viele Nullstellen in R.

BEWEIS.

Wir führen eine Induktion über $n = \deg f$. Der Fall $n = 0$ ist klar. Gelte die Behauptung also für ein n. Sei dann a eine Nullstelle von $f \in R[X]$ mit $\deg(f) = n$. Dann ist $f = (X - a)g$ für ein $\deg g = n - 1$. Wegen $f(b) = 0$, $b \neq a$ ist $g(b) = 0$ und mit der Induktionsvoraussetzung folgt: f hat höchstens n Nullstellen. □

2.22. KOROLLAR (Interpolation)

Seien K ein Körper, $a_1, ..., a_n$ paarweise verschiedene Elemente von K und $b_1, ..., b_n \in K$ beliebig.

Dann gibt es genau ein Polynom $f \in K[X]$ mit $\deg f \leq n - 1$ und $f(a_i) = b_i$.

BEWEIS.

1. Eindeutigkeit: Seien $f, g \in K[X]$ mit $f(a_i) = b_i = g(a_i)$ und $\deg f \leq n - 1$, $\deg g \leq n - 1$. Dann sind $(f - g)(a_i) = 0$ und $\deg(f - g) \leq n - 1$, also $f - g = 0$ und damit $f = g$.
2. Existenz: Definiere

$$f = \sum_{i=1}^{n} b_i \frac{(X - a_1)(X - a_2) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)}{(a_i - a_1)(a_i - a_2) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)},$$

dann gilt $f(a_i) = b_i$ für alle i. f heißt Interpolationspolynom nach Lagrange.

Alternativ kann man auch nach dem Newtonsches Interpolationsverfahen vorgehen: Mache den Ansatz

$$f = c_0 + c_1(X - a_1) + c_2(X - a_1)(X - a_2) + \cdots + c_{n-1}(X - a_1) \cdots (X - a_{n-1})$$

und bestimme die Koeffizienten c_i iterativ:

a) $f(a_1) = b_1 \Rightarrow b_1 =: c_0$.

b) $f(a_2) = b_2 \Rightarrow b_2 = b_1 + c_1(a_2 - a_1)$, d.h. $c_1 = \frac{b_2 - b_1}{a_2 - a_1}$ u.s.w. □

2.3 Primideale und maximale Ideale

2.23. Wiederholung

1. Sei R ein kommutativer Ring mit Eins. Ein R-Ideal $\mathcal{P} \neq R$ heißt Primideal, falls aus $xy \in \mathcal{P}$ folgt $x \in \mathcal{P}$ oder $y \in \mathcal{P}$.
2. $\{0\}$ ist genau dann ein Primideal in R, wenn R ein Integritätsbereich ist.
3. Ein R-Ideal I heißt maximales Ideal, wenn für beliebiges R-Ideal J gilt: $I \subseteq J \Rightarrow I = J$.
4. Jedes maximale Ideal ist ein Primideal.
5. Sei $I \subsetneq R$ ein Ideal, dann gilt: I ist maximal $\Leftrightarrow R/I$ ist ein Körper.

   Insbesondere gilt: Ist I maximal, dann ist I ein Primideal:

2.24. Satz

Ein R-Ideal $\mathcal{P} \neq R$ ist Primideal $\Leftrightarrow R/\mathcal{P}$ ist Integritätsbereich.

Beweis.

$\Rightarrow$ Seien $\mathcal{P}$ ein Primideal und $(x+\mathcal{P})(y+\mathcal{P}) = 0+\mathcal{P} = \mathcal{P}$. Zu zeigen: $x+\mathcal{P} = \mathcal{P}$ oder $y+\mathcal{P} = \mathcal{P}$.

Es gilt $(x+\mathcal{P})(y+\mathcal{P}) = xy+\mathcal{P} = \mathcal{P}$ genau dann, wenn $xy \in \mathcal{P}$. Dann ist $x \in \mathcal{P}$ oder $y \in \mathcal{P}$, also $x+\mathcal{P} = \mathcal{P}$ oder $y+\mathcal{P} = \mathcal{P}$.

$\Leftarrow$ Seien $R/\mathcal{P}$ ein Integritätsbereich und $xy \in \mathcal{P}$. Wir zeigen: $\mathcal{P}$ ist ein Primideal.

Aus $xy \in \mathcal{P}$ folgt $xy+\mathcal{P} = \mathcal{P}$, d.h. $(x+\mathcal{P})(y+\mathcal{P}) = \mathcal{P}$ und damit $x+\mathcal{P} = \mathcal{P}$ oder $y+\mathcal{P} = \mathcal{P}$, d.h. $x \in \mathcal{P}$ oder $y \in \mathcal{P}$. □

2.4 Teilbarkeit in Integritätsbereichen

2.25. Wiederholung

Seien R ein Integritätsbereich und $a, b \in R$.

1. a teilt b (in Zeichen: $a \mid b$) $:\Leftrightarrow$ es gibt ein $c \in R$ mit $ac = b$.
2. a ist assoziiert zu b (in Zeichen: $a \sim b$) $:\Leftrightarrow$ es gibt ein $c \in R^\times$ mit $ac = b \Leftrightarrow a \mid b$ und $b \mid a$.
3. $a \neq 0$ heißt unzerlegbar oder irreduzibel, falls $a \notin R^\times$ und aus $a = bc$ folgt, dass $b \in R^\times$ oder $c \in R^\times$.
4. Für das von a in R erzeugte Ideal $(a) := Ra$ gilt: $a \mid b \Leftrightarrow (b) \subseteq (a)$ und $a \sim b \Leftrightarrow (a) = (b)$.
5. $a_0, a_1, ..., a_n, ...$, heißt Teilerkette, falls $a_{i+1} \mid a_i$ und $a_i \nmid a_{i+1} \Leftrightarrow (a_0) \subsetneq (a_1) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$. ◊

2.26. Bemerkung

1. In Noetherschen Ringen gibt es keine unendlichen Teilerketten, denn jede aufsteigende Kette von Idealen bricht ab.
2. Gibt es in R keine unendlichen Teilerketten, so ist jedes $a \in R\backslash\{0\}$ eine Einheit oder ein Produkt von endlich vielen irreduziblen Elementen aus R. ◊

2.27. Wiederholung

1. $p \in R\backslash(R^\times \cup \{0\})$ heißt Primelement, falls aus $p \mid ab$ folgt, dass $p \mid a$ oder $p \mid b$, d.h. falls $ab \in (p)$ impliziert, dass $a \in (p)$ oder $b \in (p)$ gilt.

   Primelemente sind irreduzibel. Weiter ist p genau dann prim, wenn (p) ein Primideal ist.
2. Ist R ein Hauptidealring und Integritätsbereich, so sind alle irreduzible Elemente prim und jedes $a \in R\backslash(R^\times \cup \{0\})$ ist bis auf Reihenfolge und Einheiten eindeutiges Produkt von irreduziblen Elementen.

Ist R nur Integritätsbereich, für den diese beiden Bedingungen gelten, so heißt R ein ZPE-Ring ("Zerlegung in Primelemente eindeutig") oder ein faktorieller Ring.

3. Seien $a, b \in R\backslash\{0\}$ mit $a = e_1 \prod_{i=1}^{n} p_i^{\nu_i}$ und $b = e_2 \prod_{i=1}^{n} p_i^{\mu_i}$. Dann heißt

$$\mathrm{ggT}(a,b) := \prod_{i=1}^{n} p_i^{\min\{\nu_i,\mu_i\}}$$

der größte gemeinsame Teiler von a und b und

$$\mathrm{kgV}(a,b) := \prod_{i=1}^{n} p_i^{\max\{\nu_i,\mu_i\}}$$

das kleinste gemeinsame Vielfache von a und b. Diese sind bis auf eine Einheit eindeutig bestimmt.

4. Es gilt $a \mid b \Leftrightarrow \nu_i \leq \mu_i$ für alle i und damit $\mathrm{ggT}(a,b) \mid a$ und $\mathrm{ggT}(a,b) \mid b$. Weiter gilt für alle $d \in R$: Falls $d \mid a$ und $d \mid b$, dann auch $d \mid \mathrm{ggT}(a,b)$. Durch diese Eigenschaften ist der größte gemeinsame Teiler von a und b (bis auf Einheiten) eindeutig festgelegt.

   Weiter gilt: $(a,b) \subseteq (c)$ und $(a,b) \subseteq (d) \Rightarrow (c) \subseteq (d)$, d.h. (c) ist das kleinste Hauptideal über (a,b). In Hauptidealringen gilt sogar: $(a,b) = (c)$ und $c = xa + by$ für gewisse $x, y \in R$. ◊

2.28. Korollar

Ein Noetherscher Integritätsbereich ist genau dann faktoriell, wenn alle irreduziblen Elemente prim sind.

Beweis.

⇒ Klar nach Definition von faktoriellen Ringen.

⇐ Ist R Noethersch, so gibt es keine unendlichen Teilerketten in R, d.h. jedes $a \in R\backslash(R^\times \cup \{0\})$ ist endliches Produkt irreduzibler Elemente. Weiter gilt: Sind alle irreduziblen Elemente prim, so ist die Produktdarstellung eindeutig. □

2.5 Teilbarkeit in Polynomringen

2.29. Wiederholung

Sei R ein faktorieller Ring (insbesondere Integritätsbereich), z.B. $R = \mathbb{Z}$ oder $R = \mathbb{R}[X]$.

1. $K := \mathrm{Quot}(R) := \{\frac{a}{b} \mid a, b \in R,\ b \neq 0\}$ heißt Quotientenkörper von R, z.B. $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$ oder $\mathrm{Quot}(\mathbb{R}[X]) = \mathbb{R}(X)$.
2. $R^\times$ ist die Menge der invertierbaren Elemente von R und bildet eine Gruppe, die Einheitengruppe. Beispiele sind $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$ unf $(R[X])^\times = R^\times$. ◊

2.30. Definition

$f \in R[X]$ heißt primitives Polynom, falls $f = a_0 + a_1 X + \cdots + a_n X^n$ und $\mathrm{ggT}(a_0, ..., a_n) \in R^\times$.

2.31. Beispiel

$2 + 10X - 36X^2 - 3X^4$ ist in $\mathbb{Z}$ primitiv. $2 + 10X - 36X^2$ nicht. ◊

2.32. Definition

Seien R faktorieller Ring und $f = a_0 + a_1 X + \cdots + a_n X^n$. $\mathrm{ggT}(a_0, ..., a_n) =: \mathrm{I}(f)$ heißt Inhalt von f.

2.33. Bemerkung

1. $\mathrm{I}(f)$ ist bis auf Einheiten eindeutig bestimmt.
2. Für $f(X) = \mathrm{I}(f)f_0(X)$ ist $f_0(X)$ primitiv (d.h. $\mathrm{I}(f_0) = 1$). ◊

2.34. Beispiel

1. Ist $R = K$ ein Körper, dann ist jedes $f \in K[X]\backslash\{0\}$ primitiv.
2. Genau dann ist $a_0 \in R$ primitiv, wenn a_0 eine Einheit ist.
3. Sind $f \in R[X]$ irreduzibel und $\deg f > 0$, dann ist f primitiv, denn aus $f = \mathrm{I}(f)f_0,\ \deg f = \deg f_0$ folgt $\mathrm{I}(f) \in R^\times$. ◊

2.35. Lemma (Gauß)

Das Produkt primitiver Polynome ist wieder primitiv.

Beweis.

Seien $f = a_0 + a_1X + \cdots + a_nX^n$ und $g = b_0 + b_1X + \cdots + b_mX^m$ beide primitiv und $a_n \neq 0,\ b_m \neq 0$. Dann ist $fg = c_0 + x_1X + \cdots + c_{n+m}X^{n+m}$ mit $c_{n+m} = a_nb_m \neq 0$. Angenommen, es gäbe ein primes p, das alle c_i teilt, $i = 1, ..., n+m$. Wähle k, l minimal mit $p \nmid a_k$ und $p \nmid b_l$. Dann würde gelten

$$c_{k+l} = \sum_{\substack{r+s \\ = \\ k+l}} a_rb_s = \sum_{\substack{r<k \\ \text{oder} \\ s<l}} a_rb_s + a_lb_l$$

und $p \mid c_{k+l},\ p \mid \sum\limits_{\substack{r<k \\ \text{oder} \\ s<l}} a_rb_s$, aber $p \nmid a_lb_l$, was nicht möglich ist. □

2.36. Satz

Seien R ein faktorieller Integritätsbereich und $f, g \in R[X]$.

Dann gilt: $f \mid g$ in $R[X] \Leftrightarrow f \mid g$ in $K[X] = \mathrm{Quot}(R)[X]$ und $\mathrm{I}(f) \mid \mathrm{I}(g)$ in R.

Beweis.

$\Rightarrow$ Ist $fh = g$ mit $h \in R[X]$, dann $h \in K[X]$. Setze $f = \mathrm{I}(f)f_0,\ h = \mathrm{I}(h)h_0,\ g = \mathrm{I}(g)g_0$ mit f_0, g_0, h_0 primitiv. Dann ist $\mathrm{I}(f)\mathrm{I}(h)f_0h_0 = \mathrm{I}(g)g_0$ und nach dem Lemma von Gauß ist f_0h_0 primitiv, also $\mathrm{I}(f)\mathrm{I}(h) = \mathrm{I}(g)$ (bis auf Einheiten in R). Also $\mathrm{I}(f)\mathrm{I}(h) = \mathrm{I}(fh)$, d.h. $\mathrm{I}(f) \mid \mathrm{I}(g)$ in R.

$\Leftarrow$ Sei $fh = g$ mit $h \in K[X]$, d.h. $h = \frac{b}{c}h_0$ mit $h_0 \in R[X]$ primitiv. Nach Voraussetzung gilt $\mathrm{I}(f)a = \mathrm{I}(g)$ für ein $a \in R$, also $\mathrm{I}(f)f_0\frac{b}{c}h_0 = \mathrm{I}(g)g_0 = \mathrm{I}(f)ag_0$, d.h. $\frac{b}{c}f_0h_0 = ag_0 \Leftrightarrow bf_0h_0 = acg_0$, d.h. $b \sim ac$, also $\frac{b}{c} \in R$. Dann aber auch $h \in R[X]$. □

2.37. Korollar

1. Seien R faktoriell und $a \in R$ irreduzibel in R. Dann ist a irreduzibel in $R[X]$.
2. Ist $g \in R[X]$ irreduzibel in $R[X]$ mit $\deg g > 1$, dann ist g irreduzibel in $K[X]$.
3. Ist $g \in R[X]$ primitiv und irreduzibel in $K[X]$, so ist g irreduzibel in $R[X]$.

Beweis.

1. Klar.
2. Gelte $f \mid g$ in $K[X]$, Œ $f \in R[X]$ primitiv, dann $f \mid g$ in $R[X]$, d.h. $f \sim g$ oder $f \sim 1$ in $R[X]$, also auch insbesondere in $K[X]$.

3. Sei $f \in R[X]$ mit $f \mid g$ in $R[X]$, dann $f \mid g$ in $K[X]$ (d.h. $\deg f = \deg g$ oder $\deg f = 0$) und $\mathrm{I}(f) \mid \mathrm{I}(g) = 1$, also $\mathrm{I}(f) = 1$. Dann $f \sim g$ oder $f \sim 1$ in $R[X]$. □

2.38. Beispiel

Sei $R = \mathbb{Z}$, d.h. $K = \mathbb{Q}$. $q = 2X^2 + 4 \in \mathbb{Q}[X]$ ist reduzibel in $\mathbb{Z}[X]$, da $q = 2(X^2 + 2)$, aber irreduzibel in $\mathbb{Q}[X]$, da 2 eine Einheit in $\mathbb{Q}[X]$ ist.

2.39. Satz (Gauß)

Ist R faktoriell, so auch $R[X]$.

Beweis.

1. Sei $f_1, f_2, f_3, ...$ eine Teilerkette in $R[X]$, d.h. $f_{i+1} \mid f_i$. Dann auch $\mathrm{I}(f_{i+1}) \mid \mathrm{I}(f_i)$ und $\deg f_{i+1} \leq \deg f_i$. Also ist $\mathrm{I}(f_1), \mathrm{I}(f_2), \mathrm{I}(f_3), ...$ eine Teilerkette in R und es gilt $\deg f_1 \geq \deg f_2 \geq \deg f_3 \geq \cdots$ in $K[X]$. Beides bricht ab, da R faktoriell ist. Also gibt es $n \in \mathbb{N}$, so dass für alle $m \geq n$ gilt: $\mathrm{I}(f_n) \sim \mathrm{I}(f_m)$ in R und $f_n \sim f_m$ in $K[X]$, d.h. $f_n \sim f_m$ in $R[X]$. Also gibt es keine unendlichen Teilerketten in $R[X]$.

2. Sei $f \in R[X]$ irreduzibel mit $\deg f > 0$. Dann gilt: $f \mid gh$ in $R[X]$, d.h. $f \mid gh$ in $K[X]$, also $f \mid g$ oder $f \mid h$ in $K[X]$. Da $\mathrm{I}(f) = 1$, folgt weiter: $f \mid g$ oder $f \mid h$ in $R[X]$, d.h. f ist prim in $R[X]$.

   Sei jetzt $f \in R$, dann gilt $f \mid \mathrm{I}(gh) = \mathrm{I}(g)\mathrm{I}(h)$ nach dem Lemma von Gauß. Da R faktoriell ist, ist f prim in R, d.h. $f \mid \mathrm{I}(g)$ oder $f \mid \mathrm{I}(h)$, also $f \mid g$ oder $f \mid h$ in $R[X]$ und damit f prim in $R[X]$. □

2.40. Bemerkung

$K[X, Y]$ ist faktoriell, da $K[Y]$ faktoriell ist. Per Induktion folgt dann: $K[X_1, ..., X_n]$ ist faktoriell. ◊

2.41. Satz (Eisenstein-Kriterium)

Seien R ein faktorieller Ring, $p \in R$ prim und $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ primitiv.

Gilt $p \mid a_i$ für alle $0 \leq i \leq n-1$, $p \nmid a_n$ und $p^2 \nmid a_0$, so ist f irreduzibel in $R[X]$.

Beweis.

Sei $f = gh$ für gewisse $g, h \in R[X]$ mit $g \nsim f$ und $h \nsim f$, d.h. $\deg g > 0$ und $\deg h > 0$. Seien $g = b_0 + b_1 X + \cdots + b_r X^r$ mit $b_r \neq 0$, $0 < r$ und $h = c_0 + c_1 X + \cdots + c_s X^s$ mit $c_s \neq 0$, $0 < s$. Dann gelten $a_0 = b_0 c_0$ und $p^2 \nmid a_0$, d.h. $p^2 \nmid b_0$ oder $p^2 \nmid c_0$, etwa $p^2 \nmid b_0$. Damit gilt $p \mid c_0$, denn $p \mid a_0$. Sei j minimal mit $p \nmid c_{j+1}$. Dann ist $0 \leq j < s$, denn $p \nmid a_n = b_r c_s$. Es gilt

$$a_{j+1} = \sum_{\substack{l+k \\ = \\ j+1}} b_l c_k = b_0 c_{j+1} + b_1 c_j + b_2 c_{j-1} + \cdots \text{ mit } p \mid b_0 c_{j+1},\ p \nmid b_1 c_j,\ p \nmid b_2 c_{j-1},\ ...,$$

also $p \nmid a_{j+1}$, d.h. $j + 1 = n = s + r > s$, Widerspruch. □

2.42. Bemerkung (Kreisteilungspolynome & Einheitswurzeln)

1. Seien $p \in \mathbb{N}$ prim und $R = \mathbb{Z}$. $\Phi_p(X) := 1 + X + X^2 + \cdots + X^{p-1}$ heißt das p-te Kreisteilungspolynom. Es gilt $(X-1)\Phi_p(X) = X^p - 1$. Für $z \in \mathbb{C}$ gelten $z^p = 1 \Rightarrow |z| = 1$ und $|z|^2 = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2 = 1$, d.h. die p-te Einheitswurzel $z = e^{\frac{2\pi i}{p}}$ liegt auf dem Einheitskreis.

2. Φ_p ist irreduzibel in $\mathbb{Q}[X]$. Wir zeigen dazu: $\Phi_p(X+1)$ ist irreduzibel in $\mathbb{Q}[X]$.

   Einsetzen von $X + 1$ für X in $(X-1)\Phi_p(X) = X^p - 1$ ergibt:

   $$X\Phi_p(X+1) = (X+1)^p - 1 = X^p + \tbinom{p}{1} X^{p-1} + \cdots + \tbinom{p}{p-1} X.$$

   Also ist $\Phi_p(X+1) = X^{p-1} + \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-1}$. Wir wissen: $p \mid \binom{p}{1}$, $p \mid \binom{p}{2}$, ..., $p \mid \binom{p}{p-1} = p$.

   Die Einsetzung $h[X] \to h(g)$ mit $g \in R[X]$ definiert einen Ringhomomorphismus $\sigma_g : R[X] \to R[X]$.

Für $g = aX + b$ mit $a \in R^\times$ ist σ_g ein Automorphismus von $R[X]$:

$$f(X) \mapsto f(aX + b) \mapsto f\left(a\tfrac{X-b}{a} + b\right) = f(X) \ .$$

Also ist f genau dann irreduzibel, wenn $\sigma_g(f)$ irreduzibel ist für $g = aX + b,\ a \in R^\times$. Nach Eisenstein ist damit $\Phi_p(X)$ irreduzibel in $\mathbb{Q}[X]$. ◊

2.43. Beispiel

$X^{17} + 3$ und $X^5 - 36X + 2$ sind irreduzibel in $\mathbb{Z}[X]$. ◊

3 Körper

3.1 Grundbegriffe

3.1. Wiederholung

1. Ein Körper $(K, +, \cdot)$ ist ein kommutativer Ring mit Eins, so dass $K^\times = K\backslash\{0\}$.
2. Betrachte den (Ring-)Homomorphismus $\varphi : \mathbb{Z} \to K,\ n \mapsto n \cdot 1$ mit

   $$0 \cdot 1 = 0, \qquad n \cdot 1 = 1 + \cdots + 1 \qquad \text{und} \qquad -n \cdots 1 = -(1 + \cdots + 1)$$

   für alle $n \in \mathbb{N}$. Dann ist $\text{Bild}(\varphi) \subseteq K$ ein Integritätsbereich und $\text{Kern}(\varphi)$ ist ein Primideal, denn $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\text{Kern}(\varphi)$. Die Primideale in $\mathbb{Z}$ sind aber gerade $\{0\}$ und $p\mathbb{Z}$ mit p prim. Im Fall $\text{Kern}(\varphi) = \{0\}$ ist φ injektiv, d.h. eine Einbettung von $\mathbb{Z}$ in K (in Zeichen: $\mathbb{Z}\hookrightarrow K$). Andernfalls ist $\text{Kern}(\varphi) = p\mathbb{Z}$ (d.h. $p \cdot 1 = 0$) und es gilt $\text{Bild}(\varphi) = \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p \hookrightarrow K$.
3. $\mathbb{Q}$ und $\mathbb{F}_p$ sind Primkörper, besitzen also keine echten Unterkörper. Jeder Primkörper ist isomorph zu $\mathbb{F}_p$ für eine Primzahl p oder zu $\mathbb{Q}$. Sei allgemein K ein Körper, dann ist

   $$\text{Prim}(K) := \bigcap_{\substack{k \subseteq K \\ k\text{Körper}}}$$

   der Primkörper von K. Insbesondere ist $\text{char}(K) = \text{char}(\text{Prim}(K))$.
4. Gilt $\text{Kern}(\varphi) = p\mathbb{Z}$, so heißt K ein Körper der Charakteristik p (in Zeichen: $\text{char}(K) = p$). Dagegen setzen wir $\text{char}(\mathbb{Q}) := 0$. Für Körper $K \hookrightarrow L$ gilt $\text{char}(K) = \text{char}(L)$. Speziell folgt aus $\mathbb{Q} \subseteq K$ also $\text{char}(K) = 0$ bzw. aus $\mathbb{F}_p \subseteq K$, dass $\text{char}(K) = p$.
5. Sei $\text{char}(K) = p$. Dann ist $\sigma_p : K \to K$ mit $\sigma_p(a) := a^p$ ein Ringhomomorphismus, denn $1^p = 1$, $(ab)^p = a^p b^p$ und $(a + b)^p = a^p + b^p$ – dies folgt mit $\frac{p!}{k!(p-k)!} = \frac{(p-1)!}{k!(p-k)!}$ ausn dem Binomischen Lehrsatz. σ_p ist injektiv, denn ist $a \in \text{Kern}(\varphi)$, dann $0 = a^p$, also $a = 0$. Ist K endlich, so ist σ_p auch surjektiv, also $\sigma_p \in \text{Aut}(K)$, der Frobenius-Automorphismus.
6. Sei $\varphi : K \to L$ ein Körperhomomorphismus, d.h. Ringhomomorphismus zwischen Körpern. Dann ist φ entweder injektiv oder trivial, denn $\text{Kern}(\varphi)$ ist ein Ideal in K; die einzigen Ideale in K sind aber $\{0\}$ und K selbst: Sind $I \subseteq K$ ein Ideal und $a \in I\backslash\{0\}$, dann ist $a \cdot \frac{b}{a} \in I$ für alle $b \in K$, d.h. $I = K$.◊

3.2. Definition

Seien K ein Körper, k ein Unterkörper von K und A eine Teilmenge von K. Definiere

$$k[A] := \bigcap_{\substack{K \supseteq R \text{ Ring} \\ k \cup A \subseteq R}} R \qquad \text{und} \qquad k(A) := \bigcap_{\substack{K \supseteq L \text{ Körper} \\ k \cup A \subseteq L}} L.$$

$k[A]$ heißt der von A in K über k erzeugte Ring und $k(A)$ heißt der von A in K über k erzeugte Körper.

Im Fall $A = \{a_1, ..., a_n\}$ setzen wir $k[a_1, ..., a_n] := k[A]$ und $k(a_1, ..., a_n) := k(A)$.

3.3. Bemerkung

1. Seien $k \subseteq K$ Körper und $a_1, ..., a_n \in K$. Dann gelten:
$$k[a_1, ..., a_n] = \{f(a_1, ..., a_n) \mid f \in k[X_1, ..., X_n]\}$$
ist ein Ring, der in allen $R \subseteq K$ mit $k \cup \{a_1, ..., a_n\} \subseteq R$ enthalten ist, und
$$k(a_1, ..., a_n) = \left\{ \frac{f(a_1, ..., a_n)}{g(a_1, ..., a_n)} \;\middle|\; f, g \in k[X_1, ..., X_n],\ g(a_1, ..., a_n) \neq 0 \right\}$$
ist der Quotientenkörper von $k[a_1, ..., a_n]$.
2. $k(A \cup B) = k(A)(B)$, denn für $L \subseteq K$ gilt: $k \cup (A \cup B) \subseteq L \Leftrightarrow k(A) \cup B \subseteq L$. ◊

3.2 Körpererweiterungen

3.4. Definition

Seien $K \subseteq L$ Körper. Dann heißt L Körpererweiterung von K (in Zeichen: $L|K$).

Fasse L als K-Vektorraum auf. $[L : K] := \dim_K(L)$ heißt der Grad von $L|K$.

3.5. Beispiel

1. $\mathbb{R} \subseteq \mathbb{C}$: $[\mathbb{C} : \mathbb{R}] = 2$. Eine Basis ist etwa $(1, i)$, dann $\mathbb{C} = \{a \cdot 1 + b \cdot i \mid a, b \in \mathbb{R}\}$. Es gilt
$$\mathbb{C} = \mathbb{R}(i) = \{\frac{f(i)}{g(i)} \mid f, g \in \mathbb{R}[X],\ g(i) \neq 0\} = \{a + bX \mid a, b \in \mathbb{R}\} = \mathbb{R}[i].$$
Allgemein ist $\mathbb{R}[X] \subseteq \mathbb{R}(X)$.
2. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$: $[\mathbb{Q} : \mathbb{Q}(\sqrt{2})] = 2$ mit Basis $(1, \sqrt{2})$. Es gilt
$$\begin{aligned}\mathbb{Q}(\sqrt{2}) &= \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} \;\middle|\; f, g \in \mathbb{R}[X], g(\sqrt{2}) \neq 0 \right\} \\ &= \left\{ \frac{a + b\sqrt{2}}{d + e\sqrt{2}} \;\middle|\; a, b, c, d \in \mathbb{Q},\ c \neq 0 \text{ oder } d \neq 0 \right\} \\ &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},\end{aligned}$$
denn mit quadratischer Ergänzung gilt
$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} \frac{c - d\sqrt{2}}{c - d\sqrt{2}} \in \mathbb{Q} + \mathbb{Q}\sqrt{2}.$$
3. $\mathbb{Q} \subseteq \mathbb{Q}(X)$: $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$, denn $1,\ X,\ X^2,\ ...$ sind $\mathbb{Q}$-linear unabhängig.
4. $\mathbb{Q} \subseteq \mathbb{R}$: $[\mathbb{R} : \mathbb{Q}] = \infty$, der Beweis folgt später. ◊

3.6. Satz (Gradsatz)

Seien $k \subseteq K \subseteq L$ Körper. Dann gilt: $[L : k] = [L : K][K : k]$.

Im endlichdimensionalen Fall gilt weiter: Sind $(x_1, ..., x_n)$ eine Basis von K über k und $(y_1, ..., y_m)$ eine Basis von L über K, so ist $(x_1y_1,\ ...,\ x_1y_m,\ ...,\ x_2y_1,\ ...,\ ...,\ x_ny_m)$ Basis von L über k.

Beweis.

1. Lineare Unabhängigkeit: Gelte
$$0 = \sum_{j=1}^{m} \sum_{i=1}^{n} \alpha_{ij}(x_iy_j) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij}x_i \right) y_j =: \sum_{j=1}^{m} \beta_j y_j$$
mit $\beta_j \in K$.

Da die y_j linear unabhängig über K sind, sind alle $\beta_j = 0$. Da die x_i linear unabhängig über K sind, sind alle $\beta_j = \sum \alpha_{ij} x_i = 0$, d.h. auch alle $\alpha_{ij} = 0$. Also sind alle $x_i y_j$ linear unabhängig.

2. Erzeugendensystem: Sei $a \in L$, dann $a = \sum \beta_j y_j$ für gewisse $\beta_j \in K$, wobei $\beta_j = \sum \alpha_{ij} x_i$ für gewisse $\alpha_{ij} \in k$. Also ist

$$a = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} x_i \right) y_j = \sum_{j=1}^{m} \sum_{i=1}^{n} \alpha_{ij} (x_i y_j). \qquad \square$$

3.7. Korollar

Seien $k \subseteq K \subseteq L$ Körper. Dann gelten:

1. Gilt $[K : k] = [L : k]$, dann ist $[L : K] = 1$, d.h. $L = K$.
2. Ist $[L : k]$ prim, dann gilt $k = K$ oder $K = L$.
3. Zwischen $\mathbb{R}$ und $\mathbb{C}$ gibt es keinen echten Zwischenkörper.

3.8. Definition

Sind $k \subseteq K$ und $K = k(a)$, so heißt K eine einfache Erweiterung von k und a heißt ein primitives Element der Erweiterung $K|k$.

Sind $k \subseteq K$, so heißt $a \in K$ algebraisch über k, falls es ein $f \in k[X] \backslash \{0\}$ gibt mit $f(a) = 0$. Andernfalls heißt a transzendent über k. Speziell heißen algebraische Elemente von $\mathbb{C}|\mathbb{Q}$ algebraische Zahlen.

3.9. Beispiel

1. i ist ein primitives Element von $\mathbb{C}|\mathbb{R}$.
2. $\sqrt{2}$, i und $\sqrt[3]{5}$ sind algebraische Zahlen (zu $X^2 - 2 = 0$, $X^2 + 1 = 0$ und $X^3 - 5 = 0$).
3. π und e sind transzendente Zahlen. Der Beweis ist sehr schwierig, für π: Lindemann, 1882. $\Diamond$

3.10. Wiederholung

1. Seien $k \subseteq K$ und $a \in K$. Dann heißt $\varphi_a : k[X] \to K$, $f \mapsto f(a)$ ein Einsetzungshomomorphismus.
2. $\mathrm{Kern}(\varphi_a) = \{f \in k[X] \mid f(a) = 0\}$ ist ein $k[X]$-Ideal, also ein Hauptideal. Falls $\mathrm{Kern}(\varphi_a) \neq \{0\}$, so gibt es genau ein normiertes Polynom $f_a \in k[X]$ mit $\mathrm{Kern}(\varphi_a) = (f_a) = f_a k[X]$, denn gelte $(f_a) = (f'_a)$, dann $f_a \sim f'_a$ und aus der Normiertheit folgt $f_a = f'_a$.
3. f_a ist irreduzibel, da Primideal. $\mathrm{Irr}(a, k) := \mathrm{Min}(a, k) := f_a$ heißt das irreduzible Polynom oder Minimalpolynom von a über k.
4. f_a ist dasjenige normierte und irreduzible Polynom $f \in k[X] \backslash \{0\}$, für das gilt $f(a) = 0$.

   Sei nämlich f ein solches Polynom, dann folgt aus $f(a) = 0$, dass $f \in \mathrm{Kern}\varphi_a = (f_a)$. Da f irreduzibel, also $f_a \mid f$ und da f normiert, folgt $f = f_a$. $\Diamond$

3.11. Beispiel

1. $\mathrm{Irr}(\sqrt{5}, \mathbb{Q}) = X^2 - 5$.
2. $\mathrm{Irr}(\sqrt{5}, \mathbb{R}) = X - \sqrt{5}$.
3. $\mathrm{Irr}(\sqrt{-1}, \mathbb{R}) = X^2 + 1$.
4. $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$.
5. $\mathrm{Irr}(\exp(\frac{2\pi i}{5}), \mathbb{C}) = X^4 + X^3 + X^2 + X + 1$ (Irreduzibilität nach Eisenstein-Kriterium).
6. $\mathrm{Irr}(\alpha, k) = X - \alpha$ für $\alpha \in k$. $\Diamond$

3.12. Satz

Seien $k \subseteq K$ und $a \in K$. Dann sind äquivalent:

1. a ist algebraisch über k.
2. Es gilt $k[a] = k(a)$.
3. Für den Grad der Erweiterung $k(a)|k$ gilt $[k(a) : k] < \infty$.

Beweis.

1. (1) $\Rightarrow$ (2): Sei a algebraisch über k. Da (f_a) Primideal, ist (f_a) maximal, d.h. $k[X]/(f_a) \cong k[a]$ nach dem Homomorphiesatz für φ_a. Da $k[X]/(f_a)$ ein Körper ist, muss auch $k[a]$ einer sein.

2. (2) $\Rightarrow$ (3): Gelte $k[a] = k(a)$, d.h. $\text{Bild}(\varphi_a) = k[a] \cong k[X]/(f_a)$ ist ein Körper. Also ist $\text{Kern}(\varphi_a) \neq \{0\}$ sonst wäre $k[X]$ ein Körper, d.h. es gibt ein $f \in k[X]\backslash\{0\}$ mit $f(a) = 0$. Habe f die Darstellung $f(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$, Œ $\alpha_n = 1$. Wegen $f(a) = 0$ ist dann

$$a^n = -\alpha_0 - \alpha_1 a - \cdots - \alpha_{n-1} a^{n-1} \in k + ka + \cdots + ka^{n-1} = \text{span}(1,\ a,\ ...,\ a^{n-1}) =: V.$$

   V ist ein k-Vektorraum mit $\dim(V) \leq n$; aus $a^n \in V$ folgt, dass auch

$$a^{n+1} = -\alpha_0 a - \alpha_1 a^2 - \cdots - \alpha_{n-1} a^n \in ka + \cdots + ka^n \subseteq \text{span}(1,\ a,\ ...,\ a^{n-1}) = V.$$

   Per Induktion folgt: $k[a] \subseteq V$, also nach Voraussetzung auch $k(a) \subseteq V$, d.h. $\dim_k(k(a)) \leq n < \infty$.

3. (3) $\Rightarrow$ (1): Angenommen, a wäre transzendent über k, d.h. $\varphi_a : k[X] \to K$ ist injektiv. Weiter ist $\varphi_a : k[X] \to k[a]$ ein Epimorphismus, d.h. $k[X] \cong k[a]$ als Ringe. Wegen $\varphi_a(\alpha) = \alpha$ für jedes $\alpha \in k$ ist $k[X] \cong k[a]$ als k-Vektorraum. Wäre nun $\dim_k(k[X]) = \infty$, dann $\dim_k(k[a]) = \infty$, d.h. $\dim_k(k(a)) = \infty$ im Widerspruch zur Voraussetzung. □

3.13. Korollar

Seien $k \subseteq K$ Körper, $a \in K$ und $n = \deg(\text{Irr}(a, k))$.

Dann gilt $k(a) = k[a] = k \oplus ka \oplus \cdots \oplus ka^{n-1}$, d.h. $(1,\ a,\ ...,\ a^{n-1})$ ist eine Basis von $k(a)|k$.

Beweis.

Nur noch die lineare Unabhängigkeit von $\{1,\ a,\ ...,\ a^{n-1}\}$ ist zu zeigen.

Gelte $\beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1} = 0$ für $\beta_0,\ ...,\ \beta_{n-1} \in k$. Setze $g(X) := \beta_0 + \beta_1 X + \cdots + \beta_{n-1} X^{n-1}$. Wäre g nicht das Nullpolynom, dann $f_a \mid g$, da $g(a) = 0$. Dies ist ein Widerspruch, da $\deg g \leq \deg f_a$. Also ist $[k(a) : k] = \deg f_a$. □

3.14. Beispiel

1. Seien $a = \sqrt{5}$ und $k = \mathbb{Q}$, dann $\mathbb{Q}(\sqrt{5}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{5}$ (als k-Vektorraum) mit Körperoperationen

$$(\alpha + \beta\sqrt{5}) + (\gamma + \delta\sqrt{5}) = (\alpha + \gamma) + (\beta + \delta)\sqrt{5},$$
$$(\alpha + \beta\sqrt{5})(\gamma + \delta\sqrt{5}) = (\alpha\gamma + 5\beta\delta) + (\alpha\delta + \beta\gamma)\sqrt{5}.$$

2. Sind $a = \sqrt{-1}$ und $k = \mathbb{R}$, dann $\mathbb{R}(\sqrt{-1}) = \mathbb{R} \oplus \mathbb{R}\sqrt{-1}$.

3. Für $a = \sqrt[3]{2},\ k = \mathbb{Q}$ ist $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q} \oplus \sqrt[3]{2} \oplus \mathbb{Q}\sqrt[3]{4}$. ◊

3.15. Definition

$K|k$ heißt eine algebraische Körpererweiterung, falls jedes $a \in K$ algebraisch über k ist.

Andernfalls heißt k transzendent.

3.16. Satz

Sei $k \subseteq K$ eine Körpererweiterung. Dann gelten:

1. Ist $[K : k] < \infty$, dann ist $K|k$ algebraisch und es gibt $a_1, ..., a_n \in K$ mit $K = k(a_1, ..., a_n)$.
2. Sind $a_1, ..., a_n \in K$ algebraisch über k, dann ist $K' := k(a_1, ..., a_n)$ algebraisch über k und für den Grad der Körpererweiterung gilt $[K' : k] < \infty$

Beweis.

1. Seien $\dim_k(K) = m,\ a \in K$. Dann ist $\{1, a, ..., a^m\}$ linear abhängig über k, d.h. es gibt $\alpha_0, ..., \alpha_m \in k$ mit $\alpha_0 + \alpha_1 a + \cdots + \alpha_m a^m = 0$ und nicht alle $\alpha_i = 0$. Setze $g(X) := \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m$. Dann sind $g \in k[X]\backslash\{0\}$ und $g(a) = 0$. Ist $(a_1, ..., a_m)$ Basis von K über k, so ist $K = k(a_1, ..., a_m)$:

$$K = ka_1 + \cdots + ka_m \subseteq k[a_1, ..., a_m] \subseteq k(a_1, ..., a_m) \subseteq K.$$

2. Sei a_1 algebraisch über k, dann ist $[k(a_1) : k] < \infty$. Sei a_2 algebraisch über k, dann ist a_2 algebraisch über $k(a_1)$, d.h. $[k(a_1)(a_2) : k(a_1)] < \infty$. Beachte dabei: $k(a_1)(a_2) = k(a_1, a_2)$. Nach der Gradgleichung ist dann $[k(a_1, a_2) : k] = [k(a_1, a_2) : k(a_1)][k(a_1) : k] < \infty$ u.s.w. bis $[K' : k] = [k(a_1, ..., a_n) : k] < \infty$ und mit 1. folgt: $K'|k$ algebraisch. □

3.17. Korollar

Seien $K|k$ eine Körpererweiterung und $a, b \in K$ algebraisch über k. Dann sind auch $a \pm b,\ ab$ und $\frac{a}{b}$ algebraisch über k.

Insbesondere ist $L := \{a \in K \mid a \text{ ist algebraisch über } k\}$ ein Teilkörper von K.

3.18. Bemerkung

$\widetilde{\mathbb{Q}} := \{a \in \mathbb{C} \mid a \text{ ist algebraisch über } \mathbb{Q}\}$ heißt Körper der algebraischen Zahlen. ◊

3.19. Korollar

Seien $k \subseteq K \subseteq L$. Dann gilt: $L|k$ ist algebraisch $\Leftrightarrow$ $K|k$ und $L|K$ sind algebraisch (Transitivität).

Beweis.

$\Rightarrow$ Klar.

$\Leftarrow$ Sei $a \in L$. Dann gibt es $f \in K[X]\backslash\{0\}$ mit $f(a) = 0$, d.h. $f = a_0 + a_1 X + \cdots + a_n X^n$ mit $a_i \in K$. $k(a_0, ..., a_n)|k$ ist algebraisch und $[k(a_0, ..., a_n) : k] < \infty$, also auch $[k(a_0, ..., a_n)(a) : k(a_0, ..., a_n)] < \infty$, da a algebraisch über $k(a_0, ..., a_n)$. Damit $[k(a_0, ..., a_n, a) : k] < \infty$, d.h. a algebraisch über k. □

3.3 Konstruktionen mit Zirkel und Lineal

3.20. Bemerkung

Wir wollen im Folgenden untersuchen, welche **Konstruktionen** in der Ebene $\mathbb{C}$ nur mit Hilfe von **Zirkel** und **Lineal** möglich sind.

Erlaubt sind die folgenden Konstruktionen:

1. Zu zwei bereits konstruierten Punkten $P, Q \in \mathbb{C},\ P \neq Q$, die **Gerade** $G(P, Q)$ durch P und Q.
2. Zu zwei bereits konstruierten Punkten $P, Q \in \mathbb{C},\ P \neq Q$, den **Kreis** $K(P, Q)$ mit Mittelpunkt P durch Q.
3. Konstruktion neuer Punkte durch **Schnitte** von zwei Geraden, zwei Kreisen oder einer Geraden mit einem Kreis. ◊

3.21. Definition

Sei $M \subseteq \mathbb{C}$. Dann ist Kon(M) die Menge aller aus M konstruierbaren Punkte, d.h. aller $z \in \mathbb{C}$, zu denen es eine endliche Folge $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \mathbb{C}$ gibt mit $z \in M_n$ und M_ν entsteht aus $M_{\nu-1}$ durch einen elementaren Konstruktionsschritt ($\nu = 1, ..., n$), d.h. $M_\nu = M_{\nu-1} \cup \{x, y\}$.

3.22. Bemerkung

Seien $0, 1 \in M \subseteq \mathbb{C}$. Dann gelten:

1. Kon(M) ist ein Oberkörper von $\mathbb{Q}(M \cup \overline{M})$. Insbesondere ist $\mathbb{Q}$ ist aus $\{0, 1\}$ konstruierbar.
2. Ist $a \in \mathbb{C}$ konstruierbar, dann liegt auch $\sqrt{a}$ in Kon(M). ◊

3.23. Lemma

Sei L ein Unterkörper von $\mathbb{C}$ mit $L = \overline{L}$ und $i \in L$ und sei $z \in \mathbb{C}$ beliebig.

Dann gilt: Ist $z \in L$ konstruierbar, so gibt es ein $u \in L \cap \mathbb{R}$ mit $z \in L(\sqrt{u})$.

Beweis.

Gilt $z = a + ib \in \mathbb{C}$ für gewisse $a, b \in \mathbb{R}$, dann sind $a = \frac{1}{2}(z + \overline{z})$ und $b = \frac{i}{2}(z - \overline{z})$, d.h. für jedes konstruierbare $z \in \mathbb{C}$ sind auch Re(z) und Im(z) konstruierbar.

1. Schnitt zweier Geraden: Gegeben seien bereits konstruierte Punkte $p_1,\ q_1,\ p_2$ und $q_2 \in L$ mit $p_1 \neq q_1$ und $p_2 \neq q_2$. Dann definieren (p_1, q_1) und (p_2, q_2) zwei Geraden $G_1 = G(p_1, q_1)$ und $G_2 = G(p_2, q_2)$ in $\mathbb{C}$, die sich durch $g_1,\ g_2 : \mathbb{R} \to \mathbb{C}$ mit $g_1(\lambda) = p_1 + \lambda q_1$ und $g_2(\mu) = p_2 + \mu q_2$ parametrisieren lassen. Schneiden sich $G_1,\ G_2$ in einem Punkt $z \in \mathbb{C}$, so existieren $\lambda, \mu \in \mathbb{R}$ mit $z = g_1(\lambda) = g_2(\mu)$. Die Parameter λ und μ sind also Lösungen eines inhomogenen linearen Gleichungssystems über $L \cap \mathbb{R}$, bestehend aus zwei Gleichungen, mit Koeffizienten Re(p_i), Im(p_i), Re(q_i), Im(q_i) $(i = 1, 2)$. Damit liegt z in L, setze also $u = 1$.

2. Schnitt einer Geraden mit einem Kreis: Seien $p_1,\ p_2,\ q_1$ und q_2 bereits konstruiert mit $p_1 \neq p_2$ und $q_1 \neq q_2$. Sei z ein Schnittpunkt der Geraden $G(p_1, p_2)$ mit dem Kreis $K(q_1, q_2)$, dann existiert ein $\lambda \in \mathbb{R}$ mit
$$p_1 + \lambda p_2 = z \qquad \text{und} \qquad |z - q_1|^2 = |q_2 - q_1|^2.$$
Einsetzen von z in die zweite Gleichung ergibt: λ löst
$$\begin{aligned} & (\mathrm{Re}(p_1) + i\mathrm{Im}(p_1) + \lambda\mathrm{Re}(p_2) + i\lambda\mathrm{Im}(p_2) - \mathrm{Re}(q_1) - i\mathrm{Im}(q_1))^2 \\ = \ & (\mathrm{Re}(q_2) + i\mathrm{Im}(q_2) - \mathrm{Re}(q_1) - i\mathrm{Im}(q_2))^2, \end{aligned}$$
d.h. Lösung des quadrartischen Systems $\gamma_0 + \gamma_1\lambda + \gamma_2\lambda^2 = 0$, wobei die Koeffizienten $\gamma_0,\ \gamma_1$ und γ_2 gegeben sind durch
$$\begin{aligned} & ((\mathrm{Re}(p_1) - \mathrm{Re}(q_1)) + i(\mathrm{Im}(p_1) - \mathrm{Im}(q_1)))^2 - ((\mathrm{Re}(q_2) - \mathrm{Re}(q_1)) + i(\mathrm{Im}(q_2) - \mathrm{Im}(q_1)))^2 \\ & +2(\mathrm{Re}(p_2) + i\mathrm{Im}(p_2))((\mathrm{Re}(p_1) - \mathrm{Re}(q_1)) + i(\mathrm{Im}(p_1) - \mathrm{Im}(q_1)))\lambda + (\mathrm{Re}(p_2) + i\mathrm{Im}(p_2))^2\lambda^2 = 0. \end{aligned}$$
Definiere u also als die Diskriminante $u := \gamma_1^2 - 4\gamma_0\gamma_2$, dann ist $z \in L(\sqrt{u})$.

3. Seien $p_1,\ p_2,\ q_1$ und q_2 bereits konstruiert und z ein Schnittpunkt von $K(p_1, p_2)$ mit $K(q_1, q_2)$, d.h. es gelten
$$|z - p_1|^2 = |p_2 - p_1|^2 \qquad \text{und} \qquad |z - q_1|^2 = |q_2 - q_1|^2.$$
Dies liefert für $x := \mathrm{Re}(z)$ und $y := \mathrm{Im}(z)$ das nichtlineare Gleichungssystem
$$\left\{ \begin{array}{rcl} x^2 + y^2 + \gamma_1 x + \gamma_2 y + \lambda & = & 0 \\ x^2 + y^2 + \delta_1 x + \delta_2 y + \mu & = & 0 \end{array} \right.$$
für gewisse Koeffizienten $\gamma_1,\ \gamma_2,\ \delta_1,\ \delta_2,\ \lambda,\ \mu \in L$. Differenz der beiden Gleichungen ergibt ein inhomogenes lineares Gleichungssystem. Setze also wieder $u = 1$. □

3.24. Satz (Descartes)

Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Dann sind äquivalent:

1. z ist aus M elementar konstruierbar.
2. Es gibt eine Kette von Zwischenkörpern $\mathbb{Q}(M \cup \overline{M}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m \subseteq \mathbb{C}$ mit $z \in L_m$ und $[L_\nu : L_{\nu-1}] = 2$ für alle $\nu \in \{1, ..., m\}$.

Beweis.

1. (1) $\Rightarrow$ (2): Es existiere eine Kette von Konstruktionsschritten $M = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m \subseteq \mathbb{C}$ mit $z \in M_m$, $M_\nu = M_{\nu-1} \cup \{z_\nu, z'_\nu\}$. Setze $L_0 := \mathbb{Q}(M \cup \overline{M})$ und $L_1 := L_0(i)$. Dann gilt $L_1 = \overline{L_1}$ und es gibt $u_1 \in L_1 \cap \mathbb{R}$ mit $z_1, z'_1 \in L_1(\sqrt{u_1})$. Sezte $L_2 := L_1(\sqrt{u_1})$, also $M_1 \subseteq L_2$ und $L_2 = \overline{L_2}$ ... u.s.w. bis L_{m+1} mit $M_m \subseteq L_{m+1}$.
2. (2) $\Rightarrow$ (1). Wir zeigen per Induktion über ν, dass $L_\nu \subseteq \mathrm{Kon}(M)$ für alle $\nu = 1, ..., m$. Der Fall $\nu = 0$ ist klar: $L_0 \subseteq \mathrm{Kon}(M)$. Gelte die Behauptung also für $0, ..., \nu - 1$. Sei $L_{\nu-1} \subseteq \mathrm{Kon}(M)$. Es gilt $L_\nu = L_{\nu-1}(x)$ für ein $x \in L_\nu \backslash L_{\nu-1}$. Dies ist eine endliche Erweiterung, d.h. x ist algebraisch über $L_{\nu-1}$. x muss Nullstelle eines quadratischen Polynoms sein, d.h. es gibt $a, b \in L_{\nu-1}$ mit $x^2 + ax + b = 0$, also $x = -\frac{a}{2} \pm \frac{1}{2}\sqrt{a^2 - 4b} \in \mathrm{Kon}(M)$, da $\mathrm{Kon}(M)$ abgeschlossen ist unter Körperoperationen und Wurzelziehen. Weiter $L_\nu = L_{\nu-1} + L_{\nu-1}x \subseteq \mathrm{Kon}(M)$, da $x \in \mathrm{Kon}(M)$. Also $z \in L_m \subseteq \mathrm{Kon}(M)$. □

3.25. Korollar

Seien $M \subseteq \mathbb{C}$ mit $0, 1 \in M$ und $L = \mathbb{Q}(M \cup \overline{M})$. Dann gilt für alle $z \in \mathrm{Kon}(M)$: $[L(z) : L]$ ist eine Zweierpotenz.

Beweis.

Seien $L \subseteq L_1 \subseteq \cdots \subseteq L_m$ und $z \in L_m$. Dann sind $L(z) \subseteq L_m$ und $[L_m : L] = 2^m$, also $L \subseteq L(z) \subseteq L_m$. Die Gradformel liefert $2^m = [L_m : L] = [L_m : L(z)][L(z) : L]$, d.h. $[L(z) : L] = 2^\nu$ mit einem $\nu \leq m$. □

3.26. Bemerkung (Anwendungen aus der euklidischen Geometrie)

1. **Quadratur des Kreises.** Gesucht ist ein Quadrat mit Kantenlänge $\sqrt{\pi}$. Wäre $\sqrt{\pi}$ konstruierbar aus $\{0, 1\}$, so wäre $\sqrt{\pi}$ algebraisch über $\mathbb{Q}$, ein Widerspruch.
2. **Delisches Problem.** Gesucht ist ein Würfel mit Kantenlänge $\sqrt[3]{2}$. Wäre $\sqrt[3]{2}$ aus $\{0, 1\}$ konstruierbar, dann $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2^\nu$. Das ist unmöglich, da $\deg \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = \deg(X^3 - 2) = 3$.
3. **Winkeldreiteilung.** Gegeben sei der Winkel $\alpha = \frac{\pi}{3}$, dann ist $\cos\frac{\alpha}{3}$ eine Nullstelle des normierten Polynoms $f(X) = X^3 - \frac{3}{4}X - \frac{1}{8}$. f ist irreduzibel über $\mathbb{Q}$, denn mit der Substitution $X = \frac{1}{2}(1 + Z)$ folgt $f(X) = Z^3 + 3Z - 3$; dieses ist irreduzibel nach Eisenstein. Also ist $f = \mathrm{Irr}(\cos\frac{\alpha}{3}, \mathbb{Q})$. Wegen $\deg \mathrm{Irr}(\cos\frac{\alpha}{3}, \mathbb{Q}) = 3 \neq 2^\nu = [\mathbb{Q}[\cos\frac{\alpha}{3}] : \mathbb{Q}]$ für alle $\nu \in \mathbb{N}$, ist die Dreiteilung des 60°-Winkels unmöglich.
4. **Konstruktion eines regelmäßiges p-Ecks.** Sei p prim. Die Ecken e_1, e_2, ..., e_p eines regelmäßigen p-Ecks lassen sich darstellen als $e_1 = \exp\frac{2\pi i}{p}$, $e_2 = \exp\frac{4\pi i}{p}$, ..., $e_p = \exp\frac{2p\pi i}{p} = 1$. Notwendige Bedingung für $\exp\frac{2\pi i}{p} \in \mathrm{Kon}(\{0, 1\})$ ist $\deg \mathrm{Irr}(\exp\frac{2\pi i}{p}, \mathbb{Q}) = 2^m$ für ein $m \in \mathbb{N}$. Nun ist $\exp\frac{2\pi i}{p}$ eine Nullstelle des Polynoms $f(X) = X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1) = (X-1)\Phi_p(X)$ mit p-tem Kreisteilungspolynom Φ_p. Dieses ist irreduzibel über $\mathbb{Z}$, also auch über $\mathbb{Q}$, d.h. $\mathrm{Irr}(\exp\frac{2\pi i}{p}, \mathbb{Q}) = \Phi_p(X)$, also $p - 1 = 2^m$. Als unmittelbare Konsequenz erhalten wir: Das 7-Eck und das 11-Eck lassen sich nicht konstruieren.

   Weiter gilt $m = 2^n$, denn sei $t \neq 1$ ungerade mit $m = st$. Dann ist

   $$2^m + 1 = (2^s)^t + 1 = (2^s + 1)((2^s)^{t-1} - (2^s)^{t-1} + \cdots + 1),$$

   ein Widerspruch. Also ist die Bedingung $p = 2^{2^n} + 1$ notwendig für die Konstruierbarkeit. Solche p heißen Fermat-Primzahlen. Wir zeigen später: Die Bedingung ist auch hinreichend, d.h. genau dann ist das regelmäßige p-Eck konstruierbar, wenn p eine Fermat-Primzahl ist. Die einzigen derzeit bekannten Fermat-Primzahlen sind im übrigen 3, 5, 17 und 65537. ◊

3.4 Der Zerfällungskörper

3.27. Wiederholung

Seien $k \subseteq K$ eine Körpererweiterung und $f \in k[X]$. Dann gelten:

1. Genau dann ist $a \in K$ eine Nullstelle von f, wenn $(X-a)$ ein Teiler von f in $K[X]$ ist.
2. f hat höchstens $\deg f$ viele Nullstellen in K. ◊

3.28. Definition

Ein $f \in k[X]$ zerfällt in K, falls es $a_1, ..., a_n \in K$ und $b \in k$ gibt mit

$$f(X) = b\prod_{i=1}^{n}(X - a_i).$$

K heißt der Zerfällungskörper von f über k (in Zeichen: $K = \mathrm{Zfk}(f,k)$), falls es $a_1, ..., a_n \in K$ und $b \in k$ gibt mit

$$f(X) = b\prod_{i=1}^{n}(X - a_i) \qquad \text{und} \qquad K = k(a_1, ..., a_n).$$

3.29. Beispiel

1. $\mathbb{C}$ ist der Zerfällungskörper von X^2+1 über $\mathbb{R}$: Es gilt $\mathbb{C} = \mathbb{R}(i) = \mathbb{R} \oplus i\mathbb{R}$ als Vektorraum.
2. $\mathbb{Q}(\sqrt{2})$ ist der Zerfällungskörper von X^2-2 über $\mathbb{Q}$, denn es gelten $X^2-2 = (X+\sqrt{2})(X-\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q}(\sqrt{2})$.
3. $\mathbb{Q}(\sqrt[3]{2})$ ist nicht der Zerfällungskörper von X^3-2, denn $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ und X^3-2 lässt sich zerlegen in $X^3-2 = (X-\sqrt[3]{2})(X^2 + X\sqrt[3]{2} + \sqrt[3]{4})$, wobei der letztere Faktor keine reellen Nullstellen hat.
4. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ ist der Zerfällungskörper von X^3-2, denn die Nullstellen von $X^2 + X\sqrt[3]{2} + \sqrt[3]{4}$ sind $-\frac{1}{2}\sqrt[3]{2} \pm \frac{1}{2}\sqrt[3]{2}\sqrt{-3}$. Es gilt $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!$. ◊

3.30. Bemerkung

Allgemein gilt: $[K : k] \leq n!$, falls $n = \deg f$ und K Zerfällungskörper von f über k. ◊

3.31. Satz

Sei $f \in k[X]$. Dann gibt es $K \supseteq k$ mit K Zerfällungskörper von f über k.

Beweis.

Œ sei f normiert und es gelte $f \notin k$. Schreibe $f = f_1 \cdots f_m$ mit $f_i \in k[x]$ irreduzibel und $n = \deg f$, insbesondere $m \leq n$.

Wir führen eine Induktion über $n-m$: Gelte zunächst $n-m = 0$, dann $n = m$, also $f_i = X - a_i \in k[X]$, also ist k der Zerfällungskörper von f, d.h. $\deg(f_i) = 1$ und $k = K$, womit der Induktionsanfang gemacht wäre.

Sei nun $n - m > 0$, etwa $\deg(f_1) > 1$. Da f_1 irredizibel in einem Hauptidealring, ist $(f_1)_{k[X]}$ prim in einem Hauptidealring, d.h. (f_1) ist maximal und damit $k[X]/(f_1) =: L$ ein Körper. f_1 hat eine Nullstelle in L, nämlich $X + (f_1) =: \overline{x}$, denn $\overline{f_1(X)} = f_1(\overline{x})$; da $f_1(X) \in (f_1)$, folgt $f_1(\overline{x}) = 0$ in L. Also ist $k \subseteq L$ und es gibt ein $a \in L$ mit $f_1(a) = 0$. Damit ist $f_1(X) = (X-a)g_1(X)$ für ein $g_1 \in L[X]$. Über L gilt also: $f = (X-a)h_2 \cdots h_{\widetilde{m}}$ mit $m < \widetilde{m}$. Wegen $n - \widetilde{m} < n - m$, gibt es nach Induktionsvoraussetzung ein Teilkörper $K \supseteq L$, so dass K der Zerfällungskörper von f über L ist, d.h. $f = \prod(X - a_i)$ und $K = L(a_1, ..., a_n)$, Œ $a_1 = a$. Also ist $K = f(a_1)(a_2, ..., a_n)$, d.h. K ist auch der Zerfällungskörper von f über k. Weiter gilt $k(a_1) = L$, denn $L = k[X] \mid (f_1) = k[\overline{x}] = k[a] = k(a)$, da $f(a) = 0$, d.h. a ist algebraisch über k. □

3.32. Bemerkung

Sei K ein Zerfällungskörper über k, dann gilt $[K : k] < \infty$, denn $K = k(a_1, ..., a_n)$ und alle a_i sind algebraisch über k, also $[K : k] \leq n!$. $\Diamond$

3.33. Lemma

Sei $\varphi : k \to k'$ ein Körperisomorphismus. Dann gibt es einen eindeutig bestimmten Ringisomorphismus $\Phi : k[X] \to k'[X']$ mit $\Phi_{|k} = \varphi$ und $\Phi(X) = X'$.

Beweis.

1. Eindeutigkeit: Sei Ψ ein beliebiger Ringhomomorphismus mit $\Psi_{|k} = \varphi$ und $\Psi(X) = X'$. Dann gilt:
$$\begin{aligned}\Psi(a_0 + \cdots + a_n X^n) &= \Psi(a_0) + \cdots + \Psi(a_n)\Psi^n(X) \\ &= \varphi(a_0) + \cdots + \varphi(a_n)(X')^n \\ &= \Phi(a_0 + \cdots + a_n X^n).\end{aligned}$$

2. Existenz: Setze $\Phi(a_0 + \cdots + a_n X^n) := \varphi(a_0) + \cdots + \varphi(a_n)(X')^n$. Dies definiert einen Ringhomomorphismus. Φ ist surjektiv, da φ surjektiv. Außerdem ist Φ injektiv, denn sei $\Phi(a_0 + \cdots + a_n X^n) = 0$, dann $\varphi(a_0) + \cdots + \varphi(a_n)(X')^n = 0$, also sind alle $\varphi(a_i) = 0$ und damit alle $a_i = 0$, da φ injektiv ist. Also ist auch $\mathrm{Kern}(\Phi) = 0$. $\square$

3.34. Lemma

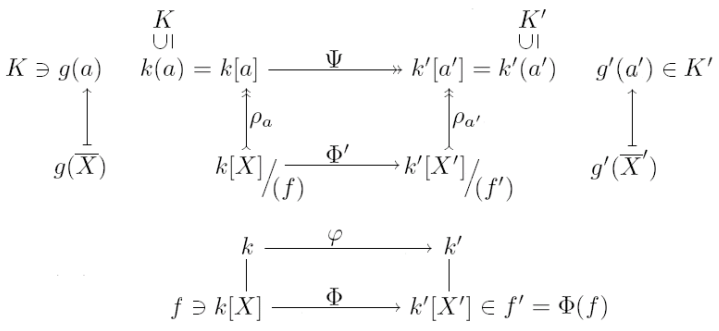
Seien $\varphi : k \to k'$ ein surjektiver Körperhomomorphismus und $\Phi : k[X] \to k'[X']$ seine Fortsetzung mit $\Phi(X) = X'$. Weiter seien $K \supseteq k$ und $K' \supseteq k'$ Körpererweiterungen, $a \in K$ und $f = \mathrm{Irr}(a, k)$.

Dann stimmt die Anzahl der Fortsetzungen $\Psi : k(a) \to K'$ mit $\Psi_{|k} = \varphi$ mit der Anzahl der verschiedenen Nullstellen von $\Phi(f)$ in K überein.

Beweis.

Seien $\Psi : k(a) \to K'$ ein Körperisomorphismus und $\Phi : k[X] \to k'[X']$ seine Fortsetzung. Dann ist $\Psi(a)$ eine Nullstelle von $\Phi(f)$:
$$\begin{aligned}0 &= \Psi(0) \\ &= \Psi(f(a)) \\ &= \Psi(a_0 + \cdots + a_{n-1}a^{n-1} + a^n) \\ &= \varphi(a_0) + \cdots + \varphi(a_{n-1})\Psi^{n-1}(a) + \Psi^n(a) \\ &= \Phi(f)(\Psi(a)),\end{aligned}$$

Sei nun $a' \in K'$ eine Nullstelle von $\Phi(f)$, dann definiert
$$\Psi(b_0 + \cdots + b_{n-1}a^{n-1}) := \varphi(b_0) + \cdots + \varphi(b_{n-1})(a')^{n-1}$$
eine eindeutige Fortsetzung von φ. Dabei sind Eindeutigkeit und additive Verträglichkeit klar. Zur multiplikativen Verträglichkeit. Seien hierfür $f := \mathrm{Irr}(a, k)$ und $f' := \mathrm{Irr}(a', k')$. Betrachte das Diagramm



ρ_a und $\rho_{a'}$ sind injektive Ringhomomorphismen, also multiplikativ verträglich, ebenso Φ'. Dann ist aber auch $\Psi = \rho_{a'} \circ \Phi' \circ \rho_a^{-1}$ einer.

Also gibt es mindestens so viele Einbettungen wie Nullstellen. Da die Einbettung für eine feste Nullstelle nach Lemma 3.33 eindeutig bestimmt ist, folgt die Behauptung. □

3.35. Korollar

Seien $k \subseteq K$ mit $a, a' \in K$ und $\mathrm{Irr}(a,k) = \mathrm{Irr}(a',k)$.

Dann gibt es genau einen Isomorphismus $\Psi : k(a) \to k(a')$ mit $\Psi_{|k} = \mathrm{id}$ und $\Psi(a) = a'$.

3.36. Satz (Fortsetzungssatz)

Seien $k \subseteq K$ und $k' \subseteq K'$ Körpererweiterungen, $\varphi : k \to k'$ ein Körperepimorphismus und Φ eine Fortsetzung von φ auf $k[X]$. Weiter seien $f \in k[X]$ ein Polynom, K ein Zerfällungskörper von f und K' ein Zerfällungskörper von $f' = \Phi(f)$.

Dann gibt es eine surjektive Fortsetzung $\Psi : K \to K'$ von φ und die Anzahl dieser Fortsetzungen von φ ist kleiner oder gleich dem Grad der Körpererweiterung $[K : k]$. Gleichheit gilt, falls f' lauter verschiedene Nullstellen in K' hat.

Beweis.

Œ sei f normiert. Wir führen eine Induktion über den Erweiterungsgrad $[K : k]$.

1. Gelte $[K : k] = 1$. Dann zerfällt f in $k[X]$, d.h. f' zerfällt in $k'[X]$, also $K' = k'$.
2. Sei nun $[K : k] > 1$. Es gibt einen irreduziblen Teiler g von f in $k[X]$ mit $\deg g > 1$. Seien $a_1, ..., a_n \in K$ und $b_1, ..., b_n \in K'$ mit

$$f = \prod_{i=1}^{n}(X - a_i), \quad g = \prod_{i=1}^{m}(X - a_i), \quad f' := \Phi(f) = \prod_{i=1}^{n}(X - b_i) \quad \text{und} \quad \Phi(g) = \prod_{i=1}^{m}(X - b_i)$$

   mit $1 < m \leq n$. Seien $\Psi_j : k(a_1) \to k'$ $(1 \leq j \leq r)$ mit r gleich der Anzahl der Nullstellen von g' in K', d.h. $r \leq m$. Es gilt $r = m$ genau dann, wenn alle $b_1, ..., b_m$ paarweise verschieden sind. Setze $L := k(a_1)$. Da K der Zerfällungskörper von f über k, ist er auch der über L, denn Zerfällungskörper entstehen ja gerade durch Adjunktion der Nullstellen, und K' ist der Zerfällungskörper von f' über $\Psi_j(L)$.

   Nach der Gradformel gilt $[K : L] = \frac{[K:k]}{[L:k]} = \frac{[K:k]}{m} < [K : k]$, da $m > 1$, und mit der Induktionsvorausstzung folgt:

   a) Ψ_j hat eine Fortsetzung auf K.

   b) Die Anzahl der Fortsetzungen ist kleiner oder gleich $[K : L]$.

   c) Gleichheit gilt, falls $f' = \Phi(f)$ lauter verschiedene Nullstellen hat.

   Mit Lemma 3.34 gibt es eine Fortsetzung $\Psi : K \to K'$ von φ. Dann ist $\Psi_{|L} = \Psi_j$ für ein $j \leq r$, also ist die Anzahl der Fortsetzungen von φ auf K kleiner oder gleich $r \cdot [K : L] \leq m \cdot [K : L] = [K : k]$. Falls f' weiter lauter verschiedene Nullstellen in K' hat, so gilt $r = m$ und die Anzahl dieser Fortsetzungen ist gleich $[K : k]$. □

3.37. Korollar (Zerfällungskörper)

Zu jedem Körper k und jedem $f \in k[X]$ gibt es bis auf Isomorphie über k (d.h. die Einschränkung auf k ist die Identität) nur einen Zerfällungskörper.

3.5 Der algebraische Abschluss

3.38. Definition

Ein Körper K heißt algebraisch abgeschlossen, falls über K jedes Polynom $f \in K[X]$ zerfällt.

K heißt der algebraische Abschluss von k, falls K algebraisch abgeschlossen und die Körpererweiterung $K|k$ algebraisch ist.

3.39. Beispiele

1. $\mathbb{C}$ ist algebraisch abgeschlossen **(Fundamentalsatz der Algebra)**.
2. $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$: $\mathbb{C} = \mathbb{R}(i)$.
3. $\mathbb{C}$ ist kein algebraischer Abschluss von $\mathbb{Q}$, denn π ist über $\mathbb{Q}$ transzendent. $\Diamond$

3.40. Satz (Algebraischer Abschluss)

Jeder Körper K hat bis auf Isomorphie genau einen algebraischen Abschluss.

Beweis.

1. Eindeutigkeit: Seien $K|k$ und $K'|k'$ algebraische Erweiterungen, K, K' algebraisch abgeschlossen und $\varphi : k \to k'$ ein Isomorphismus. Betrachte

$$\mathcal{M} := \{\varphi_1 : k_1 \to k_1' \text{ surjektiv} \mid k \subseteq k_1 \subseteq K,\ k' \subseteq k_1' \subseteq K' \text{ und } \varphi_{1|k} = \varphi\}.$$

Wir definieren eine Relation $\preccurlyeq$ auf $\mathcal{M}$ durch

$$\varphi_1 \preccurlyeq \varphi_2 \qquad :\Longleftrightarrow \qquad k_1 \subseteq k_2,\ k_1' \subseteq k_2' \text{ und } \varphi_{2|k_1} = \varphi_1.$$

Jede aufsteigende Kette $(\varphi_i)_{i\in I}$ mit $\varphi_i : k_i \to k_i'$ besitzt eine obere Schranke φ_I in $\mathcal{M}$, nämlich $\varphi_I : \bigcup\{k_i \mid i \in I\} \to \bigcup\{k_i' \mid i \in I\}$ mit $\varphi_I(a) := \varphi_i(a)$, falls $a \in k_i$. Beachte: φ_I ist ein wohldefinierter Epimorphismus, $\bigcup k_i$ ist ein Teilkörper von K und $\bigcup k_i'$ ist ein Teilkörper von K'. Also ist $\varphi_I \in \mathcal{M}$. Nach Zorns Lemma gibt es ein maximales $\varphi_m : l_m \to k_m'$. Wir zeigen: $k_m = K$ und $k_m' = K'$.

Falls $k_m \subsetneq K$, gibt es $a \in K\backslash k_m$. Dann ist $f = \mathrm{Irr}(a, k_m)$ und es existiert ein $a' \in K'$ mit $f(a') = 0$ (genauer $\Phi_m(f)(a') = 0$). Dann gibt es einen Isomorphismus $\Psi : k_m(a) \to k_m'(a')$, also war φ_m nicht maximal. Analog erhalten wir zu $K' \neq k_m'$ ein $a' \in K'\backslash k_m'$; Korollar 3.37 liefert $\Psi^{-1} : k_m'(a') \to k_m(a)$ im Widerspruch zur Maximalität von φ_m.

2. Existenz: Wähle zu jedem $f \in k[X]\backslash k$ eine Unbestimmte X_f und betrachte den Polynomring (Integritätsbereich) $R = k[X_f \mid f \in k[X]\backslash k]$; für unendliches I definieren wir

$$k[X_i \mid i \in I] := \bigcup_{\substack{E\subseteq I \\ E \text{ endl.}}} k[X_i \mid i \in E].$$

Sei A ein Ideal in R das von $\{f(X_f) \mid f \in k[X]\backslash k\}$ erzeugt werde. Wähle mit Zorns Lemma ein maximales Ideal $M \supseteq A$. Dazu müssen wir zeigen, dass A echt ist, d.h. 1 nicht in A liegt. Wäre $1 \in A$, dann $1 = \sum g_i f_i(X_{f_i})$ mit $g_1, ..., g_n \in R$. Die g_i sind Polynome, etwa in $X_{f_1}, ..., X_{f_n},\ X_{f_{n+1}}, ..., X_{f_m}$. Seien $\alpha_1, ..., \alpha_n$ Nullstellen von $f_1, ..., f_n$ mit $\alpha_1, ..., \alpha_n$ aus dem Zerfällungskörper von $f = f_1 \cdots f_n$ über k. Die Einsetzung α_i in $X_{f_i},\ 1 \le i \le n$ und 0 in $X_{f_j},\ n < j \le m$ ergibt:

$$1 = \sum_{i=1}^{n} g_i(\alpha_1, ..., \alpha_n, 0, ..., 0) f_i(\alpha_i) = 0,$$

ein Widerspruch.

Da M ein maximales Ideal ist, ist $K' := R/M$ ein Körper. Betrachte den Restklassenepimorphismus $\varphi : R \to R/M =: K',\ g \mapsto \overline{g} = g + M$. Da $\varphi_{|k} : k \to R/M$ injektiv ist, können wir $a \in k$ mit $\overline{a}$ identifizieren. Dann ist

$$\overline{g(X_{f_1}, ..., X_{f_m})} = \overline{g}(\overline{X}_{f_1}, ..., \overline{X}_{f_m}) = g(\overline{X}_{f_1}, ..., \overline{X}_{f_m})$$

wegen der Homomorphie von g und Identifikation; da $f(X_f) \in M$, gilt $0 = \overline{f(X_f)} = f(\overline{X}_f)$, d.h. $\overline{X}_f$ ist eine Nullstelle von f in K'. Setze $K = \{a \in K' \mid a \text{ algebraisch über } k\}$, dann ist K algebraisch über k. Wir haben damit gezeigt: Zu k gibt es einen algebraischen Oberkörper K, in dem jedes $f \in k[X]\backslash k$ eine Nullstelle hat.

Iteriere diesen Prozess: Zu K_n gibt es eine algebraische Erweiterung K_{n+1}. Dort hat jedes Polynom $f \in K_n[X]\backslash K_n$ eine Nullstelle. Zeige: Der Körper $\mathcal{K} := \bigcup_{n\in\mathbb{N}} K_n$ ist algebraisch abgeschlossen.

Sei $f \in \mathcal{K}[X]\backslash\mathcal{K}$ mit Darstellung $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. $a_i \in \mathcal{K}$, Œ alle $a_i \in K_n$, also hat f Nullstellen in $K_{n+1} \subseteq \mathcal{K}$. □

3.41. BEMERKUNG

Alternativ hätte man auch über einen Koeffizientenvergleich argumentieren können: Aus

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{i=1}^{n}(X - \alpha_i)$$

folgt:

$$\begin{array}{rcll} -a_{n-1} & = & (\alpha_1 + \alpha_2 + \cdots + \alpha_n) & =: \; s_1(\alpha_1, ..., \alpha_n) \\ a_{n-2} & = & (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \cdots + \alpha_{n-1}\alpha_n) & =: \; s_2(\alpha_1, ..., \alpha_n) \\ -a_{n-3} & = & (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \cdots + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n) & =: \; s_3(\alpha_1, ..., \alpha_n) \\ & \vdots & & \vdots \\ (-1)^n a_0 & = & (\alpha_1\alpha_2 \cdots \alpha_n) & =: \; s_n(\alpha_1, ..., \alpha_n). \end{array}$$

Definiere $R = k[X_{f,1}, ..., X_{f,d} \mid f \in k[X]\backslash K,\ d = \deg f]$. Sei A das von

$$\{s_i(X_{f,1}, ..., X_{f,d}) \mid a_{n-i} \text{ teilt } f = X^d + a_{d-1}X^{d-1} + \cdots + a_0,\ 1 \le i \le d,\ d = \deg f,\ f \in k[X]\backslash k\}$$

erzeugte R-Ideal und M sei maximal mit $A \subseteq M$, dann ist $K' := R/M$ ein Körper. Also ist

$$s_i(\overline{X}_{f,1}, ..., \overline{X}_{f,d}) = (\pm)a_{d-1} \qquad \Longrightarrow \qquad f = X^d + \cdots + a_0 = \prod_{i=1}^{n}(X - \overline{X}_{f,i})$$

mit $\overline{X}_{f,i} \in K'$, d.h. in K' zerfällt jedes Polynom $f \in k[X]\backslash k$. Konstruiere aus K' ein $\mathcal{K}$ wie oben, dann zerfällt jedes $f \in k[X]\backslash k$ in einem algebraischen Oberkörper $\mathcal{K}$. ◊

3.42. SATZ

Jeder algebraisch abgeschlossene Körper ist unendlich.

BEWEIS.

Sei $K = \{a_0, ..., a_n\}$ algebraisch abgeschlossen. Setze $f(X) := 1 + \prod\{(X - a_i) \mid i = 0, ..., n\} \in K[X]$. Dann hat f eine Nullstelle in K, etwa a_i, also ist $0 = f(a_i) = 1$, ein Widerspruch. □

3.6 Separable Polynome

3.43. WIEDERHOLUNG

Seien $k \subseteq K$ Körper, $a \in K$ und $f \in k[X]$ zerfalle in K.

1. $\mu(f, a) := \max\{n \in \mathbb{N}_0 \mid (X - a)^n \text{ teilt } f \text{ in } K[X]\}$ heißt die Vielfachheit der Nullstelle a von f.
2. Ist $f = b(X - a_1)^{\mu_1} \cdots (X - a_m)^{\mu_m}$ mit $b \in k$ und $a_i \in K$ paarweise verschieden, $i = 1, ..., m$, dann gilt $\mu_i = \mu(f, a_i)$.
3. Die μ_i sind unabhängig von der Wahl des Körpers K, in dem f zerfällt, denn der Zerfällungskörper von f ist bis auf Isomorphie eindeutig bestimmt. ◊

3.44. Definition

Sei $f \in k[X]\backslash k$. Dann heißt f separabel, falls jeder irreduzible Faktor von f in seinem Zerfällungskörper nur einfache Nullstellen hat.

Seien $k \subseteq K$ Körper und $a \in K$ algebraisch über k. Dann heißt a separabel über k, falls $\mathrm{Irr}(a,k)$ separabel ist.

3.45. Beispiel

$(X-a)$ und $(X-a)^2$ sind separabel. ◊

3.46. Definition

Sei R ein Ring. Die Abbildung

$$\mathrm{D} : R[X] \to R[X], \qquad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=1}^{n} i a_i X^{i-1}$$

heißt die formale Derivation oder formale Differenziation auf $R[X]$.

3.47. Bemerkung

Für alle $a, b \in R$ und alle $f, g \in R[X]$ gelten:

1. $\mathrm{D}(af+bg) = a\mathrm{D}(f) + b\mathrm{D}(g)$, d.h. D ist linear.
2. $\mathrm{D}(fg) = f\mathrm{D}(g) + \mathrm{D}(f)g$. ◊

3.48. Bemerkung

Wir argumentieren nun stets im Zerfällungskörper über k. ◊

3.49. Satz

Ein normiertes $f \in k[X]\backslash k$ hat nur einfache Nullstellen $\Leftrightarrow (f, \mathrm{D}(f)) = (1)$.

Beweis.

Habe f die Darstellung $f = \prod_{i=1}^{n} (X-a_i)^{\nu_i}$ mit a_i paarweise verschieden, $i = 1, ..., n$.

$\Rightarrow$ Seien alle $\mu_i = 1$. Dann ist $\mathrm{D}(f) = \sum_j \prod_{i \neq j} (X - a_i)$.

Sei $j \neq j_0$, dann gilt $(X-a_{j_0}) \mid \prod_{i \neq j} (X-a_i)$, da $(X-a_{j_0})$ ein Faktor des Produkts ist.

Aber: $(X-a_{j_0}) \nmid \prod_{i \neq j_0}$, d.h. $(X-a_{j_0}) \nmid \mathrm{D}(f)$, d.h. $\{f, \mathrm{D}(f)\}$ teilerfremd, also $(f, \mathrm{D}(f)) = (1)$.

$\Leftarrow$ Es sei ein $\mu_i > 1$, etwa $\mu_1 > 1$, dann $\mathrm{D}(f) = \sum_j \mu_j (X-a_j)^{\mu_j - 1} \prod_{i \neq j} (X-a_i)^{\mu_i}$.

Dann teilt $(X-a_1)$ jeden Summanden, also auch $\mathrm{D}(f)$, d.h. $(X-a_1)$ teilt $(f, \mathrm{D}(f))$ und damit gilt $(f, \mathrm{D}(f)) \neq (1)$. □

3.50. Bemerkung

Wir definieren $a \mid (b) :\Leftrightarrow a \mid b$. Dies ist wohldefiniert, denn im Hauptidealring und Integritätsbereich ist das erzeugende Element eines Ideals bis auf Einheiten eindeutig bestimmt.

In Hauptidealringen gilt: $(a,b) = (\mathrm{ggT}(a,b))$, denn $\mathrm{ggT}(a,b) = c \Leftrightarrow (a,b) = (c)$.

3.51. Korollar

1. Sei $f \in k[X]\backslash k$ normiert und irreduzibel über $k[X]$. Dann gilt: f ist separabel $\Leftrightarrow \mathrm{D}(f) \neq 0$.
2. $\mathrm{char}(k) = 0 \Rightarrow$ jedes $f \in k[X]\backslash k$ ist separabel.

Beweis.

1. $\Rightarrow$ Sei $\mathrm{D}(f) = 0$. Dann ist $(f, \mathrm{D}(f)) = (f, 0) = (f) \neq (1)$, d.h. f ist nicht separabel.

   $\Leftarrow$ Sei $\mathrm{D}(f) \neq 0$, dann $f \nmid \mathrm{D}(f)$, da $\deg f > \deg \mathrm{D}(f)$. Dann $(f, \mathrm{D}(f)) = (1)$, da f bereits irreduzibel.

2. Falls $f \notin k$, dann ist $\mathrm{D}(f) \neq 0$. □

3.52. Lemma

Sind $k \subseteq K$ eine Körpererweiterung und $f, g \in k[X]$.

Dann gilt: $(f, g) = (1)$ in $k[X] \Leftrightarrow (f, g) = (1)$ in $K[X]$.

Beweis.

$\Rightarrow$ Sei $h_1 f + h_2 g = 1$ für gewisse $h_1, h_2 \in k[X]$. Gäbe es ein $h \in K[X] \backslash K$ mit $h \mid f$ und $h \mid g$, dann auch $h \mid (h_1 f + h_2 g) = 1$, was unmöglich ist.

$\Leftarrow$ Sei $h \in k[X]$ mit $h \mid f$ und $h \mid g$ in $k[X]$. Dann gelten die Teilbarkeitsrelationen auch in $K[X]$. □

3.53. Definition

k heißt perfekt oder vollkommen, falls jedes $f \in k[X] \backslash k$ separabel ist.

3.54. Bemerkung

Insbesondere sind alle Körper k mit $\mathrm{char}(k) = 0$ vollkommen. ◊

3.55. Lemma

Sei $\mathrm{char}(k) = p$. Dann gilt $\mathrm{D}(f) = 0 \Leftrightarrow$ es gibt $g \in k[X]$ mit $f(X) = g(X^p)$.

Beweis.

$\Rightarrow$ Habe f die Darstellung $f(X) = a_0 + a_1 X + \cdots + a_m X^m$. Falls $\mathrm{D}(f) = a_1 + 2a_2 X + \cdots + m a_m X^{m-1} = 0$, dann sind alle a_i mit $p \nmid i$ bereits 0. Also ist $f = a_0 + a_p X^p + a_{2p}(X^p)^2 + \cdots + a_{lp}(X^p)^l$. Setze $g(X) := a_0 + a_p X + a_{2p} X^2 + \cdots + a_{lp} X^l$, dann $f(X) = g(X^p)$.

$\Leftarrow$ Sei $f(X) = a_0 + a_1 X^p + \cdots + a_n (X^p)^n$, dann $\mathrm{D}(f) = a_1 p X^{p-1} + \cdots + a_n n p X^{np-1} = 0$. □

3.56. Beispiel

Seien $k = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ und $f(X) = 1 + X^2 + X^4$, dann $\mathrm{D}(f) = 2X + 4X^3 = 0$. ◊

3.57. Satz

Gelte $\dim k = p$, dann ist k vollkommen $\Leftrightarrow k = k^p = \{a^p \mid a \in k\}$.

Beweis.

$\Rightarrow$ Sei k vollkommen. Wir nehmen an, es gelte $k^p \subsetneq k$, etwa $a \in k \backslash k^p$. Betrachte $f(X) = X^p - a$. Es gilt $\mathrm{D}(f) = p X^{p-1} = 0$, da $\mathrm{char}(k) = p$. Außerdem ist f irreduzibel, denn sei $f = gh$ mit irreduziblem g und K der Zerfällungskörper von g, dann hat g in K eine Nullstelle b, d.h. $f(b) = b^p - a = 0$, also $a = b^p$ in K. Damit gilt $f(X) = X^p - b^p = (X - b)^p$ in $K[X]$, da auch $\mathrm{char}(K) = p$. Dann $g(X) = (X - b)^m$ für ein $m \in \mathbb{N}$. Da g irreduzibel in $k[X]$ und k vollkommen, folgt $m = 1$, also $g(X) = X - b \in k[X]$. Also liegt b in k und damit a in k^p, was im Widerspruch zur Annahme steht.

$\Leftarrow$ Seien φ_p der Epimorphismus $\varphi_p : k \to k,\ a \to a^p$ und $f \in k[X]$ irreduzibel. Wir zeigen: $\mathrm{D}(f) \neq 0$.

Wäre $\mathrm{D}(f) = 0$, dann $f(X) = g(X^p)$, also

$$\begin{aligned} f(X) &= a_0 + a_1X^p + a_2X^{2p} + \cdots + a_nX^{np} \\ &= b_0^p + b_1^pX^p + b_2(X^2)^p + \cdots + b_n^p(X^n)^p \\ &= (b_0 + b_1X + \cdots + b_nX^n)^p, \end{aligned}$$

d.h. f kann nicht reduzibel sein. □

3.58. Beispiel

1. Sei k endlich, etwa $\dim k = p$. Dann ist $\varphi_p : k \to k,\ aa^p$ ist ein Homomorphismus, da $(a+b)^p = a^p + b^p$ und $(ab)^p = a^pb^p$. Außerdem ist φ_p injektiv und damit auch surjektiv, da k endlich ist, d.h. φ_p ist ein Isomorphismus, also $k = k^p$, d.h. jeder endliche Körper ist vollkommen.
2. $\mathbb{F}_p(X)$ ist nicht vollkommen, denn $k \supsetneq k^p$, z.B. $X \neq (\frac{f}{g})^p$, sonst $g^pX = f^p$ und $p \mid \deg f^p,\ p \nmid \deg g^pX$, was nicht sein kann. ◊

4 Galoistheorie

4.1 Die Galoisgruppe einer Erweiterung

4.1. Definition

Sei $k \subseteq K$ eine Körpererweiterung.

$$\mathrm{Gal}(K|k) := \mathrm{Aut}(K,k) = \{\sigma : K \to K \mid \sigma \text{ ist Automorphismus mit } \forall a \in k : \sigma(a) = a\}$$

heißt die Galoisgruppe der Körpererweiterung $K|k$.

4.2. Bemerkung

Es gilt für alle $a, b \in k$ und alle $x, y \in K$:

$$\sigma(ax + by) = \sigma(a)\sigma(x) + \sigma(b)\sigma(y) = a\sigma(x) + b\sigma(y).$$

Damit gilt: Falls $\sigma \in \mathrm{Gal}(K|k)$, dann $\sigma \in \mathrm{Hom}(K,K)$, also ist σ durch seine Werte auf einer k-Basis von K schon eindeutig bestimmt. □

4.3. Beispiel

1. Sei $\sigma : \mathbb{Q} \to \mathbb{Q}$ ein Automorphismus. Dann gilt: $\sigma = \mathrm{id}$.
2. Seien $K = \mathbb{Q}(\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$ und $k = \mathbb{Q}$, dann legt $\sigma(\sqrt{2}) := -\sqrt{2}$ schon $\sigma \in \mathrm{Aut}(K,k)$ eindeutig fest.
3. Sei allgemeiner $K = k(\alpha) = k \oplus k\alpha$ mit $\mathrm{Irr}(\alpha,k) = X^2 - a$ für ein $a \in k$. Dann definiert $\sigma(\alpha) := -\alpha$ einen k-Automorphismus, denn $\alpha, -\alpha$ sind die Nullstellen von $X^2 - a$. Ein solcher Automorphismus bildet Nullstellen auf Nullstellen ab:

$$0 = \sigma(0) = \sigma(\alpha^2 - a) = (\sigma(\alpha))^2 - \sigma(a) = (\sigma(\alpha))^2 - a,$$

d.h. $\sigma(\alpha)$ ist eine Nullstelle von $X^2 - a$. ◊

Dadurch erhalten wir das folgende Lemma:

4.4. Lemma

Ist $K = k(\alpha)$ eine algebraische Erweiterung, dann ist $|\mathrm{Gal}(K|k)|$ gleich der Anzahl der verschiedenen Nullstellen von $\mathrm{Irr}(\alpha,k)$ in K.

4.5. Beispiel

1. Seien $K = \mathbb{Q}(\sqrt[3]{2})$, $k = \mathbb{Q}$, also $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$. Dann $|\mathrm{Gal}(K|k)| = 1$, denn $X^3 - 2$ hat in $\mathbb{R}$ nur eine Nullstelle.

2. Seien K endlich mit $\mathrm{char}(K) = p$ und $k = \mathbb{F}_p$. Dann gilt: $\sigma_p : K \to K,\ x \mapsto x^p \in \mathrm{Gal}(K|k)$.

3. Seien $\mathrm{char}(K) = p,\ a \in k \backslash k^p$, z.B. $k = \mathbb{F}_p(X)$, und $X^p - a \in k[X]$ mit Zerfällungskörper K. Dann gibt es ein $b \in K$ mit $b^p = a$, also $X^p - a = X^p - b^p = (X-b)^p$, d.h. $K = k(b) = k \oplus kb \oplus kb^2 \oplus \cdots \oplus kb^{p-1}$. Sei $\sigma \in \mathrm{Gal}(K|k)$, dann ist $\sigma(b)$ eine Nullstelle von $X^p - a$, d.h. $\sigma(b) = b$, also auch $\sigma(b^m) = (\sigma(b))^m = b^m$, d.h. $\sigma = \mathrm{id}$. Damit folgt: $|\mathrm{Gal}(K|k)| = 1$. ◊

4.6. Bemerkung

Seien k ein Körper, $K|k$ die transzendente Körpererweiterung

$$K = k(t) = \left\{ \frac{a_0 + a_1 t + \cdots + a_n t^n}{b_0 + b_1 t + \cdots + b_m t^m} \;\middle|\; n, m \in \mathbb{N},\ a_i, b_i \in K,\ \text{nicht alle } b_i = 0 \right\}$$

und $\sigma \in \mathrm{Aut}(K|k)$. Dann ist auch $\sigma(t) =: t^*$ transzendent über k, sonst gäbe es $c_0, ..., c_r \in k$ mit $c_0 + c_1 t^* + \cdots + c_r (t^*)^r = 0$ und durch Anwendung von σ^{-1} erhält man wegen $\sigma^{-1}(t^*) = t$, dass $c_0 + c_1 t + \cdots + c_r t^r = 0$ im Widerspruch zur Transzendenz von t über k. Es gilt

$$\sigma\left(\frac{a_0 + a_1 t + ... + a_n t^n}{b_0 + b_1 t + ... + b_m tm}\right) = \frac{a_0 + a_1 t^* + ... + a_n (t^*)^n}{b_0 + b_1 t^* + ... + b_m (t^*)^m}.$$

Also ist σ durch den Wert $\sigma(t) = t^*$ schon eindeutig festgelegt.

Ansatz: $t^* := \frac{at+b}{ct+d}$ mit $ad - bc \neq 0$ liefert einen Automorphismus: Betrachte die Möbiustransformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} =: \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}.$$

Dann liefert $\tau := t^{**} := \frac{a^* t + b^*}{c^* t + d^*}$ den zu σ inversen Automorphismus: $\tau(t^*) = t^{**} = t$.

Sei nun allgemein $t^* = \sigma(t) := \frac{f(t)}{g(t)}$ für geeignete $f, g \in k[t]$, die wir Œ als teilerfremd annehmen: $(f, g) = (1)$. Setze $L := k(\sigma(t)) = k(t^*) \subseteq K = k(t)$, also $K = L(t)$. Dann ist t algebraisch über L, denn $\mathrm{Irr}(t, L) \sim f(X) - t^* g(X)$ wgeen $f(t) - t^* g(t) = 0$ nach Definition von t^*. Die Irreduzibilität erhält man so: Setze $h(X, T) := f(X) - T g(X)$. Dann ist $h(X, t^*)$ irreduzibel über L, denn f, g sind teilerfremd, also h irreduzibel in $k[X, t^*]$. Mit Gauß ist h dann irreduzibel in $k(t^*)[X]$, da h als Polynom in X primitiv ist. Mit $k(t^*) = L$ folgt die Irreduzibilität von h über L.

Also ist $K = L(t)$ und es gilt $[K : L] = \deg h(X)$. Da σ Automorphismus, gilt $L = k(\sigma(t)) = K$, also $[L : K] = 1$, d.h. $\deg h(X) = \deg(f(X) - \sigma(t) g(X)) = 1$, also $\deg f \leq 1,\ \deg g \leq 1$. Damit ist

$$\mathrm{Aut}(k(t)|k) = \left\{ \sigma : k(t) \to k(t) \;\middle|\; \sigma(t) = \frac{at + b}{ct + d} \text{ mit } a, b, c, d \in k,\ ad - bc \neq 0 \right\}. \qquad ◊$$

4.7. Lemma

Sei K der Zerfällungskörper von $f \in k[X]$. Dann gilt:

$|\mathrm{Gal}(K|k)| \leq [K : k]$, wobei Gleichheit erfüllt ist, falls f separabel ist.

Beweis.

Nach dem Fortsetzungssatz 3.36 ist die Anzahl der Isomorphismen $\Psi : K \to K$ mit $\Psi_{|k} = \mathrm{id}$ kleiner oder gleich dem Grad $[K : k]$ der Körpererweiterung $K|k$ und gleich $[K : k]$, wenn f lauter verschiedene Nullstellen hat. Schreibe $f = p_1^{\nu_1} \cdots p_m^{\nu_m}$, alle p_i paarweise verschieden, irreduzibel und Œ normiert. Ist dann f separabel, dann sind alle p_i separabel, d.h. $g := p_1 \cdots p_m$ ist separabel, also hat g lauter verschiedene Nullstellen und K ist auch Zerfällungskörper von g, d.h. die Anzahl der Ψ ist m. □

4.8. Definition

Ist G eine Untergruppe von $\mathrm{Aut}(K)$, dann heißt

$$\mathrm{Fix}(G) := \{a \in K \mid \forall \sigma \in G : \sigma(a) = a\}$$

der Fixkörper von G.

4.9. Bemerkung

1. $\mathrm{Fix}(G)$ ist ein Körper: Seien $a, b \in \mathrm{Fix}(G)$ und $\sigma \in G$, d.h. $\sigma(a) = a$ und $\sigma(b) = b$, dann auch

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b \qquad \text{und} \qquad \sigma(ab) = \sigma(a)\sigma(b) = ab,$$

   also auch $\sigma(-a) = -\sigma(a) = -a,\ \sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$ und $\sigma(0) = 0,\ \sigma(1) = 1$.

2. Sei $k \subseteq K$ eine Körpererweiterung. Dann gelten:

$$\begin{array}{rcl} \mathrm{Fix} : \{\text{Untergruppen von } \mathrm{Gal}(K|k)\} & \longrightarrow & \{\text{Zwischenkörper von } k \subseteq K\}; \\ \mathrm{Gal} : \{\text{Untergruppen von } \mathrm{Gal}(K|k)\} & \longleftarrow & \{\text{Zwischenkörper von } k \subseteq K\}. \end{array}$$

3. Sei $G < \mathrm{Gal}(K|k)$, dann $\mathrm{Fix}(G) \supseteq k$.

4. Gelte $k \subseteq L \subseteq K$, dann ist $\mathrm{Gal}(K|L) \subseteq \mathrm{Gal}(K|k)$, denn sei $\sigma \in \mathrm{Gal}(K|L)$, dann ist $\sigma(l) = l$ für alle $l \in L$, also insbesondere $\sigma(a) = a$ für alle $a \in k$, d.h. $\sigma \in \mathrm{Gal}(K|k)$. ◊

4.10. Satz (Galoiskorrespondenz)

Für $G_1, G_2 < \mathrm{Gal}(K|k),\ k \subseteq L_1, L_2 \subseteq K$ gelten:

1. Falls $G_1 \subseteq G_2$, dann $\mathrm{Fix}(G_2) \subseteq \mathrm{Fix}(G_1)$.
2. Falls $L_1 \subseteq L_2$, dann $\mathrm{Gal}(K|L_2) \subseteq \mathrm{Gal}(K|L_1)$.
3. $\mathrm{Fix}(\mathrm{Gal}(K|L_1)) \supseteq L_1$ und $\mathrm{Gal}(K|\mathrm{Fix}(G_1)) \supseteq G_1$.

Beweis.

1. Sei $a \in \mathrm{Fix}(G_2)$. Dann ist $\sigma(a) = a$ für alle $\sigma \in G_2$, also insbesondere $\sigma(a) = a$ für alle $\sigma \in G_1$, d.h. $\sigma \in \mathrm{Fix}(G_1)$.
2. Sei $\sigma \in \mathrm{Gal}(K|L_2)$. Dann gilt $\sigma(a) = a$ für alle $a \in L_2$, also insbesondere $\sigma(a) = a$ für alle $a \in L_1$, d.h. $\sigma \in \mathrm{Gal}(K|L_1)$.
3. Sei $l \in L_1$. Dann gilt $\sigma(l) = l$ für alle $\sigma \in \mathrm{Gal}(K|L_1)$, also $l \in \mathrm{Fix}(\mathrm{Gal}(K|L_1))$.

   Sei $\sigma \in G_1$. Dann gilt $\sigma(a) = a$ für alle $a \in k$, also $\sigma \in \mathrm{Gal}(K|\mathrm{Fix}(G_1))$. □

4.11. Lemma (Artin)

Seien K ein Körper und G eine Untergruppe von $\mathrm{Aut}(K)$. Dann gilt: $[K : \mathrm{Fix}(G)] \leq |G|$.

Beweis.

Setze $k := \mathrm{Fix}(G)$, Œ $n = |G|$ endlich. Seien $u_1, ..., u_m \in K$ mit $m > n$. Wir zeigen: $u_1, ..., u_m$ sind k-linear abhängig. Sei dazu $G = \{\mathrm{id} = \sigma_1, ..., \sigma_n\}$. Betrachte das homogene lineare Gleichungssystem

$$\begin{array}{ccccccc} \sigma_1(u_1)X_1 & + & \cdots & + & \sigma_1(u_m)X_m & = & 0 \\ \vdots & & \vdots & & \vdots & & \\ \sigma_n(u_1)X_1 & + & \cdots & + & \sigma_n(u_m)X_m & = & 0 \end{array} \quad . \qquad (*)$$

Wir haben n Zeilen, m Unbestimmte und $m > n$, d.h. es gibt eine nicht-triviale Lösung $(a_1, ..., a_m) \in K^m$. Wir zeigen: $(a_1, ..., a_m) \in k^m$. Sei hierfür $(b_1, ..., b_m)$ eine nicht-triviale Lösung mit minimaler Anzahl

$b_i \neq 0$, Œ $b_1 \neq 0$, sogar Œ$b_1 = 1$. Angenommen, $b_2 \notin k$, d.h. es gibt $\sigma_j \in G$ mit $\sigma_j(b_2) \neq b_2$. Dann gilt für alle $1 \leq i \leq n$:

$$\begin{aligned} 0 &= \sigma_j(0) \\ &= \sigma_j(\sigma_i(u_1)b_1 + \cdots + \sigma_i(u_m)b_m) \\ &= \sigma_j \circ \sigma_i(u_1)\sigma_j(b_1) + \cdots + \sigma_j \circ \sigma_i(u_m)\sigma_j(b_m). \end{aligned}$$

Außderdem ist

$$G = \{\sigma_1, ..., \sigma_n\} = \{\sigma_j \circ \sigma_1, ..., \sigma_j \circ \sigma_n\},$$

d.h. σ_j permutiert lediglich die Zeilen von $(*)$. Also ist $(\sigma_j(b_1), ..., \sigma_j(b_m))$ ebenfalls eine Lösung von $(*)$ und damit auch $(b_1 - \sigma_j(b_1), ..., b_m - \sigma_j(b_m))$. Nun gelten aber: $b_1 - \sigma_j(b_1) = 1 - 1 = 0$, $b_2 - \sigma_j(b_2) \neq 0$ und $b_i = 0$, d.h. $b_i - \sigma_j(b_i) = 0$ für alle $1 \leq i \leq n$, d.h. wir erhalten einen zusätzlichen Nulleintrag, aber nicht die triviale Lösung. Dies steht im Widerspruch zur Minimalität der Anzahl der $b_i \neq 0$. □

4.2 Galoiserweiterungen & Hauptsatz der Galoistheorie

4.12. Definition

Sei $k \subseteq K$ algebraisch. K heißt separabel über k, falls $\mathrm{Irr}(a, k)$ separabel ist für alle $a \in K$.

K heißt normal über k, falls jedes irreduzible $f \in k[X]$ mit einer Nullstelle in K über K in Linearfaktoren zerfällt.

$K|k$ heißt eine Galoiserweiterung, falls K der Zerfällungskörper eines separablen Polynoms $f \in k[X]$ ist.

4.13. Bemerkung

Ist k vollkommen und ist $K \supseteq k$ algebraisch, dann ist $K|k$ separabel. ◊

4.14. Satz

Für $k \subseteq K$ sind äquivalent:

1. $K|k$ ist eine Galoiserweiterung.
2. $k = \mathrm{Fix}(G)$ für eine gewisse endliche Untergruppe G von $\mathrm{Gal}(K|k)$.
3. $K|k$ ist endlich dimensional, normal und separabel.

Beweis.

1. (1) ⇒ (2): Setze $G = \mathrm{Gal}(K|k)$ und $L = \mathrm{Fix}(G)$. Zu zeigen: $k = L$.

   Es ist $k \subseteq L \subseteq K$ mit $f \in k[X]$ separabel und K der Zerfällungskörper von f über k. Also $|G| = [K : k]$ nach Lemma 4.7 und f separabel über L, K Zerfällungskörper von f über L, d.h. $|\mathrm{Gal}(K|L)| = [K : L]$. Gleichzeitig ist $\mathrm{Gal}(K|L) \subseteq \mathrm{Gal}(K|k) = G$. Sei $\sigma \in G$. Dann $\sigma_L = \mathrm{id} \Rightarrow \sigma \in \mathrm{Gal}(K|L)$, d.h. $G = \mathrm{Gal}(K|L)$. Damit $[K : k] = [K : L] \Rightarrow k = L$. Wir haben also sogar gezeigt: $k = \mathrm{Fix}(\mathrm{Gal}(K|k))$.

2. (2) ⇒ (3): Sei $k = \mathrm{Fix}(G)$ mit $G < \mathrm{Gal}(K|k)$ und G endlich. Nach dem Lemma von Artin 4.11 ist $[K : k] \leq |G| < \infty$. Sei $f \in k[X]$ irreduzibel und normiert mit $f(a) = 0$ für ein $a \in K$. Zu zeigen: f zerfällt in $K[X]$ in lauter verschiedene Linearfaktoren.

   Betrachte dazu $\{\sigma(a) \mid \sigma \in G\} = \{a = a_1, ..., a_m\}$, wobei $a_1, ..., a_m$ die m verschiedene Nullstellen von f seien; insbesondere also $m \leq |G|$. Für $\varphi \in G$ gilt: $\{a_1, ..., a_m\} = \{\varphi(a_1), ..., \varphi(a_m)\}$. Wir definieren $g(X) = (X - a_1) \cdots (X - a_m) \in K[X]$. Die Koeffizienten von g sind invariant unter $\varphi \in G$, denn $\varphi(g) = (X - \varphi(a_1)) \cdots (X - \varphi(a_m)) = (X - a_1) \cdots (X - a_m)$, d.h. $g \in k[X]$, d.h. $g \mid f$ in $k[X]$ und da beide normiert, folgt $g = f$. Also zerfällt f in K in lauter verschiedene Linearfaktoren.

3. (3) ⇒ (1): Sei $K|k$ eine endliche Erweiterung, dann ist $K = k(a_1, ..., a_n)$ algebraisch. Sei $f_i = \mathrm{Irr}(a_i, k)$. Da $K|k$ separabel, zerfällt f_i in paarweise verschiedene Linearfaktoren in K und da $K|k$ normal, ist $f := f_1 \cdots f_n$ separabel und K ist der Zerfällungskörper von f. □

4.15. Korollar

Für Galoiserweiterungen gelten:

$\mathrm{Fix} \circ \mathrm{Gal} = \mathrm{id}$ auf den Zwischenkörpern $k \subseteq L \subseteq K$ und $\mathrm{Gal} \circ \mathrm{Fix} = \mathrm{id}$ auf den Untergruppen von $\mathrm{Gal}(K|k)$.

Beweis.

1. Wir haben eben gezeigt: $\mathrm{Fix}(\mathrm{Gal}(K|k)) = k$. Mit $K|k$ ist auch $K|L$ eine Galoiserweiterung, denn da K der Zerfällungskörper von $f \in k[X]$ ist, ist K auch der Zerfällungskörper von $f \in L[X]$. Also gilt auch $\mathrm{Fix}(\mathrm{Gal}(K|L)) = L$.

2. Seien G eine endliche Untergruppe von $\mathrm{Gal}(K|k)$ und $L := \mathrm{Fix}(G)$. Wir wissen, dass $G \subseteq \mathrm{Gal}(K|L)$ gilt, und wollen zeigen, dass $G = \mathrm{Gal}(K|L)$, wobei $K|L$ eine Galoiserweiterung ist. Nach Lemma 4.7 ist $|\mathrm{Gal}(K|L)| \leq [K : L]$ und nach dem Lemma von Artin 4.11 gilt $[K : L] \leq |G|$. Wir erhalten also $|G| \leq |\mathrm{Gal}(K|L)| = [K : L] \leq |G|$, d.h. $G = \mathrm{Gal}(K|L)$.

$$\begin{array}{ccc} K & \longmapsto & \{\mathrm{id}\} \\ \cup\mathrm{I} & & \mathrm{I}\cap \\ \mathrm{Fix}(H) = L & \underset{\mathrm{Fix}}{\overset{\mathrm{Gal}}{\rightleftarrows}} & H = \mathrm{Gal}(K|L) \\ \cup\mathrm{I} & & \mathrm{I}\cap \\ k & \longmapsto & G \end{array}$$

Also sind die Abbildungen Fix und $\mathrm{Gal}(K|\cdot)$ bijektiv und invers zueinander. □

4.16. Satz (Hauptsatz der Galoistheorie)

Sei $K|k$ eine Galoiserweiterung. Dann sind die Zuordnungen $\mathrm{Fix}(H)$ und $\mathrm{Gal}(K|L)$ zwischen Untergruppen H der Galoisgruppe $G = \mathrm{Gal}(K|k)$ und den Zwischenkörpern L von $k \subseteq K$ bijektiv und invers zueinander.

Weiter gelten:

1. $H_1 \supseteq H_2 \Leftrightarrow \mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2)$.
2. $|H| = [K : \mathrm{Fix}(H)]$ und $[\mathrm{Fix}(H) : k] = [G : H]$.
3. H ist Normalteiler von $G \Leftrightarrow \mathrm{Fix}(H)$ ist normal über k. In diesem Fall gilt: $\mathrm{Gal}(\mathrm{Fix}(H)|k) \cong G/H$.

Beweis.

1. Noch zu zeigen: $\mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2) \Rightarrow H_1 \supseteq H_2$. Es gilt

$$\mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2) \quad \Longrightarrow \quad H_1 = \mathrm{Gal}(K|\mathrm{Fix}(H_1)) \supseteq \mathrm{Gal}(K|\mathrm{Fix}(H_2)) = H_2.$$

2. Setze $L := \mathrm{Fix}(H)$. Nach Lemma 4.7 gilt $|H| = \mathrm{Gal}(\mathrm{Fix}(H)) = \mathrm{Gal}(K|L) = [K : L]$, da $K|L$ separabel ist. Weiter gilt nach dem Gradsatz:

$$[L : K] = \frac{[K : k]}{[K : L]} = \frac{|G|}{|H|} = [G : H].$$

3. a) Es gilt $\sigma(L) = \mathrm{Fix}(\sigma H \sigma^{-1})$ für $\sigma \in \mathrm{Gal}(K|k)$:

$$\begin{aligned} (\sigma\tau\sigma^{-1})(a) = a \text{ für alle } \tau \in H &\Leftrightarrow (\tau\sigma^{-1})(a) = \sigma^{-1}(a) \text{ für alle } \tau \in H \\ &\Leftrightarrow \sigma^{-1}(a) \in \mathrm{Fix}(H) = L \\ &\Leftrightarrow a \in \sigma(L). \end{aligned}$$

b) Es gilt $\sigma_1(L) = \sigma_2(L) \Leftrightarrow \sigma_1 H \sigma_1^{-1} = \sigma_2 H \sigma_2^{-1}$:

$$\begin{aligned} \sigma_1(L) = \sigma_2(L) &\Leftrightarrow \mathrm{Fix}(\sigma_1 H \sigma_1^{-1}) = \mathrm{Fix}(\sigma_2 H \sigma_2^{-1}) \\ &\Leftrightarrow \sigma_1 H \sigma_1^{-1} = \sigma_2 H \sigma_2^{-1}. \end{aligned}$$

c) Es gilt $H \lhd G \Leftrightarrow \sigma(L) = L$ für alle $\sigma \in G$.

$\Rightarrow$ Definiere res : $G \to \mathrm{Gal}(L|k)$ durch $\sigma \mapsto \sigma_{|L}$. res ist ein Gruppenhomomorphismus, denn es gilt $(\sigma \circ \tau)_{|L} = \sigma_{|L} \circ \tau_{|L}$. Setze $\overline{G} := \mathrm{Bild}(\mathrm{res})$. Dann ist $\overline{G}$ eine Untergruppe von $\mathrm{Gal}(L|k)$. $k = \mathrm{Fix}(G) \Rightarrow k \subseteq \mathrm{Fix}(\overline{G})$, sogar $k = \mathrm{Fix}(\overline{G})$. Also ist $(L|k)$ eine Galoiserweiterung und damit normal. Weiter gilt: $\mathrm{Kern}(\mathrm{res}) = H$, denn $\sigma_{|L} = \mathrm{id}$, d.h. $\sigma \in \mathrm{Gal}(K|L) = H$.

$\Leftarrow$ Sei L normal über k, d.h. $L|k$ ist Galoisch, und sei $\sigma \in G$. Zu zeigen: $\sigma(L) = L$.

L ist der Zerfällungskörper eines separablen Polynoms $f \in k[X]$, d.h. $f(X) = \prod(X - a_i)$ mit $L = k(a_1, ..., a_m)$. σ permutiert die a_i, d.h. $\sigma(L) \subseteq L$ und da $[L : k] < \infty$, folgt $\sigma(L) = L$.

$\mathrm{Gal}(\mathrm{Fix}(H)|k) \cong G/H$ erhält man dann aus dem Homomorphiesatz, angewandt auf den Einschränkungshomomorphismus res. □

4.3 Anwendungen der Galoistheorie

4.17. Lemma

Seien K ein Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.

Beweis.

Sei $a \in G$ mit $\mathrm{Ord}(a) = n$, wobei n das kleinste gemeinsame Vielfache der Ordnungen aller Elemente in G bezeichnet. Dann sind alle $b \in G$ Nullstellen von $X^n - 1$. Also ist $|G| \leq n$ und zugleich $\mathrm{Ord}(a) = n$, d.h. $|a^{\mathbb{Z}}| = n \leq |G|$, also $G = a^{\mathbb{Z}}$. □

4.18. Satz (Satz vom primitiven Element)

Sei $K = k(a_1, ..., a_n)$ mit alle a_i algebraisch über k und $a_2, ..., a_n$ separabel über k. Dann gibt es ein primitives Element $\delta \in K$ mit $K = k(\delta)$, d.h. $K|k$ ist einfach.

Beweis.

Œ betrachten wir den Fall $n = 2$; der Rest folgt mit Induktion.

1. Ist k endlich, dann ist auch K endlich. Nach Lemma 4.17 sind endliche multiplikative Untergruppen von K stets zyklisch, also $K = k(a^{\mathbb{Z}}) = k(a)$.

2. Ist k unendlich, so betrachte $K = k(\alpha, \beta)$, α, β algebraisch, β separabel über k. Seien $f = \mathrm{Irr}(\alpha, k)$, $g = \mathrm{Irr}(\beta, k)$ und L der Zerfällungskörper von fg über K, d.h. L enthalte alle Nullstellen $\alpha = \alpha_1, ..., \alpha_n$ von f und $\beta = \beta_1, ..., \beta_m$ von g. Wähle $c \in k$, so dass $\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$ für alle $j \neq 1$ und alle i, d.h. $c \neq \frac{\alpha_1 - \alpha_i}{\beta_j - \beta_1}$ (dies ist möglich, da k unendlich ist). Setze $\delta := \alpha_1 + c\beta_1 = \alpha + c\beta$. Dann $k(\delta) \subseteq k(\alpha, \beta) = K$. Wir zeigen also noch: $k(\alpha, \beta) \subseteq k(\delta)$.

   β ist Nullstelle von $g(X)$ und von $f(\delta - cX) =: f_1(X)$. Sei $\gamma \in L \backslash \{\beta\}$ eine Nullstelle von g, d.h. $\gamma = \beta_j$ für ein $j \neq 1$. Dann $\delta - c\gamma = \delta - c\beta_j \neq \alpha_i$ für alle i, also $f(\delta - c\gamma) = f_1(\gamma) \neq 0$. Da β separabel, folgt $X - \beta = \mathrm{ggT}(g, f_1)$ in f_1 und $g \in k(\delta)[X]$, also gibt es $\epsilon \in k(\delta)$ und $h_1, h_2 \in k(\delta)[X]$ mit $\epsilon(X - \beta) = h_1 f_1 + h_2 g$, d.h. $\epsilon(X - \beta) \in k(\delta)[X]$, also $\frac{\epsilon\beta}{\epsilon} = \beta \in k(\delta)$. Dann auch $\alpha = \delta - c\beta \in k(\delta)$, d.h. $k(\alpha, \beta) \subseteq k(\delta)$. □

4.19. Korollar

Ist $K|k$ endlich und separabel, dann ist die Körpererweiterung einfach.

Sind k vollkommen und $K|k$ algebraisch, dann gilt: $K|k$ ist endlich $\Leftrightarrow$ $K|k$ ist einfach.

4.20. Satz (Fundamentalsatz der Algebra)

Sei $(R, \leq)$ ein reell abgeschlossener Körper, d.h. alle $x \geq 0$ seien Quadrate und jedes Polynom ungeraden Grades habe eine Nullstelle in R.

Dann ist $C := R(\sqrt{-1})$ algebraisch abgeschlossen. Speziell ist $\mathbb{C} := \mathbb{R}(\sqrt{-1})$ algebraisch abgeschlossen.

Beweis.

1. C ist quadratisch abgeschlossen: Definiere $i := \sqrt[+]{-1}$. Zu $x + iy$ setze

$$w = \begin{cases} \sqrt[+]{\frac{x + \sqrt[+]{x^2+y^2}}{2}} + i\sqrt[+]{\frac{-x + \sqrt[+]{x^2+y^2}}{2}}, & y \geq 0, \\ \sqrt[+]{\frac{x + \sqrt[+]{x^2+y^2}}{2}} - i\sqrt[+]{\frac{-x + \sqrt[+]{x^2+y^2}}{2}}, & y < 0 \end{cases}.$$

   Dann gilt $x + iy = w^2$.

2. Jedes Polynom vom Grad 2 zerfällt über C in Linearfaktoren: Sei $f = aX^2 + bX + c \in C[X]$. Dann ist

$$f(X) = a\left(X + \frac{b + \sqrt{b^2 - 4ac}}{2}\right)\left(X + \frac{b - \sqrt{b^2 - 4ac}}{2}\right) \in C[X],$$

   denn nach 1. existiert $\sqrt{b^2 - 4ac}$ in C. Also hat C keine Erweiterung $[K : C]$ vom Grad 2, sonst $K = C(\alpha)$ und es gäbe ein irreduzibles Polynom vom Grad 2, ein Widerspruch.

3. C hat keine endliche echte Erweiterung $[k : C]$: Angenommen, es gäbe eine endliche Erweiterung $k|C$ mit $[k : C] \geq 2$. Seien $f = \mathrm{Irr}(\alpha, R)$ mit $k = R(\alpha)$ und K der Zerfällungskörper von f über k. Dann ist $K|R$ eine echte Galoiserweiterung. $G := \mathrm{Gal}(K|R)$ ist endlich, denn $|G| = [K : R]$, etwa $2^m n$, $2 \nmid n$. Sei U eine 2-Sylow-Untergruppe von G, also $|U| = 2^m$. Dann ist $[\mathrm{Fix}(U) : R]$ ungerade. Sei $\mathrm{Fix}(U) = R(\beta)$, d.h. $\deg \mathrm{Irr}(\beta, R) = n$. Da R reell abgeschlossen ist, folgt $n = 1$, d.h. $\mathrm{Fix}(U) = R$. Also ist $\mathrm{Gal}(K|R) = G$ eine 2-Gruppe.

   $H := \mathrm{Gal}(K|C)$ ist eine Untergruppe von G vom Index 2: $|H| = 2^{m-1}$. Ist $m - 1 > 0$, so gibt es eine Untergruppe H_1 von H mit $|H_1| = 2^{m-2}$, also $[H : H_1] = 2 = [\mathrm{Fix}(H_1) : \mathrm{Fix}(H)]$. Dies ist unmöglich, da C keine Erweiterung vom Grad 2 erlaubt. Also $m - 1 = 0$, d.h. $K = C$. □

4.21. Definition

$a \in K$ heißt n-te Einheitswurzel, falls $a^n = 1$, d.h. falls a Nullstelle von $X^n - 1$ ist.

Der Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ heißt der n-te Kreisteilungskörper.

α heißt n-te primitive Einheitswurzel, falls $\mathrm{Ord}(\alpha) = n$.

Sei $a \in K$. Dann heißt $X^n - a \in k[X]$ reines Polynom.

4.22. Bemerkung

Seien $\mathrm{char}(k) = 0$ und K der Zerfällungskörper von $X^n - 1$ über k. Da $X^n - 1$ teilerfremd zu nX^{n-1}, hat $X^n - 1$ n verschiedene Nullstellen $\alpha_1, ..., \alpha_n$ in K. Die Menge aller Nullstellen von $X^n - 1$ ist eine endliche Untergruppe von $K^\times$, also zyklisch nach Lemma 4.17. Damit ist $\{\alpha_1, ..., \alpha_n\} = \{1, \alpha, ..., \alpha^{n-1}\} =: U_n$ eine Gruppe. ◊

4.23. Satz

Seien $\mathrm{char}(k) = 0$ und K der Zerfällungskörper von $X^n - 1 \in k[X]$.

Dann ist $\mathrm{Gal}(K|k)$ abelsch.

Beweis.

Seien $K = k(\alpha)$, α eine primitive n-te Einheitswurzel und $\sigma \in \mathrm{Gal}(K|k)$. σ ist eindeutig bestimmt durch $\sigma(\alpha) = \alpha^m$ für ein $m \in \mathbb{Z}$, denn es gilt $\sigma(\alpha^l) = (\alpha^m)^l = \alpha^{ml}$. Also ist $\sigma_{|U_n} \in \mathrm{Aut}(U_n, \cdot)$ und $G = \mathrm{Gal}(K|k) \cong \{\sigma_{|U_n} \mid \sigma \in G\} < \mathrm{Aut}(U_n, \cdot)$. Es ist $(\mathbb{Z}_n, +) \cong (U_n, \cdot)$ mit $i \mapsto \alpha^i$; beachte dabei: $\alpha^i\alpha^j = \alpha^{i+j}$. Zu zeigen ist also: $\mathrm{Aut}(\mathbb{Z}_n, +)$ ist abelsch. Wir wissen: $\mathbb{Z}_n^\times$ ist abelsch. Es genügt also zu zeigen, dass $\mathrm{Aut}(\mathbb{Z}_n, +) \cong \mathbb{Z}_n^\times$.

1. Sei $m \in \mathbb{Z}_n^\times$. Dann wird durch $\Psi : i \mapsto mi$ ein Automorphismus auf $(\mathbb{Z}, +)$ definiert: Für alle i, j gilt $\Psi(i + j) = m(i + j) = mi + mj = \Psi(i) + \Psi(j)$; da $m \neq 0$, gilt $\mathrm{Kern}(\Psi) = 0$, also Ψ injektiv, und mit $j \in (\mathbb{Z}_n, +) \Rightarrow j = m(m^{-1}j)$ folgt: Ψ ist surjektiv.

2. Sei $\tau : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ ein Automorphismus. Dann ist τ durch $\tau(1)$ festgelegt: Aus $\tau(1) = m$ folgt $\tau(i) = im$, $0 \leq i \leq m$. Weiter gibt es für jede Einheit $m \in (\mathbb{Z}, +)$ einen Automorphismus $\tau : i \mapsto mi$, denn $\tau^{-1}(i) = im^{-1}$.

3. m_1m_2 induziert $i \mapsto (m_1m_2)i = m_1(m_2i) = (\tau_1 \circ \tau_2)(i)$. □

4.24. Satz

Seien $a \in k$, K der Zerfällungskörper von $X^n - a$ und $X^n - 1$ zerfalle in k, d.h. k enthält alle n-ten Einheitswurzeln.

Dann ist $\mathrm{Gal}(K|k)$ zyklisch.

Beweis.

Sei $U_n = \langle\alpha\rangle$, $|U_n| = n$ und $w \in K$ mit $w^n = a$, d.h. $(w\alpha^j)^n = a$ und $w\alpha^j$ $(0 \leq j \leq n - 1)$ sind alle Nullstellen von $X^n - a$ und $K = k(w)$ ist der Zerfällungskörper von $X^n - a$. Betrachte $\Psi : \mathrm{Gal}(K|k) \to U_n$ mit $\sigma \mapsto \beta \in U_n$, falls $\sigma(w) = \beta w$. Es gilt $\sigma \circ \tau \mapsto \beta_{\sigma\circ\tau} = \beta_\sigma\beta_\tau$, denn

$$\beta_{\sigma\circ\tau}w = (\sigma \circ \tau)(w) = \sigma(\tau(w)) = \sigma(\beta_\tau w) = \beta_\tau\sigma(w) = \beta_\tau\beta_\sigma w = \beta_\sigma\beta_\tau w,$$

da U_n zyklisch, also abelsch. Gilt $\beta_\sigma = 1$ (d.h. liegt σ im Kern von Ψ), dann $\sigma(w) = \beta_\sigma w = w$, d.h. $\sigma = \mathrm{id}$. Also ist Ψ ein injektiver Homomorphismus, d.h. $\Psi(\mathrm{Gal}(K|k))$ ist eine Untergruppe von U_n, also zyklisch. □

4.25. Satz

Seien $K|k$ eine Galoiserweiterung, $\mathrm{Gal}(K|k) \cong \mathbb{Z}_p$ mit p prim und k enthalte alle p-ten Einheitswurzeln.

Dann gibt es ein $d \in K$ mit $K = k(d)$ und $d^p = a \in k$.

Beweis.

Seien $\alpha \in k$ primitive p-te Einheitswurzel, $\langle\alpha\rangle = \{1, \alpha, \alpha^2, ..., \alpha^{p-1}\}$, $\mathrm{Gal}(K|k) = \langle\sigma\rangle = \{\mathrm{id}, \sigma, ..., \sigma^{p-1}\}$ und $c \in K\backslash k$ beliebig. Da $[k(c) : k] = p$ und $k \subseteq k(c) \subseteq K$, gilt dann $K = k(c)$. Zu $\beta \in \langle\alpha\rangle$ definiere $(\beta, c) := c + \sigma(c)\beta + \sigma^2(c)\beta^2 + \cdots + \sigma^{p-1}(c)\beta^{p-1}$, die Lagrangesche Resolvente. Dann ist

$$\sigma((\beta, c))\beta = \sigma(c)\beta + \sigma^2(c)\beta^2 + \cdots + \sigma^{p-1}(c)\beta^{p-1} + \sigma^p(c)\beta^p = (\beta, c);$$

beachte dabei: $\beta^p = (\alpha^i)^p = (\alpha^p)^i = 1$ für $0 \leq i \leq p - 1$ und $\sigma^p(\beta) = \mathrm{id}(\beta) = \beta$. Wir erhalten $\sigma((\beta, c)) = (\beta, c)\beta^{-1}$, d.h. $\sigma((\beta, c)^p) = \sigma((\beta, c))^p\beta^{-p} = (\beta, c)^p$, folglich ist $(\beta, c)^p$ invariant unter σ und damit auch unter σ^2, σ^3, ... Also ist $\sigma \in \mathrm{Fix}(G) = k$. Setze $\beta_i := \alpha^i \in \langle\alpha\rangle$ für $0 \leq i \leq p - 1$ und betrachte das inhomogene lineare Gleichungssystem

$$\begin{array}{ccccccccc} X_1 & + & \beta_0 X_2 & + & \cdots & + & \beta_0^{p-1}X_p & = & (\beta_0, c) \\ \vdots & & \vdots & & \vdots & & \vdots & & \\ X_1 & + & \beta_{p-1}X_2 & + & \cdots & + & \beta_{p-1}^{p-1}X_p & = & (\beta_{p-1}, c) \end{array} \quad . \qquad (*)$$

Dieses wird gelöst von $(c, \sigma(c), ..., \sigma^{p-1}(c))$. Wir zeigen: Es gibt keine weiteren Lösungen. Dazu betrachten

wir die Van-der-Monde-Determinante

$$\det \begin{pmatrix} 1 & \beta_0 & \cdots & \beta_0^{p-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_{p-1} & \cdots & \beta_{p-1}^{p-1} \end{pmatrix} = \prod_{i<j} (\beta_i - \beta_j) \neq 0.$$

Es können nicht alle (β_i, c) in k liegen, sonst läge auch c in k. Also gibt es ein i_0 mit $(\beta_{i_0}, c) \in K \backslash k$. Wir wählen $d := (\beta_{i_0}, c)$, dann gilt $d^p \in k$. □

4.26. Satz (Konstruktion regelmäßiger p-Ecke)

Sei p eine Fermat-Primzahl, d.h. $p \in \mathbb{N}$ prim mit $p = 2^s + 1$ für ein $s \in \mathbb{N}$.

Dann ist $\alpha := \exp(\frac{2\pi i}{p})$ mit Zirkel und Lineal konstruierbar.

Insbesondere sind das regelmäßige Fünfeck und das regelmäßige Siebzehneck konstruierbar.

Beweis.

$K_p := \mathbb{Q}(\alpha)$ ist der Zerfällungskörper von $X^p - 1$ über $\mathbb{Q}$, $K_p|\mathbb{Q}$ ist eine Galoiserweiterung und die zugehörige Galoisgruppe $G := \mathrm{Gal}(K_p|\mathbb{Q})$ eine 2-Gruppe, denn $|G| = [K_p : \mathbb{Q}] = p - 1 = 2^s$. Dann hat $G =: G_s$ eine Untergruppe G_{s-1} mit $|G_{s-1}| = 2^{s-1}$, also $[G_s : G_{s-1}] = 2$. Entsprechend gibt es $G_{s-2} < G_{s-1}$ mit $|G_{s-2}| = 2^{s-2}$ ..., also hat G eine Kompositionsreihe

$$\{\mathrm{id}\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{s-1} \lhd G_s = G.$$

Dann gilt auch für die zugehörigen Fixkörper

$$K_p = \mathrm{Fix}(\{\mathrm{id}\}) \supseteq L_1 \supseteq L_2 \supseteq \cdots \supseteq L_{s-1} \supseteq L_s = \mathbb{Q},$$

dass $[L_{s-1} : \mathbb{Q}] = 2$ und $[L_{i-1} : L_i] = 2$ für alle i. Nach Satz 3.24 ist α dann mit Zirkel und Lineal konstruierbar. □

4.27. Definition

Seien $\mathrm{char}(k) = 0$ und $f \in k[X] \backslash k$ normiert. Wir sagen, $f = 0$ ist (mit Radikalen) über k auflösbar, falls es eine Kette

$$k = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = K$$

von Körpern gibt mit $K_{i+1} = K_i(d_i)$, $d_i^{n_i} = a_i \in K_i$ für ein $n_i \in \mathbb{N}$, so dass K den Zerfällungskörper von f über k umfasst.

4.28. Bemerkung

Setze $\sqrt[n_i]{a_i} := d_i$. Dann gilt: $K_{i+1} = K_i(\sqrt[n_i]{a_i}) = K_i \oplus K_i \sqrt[n_i]{a_i} \oplus \cdots \oplus K_i \sqrt[n_i]{a_i^{n_i - 1}}$. ◊

4.29. Satz (Auflösbarkeit in Radikale)

Seien $\mathrm{char}(k) = 0$ und $f \in k[X] \backslash k$ normiert. Dann gilt:

$f(X) = 0$ ist über k auflösbar $\Leftrightarrow$ die Galoisgruppe des Zerfällungskörpers von f über k ist auflösbar.

Beweis.

$\Leftarrow$ Sei K der Zerfällungskörper von f über k, Œ $(f, f') = (1)$, d.h. f hat keine mehrfachen Nullstellen. Weiter seien $G = \mathrm{Gal}(K|k)$, $n = |G| = [K : k]$, G auflösbar und α eine primitive n-te Einheitswurzel, d.h. $\alpha^{\mathbb{Z}}$ beinhaltet alle Nullstellen von $X^n - 1$. Gesucht ist eine Körperkette $k = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m$, $K \subseteq K_m$, mit $K_{i+1} = K_i(\sqrt[n_i]{d_i})$, $d_i \in K_i$, d.h. eine Radikalerweiterung.

Setze $K_1 = k$ und $K_2 = K_1(\alpha)$. Seien $a_1, ..., a_r$ alle Nullstellen von f in $K \backslash k$, also $K = k(a_1, ..., a_r)$ und $[K : k] = r$. $K(\alpha)|k(\alpha)$ ist eine Galoiserweiterung und $K(\alpha)$ ist der Zerfällungskörper von f über $k(\alpha)$. Zu $H := \mathrm{Gal}(K(\alpha)|k(\alpha))$ ist $\Phi : H \to G$, $\sigma \mapsto \sigma_{|K}$ injektiv, denn $\sigma_{|K} = \mathrm{id}$, d.h. $\sigma(a_i) = a_i$ für alle

i, also $\sigma = \mathrm{id}$. Φ definiert also einen Isomorphismus zwischen H und G, d.h. nach Homomorphiesatz: $H \cong U < G$. Da G auflösbar ist, ist auch H auflösbar. Nach Satz 1.51 gibt es eine Normalreihe $H = H_2 \rhd H_3 \rhd \cdots \rhd H_m = \{1\}$ mit H_j/H_{j+1} zyklisch von Primzahlordnung. Setze $K_i := \mathrm{Fix}(H_i)$ für $2 \le i \le m$. Dann $K_2 \subseteq K_3 \subseteq \cdots \subseteq K_m = K(\alpha)$ und wegen $H_i \rhd H_{i+1}$ ist K_{i+1} Galoisch über K_i und $\mathrm{Gal}(K_{i+1}|K_i) \cong H_i/H_{i+1} \cong \mathbb{Z}_{p_i}$ nach dem Hauptsatz der Galoistheorie.

Wegen $p_i := |H_i/H_{i+1}| = |H_i|/|H_{i+1}| \mid |H| \mid |G|$ liegt in K_i jede p_i-te Einheitswurzel, denn es gilt $1 = \alpha^n = \alpha^{p_i s} = (\alpha^{p_i})^s$, d.h. α ist eine p_i-te Einheitswurzel. Damit $K_{i+1} = K_i(\sqrt[p_i]{d_i})$ für ein $d_i \in K_i$ $(2 \le i \le m)$.

$\Rightarrow$ Seien $k = K_1 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$ mit $K_{i+1} = K_i(d_i)$, $d_i^{n_i} = a_i \in K_i$ und $\mathrm{Zfk}(f,k) \subseteq K$. Wir suchen einen Oberkörper $L \supseteq K$, so dass $L|k$ Galoisch ist und $\mathrm{Gal}(L|k)$ auflösbar ist, dann ist $\mathrm{Gal}(\mathrm{Zfk}(f,k)|k) \cong \mathrm{Gal}(L|k)/\mathrm{Gal}(L|\mathrm{Zfk}(f,k))$, also auflösbar.

Konstruktion von L: Betrachte

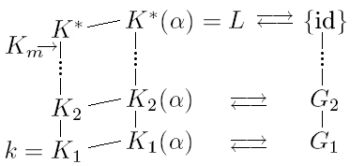
$$k = K_1 \subseteq K_2 = K_1(d_1) = k(d_1) \subseteq k(d_1,d_2) \subseteq \cdots \subseteq k(d_1,...,d_{m-1}) = K,$$

d.h. $[K:k] < \infty$. Nach dem Satz vom primitiven Element 4.18 ist $K = k(b)$ für ein $b \in K$. Setze $g = \mathrm{Irr}(b,k)$ und $K^* := \mathrm{Zfk}(g,k)$. Dann ist $K^*|k$ Galoisch. Setze $G^* := \mathrm{Gal}(K^*|k)$ mit $|G| < \infty$ und $G^* = \{\mathrm{id} = \sigma_1, ..., \sigma_r \mid r = [K^* : k]\}$.

Für $F := k(\sigma_1(K) \cup \cdots \cup \sigma_r(K))$ gilt $\sigma_i(F) = F$ für alle $i = 1,...,r$, also ist $F|k$ eine normale Galoiserweiterung. Œ setze $K^* = F$. Es gilt $F = k(\sigma_1(d_1), ..., \sigma_1(d_{m-1}), \sigma_2(d_1), ..., ..., \sigma_r(d_{m-1}))$, denn $\sigma_i(K) = k(\sigma_i(d_1), ..., \sigma_i(d_{m-1}))$. Wir erhalten also eine Radikalerweiterungskette

$$k \subseteq k(\sigma_1(d_1)) \subseteq \cdots \subseteq M := k(\sigma_1(d_1), ..., ..., \sigma_r(d_{m-2})) \subseteq K^* \subseteq M(\sigma_r(d_{m-1})).$$

Seien nun $n = \mathrm{kgV}\{n_i\}$ und $L = K^*(\alpha)$, α primitive n-te Einheitswurzel. Da $K^*|k$ Galoisch, ist K^* Zerfällungskörper eines separablen Polynoms $h \in k[X]$. h zerfällt auch in L und L ist Zerfällungskörper von $h(X)(X^n - 1) \in k[X]$, also ist auch $L|k$ Galoisch. Noch zu zeigen: $\mathrm{Gal}(L|k) =: G$ ist auflösbar.



Wir brauchen eine Normalreihe $G \rhd G_1 \rhd G_2 \rhd \cdots \rhd \{1\}$. $k(\alpha)|k$ ist abelsch, außderdem Galoisch, denn $k(\alpha)$ ist Zerfällungskörper von $X^n - 1 \in k[X]$. $K_2(\alpha)|K_1(\alpha)$ ist normal, da $K_2(\alpha) = K_1(\alpha)(\sqrt[n_1]{d_1})$, und abelsch, da zyklisch; $X^{n_1} - \alpha_1 \in K_1(\alpha)[X]$ und $n_1 \mid n$, d.h. $K_1(\alpha)$ enthält die n_1-te Einheitswurzel. Mit dem Hauptsatz der Galoistheorie folgt dann: $G \rhd G_1 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd \{\mathrm{id}\}$ und weiter $G_i/G_{i+1} \cong \mathrm{Gal}(K_{i+1}(\alpha)|K_i(\alpha))$ abelsch. □

4.30. KOROLLAR

Sei $\mathrm{char}(k) = 0$. Dann ist jede Gleichung vom Grad $n \le 4$ über k auflösbar.

BEWEIS.

Sei $n = \deg f \le 4$, f habe Œ keine mehrfachen Nullstellen in k (sonst zerlege f in $f_1^{\nu_1} \cdots f_m^{\nu_m}$ mit alle $f_i \in k[X]$ irreduzibel und betrachte $f_1 \cdots f_m$; dieses Polynom hat dann keine mehrfachen Nullstellen) und K der Zerfällungskörper von f über k. Dann gilt $\mathrm{Gal}(K|k) \cong G$ für ein $G < S_n$: Zu $K = k(\alpha_1, ..., \alpha_n)$ mit $\alpha_1, ..., \alpha_n \in K$ Nullstellen von f, ist $\sigma \in \mathrm{Gal}(K|k)$ eindeutig bestimmt durch die Permutation $\sigma : \{\alpha_1, ..., \alpha_n\} \mapsto \{\alpha_1, ..., \alpha_n\}$. Da für $n \le 4$ die S_n und alle ihre Untergruppen auflösbar sind, ist dann auch $\mathrm{Gal}(K|k)$ auflösbar. □

4.31. LEMMA

Seien p eine Primzahl und H eine Untergruppe von S_p. Für alle $i, j \in \{1, ..., p\}$ gebe es ein $\sigma \in H$ mit $\sigma(i) = j$. Weiter enthalte H eine Transposition.

Dann gilt $H = S_p$.

Beweis.

$i \sim j :\Leftrightarrow i = j$ oder $(i\ j) \in H$ definiert eine äquivalenzrelation auf $\{1, ..., p\}$, dann $i \sim j \Leftrightarrow \sigma(i) \sim \sigma(j)$ für alle $\sigma \in H$ und alle $i, j \in \{1, ..., p\}$:

$\Rightarrow$ Sei $i \sim j$. Trivialerweise gilt $i = j \Rightarrow \sigma(i) = \sigma(j)$. Ist $i \neq j$, dann $(i\ j) \in H$ und $\sigma(i) \neq \sigma(j)$, da σ bijektiv. Also auch $\sigma(i\ j)\sigma^{-1} = (\sigma(i), \sigma(j)) \in H$, d.h. in jedem Fall $\sigma(i) \sim \sigma(j)$.

$\Leftarrow$ Sei $\sigma(i) \sim \sigma(j)$. Ist $\sigma(i) = \sigma(j)$, dann auch $i = j$, da σ invertierbar. Sonst $\sigma^{-1}(\sigma(i)\sigma(j))\sigma = (i\ j) \in H$.

Betrachte nun die äquivalenzklasse $[i] = \{j \in \{1, ..., p\} \mid j \sim i\}$. Wir zeigen, dass alle äquivalenzklassen die gleiche Anzahl an Elementen haben. Sei $j \in [i] \Leftrightarrow j \sim i \Leftrightarrow \sigma(j) \sim \sigma(i) \Leftrightarrow \sigma(j) \in [\sigma(i)]$, also $|[i]| = |[\sigma(i)]|$. Sei $i \in \{1, ..., p\}$. Dann gibt es für jedes $k \in \{1, ..., p\}$ ein $\sigma \in H$ mit $\sigma(i) = k$, d.h. alle äquivalenzklassen haben die gleiche Anzahl S an Elementen.

Nun wissen wir aber, dass äquivalenzklassen disjunkt sind, d.h. $[\cdot]_1 \cup \cdots \cup [\cdot]_l = \{1, ..., p\}$. Wegen $|[\cdot]_k| = S$ für alle $k \in \{1, ..., l\}$ folgt $Sl = p$, d.h. $S = 1$ oder $S = p$. $S = 1$ ist unmöglich, sonst gäbe es gar keine Transpositionen in H, was im Widerspruch zur Voraussetzung steht. Also ist $S = p$, d.h. alle Transpositionen aus S_p liegen in H und damit $S_p = H$, da jede Permutation Produkt aus Transpositionen ist. □

4.32. Satz

Seien p eine Primzahl und $f \in \mathbb{Z}[X]$ irreduzibel mit $\deg f = p$ und genau zwei nicht reellen Nullstellen.

Dann gilt $\mathrm{Gal}(\mathrm{Zfk}(f, \mathbb{Q})|\mathbb{Q}) \cong S_p$.

Beweis.

Sei a eine Nullstelle von f. Dann ist $\overline{f(a)} = 0 = f(\overline{a})$, also hat der Automorphismus τ mit $\tau(a) = \overline{a}$ aus $G = \mathrm{Gal}(\mathrm{Zfk}(f, \mathbb{Q})|\mathbb{Q})$ die Ordnung 2. $G \cong H < S_p$; dabei entspricht τ eine Transposition in S_p. H operiert transitiv auf den Nullstellen $\alpha_1, ..., \alpha_n$ von f: f ist irreduzibel, also kann ein beliebiges α_i auf jedes α_j abgebildet werden. Nach Lemma 4.31 gilt $H = S_p$. □

4.33. Bemerkung (Nicht-Auflösbarkeit von Gleichungen fünften Grades)

$f = X^5 - 2X^4 + 2$ ist irreduzibel nach Eisenstein und besitzt genau zwei komplexe Nullstellen.

Da S_5 nicht auflösbar ist, ist auch f nicht auflösbar. ◊

4.4 Galoisgruppe & symmetrische Gruppe

4.34. Definition

Seien k ein Körper, $R = k[X_1, ..., X_n]$ und $K = \mathrm{Quot}(R) = k(X_1, ..., X_n)$. Dann heißen

$$\begin{aligned} s_0 &:= 1, \\ s_1 &:= X_1 + \cdots + X_n, \\ s_2 &:= X_1X_2 + \cdots + \cdots + X_{n-1}X_n, \ ..., \\ s_n &:= X_1 \cdot X_2 \cdots X_n \end{aligned}$$

bzw. allgemein für $\nu = 0, ..., n$

$$s_\nu := \sum_{\substack{1 \le i_1 \\ < \cdots < \\ i_\nu \le n}} X_{i_1} \cdots X_{i_\nu}$$

die elementaren symmetrischen Funktionen in $X_1, ..., X_n$.

4.35. Bemerkung

Für $\sigma \in S_n$ definiert $\varphi_\sigma(X_i) := X_{\sigma_i}$ einen Automorphismus φ_σ auf $k(X_1, ..., X_n)$. ◊

4.36. Satz

$K|k(s_1,...,s_n)$ ist eine Galoiserweiterung und es gilt $\mathrm{Gal}(K|k(s_1,...,s_n)) = \{\varphi_\sigma \mid \sigma \in S_n\} \cong S_n$.

Beweis.

Setze $L := \mathrm{Fix}(G) \supseteq k(s_1,...,s_n)$. Zu zeigen: $L = k(s_1,...,s_n)$. Betrachte das Polynom

$$f(X) := (X - X_1)\cdots(X - X_n) \in K[X] = \sum_{i=0}^{n} (-1)^i s_i X^{n-i} \in k(s_1,...,s_n)[X].$$

f ist irreduzibel über $k(s_1,...,s_n)$, da $G \cong S_n$ transitiv auf den Nullstellen von f operiert, und außerdem separabel. Es gilt

$$\mathrm{Zfk}(f, k(s_1,...,s_n)) = k(s_1,...,s_n)(X_1,...,X_n) = k(X_1,...,X_n) = K$$

Wegen $n! \geq [K : k(s_1,...,s_n)] \geq [K : L] = |G| = |S_n| = n!$ ist $[K : k(s_1,...,s_n)] = [K : L]$, d.h. $L = k(s_1,...,s_n)$. □

4.37. Definition

$f \in K$ heißt symmetrische Funktion, falls $\varphi_\sigma(f) = f$ für alle $\sigma \in S_n$, d.h. falls $f \in \mathrm{Fix}(G)$ mit $G = \{\varphi_\sigma \mid \sigma \in S_n\} \cong S_n$.

4.38. Bemerkung

Insbesondere gilt: Ist f symmetrisch, so ist $f \in k(s_1,...,s_n)$. ◊

4.39. Lemma

Die $n!$ Monome $X_1^{\nu_1}\cdots X_n^{\nu_n}$ mit $0 \leq \nu_j \leq n - j$ bilden eine Modulbasis von $k[X_1,...,X_n]$ über $k[s_1,...,s_n]$, d.h. jedes $f \in k[X_1,...,X_n]$ hat eine eindeutige Darstellung

$$f = \sum_{\substack{1\leq j\leq n \\ 0\leq \nu_j \leq n-j}} p_{\nu_1,...,\nu_n} X_1^{\nu_1}\cdots X_n^{\nu_n}$$

mit $p_{\nu_1,...,\nu_n} \in k[s_1,...,s_n]$.

Beweis.

Es ist

$$(X - X_1)\cdots(X - X_n) = \sum_{i=0}^{n} (-1)^i s_i X^{n-i},$$

d.h. X_1 ist Nullstelle eines normierten Polynoms über $k[s_1,...,s_n]$ vom Grad n. Setze $s := (s_1,...,s_n)$. Dann $X_1^n \in k[s]1 + k[s]X_1 + \cdots + k[s]X_1^{n-1}$, also sind X_1^{n+1}, X_1^{n+1}, ... $\in k[s] + k[s]X_1 + \cdots + k[s]X_1^{n-1}$. X_2 ist Nullstelle von $(X_2)\cdots(X - X_n) \in k[s][X_1][X]$ und dieses Polynom ist normiert vom Grad $n-1$, d.h. X_2^{n-1}, X_2^n, X_2^{n+1}, ... $\in k[s, X_1]1 + k[s, X_1]X_2 + \cdots + k[s, X_1]X_2^{n-2}$. $k[s, X_1] \subseteq k[s] + k[s]X_1 + \cdots + k[s]X_1^{n-1}$ u.s.w. ergibt: $k[s][X_1,...,X_n]$ wird als Modul über $k[s]$ von folgenden $n(n-1)(n-2)\cdots 2 = n!$ Monomen erzeugt:

$$X_1,\ ...,\ X_1^{n-1},\ X_2,\ ...,\ X_2^{n-2},\ X_1X_2,\ ...,\ ...,\ X_1^{n-1}X_2^{n-2},\ ...,\ ....$$

Dann wird der Körper $K = k(s)[X_1,...,X_n]$ über $k(s)$ von diesen Polynomen erzeugt und da gilt $[k(s)[X_1,...,X_n] : k(s)] = n!$, sind diese linear unabhängig über $k(s)$ bzw. $k[s]$. □

4.40. Bemerkung

k lässt sich auch durch einen beliebigen faktoriellen Ring ersetzen. ◊

4.41. Satz

Jedes symmetrische Polynom ist ein Polynom in $s_1, ..., s_n$.

Beweis.

Sei $f \in k[X_1, ..., X_n]$ symmetrisch. Dann ist $f \in k(s_1, ..., s_n)$ und mit Lemma 4.39 folgt:

$$f = \sum p_{\nu_1,...,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n}$$

mit $p_{\nu_1,...,\nu_n} \in k[s_1, ..., s_n]$, d.h. $f = p_{0,...,0} \in k[s_1, ..., s_n]$. Die Monome X^ν sind auch über $k(s_1, ..., s_n)$ linear unabhängig. □

4.42. Bemerkung

Die Galoisgruppe des Zerfällungskörpers von g über $k(s_1, ..., s_n)$ ist die symmetrische Gruppe S_n. ◊

5 Reelle Körper

5.1 Angeordnete Körper

5.1. Wiederholung

$\leq$ ist eine partielle Ordnung auf einer Menge A, falls für alle $a, b, c \in A$ gelten:

1. $a \leq a$,
2. $a \leq b$ und $b \leq c \Rightarrow a \leq c$ und
3. $a \leq b$ und $b \leq a \Rightarrow a = b$.

$\leq$ heißt lineare Ordnung, falls zusätzlich für alle $a, b \in A$ gilt:

4. $a \leq b$ oder $b \leq a$.

Wir schreiben $a < b$ für $a \leq b$ und $a \neq b$. ◊

5.2. Beispiel

$\subseteq$ als Mengeninklusion ist eine partielle Ordnung auf einer Menge von Mengen. ◊

5.3. Definition

$(K, \leq)$ heißt angeordneter Körper, wenn K ein Körper ist und $\leq$ eine lineare Ordnung auf K definiert mit
5. $a \leq b \Rightarrow a + c \leq b + c$ und
6. $0 \leq a, b \Rightarrow 0 \leq ab$ für alle $a, b \in K$.

5.4. Wiederholung

1. $a \leq b \Leftrightarrow 0 \leq b - a$.
2. $0 \leq a^2$, denn $0 \leq a$ oder $a \leq 0 \Leftrightarrow 0 \leq a$ oder $0 \leq -a$, also $0 \leq aa = (-a)(-a) = a^2$.
3. Insbesondere ist $0 < 1$.

5.5. Bemerkung

1. $\mathbb{C}$ ist kein angeordneter Körper, denn wäre $\leq$ eine Ordnung von $\mathbb{C}$, so $0 \leq i^2 = -1 \Rightarrow 1 \leq 0$.
2. $a \leq b$ und $c \leq d \Rightarrow a + c \leq b + d$. $a \leq b$ und $0 \leq c \Rightarrow 0 \leq bc - ac \Leftrightarrow ac \leq bc$.
3. $0 < a \Rightarrow 0 < a\frac{1}{a^2} = \frac{1}{a}$. Außerdem $0 < a < b \Rightarrow 0 < \frac{1}{b} < \frac{1}{a}$, denn $0 < b - a \Rightarrow 0 < \frac{b-a}{ab} = \frac{1}{a} - \frac{1}{b} \Leftrightarrow \frac{1}{b} < \frac{1}{a}$.
4. $0 < ab \Leftrightarrow 0 < \frac{a}{b}$.

5. $0 < n$ für alle $n \in \mathbb{N}$, denn induktiv erhalten wir $0 < 1 = 1^2$ und $0 < n \Rightarrow 1 < n+1 \Rightarrow 0 < n+1$.

6. Insbesondere hat jeder angeordnete Körper K die Charakteristik 0, d.h. $\mathbb{Q} \subseteq K$. ◊

5.6. Beispiel

1. $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$ sind angeordnete Körper.

2. $\mathbb{Q}(\sqrt{2}) := \mathbb{Q}[X]/X^2 - 2 = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2} = \mathbb{Q}(\overline{X})$. Betrachte den Automorphismus $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ mit $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ für $a, b \in \mathbb{Q}$ und die Einbettungen $\epsilon_1 : \mathbb{Q}(\sqrt{2}) \to \mathbb{R},\ a + b\overline{X} a + b\sqrt{2}$ und $\epsilon_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{R},\ a + b\overline{X} \mapsto a - b_+\sqrt{2}$, d.h. $\epsilon_2 = \epsilon_1 \circ \tau$. Wir definieren $\leq_1$ und $\leq_2$ auf $\mathbb{Q}(\sqrt{2})$: Seien $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$. Dann gelten:

   a) $a \leq_1 b :\Leftrightarrow \epsilon_1(\alpha) \leq \epsilon_1(\beta)$ in $\mathbb{R}$, d.h. insbesondere $0 <_1 \overline{X}$.

   b) $a \leq_2 b :\Leftrightarrow \epsilon_2(\alpha) \leq \epsilon_2(\beta)$ in $\mathbb{R}$, d.h. insbesondere $\overline{X} <_2 0$. ◊

5.7. Definition

$(K, \leq)$ heißt archimedisch geordnet, falls es zu jedem $\alpha \in K$ ein $n \in \mathbb{N}$ gibt mit $\alpha \leq n$.

5.8. Bemerkung

$\mathbb{R}(X)$ hat unendlich viele Anordnungen. Diese sind alle nicht-archimedisch. ◊

5.9. Lemma

Ist $(K, \leq)$ archimedisch geordnet, so liegt $\mathbb{Q}$ dicht in K, d.h. zu $a < b$ gibt es stets ein $r \in \mathbb{Q}$ mit $a < r < b$.

Beweis.

Sei $a < b \Rightarrow 0 < b - a \Rightarrow 0 < \frac{1}{b-a} < m$ für ein $m \in \mathbb{N}$, da K archimedisch ist. Damit $1 < m(b-a)$, also $ma < mb - 1$. Wähle $n \in \mathbb{Z}$ minimal mit $mb \leq n + 1$; dann $ma < mb - 1 \leq n < mb$, also $a < \frac{n}{m} < b$. □

5.10. Definition

$(K, \leq)$ heißt schnittvollständig, falls für alle $U, O \subseteq K$ mit $U, O \neq \emptyset$ und $U \leq O$ (d.h. $u \leq o$ für alle $u \in U,\ o \in O$) ein $a \in K$ existiert mit $U \leq \{a\} \leq O$.

$U \leq O$ heißt Dedekind-Schnitt, falls $U, O \neq \emptyset,\ U \leq O$ und $U \cup O = K$.

5.11. Lemma

Jeder schnittvollständige Körper $(K, \leq)$ ist archimedisch.

Beweis.

Gäbe es ein $a \in K$ mit $a > \mathbb{N}$, dann setze $U = \mathbb{N},\ O = \{x \in K \mid x \geq \mathbb{N}\}$. Damit $U, O \neq \emptyset$ und $U \leq O$, also gibt es ein $x \in K$ mit $U \leq x \leq O$. Dann $\mathbb{N} \leq x \Rightarrow \mathbb{N} < x - 1$, also $x - 1 \in O$. Dann folgt aber $x \leq x - 1$, Widerspruch. □

5.12. Satz (Hölder)

Jeder archimedisch angeordnete Körper $(K, \leq)$ lässt sich ordnungstreu in $(\mathbb{R}, \leq)$ einbetten, d.h. es gibt einen Epimorphismus $\rho : K \to \mathbb{R}$ mit $\alpha \leq \beta \Rightarrow \rho(\alpha) \leq \rho(\beta)$ für alle $\alpha, \beta \in K$.

Beweis.

Definiere $\rho_{|\mathbb{Q}} = \mathrm{id}$. Seien $a \in K,\ U_a := \{s \in \mathbb{Q} \mid s < a\}$ und $O_a := \{r \in \mathbb{Q} \mid a \leq r\}$. Damit gilt

$U_a \neq \emptyset,\ O_a \neq \emptyset$ und $U_a \cup O_a = \mathbb{Q}$. Betrachte nun $U_a,\ O_a$ in $\mathbb{R}$. Wähle $x \in \mathbb{R}$ mit $U_a \leq x \leq O_a$. Dann ist x eindeutig bestimmt, denn wäre $U_a \leq x' \leq O_a$, Œ $x < x'$, dann wähle $t \in \mathbb{Q}$ mit $x < t < x'$. Aus $t < x'$ folgt $t \in U_a$ und aus $x < t$ folgt $t \in O_a$, was unmöglich ist, da die Mengen disjunkt sind. Setze $\rho(a) = x$. Dann gelten $\rho(a+b) = \rho(a) + \rho(b)$ und $\rho(ab) = \rho(a)\rho(b)$ und ρ ist ordnungstreu. □

5.13. Korollar

$(\mathbb{R}, \leq)$ ist bis auf Isomorphie der einzige schnittvollständige, angeordnete Körper.

Beweis.

Sei $(K, \leq)$ schnittvollständig und damit auch archimedisch. Dann ist obiger Epimorphismus $\rho : K \to \mathbb{R}$ surjektiv. □

5.14. Definition

Sei $T \subseteq K$. T heißt Präordnung oder Präpositivbereich, falls gelten:

1. $T + T \subseteq T$,
2. $T \cdot T \subseteq T$,
3. $K^2 \subseteq T$,
4. $-1 \notin T$.

T heißt Positivbereich, falls zusätzlich gilt:

5. $T \cup -T = K$.

5.15. Bemerkung

Ist T ein Positivbereich, so folgt 3. $K^2 \subseteq T$ schon aus den anderen Axiomen, denn $a \in T \Rightarrow a^2 = aa \in T$ und $a \notin T \Rightarrow -a \in T \Rightarrow a^2 = (-a)(-a) \in T$. ◊

5.16. Beispiel

Sei $\leq$ eine Anordnung auf K. Dann ist $P_\leq := \{a \in K \mid a \geq 0\}$ ein Positivbereich. ◊

5.17. Bemerkung

Es gilt $P \cap -P = \{0\}$, denn gäbe es ein $x \in P \cap -P,\ x \neq 0$, dann $-1 = x(-x)(\frac{1}{x})^2 \in P$. ◊

5.18. Lemma

Sei $P \subseteq K$ ein Positivbereich. Dann definiert $a \leq b :\Leftrightarrow b - a \in P$ eine Anordnung auf K.

Beweis.

1. $a \leq a$ gilt, da $0 = 0^2 \in P$.
2. $a \leq b$ und $b \leq c \Rightarrow a \leq c$ gilt, da $P + P \subseteq P$.
3. $a \leq b$ und $b \leq a \Rightarrow a = b$, denn $b - a \in P$ und $-(b-a) \in P \Rightarrow b - a = 0 \Leftrightarrow b = a$.
4. Es gilt $a \leq b$ oder $b \leq a$, denn $P \cup -P = K$.
5. $a \leq b \Rightarrow a + c \leq b + c$ nach Definition von $\leq$.
6. $0 \leq a, b \Rightarrow 0 \leq ab$ folgt aus $P \cdot P \subseteq P$. ◊

5.19. Bemerkung

Wegen $P_{\leq_P} = P$ und $\leq_{P_\leq} = \leq$, entsprechen sich Anordnungsaxiome und Positivbereich bijektiv. ◊

5.20. Lemma

Seien $T \subseteq K$ eine Präordnung und $x \notin T$. Dann ist $T' := T - xT$ eine Präordnung.

Beweis.

1. Es gilt $T' + T' \subseteq T'$, da T additiv abgeschlossen ist.
2. Es gilt $T' \cdot T' \subseteq T - xT + x^2T \subseteq T - xT = T'$.
3. Es gilt $K^2 \subseteq T'$, da bereits $K^2 \subseteq T$.
4. Falls $-1 = t_1 - xt_2,\ t_1, t_2 \in T$ mit $t_2 \neq 0$, dann läge auch $x = (t_1 + 1)\frac{t_2}{t_2^2}$ in T. ◊

5.21. Lemma

Es gilt: T ist bzgl. $\subseteq$ eine maximale Präordnung $\Leftrightarrow$ T ist ein Positivbereich.

Beweis.

$\Rightarrow$ Sei $x \notin T$. Dann $-x \in T - xT \supseteq T$ und da T maximal, gilt $T = T - xT \Rightarrow -x \in T$.

$\Leftarrow$ Wir nehmen an, dass $T \subsetneq T'$. Sei $x \in T' \backslash T$, dann $-x \in T \Rightarrow -x \in T'$, also $x \in T' \cap -\widetilde{T'}$. Dann gilt aber $x = 0$, was unmöglich ist, da $x \notin T$. □

5.22. Satz

Sei T eine Präordnung. Dann gilt:

$$T = \bigcap_{\substack{P \supseteq T \\ P \text{ Positivbereich}}} P.$$

Beweis.

$\subseteq$ Klar nach Konstruktion.

$\supseteq$ Wir nehmen an, es gibt $x \in \bigcap\{P \supseteq T \mid P \text{ Positivbereich}\}$ mit $x \notin T$. $T' := T - xT \supseteq T$ ist eine Präordnung. Mit Zorns Lemma wählen wir eine maximale Präordnung Q über T'. Dann ist Q ist ein Positivbereich mit $T \subseteq Q$. Weiter gilt $-x \in T' \subseteq Q$ und $x \in Q$. Also ist $x \in Q \cap -Q = \{0\}$, ein Widerspruch. □

5.23. Bemerkung

Betrachte die Menge aller Quadratsummen über K,

$$\sum K^2 := \left\{ \sum_{i=1}^{n} a_i^2 \;\middle|\; n \in \mathbb{N},\ a_i \in K \right\}.$$

Es gilt

$$\sum K^2 + \sum K^2 \subseteq \sum K^2, \qquad \sum K^2 \cdot \sum K^2 \subseteq \sum K^2 \qquad \text{und} \qquad K^2 \subseteq \sum K^2. \qquad \text{◊}$$

Dies motiviert zu folgendem Lemma:

5.24. Lemma

Es gilt: K besitzt eine Anordnung $\Leftrightarrow$ $-1 \notin \sum K^2$.

Beweis.

$\Rightarrow$ Klar, da $\sum a^2 > 0$ für alle $a \in K$.

$\Leftarrow$ Sei $-1 \notin \sum K^2$, dann ist $\sum K^2$ eine Präordnung. Wähle mit Zorns Lemma eine maximale Präordnung P über $\sum K^2$. Dann ist P ein Positivbereich. □

5.25. Definition

Ein Körper K heißt reeller Körper, wenn er eine Anordnung besitzt.

5.26. Bemerkung

1. Nach Lemma 5.24 wäre eine äquivalente Formulierung: $-1 \notin \sum K^2$.
2. Ist K reell, dann ist $\sum K^2$ in allen Präordnungen von K enthalten. ◊

5.2 Fortsetzungen von Anordnungen

5.27. Wiederholung

Sei $L|K$ eine Körpererweiterung. $(K, \leq_1) \subseteq (L, \leq_2) :\Leftrightarrow$ für alle $a, b \in K$ gilt: $a \leq_1 b \Leftrightarrow a \leq_2 b$.

äquivalente Formulierung: $(K, P_1) \subseteq (L, P_2) :\Leftrightarrow P_2 \cap K = P_1$. ◊

5.28. Lemma

Es sind äquivalent:

1. Ein Positivbereich P von K lässt sich auf L fortsetzen.
2. $T_L(P) := \left\{ \sum_{i=1}^{n} p_i \beta_i^2 \mid n \in \mathbb{N},\ p_i \in P,\ \beta_i \in L \right\}$ ist eine Präordnung von L.

Beweis.

$\Rightarrow$ Sei $(K, P) \subseteq (L, P')$, dann $T_L(P) + T_L(P) \subseteq T_L(P)$, $T_L(P) \cdot T_L(P) \subseteq T_L(P)$ und $L^2 \subseteq T_L(P)$. Weiter gilt $T_L(P) \subseteq P'$, denn alle Summanden liegen in P', also auch die ganze Summe. Wegen $-1 \notin P'$ liegt auch -1 nicht in $T_L(P)$.

$\Leftarrow$ Seien $T_L(P)$ eine Präordnung und $P' \supseteq T_L(P)$ Positivbereich von L. Dann ist $P'' := P' \cap K \supseteq P$ Positivbereich von K. Damit $P = P''$, da Positivbereiche maximale Präordnungen sind. □

5.29. Satz

Seien $L = K(\sqrt{a})$, $a \in K \backslash K^2$ und P ein Positivbereich von K. Dann gilt:

P hat eine Fortsetzung auf $L \Leftrightarrow a \in P$.

Beweis.

$\Rightarrow$ Sei $(K, P) \subseteq (L, P')$. Dann gilt für jedes $a \in L$, dass $a = (\sqrt{a})^2 \in P' \cap K = P$.

$\Leftarrow$ Sei $a \in P$. Wir zeigen: $-1 \notin T_L(P)$. Läge -1 in $T_L(P)$, d.h. $-1 = \sum a_i (x_i + y_i \sqrt{a})^2$ mit $a_i \in P$ und $x_i, y_i \in K$, dann $-1 = \sum a_i x_i^2 + a_i a y_i^2 \in P$, ein Widerspruch. Nach Lemma 5.28 ist P damit fortsetzbar. □

5.30. Beispiel

1. $(\mathbb{Q}, \leq)$ lässt sich auf $\mathbb{Q}(\sqrt{2})$ fortsetzen.
2. $(\mathbb{Q}, \leq)$ lässt sich nicht auf $\mathbb{Q}(\sqrt{-2})$ fortsetzen. ◊

5.31. Satz

Sei $[L : K] = 2n + 1$. Dann lässt sich jeder Positivbereich P von K auf L fortsetzen.

Beweis.

Angenommen, es gäbe ein Gegenbeispiel (L, K, P) von minimalem Grad. Nach dem Satz vom primitiven

Element 4.18 gilt: $L = K(\alpha) = K[X]/(f)$ mit $f = \mathrm{Irr}(\alpha, K)$, $\deg f = 2n+1$. Nach Annahme liegt -1 in $T_L(P)$, d.h. es gibt $a_i \in P$ und $\gamma_i \in L$ mit $-1 = \sum a_i \gamma_i^2$ in $K[X]/(f)$. Also gilt

$$1 + \sum_i a_i f_i^2 = fh \qquad (*)$$

für gewisse $f_i, h \in K[X]$, Œ $\deg f_i \leq 2n$. Die linke Seite von $(*)$ hat geraden Grad (da Leitkoeffizienten von $a_i f_i^2$ aus P sind, können sich die Leitmonome nicht gegenseitig auslöschen) und dieser Grad beträgt höchstens $4n$. Also hat h ungeraden Grad von höchstens $2n-1$. Wähle einen irreduziblen Faktor h_1 von h mit ungeradem Grad. Sei β eine Nullstelle von h_1. Dann ist $(K(\beta), K, P)$ ein Gegenbeispiel von echt kleinerem Grad als (K, L, P). Setzt man β in $(*)$ ein, ergibt sich $1 + \sum a_i f_i^2(\beta) = 0$. Wegen $-1 \in T_{K(\beta)}(P)$ lässt sich P auf $K(\beta)$ nicht fortsetzen, ein Widerspruch. □

5.32. Satz

Jeder Positivbereich P von K lässt sich auf $K(X)$ fortsetzen.

Beweis.

X ist transzendent über K. Wir nehmen an, -1 liegt in $T_{K[X]}(P)$, d.h. $-1 = \sum_i a_i f_i^2$ für gewisse $f_i \in K[X]$. Schreibe $f_i = \frac{g_i}{h}$ mit $g_i, h \in K[X]$ und Œ teile kein irreduzibler Faktor von h alle g_i, also $h^2 + \sum_i a_i g_i^2 = 0$. Einsetzen von 0 liefert $h^2(0) + \sum_i a_i g_i^2(0) = 0$ und alle Summanden liegen in P, also $0 = h(0) = g_i(0)$ für alle i. Damit $X \mid h$ und $X \mid g_i$ für alle i, ein Widerspruch. □

5.3 Reell abgeschlossene Körper

5.33. Definition

Ein angeordneter Körper $(K, \leq)$ heißt maximal angeordnet, falls sich $\leq$ auf keine echte algebraische Erweiterung von K fortsetzen lässt.

Ein reeller Körper K heißt reell abgeschlossen, wenn er keine echte algebraische reelle Erweiterung besitzt.

5.34. Lemma

Ist $(K, \leq)$ maximal angeordnet, so ist jedes nicht-negative Element von K ein Quadrat.

Insbesondere ist $\leq$ die einzige Anordnung auf K.

Beweis.

Sei $a \in K$, $a \geq 0$. Angenommen, $a \notin K^2$. Dann ist $K(\sqrt{a})$ eine echte Erweiterung von K, auf die sich $\leq$ fortsetzen lässt, da $a \geq 0$, ein Widerspruch. Also ist $P_\leq = K^2$. Ist Q nun ein weiterer Positivbereich von K, dann $P_\leq \subseteq Q$ und damit $Q = P_\leq$ wegen der Maximalität von $P_\leq$. □

5.35. Lemma

K ist reell abgeschlossen $\Leftrightarrow$ K besitzt genau eine Anordnung $\leq$ und $(K, \leq)$ ist maximal angeordnet.

Beweis.

$\Rightarrow$ Sei P ein Positivbereich von K. Dann ist (K, P) maximal angeordnet. Also ist nach Lemma 5.34 P die einzige Anordnung von K.

$\Leftarrow$ Hätte K eine echte algebraische reelle Erweiterung L, so hätte L eine Anodnung, welche die einzige Anordnung $\leq$ von K fortsetzen würde, was im Widerspruch dazu steht, dass $(K, \leq)$ bereits maximal angeordnet ist. □

5.36. Satz (Artin & Schreier, 1926)

Es sind äquivalent:

1. K ist reell abgeschlossen.
2. K^2 ist Positivbereich von K und jedes $f \in K[X]$ von ungeradem Grad hat eine Nullstelle in K.
3. $K \neq K(\sqrt{-1})$ und $K(\sqrt{-1})$ ist algebraisch abgeschlossen.

Beweis.

1. (1) $\Rightarrow$ (2): Ist K reell abgeschlossen, dann ist K^2 ein Positivbereich. Sei $p \in K[X]$ mit $\deg p$ ungerade. Zu zeigen: p hat eine Nullstelle in K. Œ sei p irreduzibel. Dann lässt sich $P = K^2$ auf $K[X]/(p)$ fortsetzen. Wegen $K[X]/(p) = K$ hat p eine Nullstelle in K.
2. (3) $\Rightarrow$ (1): Wir zeigen $K^2 + K^2 = K^2$. Seien $a, b \in K$. Es gilt $a + b\sqrt{-1} = (x + y\sqrt{-1})^2$ für gewisse $x, y \in K$, d.h. $x^2 - y^2 = a$ und $2xy = b$. Also $a^2 + b^2 = x^4 - 2x^2y^2 + y^4 + 4x^2y^2 = (x^2 + y^2)^2 \in K^2$. Weiter gilt: $-1 \notin K^2$, also insbesondere $-1 \notin \sum K^2$, d.h. $\sum K^2$ bildet eine Präordnung. Damit gibt es auf K eine Anordnung, d.h. K ist reell.

   Sei nun L eine algebraische Erweiterung von K. Da $K(\sqrt{-1})$ der algebraische Abschluss von K ist, gilt $K \subseteq L \subseteq K(\sqrt{-1})$. Aus $[K(\sqrt{-1}) : K] = 2$ folgt dann $L = K$ oder $L = K(\sqrt{-1})$. Auf $K(\sqrt{-1})$ gibt es aber keine Anordnung.
3. (2) $\Rightarrow$ (3): Dies ist der Fundamentalsatz der Algebra.

6 Übungsaufgaben

6.1 Aufgaben zur Gruppentheorie

6.1. Aufgabe

Seien G eine Gruppe und $\mathrm{Z}(G) := \{a \in G \mid \forall x \in G : ax = xa\}$ ihr Zentrum. Man zeige:

1. $\mathrm{Z}(G)$ ist eine abelsche Untergruppe von G.
2. $\mathrm{Z}(G) \lhd G$.
3. Ist $G/\mathrm{Z}(G)$ zyklisch, dann ist G abelsch. ◊

6.2. Aufgabe

Seien G_1, G_2 Gruppen, $H_1 < G_1$, $H_2 < G_2$ und $f : G_1 \to G_2$ ein Gruppenhomomorphismus. Man zeige oder widerlege:

1. $H_1 \lhd G_1 \Rightarrow f(H_1) \lhd G_2$.
2. $H_2 \lhd G_2 \Rightarrow f^{-1}(H_2) \lhd G_1$. ◊

6.3. Aufgabe

Sei G eine endliche Gruppe. Man zeige:

1. Ist H eine p-Sylow-Untergruppe von G, dann gilt: $H \lhd G \Leftrightarrow H$ ist einzige p-Sylow-Untergruppe von G.
2. Gibt es Primzahlen p, q mit $pq^2 = |G|$, so besitzt G eine p- oder eine q-Sylow-Untergruppe, die Normalteiler von G ist. ◊

6.4. Aufgabe

Seien G eine endliche Gruppe, $H < G$, p die kleinste Primzahl, die $|G|$ teilt, und $X := \{gH \mid g \in G\}$ die Menge der Linksnebenklassen von H und es gelte $|X| = p$.

Man zeige: H ist ein Normalteiler von G. ◊

6.5. Aufgabe

1. Man zeige, dass je zwei m-Zykel in S_n zueinander konjugiert sind.
2. Man bestimme die Anzahl der n-Zykel in S_n. ◊

6.6. Aufgabe

Man zeige, dass $(1\ 2)$ und $(1\ 2\ \cdots\ n)$ die Gruppe S_n erzeugen. ◊

6.7. Aufgabe

Seien p eine Primzahl und H eine Untergruppe von S_p. Für alle $i, j \in \{1, ..., p\}$ gebe es ein $\sigma \in H$ mit $\sigma(i) = j$. Weiter enthalte H eine Transposition.

Man zeige, dass $H = S_p$. ◊

6.8. Aufgabe

Seien G eine Gruppe und $a \in G$.

1. Man zeige: Die Konjugation $\rho_a : G \to G,\ b \mapsto aba^{-1}$ ist ein Automorphismus.
2. Weiter gebe man sowohl für eine abelsche als auch für eine nicht-abelsche Gruppe einen Automorphismus an, der keine Konjugation ist. ◊

6.9. Aufgabe

Seien G eine Gruppe, $N \lhd G$ und es gebe keine echte Zwischengruppe von N und G.

Man zeige, dass je zwei Untergruppen $H_1 \neq \{1\}$ und $H_2 \neq \{1\}$ von G mit $N \cap H_1 = N \cap H_2 = \{1\}$ isomorph zueinander sind. ◊

6.10. Aufgabe

Die Diedergruppe D_n ist für jedes $n \geq 2$ auflösbar. ◊

6.11. Aufgabe

Seien G eine endliche Gruppe, X eine endliche Menge und $\circ : G \times X \to X,\ (g, x) \mapsto g \circ x$ eine Gruppenoperation. Weiter bezeichnen $F(g) := |\{x \in X \mid gx = x\}|$ die Anzahl der Fixpunkte von g in X und s die Anzahl der Bahnen in X.

Man zeige: $s = \frac{1}{|G|} \sum\limits_{g \in G} F(g)$. ◊

6.12. Aufgabe

Seien G eine endliche Gruppe, $H < G$ und es gelte $G = \bigcup\limits_{g \in G} gHg^{-1}$. Man zeige, dass $G = H$. ◊

6.13. Aufgabe

Jede Gruppe G der Ordnung $2^n 3$ hat einen Normalteiler vom Index 2 oder 3. ◊

6.14. Aufgabe

Man gebe eine Gruppe G und eine Gruppenoperation auf $\mathbb{C}$ an, deren Bahnen gerade die Mengen

$$B_r := \{z \in \mathbb{C} \mid |z| = r\}$$

mit $r \in \mathbb{R}_0^+$ sind. ◊

6.15. Aufgabe

Seien G eine Gruppe, X eine Menge und $G \times X \to X,\ (g, x) \mapsto gx$ eine Gruppenoperation.

1. Man zeige: Liegen $x_1, x_2 \in X$ in der selben Bahn (das heißt $Gx_1 = Gx_2$), so sind die zugehörigen Fixgruppen G_{x_1} und G_{x_2} zueinander konjugiert.
2. Weiter zeige man, dass die Umkehrung im Allgemeinen nicht gilt. ◊

6.2 Aufgaben zur Ringtheorie

6.16. Aufgabe

Sei R ein kommutativer Ring mit 1. Für Ideale I, J in R definiert man

$$I : J := \{x \in R \mid \forall b \in J : bx \in I\}.$$

Man zeige:

1. $I : J$ ist ein Ideal.
2. Für alle Ideale I, J, K in R gilt $(I : J) : K = I : (J \cdot K)$.
3. Ist R ein Integritätsbereich und sind I, J und $I + J$ Hauptideale in R, so ist auch $I : J$ ein Hauptideal in R. ◊

6.17. Aufgabe

Seien R ein kommutativer Ring mit 1 und $I_1, ..., I_n$ Ideale in R mit $I_i + I_j = R$ für alle $i, j \in \{1, ..., n\}$ mit $i \neq j$.

Dann gilt

$$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n.$$ ◊

6.18. Aufgabe

Für jede Primzahl p bezeichne $\mathbb{F}_p$ den Körper $\mathbb{Z}/(p)$. Man zeige:

1. $\mathbb{F}_2[X]/(X^3 + X + 1)$ ist ein Körper.
2. $\mathbb{F}_3[X]/(X^3 + X + 1)$ ist kein Körper. ◊

6.19. Aufgabe

Gegeben sei $R := \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Man zeige:

1. R ist ein Noetherscher Integritätsbereich.
2. 2 ist irreduzibel in R, aber nicht prim.
3. R ist nicht faktoriell. ◊

6.20. Aufgabe

Seien R ein kommutativer Ring mit 1, $S \subseteq R$ eine multiplikative Menge, d.h. $1 \in S$ und $SS \subseteq S$, und I ein Ideal in R mit $I \cap S = \emptyset$. Man zeige:

1. Die Menge aller Ideale J in R mit $I \subseteq J$ und $J \cap S = \emptyset$ besitzt ein maximales Element.
2. Jedes solche maximale Element ist ein Primideal. ◊

6.21. Aufgabe

Seien A ein kommutativer Ring mit 1, $\mathrm{Spec}(A) := \{I \subseteq A \mid I \text{ Primideal in } A\}$ und $K \subseteq \mathrm{Spec}(A)$ eine nicht-leere Kette in $\mathrm{Spec}(A)$.

Man zeige: $\bigcap K \in \mathrm{Spec}(A)$, d.h. der Schnitt aller Primideale in K ist wieder ein Primideal. ◊

6.22. Aufgabe

Seien A ein kommutativer Ring mit 1 und $p \in \mathrm{Spec}(A)$.

Man zeige, dass $\mathrm{Spec}(A)$ dann ein minimales Element q besitzt mit $q \subseteq p$. ◊

6.23. Aufgabe

Seien $B \subseteq A$ Ringe mit 1 und $q \in \mathrm{Spec}(A)$ minimal.

Man zeige, dass es ein $p \in \mathrm{Spec}(A)$ minimal gibt mit $p \cap B = q$. ◊

6.24. Aufgabe

Man untersuche die folgenden Polynome auf Irreduzibilität in $\mathbb{Q}[X]$:

1. $p_a := X^4 - 9X^3 - 6X + 3$
2. $p_b := X^6 + X^3 + X + 1$
3. $p_c := 2X^3 - 5X + 1$
4. $p_d := X^4 + 1$
5. $p_e := 2X^4 + 6X^3 - 54X^2 + 18X + 6$. ◊

6.25. Aufgabe

Seien R ein kommutativer Ring mit 1, I, J Ideale in R und p ein Primideal in R.

Man zeige: $IJ \subseteq p \Rightarrow I \subseteq p$ oder $J \subseteq p$. ◊

6.3 Aufgaben zur Körpertheorie

6.26. Aufgabe

Seien R ein faktorieller Integritätsbereich mit Quotientenkörper K, $f \in R[X]$ ein normiertes Polynom und $a \in K$ mit $f(a) = 0$.

Man zeige: $a \in R$. Weiter folgere man für $m, n \in \mathbb{N}$:

$$\sqrt[m]{n} \in \mathbb{N} \qquad \Longleftrightarrow \qquad \sqrt[m]{n} \in \mathbb{Z}.$$ ◊

6.27. Aufgabe

Gesucht ist das Minimalpolynom von $\sqrt{2} + \sqrt{5}$ über $\mathbb{Q}$. ◊

6.28. Aufgabe

Man zeige, dass es ein $a \in \mathbb{R}$ gibt mit $a^3 - a^2 + a + 2 = 0$, und bestimme das Minimalpolynom von a über $\mathbb{Q}$. ◊

6.29. Aufgabe

Es sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Man zeige, dass $\mathrm{Kon}(M)$ ein Oberkörper von $\mathbb{Q}(M \cup \overline{M})$ ist. ◊

6.30. Aufgabe

Sei $M \subseteq \mathbb{C}$ mit $0, 1 \in M$. Dann gilt: $a \in \mathrm{Kon}(M) \Rightarrow \sqrt{a} \in \mathrm{Kon}(M)$. ◊

6.31. Aufgabe

Gesucht sind die Zerfällungskörper und deren Grade über $\mathbb{Q}$ von

1. $X - 18$,
2. $X^2 - 2$,
3. $X^4 + X^2 + 1$ und
4. $X^5 - 1$. ◊

6.32. Aufgabe

Gegeben seien die Körper K und L sowie der Ring R. Es gelte $K \subseteq R \subseteq L$ und die Körpererweiterung $L|K$ sei algebraisch.

Man zeige, dass dann auch R ein Körper ist. ◊

6.33. Aufgabe

Gegeben seien der Körper K und ein Polynom $f \in K[X]$ vom Grad $n \in \mathbb{N}_0$. L bezeichne den Zerfällungskörper von f über K. Man zeige: $[L : K] \mid n!$ (in $\mathbb{Z}$). ◊

6.34. Aufgabe

Seien $L|K$ eine Körpererweiterung, $a \in K,\ f := X^n - a \in K[X]$ irreduzibel in $K[X]$ und $b \in L$ Nullstelle von f.

Man zeige, dass für alle $m \in \mathbb{Z}$ gilt:

$$[K(b^m) : K] = \frac{n}{\mathrm{ggT}(m, n)}$$ ◊

6.35. Aufgabe

Seien $L|K$ eine algebraische Körpererweiterung und jedes Polynom aus $K[X]$ zerfalle über L.

Man zeige, dass L dann algebraisch abgeschlossen ist. ◊

6.36. Aufgabe

Sei K ein endlicher Körper mit $\mathrm{char}(K) = p$.

1. Man zeige: Es gibt ein $n \in \mathbb{N}$ mit $|K| = p^n$.
2. Weiter zeige man: Sind p prim, $n \in \mathbb{N}$ und $|K| = p^n$, dann ist K der Zerfällungskörper des Polynoms $X^{p^n} - X \in \mathbb{F}_p[X]$ über $\mathbb{F}_p$. ◊

6.37. Aufgabe

Gegeben seien nun ein primes p, ein $\in \mathbb{N},\ q := X^{p^n} - X \in \mathbb{F}_p[X]$ und $L = \mathrm{Zfk}(q, \mathbb{F}_p)$.

Zu beweisen sind folgende Aussagen:

1. q hat nur einfache Nullstellen in L.
2. $K := \{a \in L \mid a^{p^n} = a\}$ ist ein Unterkörper von L.
3. $L = K$.
4. $|K| = p^n$. ◊

6.38. Aufgabe

1. Man zeige: Zu jedem endlichen Körper K gibt es genau ein Paar $(p, n)\mathbb{N} \times \mathbb{N}$ mit p prim und $|K| = p^n$.
2. Weiter weise man nach, dass es zu jedem Paar $(p, n) \in \mathbb{N} \times \mathbb{N}$ mit p prim (bis auf Isomorphie) genau einen endlichen Körper K mit $|K| = p$ gibt.

   Dieser ist der Zerfällungskörper von $X^{p^n} - X \in \mathbb{F}_p[X]$ über $\mathbb{F}_p$. ◊

6.39. Aufgabe

Seien $L|K$ eine normale, algebraische Körpererweiterung, $\overline{L}$ der algebraischer Abschluss von L. Seien $x, y \in L$.

Man zeige die äquivalenz folgender Aussagen:

1. x und y haben das selbe Minimalpolynom über K.
2. Es gibt einen Automorphismus der Körpererweiterung $L|K$, der x auf y abbildet.
3. Es gibt einen Automorphismus der Körpererweiterung $\overline{L}|K$, der x auf y abbildet. ◊

6.40. Aufgabe

Seien K ein Körper und $f \in K[X]$ irreduzibel mit Zerfällungskörper L.

Man zeige, dass alle Nullstellen von f in L die selbe Vielfachheit haben. ◊

6.4 Aufgaben zur Galoistheorie

6.41. Aufgabe

Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

1. Man bestimme $[K : \mathbb{Q}]$.
2. Warum ist $K|\mathbb{Q}$ eine Galoiserweiterung?
3. Man bestimme $|\mathrm{Gal}(K|\mathbb{Q})|$.
4. Welche Gruppen der Ordnung 4 gibt es?
5. Wie viele Untergruppen hat $\mathbb{Z}_4$?
6. Man zeige: $\mathrm{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
7. Man gebe alle Zwischenkörper von $K|\mathbb{Q}$ an.
8. Man zeige: $\mathbb{Q}(\sqrt{2} + \sqrt{5}) = K$. ◊

6.42. Aufgabe

Seien $f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$ und K der Zerfällungskörper von f über $\mathbb{Q}$.

1. Man zeige: f ist irreduzibel in $\mathbb{Q}[X]$.
2. Man rechne nach, dass für alle $a \in K$ mit $f(a) = 0$ gilt: $f(a^2 - 2) = 0$ und $K = \mathbb{Q}(a)$.
3. Man bestimme $[K : \mathbb{Q}]$.
4. Man zeige: $\mathrm{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_3$. ◊

6.43. Aufgabe

Sei $K = 0, 1, a, b$ ein Körper mit 4 Elementen. Man zeige:

1. $\mathrm{char}(K) = 2$ (das heißt $1 + 1 = 0$ in K).
2. Für alle $x \in K$ gilt $x^2 = 1 \Rightarrow x = 1$.
3. Weiter gebe man (ohne Begründung) eine Additions- und Multiplikationstabelle für K an. ◊

6.44. Aufgabe

Seien K ein Körper mit $\mathrm{char}(K) \neq 2$ (d.h. $2 = 1 + 1 \neq 0$ in K) und die Körpererweiterung $L|K$ vom Grad 2^n habe die Gestalt $L = K(\sqrt{a_1}, ..., \sqrt{a_n})$ mit $a_1, ..., a_n \in K$. Sei $x := \sqrt{a_1} + \cdots + \sqrt{a_n}$.

Man zeige:

1. $L|K$ ist eine Galoiserweiterung.
2. Es gibt kein $\sigma \in \mathrm{Gal}(L|K(x))$ mit $\sigma \neq \mathrm{id}_L$.
3. $L = K(x)$. ◊

6.5 Aufgaben zur Theorie angeordneter Körper

6.45. Aufgabe

Seien $(K, \leq)$ ein archimedisch angeordneter Körper, $U_a := \{r \in \mathbb{Q} \mid r < a\}$, $O_a := \{r \in \mathbb{Q} \mid a \leq r\}$ und $\rho : K \to \mathbb{R}$ eine Abbildung mit $U_a \leq \rho(a) \leq O_a$.

Man zeige:

1. ρ ist ein Ringhomomorphismus.
2. Für alle $a, b \in K$ gilt: $a \leq b \Leftrightarrow \rho(a) \leq \rho(b)$.
3. Ist $(K, \leq)$ schnittvollständig, dann ist ρ ein Isomorphismus angeordneter Körper. ◊

6.46. Aufgabe

Seien K ein Körper und P ein Positivbereich von K. Man zeige:

1. $K^2 \subseteq P$ und $P \cap -P = \{0\}$.
2. Ist $\subseteq$ eine Anordnung von K, dann ist $P_{\leq} := \{a \in K \mid a \geq 0\}$ ein Positivbereich von K.
3. Ist P ein Positivbereich von K, so wird durch $a \leq_P b :\Leftrightarrow b - a \in P$ $(a, b \in K)$ eine Anordnung von K definiert.
4. Durch $\leq \mapsto P_{\leq}$ und $P \mapsto \leq_P$ werden zueinander inverse Bijektionen zwischen der Menge der Anordnungen von K und der Menge der Positivbereiche von K definiert. ◊

6.47. Aufgabe

Für ein Polynom $f \in \mathbb{R}[X]$ bezeichne $\mathrm{lc}(f)$ seinen Leitkoeffizienten.

1. Man zeige, dass

$$P := \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{R}[X],\ g \neq 0,\ f = 0 \text{ oder } \mathrm{lc}(fg) > 0 \right\} \subseteq \mathbb{R}(X)$$

   ein Positivbereich von $\mathbb{R}(X)$ ist.
2. Weiter zeige man, dass seine zugehörige Anordnung $\leq_P$ nicht archimedisch ist. ◊

6.48. Aufgabe

Man zeige, dass der Körper

$$K := \mathbb{Q}(X)(\sqrt{-(1 + X^2)})$$

(X eine Unbestimmte) sich nicht anordnen lässt. ◊

Index