Algebra 1

Mitschrift von www.kuertz.name

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

Klaas Ole Kürtz (klaasole@kuertz.net)

Inhaltsverzeichnis

Organisatorisches

- Inhalt der Vorlesung: **Körpertheorie**
- **Ziel**: Bestimmung aller Körper
- **Idee**: kleinste Körper $\rightarrow$ Körpererweiterungen
- **Anwendungen**:
  1. Lösung z.B. der Gleichung $x^2+px+q=0 \Rightarrow x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$ (in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$); Gibt es ähnliche Formeln für $x^n + ... + a_1 \cdot x + a_0 = 0$?

     Ja, falls $n \leq 4$ (1545 Cardano: Ars Magna), 1826 hat Abel in „Crelle J. f. d. r. u. a. Mathematik 1" gezeigt, daß dies für $n = 5$ nicht gelingt. Galois zeigte dies 1832 für $n \geq 5$.
  2. Sind gewisse Konstruktionen mit Zirkel und Lineal möglich (Kubus mit doppeltem Volumen, Dreiteilung eines Winkels, 17-Eck)?
- Literatur[1]:
  - E. Artin: Galoissche Theorie, Teubner, Leipzig 1965
  - G. Fischer, R. Sacher: Einführung in die Algebra, Teubner 1974
  - B. Hornfeck: Algebra, 3. Auflage, deGruyter 1976
  - I. M. Isaacs: Algebra - a produate course, Brooks/Cole 1993
  - N. Jacobsen: Lecutres in abstract algebra III, von Norstrand 1964 bzw. Springer 1975
  - N. Jacobsen: Basic Algebra I, Freeman 1974
  - O. Körner: Algebra, 2. Auflage, Aula 1990
  - S. Lang: Algebra, Addison-Wesley 1965
  - F. Lorenz: Einführung in die Algebra I, BI Wissenschatfverlag 1987
  - I. Steward: Galois Theory, 2. Auflage, Chapman and Hall 1989
  - B. L. v. d. Waerden: Algebra I (+ II), original Springer 1930, 9. Auflage 1993

[1] „Man muß sich schon anstrengen, um ein schlechtes Buch über dieses Thema zu schreiben."

1 Grundlagen

1.1 Teilringe von Körpern

1.1.1 Ringe und Teilringe

DEFINITIONEN:

- Eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring*, falls gilt:
  1. $(R, +)$ ist eine abelsche Gruppe.
  2. $(ab)c = a(bc)$ für alle $a, b, c \in R$
  3. $(a + b)c = ac + bc$ und $a(b + c) = ab + ac$ für alle $a, b, c \in R$
- Der Ring R heißt
  - *kommutativ*, wenn $ab = ba$ für alle $a, b \in R$
  - *Ring mit Eins*, wenn $I \in R \setminus \{0\}$ existiert mit $Ia = aI = a$ für alle $a \in R$
  - *Schiefkörper*, wenn $(R \setminus \{0\}, \cdot)$ eine Gruppe ist
  - *Körper*, wenn $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist
- Die Teilmenge T des Ringes R heißt ein *Teilring (Teilkörper)* von R, wenn T mit den Einschränkungen der auf R erklärten Verknüpfungen $+, \cdot$ ein Ring (Körper) ist.

  Es ergeben sich folgende Möglichkeiten:
  - Teilring eines Ringes, z.B. $2\mathbb{Z}$ von $\mathbb{Z}$ (schreibe $2\mathbb{Z} \leq \mathbb{Z}$)
  - Teilring eines Körpers, z.B. $\mathbb{Z}$ von $\mathbb{Q}$
  - Teilkörper eines Ringes, z.B. $\mathbb{R}$ von $\mathbb{R} \times \mathbb{R}$ oder $\mathbb{R}$ von $\mathbb{R}[x]$
  - Teilkörper eines Körpers, z.B. $\mathbb{Q}$ von $\mathbb{R}$ (schreibe $\mathbb{Q} \leq \mathbb{R}$)

LEMMA: Sei R ein Ring, $T \subseteq R$. T ist ein Teilring von R genau dann, wenn

1. $T \neq \emptyset$ und
2. $a, b \in T \Rightarrow a - b \in T, a \cdot b \in T$

1.1.2 Nullteiler, Integritätsbereiche

DEFINITIONEN:

- Ein Element $a \in R$ mit $a \neq 0$ heißt *Nullteiler*, wenn es ein $b \in R \setminus \{0\}$ gibt, so daß $a \cdot b = 0$ ist.

  Ist R ein Teilring des Körpers K und $a \in R$ mit $a \neq 0$, so folgt aus $a \cdot b = 0$ wegen $a^{-1} \in K$, daß $0 = a^{-1}(ab) = b$. Insbesondere hat R keine Nullteiler.

- Ein kommutativer Ring ohne Nullteiler heißt *Integritätsbereich*.

LEMMA: Jeder Teilring eines Körpers ist ein Integritätsbereich.

1.1.3 Quotientenkörper

DEFINITION: Sei R ein Integritätsbereich ungleich Null. Der Körper Q ist *ein Quotientenkörper* von R, wenn gilt:

1. R ist ein Teilring von Q

2. Zu jedem $a \in Q$ existieren $r, s \in R$ mit $a = r \cdot s^{-1}$ (mit $s^{-1} \in Q$)

BEISPIELE:

- $\mathbb{Q}$ ist Quotientenkörper von $\mathbb{Z}$ und auch von $2\mathbb{Z}$, $\mathbb{R}$ ist kein Quotientenkörper

- Sei K Körper, dann ist $K(x)$ (Körper der rationalen Funktionen) Quotientenkörper von $K[x]$

SATZ: Jeder Integritätsbereich $R \neq 0$ besitzt einen Quotientenkörper.

KOROLLAR: Die Integritätsbereiche sind genau die Teilringe von Körpern.

BEWEIS: Sei $M := \{(r,s) \mid r, s \in R \text{ mit } s \neq 0\} = R \times (R \setminus \{0\})$. Definiere nun $(r_1, s_1) \sim (r_2, s_2) :\Leftrightarrow r_1 s_2 = r_2 s_1$.

1. *Behauptung:* $\sim$ ist eine Äquivalenzrelation. *Beweis:*

   - Reflexivität: Aus $rs = rs$ folgt $(r,s) \sim (r,s)$.
   - Symmetrie: Aus $(r_1, s_1) \sim (r_2, s_2)$ folgt $r_1 s_2 = r_2 s_1$ und damit $(r_2, s_2) \sim (r_1, s_1)$.

- Transitivität: Sei $(r_1, s_1) \sim (r_2, s_2)$ und $(r_2, s_2) \sim (r_3, s_3)$, dann gilt $r_1 s_2 = r_2 s_1$ und $r_2 s_3 = r_3 s_2$. Es folgt:

  $$r_1 s_2 s_3 = r_2 s_1 s_3 \overset{komm.}{=} r_2 s_3 s_1 = r_3 s_2 s_1$$

  Damit gilt:

  $$0 = r_1 s_2 s_3 - r_3 s_2 s_1 \overset{Ring}{=} (r_1 s_3 - r_3 s_1) s_2$$

  Da $s_2 \neq 0$ ist folgt mit der Nullteilerfreiheit:

  $$r_1 s_3 - r_3 s_1 = 0 \Rightarrow (r_1, s_1) \sim (r_3, s_3)$$

Die Äquivalenzklasse zu (r, s) sei mit $\frac{r}{s}$ bezeichnet, sei K die Menge der Äquivalenzklassen. Definiere nun

$$\frac{r_1}{s_1} \oplus \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \quad \text{und} \quad \frac{r_1}{s_1} \circ \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

2. *Behauptung:* $(K, \oplus, \circ)$ ist ein Körper. *Beweis:*

   (a) Die Definitionen sind unabhängig von den gewählten Repräsentanten: Sei $(r_1, s_1) \sim (u_1, v_1)$ und $(r_2, s_2) \sim (u_2, v_2)$, d.h. $r_1 v_1 = s_1 u_1$ und $r_2 v_2 = s_2 u_2$. Dann gilt:

   $$\begin{aligned} (r_1 s_2 + r_2 s_1) v_1 v_2 &= r_1 s_2 v_1 v_s + r_2 s_1 v_1 v_2 \\ &= s_1 u_1 s_2 v_2 + s_2 u_2 s_1 v_1 \\ &= s_1 s_2 (u_1 v_2 + u_2 v_1) \\ \Rightarrow (r_1 s_2 + r_2 s_1, s_1 s_2) &\sim (u_1 v_2 + u_2 v_1, v_1 v_2) \\ \Rightarrow &\oplus \text{ wohldefiniert} \\ \text{und } r_1 r_2 v_1 v_2 &= s_1 u_1 s_2 u_2 \\ \Rightarrow (r_1 r_2, s_1 s_2) &\sim (u_1 u_2, v_1 v_2) \\ \Rightarrow &\circ \text{ wohldefiniert} \end{aligned}$$

   (b) Distributivgesetz:

   $$\begin{aligned} \left(\frac{r_1}{s_1} \oplus \frac{r_2}{s_2}\right) \circ \frac{r_3}{s_3} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \circ \frac{r_3}{s_3} \\ &= \frac{r_1 s_2 r_3 + r_2 s_1 r_3}{s_1 s_2 s_3} \\ \frac{r_1}{s_1} \circ \frac{r_3}{s_3} \oplus \frac{r_2}{s_2} \circ \frac{r_3}{s_3} &= \frac{r_1 r_3}{s_1 s_3} \oplus \frac{r_2 r_3}{s_2 s_3} \\ &= \frac{r_1 r_3 s_2 s_3 + r_2 r_3 s_1 s_3}{s_1 s_3 s_2 s_3} \\ &= \frac{s_3 (r_1 s_2 r_3 + r_2 s_1 r_2)}{s_3 (s_1 s_2 s_3)} \end{aligned}$$

(c) $(K, \oplus)$ ist abelsche Gruppe: Da $R \neq 0$, existiert $a \in R$ mit $a \neq 0$. Dieses sei fest gewählt. Dann ist $\frac{0}{a}$ das Nullelement:

$$\frac{r}{s} \oplus \frac{0}{a} = \frac{ra + s0}{sa} = \frac{r}{s}$$

Invers gegenüber $\oplus$ zu $\frac{r}{s}$ ist $\frac{-r}{s}$:

$$\frac{r}{s} \oplus \frac{-r}{s} = \frac{rs - rs}{s^2} = \frac{0}{s^2} = \frac{0}{a}$$

(d) $(K \setminus \{0\}, \circ)$ ist eine Gruppe: Einselement: $\frac{a}{a}$:

$$\frac{r}{s} \circ \frac{a}{a} = \frac{ra}{sa} = \frac{r}{s}$$

Inverses zu $\frac{r}{s}$ ist $\frac{s}{r}$ (wobei ja $\frac{r}{s} \neq \frac{0}{a}$):

$$\frac{r}{s} \circ \frac{s}{r} = \frac{rs}{sr} = \frac{a}{a}$$

3. *Behauptung:* Die Abbildung $\sigma : R \to K$ mit $r \mapsto \frac{ra}{a}$ ist ein Monomorphismus. Somit ist $R^\sigma := \{r^\sigma \mid r \in R\}$ ist zu R isomorpher Teilring von K. *Beweis:*

   (a) Injektivität:

   $$r^\sigma = s^\sigma \Rightarrow \frac{ra}{a} = \frac{sa}{a} \Rightarrow ra^2 = sa^2 \Rightarrow (r-s)a^2 = 0 \overset{nullt.f.}{\Longrightarrow} r = s$$

   (b) Homomorphieeigenschaften bezüglich $\oplus$:

   $$r^\sigma \oplus s^\sigma = \frac{ra}{a} \oplus \frac{sa}{a} = \frac{ra^2 + sa^2}{a^2} = \frac{(r+s)a \circ a}{a \circ a} = \frac{(r+s)a}{a} = (r+s)^\sigma$$

   (c) Homomorphieeigenschaften bezüglich $\circ$:

   $$r^\sigma \circ s^\sigma = \frac{ra}{a} \circ \frac{sa}{a} = \frac{rsa^2}{a^2} = \frac{rsa}{a} = (rs)^\sigma$$

4. *Behauptung:* $\frac{r}{s} \in K \Rightarrow \frac{r}{s} = r^\sigma \circ (s^\sigma)^{-1}$ *Beweis:*

   $$r^\sigma \circ (s^\sigma)^{-1} = \frac{ra}{a} \circ \frac{a}{sa} = \frac{raa}{asa} = \frac{r}{s}$$

5. *Behauptung:* R ist ein Teilring von Q. *Beweis:* Wende (1.1.4) an auf $\sigma : R \to K = S$. Dann existiert ein Ring T und ein Isomorphismus $\tau : S \to T$ mit $r^{\sigma\tau} = r$ für alle $r \in R$. Dann ist T ein Körper und R ein Teilring von T.

6. *Behauptung:* Zu jedem $a \in Q$ existieren $r, s \in R$ mit $a = r \cdot s^{-1}$ (mit $s^{-1} \in Q$). *Beweis:* Zu jedem $x \in T$ existiert $\frac{r}{s} \in K$ mit

   $$x = \left(\frac{r}{s}\right)^\tau \overset{(4)}{=} \left(r^\sigma \circ (s^\sigma)^{-1}\right)^\tau = r^{\sigma\tau} \cdot (s^{\sigma\tau})^{-1} = r \cdot s^{-1}$$

1.1.4 Einbettungssatz

SATZ: Sei σ ein Monomorphismus des Ringes R in den Ring S. Dann existiert ein Ring T und ein Isomorphismus $\tau : S \to T$ mit folgenden Eigenschaften:

1. R ist ein Teilring von T und
2. $r^{\sigma\tau} = r$ für alle $r \in R$

HILFSSATZ:

Satz: Zu jeder Menge M existiert eine disjunkte gleichmächtige Menge.

Beweis: Sei $N = \mathcal{P}(M)$ die Potenzmenge von M und für jedes $n \in N$ sei $(M, n) := \{ (m, n) \mid m \in M\}$. Offenbar sind alle (M, n) zu M gleichmächtig, denn $\varphi : M \to (M, n)$ mit $m \mapsto (m, n)$ ist bijektiv. Existiert nun $n \in N$ mit $M \cap (M, n) = \emptyset$, so ist die Behauptung bewiesen.

Angenommen, es existiert kein solches n, d.h. $M \cap (M, n) \neq \emptyset$ für alle $n \in N$. Definiere dann die Abbildung

$$\varphi : M \to N \text{ mit } m \mapsto \begin{cases} \{m\} & \text{falls} \quad m \notin (M, n)\ \forall\, n \in N \\ n & \text{falls} \quad m \in (M, n) \text{ für ein } n \in N \end{cases}$$

Dabei ist der zweite Fall ($m^\varphi = n$) wohldefiniert, da für $n_1 \neq n_2$ aus N offenbar $(M, n_1) \cap (M, n_2) = \emptyset$ ist, also m in genau einem (M, n) liegt. Für jedes $n \in N$ existiert nach Annahme ein $m \in M \cap (M, n)$ mit $m^\varphi = n$. Also ist φ surjektiv. Dies ist ein Widerspruch, da keine surjektive Abbildung von einer Menge in ihre Potenzmenge existiert[2].

BEWEIS: Nach Hilfssatz existiert eine zu $R \cup S$ gleichmächtige disjunkte Menge. Insbesondere existiert eine Menge U disjunkt zu $R \cup S$ und eine Bijektion $\varphi : S \setminus R^\sigma \to U$. Sei nun $T = R \cup U$ und

$$\tau : S \to T \text{ mit } x \mapsto \begin{cases} x^\varphi & \text{falls} \quad x \in S \setminus R^\sigma \\ x^{\sigma^{-1}} & \text{falls} \quad x \in R^\sigma \end{cases}$$

Dann ist τ bijektiv. Für $a, b \in S$ sei $a^\tau \oplus b^\tau := (a + b)^\tau$ und $a^\tau \circ b^\tau = (a \cdot b)^\tau$. Dann ist $(T, \oplus, \circ)$ ein Ring und offenbar τ ein Isomorphismus. Für $r \in R$ ist $r^{\sigma\tau} = (r^\sigma)^{\sigma^{-1}} = r$. Da τ ein Isomorphismus ist, ist $(R^\sigma)^\tau$ ein Teilring von T.

1.1.5 Eindeutigkeit des Quotientenkörpers

SATZ: Seien R_1 und R_2 Integritätsbereiche ungleich Null und sei $\sigma : R_1 \to R_2$ ein Isomorphismus. Sind Q_1 und Q_2 Quotientenkörper von R_1 bzw. R_2, so existiert ein Isomorphismus $\bar{\sigma} : Q_1 \to Q_2$ mit $r^{\bar{\sigma}} = r^\sigma$ für alle $r \in R_1$.

[2] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 1.3.4

Beweis: Jedes $x \in Q_i$ läßt sich schreiben als $x = \frac{r}{s}$ mit $r, s \in R_1$. Definiere:

$$\bar{\sigma} : Q_1 \to Q_2 \text{ mit } \frac{r}{s} \mapsto \frac{r^\sigma}{s^\sigma} \; (r, s \in R_i, s \neq 0)$$

Dann ist $\bar{\sigma}$ wohldefiniert („$\Rightarrow$“) und injektiv („$\Leftarrow$“), da für $r_i, s_i \in R_i$ gilt:

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \Leftrightarrow r_1 s_2 = r_2 s_1 \overset{isom.}{\Longleftrightarrow} r_1^\sigma s_2^\sigma = (r_1 s_2)\sigma = (r_2 s_1)\sigma = r_2^\sigma s_1^\sigma \Leftrightarrow \frac{r_1^\sigma}{s_1^\sigma} = \frac{r_2^\sigma}{s_2^\sigma}$$

Da Q_2 Quotientenkörper von R_2 ist, ist $\bar{\sigma}$ surjektiv.

$$\begin{aligned} \left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right)^{\bar{\sigma}} &= \left(\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\right)^{\bar{\sigma}} \\ &= \frac{(r_1 s_2 + r_2 s_1)^\sigma}{(s_1 s_2)^\sigma} \\ &= \frac{r_1^\sigma s_2^\sigma + r_2^\sigma s_1^\sigma}{s_1^\sigma s_2^\sigma} = \frac{r_1^\sigma}{s_1^\sigma} + \frac{r_2^\sigma}{s_2^\sigma} \end{aligned}$$

Zudem stimmt $\bar{\sigma}$ mit σ überein[3]: sei $a \in R \setminus \{0\}$. Für $r \in R$ ist dann

$$r^{\bar{\sigma}} = \left(\frac{ra}{a}\right)^{\bar{\sigma}} = \frac{(ra)^\sigma}{a^\sigma} = \frac{r^\sigma a^\sigma}{a^\sigma} = r^\sigma$$

Korollar: Für $R_1 = R_2 = R$ und $\sigma = \mathrm{id}$ erhalten wir: Je zwei Quotientenkörper des Integritätsbereiches $R \neq 0$ sind über R isomorph, d.h. es existiert ein Isomorphismus σ zwischen ihnen mit $r^\sigma = r$ für alle $r \in R$.

1.1.6 Quotientenkörper als Teilkörper

Satz: Ist $R \neq 0$ Teilring eines Körpers K, so enthält K einen Quotientenkörper von R als Teilkörper.

Beweis: Definiere folgende Menge:

$$Q := \left\{ \frac{r}{s} \;\middle|\; r, s \in R, s \neq 0 \right\} \subseteq K$$

Wir zeigen zunächst: $Q \leq K$.

- Null: Offensichtlich ist $0 \in Q$
- Eins: $\frac{a}{a} = 1 \in Q$

[3] Diese Vorlesung hat Mike Aizatulin geTEXt, vielen Dank!

- $\frac{r_1}{s_1} - \frac{r_2}{s_2} = \frac{r_1 s_2 - r_2 s_1}{s_1 s_2} \in Q$
- $\frac{r}{s} \neq 0 \Rightarrow \frac{s}{r} \in Q$

Zu zeigen bleibt nach (1.1.3): R ist ein Teilring von Q. Es gilt $R \subseteq Q$, da zu $r \in R$ immer $r = \frac{ra}{a} \in Q$ ist, d.h. R ist Teilring von Q.

1.1.7 Ideale, Faktorringe

Sei R ein kommutativer Ring mit Eins (vieles geht auch ohne Eins).

DEFINITION: Eine Teilmenge $I \subseteq R$ heisst *Ideal* (in Zeichen $I \trianglelefteq R$), wenn gilt:

- $(I, +)$ ist eine Untergruppe von $(R, +)$ (d.h. $I \neq \emptyset$; $a, b \in I \Rightarrow a - b \in I$)
- $a \in I, r \in R \Rightarrow ar \in I$, d.h. $IR \subseteq I$ (bei einem Ring mit Eins auch $IR = I$)

BEMERKUNGEN:[4]

1. Ideale sind spezielle Teilringe, aber z.B. $\mathbb{Z}$ ist nur Teilring und kein Ideal von $\mathbb{Q}$.
2. Beispiele von Idealen sind 0, R, für $a \in R$ ist $Ra = \{ra \mid r \in R\}$ das kleinste Ideal, das a enthält. Das ist aber falsch, falls der Ring keine Eins hat, z.B. $R = 2\mathbb{Z}, a = 2, Ra = 4\mathbb{Z}$ damit $a \notin Ra$
3. In $\mathbb{Z}$ haben alle Ideale die Gestalt $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ für ein $n \in \mathbb{N}_0$.
4. Sind I, J Ideale, so auch $I + J = \{a + b \mid a \in I, b \in J\}$

SATZ: Sei I ein Ideal von R. Dann ist die Menge $R/I = \{r+I \mid r \in R\}$ der Restklassen von $(R, +)$ nach $(I, +)$ zusammen mit den Verküpfungen

$$(r+I) \oplus (s+I) := (r+s)+I$$
$$\text{und } (r+I) \circ (s+I) := rs+I$$

ein Ring mit Eins (wobei $1 = 1+I$), der *Faktorring* von R nach I. Zudem ist folgende Abbildung ϱ ein Epimorphismus von R nach R/I mit ist Kern $\varrho = I$:

$$\varrho : R \to R/I \text{ mit } \varrho : r \mapsto r+I$$

Die Abbildung ϱ heisst der *natürliche Homomorphismus* von R auf R/I.[5]

[4] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 6

1.1.8 Homomorphiesatz

Seien R, S kommutative Ringe mit Eins, $\sigma : R \to S$ ein Homomorphismus.[6]

Bemerkungen:[7]

- Aus $I \trianglelefteq R$ folgt $I^\sigma \trianglelefteq R^\sigma$ (nicht unbedingt $I^\sigma \trianglelefteq S$)
- Aus $J \trianglelefteq S$ (oder $J \trianglelefteq R^\sigma$) folgt $\sigma^{-1}(J) = \{x \in R \mid x^\sigma \in J\} \trianglelefteq R$.
- Insbesondere ist $\operatorname{Kern}\sigma = \{x \in R \mid x^\sigma = 0\} = \sigma^{-1}(0) \trianglelefteq R$

Satz: Sei $I = \operatorname{Kern}\sigma$. Dann ist $\sigma = \varrho \circ \tau$, wobei ϱ der natürliche Homomorphismus von R auf R/I ist und folgende Abbildung ein Monomorphismus ist (d.h. τ ist injektiv):

$$\tau : R/I \to S \text{ mit } r{+}I \mapsto r^\sigma$$

Insbesondere ist $R^\sigma \backsimeq R/I$.

Beweis: Da $r^\sigma = (r{+}I)^\tau$ für $r \in R$, ist offenbar $\sigma = \varrho \circ \tau$, falls τ eine Abbildung ist. Für $r, s \in R$ gilt

$$r^\sigma = s^\sigma \Leftrightarrow 0 = r^\sigma - s^\sigma \overset{\text{Hom.}}{=} (r-s)^\sigma$$
$$\overset{\text{Kern}}{\Longleftrightarrow} r - s \in \operatorname{Kern}\sigma = I \overset{\text{Restkl.}}{\Longleftrightarrow} r{+}I = s{+}I$$

Von rechts nach links gelesen: τ ist wohldefiniert. *Von links nach rechts:* Ist $(r{+}I)^\tau = (s{+}I)^\tau$, d.h. $r^\sigma = s^\sigma$, so folgt $r{+}I = s{+}I$, d.h. τ ist injektiv.

Ferner gilt für die Addition (und analog mit Multiplikation):

$$((r{+}I) + (s{+}I))^\tau = ((r{+}s) + I)^\tau = (r+s)^\sigma = r^\sigma + s^\sigma = (r{+}I)^\tau + (s{+}I)^\tau$$

Somit ist τ ein Monomorphismus. Als Abbildung von $R/I \to R^\sigma$ betrachtet ist τ ein Isomorphismus. □

Zusatz: Die Ideale von R^σ sind genau die H^σ mit $I \subseteq H \trianglelefteq R$, wobei $I = \operatorname{Kern}\sigma$. Ist $\mathcal{M} := \{H \mid I \subseteq H \trianglelefteq R\}$ und $\mathcal{N} := \{J \mid J \trianglelefteq R^\sigma\}$, so ist

$$\bar\sigma : \mathcal{M} \to \mathcal{N} \text{ mit } H \mapsto H^\sigma$$

eine Bijektion mit

$$H_1 \subseteq H_2 \Longleftrightarrow H_1^{\bar\sigma} \subseteq H_2^{\bar\sigma} \tag{$\star$}$$

[6] d.h. $(a+b)^\sigma = a^\sigma + b^\sigma$ und $(ab)^\sigma = a^\sigma b^\sigma$ für alle $a, b \in R$

[7] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 7

Beweis: Die Eigenschaft ($\star$) ist trivial. Nach obiger Bemerkung ist $\bar{\sigma}$ wohldefiniert, wir definieren die Umkehrabbildung

$$\sigma^* : \mathcal{N} \to \mathcal{M} \text{ mit } J \mapsto \sigma^{-1}(J)$$

Offenbar ist dann $I = \sigma^{-1}(0) \subseteq \sigma^{-1}(J)$.

Wir zeigen: $\sigma^* \circ \bar{\sigma} = \mathrm{id}_{\mathcal{N}}$ und $\bar{\sigma} \circ \sigma^* = \mathrm{id}_{\mathcal{M}}$ (also $\bar{\sigma}$ bijektiv):

1. Ist $J \in \mathcal{N}$, d.h $J \trianglelefteq R^\sigma$, so gilt

   $$J^{\sigma^* \bar{\sigma}} = (\sigma^{-1}(J))^\sigma = \left\{ t^\sigma \mid t \in \sigma^{-1}(J) \right\} = J$$

   (da $J \subseteq R^\sigma$)

2. Ist $J \in \mathcal{M}$, d.h. $I \subseteq H \trianglelefteq R$, so gilt

   $$H^{\bar{\sigma} \circ \sigma^*} = \sigma^{-1}(H^\sigma) \supseteq H$$

   Sei $x \in \sigma^{-1}(H^\sigma)$, dann

   $$\begin{aligned} &\exists\, h \in H \text{ mit } h^\sigma = x^\sigma \\ \Rightarrow\ & 0 = x^\sigma - h^\sigma = (x-h)^\sigma \\ \Rightarrow\ & x - h \in \operatorname{Kern} \sigma = I \subseteq H \text{ und } x = (x-h) + h \in H \\ \Rightarrow\ & \sigma^{-1}(H^\sigma) = H \end{aligned}$$

Korollar: Sei $I \trianglelefteq R$. Die Ideale von R/I sind genau die Ideale $H/I = \{ h{+}I \mid h \in H \}$ mit $I \subseteq H \trianglelefteq R$

Beweis: Wende Zusatz an auf ϱ - den natürlichen Homomorphismus und beachte, dass $H^\varrho = \{ h^\varrho \mid h \in H \} = \{ h{+}I \mid h \in H \} = H/I$

1.1.9 Primideale

Sei R ein kommutativer Ring (mit Eins) und sei $I \trianglelefteq R$.

Definition: I ist ein *Primideal*, wenn für alle $a, b \in R$ gilt: $ab \in I \Rightarrow a \in I$ oder $b \in I$. In jedem Fall ist R ein Primideal.

Beispiel: $R = \mathbb{Z}$. Für $n \in \mathbb{N}_0$ gilt: $n\mathbb{Z}$ ist Primideal genau dann, wenn n eine Primzahl oder 1 oder 0 ist.

Beweis:

„$\Rightarrow$" Sei $n > 1$. Wäre n echt zerlegbar, $n = n_1 n_2$ mit $n_i < n, n_i \in \mathbb{N}$, so wäre $n_1 n_2 \in n\mathbb{Z}$, aber $n_1 \notin n\mathbb{Z}$ und $n_2 \notin n\mathbb{Z}$. Also ist n Primzahl.

„$\Leftarrow$“ Sei $n \in \mathbb{P}$ und $ab \in n\mathbb{Z}$, d.h. $ab = nm$ mit $m \in \mathbb{Z}$, dann folgt

$$n \mid ab \overset{\text{prim}}{\Longrightarrow} n \mid a \ \vee \ n \mid b \Longrightarrow a \in n\mathbb{Z} \ \vee \ b \in n\mathbb{Z}$$

SATZ: R/I ist ein Integritätsbereich genau dann, wenn I Primideal ist.

BEWEIS:

„$\Rightarrow$“ Sei R/I Integritätsbereich, seien $a, b \in R$ und $ab \in I$. Dann gilt im R/I:

$$0 = ab + I = (a+I)(b+I) \overset{\text{nullt}}{\Longrightarrow} a+I = 0 \ \vee \ b+I = 0$$

Daraus folgt, daß $a \in I$ oder $b \in I$ gilt.

„$\Leftarrow$“ Sei I Primideal. Seien $a+I, b+I \in R/I$ mit $0 = (a+I)(b+I) = ab+I$. Dann ist also $ab \in I$, damit $a \in I$ oder $b \in I$, also $a+I = 0$ oder $b+I = 0$

1.1.10 maximale Ideale

Sei R ein kommutativer Ring mit Eins und sei $I \trianglelefteq R$.

DEFINITION: I ist ein *maximales Ideal*, wenn $I \neq R$ und $I \subseteq H \trianglelefteq R \Rightarrow (H = I) \vee (H = R)$.

SATZ: R/I ist ein Körper genau dann, wenn I ein maximales Ideal in R ist.

HILFSSATZ:

Satz: Sei R ein kommutativer Ring mit Eins. R ist Körper genau dann, wenn R genau zwei Ideale hat (0, R).

Beweis:

„$\Rightarrow$“ $R \neq 0$, d.h. 0 und R sind bereits zwei Ideale. Sei also $0 \neq I \trianglelefteq R$, dann existier $a \in I$ mit $a \neq 0$. Für beliebiges $r \in R$ ist dann $r = (ra^{-1})a \in I$, also ist $I = R$.

„$\Leftarrow$“ $R \neq 0$, und $0, R$ sind die einzigen Ideale. Zu zeigen: Inverses Element. Sei $0 \neq a \in R$. Dann ist $a \in Ra \trianglelefteq R$, also ist $Ra = R$. Damit existiert $b \in R$ mit $ba = 1$, also hat a ein Inverses, d.h. R ist Körper.

BEWEIS: R/I ist nach Hilfssatz genau dann ein Körper, wenn R/I genau zwei Ideale hat. Nach Korollar (1.1.8) ist dies äquivalent dazu, daß I und R die einzigen Ideale oberhalb I und $I \neq R$ ist. Damit ist I maximales Ideal.

KOROLLAR: Wenn I ein maximales Ideal ist, ist I Primideal.

BEWEIS: mit (1.1.9) und (1.1.10), die Umkehrung gilt nicht immer (aber oft!).

1.1.11 Primkörper

Definition: Ein Körper, der keinen echten Teilkörper besitzt, heißt *Primkörper*

Beispiele:

1. $\mathbb{Q}$ ist ein Primkörper. *Beweis:* Sei $T \leq \mathbb{Q}$, also $T \neq 0$, damit existiert $t \in T \setminus \{0\}$, also ist $1 = \frac{t}{t} \in T$. Damit ist auch $n \cdot 1 \in T$ (also $\mathbb{N} \subseteq T$), ebenso die inversen $-n \in T$ (also $\mathbb{Z} \subseteq T$), dann sind jedoch auch alle $\frac{n}{m} \in T$ (mit $m \neq 0$, also $\mathbb{Q} \subseteq T$), damit ist $T = \mathbb{Q}$.

2. $\mathbb{Z}_P = \mathbb{Z}/p\mathbb{Z} = GF(p)$ mit p Primzahl ist ein Primkörper. *Beweis:* Sei $T \leq \mathbb{Z}/p\mathbb{Z}$, also $T \neq 0$, damit existiert $t \in T \setminus \{0\}$, also ist $1 + p\mathbb{Z} \in T$. Damit ist auch $n \cdot (1 + p\mathbb{Z}) \in T$, also $T = \mathbb{Z}/p\mathbb{Z}$

Lemma: Jeder Körper K enthält genau einen Primkörper $P = \bigcap_{T \leq K} T$ als Teilkörper.

Beweis: Offenbar ist $P \leq K$. Ist $S \leq P$, so ist $S \leq K$. Dann ist $P = \bigcap_{T \leq K} T \leq S$, also ist $P = S$. Also ist P Primkörper. Wäre $Q \leq K$ ein weiterer Primkörper, dann ist $P = \bigcap_{T \leq K} T \leq Q$, also $P = Q$.

Satz: Jeder Primkörper ist entweder zu $\mathbb{Q}$ oder zu einem $GF(p) = \mathbb{Z}/p\mathbb{Z}$ mit $p \in \mathbb{P}$ isomorph.

Beweis: Sei K ein Primkörper, $1 \in K$ und sei[8] $\sigma : \mathbb{Z} \to K$ mit $\sigma : n \mapsto n \cdot 1$. Offenbar gilt:

$$\begin{aligned} (n+m)^\sigma = (n+m) \cdot 1 &= n \cdot 1 + m \cdot 1 = n^\sigma + m^\sigma \\ \text{und } (n \cdot m)^\sigma = (n \cdot m) \cdot 1^2 &= (n \cdot 1) \cdot (m \cdot 1) = n^\sigma \cdot m^\sigma \end{aligned}$$

Damit ist σ ein Ringhomomorphismus. Somit ist $R := \mathbb{Z}^\sigma$ ein Teilring des Körpers K und $R \neq 0$, da $1 \in R$. Mit (1.1.2) ist R ein Integritätsbereich. Nach Homomorphiesatz (1.1.8) ist $R = \mathbb{Z}^\sigma \simeq \mathbb{Z}/\operatorname{Kern}\sigma$. Nach (1.1.9) $\operatorname{Kern}\sigma$ ein Primideal, nach Beispiel in (1.1.9) ist also $\operatorname{Kern}\sigma = p\mathbb{Z}$ für ein $p \in \mathbb{P}$ oder $\operatorname{Kern}\sigma = 0$.

1. Fall: $\operatorname{Kern}\sigma = p\mathbb{Z}$ mit $p \in \mathbb{P}$. Dann ist $R \simeq \mathbb{Z}/p\mathbb{Z} = GF(p)$, also Teilkörper von K. Da K ein Primkörper ist, folgt: $R = K$.

2. Fall: $\operatorname{Kern}\sigma = 0$. Dann ist $R \simeq \mathbb{Z}/\operatorname{Kern}\sigma = \mathbb{Z}$. Nach (1.1.6) enthält K einen Quotientenkörper Q von R als Teilkörper. Nach Satz (1.1.5) ist Q isomorph zum Quotientenkörper von $\mathbb{Z}$, also $Q \simeq \mathbb{Q}$. Da K Primkörper ist, ist $K = Q \simeq Q$.

[8] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 1.5.3 und 1.6.1

1.1.12 Die Charakteristik eines Körpers

Sei K ein Körper, sei P der in K enthaltene Primkörper.

Definition: Die Charakteristik eines Körpers sei definiert als

$$\operatorname{char} K := \begin{cases} p & \text{falls} \quad P \simeq \mathbb{Z}/p\mathbb{Z} \\ 0 & \text{falls} \quad P \simeq \mathbb{Q} \end{cases}$$

Bemerkung:

1. Die alte Definition[9] besagt dasselbe:

$$\operatorname{char} K := \begin{cases} 0 \text{ falls } n \cdot 1 \neq 0 \; \forall \, n \in \mathbb{Z} \\ \min \{ n \in \mathbb{N} \mid n \cdot 1 = 0 \} \text{ sonst} \end{cases}$$

2. $K \leq L \Rightarrow \operatorname{char} K = \operatorname{char} L$, *Beweis:* P ist auch Primkörper von L.

1.2 Teilbarkeitstheorie in Ringen

Teilbarkeit in $\mathbb{Z}$: Es gilt $a \mid b \Leftrightarrow \; \exists \, c \in \mathbb{Z}$ mit $ac = b \Leftrightarrow a\mathbb{Z} \supseteq b\mathbb{Z}$; jede Zahl $n \in \mathbb{Z} \setminus \{0, 1\}$ hat vier „triviale“ Teiler $\pm n$ und ± 1; eine Primzahl hat nur diese vier Teiler, jede Zahl hat eine eindeutige Primfaktorzerlegung $n = \varepsilon p_1^{a_1} \cdots p_r^{a_r}$ mit $\varepsilon = \pm 1$, $p_i \in \mathbb{P}$ und $\alpha_i \in \mathbb{N}_0$ eindeutig bestimmt.

Frage: Geht das in beliebigen Ringen? **Antwort:** Natrürlich nicht, man braucht vernünftige Eigenschaften von R:

- **Kommutativität**, falls nicht: Beispielsweise

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

- **Ring mit Eins**, falls nicht: Bei $R = 2\mathbb{Z}$ ist die eindeutige Primfaktorzerlegung nicht möglich: $12 = (-2) \cdot (-6) = 2 \cdot 6$

- **Nullteilerfreiheit**, falls nicht: keine eindeutige Primfaktorzerlegung, beispielsweise in $\mathbb{Z}/6\mathbb{Z}$ gilt:

$$(3 + 6\mathbb{Z})(2 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 0 \text{ aber } (3 + 6\mathbb{Z}) \cdot (3 + 6\mathbb{Z}) = (3 + 6\mathbb{Z})$$

[9] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 1.6.3

1.2.1 Teiler, Assoziierte, Einheiten

Sei R ein Integritätsbereich mit Eins und $a, b \in R \setminus \{0\}$.

DEFINITIONEN:

1. Teiler: $a \mid b :\Longleftrightarrow \exists\, c \in R$ mit $ac = b \overset{\text{Bem.}}{\Longleftrightarrow} Ra \supseteq Rb$
2. assoziiert: $a \sim b :\Longleftrightarrow (a \mid b) \wedge (b \mid a) \overset{\text{s.oben}}{\Longleftrightarrow} Ra = Rb$ (wobei $\sim$ eine Äquivalenzrelation ist)
3. a Einheit $:\Longleftrightarrow \exists\, a' \in R$ mit $aa' = 1 \Longleftrightarrow a \mid 1$

SATZ:

1. Die Einheiten von R bilden eine Gruppe $(E(R), \cdot)$.
2. a ist Einheit genau dann, wenn $Ra = R$.
3. $a \sim b$ und $ac = b \Rightarrow c \in E(R)$
4. $a \sim b \Leftrightarrow \exists\, e \in E(R)$ mit $ae = b \Leftrightarrow \exists\, e' \in E(R)$ mit $a = be'$

BEWEIS:

1. Seien $e, e' \in E(R)$. Dann existieren f, f' mit $ef = 1 = e'f'$. Dann ist $ee'ff' = 1 \cdot 1 = 1$, also ist ee' eine Einheit. Damit ist $1 \in E(R)$, das inverse Element ist vorhanden ($ef = 1 \Rightarrow f = e^{-1}$ Gruppe).
2. „$\Rightarrow$“ $a \in E(R) \Rightarrow \exists\, f$ mit $af = 1$. Für $r \in R$ ist $r = r \cdot 1 = r \cdot a \cdot f \in Ra$, damit ist $R \subseteq Ra$.

   „$\Leftarrow$“ $Ra = R \Rightarrow \exists\, b \in R$ mit $ba = 1 \Rightarrow a \in E(R)$
3. Sei $a \sim b$. Dann existiert $c \in R$ mit $ac = b$ und es existiert $d \in R$ mit $bd = a$. Daraus folgt: $a = bd = acd \Rightarrow a(1 - cd) = 0 \Rightarrow 1 - cd = 0 \Rightarrow cd = 1$
4. „$\Rightarrow$“ siehe (3)

   „$\Leftarrow$“ Sei also $e \in E(R)$ mit $ae = b$ (also $a \mid b$). Es existiert e' mit $ee' = 1$, daraus folgt $a = a \cdot 1 = a \cdot e \cdot e' = be'$, damit ist $b \mid a$, also $a \sim b$

BEISPIELE:

1. $R = \mathbb{Z}$: es ist $E(\mathbb{Z}) = \{1, -1\}$ und es gilt $a \sim b \Leftrightarrow b = \pm a$.
2. K Körper: $a \mid b$ gilt immer, da $b = a(a^{-1}b)$, damit ist $E(K) = K \setminus \{0\}$

3. $K[x] = R$ mit K Körper: Einheiten sind Polynome vom Grad 0, also $E(K[x]) = K \setminus \{0\}$, *Beweis:* Aus $f \cdot g = 1$ folgt, daß $\operatorname{grad} f + \operatorname{grad} g = \operatorname{grad} 1 = 0$, also ist $\operatorname{grad} f = 0$, damit $f \in K \setminus \{0\}$

1.2.2 Primelemente und unzerlegbare Elemente

Sei R Integritätsbereich mit Eins.

Definition: Sei $p \in R$ mit $p \notin E(R) \cup \{0\}$.

1. p heißt *Primelement* von R, wenn für alle $a, b \in R$ gilt:

$$p \mid ab \Rightarrow (p \mid a) \vee (p \mid b)$$

2. p heißt *unzerlegbar*[10], wenn für alle $a, b \in R$ gilt:

$$p = ab \Rightarrow (a \in E(R)) \vee (b \in E(R))$$

   Die Menge der unzerlegbaren Elemente heißt $U(R)$.

3. p heißt *zerlegbar* genau dann, wenn p nicht unzerlegbar heißt. Die Menge der zerlegbaren Elemente heißt $Z(R)$.

Bemerkung:

$$R = \{0\} \uplus E(R) \uplus U(R) \uplus Z(R)$$

Satz: Sei $p \in R \setminus (E(R) \cup \{0\})$. Dann gilt:

1. p Primelement $\Rightarrow p$ unzerlegbar
2. p Primelement $\Leftrightarrow Rp$ Primideal
3. p unzerlegbar $\Leftrightarrow$ Es existiert kein Element $a \in R$ mit $Rp \subset Ra \subset R$

Beweis:

1. Sei p Primelement und $a, b \in R$ mit $p = ab = p \cdot 1$. Also ist $p \mid ab$, damit gilt nach Definition $p \mid a$ oder $p \mid b$. Ist $p \mid a$, so existiert $c \in R$ mit $p \cdot c = a$, also $p = a \cdot b = p \cdot c \cdot b$. Damit folgt $1 = cb$, damit ist $b \in E(R)$. Ist $p \mid b$, so folgt $a \in E(R)$.

2. $p \mid x$ genau dann, wenn $x \in Rp$. Mit $ab \in Rp$ folgt $a \in Rp$ oder $b \in Rp$.

[10] zum Teil als *irreduzibel* bezeichnet

3. „⇒“ Sei $a \in R$ mit $Rp \subseteq Ra \subseteq R$. Dann existiert $b \in R$ mit $p = ab$. Daraus folgt $a \in E(R)$ (hier folgt $Ra = R$ nach (1.2.1) 2.) oder $b \in E(R)$ (hier folgt $p \sim a$ und $Rp = Ra$ nach (1.2.1) 4.).

   „⇐“ Seien $a, b \in R$ mit $p = ab$. Dann folgt $Rp \subseteq Ra$. Dann folgt $Ra = R$ oder $Ra = Rp$. Damit ist entweder $a \in E(R)$ (mit (1.2.1) 2.) oder $a \sim p$ und damit $b \in E(R)$ (mit (1.2.1) 3.). Damit ist p unzerlegbar.

1.2.3 Hauptidealringe

DEFINITION: Ein Integritätsbereich mit Eins, in dem jedes Ideal Hauptideal ist, heißt *Hauptidealring* (HIR).[11]

SATZ: Sei R ein Hauptidealring und $p \in R$ und $I \trianglelefteq R$ mit $0 < I < R$. Dann gilt:

1. p unzerlegbar $\Leftrightarrow$ p Primelement
2. I Primideal $\Leftrightarrow$ I maximales Ideal

BEWEIS:

1. Sei $p \notin E(R) \cup \{0\}$.

   „⇒“ Satz (1.2.2) 1.

   „⇐“ Sei p unzerlegbar. Nach (1.2.2) 3. ist im Hauptidealring Rp maximales Ideal, also mit (1.1.10) ist Rp Primideal, damit ist p Primelement mit (1.2.2) 2.

2. Sei $I = Rp$ mit $p \in R$. Wegen[12] $0 < I < R$ ist $p \notin E(R) \cup \{0\}$ (1.2.1). Rp Primideal ist nach (1.2.2) 2. äquivalent zu p Primelement, wie eben gezeigt ist p unzerlegbar, mit (1.2.2) 3. folgt $I = Rp$ maximales Ideal.

KOROLLAR: Sei K ein Körper. Dann sind für jedes Ideal I von $K[x]$ mit $0 < I < K[x]$ die folgenden Aussagen äquivalent:

1. I ist Primideal (d.h. $K[x]/I$ ist Integritätsbereich)
2. I ist maximales Ideal (d.h. $K[x]/I$ ist Körper)
3. Es existiert ein irreduzibles Polynom $f \in K[x]$ mit $I = K[x]f$

[11] „Aus dem Satz folgt, daß im Hauptidealring alles bestens ist!“
[12] anderer Prof guckt kurz rein, einziger Kommentar: „Stimmt das?!“

BEWEIS: ($1 \Leftrightarrow 2$) ist Satz (1.2.3) 2., ($2 \Leftrightarrow 3.$) ist Satz (1.2.2) 3[13].

1.2.4 Euklidische Ringe

DEFINITION: Ein Integritätsbereich R ist ein *euklidischer Ring*, wenn es eine Abbildung $g : R \setminus \{0\} \to \mathbb{N}_0$ gibt mit der folgenden Eigenschaft:

($\star$) Zu je zwei Elementen $a, b \in R$ mit $a \neq 0$ existieren Elemente $q, r \in R$ mit $b = qa + r$ wobei $r = 0$ oder $g(r) < g(a)$

BEISPIEL: $R = \mathbb{Z}$ mit $g(a) = |a|$; $R = K[x]$ mit $g = \text{grad}$[14]

SATZ: Jeder euklidische Ring $\neq 0$ ist ein Hauptidealring.

BEWEIS: Sei R ein euklidischer Ring mit „Gradfunktion" $g : R \setminus \{0\} \to \mathbb{N}_0$. Sei $0 \neq I \trianglelefteq R$. Dann existiert $a \in I$ mit $a \neq 0$ und somit ist $\{\, g(x) \mid x \in I \setminus \{0\}\} \neq \emptyset$. Dann existiert ein kleinstes Element dieser Menge, d.h. es existiert $a_0 \in I$ mit $g(a_0)$ minimal.

> *Behauptung:* $I = Ra_0 = \{\, ra_0 \mid r \in R\}$. *Beweis:* Da $I \trianglelefteq R$, ist $Ra_0 \subseteq I$. Sei $b \in I$ Nach ($\star$) existieren Elemente $q, r \in R$ mit $b = qa_0 + r$, wobei $r = 0$ oder $g(r) < g(a_0)$. Da $r = b - qa_0 \in I$, ist $g(r) < g(a_0)$ nach Wahl von a_0 unmöglich, also $r = 0$. Somit ist $b = qa_0 \in Ra_0$.

Wende dies an auf $I = R$, damit existiert $a \in R$ mit $R = Ra$, also existiert $e \in R$ mit $a = ea$.

> *Behauptung:* e ist Eins. *Beweis:* Sei $x \in R = Ra$. Dann existiert $b \in R$ mit $x = ba$, damit ist $ex = eba = ba = x$

Somit ist $I = Ra_0$ das von a_0 erzeugte Hauptideal.

1.2.5 Der Gaußsche Ring und Teilringe von $\mathbb{C}$

Sei $0 \neq n \in \mathbb{Z}$, so daß n kein Quadrat in $\mathbb{Z}$ ist, und sei $s \in \mathbb{C}$ mit $s^2 = n$. Offenbar:

1. $n > 0$, dann folgt $s = \pm\sqrt{n}$ (wobei $\sqrt{n}$ die positive reelle Wurzel ist)
2. $n < 0$, dann folgt $s = \pm(i \cdot \sqrt{-n})$ (mit $i^2 = -1$)

DEFINITIONEN:

[13] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 6.5
[14] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 6.2

1. Sei $R_n := \{a + bs \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

   Behauptung: R_n ist ein $\mathbb{Z}$ enthaltender Teilring von $\mathbb{C}$, also ein Integritätsbereich mit Eins. *Beweis:* $\mathbb{Z} \subseteq R_n$, es folgt $R_n \neq \emptyset$. Es gilt $(a+bs)-(c+ds) = (a-c)+(b-d)s \in R_n$, zudem ist $(a+bs)(c+ds) = ac + bds^2 + (ad+bc)s = ac + nbd + (ad+bc)s \in R_n$.

   Behauptung: Für fest gewähltes s mit $s^2 = n$ ist die Darstellung der Elemente $a + bs \in R_n$ eindeutig. *Beweis:* Aus $a + bs = c + ds$ folgt: $(b-d)s = c - a$. Entweder $b - d = 0 = c - a$ (Darstellung eindeutig) oder $s = \frac{c-a}{b-d} \in \mathbb{Q}$ (Widerspruch).

2. Sei $R_{-1} = \{a + bi \mid a, b \in \mathbb{Z}\}$ der *Gaußsche Ring*.

3. Definiere die Norm $N : R_n \to \mathbb{Z}$, $N(a + bs) = (a + bs)(a - bs) = a^2 - b^2s^2 = a^2 - nb^2 \in \mathbb{Z}$.

   Behauptung: $N(xy) = N(x)N(y)$ *Beweis:* $x = a + bs, y = c + ds$, es folgt

$$\begin{aligned} N(x)N(y) &= (a+bs)(a-bs)(c+ds)(c-ds) \\ &= ((ac+s^2bd)+(ad+bc)s)((ac+s^2bd)-(ad+bc)s) \\ &= N(xy) \end{aligned}$$

   Damit ist N multiplikativ.

   Behauptung: Aus $x \mid y$ in R_n folgt: Es existiert $z \in R_n$ mit $xz = y$ und damit $N(x)N(z) = N(y)$, also $N(x) \mid N(y)$ in $\mathbb{Z}$.

   Bemerkung: $e \in E(R_n)$ ist äquivalent zu $N(e) = \pm 1$.

   Behauptung: $E(R_{-1}) = \{1, -1, i, -i\}$ und $E(R_{-m}) = \{1, -1\}$ für $1 < m \in \mathbb{N}$. *Beweis:* Für $n = -m$, $m \in \mathbb{N}$ ist $N(a + bs) = a^2 + mb^2 \geq 0$; $a + bs \in E(R_n)$ folgt $a^2 + mb^2 \mid 1$, also $a^2 + mb^2 = 1$, dann folgt

   (a) $a \pm 1, b = 0$ für $m > 1$

   (b) $a = \pm 1, b = 0$ oder $a = 0, b = \pm 1$ für $m = 1$

4. $Q_n := \{a + bs \mid a, b \in \mathbb{Q}\}$ ist der in $\mathbb{C}$ enthaltene Quotientenkörper von R_n mit

$$N : Q_n \to \mathbb{Q} \text{ mit } a + bs \mapsto (a+bs)(a-bs) = a^2 - nb^2 \in \mathbb{Q}$$

   Beweis: siehe Aussagen über N weiter oben, zudem: $x = a + bs \neq 0 \Rightarrow N(x) = (a+bs)(a-bs) = a^2 - nb^2 \neq 0$, damit folgt das Inverse Element:

$$1 = (a+bs) \cdot \left(\frac{a}{N(x)} - \frac{b}{N(x)} s \right)$$

SATZ: Für $n = -1, -2, 2, 3$ ist R_n ein euklidischer Ring, also ein Hauptidealring. Insbesondere ist der Gaußsche Ring ein euklidischer Ring.

BEWEIS: Sei $g(x) := |N(x)|$ für $0 \neq x \in R_n$. Zu zeigen:

($\star$) Zu je zwei Elementen $u, v \in R_n$ mit $v \neq 0$ existieren Elemente $q, r \in R$ mit $u = qv + r$ wobei $r = 0$ oder $g(r) < g(v)$

In Q_n existiert v^{-1} und somit $uv^{-1} \in Q_n$, d.h. es existieren $a, b \in \mathbb{Q}$ mit $uv^{-1} = a + bs$. Da $a, b \in \mathbb{Q}$ existieren $x, y \in \mathbb{Z}$ mit $|a - x| \leq \frac{1}{2}$ und $|b - y| \leq \frac{1}{2}$. Sei $q := x + ys \in R_n$.

Sei $r := u - qv$, dann ist $u = qv - r$ und $r = 0$ oder es gilt $g(r) < g(v)$ wegen:

$$\begin{aligned} g(u - qv) &= g(uv^{-1}v - qv) = g(\overbrace{(uv^{-1} - q)v}^{\in R_n}) = \left|N((uv^{-1} - q) \cdot v)\right| \\ &\overset{\in Q_n}{=} \left|N(uv^{-1} - q)\right| \cdot |N(v)| = |N(a - x) + (b - y)s| \cdot g(v) \\ &= \left|(a - x)^2 - n(b - y)^2\right| \cdot g(v) \leq \left|\frac{1}{4} - n\frac{1}{4}\right| \cdot g(v) < g(v) \end{aligned}$$

BEMERKUNG: R_{-3} ist kein Hauptidealring BEWEIS: Die Zahl 2 ist unzerlegbar, aber kein Primelement in R_{-3} (1.2.3)

Unzerlegbarkeit: Angenommen, $2 = xy$ mit $x, y \in R_{-3}$. Dann folgt $4 = N(2) = N(x) \cdot N(y)$ und aus $x = a + bs$ folgt $N(x) = a^2 + 3b^2 \neq 2$. O.B.d.A folgt $N(x) = 1$ und $N(y) = 4$. Dann ist $x \in E(R_n)$, also ist 2 unzerlegbar.

Kein Primelement: $(1+s)(1-s) = 1-s^2 = 4 = 2 \cdot 2$, damit gilt $2 \mid (1+s)(1-s)$, aber $2 \nmid (1 \pm s)$ (denn $2(a + bs) = 2a + 2bs \neq 1 \pm s$).

1.2.6 Die Primelemente im Gaußschen Ring

Sei $R := \{a + bi \mid a, b \in \mathbb{Z}\}$.

HILFSSATZ:

Behauptung: Ist q ein Primelement in R, so existiert eine Primzahl p in $\mathbb{Z}$ mit $q \mid p$ in R. *Beweis:* Sei $q = a + bi$. Dann ist $\mathbb{Z} \ni a^2 + b^2 = N(q) = (a + ib)(a - ib)$, wobei $N(q) \neq 0, \pm 1$. Somit existieren Primzahlen $p_1, ..., p_r$ in $\mathbb{Z}$ mit $p_1 \cdot ... \cdot p_r = a^2 + b^2 = q(a - bi)$. Da q Primelement ist, existiert i mit $q \mid p_i$ in R.

Lemma: Ist p eine Primzahl in $\mathbb{Z}$, so gilt entweder

1. p ist ein Primelement in R oder
2. $p = a^2 + b^2 = (a + bi)(a - bi)$ mit $a \pm bi$ Primelemente in R.

Ist q Primelement in R mit $q \mid p$, so ist im Fall (1) $q \sim p$, im Fall (2) ist $q \sim a \pm bi$.

Beweis: Sei p kein Primelement in R. Dann existieren $x, y \in R$ mit $p = xy$ und $x, y \notin E(R)$. Dann ist $p^2 = N(p) = N(x)N(y)$ und $N(x) \neq 1 \neq N(y)$. Dann ist $N(x) = p = N(y)$. Mit $x = a+bi$ ist dann also $p = N(x) = a^2+b^2 = (a + ib)(a - ib)$. Ist $x = uv$, dann ist $p = N(x) = N(u) \cdot N(v)$. Dann folgt $N(u) = 1$ oder $N(v) = 1$, d.h. $u \in E(R)$ oder $v \in E(R)$.

Ist p Primelement und $q \mid p$, dann folgt $q \cdot c = p$ mit $c \in E(R)$, also $q \sim p$. Im Fall (2) ist $q \mid p = (a + ib)(a - ib)$, also $q \mid a \pm ib$, dann ist $q \sim a \pm ib$.

Fallunterscheidung:

1. $p = 2 = a^2 + b^2 \Rightarrow a = \pm 1, b = \pm 1$, also $2 = (1 + i)(1 - i)$.
2. $p \equiv 3(\text{mod } 4)$ kann wegen $a^2 + b^2 \not\equiv 3(\text{mod } 4)$ nicht Fall (2) sein, dann ist p Primelement in R.
3. $p \equiv 1(\text{mod } 4)$: Bei $\prod_{b\in K^*} k$ heben sich k und k^{-1} auf, es sei denn, $k = k^{-1} \Rightarrow k^2 = 1$, also $k = \pm 1$:

   $$\text{jeder endlicher Körper: } \prod_{b\in K^*} k = -1$$

   Angewandt auf $K = \mathbb{Z}/p\mathbb{Z}$ mit $\bar{n} = n + p\mathbb{Z}$ für $n \in \mathbb{Z}$:

   $$\begin{aligned} \overline{-1} &= \bar{1} \cdot \bar{2} \cdot \ldots \cdot \overline{\frac{p-1}{2}} \cdot \overline{(p-1)} \cdot \overline{(p-2)} \cdot \ldots \cdot \overline{(p - \frac{p-1}{2})} \\ &= \overline{(-1)}^{\frac{p-1}{2}} \cdot \left(\bar{1} \cdot \bar{2} \cdot \ldots \cdot \overline{\frac{p-1}{2}}\right)^2 = \bar{m}^2 \text{ mit } m := \left(\frac{p-1}{2}\right)! \end{aligned}$$

   Dann ist $0 = \bar{m}^2 + \bar{i} = \overline{m^2 + 1}$, d.h. $m^2 + 1 \in p\mathbb{Z}$, d.h. $p \mid m^2 + 1 = (m + i)(m - i)$. Also $p \nmid m \pm i$ (denn $p \cdot (a + bi) = pa + pbi$), damit ist p kein Primelement, also existieren nach Lemma $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2 = (a + bi)(a - bi)$.

SATZ: Die Primelemente von R sind genau

1. $1+i$
2. die Primzahlen mit $p \equiv 3 (\mathrm{mod}\ 4)$
3. alle $a \pm bi$, wobei $a, b \in \mathbb{N}$ mit $a < b$ und $a^2 + b^2 = p$ eine Primzahl in $\mathbb{Z}$ mit $p \equiv 1 (\mathrm{mod}\ 4)$ ist,

und alle Produkte dieser Elemente mit Einheiten $\{\pm 1, \pm i\}$.

KOROLLAR (Fermat): Ist p eine Primzahl in $\mathbb{Z}$ mit $p \equiv 1 (\mathrm{mod}\ 4)$, so existieren (eindeutig) $a + b \in \mathbb{N}$ mit $p = a^2 + b^2$.

Eindeutigkeit: $p^2 = a^2 + b^2 = (a+ib)(a-ib) = c^2 + b^2 = (c+id)(c-id) \Rightarrow c + id \sim a \pm ib \Rightarrow \{c, d\} = \{a, b\}$.

1.2.7 ZPE-Ringe

Sei weiterhin R ein Integritätsbereich mit Eins.

SATZ: Folgende Eigenschaften sind äquivalent[15]:

1. Jedes $a \in R \setminus (E(R) \cup \{0\})$ ist ein Produkt von Primelementen.
2. (a) Jedes $a \in R \setminus (E(R) \cup \{0\})$ ist ein Produkt unzerlegbarer Elemente.
   (b) Sind $q_1, ..., q_s$ und $q'_1, ..., q'_t$ unzerlegbare Elemente in R mit $q_1 \cdot ... \cdot q_s = q'_1 \cdot ... \cdot q'_t$, so gilt $s = t$ und bei geeigneter Numerierung ist $q_i \sim q'_i$ für $i = 1, ..., s$.

LEMMA: Sowohl (1) als auch (2) impliziert: Aus q unzerlegbar folgt q Primelement.

BEWEIS des Lemmas: Sei $q \in R$ unzerlegbar. Fallunterscheidung:

1. Es gelte (1). Dann existieren p_i mit $q = p_1 \cdots p_r$. Wäre $r > 1$, so wäre $q = p_1(p_2 \dots p_r)$. Nach der Definition der Unzerlegbarkeit folgt, daß entweder p_1 oder $p_2 \cdots p_2 \in E(R)$ eine Einheit ist, der erste Fall entfällt sofort, im zweiten Fall folgt $c \in R$ mit $p_2 \cdots p_r \cdot c = 1$, dann ist $p_2 \in E(R)$, Widerspruch. Also $r = 1$, d.h. $q = p_1$ ist Primelement.
2. Es gelte (2). Seien $a, b \in R$ mit $q \mid ab$, also $qc = ab$ mit $c \in R$. Ist $a \in E(R)$, so gilt $a^{-1}qc = b$, d.h. $q \mid b$. Ist $b \in E(R)$, so folgt $q \mid a$.

Angenommen, weder a noch b sind Einheiten. Nach (2a) existieren q_i, q'_j unzerlegbar mit $a = q_1 \cdots q_s$, $b = q'_1 \cdots q'_t$, ferner $c \in E(R)$ oder $c = q''_1 \cdots q''_n$ mit unzerlegbaren Elementen q''_i.

$$q_1 \cdots q_s \cdot q'_1 \cdots q'_t q \cdot q''_1 \cdots q''_n \text{ oder } = qc$$

Nach (2b) existiert i mit $q \sim q_i$ oder $q \sim q'_i$, d.h. $q \mid a$ oder $q \mid b$.

Damit ist q Primelement. Beweis des Satzes:

„(1) $\Rightarrow$ (2)“ Nach (1.2.2) ist jedes Primelement unzerlegbar, d.h. (2a) folgt aus (1). Zu zeigen bleibt (2b) mit Induktion nach $\min(s,t)$.

- Induktionverankerung: $s = \min(s,t) = 1$, dann ist $q_1 = q'_1 \cdots q'_t$, da q unzerlegbar folgt $t = 1$, d.h. $q_1 = q'_1$.
- Induktionsannahme: Sei $s \in \mathbb{N}$, sei die Aussage richtig für Darstellungen mit $\min(s,t) < s$.
- Induktionsschritt: Sei $s = \min(s,t)$. Sei $q_1 \cdots q_s = q'_1 \cdots q'_t$, dann folgt $q_1 \mid q'_1 \cdots q'_t$. Mit Lemma und q_1 Primelement folgt: $q_1 \mid q'_1$, d.h. (bei geeigneter Numerierung) $q'_1 = q_1\varepsilon$. Da q'_1 unzerlegbar, folgt $\varepsilon \in E(R)$. Also ist $q_1 \sim q'_1$. Es gilt weiterhin $q_1 \cdots = \varepsilon q_1 \cdot q'_2 \cdots q'_t$, damit folgt $q_2 \cdots q_s = (\varepsilon q'_2) q'_3 \cdots q'_t$. Mit Induktionsannahme ist $s = t$ und $q_i \simeq q'_i$ für $i \geq 2$.

„(2) $\Rightarrow$ (1)“ Nach Lemma gilt (2a) $\Rightarrow$ (1).

Definition: Ein Integritätsbereich mit Eins, der eine der beiden Eigenschaften (1) oder (2) (und damit beide) hat, heißt *ZPE-Ring* oder *faktoriell*.

Bemerkungen:

1. Auch im ZPE-Ring gilt: p Primelement genau dann, wenn p unzerlegbar ist (mit Satz (1.2.2) und Lemma)
2. R_{-3} ist auch kein ZPE-Ring.

1.2.8 Primfaktorzerlegung in Hauptidealringen

Sei R ein Hauptidealring.

Lemma: Jede aufsteigende Kette von Idealen in R bricht (nach endlich vielen Schritten) ab (der Ring ist *noethersch*), d.h. ist $(I_n)_{n\in\mathbb{N}}$ eine Folge von Idealen mit $I_i \subseteq I_{n+1}$ für alle $n \in \mathbb{N}$, so existiert ein $n_0 \in \mathbb{N}$ mit $I_n = I_{n_0}$ für alle $n \geq n_0$.

Beweis: Sei $J := \bigcup_{n\in\mathbb{N}} I_n$. *Behauptung:* $J \trianglelefteq R$, *Beweis:* $J \neq \emptyset$, $x, y \in J \Rightarrow n, m \in \mathbb{N}$ mit $x \in I_n, y \in I_m$. Sei o.B.d.A. $n \leq m$, und da $I_n \subseteq I_m$ gilt $x, y \in I_m$, damit ist $x - y \in I_m \subseteq J$; $x \in J, r \in R \Rightarrow\ \exists\, n \in \mathbb{N}$ mit $x \in I_n \Rightarrow rx \in I_n \subseteq J$, also ist J Ideal.

Da R Hauptidealring, existiert $a \in R$ mit $J = Ra \ni a$. Da $J = \bigcup_{n\in\mathbb{N}} I_n$ ist, existiert $n_0 \in \mathbb{N}$ mit $a \in I_{n_0}$. Für $n \geq n_0$ gilt: $I_{n_0} \subseteq I_n \subseteq J = Ra \subseteq I_{n_0} \Rightarrow I_{n_0} = I_n$.

Satz: Jeder Hauptidealring ist ein ZPE-Ring.

Beweis: Wir zeigen (2a). Angenommen, (2a) sei falsch. Dann ist

$$M := \{a \in R \setminus (E(R) \cup \{0\}) \mid a \text{ nicht Produkt unzerlegbarer Elemente}\} \neq \emptyset$$

Wir definieren mittels vollständiger Induktion eine Folge $(a_n)_{n\in\mathbb{N}}$ in $M \cup \{0\}$ mit

$$Ra_{n-1} \subsetneq Ra_n\ \forall\, n \in \mathbb{N} \tag{$\star$}$$

- Induktionsanfang: $a_0 = 0$, $a_1 \in M$ (irgendwie), dann ist $a_1 \neq 0$ und somit $Ra_0 \subsetneq Ra_1$.
- Induktionsannahme: Seien $a_0, \ldots, a_n$ definiert mit $(\star)$.
- Induktionsschritt: Dann ist $Ra_n \neq 0$, also $a_n \in M$. Insbesondere ist a_n nicht unzerlegbar, d.h. (nach (1.2.2)) es existieren $b, c \in R \setminus (E(R) \cup \{0\})$ mit $a_n = bc$. Dann ist b oder c nicht Produkt unzerlegbarer Elemente, etwa b, also $b \in M$. Setze $a_{n+1} := b$. Da $a_n = bc$ folgt $Ra_n \subseteq Rb$. Wäre nun $Ra_n = Rb$, so wäre $a_n \sim b$ und damit (1.2.1) $c \in E(R)$, Widerspruch. Also ist $Ra_n \subsetneq Rb = Ra_{n+1}$.

Das liefert Widerpruch zum Lemma (noethersche Eigenschaft). Aus (2a) folgt (1), denn unzerlegbar entspricht Primelement. Damit gilt:

$$\boxed{R \text{ euklidisch}} \Rightarrow \boxed{R \text{ Hauptidealring}} \Rightarrow \boxed{R \text{ ZPE-Ring}}$$!

Die Umkehrung Hauptidealring $\Rightarrow$ euklidisch gilt nicht unbedingt, Gegenbeispiel ist $R = \left\{ a + b\left(\frac{1+i\sqrt{19}}{2}\right) \;\middle|\; a, b \in \mathbb{Z} \right\}$.

1.2.9 Größter gemeinsamer Teiler

Sei R ein Integritätsbereich mit Eins und $a_1, \ldots, a_n \in R$.

Definitionen:

1. $d \in R$ ist ein (!) größter gemeinsamer Teiler von $a_1, \dots, a_n$, wenn gilt:
   (a) $d \mid a_i$ für $i = 1, \dots, n$ (d.h. d ist ein gemeinsamer Teiler)
   (b) aus $t \mid a_i$ für $i = 1, \dots, n$ folgt $t \mid d$
2. $\mathrm{ggT}(a_1, \dots, a_n) = \{ d \mid d$ ist ein größter gemeinsamer Teiler von $a_1, \dots, a_n \}$
3. $a_1, \dots, a_n$ heißen *teilerfremd*, wenn $1 \in \mathrm{ggT}(a_1, \dots, a_n) \Leftrightarrow \mathrm{ggT}(a_1, \dots, a_n) = E(R)$.

Bemerkungen:

- Die Menge ggT kann leer sein.
- Ist $d \in \mathrm{ggT}(a_1, \dots, a_n)$, so ist $\mathrm{ggT}(a_1, \dots, a_n) = \{ d' \mid d' \sim d \}$, *Beweis:* „$\subseteq$“ $d, d' \in \mathrm{ggT}(a_1, \dots, a_n) \Rightarrow d' \mid d \wedge d \mid d' \Rightarrow d' \sim d$; „$\supseteq$“ trivial.

Satz:

1. Ist R ein ZPE-Ring, so ist $\mathrm{ggT}(a_1, \dots, a_n) \neq \emptyset$ für alle $a_i \in R$.
2. (Bezout) Ist R ein Hauptidealring und $d \in \mathrm{ggT}(a_1, \dots, a_n)$, so existiert $r_i \in R$ mit $d = r_1 a_1 + \dots + r_n a_n$.

Beweis:

1. Es gilt $\mathrm{ggT}(0) = 0$, somit sei $a_i \neq 0$ für alle i. Sei P ein Repräsentantensystem der Assoziiertenklassen der Primelemente in R. Dann existieren $\varepsilon_i, \alpha_{p,i} \in \mathbb{N}_0$ (mit $p \in P$, $i \in \{1, \dots, n\}$) mit $e_i = \prod_{p \in P} p^{\alpha_{p,i}}$ wobei nur endlich viele $\alpha_{p,i} \neq 0$ sind. Sei $\alpha_p = \min \{ \alpha_{p,i} \mid i = 1, \dots, n \}$. Dann ist $d := \prod_{p \in P} p^{\alpha_p} \in \mathrm{ggT}(a_1, \dots, a_n)$. Offenbar $d \mid a_i$ (wegen $\alpha_p \leq \alpha_{p,i}$) und jeder gemeinsame Teiler $t = \varepsilon \prod_{p \in P} p^{\beta_p}$ erfüllt $\beta_p \leq \alpha_{p,i}$ für alle i, also $\beta_p \leq \alpha_p$, also $t \mid d$.
2. $Ra_1 + Ra_2 + \dots + Ra_n \trianglelefteq R$; also existiert $x \in R$ mit $Ra_1 + \dots + Ra_n = Rx$, also existieren $x_i \in R$ mit $x = x_1 a_1 + \dots + x_n a_n$. Da $a_i \in Ra_i \subseteq Rx$, ist $x \mid a_i$ für alle i. Damit ist $x \mid d$, d.h. es existiert $y \in R$ mit $d = xy = (x_1 y) a_1 + \dots + (x_n y) a_n$.

KOROLLAR: Im Hauptidealring gilt für $a_1, \ldots, a_n \in R$ und $a, b, c \in R$:

1. $a_1, \ldots, a_n$ teilerfremd genau dann, wenn $r_i \in R$ existieren mit $1 = r_1a_1 + \ldots r_na_n$
2. Sind a, b teilerfremd, so folgt
   (a) $a \mid bc \Rightarrow a \mid c$
   (b) $a, b \mid c \Rightarrow ab \mid c$

1.2.10 Der euklidische Algorithmus

Sei R ein euklidischer Ring mit Gradfunktion g und seien $a, b \in R$ mit $a \neq 0$. Dann existieren $q_i, r_i \in R$ mit

$$\begin{aligned} b &= q_0a + r_1 \text{ mit } g(r_1) < g(a) \\ a &= q_1r_1 + r_2 \text{ mit } g(r_2) < g(r_1) \\ r_1 &= q_2r_2 + r_3 \text{ mit } g(r_3) < g(r_2) \\ &\vdots \\ r_{n-2} &= q_{n-1}r_{n-1} + r_n \text{ mit } g(r_n) < g(r_{n-1}) \\ r_{n-1} &= q_nr_n \end{aligned}$$

BEHAUPTUNG: $r_n \in ggT(a, b)$.

BEWEIS: Wenn man die Kette von unten nach oben durchgeht ergibt sich: $r_n \mid a, b$. Sei nun $t \in R$ mit $t \mid a, b$. Wenn man jetzt die Kette von oben nach unten durchgeht, folgt:

$$\begin{aligned} & t \mid b - q_0a = r_1 \\ \Rightarrow\ & t \mid a - q_1r_1 = r_2 \\ \Rightarrow\ & \ldots \\ \Rightarrow\ & t \mid r_n \end{aligned}$$

Aus dem Verfahren bekommt man r_n als Linearkombination von a und b:

$$r_n = sa + tb,\ s, t \in R$$

ZUSATZ: Ist $b \in ggT(a_1, \ldots, a_{n-1})$, so gilt für alle $d \in R$:

$$d \in ggT(a_1, \ldots, a_n) \Leftrightarrow d \in ggT(b, a_n)$$

Damit kann man mit Induktion den obigen Algorithmus auf beliebige Anzahl der Elemente erweitern.

1.3 Polynomringe

Wir wollen die Theorie aus Paragraph (1.2) auf $K[x]$ anwenden. $K[x]$ hat eindeutige Primfaktorzerlegung, wobei Primelemente die irreduziblen Polynome sind. Das nutzt aber nur, wenn man Primelemente „kennt“. Problem: es gibt unendlich viele Polynome mit kleinerem Grad, die ein gegebenes Polynom teilen können.

1.3.1 Polynomringe über Ringen

Elemente von $R[x]$ werden geschrieben als

$$f = \sum_{i=0}^{n} a_i x^i, \; a_i \in R$$

Bemerkung: Ist R ein Integritätsbereich (mit Eins), so auch $R[x]$.

Beweis: Mit dem Gradsatz:

$$\mathrm{grad}(f \cdot g) = \mathrm{grad}(f) + grad(g)$$

Beispiele:

- $\mathbb{Z}[x] \leq \mathbb{Q}[x]$
- Polynomring über zwei Variablen kann man definieren als $(K[x])[y]$, da

$$\sum a_i(x) y^i = \sum b_{ij} x^i y^j$$

Leider sind diese Ringe keine Hauptidealringe: Beispiele:

- In $R = \mathbb{Z}[x]$ ist $R \cdot 2 + Rx$ kein Hauptideal.
- In $R = (K[x])[y]$ ist $Rx + Ry$ kein Hauptideal. *Beweis:* Angenommen $Rx + Ry = Rf$ mit $f \in R = \sum_{i=0}^{n} a_i(x) y^i, \; a_n(x) \neq 0$. Da $x \in Rf$, so existiert $g \in R$ mit $x = gf$. Mit dem Gradsatz in y folgt dann: $\mathrm{grad}(f) = 0$, d.h. $f = a_0(x)$. Da $y \in Rf$, so existiert ein $h = \sum_{i=0}^{m} c_i(x) y^i \in R$ mit

$$\begin{aligned} y &= h \cdot f = a_0(x) \cdot \sum_{i=0}^{m} c_i(x) y_i \\ &\overset{Gradsatz}{=} a_0(x)(c_0(x) + c_1(x) y) \end{aligned}$$

Somit
$$1 = a_0(x) \cdot c_1(x) = c_1(x) \cdot f \in Rf = Rx + Ry$$
Es existieren also $u, v \in R$ mit $1 = ux + vy$. Daraus ergibt sich mit dem Gradsatz: $1 = 0$, Widerspruch.

SATZ: Sei R ein kommutativer Ring mit Eins. Dann gilt: $R[x]$ Hauptidealring $\Leftrightarrow$ R Körper.

LEMMA (Einsetzhomomorphismus): Sei R ein kommutativer Teilring eines (nicht notwendig kommutativen) Ringes S. Zu jedem $f = \sum_{i=0}^n a_i x^i \in R[x]$ und $s \in S$ definieren wir
$$f(s) = \sum_{i=0}^n a_i s^i$$
Ist $as = sa$ für alle $a \in R$ so gilt für alle $f, g \in R[x]$:
$$\begin{aligned} (f+g)(s) &= f(s) + g(s) \\ (fg)(s) &= f(s) \cdot g(s) \end{aligned}$$
d.h. die Abbildung $\phi_s : R[x] \to S, f \mapsto f(s)$ ist ein Homomorphismus, der Einsetzhomomorphismus zu $s \in S$.

BEWEIS des Satzes:

„$\Leftarrow$“ bekannt

„$\Rightarrow$“ Wir betrachten
$$\phi_0 : R[x] \to R, f = \sum_{i=0}^n a_i x^i \mapsto f(0) = a_0$$
ϕ_0 ist also ein Homomorphismus mit $\mathrm{Bild}(\phi_0) = R$. Daraus folgt $R \simeq R[x]/\operatorname{Kern}\phi_0$. Da $R \leq R[x]$ und $R[x]$ ein Hauptidealring ist, folgt: R ist Integritätsbereich. Mit 1.1.9 folgt: $\operatorname{Kern}\phi_0$ ist Primideal in $R[x]$. Wegen $0 < \operatorname{Kern}\phi_0 < R[x]$ ergibt sich: $\operatorname{Kern}\phi_0$ ist maximales Ideal, damit ist $R[x]/\operatorname{Kern}\phi_0 \simeq R$ ein Körper.

1.3.2 Hauptsatz

HAUPTSATZ (GAUSS 1777-1855): Ist R ein ZPE-Ring, so auch $R[x]$.

KOROLLAR: $K[x_1, \ldots, x_n] := (K[x_1, \ldots, x_{n-1}])[x_n]$ ist ein ZPE-Ring, wenn K einer ist, insbesondere wenn K ein Körper ist. Ferner ist $\mathbb{Z}[x]$ ein ZPE-Ring.

BEWEISidee: $R[x]$ einbetten in $K[x]$ mit K - Quotientenkörper von R:

$$f = \sum_{i=0}^{n} a_i x^i = d \cdot \sum_{i=0}^{n} b_i x^i \text{ mit } d \in ggT(a_1, \dots, a_n)$$

1.3.3 Primitive Polynome

Sei R ein ZPE-Ring und K ein Quotientenkörper von R.

DEFINITION: $g = \sum_{i=0}^{n} a_i x^i \in R[x]$ heißt *primitiv*, wenn $1 \in \text{ggT}(a_0, \dots, a_n)$.

BEISPIELE:

- Jedes normierte Polynom, d.h. $x^n + a_{n-1}x^{n-1} + \ldots + a_0$, ist primitiv.
- $g(x) = 6x^2 + 10x + 15$ ist primitiv.

LEMMA:

1. $f \in R[x] \Rightarrow f = dg$ mit $d \in R$ und g primitiv aus $R[x]$
2. $f \in K[x] \Rightarrow f = kg$ mit $k \in K$ und g primitiv aus $R[x]$
3. $f \in R[x], f = cg$ mit $c \in K$ und g primitiv $\Rightarrow c \in R$

BEWEIS:

- Sei $f = \sum_{i=0}^{n} a_i x^i$. Sei $d \in \text{ggT}(a_0, \dots, a_n)$. Dann existieren b_i mit $a_i = db_i$, also
$$f = \sum_{i=0}^{n} db_i x^i = d \cdot \sum_{i=0}^{n} b_i x^i$$
Sei $c \in \text{ggT}(b_0, \dots, b_n)$, dann existieren $c_i \in R$ mit $b_i = cc_i$, also $a_i = dcc_i$ d.h. dc teilt alle a_i und damit auch d. Mit (1.2.1) (iii) folgt: $c \in E(R)$. Somit ist $\sum_{i=0}^{n} b_i x^i$ primitiv.

- Da $f \in K[x]$, so gilt: $a_i = \frac{r_i}{s_i}$ mit $r_i, s_i \in R$. Dann aber $s_0 \dots s_n \cdot f \in R[x]$. Mit Anwendung von (a) folgt: $s_0 \dots s_n f = dg$ mit $d \in R$ und g primitiv, dann
$$f = \frac{d}{s} g \text{ mit } s = s_0 \dots s_n$$
also $\frac{d}{s} \in K$.

- Sei $c = \frac{a}{b}$ mit $a, b \in R$. Da R ZPE-Ring, können wir gemeinsame Primfaktoren aus a und b kürzen, also wir können annehmen: a und b sind teilerfremd. Angenommen b ist keine Einheit. Dann existiert ein Primelement $p \in R$ mit $p \mid b$. Wegen

  $$f = c \cdot g = c \cdot \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} \frac{ab_i}{b} x^i$$

  folgt: $p \mid b \mid ab_i$. Da $p \nmid a$ und p Primelement, so folgt: $p \mid b$ für alle i. Das ist ein Widerspruch dazu, dass g Primitiv ist.

SATZ (Gaußsches Lemma): Sind $f, g \in R[x]$ primitiv, so auch fg.

BEWEIS: Seien $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{i=0}^{m} b_i x^i$ primitiv. Angenommen, $f \cdot g$ wäre nicht primitiv. Dann existiert p Primelement in R, das alle Koeffizienten von fg teilt. Da f und g primitiv, existieren $k, l \in \mathbb{N}_0$ mit $p \mid a_0, \ldots, a_{k-1}$, aber $p \nmid a_k$ und $p \mid b_0, \ldots, b_{l-1}$, aber $p \nmid b_l$.

$$\begin{aligned}
\underbrace{c_{k+l}}_{p|\ldots} &= \sum_{i=0}^{k+l} a_i b_{k+l-i} \\
&= \underbrace{a_0 b_{k+l} + a_1 b_{k+l-1} + \ldots + a_{k-1} b_{l+1}}_{p|\ldots} + a_k b_l + \underbrace{a_{k+1} b_{l-1} + \ldots + a_{k+l} b_0}_{p|\ldots}
\end{aligned}$$

Damit teilt p auch $a_k b_l$, aber $p \nmid a_k$ und $p \nmid b_l$, Widerspruch! Also ist $f \cdot g$ primitiv.

1.3.4 Irreduzible Polynome

Seien R, K wie in (1.3.3).

DEFINITION: $g \in R[x]$ heißt (in $R[x]$) *irreduzibel*, wenn g unzerlegbar in $R[x]$ und $\operatorname{grad} g \geq 1$.

BEMERKUNGEN:

1. $E(R[x]) = E(R)$ wegen Gradsatz ($g \cdot h = 1 \Rightarrow \operatorname{grad} g = 0 = \operatorname{grad} h \Rightarrow g \in E(R)$).

2. Unzerlegbare Elemente aus R bleiben unzerlegbar in $R[x]$ (Gradsatz).

3. Jedes irreduzible Polynom ist primitiv (denn $f = dg$ wäre für $d \notin E(R)$ echte Zerlegung).

SATZ: Ein primitives Polynom aus $R[x]$ ist genau dann in $R[x]$ irreduzibel, wenn es in $K[x]$ irreduzibel ist.

BEWEIS: Sei $f \in R[x]$ primitiv und sei $\operatorname{grad} f \geq 1$ (Polynome vom Grad 0 sind weder in $R[x]$ noch in $K[x]$ irreduzibel).

„$\Leftarrow$“ Sei f in $K[x]$ irreduzibel. Angenommen, $f = gh$ mit $g, h \in R[x]$. Da $g, h \in K[x]$ und f dort irreduzibel, folgt: $\operatorname{grad} g = 0$ oder $\operatorname{grad} h = 0$, also etwa $g \in K$. Da $g \in R[x]$ folgt $g \in R$. Da f primitiv, folgt $g \in E(R) = E(R[x])$. Damit ist f in $R[x]$ unzerlegbar.

„$\Rightarrow$“ Sei f in $R[x]$ irreduzibel. Angenommen, $f = \varphi_1\varphi_2$ mit $\varphi_i \in K[x]$. Nach (1.3.3) existieren $c_i \in K$ und g_i primitiv mit $\varphi_i = c_i g_i$ $(i = 1, 2)$. Somit $f = c_1c_2g_1g_2$. Nach (1.3.3) ist auch g_1g_2 primitiv. Nach Lemma (1.3.3) ist $c_1c_2 \in R$. Da f unzerlegbar in $R[x]$ ist, folgt, daß g_1 oder g_2 eine Einheit in $R[x]$ ist, also $g_i \in R$ für ein i. Dann ist $\varphi_i = c_i g_i \in K$. Also ist f irreduzibel in $K[x]$.

KOROLLAR: Ist $0 \neq f \in K[x]$ und $f = k \cdot g$ mit $k \in K$ und $g \in R[x]$ primitiv (wie in Lemma (1.3.3)), so gilt: f ist irreduzibel in $K[x] \overset{\text{trivial}}{\Longleftrightarrow} \frac{1}{k} f = g$ irreduzibel in $K[x] \overset{\text{Satz}}{\Longleftrightarrow} g$ irreduzibel in $R[x]$.

1.3.5 Beweis des Hauptsatzes

HAUPTSATZ (1.3.2): Ist R ein ZPE-Ring, so auch $R[x]$.

BEWEIS: Nach Bemerkung aus (1.3.4) ist $E(R[x]) = E(R)$. Unzerlegbare Elemente in $R[x]$ sind:

1. Unzerlegbare Elemente (Primelemente) von R
2. Irreduzible Polynome in $R[x]$ (die sind insbesondere primitiv)

Sei K ein Quotientenkörper von R.

2. (a) (Existenz der Zerlegung) Sei also $f \in R[x] \setminus (E(R[x]) \cup \{0\})$. Dann ist $f \in K[x]$, also entweder Einheit in $K[x]$ oder Produkt irreduzibler Polynome aus $K[x]$.
   i. Falls $f \in E(K[x])$, so folgt $f \in K \Rightarrow f \in R \Rightarrow$ es existieren Primelemente $p_i \in R$ mit $f = p_1 \cdot \ldots \cdot p_r$, fertig.
   ii. Falls $f \notin E(K[x])$, so folgt (da $K[x]$ ZPE-Ring ist), daß $\varphi_i \in K[x]$ existiert, irreduzibel mit $f = \varphi_i \cdot \ldots \cdot \varphi_m$. Nach Lemma (1.3.3) existieren $c_i \in K$ und g_i primitiv mit $\varphi_i = c_i g_i$

$(i = 1, \dots, m)$, also $f = c_1 \cdot \ldots \cdot c_m \cdot g_1 \cdot \ldots \cdot gm_m$. Mit Satz (1.3.3) folgt, daß $g_1 \cdot \ldots \cdot g_1$ primitiv sind, damit folgt wieder mit (1.3.3), daß $c_1 \cdot \ldots \cdot c_m \in R$. Nach Korollar (1.3.4) ist g_i irreduzibel in $R[x]$. Da $c_1 \cdot \ldots \cdot c_m \in R$ existieren Primelemente $q_j \in R$ mit $c_1 \cdot \ldots \cdot c_m = q_1 \cdot \ldots \cdot q_r$ (oder $c_1 \cdot \ldots \cdot c_m \in E(R)$). Somit $f = q_1 \cdot \ldots \cdot q_r \cdot g_1 \cdot \ldots \cdot g_m$ Produkt unzerlegbarer Element aus $R[x]$.

(b) (Eindeutigkeit der Zerlegung) Sei $p_1 \cdot \ldots \cdot p_r \cdot g_1 \cdot \ldots \cdot g_m = q_1 \cdot \ldots \cdot q_s \cdot h_1 \cdot \ldots \cdot h_n$ mit p_i, q_i Primelemente in R und g_i, h_i irreduzibel in $R[x]$. Nach Satz (1.3.4) sind alle g_i, h_j irreduzibel in $K[x]$ und $g_1 \cdot \ldots \cdot g_m = d \cdot h_1 \cdot \ldots \cdot h_n$ mit $d = \frac{q_1 \cdot \ldots \cdot q_s}{p_1 \cdot \ldots \cdot p_r} \in K$. Da $K[x]$ ein ZPE-Ring ist, folgt $m = n$, und bei geeigneter Numerierung $g_i = c_i h_i$ für $i = 1, \dots, n$ mit $c_i \in K$. Nach Lemma (1.3.3) ist $c_i \in R$ (da h_i primitiv). Da g_i primitiv, folgt $c_i \in E(R) = E(R[x])$, damit folgt $g_i \sim h_i$. Eingesetzt ergibt sich:

$$p_1 \cdot \ldots \cdot p_r \cdot c_1 \cdot \ldots \cdot c_m \cdot h_1 \cdot \ldots \cdot h_m = q_1 \cdot \ldots \cdot q_s \cdot h_1 \cdot \ldots \cdot h_m$$

Da $R[x]$ nullteilerfrei ist, folgt, daß $p_1 \cdot \ldots \cdot p_r \cdot c_1 \cdot \ldots \cdot c_m = q_1 \cdot \ldots \cdot q_s$. Es folgt weiter (da R ZPE-Ring ist), daß $r = s$ und $p_i \sim q_i$ in R (bei geeigneter Numerierung), also auch $p_i \sim q_i$ in $R[x]$.

1.3.6 Eisensteinsches Irreduzibilitätskriterium

Sei R ein ZPE-Ring und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit $n \geq 1$.

Satz (Eisenstein 1823-1852): Wenn es ein Primelement $p \in R$ gibt mit

$$p \mid a_0, \dots, a_{n-1} \text{ und } p \nmid a_n \text{ und } p^2 \nmid a_0,$$

dann ist $f = c \cdot g$ mit $c \in R$ und einem (primitiven) irreduziblen Polynom $g \in R[x]$. Insbesondere ist f irreduzibel in $K[x]$ für jeden Quotientenkörper K von R.

Beweis: Angenommen, $f = g \cdot h$ mit $g = \sum_{i=0}^{r} b_i x^i$ und $h = \sum_{i=0}^{s} c_i x^i$ mit $1 \leq r, s$ und $b_r \neq 0 \neq c_s$. Dann ist $a_0 = b_0 c_0$. Da $p \mid a_0$ und p Primelement, folgt $p \mid b_0$ oder $p \mid c_0$, etwa $p \mid b_0$. Da $p^2 \nmid a_0$, folgt $p \nmid c_0$. Da $p \nmid a_n$, kann p nicht alle Koeffizienten von g teilen. Somit existiert $j \in \{1, \dots, r\}$ mit $p \nmid b_j$, aber $p \mid b_0, \dots, b_{j-1}$. Dann ist, da $s \geq 1$, also $r < n$, offenbar $j < n$, also

$$p \mid a_j = \sum_{i=0}^{j} b_i c_{j-i} = \underbrace{b_0 c_j + b_1 c_{j-1} + \ldots + b_{j-1} c_1}_{p \mid \ldots} + b_j c_0$$

Damit teilt p auch $b_j c_0$, aber $p \nmid b_j$ und $p \nmid c_0$. Widerspruch!

Ist also $f = d \cdot \varphi$ mit $d \in R$ und $\varphi \in R[x]$ primitiv, so ist φ irreduzibel (denn $\varphi = u \cdot v \Rightarrow f = d \cdot u \cdot v \Rightarrow \operatorname{grad} u = 0$ etwa, also $u \in E(R)$). Nach Korollar (1.3.4) ist f irreduzibel in $K[x]$.

Beispiele:

1. Für $n \geq 1$ und p Primzahl ist $f = x^n - p$ irreduzibel in $\mathbb{Q}[x]$. Eisenstein mit p für dieses Polynom! Zu jedem Grad n existieren also unendlich viele irreduzible Polynome vom Grad n. Für $n > 1$ ist $\sqrt[n]{p} \notin \mathbb{Q}$.

2. Das Polynom $f = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} \Rightarrow 9f = 2x^5 + 15x^4 + 9x^3 + 3$ mit Eisenstein für $p = 3$.

1.3.7 Kreisteilungspolynome

Sei p eine Primzahl.[16]

Satz: Das p-te Kreisteilungspolynom $\phi_p := \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$ ist irreduzibel über $\mathbb{Q}$ (und $\mathbb{Z}$).

Beweis: *Trick:* Betrachte $R = \mathbb{Q} \leq \mathbb{Q}[x] = S$ und setze $x + 1 \in S$ in ϕ_p ein. Das liefert $f = \phi_p(x+1) = \sum_{i=0}^{p-1}(x+1)^i \in \mathbb{Q}[x]$. Wäre $\phi_p = g \cdot h$ mit Polynomen g, h vom Grade ≥ 1, so folgte $f = \phi_p(x+1) = g(x+1)h(x+1)$ und $\operatorname{grad} g(x+1) = \operatorname{grad} g$, genauso für h. Zu zeigen: f ist irreduzibel, dann folgt ϕ_p ist irreduzibel.

$$\begin{aligned} f &= \phi_p(x+1) = \sum_{i=0}^{p-1}(x+1)^i = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{\left(\sum_{i=0}^{p} \binom{p}{i} x^i\right) - 1}{x} \\ &= x^{p-1} + \binom{p}{p-1} x^{p-2} + \ldots + \binom{p}{2} x + \binom{p}{1} \end{aligned}$$

Da $p \mid \binom{p}{i}$ (für $1 \leq i \leq p-1$) und $p \nmid 1$ sowie $p^2 \nmid \binom{p}{1} = p$ gilt, ist f nach Eisensteinsches Kriterium irreduzibel. Beispiel:

3. x^2+1 (mit $x+1$ eingesetzt) ergibt x^2+2x+2, irreduzibel nach Eisenstein mit $p = 2$ und $(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, mit Eisenstein folgt: $x^4 + 1$ irreduzibel

[16] „Dies Polynom sieht erstmal nicht nach Eisenstein aus!“

1.3.8 Modulo-p-Kriterium

LEMMA: Seien R und S kommutative Ringe mit Eins und sei $\sigma : R \to S$ ein Homomorphismus. Dann ist $\bar{\sigma} : R[x] \to S[x]$ mit $f = \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} a_i^\sigma x^i$ ein Homomorphismus. Ist σ ein Isomorphismus, so auch $\bar{\sigma}$.

BEWEIS: Seien $f = \sum a_i x^i$, $g = \sum b_i x^i$. Dann ist

$$(a_i + b_i)^\sigma = a_i^\sigma + b_i^\sigma \quad \Rightarrow \quad (f+g)^{\bar{\sigma}} = f^{\bar{\sigma}} + g^{\bar{\sigma}}$$

$$c_k^\sigma = \left(\sum_{i=0}^{k} a_i b_{k-i} \right)^\sigma = \sum_{i=0}^{k} a_i^\sigma b_{k-i}^\sigma \quad \Rightarrow \quad (f \cdot g)^{\bar{\sigma}} = f^{\bar{\sigma}} \cdot g^{\bar{\sigma}}$$

FOLGERUNG: Ist $f = g \cdot h$ in $R[x]$, so ist $f^{\bar{\sigma}} = g^{\bar{\sigma}} \cdot h^{\bar{\sigma}}$ in $S[x]$. Ist $S[x]$ ein ZPE-Ring, so existieren irreduzible Polynome $q_i, \tilde{q}_i$ in $S[x]$ mit $f^{\bar{\sigma}} = q_1 \cdot \ldots \cdot q_r \cdot \tilde{q}_1 \cdot \ldots \tilde{q}_s$ und $g^{\bar{\sigma}} = q_1 \cdot \ldots \cdot q_r$ und $h^{\bar{\sigma}} = \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$.

- *Einfachster Fall:* Ist $f^{\bar{\sigma}}$ irreduzibel in $S[x]$, so muß $g^{\bar{\sigma}}$ oder $h^{\bar{\sigma}}$ Einheit sein. *Problem:* $f = 25x^3 + 75x^2 + 7$ in $\mathbb{Z}/5\mathbb{Z}$ ist $f^{\bar{\sigma}} = 2$.
- *Spezialfall:* $R = \mathbb{Z}$, p Primzahl, $S = \mathbb{Z}/p\mathbb{Z} = \mathrm{GF}(p)$, σ natürlicher Epimorphismus, $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{r} b_i x^i$, $h = \sum_{i=0}^{s} c_i x^i$ und $f = gh$, $a_n \neq 0$, $b_r \neq 0 \neq c_s \Rightarrow a_n = b_r \cdot c_s$. Gilt $p \nmid a_n$, so folgt $a_n^\sigma \neq 0$, wegen $a_n^\sigma = b_r^\sigma \cdot c_s^\sigma$ sind dann auch $b_r^\sigma \neq 0 \neq c_s^\sigma$.

SATZ (Modulo-p-Kriterium): Sei $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ primitiv, p eine Primzahl und $\sigma : \mathbb{Z} \to \mathrm{GF}(p)$ der natürliche Homomorphismus. ist $p \nmid a_n$ und $f^{\bar{\sigma}}$ irreduzibel in $\mathrm{GF}(p)[x]$, so ist f irreduzibel in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$.

BEWEIS: Da f primitiv, muß obiges $g \in \mathbb{Z}[x]$ von Grad 0 eine Einheit in $\mathbb{Z}[x]$, also $\pm$ 1. Nach Satz (1.3.4) ist f auch über $\mathbb{Q}$ irreduzibel.

BEISPIEL:

4. $f = x^4 + 15x^3 + 7$
   - $p = 7$: $f^{\bar{\sigma}} = x^4 + x^3 = x^3(x+1)$ nicht irreduzibel, keine Aussage
   - $p = 3$: $f^{\bar{\sigma}} = x^4 + 1 = x^4 - 3x^2 + 1 = (x^2 + x - 1)(x^2 - x - 1)$ nicht irreduzibel, keine Aussage
   - $p = 5$: $f^{\bar{\sigma}} = x^4 + 2 = (x - a)(x^3 + \ldots)$ (daraus folgt $a^4 = -2 = 3$, aber $a^4 \in \{0, 1\}$, Widerspruch) oder

$$\begin{aligned} x^4 + 2 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + \underbrace{(a+c)}_{=0} x^3 + \underbrace{(b + d + ac)}_{=0} x^2 + \underbrace{(ad + bc)}_{0} x + \underbrace{bd}_{=2} \end{aligned}$$

Damit folgt $a = -c$, $a(d-b) = 0$ (wobei $d = b$ zum Widerspruch $b^2 = 2$ führt), also $a = 0$, $c = 0$, $b = -d$, dann folgt[17] $b^2 = -2 = 3$, auch ein Widerspruch. Damit ist $f^{\bar{\sigma}}$ irreduzibel, mit obigem Satz auch f irreduzibel.

1.3.9 Polynome mit vorgegebenen Werten

IDEE: $f \in \mathbb{Z}[x]$ und $f = gh$, wobei für $a \in \mathbb{Z}$ $f(a) = g(a) \cdot h(a)$ ist.[18]

LEMMA: Sei $0 \neq f \in K[x]$.

1. Ist $a \in K$ mit $f(a) = 0$, so existiert $g \in K[x]$ mit $f = (x-a) \cdot g$
2. Sind $a_i, \ldots, a_k$ paarweise verschiedene Nullstellen von f, so existiert $g \in K[x]$ mit $f = g \cdot \prod_{i=1}^{k}(x - a_i)$
3. f hat höchstens $n = \operatorname{grad} f$ Nullstellen.

SATZ (LAGRANGE 1736-1813): Seien $\alpha_0, \ldots, \alpha_n \in K$ paarweise verschieden und seien $k_0, \ldots, k_n \in K$. Dann existiert genau ein Polynom $f \in K[x]$ mit $\operatorname{grad} f \leq n$, das an den Stellen $\alpha_0, \ldots, \alpha_n$ die Werte $k_0, \ldots, k_n$ annimmt (mit $f(\alpha_i) = k_i$ für $i = 0, \ldots, n$), nämlich

$$f = \sum_{i=0}^{n} k_i \frac{(x-\alpha_0) \cdot \ldots \cdot (x - \alpha_{i-1}) \cdot (x - \alpha_{i+1}) \cdot \ldots \cdot (x - \alpha_n)}{(\alpha_i - \alpha_0) \cdot \ldots \cdot (\alpha_i - \alpha_{i-1}) \cdot (\alpha_i - \alpha_{i+1}) \cdot \ldots \cdot (\alpha_i - \alpha_n)}$$

BEWEIS: Offenbar ist das angegebene f ein Polynom vom Grade $\leq n$. Für jedes $j \in \{1, \ldots, n\}$ ist $f(\alpha_j) = k_j$, da der j-te Summand gleich k_j ist und alle anderen Summanden gleich 0 sind. Sind g, h zwei solche Polynome, dann folgt $(g-h)(\alpha_i) = 0$ für alle i, damit hat $(g-h)$ den Grad $\leq n$, aber $n+1$ Nullstellen, damit ist $g - h = 0$.

BEMERKUNGEN:

1. Gut zu benutzen für Lehrer `:o)`, liefert schöne Funktionen mit vorgegebenen Werten!
2. Ist R ein Integritätsbereich, so gilt das Lemma im Quotientenkörper K, desgleichen der Satz

[17] „Vielleicht hab ich's jetzt zu schnell gemacht!"

[18] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, 6.7

1.3.10 Kronecker-Test auf Irreduzibilität

Sei $f^* = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ gegeben. Kronecker (1829-1891)

Vorbereitung: Schreibe $f^* = c \cdot f$ mit $c \in \mathbb{Q}$, $f \in \mathbb{Z}[x]$ primitiv (Lemma (1.3.3)).

Test: f ist zu testen. Sei $\operatorname{grad} f = n$. Ist $f = g \cdot h \in \mathbb{Z}[x]$, so ist oBdA $\operatorname{grad} g \leq \frac{n}{2}$. Ist also f reduzibel, so existiert ein Polynom g vom Grad $\leq \frac{n}{2}$ mit $g(a) \mid f(a)$ für alle $a \in \mathbb{Z}$. Sei $m = \left\lfloor \frac{n}{2} \right\rfloor$.

1. Wähle $\alpha_0, \ldots, \alpha_m \in \mathbb{Z}$.

2. Bestimme $f(\alpha_i)$ für $i = 0, \ldots, m$ (möglichst so, daß $f(\alpha_i)$ möglichst wenige Teiler haben).

3. Bestimme sämtliche Teiler von $f(\alpha_i)$, sei $M_i = \{c \in \mathbb{Z} \mid (c \mid f(\alpha_i))\}$.

4. Zu jeder Auswahl $(k_0, \ldots, k_m) \in M_0 \times \ldots \times M_m$:

   (a) Bilde das eindeutig bestimmte (1.3.9) Polynom $g \in \mathbb{Q}[x]$ vom Grad $\leq m$ mit $g(\alpha_i) = k_i$ für $i = 0, \ldots, m$.

   (b) Fallunterscheidung:

      i. Falls $g \notin \mathbb{Z}[x]$ oder $g \in \mathbb{Z}[x]$ aber $g \nmid f$, gehe zum nächsten $(m+1)$-Tupel $(k_0, \ldots, k_m)$ über.

      ii. Falls $g \in \mathbb{Z}[x]$ mit $g \mid f$, so ist f reduzibel, Abbruch.

5. Falls bei keinem $(m+1)$-Tupel abgebrochen wurde, existiert kein Teiler, damit ist f irreduzibel.

Da jede Teiler g im Verfahren für $(k_0, \ldots, k_m) = (g(\alpha_0), \ldots, g(\alpha_m))$ auftritt, gilt: Tritt im Verfahren kein Teiler auf, damit ist f irreduzibel.

Beispiel:

5. Beispiel zum Kronecker-Test:

$$\begin{aligned} f^* &= \frac{5}{2}x^5 - 7x^4 - \frac{7}{3}x^3 + \frac{161}{6}x^2 + \frac{7}{2} \\ &= \frac{7}{6}(3x^5 - 6x^4 - 2x^3 + 23x^2 - 35x + 3) \end{aligned}$$

Damit ist $n = 5, m = 2$. Finden der α_i:

i	x	$f(x)$	α_i	$f(\alpha_i)$	M_i
0	0	3	-2	-11	$\{1, -1, 11, -11\}$
	1	14			
	-1	54			
1	2	9	0	3	$\{1, -1, 3, -3\}$
	-2	-11			
2	3	294	2	9	$\{1, -1, 3, -3, 9, -9\}$

Damit kann man für jedes i das Polynom g bestimmen, was an den Stellen α_i die Werte k_i annehmen:

$$\begin{aligned} g &= k_0 \frac{(x-\alpha_1)(x-\alpha_2)}{(\alpha_0-\alpha_1)(\alpha_0-\alpha_2)} + k_1 \frac{(x-\alpha_0)(x-\alpha_2)}{(\alpha_1-\alpha_0)(\alpha_0-\alpha_2)} + k_2 \frac{(x-\alpha_0)(x-\alpha_1)}{(\alpha_2-\alpha_0)(\alpha_2-\alpha_1)} \\ &= \frac{(k_0 - 2k_1 + k_2)x^2 + (-2k_0 + 2k_2)x + 8k_1}{8} \end{aligned}$$

Da für $(k_0, k_1, k_2) \in M_0 \times M_1 \times M_2$ gibt es $4 \cdot 4 \cdot 6 = 96$ Kombinationsmöglichkeiten, hier nur exemplarisch drei davon:

(a) $k_0 = 1, k_1 = -1, k_2 = 3, \Rightarrow y = \frac{3}{4}x^2 + \frac{1}{2}x - 1 \notin \mathbb{Z}[x]$

(b) $k_0 = -1, k_1 = -3, k_2 = 3 \Rightarrow g = x^2 + x - 3g(3) = q \nmid 294 = f(3) \Rightarrow g \nmid f$

(c) $k_0 = 11, k_1 = 3, k_2 = 3 \Rightarrow g = x^2 - 2x + 3, f = (x^2 - 2x + 3)(3x^2 - 11x + 1)$

2 Körpererweiterungen

2.4 Einfache Körpererweiterungen

2.4.1 Körpererweiterungen

Seien K, L Körper mit $K \leq L$.

DEFINITION:

1. Wir nennen L einen *Erweiterungskörper* von K und das Paar (K, L) eine *Körpererweiterung* L/K.

2. Oft wird für $S \subseteq L$ folgende Menge das Erzeugnis genannt: $\langle S \rangle := \bigcap_{S \subseteq T \leq L} T$. Hier jedoch:

$$K(S) := \bigcap \{T \mid K, S \subseteq T \leq L\}$$

   Wobei $K(S)$ gesprochen wird als K *adjungiert* S. Offenbar ist $K(S)$ der kleinste Teilkörper von L, der K und S enthält; man sagt „$K(S)$ entsteht aus K durch *Adjunktion* der Menge S“. Für $S = \{\alpha_1, \ldots, \alpha_n\}$ schreibt man $K(\alpha_1, \ldots, \alpha_n)$ statt $K(\{\alpha_1, \ldots, \alpha_n\})$.

3. (K, L) ist eine *einfache Körpererweiterung*, wenn es ein $\alpha \in L$ gibt, so dass $L = K(\alpha)$. Jedes solche α nennt man ein *primitives Element* der Körpererweiterung (K, L).

SATZ: Sei (K, L) eine Körpererweiterung und sei $S \subseteq L$. Sei $R_0 := K \cup S$ und induktiv definiert $R_{n+1} := \{a - b, ac^{-1} \mid a, b, c \in R_n, c \neq 0\}$ für alle $n \in \mathbb{N}_0$. Dann ist $K(S) = \bigcup_{n=0}^{\infty} R_n$.

BEWEIS: Sei[19] $W := \bigcup_{n=0}^{\infty} R_n$, zu zeigen: $K(S) = W$.

„$\subseteq$“ Wir zeigen: $W \leq L$ (daraus folgt, da $K \cup S \subseteq R_0 \subseteq W$, dass $K(S) \subseteq W$). *Beweis:* $R_n \subseteq R_{n+1}$ für alle n, denn $0, 1 \in R_0$ für alle n (triviale Induktion) und somit $a - 0 \in R_{n+1}$ für $a \in R_n$. Wenn $\alpha, \beta \in W$, so ex. n, m mit $\alpha \in R_n, \beta \in R_m, n \leq m$ (o.B.d.A.), damit $\alpha\beta \in R_m$, also $\alpha - \beta \in R_{m+1}, \alpha\beta^{-1} \in R_{m+1} \subseteq W$, d.h. $\alpha - \beta \in W, \alpha\beta^{-1} \in W$, daraus folgt: $W \leq L$.

„$\supseteq$“ Wir zeigen: $R_n \subseteq K(S)$ für alle $n \in \mathbb{N}_0$. *Beweis:* Induktion. $R_0 \subset K(S)$ nach Definition. $R_n \subseteq K(S) \Rightarrow a - b \in K(S)$ und $ac^{-1} \in K(S)$ für $a, b \in R_n \Rightarrow R_{n+1} \subseteq K(S) \Rightarrow W = \bigcup_{n=0}^{\infty} \subseteq K(S)$

[19] „Sie sehen dem Satz schon an, daß er unschön ist und nicht viel nützt!“

Beispiele:

6. $(\mathbb{Q},\mathbb{R}),(\mathbb{Q},\mathbb{C}),(\mathbb{R},\mathbb{C})$ sind Köreperweiterungen.

   (a) $(\mathbb{R},\mathbb{C})$ ist einfach, denn $\mathbb{C}=\mathbb{R}(i)$ Und somit muß jedes $T\leq\mathbb{C}$ mit $\mathbb{R}\leq T, i\in T$ alle $a+bi$ enthalten, also $T=\mathbb{C}$. Auch $-i$ ist primitives Element und jedes $u\in\mathbb{C}\setminus\mathbb{R}$ ist primitives Element.

   (b) $(\mathbb{Q},\mathbb{R})$ ist nicht einfach. *Beweis:* Aus $\mathbb{R}=\mathbb{Q}(\alpha)$ folgt: $\mathbb{R}=\bigcup_{n=0}^{\infty}R_n$ mit $R_0=\mathbb{Q}\cup\{\alpha\}$ (also abzählbar). Ist R_n abzählbar, so ist (wegen der Existenz einer surjektiven Abbildung $R_n\times R_n\to\{a-b\mid a,b\in R_n\}$) auch R_{n+1} abzählbar, somit letztendlich auch $\mathbb{Q}(\alpha)=\bigcup_{n=0}^{\infty}R_n$ abzählbar, damit kann $\mathbb{Q}(\alpha)$ nicht gleich $\mathbb{R}$ sein.

2.4.2 Algebraische und transzendente Erweiterungen

$K\leq L,\alpha\in L$. *Frage:* Wie sieht $K(\alpha)$ aus? $1,\alpha,\alpha^2,\alpha^n$ liegen in $K(\alpha)$. Damit auch $\sum_{i=0}^{n}k_i\alpha^i=f(\alpha)$ mit $f=\sum_{i=0}^{n}k_ix^i$.

Lemma: $\phi_\alpha: K[x]\to K(\alpha)$ mit $f\mapsto f(\alpha)$ ist ein Homomorphismus mit $k^{\phi_\alpha}=k$ für alle $k\in K$ (da k ein konstantes Polynom) und $x^{\phi_\alpha}=\alpha$.

Beweis: Lemma (1.3.1)

Definitionen: Sei $K\leq L$ Körper, $\alpha\in L$.

- α heißt *algebraisch über K* $\Leftrightarrow$ $\operatorname{Kern}\phi_\alpha\neq 0$ ($\Leftrightarrow\exists f\in K[x]$ mit $f\neq 0$ und $f(\alpha)=0$).

- α heißt *transzendent über K* $\Leftrightarrow$ $\operatorname{Kern}\phi_\alpha=0$ ($\Leftrightarrow f(\alpha)=0\Rightarrow f=0$).

Beispiele:

7. $\alpha\in K\Rightarrow f=x-\alpha\in K[x]$ und $f(\alpha)=\alpha-\alpha=0$. Also ist jedes Element aus K algebraisch über K.

8. $K=\mathbb{Q},L=\mathbb{C},\alpha=\sqrt{2}\Rightarrow f=x^2-2\Rightarrow f(\alpha)=(\sqrt{2})^2-2=0$. Auch $\alpha=\sqrt[5]{7}$ usw.[20] ist algebraisch (über $\mathbb{Q}$) $\alpha=i$ ist algebraisch (Nullstelle von x^2+1) über $\mathbb{Q}$.

9. π und e sind transzendent über $\mathbb{Q}$ (definiert mit Hilfe der Analysis[21]: $e=\exp(1)$ und $\frac{\pi}{2}$ kleinste positive Nullstelle von $\cos x$, Beweis zur

[20] Nehmen wir $\sqrt[5]{7}$, meine Lieblingszahl!
[21] „Cosinus, die wilde Reihe!“

transzendenten Erweiterung: Stewart Seite 68-77, der Beweis für e ist von HERMITE (1873), für π von LINDEMANN (1882)), aber π und e sind nach Beispiel 2 algebraisch über $\mathbb{R}$.

10. Für K Körper, $L := K(x)$ der Körper der rationalen Funktionen über K und $\alpha = x \in L$ betrachte $K[t]$ über K. Setzt man $\alpha = x \in L$ in Polynom $f = \sum_{i=0}^{n} a_i t^i \in K[t]$ ein, so erhält man $f(x) = \sum_{i=0}^{n} a_i x^i$. Dieses ist gleich 0 genau dann, wenn $a_i = 0$ für alle i, genau dann, wenn $f = 0$. Also ist $\operatorname{Kern} \Phi_x = \{0\}$, d.h. x transzendent über K.

    Bemerkung: L ist tatsächlich K adjungiert $\{x\}$, d.h. die alte Bezeichnung $K(x)$ passt mit Definition (2.4.1) zusammen. *Beweis:* Jeder Teilkörper T von L, der K und x enthält, enthält nach Lemma (2.4.2) alle $f(x)$ und dann auch $\frac{f(x)}{g(x)}$ für $g(x) \neq 0$, also ganz L.

2.4.3 Einfach transzendente Körpererweiterungen

DEFINITION: Seien K, L_1, L_2 Körper mit $K \leq L_i$. Dann heißen L_1 und L_2 *über K isomorph*, wenn es einen Isomorphismus $\sigma : L_1 \to L_2$ gibt mit $k^\sigma = k$ für alle $k \in K$.

SATZ: Ist (K, L) eine Körpererweiterung und $\alpha \in L$ transzendent über K, so existiert ein Isomorphismus $\varphi : K(x) \to K(\alpha)$ mit $k^\varphi = k$ für alle $k \in K$ und $x^\varphi = \alpha$; insbesondere sind $K(x)$ und $K(\alpha)$ über K isomorph.

BEWEIS[22]: Nach Lemma (2.4.2) existiert ein Homomorphismus $\phi_\alpha : K[x] \to K(\alpha)$ mit $k^{\phi_\alpha} = k$ für alle $k \in K$ und $x^{\phi_\alpha} = \alpha$. Da α transzendent, ist $\operatorname{Kern} \phi_\alpha = 0$, d.h. ϕ_α ist ein Monomorphismus und induziert einen Isomorphismus $\sigma : K[x] \to K[x]^{\phi_\alpha} =: R \leq K(\alpha)$. Da[23] $R \neq 0$, enthält nach Satz (1.1.6) $K(\alpha)$ einen Quotientenkörper Q von R als Teilkörper. Offenbar ist $K, \{\alpha\} \subseteq R \subseteq Q$. Da $K(\alpha)$ der kleinste solche Teilkörper von L ist, folgt $Q = K(\alpha)$. Nach Satz (1.1.5) läßt sich σ zu einem Isomorphismus $\bar{\sigma} : K(x) \to Q = K(\alpha)$ fortsetzen. Somit $k^{\bar{\sigma}} = k\sigma = k$ für alle $k \in K$ und $x^{\bar{\sigma}} = x^\sigma = x$.

BEMERKUNG: Siehe Beispiel (9) in (2.4.2): Es ist $\mathbb{Q}(e) \simeq \mathbb{Q}(x) \simeq \mathbb{Q}(\pi)$, daraus folgt natürlich nicht $e = \pi$!

[22] siehe auch Beweis zu (1.1.11)
[23] „Er ist dicke von null verschieden…“

2.4.4 Einfache algebraische Körpererweiterungen

Satz: Ist (K, L) eine Körpererweiterung und $\alpha \in L$ algebraisch über K, dann gilt:

1. Es existiert genau ein normiertes (d.h. höchster Koeffizient ist 1) irreduzibles Polynom $p_\alpha \in K[x]$ mit
   (a) $p_\alpha(\alpha) = 0$ und
   (b) $f(\alpha) = 0 \Rightarrow p_\alpha \mid f$, d.h. mit $\operatorname{Kern} \phi_\alpha = K[x]p_\alpha$
2. Es ist $K(\alpha) \simeq K[x]/K[x]p_\alpha$; genauer: es existiert ein Isomorphismus $\bar{\phi}_\alpha$ von $K[x]/K[x]p_\alpha$ auf $K(\alpha)$ mit $(k+K[x]p_\alpha)^{\bar{\phi}_\alpha} = k$ für alle $k \in K$ und $(x+K[x]p_\alpha)^{\bar{\phi}_\alpha} = \alpha$
3. Ist $\operatorname{grad} p_\alpha = n$, so bilden $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ eine Basis von $K(\alpha)$ über K (als K-Vektorraum), d.h. jedes $\beta \in K(\alpha)$ läßt sich eindeutig in der Form $\beta = \sum_{i=0}^{n-1} c_i \alpha^i$ mit $c_i \in K$ darstellen.

Definition: p_α heißt *Minimalpolynom* oder *definierendes Polynom*

Beweis:

1. Nach Lemma (2.4.2) ist $\phi_\alpha : K[x] \to K(\alpha), f \mapsto f(\alpha)$ ein Homomorphismus mit $k^{\phi_\alpha} = k$ für alle $k \in K$ und $x^{\phi_\alpha} = x$. Da α algebraisch über K, ist $\operatorname{Kern} \phi_\alpha \neq 0$. Es gilt $\operatorname{Bild} \phi_\alpha = K[x]^{\phi_\alpha}$ ist ein Teilring von $K(\alpha)$, also Integritätsbereich ungleich Null. Nach (1.1.9) ist $\operatorname{Kern} \phi_\alpha$ ein Primideal im Hauptidealring $K[x]$ mit $0 \overset{\text{Kern}\neq 0}{<} \operatorname{Kern} \phi_\alpha \overset{\text{Bild}\neq 0}{<} K[x]$. Nach Korollar (1.2.3) existiert irreduzibles Polynom $p \in K[x]$ mit $\operatorname{Kern} \phi_\alpha = K[x]p$. Sei $p_\alpha \sim p$ mit höchstem Koeffizienten 1. Offenbar erfüllt p_α (1*a*) und (1*b*).

   Hat q die Eigenschaften (1*a*) und (1*b*), dann gilt $\operatorname{Kern} \phi_\alpha = K[x]q$, wenn q normiert ist, so folgt $q = p_\alpha$.

2. Der Homomorphiesatz besagt: $\operatorname{Bild} \phi_\alpha \simeq K[x]/K[x]p_\alpha$, nach Korollar (1.2.3) ist $K[x]p_\alpha$ ein maximales Ideal, also ist $\operatorname{Bild} \phi_\alpha$ ein Teilkörper von $K(\alpha)$, der K und α enthält. Da $K(\alpha)$ der kleinste solche Teilkörper von L ist, folgt: $K(\alpha) = \operatorname{Bild} \phi_\alpha \simeq K[x]/K[x]p_\alpha$.

   Für den Isomorphismus $\sigma : K[x]/K[x]p_\alpha \to \operatorname{Bild} \phi_\alpha$ gilt $(k+\operatorname{Kern} \phi_\alpha)^\sigma = k^{\phi_\alpha} = k$ und $(x + \operatorname{Kern} \phi_\alpha)^\sigma = x^{\phi_\alpha} = \alpha$.

3. Es ist $K(\alpha) = \operatorname{Bild} \phi_\alpha = \{ f(\alpha) \mid f \in K[x]\}$. Für $f \in K[x]$ existieren $q, r \in K[x]$ mit $f = q \cdot p_\alpha + r$ und $\operatorname{grad} r < \operatorname{grad} p_\alpha$. Also $f(\alpha) = q(\alpha) \cdot p_\alpha(\alpha) + r(\alpha) = r(\alpha)$.

   Eindeutigkeit der Darstellung: Angenommen, $r, s \in K[x]$ vom Grad kleiner n mit $r(\alpha) = \beta = s(\alpha)$. Dann folgt: $(r-s)(\alpha) = r(\alpha) - s(\alpha) = 0$. Damit ist $(r - s) \in \operatorname{Kern} \phi_\alpha = K[x]p_\alpha$. Damit existiert $q \in K[x]$ mit $r - s = q \cdot p_\alpha$. Der Grad von $r-s$ ist kleiner n, folgt aus der Gradformel, daß $q \cdot p_\alpha$ den Grad 0 haben muß, damit ist $q = 0$ und somit $r = s$.

FRAGEN: Wie erhält man p_α und wie rechnet man in $K(\alpha)$?

ANTWORT:

- Beispiel (6a): $K = \mathbb{Q}$, $L = \mathbb{C}$, aus $\alpha = \sqrt{1+\sqrt{3}}$ erhält man $\alpha^2 = 1+\sqrt{3}$, dann erhält man $(\alpha^2-1)^2 = 3$, damit ist $\alpha^4 - 2\alpha^2 + 1 = 3$, es ist also α Nullstelle von $p_\alpha = x^4 - 2x^2 - 2$ (irreduzibel nach Eisenstein).

  Beispiel (6a): $\alpha = e^{\frac{2\pi i}{3}}$, dann ist $\alpha^3 = e^{2\pi i} = 1$. Damit: $x^3 - 1 = (x-1)(x^2+x+1)$ (reduzibel, richtigen der Faktoren suchen), damit ist $p_\alpha = x^2 + x + 1$.

- In $K(\alpha)$ rechnet man wie in $K[x]/K[x]p_\alpha$. Geht's auch einfacher? Sei $n = \operatorname{grad} p_\alpha$, $f, g \in K[x]$ mit Grad kleiner als n. Betrachte $\beta = f(\alpha), \gamma = g(\alpha)$

  – Addition/Subtraktion:

  $$\beta \pm \gamma = f(\alpha) \pm g(\alpha) = (f \pm g)(\alpha)$$

  – Multiplikation: verwende Division mit Rest: $fg = qp_\alpha + r$, wobei $q, r \in K[x]$ und $\operatorname{grad} r < n$; dann ist

  $$\beta \cdot \gamma = f(\alpha) \cdot g(\alpha) = (f \cdot g)(\alpha) = q(\alpha)p_\alpha(\alpha) + r(\alpha) = r(\alpha)$$

  – Division: Wie Multiplikation, gebraucht wird nur γ^{-1} Da $\operatorname{grad} g < n$ und p_α irreduzibel, ist $1 \in \operatorname{ggT}(g, p_\alpha) = K^*$. Mit Satz (1.2.9) existieren $q_1, q_2 \in K[x]$ mit $1 = q_1 p_\alpha + g q_2$. Setze nun α ein:

  $$1 = 1(\alpha) = q_1(\alpha)p_\alpha(\alpha) + g(\alpha)q_2(\alpha) = g(\alpha)q_2(\alpha) = \gamma \cdot q_2(\alpha)$$

  Somit ist $q_2(\alpha)$ das inverse zu γ (hat auch den richtigen Grad, wie leicht einzusehen ist).

BEISPIEL:

11. $\mathbb{Q}(\sqrt[3]{2})$, dann ist $p_\alpha = x^3 - 2$ für $\alpha = \sqrt[3]{2}$. Die Elemente haben also die Form $c_0 + c_1\sqrt[3]{2} + c_2(\sqrt[3]{2})^2$. Sei zum Beispiel $\gamma = 1 - \sqrt[3]{2} + (\sqrt[3]{2})^2 = g(\alpha)$ mit $g = x^2 - x + 1$, gesucht ist γ^{-1}.

$$\begin{aligned}
x^3 - 2 &= (x^2 - x + 1) \cdot x + (x^2 - x - 2) \\
(x^2 - x + 1) &= (x^2 - x - 2) \cdot 1 + 3 \\
3 &= (x^2 - x + 1) - (x^2 - x - 2) \\
&= (x^2 - x + 1) - ((x^3 - 2) - x(x^2 - x + 1)) \\
&= -(x^3 - 2) + (x + 1) \cdot (x^2 - x + 1) \\
1 &= -\frac{1}{3}p_\alpha + \frac{1}{3}(x + 1)g
\end{aligned}$$

Damit[24] ist $\gamma^{-1} = \frac{1}{3}(\sqrt[3]{2} + 1)$.

2.4.5 Konstruktion einfach algebraischer Körpererweiterungen

Satz: Ist K ein Körper und p ein irreduzibles Polynom aus $K[x]$, so gibt es einen einfachen algebraischen Erweiterungskörper $K(\alpha)$ von K, und bis auf Isomorphie über K auch nur einen, mit $p(\alpha) = 0$.

Beweis: Sei $S = K[x]/K[x]p$, nach Korollar (1.2.3) ist $K[x]p$ ein maximales Ideal in $K[x]$ und damit S ein Körper. Sei $\nu : K[x] \to S$ der natürliche Homomorphismus. Für $k \in K$ ist $k^\nu = k + K[x]p \neq 0$, d.h. $\nu|_K$ ist ein Monomorphismus. Nach Satz (1.1.4) existiert ein Ring $L \geq K$ und ein Isomorphismus $\sigma : S \to L$ mit $k^{\nu\sigma} = k$ für alle $k \in K$. Da S Körper ist, ist L auch ein Körper. Sei $\alpha := x^{\nu\sigma}$. Sei $p = \sum_{i=0}^n a_i x^i$. Dann ist

$$\begin{aligned}
p(\alpha) &= \sum_{i=0}^n a_i \alpha^i \\
\text{wegen } a_i = a_i^{\nu\sigma} \quad &= \sum_{i=0}^n a_i^{\nu\sigma} (x^{\nu\sigma})^i \\
\text{wegen } \nu\sigma \text{ Homomoprhismus} \quad &= \left(\sum_{i=0}^n a_i x^i\right)^{\nu\sigma} \\
&= p^{\nu\sigma} = 0^\sigma = 0
\end{aligned}$$

Damit ist $K(\alpha)$ in L die gesuchte einfache algebraische Erweiterung. Der folgende Satz (2.4.6) angewandt mit $\sigma = \mathrm{id}$ liefert zudem die Eindeutigkeit.

[24]„Der größte gemeinsame Teiler war 1, also 3 zum Beispiel!“

2.4.6 Isomorphismus

SATZ: Sei σ ein Isomorphismus des Körpers K auf den Körper $K^\sigma = \{a^\sigma \mid a \in K\}$ und sei $p = \sum_{i=0}^n a_i x^i \in K[x]$ irreduzibel. Dann ist $p^{\bar\sigma} = \sum_{i=0}^n a_i^\sigma x^i \in K^\sigma[x]$ irreduzibel. Seien $K(\alpha)$ und $K^\sigma(\beta)$ (einfache algebraische) Erweiterungen von K bzw. K^σ mit Nullstellen α von p bzw. β von $p^{\bar\sigma}$. Dann kann σ fortgesetzt werden zu einem Isomorphismus $\sigma^* : K(\alpha) \to K^\sigma(\beta)$ mit $\alpha^{\sigma^*} = \beta$.

BEWEIS: Nach Lemma (1.3.8) ist $\bar\sigma : K[x] \to K^\sigma[x]$ ein Ringisomorphismus. Sei $p^{\bar\sigma} = f \cdot g$, somit $p = f^{\bar\sigma^{-1}} \cdot g^{\bar\sigma^{-1}}$, also $f^{\bar\sigma^{-1}}$ oder $g^{\bar\sigma^{-1}}$ hat Grad 0, womit entweder f oder g den Grad 0 hat. Nach Satz (2.4.4)(b) ist

$$\begin{tikzcd}
K(\alpha) \arrow[d, "\bar\phi_\alpha^{-1}"'] & K^\sigma(\beta) \\
K[x]/K[x]p \arrow[r, dashed, "\tau?"] & K^\sigma[x]/K^\sigma[x]p^{\bar\sigma} \arrow[u, "\bar\phi_\beta"']
\end{tikzcd}$$

Gesucht ist also die Abbildung τ. Sei

$$\tau : K[x]/K[x]p \to K^\sigma[x]/K^\sigma[x]p^{\bar\sigma} \text{ mit } f + K[x]p \mapsto f^{\bar\sigma} + K^\sigma[x]p^{\bar\sigma}$$

Dann ist:

$$\begin{array}{rcl}
 & & f + K[x]p = g + K[x]p \\
 & \Leftrightarrow & f - g \in K[x]p \\
 & \Leftrightarrow & p \mid f - g \\
\text{wegen } \bar\sigma \text{ Isom.} & \Leftrightarrow & p^{\bar\sigma} \mid f^{\bar\sigma} - g^{\bar\sigma} \\
 & \Leftrightarrow & f^{\bar\sigma} + K^\sigma p^{\bar\sigma} = g^{\bar\sigma} + K^\sigma[x]p^{\bar\sigma}
\end{array}$$

Also ist τ wohldefiniert („$\Rightarrow$“) und injektiv („$\Leftarrow$“), die Surjektivität von τ ist trivial, da $\bar\sigma$ Isomorphismus ist.

Sei $\sigma^* = \bar\phi_\alpha^{-1}\tau\bar\phi_\beta : K(\alpha) \to K^\sigma(\beta)$. Dies ist ein Isomorphismus, da $\bar\phi_\alpha = \bar\phi_\beta$ ein Isomorphismus ist. Für $k \in K$ gilt:

$$\begin{array}{rcl}
k\sigma^* & = & (k + K[x]p)^{\tau\bar\phi_\beta} \\
 & \overset{\tau}{=} & (k^{\bar\sigma} + K^\sigma[x]p^{\bar\sigma})^{\bar\phi_\beta} \\
 & \overset{\bar\sigma}{=} & (k^\sigma + K^\sigma[x]p^{\bar\sigma})^{\bar\phi_\beta} \\
 & \overset{\bar\phi_\beta}{=} & k^\sigma \\
\alpha^{\sigma^*} & = & (x + K[x])^{\tau\bar\phi_\beta} \\
 & \overset{1^\sigma=1}{=} & (x + K^\sigma[x]p^{\bar\sigma})^{\bar\phi_\beta}
\end{array}$$

BEISPIEL:

7. Betrachte $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[3]{2} \in \mathbb{R}, p = x^3 - 2$. Seien

$$\begin{aligned} \beta &= \alpha \cdot e^{\frac{2\pi i}{3}} \to \beta^3 = \alpha^3 e^{2\pi i} = \alpha^3 = 2 \\ \gamma &= \alpha \cdot e^{\frac{4\pi i}{3}} \to \gamma^3 = \alpha^3 e^{4\pi i} = 2 \end{aligned}$$

Dann ist $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta) \simeq \mathbb{Q}(\gamma)$, die Elemente in $\mathbb{Q}(\alpha)$ haben die Form $c_0 + c_1\alpha + c_2\alpha^2$

2.5 Endliche Körpererweiterungen, Grad

2.5.1 Grad einer Körpererweiterung

SATZ: Seien $K \leq L$ Körper. Dann ist L ein Vektorraum über K, wenn als Addition die Addition im Körper L und als Skalarmultiplikation mit Elementen aus K die in L erklärte Körpermultiplikation genommen wird.

BEWEIS: Addition und Skalarmultiplikation sind offensichtlich wohldefiniert, $(L, +)$ abelsche Gruppe ist trivial, weil L Körper ist. Für $\lambda, \mu \in K, a, b \in L$ gilt:

$$\begin{aligned} (\lambda + \mu)a &= \lambda a + \mu a \\ \lambda(a + b) &= \lambda a + \lambda b \\ (\lambda\mu)a &= \lambda(\mu a) \end{aligned}$$

DEFINITION:

1. Sei $[L : K] := \dim_K L =$ *Grad der Körpererweiterung* (K, L) oder *Grad von L über K*

2. L heißt *endlich über K* bzw. (K, L) heißt endlich genau dann, wenn $[L : K] < \infty$

BEISPIELE:

1. Ist $K \leq L$ und $\alpha \in L$ algebraisch über K, so ist $[K(\alpha) : K] = n$, wobei $n = \operatorname{grad} p_\alpha$ der Grad des Minimalpolynoms von α ist.

2. Betrachte $[\mathbb{C} : \mathbb{R}] = 2$, die Basis ist $\{1, i\}$, Minimalpolynom ist demnach $x^2 + 1$.

3. Sonderfall: $[L : K] = 1$, dann ist $L = K$

4. Es gilt: $[\mathbb{R} : \mathbb{Q}] = \infty$; *Beweis:* Endlich dimensionaler $\mathbb{Q}$-Vektorraum ist abzählbar.

2.5.2 Algebraische Körpererweiterungen

Seien $K \leq L$ Körper.

DEFINITION: (K, L) heißt *algebraisch* (oder L algebraisch über K), wenn jedes $\alpha \in L$ algebraisch über K ist.

SATZ: Jede endliche Körpererweiterung ist algebraisch.

BEWEIS: Sei $[L : K] = n \in \mathbb{N}$ und $\alpha \in L$. Dann sind $1, \alpha, \alpha^2, \ldots, \alpha^n$ $n+1$ Elemente des n-dimensionalen K-Vektorraum L, also linear abhängig. Somit existieren $c_i \in K$, nicht alle 0 mit $c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0$, somit $f := \sum_{i=0}^{n} c_i x^i \in K[x], f \neq 0$ und $f(\alpha) = 0$. Nach Definition (2.4.2) ist α algebraisch über K, also L algebraisch über K.

BEMERKUNGEN:

1. $\operatorname{grad} f \leq n$ und $p_\alpha \mid f$ nach (2.4.4), also $\operatorname{grad}[K(\alpha) : K] \leq n = [L : K]$
2. Aus $[L : K] < \infty$ folgt: L hat keine transzendente Elemente über K, also $[\mathbb{R} : \mathbb{Q}] = \infty$, weil $\mathbb{R}$ transzendente Elemente über $\mathbb{Q}$ besitzt.
3. Gilt die Umkehrung des Satzes?

BEISPIEL:

5. $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$. Minimalpolynome sind $x^2 - 2$ und $x^2 + 1$.

$$\begin{aligned} \mathbb{Q}(\sqrt{2}) &= \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\} \subseteq \mathbb{R} \\ \mathbb{Q}(\sqrt{2})(i) &= \left\{ (a + b\sqrt{2}) + (c + d\sqrt{2})i \;\middle|\; a, b, c, d \in \mathbb{Q} \right\} \\ &= \left\{ a + b\sqrt{2} + ci + d(\sqrt{2})i \;\middle|\; a, b, c, d \in \mathbb{Q} \right\} \end{aligned}$$

Dies ist ein 4-dimensionaler Raum mit Basis $\{1, \sqrt{2}, i, i\sqrt{2}\}$.

2.5.3 Gradsatz (1)

SATZ: Seien $K \leq L \leq M$ Körper und $\alpha_1, \ldots, \alpha_n$ eine Basis von L über K und $\beta_1, \ldots, \beta_m$ Basis von M über L. Dann bilden die $\alpha_i\beta_j (i = 1, \ldots, n, j = 1, \ldots, m)$ eine Basis von M über K. Insbesondere ist $[M : K]$ endlich und $[M : K] = [M : L] \cdot [L : K]$.

BEWEIS: Jedes $\gamma \in M$ ist von der Form $\gamma = \sum_{i=1}^{m} b_i\beta_i$ mit $b_i \in L$. Da $\alpha_1, \ldots, \alpha_n$ Basis von L über K, existieren $a_{ij} \in K$ mit $b_i = \sum_{i=1}^{n} a_{ij}\alpha_j$. Somit

$$\begin{aligned}\gamma &= \sum_{i=1}^{m}(\sum_{i=1}^{n} a_{ij}\alpha_j)\beta_i \\ &= \sum_{i,j=1}^{n,m} a_{ij}\alpha_j\beta_i\end{aligned}$$

Damit ist $(\alpha_j\beta_i)_{j=1,\ldots,n,i=1,\ldots,m}$ Erzeugendensystem des K-Vektorraumes M.

$$\begin{aligned} 0 &= \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}\alpha_j\beta_i = \sum_{i=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_j\right)\beta_i \\ \beta_i \text{ lin. unabh. über } L &= \sum_{j=1}^{n} a_{ij}\alpha_j \;\forall\, i = 1, \ldots, m \\ \alpha_i \text{ lin. unabh. über } K &= \alpha_{ij} \;\forall\, j = 1, \ldots, n \;\forall\, i = 1, \ldots, m\end{aligned}$$

2.5.4 Gradsatz (2)

KOROLLAR: Ist L eine endliche Erweiterung von K, so ist der Grad jedes Zwischenkörpers T über K ein Teiler von $[L : K]$. Insbesondere: ist $\alpha \in L$, so ist α algebraisch über K und $\operatorname{grad} p_\alpha = [K(\alpha) : K] \mid [L : K]$.

BEWEIS: $K \leq T \leq L, [L : K]$ endlich $\Rightarrow [T : K] < \infty$ und $[L : T] < \infty \Rightarrow [L : K] = [L : T] \cdot [T : K]$.

2.5.5 endliche bzw. iterierte einfache Erweiterung

KOROLLAR: Jede iterierte einfache algebraische Erweiterung $K(\alpha_1, \ldots, \alpha_r)$ von K (d.h. α_i ist algebraisch über $K(\alpha_1, \ldots, \alpha_{i-1})$ für alle i) ist endlich über K. Somit fallen die Begriffe *iterierte einfache algebraische Erweiterung* und *endliche Erweiterung* zusammen.

BEWEIS: Für jedes i ist $[K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})] = [(K(\alpha_1, \ldots, \alpha_{i-1}))(\alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]$ endlich, also (triviale Induktion) $[K(\alpha_1, \ldots, \alpha_i) : K] < \infty$. Ist umgekehrt $[L : K] < \infty$, so existiert eine Basis $\alpha_1, \ldots, \alpha_r$ über K, also $L = K(\alpha_1, \ldots, \alpha_r)$ und jedes α_i ist algebraisch über K (nach (2.5.2)), erst recht über $K(\alpha_1, \ldots, \alpha_{i-1})$.

2.5.6 algebraische Erweiterungen algebraischer Erweiterungen

Satz: Seien $K \leq L \leq M$ Körper. Ist L algebraisch über K und M algebraisch über L, so ist M algebraisch über K.

Beweis: Sei $\beta \in M$. Nach Voraussetzung ist β algebraisch über L, d.h. es existiert $f = \sum_{i=0}^{n} \alpha_i x^i \in L[x]$ mit $f \neq 0$ und $f(\beta) = 0$. Somit ist β algebraisch über $K(\alpha_0, \ldots, \alpha_n)$. Da $\alpha_i \in L$, ist α_i algebraisch über K für $i = 0, \ldots, n$, also α_i algebraisch über $K(\alpha_0, \ldots, \alpha_{i-1})$. Somit ist $K(\alpha_0, \ldots, \alpha_n, \beta)$ eine iterierte einfache algebraische Erweiterung, also endlich über K. Nach Satz (2.5.2) ist β algebraisch über K. Also ist M algebraisch über K.

2.5.7 algebraischer Abschluß

Seien $K \leq L$ Körper.

Definition: $\mathfrak{A}(K, L) := \{\alpha \in L \mid \alpha \text{ algebraisch über } K\}$ heißt der *algebraische Abschluß von K in L.*

Satz: $\mathfrak{A}(K, L)$ ist ein Teilkörper von L, der größte über K algebraische Teilkörper von L. Ist $\beta \in L \setminus \mathfrak{A}(K, L)$, so ist $(\mathfrak{A}(K, L))(\beta)$ transzendent über $\mathfrak{A}(K, L)$.

Beweis: $K \subseteq \mathfrak{A}(K, L)$ (Beispiel (2)), zu zeigen: Für $a, b, c \in \mathfrak{A}(K, L)$ mit $c \neq 0$ sind $a \pm b, ac^{-1} \in \mathfrak{A}(K, L)$. Für $a, b \in \mathfrak{A}(K, L)$ ist $K(a, b) = (K(a))(b)$ nach (2.5.5) endlich über K, nach (2.5.2) also algebraisch, somit sind $a \pm b, ab, ab^{-1} \in K(a, b)$ algebraisch über K.

Wäre $(\mathfrak{A}(K, L))(\beta)$ algebraisch über $\mathfrak{A}(K, L)$, folgt mit (2.5.6), daß $(\mathfrak{A}(K, L))(\beta)$ algebraisch über K, Widerspruch!

Beispiel:

6. $\mathfrak{A}(\mathbb{Q}, \mathbb{C})$ wird die *Menge der algebraischen Zahlen* genannt. Sowohl $\mathfrak{A}(\mathbb{Q}, \mathbb{C})$ als auch $\mathfrak{A}(\mathbb{Q}, \mathbb{R})$ sind unendliche algebraische Erweiterungen von $\mathbb{Q}$. *Beweis:* Sei $L = \mathfrak{A}(\mathbb{Q}, \mathbb{C})$ oder $L = \mathfrak{A}(\mathbb{Q}, \mathbb{R})$. Angenommen, $[L : \mathbb{Q}] < \infty$, dann ist $[L : \mathbb{Q}] = n$ für ein $n \in \mathbb{N}$. Nach Eisenstein ist $f = x^{n+1} - 2$ irreduzibel über $\mathbb{Q}$ und $\sqrt[n+1]{2} \in L$, mit Beispiel (1) ist $[\mathbb{Q}(\sqrt[n+1]{2}) : \mathbb{Q}] = n + 1 \mid n$ (nach (2.5.4))

2.6 Konstruktionen mit Zirkel und Lineal

Descartes (1638) hat bewiesen, daß folgende Konstruktionen (nur mit Zirkel und Lineal) unmöglich sind:

1. **Quadratur des Kreises**, d.h. zu einem gegebenen Kreis ein flächengleiches Quadrat konstruieren.

2. **Kubusverdopplung**, d.h. zu gegebener Würfelkante eine Kante des Würfels mit doppeltem Volumen konstruieren.

3. **Trisektion des Winkels**, d.h. zu einem gegebenen Winkel φ den Winkel $\frac{\varphi}{3}$ zu konstruieren.

2.6.1 Formulierung des Problems

Seien $E = \mathbb{R}^2$, $P_i = (x_i, y_i)$; sei $d(P_1, P_2) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$. Die *Gerade* durch P_1 und P_2 sei definiert durch[25]

$$P_1P_2 = \begin{cases} \left\{ (x,y) \mid \frac{x-x_1}{x_2-x_1} = \frac{y-y_1}{y_2-y_1} \right\} & \text{falls} \quad x_1 \neq x_2 \text{ und } y_1 \neq y_2 \\ \{ (x,y) \mid x = x_1 \} & \text{falls} \quad x_1 = x_2 \text{ und } y_1 \neq y_2 \\ \{ (x,y) \mid y = y_1 \} & \text{falls} \quad x_1 \neq x_2 \text{ und } y_1 = y_2 \end{cases}$$

Der *Kreis* um P_0 mit Radius r ist $k = \{ (x,y) \mid (x-x_0)^2 + (y-y_0)^2 = r^2 \}$.

Gegeben sei $\mathfrak{P} \subseteq \mathbb{R}^2$. Operationen:

(L) Wähle zwei verschiedene Punkte P_1 und P_2 aus $\mathfrak{P}$ und „ziehe" Gerade durch P_1 und P_2 (d.h. betrachte die Gerade P_1P_2 wie oben definiert).

(Z) Wähle zwei verschiedene Punkte P_1 und P_2 aus $\mathfrak{P}$, „nehme den Abstand $d(P_1, P_2)$ in den Zirkel" und zeichne Kreis um P_0 mit diesem Radius (d.h. betrachte $k = \{ (x,y) \mid (x-x_0)^2 + (y-y_0)^2 = d^2 \}$).

DEFINITIONEN:

1. Ein Punkt $P \in E$ heißt *im ersten Schritt aus $\mathfrak{P}$ konstruierbar*, wenn P Schnittpunkt zweier durch (L) oder (Z) „konstruierter" Objekte ist.

2. Ein Punkt $P \in E$ heißt *konstruierbar aus $\mathfrak{P}$*, falls es eine endliche Folge $P_1, \ldots, P_n$ von Punkten aus E gibt mit $P_n = P$, so daß für jedes i gilt: P_i ist im ersten Schritt aus $\mathfrak{P}_{i-1} := \mathfrak{P} \cup \{P_1, \ldots, P_{i-1}\}$ konstruierbar.

3. Eine Gerade $g \subseteq E$ heißt *im ersten Schritt aus $\mathfrak{P}$ konstruierbar*, wenn $g = P_1P_2$ mit $P_i \in \mathfrak{P}$ ist.

4. Eine Gerade $g \subseteq E$ heißt *konstruierbar aus $\mathfrak{P}$*, wenn es konstruierbare Punkte P_i gibt mit $g = P_1P_2$.

[25] Siehe auch KOECHER/KRIEGER, Ebene Geometrie, 1993

2.6.2 Beispiele

1. Sind P_1 und P_2 konstruierbar, so ist auch der Mittelpunkt von P_1 und P_2 konstruierbar.

2. Wenn $P_0 \notin P_1P_2$ konstruierbar ist, so ist auch das Lot von P_0 auf P_1P_2 konstruierbar.

3. Wenn $P_0 \in P_1P_2$ konstruierbar ist, so ist die Senkrechte in P_0 auf P_1P_2 konstruierbar.

4. Wenn $P_0 \notin P_1P_2$ konstruierbar ist, so ist auch die Parallele zu P_1P_2 durch P_0 konstruierbar.

2.6.3 Definitionen

DEFINITIONEN: Sei $\mathfrak{P} \subseteq \mathbb{R}^2$.

1. $S := S(\mathfrak{P}) := \{a \in \mathbb{R} \mid \exists\, b : ((a,b) \in \mathfrak{P}) \vee ((b,a) \in \mathfrak{P})\}$ sei die Menge aller Koordinaten von Punkten aus $\mathfrak{P}$

2. $\mathcal{K} := \mathcal{K}(\mathfrak{P}) := \mathbb{Q}(S(\mathfrak{P}))$

2.6.4 Grad der Erweiterung um einen Punkt

LEMMA: Sei $\mathfrak{P} \subseteq \mathbb{R}^2$ und $P \in \mathbb{R}^2$ im ersten Schritt aus $\mathfrak{P}$ konstruierbar. Ist $K = \mathcal{K}(\mathfrak{P})$ und $L = \mathcal{K}(\mathfrak{P} \cup \{P\})$, so existiert ein Körper T mit $K \leq T \leq L$, $[T : K] \leq 2$ und $[L : T] \leq 2$. Somit ist $[L : K] = 1, 2$ (oder 4).

BEWEIS: Sei $P = (a,b)$. Mehrere Möglichkeiten, wie P konstruiert wurde:

- Entstanden aus dem Schnitt einer Geraden g und eines Kreises k (d.h. $\{P\} = g \cap k$): Sei $g = P_1P_2$ mit $P_i \in \mathfrak{P}$ (wobei), $k = \{(x,y) \mid (x-x_0)^2 + (y-y_0)^2 = d^2\}$, $P_0 = (x_0, y_0) \in \mathfrak{P}$, $d^2 = (x_3 - x_4)^2 + (y_3 - y_4)^2$.

  Aus $\frac{a-x_1}{x_2-x_1} = \frac{b-y_1}{y_2-y_1}$ folgt $b = \frac{y_2-y_1}{x_2-x_1}(a-x_1) + y_1$. Somit ist, da $P \in g \cap k$,

$$\begin{aligned} d^2 &= (a-x_0)^2 + (b-y_0)^2 \\ &= (a-x_0)^2 + \left(\frac{y_2-y_1}{x_2-x_1}(a-x_1) + y_1 - y_0\right)^2 \end{aligned}$$

  Also ist das Polynom $(x-x_0)^2 + \left(\frac{y_2-y_1}{x_2-x_1}(x-x_1) + y_1 - y_0\right)^2 - d^2$ vom Grad kleiner gleich 2 mit Koeffizienten aus $K[x] = \mathbb{Q}(S)[x]$, das a

als Nullstelle hat. Somit hat $T := K(a)$ höchstens den Grad 2 über K. Genauso hat b höchstens den Grad 2 über K, erst recht über T. Damit ist $L = \mathcal{K}(\mathfrak{P} \cup \{P\}) = \mathbb{Q}(S, a, b) = K(a, b) = T(b)$, also ist $[L : K] \in \{1, 2, 4\}$.

- Entstanden aus dem Schnitt zweier Geraden oder zweier Kreise: analog

2.6.5 Kette von Erweiterungen

SATZ: Sei $\mathfrak{P} \subseteq \mathbb{R}^2$ und $K = \mathcal{K}(\mathfrak{P})$. Ist $P = (a, b) \in \mathbb{R}^2$ konstruierbar aus $\mathfrak{P}$, so sind a und b algebraisch über K und es existieren Teilkörper L_i von $\mathbb{R}$ mit $K = L_0 \leq L_1 \leq \ldots \leq L_k \geq K(a, b)$ und $[L_i : L_{i-1}] = 2$ für $i = 1, \ldots, k$. Insbesondere sind $[K(a) : K]$ und $[K(b) : K]$ Potenzen von 2.

BEWEIS:

- Existenz der L_i: Nach Definition (2.6.1) existieren $P_i, (i = 1, \ldots, n)$ mit $P_n = P = (a, b)$ und P_i im ersten Schritt aus $\mathfrak{P}_{i-1} := \mathfrak{P} \cup \{P_1, \ldots, P_{i-1}\}$ konstruierbar. Sei $K_i = \mathcal{K}(\mathfrak{P}_i), (i = 0, \ldots, n), (\mathfrak{P}_0 = \mathfrak{P})$. Es gilt

$$K_0 = K \leq K_1 \leq K_2 \leq \ldots \leq K_n \geq K(a, b)$$

Definiere folgendes Prädikat:

(A_i) Es existieren $T_0, \ldots, T_{2i}$ mit $[T_j : T_{j-1}] \leq 2, T_0 \geq K, T_{2i} \geq K_i$.

Beweis durch Induktion.

  - A_0 ist mit $T_0 = K$ trivial erfüllt.
  - Sei (A_i) richtig und seien $K_0 = T_0 \leq T_1 \leq \ldots \leq T_{2i} \geq K_i$ und $[T_j : T_{j-1}] \leq 2$.
  - Lemma (2.6.4) mit $K_{\text{dort}} = K_i$ und $L_{\text{dort}} = \mathcal{K}(\mathfrak{P}_i \cup \{P_{i+1}\}) = \mathcal{K}(\mathfrak{P}_{i+1}) = K_{i+1}$ liefert: es existiert ein Körper T mit $K_i \leq T \leq K_{i+1}$ und $[T : K_i] \leq 2, [K_{i+1} : T] \leq 2$.

    Da $[T : K_i] \leq 2$, existiert $\alpha \in T$ mit $T = K_i(\alpha)$ und da $[K_{i+1} : T] \leq 2$, existiert $\beta \in K_{i+1}$ mit $K_{i+1} = T(\beta)$. Setze $T_{2i+1} := T_{2i}(\alpha)$ und $T_{2i+2} := T_{2i+1}(\beta)$.

    Behauptung: (A_{i+1}) gilt. Da $K_i \leq T_{2i}$, folgt: $K_i(\alpha) \leq T_{2i}(\alpha) = T_{2i+1}$. Daraus folgt: $T(\beta) \leq T_{2i+1}(\beta) = T_{2i+2}$. Da α Nullstelle eines Polynoms vom grad ≤ 2 aus $K_i[x] \subseteq T_{2i}[x]$ folgt mit (2.5.1): $[T_{2i+1} : T_{2i}] \leq 2$. Da β Nullstelle eines Polynoms vom grad ≤ 2 aus $T[x] \subseteq T_{2i+1}[x]$ folgt mit (2.5.1): $[T_{2i+2} : T_{2i+1}] \leq 2$. Für

$i = n$ erhalten wir $K = T_0 \leq \ldots \leq T_{2n} \geq K_n \geq K(a,b)$ und $[T_j : T_{j-1}] \leq 2$; nun lasse man überflüssige T_j weg.

- „Insbesondere“: $K \leq K(a) \leq K(a,b) \leq L_k$ und $[L_k : K] = 2^k$ nach (2.5.3). Mit (2.5.4) folgt: $[K(a) : K] \mid 2^k$.

2.6.6 einfache Konstruktionen

Lemma: Sei $\mathfrak{P} \subseteq \mathbb{R}^2$ mit $(0,0),(1,0) \in \mathfrak{P}$. Dann gilt:

(a) Sind $(a,0),(b,0)$ konstruierbar aus $\mathfrak{P}$, so ist auch (a,b) konstruierbar aus $\mathfrak{P}$.

(b) Sind $(a,0),(b,0)$ konstruierbar aus $\mathfrak{P}$, so sind alle Punkte der Form $(a \pm b, 0)$, $(a \cdot b, 0)$ und $(a \cdot b^{-1}, 0)$ konstruierbar aus $\mathfrak{P}$.

(c) Ist $(a,0)$ konstruierbar aus $\mathfrak{P}$ und $a \geq 0$, so ist $(\sqrt{a}, 0)$ konstruierbar aus $\mathfrak{P}$.

Beweis:

(a) Folgt sofort aus (2.6.2).

(b) Mit Strahlensätzen folgt: $(s,0) = \left(\frac{a}{b}, 0\right)$. Produkt: Finde zuerst $\left(\frac{1}{b}, 0\right)$, dann verwende: $(a((b^{-1})^{-1}), 0) = (ab, 0)$.

(c) Es gilt $s^2 = a \cdot 1$, also $s = \sqrt{a}$.

2.6.7 konstruierbare Punkte

Satz: Sei $\mathfrak{P} \subseteq \mathbb{R}^2$ mit $(0,0),(1,0) \in \mathfrak{P}$ und sei $K = \mathcal{K}(\mathfrak{P})$. Seien $K = K_0 \leq K_1 \leq \ldots \leq K_n = L$ Teilkörper von $\mathbb{R}$ mit $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, n$. Sind $a, b \in L$, so ist der Punkt (a,b) konstruierbar aus $\mathfrak{P}$.

Beweis: In drei Schritten:

1. Ist $c \in K$, so ist $(c,0)$ aus $\mathfrak{P}$ konstruierbar. Da $K = \mathbb{Q}(S)$, gilt nach (2.4.1): $K = \bigcup_{i=0}^{\infty} R_i$ mit $R_0 = \mathbb{Q} \cup S$ und $R_{i+1} = \left\{ a - b, \frac{a}{c} \;\middle|\; a, b, c, \in R_i, c \neq 0 \right\}$.

   Offensichtlich sind $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ konstruierbar aus $\mathfrak{P}$. Für $s \in S$ existiert $t \in \mathbb{R}$ mit $(s,t) \in \mathfrak{P}$. Damit sind $(s,0)$ und $(t,0)$ konstruierbar aus $\mathfrak{P}$. Somit gilt für alle $r \in R_0 : (r,0)$ ist aus $\mathfrak{P}$ konstruierbar.

   Mit (2.6.6) gilt für alle $s \in R_{i+1}$: $(s,0)$ ist aus $\mathfrak{P}$ konstruierbar. Damit folgt: alle Punkte $(r,0)$ mit $r \in \bigcup_{i=0}^{\infty} R_i = K$ sind aus $\mathfrak{P}$ konstruierbar.

2. Angenommen nicht alle Punkte $(c, 0)$ mit $c \in L$ sind aus $\mathfrak{P}$ konstruierbar. Dann existiert $j \in \mathbb{N}$ mit: alle Punkte $(c, 0)$ mit $c \in K_j$ sind konstruierbar, aber existiert $d \in K_{j+1}$ mit $(d, 0)$ nicht konstruierbar. Da $[K_{j+1} : K_j] = 2$, existiert $p_d = x^2 + \alpha x + \beta \in K_j[x]$ irreduzibel mit $p_d(d) = 0$. Es gilt:

$$\begin{aligned} & & d = -\frac{\alpha}{2} \pm \sqrt{\frac{\alpha^2}{4} - \beta} \in \mathbb{R} \\ & \implies & \frac{\alpha^2}{4} - \beta \in K_j \\ & \implies & \left(\frac{\alpha^2}{4} - \beta, 0\right) \text{ konstruierbar} \\ \text{mit (2.6.6)} & \implies & \left(\sqrt{\frac{\alpha^2}{4} - \beta}, 0\right) \text{ konstruierbar} \\ \text{mit (2.6.6)} & \implies & \left(-\frac{\alpha}{2} \pm \sqrt{\frac{\alpha^2}{4} - \beta}, 0\right) = (d, 0) \text{ konstruierbar} \end{aligned}$$

Dies ist ein Widerspruch. Somit gilt: $(c, 0)$ konstruierbar für alle $c \in L$.

3. Da somit $(a, 0)$ und $(b, 0)$ konstruierbar sind, ist auch (a, b) konstruierbar.

2.6.8 Kubusverdopplung

Satz: Die Kubusverdopplung ist mir Zirkel und Lineal unmöglich.

Beweis: Einheitswürfel sei gegeben, d.h. Kante habe Länge 1, das Volumen ist damit 1. Gesucht ist Würfel mit Volumen 2, genauer dessen Kante $(a, 0)$. Es gilt: $\mathfrak{P} = \{(0, 0), (1, 0)\}$, damit $K = \mathcal{K}(\mathfrak{P}) = \mathbb{Q}$. Somit ist $a^3 = 2$, damit ist a Nullstelle von $x^3 - 2$ irreduzibel (Eisenstein), daraus folgt: $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Mit (2.6.5) folgt: $(a, 0)$ ist nicht konstruierbar.

2.6.9 Quadratur des Kreises

Satz: Die Quadratur des Kreises ist mir Zirkel und Lineal unmöglich.

Beweis: Gegeben sei der Einheitskreis. Gesuch ist ein Quadrat mit gleicher Fläche, genauer der Punkt $(a, 0)$ mit $a^2 = \pi$, also $a = \sqrt{\pi}$. Es gilt wieder $K = \mathbb{Q}$. Wäre $\sqrt{\pi}$ algebraisch über $\mathbb{Q}$, so auch $\sqrt{\pi}^2 = \pi$, Widerspruch.

2.6.10 Dreiteilung des Winkels

Satz: Der Winkel φ kann genau dann mit Zirkel und Lineal gedrittelt werden, wenn das Polynom $4x^3 - 3x - \cos\varphi$ reduzibel über $\mathbb{Q}(\cos\varphi) = K$ ist.

Beweis: Gegeben seien neben den Punkten $(0,0), (1,0)$ auch $(\cos\varphi, \sin\varphi)$ oder $(\cos\varphi, 0)$, dann ist $K = \mathcal{K}(\mathfrak{P}) = \mathbb{Q}(\cos\varphi)$. Gesucht ist $\left(\cos\frac{\varphi}{3}, 0\right)$. Es gilt mit $\psi = \frac{\varphi}{3}$

$$\begin{aligned}
\Re(\cos 3\psi + i\sin 3\psi) &= \Re(e^{i3\psi}) = \Re\left(\left(e^{i\psi}\right)^3\right) = \Re((\cos\psi + i\sin\psi)^3) \\
&= \Re((\cos\psi)^3 + 3(\cos\psi)^2(i\sin\psi) + 3(\cos\psi)(i\sin\psi)^2 + (i\sin\psi)^3) \\
&= \Re((\cos\psi)^3 - 3(\cos\psi)(\sin\psi)^2 + i\cdot(3(\cos\psi)^2(\sin\psi) - (\sin\psi)^3)) \\
&= (\cos\psi)^3 - 3(\cos\psi)(\sin\psi)^2 \\
&= (\cos\psi)^3 - 3(\cos\psi)(1-\cos^2\psi) \\
&= 4\cos^3\psi - 3\cos\psi \\
\Longrightarrow 0 &= 4\cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3} - \cos\varphi
\end{aligned}$$

Damit ist $\cos\frac{\varphi}{3}$ Nullstelle von $f = 4x^3 - 3x - \cos\varphi$.

- Ist f irreduzibel über $K = \mathbb{Q}(\cos\varphi)$, so ist $\operatorname{grad}(\cos\frac{\varphi}{3}) = 3$, damit ist nach Satz (2.6.5) $\left(\cos\frac{\varphi}{3}, 0\right)$ nicht konstruierbar.
- Ist f reduzibel, so ist $f = g\cdot h$ mit $\operatorname{grad} g, h \le 2$. Da $p_{\cos\frac{\varphi}{3}} \mid f$, gilt $p_{\cos\frac{\varphi}{3}} \mid g$ oder h. Damit ist $\operatorname{grad}(\cos\frac{\varphi}{3}) \le 2$, daher ist $\left(\cos\frac{\varphi}{3}, 0\right)$ nach Satz (2.6.7) konstruierbar.

Korollar: Der Winkel $\varphi = \pi$ ist drittelbar, der Winkel $\varphi = \frac{\pi}{3}$ ist nicht drittelbar mit Zirkel und Lineal, insbesondere gibt es kein allgemeines Verfahren zur Winkeldrittelung.

Beweis: Für $\varphi = \pi$ ist $4x^3 - 3x - \cos\varphi = 4x^3 - 3x + 1$ über $K = \mathbb{Q}$ reduzibel, da $\frac{1}{2}$ Nullstelle ist. Zudem ist $\cos\frac{\pi}{3} = \frac{1}{2}$, der Punkt $(\frac{1}{2}, 0)$ ist aber leicht konstruierbar.

Zu $\varphi = \frac{\pi}{3}$: Das Polynom $f = 4x^3 - 3x - \frac{1}{2}$ über $K = \mathbb{Q}(\frac{1}{2}) = \mathbb{Q}$ ist irreduzibel: Setze $2t + 2$ in $2f$ ein:

$$\begin{aligned}
g(t) &= 8\cdot 2^3(t+1)^3 - 12(t+1) - 1 \\
&= 64(t^3 + 3t^3 + 3t + 1) - 12t - 12 - 1 \\
&= 64t^3 + 3\cdot 64t^2 + 3\cdot 60t + 3\cdot 17
\end{aligned}$$

Nach Eisenstein $(p = 3)$ ist dieses Polynom irreduzibel.

Bemerkungen:

- Siehe auch L. Bieberbach: Theorie der geometrischen Konstruktionen, Birkhäuser 1952; oder in I. Stewart, S. 64.

- Winkeldrittelung geht mit Zirkel und „markiertem“ Lineal (Lineal mit einem fest markierten Abstand d). Nehme dazu an, daß der Winkeln $0 < \varphi < \frac{\pi}{2}$ erfüllt (halbiere Winkel mehrfach, dann dritteln, dann wieder oft genug verdoppeln).

2.7 Zerfällunngskörper, normale Erweiterungen

2.7.1 Zerfällungskörper

Sei K Körper und $f \in K[x]$ und $0 \neq f \in K[x]$.

Definition: Ein Erweiterungskörper L von K heißt ein *Zerfällungskörper* von f über K, wenn es Elemente $\alpha_1, \dots, \alpha_n \in L$ und $c \in K$ gibt mit

(1) $f = c(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ und

(2) $L = K(\alpha_1, \dots, \alpha_n)$.

Für $f = 0$ sei K der Zerfällungskörper.

Bemerkung: Wir schreiben auch $K(f)$ für „den“ Zerfällungskörper (nach dem wir Eindeutigkeit bis auf Isomorphie bewiesen haben).

Beispiel:

1. $\mathbb{C}$ ist ein Zerfällungskörper des Polynoms $f = x^2 + 1$ über $\mathbb{R}$, da $\alpha_1 = i$ und $\alpha_2 = -1$, somit ist $x^2 + 1 = (x + i)(x - i)$, und $\mathbb{C} = \mathbb{R}(i, -i)$.

Lemma: Ist L ein Zerfällungskörper von f über K und ist $K \leq M \leq L$, so ist L auch ein Zerfällungskörper von f über M.

Beweis: Die Eigenschaft (2.7.1) ist mit denselben α_i erfüllt, und (2.7.1) ergibt sich wegen $L = K(\alpha_1, \dots, \alpha_n) \leq M(\alpha_1, \dots, \alpha_n) = L$.

Satz: Ist K ein Körper und $f \in K[x]$, so existiert ein Zerfällungskörper L von f über K, und je zwei solche Zerfällungskörper von f sind über K isomorph.

Beweis:

- Existenz: Induktion nach grad f.

– Induktionsverankerung: $\operatorname{grad} f = 0$ oder 1. Für $f = c$ konstant ist K der Zerfällungskörper, ein Polynom ersten Grades $f = cx+d$ mit $c \neq 0$ hat die Nullstelle $\alpha_1 = -\frac{d}{c} \in K$, also ist K Zerfällungskörper.

– Induktionsvoraussetzung: Sei $\operatorname{grad} f = n > 1$ und die Aussage gelte für alle Polynome vom Grad kleiner n über jedem Körper.

– Induktionsschluß: Offenbar existieren $p, q \in K[x]$ mit p irreduzibel und $f = pq$ (es kann $q = 1$ sein). Nach Satz (2.4.5) existiert ein Körper $L_1 = K(\alpha_1)$ mit $p(\alpha_1) = 0$. Da $f \in L_1[x]$, existiert $g \in L_1[x]$ mit $f = (x-\alpha_1)g$, Lemma (1.3.9). Mit der Gradformel für Polynome ist $\operatorname{grad} g = n - 1 < n$. Nach Induktionsvoraussetzung existiert ein Zerfällungskörper L von g über L_1, d.h. es existieren $\alpha_2, \dots, \alpha_n \in L$ und $c \in L$ mit $g = c(x - \alpha_2) \dots (x - \alpha_n)$ und $L = L_1(\alpha_2, \dots, \alpha_n)$, daraus folgt

$$f = (x - \alpha_1)g = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

wobei $\alpha_i \in L$ und $c \in K$ (da höchster Koeffizient von $f \in K[x]$). Zudem ist $L = L_1(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Bemerkung: Der Beweis war konstruktiv und liefert: $[K(f) : K] \leq (\operatorname{grad} f)!$, da $[L_1 : K] = [K(\alpha_1) : K] = \operatorname{grad} p \leq \operatorname{grad} f = n$ ist und $[L : L_1] \leq (\operatorname{grad} g)! \leq (n-1)!$ ist, damit ist nach (2.5.3) auch $[L : K] = [L : L_1] \cdot [L_1 : K] \leq (n-1)! \cdot n = n!$.

2.7.2 Polynome kleinen Grades

Sei K ein Körper, $f \in K[x]$.

1. $\operatorname{grad} f \leq 1$ folgt $K(f) = K$

2. $\operatorname{grad} f = 2$, etwa $f = x^2 + px + q$, falls reduzibel, so ist $K(f) = K$, andernfalls ist $f = x^2+px+q = (x-\alpha_1)(x-\alpha_2) = x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2$. Somit ist $\alpha_2 = -p - \alpha_1$, damit ist $[K(f) : K] = 2$.

3. $\operatorname{grad} f = 3$, falls reduzibel mit $f = g \cdot h$ und $\operatorname{grad} g = 2$, so ist $K(f) = K(g)$, siehe oben. Falls f irreduzibel, so ist $[K(\alpha) : K] = 3$ mit $f(\alpha) = 0$, damit folgt $f = (x - \alpha) \cdot g$ mit $g \in K(\alpha)[x]$, damit folgt:

   Entweder g reduzibel in $K(\alpha)[x]$, dann ist $K(f) = K(\alpha)$; oder g irreduzibel in $K(\alpha)[x]$, damit ist $[K(\alpha)(g) : K(\alpha)] = 2$, damit ist $[K(f) : K] = 6$.

Beispiel:

2. Sei $f = x^3 - 2$. (a) $K = \mathbb{Q}$ oder (b) $K = \mathbb{Q}(\varrho)$ mit $\varrho = e^{\frac{2\pi i}{3}}$.

   (a) $K = \mathbb{Q}$: Dann ist $\alpha = \sqrt[3]{2} \in \mathbb{R}$, $(\varrho\alpha)^3 = \varrho^3\alpha^3 = \alpha^3 = 2$, $(\varrho^2\alpha)^3 = \varrho^6\alpha^3 = 2$; $x^3-2 = (x-\alpha)(x^2+\alpha x+\alpha^2) = (x-\alpha)(x-\varrho\alpha)(x-\varrho^2\alpha) = (x-\alpha)(x^2-(\varrho+\varrho^2)\alpha+\varrho^3\alpha^2)$, damit ist $[K(f):K] = 6$

   (b) $K = \mathbb{Q}(\varrho)$: Da $\varrho^2 + \varrho + 1 = 0$, hat ϱ (höchstens) den Grad 2 über $\mathbb{Q}$. Daher ist mit (2.5.3) $\alpha \notin K$, also $x^3 - 2$ irreduzibel über K, es folgt also $[K(\alpha) : K] = 3$. Dann ist $x^3 - 2 = (x - \alpha)g$ mit $g \in K(\alpha)[x]$. Da $\varrho\alpha, \varrho^2\alpha \in K(\alpha)$, $K(f) = K(\alpha)$, $[K(f) : K] = 3$.

2.7.3 Isomorphismus der Polynomringe

Lemma: Sei $K \leq L$ und σ ein Isomorphismus von L auf L^σ; sei $\bar{\sigma} : L[x] \to L^\sigma[x]$ wie in (1.3.8) definiert. Dann gilt:

1. $[L^\sigma : K^\sigma] = [L : K]$.
2. Ist $f \in L[x]$ und $\alpha \in L$ mit $f(\alpha) = 0$, so ist $f^{\bar{\sigma}}(\alpha^\sigma) = 0$.
3. Ist $f \in K[x], k^\sigma = k$ für alle $k \in K$ und $L^\sigma = L$ (also σ ein Automorphismus von L über K), so permutiert σ die Nullstellen von f in L.

Beweis:

1. Seien $\alpha_1, \dots, \alpha_n \in L$ linear unabhängig über K. *Behauptung:* $\alpha_1^\sigma, \dots, \alpha_n^\sigma \in L^\sigma$ sind linear unabhängig über K^σ. *Beweis:* sind $c_i \in K^\sigma$ mit $\sum_{i=1}^n c_i\alpha_i^\sigma = 0$, so gilt:
$$0 = 0^{\sigma^{-1}} = \left(\sum_{i=1}^n c_i\alpha_i^\sigma\right)^{\sigma^{-1}} = \sum_{i=1}^n c_i^{\sigma^{-1}}\alpha_i$$
Da $\alpha_1, \dots, \alpha_n$ linear unabhängig sind, folgt: $c_i^{\sigma^{-1}} = 0$ für $i = 1, \dots, n$, damit auch $c_i = 0$ für $i = 1, \dots, n$. Somit $[L^\sigma : K^\sigma] \geq [L : K]$. Anwendung auf σ^{-1} liefert:
$$[L : K] = [(L^\sigma)^{\sigma^{-1}} : (K^\sigma)^{\sigma^{-1}}] \geq [L^\sigma : K^\sigma]$$

2. Sei $\alpha \in L$ mit $f(\alpha) = 0$, $f = \sum_{i=0}^n a_ix^i$, dann $f^\sigma = \sum_{i=0}^n a_i^\sigma x^i$. Es gilt:
$$0^\sigma = (f(\alpha))^\sigma = \left(\sum_{i=0}^n a_i\alpha^i\right)^\sigma = \sum_{i=0}^n a_i^\sigma(\alpha^\sigma)^i = f^{\bar{\sigma}}(\alpha^\sigma)$$

3. Hier ist nach Voraussetzung $f^\sigma = \sum_{i=0}^n a_i^\sigma x^i = \sum_{i=0}^n a_i x^i = f$. Ist also $M := \{\alpha \in L \mid f(\alpha) = 0\}$, so ist $M^\sigma \subseteq M$. Ist $f = 0$, so ist die Aussage trivial. Ist $f \neq 0$, so ist M endlich und $\sigma|_M : M \to M$ injektiv (da Isomorphismus), damit surjektiv, also Permutation.

2.7.4 Isomorphismus der Zerfällungskörper

Satz: Sei σ ein Isomorphismus des Körpers K auf K^σ, $f \in K[x]$ und $f^{\bar\sigma}$ wie in (1.3.8) definiert. Sind L und M Zerfällungskörper von f über K bzw. $f^{\bar\sigma}$ über K^σ, so existiert ein Isomorphismus $\sigma^* : L \to M$, der σ fortsetzt.

Bemerkungen:

1. Eindeutigkeit in (2.7.1) folgt mit $\sigma = \mathrm{id}$.

2. Zerfällungskörper über $\mathbb{Q}$ sind immer in $\mathbb{C}$ enthalten, daher „einfach “zu konstruieren.

Beweis: Induktion nach $[L : K]$

- Ist $[L : K] = 1$, so existieren $\alpha_i \in K, c \in K$ mit $f = c(x-\alpha_1)\ldots(x-\alpha_n)$. Da $\bar\sigma$ Homomorphismus ist (1.3.8), ist $f^{\bar\sigma} = c^\sigma(x - \alpha_1^\sigma)\ldots(x - \alpha_n^\sigma)$, wobei $\alpha_i^\sigma \in K^\sigma$. Daraus folgt: K^σ ist der einzige Zerfällungskörper von $f^{\bar\sigma}$ über K^σ, also $M = K^\sigma$. Setze $\sigma^* = \sigma$.

- Sei also $[L : K] > 1$ und Satz (2.7.4) richtig für alle Zerfällungskörper mit kleinerem Grad über dem Grundkörper. Da $[L : K] > 1$, existiert ein irreduzibles Polynom $p \in K[x]$ mit $\operatorname{grad} p \geq 2$ und $f = p \cdot q$, wobei $q \in K[x]$. Da $L = K(f)$, existieren nach Definition $\alpha_i \in L, c \in K$ mit $f = c(x-\alpha_1)\ldots(x-\alpha_n) = p\cdot q$. Mit Eindeutigkeit der Primfaktorzerlegung über dem ZPE-Ring $L[x]$ folgt: $p = c^*(x-\alpha_1)\ldots(x-\alpha_r)$ bei geeigneter Nummerierung, wobei $r \geq 2$. Sei $\alpha = \alpha_1$.

  Da $\bar\sigma$ Homomorphismus, ist $f^{\bar\sigma} = p^{\bar\sigma} q^{\bar\sigma}$. Nach (1.3.8) ist $p^{\bar\sigma}$ irreduzibel in $K^\sigma[x]$. In M existieren β_i mit $f^{\bar\sigma} = d(x - \beta_i)\ldots(x - \beta_n)$, daraus folgt bei geeigneter Nummerierung $p^{\bar\sigma} = d^*(x - \beta_1)\ldots(x - \beta_r)$. Sei $\beta = \beta_1$.

  Nach Satz (2.4.6) (angewandt auf $K, p, \sigma, \alpha, \beta$) existiert Isomorphismus $\sigma_1 : K(\alpha) \to K^\sigma(\beta)$ mit $\sigma_1|_K = \sigma$. Nach Lemma (2.7.1) ist $L = K(\alpha)(f)$ und $M = K^\sigma(\beta)(f^{\bar\sigma})$. Nach Gradsatz ist $[L : K(\alpha)] = \frac{[L:K]}{[K(\alpha):K]} < [L : K]$, da $K(\alpha) > K$. Nach Induktionsannahme existiert Fortsetzung $\sigma^* : L \to M$ von σ_1, also von σ.

2.7.5 normale Körpererweiterungen = Zerfällungskörper

Seien $K \leq L$ Körper.

DEFINITION: L heißt *normal* über K (oder die Erweiterung (K, L) heißt *normal*), wenn L endlich über K ist und jedes irreduzible Polynom $g \in K[x]$, das in L eine Nullstelle hat, in L in Linearfaktoren zerfällt, d.h.

$$\begin{array}{rl} & g \in K[x] \text{ irreduzibel}, \ \exists \alpha \in L \text{ mit } g(\alpha) = 0 \\ \Longrightarrow & \exists \alpha_i \in L, c \in K \text{ mit } g = c(x - \alpha_1) \ldots (x - \alpha_n) \end{array}$$

BEISPIELE:

1. $\mathbb{C}$ ist normal über $\mathbb{R}$ mit Fundamentalsatz der Algebra (und $[\mathbb{C} : \mathbb{R}] = 2$). Diesen Satz brauchen wir aber nicht, siehe Beispiel 3.

2. Falls $[L : K] \leq 2$, so ist L normal über K. *Beweis:* $[L : K] = 1 \Rightarrow L = K$, ist $g \in K[x]$ irreduzibel mit Nullstelle in K, so ist $\operatorname{grad} g = 1$. Falls $[L : K] = 2$ und $g \in K[x]$ irreduzibel mit Nullstelle α in K, so ist $K(\alpha) \leq L$. Mit (2.5.3) folgt: $[K(\alpha) : K] \mid [L : K] = 2$. Damit falls $\alpha \in K$, folgt $\operatorname{grad} g = 1$. Falls $\alpha \notin K$, so ist $\operatorname{grad} g = [K(\alpha) : K] = 2$, mit (2.7.2) folgt: $g = c(x - \alpha)(x - \beta)$ mit $\beta \in L$.

3. Für $K = \mathbb{Q}$ und $L = \mathbb{R}$ oder $\mathbb{C}$ ist L nicht normal über K, da $[L : K] = \infty$.

4. $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal über $\mathbb{Q}$. Die Nullstellen von $x^3 - 2$ sind $\sqrt[3]{2}, \varrho\sqrt[3]{2}, \varrho^2\sqrt[3]{2}$ für $\varrho = e^{\frac{2\pi i}{3}}$, wobei nur die erste dieser Nullstellen in $\mathbb{Q}(\sqrt[3]{2})$ liegt (siehe Beispiel zu (2.7.2)).

SATZ: Genau dann ist L normal über K, wenn L Zerfällungskörper eines geeigneten Polynoms $f \in K[x]$ über K ist. Ist L normal über K und $L = K(\alpha_1, \ldots, \alpha_n)$ und $p_i = p_{\alpha_i}$ das Minimalpolynom von α_i über K ($i = 1, \ldots, n$), so ist $L = K(f)$ mit $f = \prod_{i=1}^n p_i$.

BEWEIS: Ist L normal über K, so $[L : K] < \infty$, also existieren obige α_i und sind (nach (2.5.2)) algebraisch über K. Also existieren p_i und f. Da L normal über K ist, existieren $\alpha_{ij} \in L$ mit

$$\begin{array}{rcl} p_i & = & c_i(x - \alpha_{i1}) \ldots (x - \alpha_{ir_i}), \text{ wobei } \alpha_{i1} = \alpha_i \\ & \Rightarrow & f = \prod_{i=1}^{n} c_i \prod_{j=1}^{r_i} (x - \alpha_{ij}) \\ L & = & K(\alpha_1, \ldots, \alpha_n) \leq K(\alpha_{ij} \mid i = 1, \ldots, n, j = 1, \ldots, r_i) \leq L \end{array}$$

Es folgt: $L = K(f)$.

Sei nun $L = K(f)$ für $f \in K[x]$, also existieren $\alpha_i \in L$ und $c \in K$ mit $f = c(x-\alpha_1)\dots(x-\alpha_n)$. Nach Bemerkung (2.7.1) ist $[L : K] < \infty$.

Behauptung: Ist $g \in K[x]$ irreduzibel und sind β_1, β_2 Nullstellen von g in Erweiterungskörpern von L, so ist $[L(\beta_1) : K] = [L(\beta_2) : K]$

Beweis: $L(\beta_i)$ ist Zerfällungskörper von f über $K(\beta_i)$, da $\alpha_i \in L(\beta_i)$ und

$$K(\beta_i)(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n, \beta_i) = L(\beta_i)$$

Nach (2.4.6) existiert Isomorphismus $\sigma_1 : K(\beta_1) \to K(\beta_2)$ über K, also $f^{\bar{\sigma}} = f$. Mit (2.7.4) folgt: es existiert Fortsetzung $\sigma^* : L(\beta_1) \to L(\beta_2)$ von σ. Nach (2.7.3) ist $[L(\beta_1) : K] = [L(\beta_2) : K]$. □

Sei $g \in K[x]$ irreduzibel und $\beta \in L$ mit $g(\beta) = 0$. Betrachte $L(g)$ und $\beta_i \in L(g)$ mit $g(\beta_i) = 0$. Dann folgt:

$$[L : K] = [L(\beta) : K] = [L(\beta_i) : K] = [L(\beta_i) : L] \cdot [L : K]$$

Daraus folgt: $[L(\beta_i) : L] = 1$, also $\beta_i \in L$. Also zerfällt g in L.

2.7.6 Normalität über Zwischenkörpern

Korollar: Seien $K \leq M \leq L$ Körper. Falls L normal über K ist, so ist L normal über M.

Beweis: Aus L normal über K folgt mit (2.7.5), daß ein $f \in K[x]$ existiert mit $L = K(f)$; Lemma (2.7.1) sagt aus: $L = M(f)$, wieder mit (2.7.5) ist L normal über M.

2.7.7 Ausbau einer Erweiterung zu einer normalen Erweiterung

Satz: Seien $K \leq L$ Körper mit $[L : K] < \infty$. Dann gilt:

1. Es existieren Erweiterungskörper M von L mit M normal über K.
2. Je zwei kleinste solche Erweiterungskörper sind über L isomorph.

Beweis:

1. Da $[L : K] < \infty$, existieren $\alpha_i \in L$ mit $L = K(\alpha_1, \dots, \alpha_n)$. Nach Satz (2.5.2) ist α_i algebraisch über K, sei $p_i = p_{\alpha_i}$. Sei $f = \prod_{i=1}^{n} p_i \in K[x] \subseteq L[x]$. Sei $M = L(f)$ ein Zerfällungskörper. Dann existieren $\beta_i \in M$ mit

$f = c(x-\beta_1)\cdot\ldots\cdot(x-\beta_r)$. Da α_i ($i \in \{1,\ldots,n\}$) eine Nullstelle von f in $L \leq M$ ist, existiert j mit $\alpha_i = \beta_j$.

Wir wollen zeigen: $M = K(f)$, zu zeigen bleibt dafür: $M = K(\beta_1,\ldots,\beta_r)$. Offenbar ist $K(\beta_1,\ldots,\beta_r) \geq K(\alpha_1,\ldots,\alpha_n) = L$; also ist $K(\beta_1,\ldots,\beta_r) \geq L(\beta_1,\ldots,\beta_r) = M$.

2. als Übungsaufgabe 35

2.7.8 Automorphismus

Satz: Sei $K \leq M \leq L$ und L normal über K. Ist $\nu : M \to L$ ein Monomorphismus über K (d.h. mit $a^\nu = a$ für alle $a \in K$), so existiert ein Automorphismus σ von L mit $\sigma|_M = \nu$.

Beweis: Nach Satz (2.7.5) ist $L = K(f)$ mit $f \in K[x]$. Nach Lemma (2.7.1) ist dann $L \overset{(2.7.1)}{=} M(f) \overset{(2.7.1)}{=} M^\nu(f) = M^\nu(f^{\bar\nu})$ (da $f = f^{\bar\nu}$ wegen „über K“). Nach Satz (2.7.4) existiert ein Isomorphismus $\sigma : M(f) = L \to M^\nu(f^{\bar\nu}) = L$ mit $\sigma|_M = \nu$.

2.7.9 Isomorphismus zwischen Nullstellen

Sei L normal über K. Sind $\alpha \in L$ und $\beta \in L$ Nullstellen des irreduziblen Polynoms $p \in K[x]$, so existiert ein Isomorphismus σ von L über K mit $\alpha^\sigma = \beta$.

Beweis: Wende (2.7.8) an mit $M = K(\alpha) \leq L$ und $\nu : K(\alpha) \to K(\beta)$ mit $\alpha^\nu = \beta$, der nach Satz (2.4.6) existiert.

2.7.10 Algebraisch abgeschlossene Körper

Satz: Die folgenden Eigenschaften des Körpers K sind äquivalent:

(a) K besitzt keine echte algebraische Erweiterung (aus $L \geq K$ mit L algebraisch über K folgt: $L = K$)

(b) Jedes Polynom $f \in K[x]$ vom Grade ≥ 1 besitzt eine Nullstelle in K.

(c) Jedes Polynom $f \in K[x]$ zerfällt in Linearfaktoren (d.h. es existieren $c, \alpha_1, \ldots, \alpha_n \in K$ mit $f = c(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$).

(d) Jedes irreduzible Polynom über K hat den Grad 1.

DEFINITION: Ein Körper mit einer (und damit allen) dieser vier Eigenschaften heißt *algebraisch abgeschlossen*.

BEWEIS:

(a) $\Rightarrow$ (c) Sei $L = K(f)$. Mit (2.7.1) und (2.5.2) folgt: L ist algebraisch über K, also ist $L = K$.

(c) $\Rightarrow$ (b) trivial

(b) $\Rightarrow$ (d) Sei $p \in K[x]$ irreduzibel. Nach (b) existiert $\alpha \in K$ mit $p(\alpha) = 0$. Nach (1.3.9) ist $p = (x - \alpha) \cdot g$ mit $g \in K[x]$. Da p irreduzibel ist, ist $g \in K$, also $\operatorname{grad} p = 1$.

(d) $\Rightarrow$ (a) Sei $L \geq K$ algebraisch über K. Für $\alpha \in L$ existiert $p_\alpha \in K[x]$ irreduzibel mit $p_\alpha(\alpha) = 0$ (Satz (2.4.4)). Da $\operatorname{grad} p_\alpha = 1$, ist $\alpha \in K$.

2.7.11 Algebraisch abgeschlossene Körper

SATZ: Zu jedem Körper K existiert ein Erweiterungskörper $\mathfrak{A}(K)$ mit

1. $\mathfrak{A}(K)$ ist algebraisch abgeschlossen.
2. $\mathfrak{A}(K)$ ist algebraisch über K.

Je zwei solche Körper sind über K isomorph.

DEFINITION: Wir nennen $\mathfrak{A}(K)$ „den“ *algebraischen Abschluß* von K.

HILFSMITTEL für den Beweis:

ZORNSCHES LEMMA: Sei M eine nichtleere (teilweise) geordnete Menge. Hat jede Kette $\mathcal{K}$ in M eine obere Schranke in M, so existiert ein maximales Element in M. [26]

LEMMA: Ist K ein Körper und L algebraisch über K, so ist $|L| \leq |K[x]|$.

BEWEIS: Zu $p \in K[x]$, p irreduzibel, sei $N_p := \{\alpha \in L \mid p(\alpha) = 0\}$. Sei $\sigma_p : N_p \to \left\{p^i \mid i \in \mathbb{N}\right\}$ injektiv. Definiere $\sigma : L \to K[x]$. Für $\alpha \in L$ existiert $p_\alpha \in K[x]$ Minimalpolynom. Somit $\alpha \in N_p$ und wir definieren $\alpha^\sigma := \alpha^{\sigma_{p_\alpha}}$.

Zur Injektivität von σ: Sei $\alpha \neq \beta$ Ist $p_\alpha = p_\beta =: p$, so sind $\alpha, \beta \in N_p$, somit $\alpha^\sigma = \alpha^{\sigma_p} \neq \beta^{\sigma_p} = \beta^\sigma$. Ist $p_\alpha \neq p_\beta$, so ist $\alpha^\sigma = p_\alpha^i$ und $\beta^\sigma = p_\beta^j$ für $i, j \in \mathbb{N}$. Da ZPE-Ring, ist $p_\alpha^i \neq p_\beta^j$.

BEWEIS:

[26] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, Seite 33

1. Sei $K = (K, +, \cdot)$ ein Körper, sei $X = K \cup \mathcal{P}(K[x])$.[27] Sei

$$\Gamma = \{ (L, \oplus, \circ) \mid L \subseteq X,\ (K, +, \cdot) \leq (L, \oplus, \circ),\ L \text{ alg. über } K \}$$

Definiere[28] $(L_1, +_1, \cdot_1) \leq (L_2, +_2, \cdot_2) :\Leftrightarrow L_1$ Teilkörper von L_2. Offensichtlich ist $\leq$ eine (teilweise) Ordnung auf Γ. Zudem ist $K \in \Gamma \neq \emptyset$. Sei Δ eine Kette Γ. Sei $\bar{L} := \bigcup_{L \in \Delta} L \subseteq X$ und für $a, b \in \bar{L}$ existieren $(L_1, +_1, \cdot_1), (L_2, +_2, \cdot_2) \in \Delta$ mit $a \in L_1, b \in L_2$; etwa $L_1 \leq L_2$, dann gilt. $a, b \in L_2$. Definiere nun $a \oplus b := a +_2 b$ und $a \circ b = a \cdot_2 b$.

Behauptung: $(\bar{L}, \oplus, \circ)$ ist ein Körper. *Beweis:* Sind $a, b, c \in L$; $a \in L_1, b \in L_2, c \in L_3$, etwa $L_1 \leq L_2 \leq L_3$, so ist $a, b, c \in L_3$. Hier gelten alle Körpergesetze, also auch für $\oplus, \circ$.

Mit $L_i \in \Delta$ folgt: $L_i \leq (\bar{L}, \oplus, \circ)$ (so sind $\oplus, \circ$ definiert). Somit ist $(\bar{L}, \oplus, \circ)$ eine obere Schranke von Δ. Nach Zornschem Lemma existiert ein maximales Element $(A, \oplus, \circ)$ in Γ.

Behauptung: A ist ein algebraischer Abschluß von K. *Beweis:* Sei $B \geq A$, B algebraisch über A, dann folgt mit (2.5.6), daß B algebraisch über K ist. Mit Lemma ist $|A|, |B| \leq |K[x]|$. Da X nicht Vereinigung zweier Teilmengen kleinerer Mächtigkeit ist, ist $|X \setminus A| > |K[x]| \geq |B \setminus A|$.

Somit existiert eine injektive Abbildung ν von $B \setminus A$ in $X \setminus A$. Somit $B^\nu \simeq B$ algebraisch über K, damit ist $B^\nu \in \Gamma$, da A maximal ist, ist $B^\nu = A$, damit ist $A = B$.

2. Da $A \in \Gamma$, ist A algebraisch über K.

2.7.12 Isomorphismus zwischen algebraischen Abschlüssen

Satz: Sei $\varrho : K \to K^\varrho$ ein Isomorphismus und seien A bzw. B algebraische Abschlüsse von K bzw. K^ϱ. Dann existiert ein Isomorphismus $\sigma : A \to B$ mit $\sigma|_K = \varrho$.

Beweis: Sei Γ die Menge aller Isomorphismen σ eines K enthaltenen Teilkörpers A_1 von A auf einen Teilkörper B_1 von B mit $\sigma|_K = \varrho$. Offenbar ist $\Gamma \neq \emptyset$, da $\varrho \in \Gamma$. Die benötigte Ordnung auf Γ wird definiert durch: Für alle $\sigma : A_1 \to B_2$ und $\tau : A_2 \to B_2$ mit $A_1 \leq A_2$ und $B_1 \leq B_2$ ist

$$\sigma \leq \tau :\Leftrightarrow \tau|_{A_1} = \sigma$$

[27] wobei X einfach groß gegenüber K ist und K enthält

[28] „Ich betrachte einfach die Menge aller Körper in dieser Menge. Das kann ich doch einfach tun…das kann mir zumindest keiner verbieten!“

Das ist eine teilweise Ordnung auf Γ. Sei $\Delta \subseteq \Gamma$ eine Kette, $\delta : A_\delta \to B_\delta$ für $\delta \in \Delta$. Sei $L = \bigcup_{\delta \in \Delta} A_\delta$. Dann ist $L \leq A$ (da die α_δ eine Kette bilden). Für $a \in L$ existiert $\delta \in \Delta$ mit $a \in A_\delta$. Dann sei $a^\lambda := a^\delta$. Das liefert $\lambda : L \to B$, da $a \in A_{\delta_1}, A_{\delta_2} \Rightarrow$ (etwa) $\delta_1 \leq \delta_2 \Rightarrow a^{\delta_1} = a^{\delta_2}$.

Sind $a, b \in L$ mit $a \in A_{\delta_1}$ und $b \in A_{\delta_2}$ (etwa $A_{\delta_1} \leq \delta_2$, d.h. $A_{\delta_1} \leq A_{\delta_2}$). Also ist

$$(a+b)^\lambda = (a+b)^{\delta_2} = a^{\delta_2} + b^{\delta_2} = a^\lambda + b^\lambda$$

Genauso für Multiplikation und Injektivität. Somit $\lambda \in \Gamma$ und für $\delta \in \Delta$ ist $A_\delta \leq L$ und $\delta \leq \gamma$.

Nach Zornschem Lemma existiert ein maximales Element $\sigma : T \to T^\sigma \in \Gamma$. Ist $T = A$, so sind wir fertig: Denn dann ist T algebraisch abgeschlossen, also hat jedes Polynom aus $T[x]$ eine Nullstelle, mit (2.7.3) gilt dasselbe für T^σ, mit (2.7.10) ist also T^σ algebraisch abgeschlossen. Da B algebraisch über K^ϱ, also auch über T^σ, folgt $B = T^\sigma$. Damit tut σ das Verlangte.

Angenommen, $T \neq A$. Dann existiert $\alpha \in A \setminus T$ mit A algebraisch über K, existiert $f \in K[x]$ irreduzibel mit $f(\alpha) = 0$. Da A algebraisch abgeschlossen, existieren $\alpha = \alpha_1, \ldots, \alpha_n \in A$ und $c \in K$ mit $f = x(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$. Da B algebraisch abgeschlossen ist, zerfällt $f^{\bar{\sigma}}$ in B und somit existiert $T^\sigma(f^{\bar{\sigma}}) \leq B$. Nach Satz (2.7.4) existiert eine Fortsetzung $\tau : T(f) \to T^\sigma(f^\sigma)$ von σ. Offenbar ist $\tau \in \Gamma$ und $\sigma \leq \tau$. Wegen $\alpha \in A \setminus T$, ist $\tau > \sigma$, Widerspruch!

2.8 endliche (Gruppen und) Körper

2.8.1 Erzeugnis, zyklische Gruppen

Seien $(G, \cdot)$ und $(\bar{G}, \circ)$ Gruppen, $H \subseteq G$ und $g \in G$. Wir (sollten) kennen:

1. $|G| :=$ Anzahl der Elemente in G *(Ordnung)*
2. $\sigma : G \to \bar{G}$ ist ein *Homomorphismus* genau dann, wenn $(a \cdot b)^\sigma = a^\sigma \circ b^\sigma$ für alle $a, b \in G$
3. Endomorphismus, Monomorphismus, Epimorphismus, Automorphismus, Isomorphismus wie immer
4. $H \leq G$ *(Untergruppe)* genau dann, wenn $(H, \cdot|_{H \times H})$ eine Gruppe ist. Dies ist genau dann, wenn $H \neq \emptyset$ und mit $x, y \in H$ auch $xy^{-1} \in H$
5. aus $H_i \leq G$ (mit $i \in I$) folgt: $\bigcap_{i \in I} H_i \leq G$.
6. Potenzen von g: $g^0 := 1$ und $g^n := g^{n-1} \cdot g$ und $g^{-n} = (g^{-1})^n$ (für $n \in \mathbb{N}$) und analog für additiv geschriebene Gruppe[29]

[29] siehe Bernd Stellmacher, Lineare Algebra 2001/2002, Satz 1.5.3

7. $g^{n+m} = g^n \cdot g^m$ für $n, m \in \mathbb{Z}$, insbesondere $(g^n)^{-1} = g^{-n}$

8. $(g^n)^m = g^{nm} = (g^m)^n$

DEFINITIONEN:

1. $\langle H \rangle = \bigcap \{ U \mid H \subseteq U \leq G \}$ ist das *Erzeugnis von H in G* (und in Kurzschreibweise $\langle g \rangle := \langle \{g\} \rangle$)

2. G heißt *zyklisch*, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$.

SATZ: Ist $G = \langle g \rangle$ zyklisch, so ist $G = \{ g^m \mid m \in \mathbb{Z} \}$. Dann gibt es zwei Möglichkeiten:

(i) Alle Potenzen g^i (mit $i \in \mathbb{Z}$) sind paarweise verschieden. Dann ist $|G|$ unendlich und $g^i \cdot g^j = g^{i+j}$ beschreibt die Multiplikation in G.

(ii) Es existiert $k \in \mathbb{N}$ mit $g^k = 1$. Ist n die kleinste solche Zahl, so ist $G = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$ und diese sind paarweise verschieden, also $|G| = n$.

BEWEIS: Sei $M := \{ g^m \mid m \in \mathbb{Z} \}$. Dann ist $M \neq \emptyset$ und mit g^i und g^j ist auch $g^i \cdot (g^j)^{-1} = g^{i-j} \in M$, also ist M eine Untergruppe. Jede Untergruppe $U \leq G$ mit $g \in U$ enthält offenbar alle Potenzen von g, also M. Damit ist $M = \cap \{ U \mid g \in U \leq G \} = \langle g \rangle$. Sind alle g^i paarweise verschieden, bleibt nichts zu zeigen. Sei also $g^i = g^j$, etwa $i > j$. Dann ist $i - j \in \mathbb{N}$ und $g^{i-j} = g^i \cdot g^{-j} = g^i (g^j)^{-1} = 1$. Somit sind $g^0, \ldots, g^{n-1}$ paarweise verschieden. Für $m \in \mathbb{Z}$ existieren q, r mit $m = qn + r$, $0 \leq r < n$, dann folgt: $g^m = g^{qn+r} = g^{qn} \cdot g^r = (g^n)^q \cdot g^r = 1 g^r = g^r$.

KOROLLAR: Für jedes $n \in \mathbb{N} \cup \{\infty\}$ gibt es bis auf Isomorphie genau eine zyklische Gruppe der Ordnung n.

BEWEIS: Daß je zwei solche Gruppen isomorph sind, folgt aus dem Satz und den Potenzgesetzen. Existenz: $(\mathbb{Z}, +)$ zyklisch erzeugt von 1; $(\mathbb{Z}/n\mathbb{Z}, +)$ zyklisch erzeugt von $1 + n\mathbb{Z}$.

2.8.2 Der Satz von LAGRANGE

Sei G eine Gruppe, $H \leq G$ und $g \in G$.

DEFINITIONEN:

1. $Hg := \{hg \mid h \in H\}$ ist die Rechtsrestklasse von g nach H.

   $gH := \{gh \mid h \in H\}$ ist die Linksrestklasse von g nach H.

2. $|G : H| :=$ Anzahl der verschiedenen Rechtsrestklassen von H in G (der *Index*)

BEMERKUNGEN:

1. Im allgemeinen ist $Hg \neq gH$, zum Beispiel: Für $G = S_3 (= \Sigma_3)$ und $H = \langle(12)\rangle = \{id, (12)\}$ sowie $g = (23)$ ist $Hg = \{(23), (132)\} \neq \{(23), (123)\} = gH$.

2. Es gibt genauso viele Links- wie Rechtsrestklassen, *Beweis:* Nach gleich gezeigtem Lemma ist $G = \biguplus_{r \in R} Hr$ (disjunkte Vereinigung und R ein Repräsentantensystem für die Rechtsrestklassen), mit Aufgabe 37 ist $G = G^{-1} = \biguplus_{r \in R} (Hr)^{-1} = \biguplus_{r \in R} r^{-1}H$. Somit ist R^{-1} ein Repräsentantensystem für die Linksrestklassen.

LEMMA:

(a) $G = \cup_{g \in G} Hg$

(b) Für $a, b \in G$ sind äquivalent:

  (1) $Ha = Hb$

  (2) $Ha \cap Hb \neq \emptyset$

  (3) $ab^{-1} \in H$

BEWEIS:

(a) Mit $g \in G$ ist $g = 1g \in Hg$, damit ist $G \subseteq \bigcup_{g \in G} Hg$

(b) Kreisschluß:

(1)⇒(2) trivial, da $H \neq \emptyset$

(2)⇒(3) sei $x \in Ha \cap Hb$, damit existieren $h_1, h_2 \in H$ mit $h_1 a = x = h_2 b$. Damit ist $ab^{-1} = h_1^{-1} h_2 \in H$.

(3)⇒(1) mit $ab^{-1} \in H$ ist $H \ni (ab^{-1})^{-1} = (b^{-1})^{-1} a^{-1} = ba^{-1}$; für $h \in H$ ist $ha = (hab^{-1})b \in Hb$ und damit $Ha \subseteq Hb$, analog: $hb = (hba^{-1})a \in Ha$ und damit $Hb \subseteq Ha$.

Satz von Lagrange (1736-1813): Ist G eine endliche Gruppe und $H \leq G$, so ist $|G| = |H| \cdot |G : H|$, d.h. Ordnung und Index von Untergruppen sind Teiler der Gruppenordnung.

Beweis: Nach dem Lemma ist G disjunkte Vereinigung der $|G : H|$ verschiedenen Rechtsrestklassen Hg von H. Die Abbildung $\tau : H \to Hg, h \mapsto hg$ ist bijektiv: aus $h_1 g = h_2 g$ folgt: $h_1 = h_2$ (Injektivität). Surjektivität folgt aus der Definition.

2.8.3 Elementordnung

Sei G eine Gruppe, $g \in G$.

Definition: Sei $o(g)$ die kleinste natürliche Zahl mit $g^n = 1$ (bzw. ∞, wenn kein solches n existiert). $o(g)$ heißt *Ordnung* von g.

Eigenschaften:

1. $o(g) = |\langle g \rangle|$ (Satz (2.8.1)).
2. $o(g)$ teilt $|G|$, falls $|G|$ endlich (Satz (2.8.2)).
3. Ist $o(g) = n$, so gilt für alle $k \in \mathbb{N}$: genau dann ist $g^k = 1$, wenn $n \mid k$. *Beweis:*

   „$\Leftarrow$“ Falls $n \mid k$, d.h. $k = n \cdot r$ mit $r \in \mathbb{Z}$, so ist $g^k = g^{nr} = (g^n)^r = 1^r = 1$.

   „$\Rightarrow$“ Sei $k = qn + r; q, r \in \mathbb{Z}; 0 \leq r < n$. Es gilt $1 = g^k = g^{qn+r} = g^{qn} \cdot g^r = g^r$, daraus folgt: $r = 0$, also ist $n \mid k$.

4. Ist $o(g) = n, d \mid n$, so ist $o(g^d) = \frac{n}{d}$. *Beweis:*

$$(g^d)^{\frac{n}{d}} = g^{d \cdot \frac{n}{d}} = g^n = 1$$

   Offenbar ist $\frac{n}{d}$ die kleinste natürliche Zahl mit dieser Eigenschaft.

Beispiele:

1. Sei $G = S_3$. Die Elemente $(123), (132)$ haben Ordnung 3, $(12), (13), (23)$ haben Ordnung 2.
2. Sei $G = S_6$. Für $g = (123456)$ ist $o(g) = 6$, für $g^2 = (135)(246)$ ist $o(g^2) = 3 = \frac{6}{2}$. Für $g^3 = (14)(25)(36)$ ist $o(g^3) = 2 = \frac{6}{3}$.

LEMMA: Sind $a, b \in G$ mit $ab = ba$ und $\text{ggT}(o(a), o(b)) = 1$, so ist $o(ab) = o(a)o(b)$.

BEWEIS: Sei $o(a) = r, o(b) = s$. Dann ist $(ab)^{rs} = a^{rs}b^{rs} = 1$. Sei $n \in \mathbb{N}$ mit $(ab)^n = 1$, dann folgt $1 = (ab)^{ns} = a^{ns}b^{ns} = a^{ns}$, daraus folgt mit Bemerkung (3): $r \mid ns$, also $r \mid n$ (da $(r, s) = 1$, Aufg. 15). Genauso $s \mid n$, es folgt (Aufg 15): $rs \mid n$, also $rs \leq n$. Damit $o(ab) = rs = o(a)o(b)$.

KOROLLAR: Ist A eine endliche abelsche Gruppe und $a \in A$ mit $o(a)$ maximal, so gilt: $o(b) \mid o(a)$ für jedes $b \in A$.

BEWEIS: Angenommen, die Behauptung sei falsch. Dann existiert $b \in A$ mit $o(b) \nmid o(a)$. Dann existieren $p \in \mathbb{P}$ und $r, s, n, m \in \mathbb{N}$ mit

$$o(b) = p^n \cdot r,\ o(a) = p^m \cdot s,\ (p, r) = (p, s) = 1,\ n > m$$

Nach (4) ist $o(b^r) = p^n, o(a^{p^m}) = s$. Mit Lemma folgt: $o(b^r a^{p^m}) = p^n s > p^m s = o(a)$, Widerspruch zur Maximalität von $o(a)$.

2.8.4 multiplikative Gruppe eines Körpers

SATZ: Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.

BEWEIS: Sei $G \leq (K \setminus \{0\}, \cdot)$ endlich, K Körper. Sei $a \in G$ ein Element maximaler Ordnung, etwa $o(a) = n$. Nach Korollar (2.8.3) gilt dann: $o(g) \mid n$ für alle $g \in G$. Nach (3) aus (2.8.3) folgt: $g^n = 1$. Somit ist jedes $g \in G$ Nullstelle des Polynoms $x^n - 1$. Nach (1.3.9) hat dieses Polynom höchstens n Nullstellen. Diese Nullstellen sind: $a^0 = 1, a, a^2, \ldots, a^{n-1}$ (nach Satz (2.8.1)). Daraus folgt: $G = \{1, a, a^2, \ldots, a^{n-1}\}$, d.h. G ist zyklisch.

2.8.5 endlicher Körper

KOROLLAR: Sei K ein endlicher Körper. Dann gilt:

1. Die multiplikative Gruppe $K^* = (K \setminus \{0\}, \cdot)$ von K ist zyklisch.
2. K ist eine einfache Erweiterung des in K enthaltenen Primkörpers.

BEWEIS von (2): Ist F der Primkörper und $K^* = \langle a \rangle$, so gilt $F(a) \supseteq \{1, a, a^2, \ldots\} \cup \{0\} = K$.

2.8.6 mehrfache Nullstellen von Polynomen.

DEFINITIONEN: Sei K ein Körper, $f = \sum_{i=0}^{n} a_i x^i \in K[X]$ und $\alpha \in K$.

- α heißt *k-fache Nullstelle von f* genau dann, wenn $f = (x-\alpha)^k \cdot g$ mit $g \in K[x], g(\alpha) \neq 0$. Falls $k = 1$, heißt α *einfache Nullstelle*, sonst *mehrfache Nullstelle*.
- Sei $f' := \sum_{i=1}^{n} i a_i x^{i-1}$, die *Ableitung* von f.

LEMMA: Seien $f, g \in K[x]$. Dann gilt:

1. $(cf)' = cf', (f+g)' = f' + g'$
2. $(fg)' = f'g + fg'$
3. Für $n \in \mathbb{N}$ ist $((x-\alpha)^n)' = n(x-\alpha)^{n-1}$.

BEWEIS:

1. trivial.
2. Wegen (a) ist (b) nur für $f = x^n$ und $g = x^m$ zu beweisen.
$$\begin{aligned} f'g + fg' &= nx^{n-1} \cdot x^m + x^n \cdot m \cdot x^{m-1} \\ &= (n+m)x^{n+m-1} = (fg)' \end{aligned}$$
3. Vollständige Induktion. Für $n = 1 : 1 = 1$. Für $n > 1$ gilt
$$\begin{aligned} (x-\alpha)^n &= (x-\alpha)(x-\alpha)^{n-1} \\ ((x-\alpha)^n)' &= 1 \cdot (x-\alpha)^{n-1} + (x-\alpha)(n-1)(x-\alpha)^{n-2} = n \cdot (x-\alpha)^{n-1} \end{aligned}$$

SATZ: Sei $\alpha \in K$ mit $f(\alpha) = 0$. Genau dann ist α eine mehrfache Nullstelle, wenn $f'(\alpha) = 0$.

BEWEIS: Sei $f = (x-\alpha)^k \cdot g$ mit $g(\alpha) \neq 0, k \geq 1$. Es gilt
$$f' = k \cdot (x-\alpha)^{k-1} g + (x-\alpha)^k \cdot g'$$

Ist α mehrfache Nullstelle, so ist $k \geq 2$, also $f'(\alpha) = 0$, da $\alpha - \alpha$ als Faktor in $f'(\alpha)$ auftritt.

Sei $f'(\alpha) = 0$. Angenommen $k = 1$, d.h. $f = (x-\alpha)g$, es folgt ein Widerspruch, da
$$\begin{aligned} f' &= g + (x-\alpha)g' \\ 0 &= f'(\alpha) = g(\alpha) + (\alpha - \alpha)g'(\alpha) = g(\alpha) \end{aligned}$$

2.8.7 Hauptsatz

Zu jeder Primzahlpotenz $p^n (p \in \mathbb{P}, n \in \mathbb{N})$ gibt es bis auf Isomorphie genau einen Körper $GF(p^n)$ mit p^n Elementen, nämlich den Zerfällungskörper des Polynoms $x^{p^n} - x$ über $GF(p) = \mathbb{Z}/p\mathbb{Z}$. Jeder endliche Körper ist zu einem solchen $GF(p^n)$ isomorph.

Beweis: Sei K ein endlicher Körper. Da $\mathbb{Q}$ unendlich, ist der Primkörper F von K nach (1.1.11) isomorph zu $GF(p)$ für ein $p \in \mathbb{P}$.

Nach Satz (2.5.1) ist K ein Vektorraum über F der Dimension n für ein $n \in \mathbb{N}$. Laut dem Hauptsatz über endlichdimensionale Vektorräume ist $K \simeq F^n = \{(x_1, \ldots, x_n) \mid x \in F\}$ (als Vektorraum), wobei $|F^n| = p^n$. Somit $|K| = p^n$, also $|K^*| = p^n - 1$.

Für jedes $a \in K^*$ gilt nach (2) aus (2.8.3): $o(a) \mid p^n - 1$; nach (3) aus (2.8.3) ist $a^{p^n-1} = 1$, also $a^{p^n} - a = 0$. Das gilt auch für $a = 0$. Also alle Elemente von K sind Nullstellen des Polynoms $x^{p^n} - x$. Ist also $K = \{\alpha_1, \ldots, \alpha_{p^n}\}$, so folgt: $x^{p^n} - x = (x - \alpha_1) \ldots (x - \alpha_{p^n})$. Ferner $K = F(\alpha_1, \ldots, \alpha_{p^n})$. Nach Def. (2.7.1) ist K ein Zerfällungskörper von $x^{p^n} - x$ über F.

Ist K_1 ein weiterer Körper mit p^n Elementen und F_1 sein Primkörper, so ist $F_1 \simeq GF(p) \simeq F$ und K_1 ein Zerfällungskörper von $x^{p^n} - x$ über F_1. Sei $\sigma : F \to F_1$ ein Isomorphismus, dann ist $\left(x^{p^n} - x\right)^\sigma = x^{p^n} - x$. Nach Satz (2.7.4) existiert ein Isomorphismus von K auf K_1.

Zu zeigen bleibt: zu jeder Primzahlpotenz p^n existiert ein Körper mit p^n Elementen. Sei $F = GF(p)$ und $L = F\left(x^{p^n} - x\right)$. Sei $K := \left\{\alpha \in L \mid \alpha^{p^n} - \alpha = 0\right\}$. Für $f = x^{p^n} - x$ ist $f' = p^n \cdot x^{p^n-1} - 1 = -1$, also $f'(\alpha) \neq 0$ für alle $\alpha \in K$. Nach Satz (2.8.6) sind alle $\alpha \in K$ einfache Nullstellen von f, und somit $f = (x - \alpha_1) \ldots (x - \alpha_{p^n})$ mit $\alpha_i \in K$ und $\alpha_i \neq \alpha_j$ für $i \neq j$. Also folgt: $|K| = p^n$.

Behauptung: K ist ein Teilkörper von L. *Beweis:* für $\alpha, \beta \in K$ gilt: $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ (Aufgabe 8 und Induktion). Damit ist $\alpha + \beta \in K$. Weiter gilt $(\alpha \cdot \beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha\beta$, damit folgt $\alpha\beta \in K$, genauso $\alpha\beta^{-1} \in K$.

2.8.8 Teilkörper endlicher Körper

Satz: Zu jedem Teiler d von n enthält $GF(p^n)$ genau einen Teilkörper mit p^d Elementen (also den Körper $GF(p^d)$). Das sind alle Teilkörper von $GF(p^n)$.

Beweis:

Hilfssatz: Sei $p \in \mathbb{P}$ und $d, n \in \mathbb{N}$. Dann gilt: $p^d - 1 \mid p^n - 1 \Leftrightarrow d \mid n$. *Beweis:*

„$\Leftarrow$“ Aus $d \mid n$ folgt $n = de$, also $(p^d - 1)(p^{n-d} + p^{n-2d} + \ldots + p^{n-(e-1)d} + 1) = p^n - 1$.

„$\Rightarrow$“ Seien $q, r \in \mathbb{Z}$ mit $n = q \cdot d + r$ und $0 \leq r < d$. Dann gilt

$$p^d - 1 \mid p^n - 1 = p^n - p^{qd} + p^{qd} - 1 = p^{qd}(p^r - 1) + \underbrace{p^{qd} - 1}_{p^d - 1 \mid \ldots}$$

Damit gilt: $p^d - 1 \mid p^{qd}(p^r - 1)$, da $\mathrm{ggT}(p^d - 1, p^{qd}) = 1$ gilt $p^d - 1 \mid p^r - 1$, da aber $d > r$ ist, ist $r = 0$, also $d \mid n$.

Sei $d \mid n$. Nach Hilfssatz ist $p^d - 1 \mid p^n - 1 = |K^*|$ mit $K = GF(p^n)$. Nach Aufgabe 38 existiert eine Untergruppe $H \leq K^*$ mit $|H| = p^d - 1$. Nach (2) in (2.8.3) teilt $o(h)$ die Ordnung $|H| = p^d - 1$ für jedes $h \in H$, also $h^{p^d - 1} = 1$, also $h^{p^d} = h$, d.h. h ist Nullstelle von $x^{p^d} - x$. Zusammen mit 0 sind das alle Nullstellen des Polynoms $x^{p^d} - x$, d.h. K enthält $GF(p)(x^{p^d} - x) = GF(p^d)$.

Sei T nun irgendein Teilkörper von $K = GF(p^n)$. Dann ist $T^* \leq K^*$ und nach Lagrange gilt $|T^*| \mid |K^*| = p^n - 1$; ferner $T \simeq GF(p^d)$ für ein d (nach (2.8.7)) und somit $p^d - 1 \mid p^n - 1$. Nach Hilfssatz gilt $d \mid n$. Wie eben ist $T = GF(p)(x^{p^d} - x)$.

Beispiel:

- $p = 7$ und $n = 6$, dann existieren

$$\begin{array}{ccccc} & & GF(7^6) & & \\ & \nearrow & & \nwarrow & \\ GF(7^2) & & & & GF(7^3) \\ & \nwarrow & & \nearrow & \\ & & GF(7) & & \end{array}$$

3 Die Galoissche Theorie

3.9 Separabilität, Satz vom primitiven Element

3.9.1 separabel

DEFINITIONEN: Seien $K \leq L$ Körper.

1. Ein irreduzibles Polynom $f \in K[x]$ heißt *separabel (über K)*, wenn f im Zerfällungskörper $K(f)$ nur einfache Nullstellen besitzt, d.h. $f = c(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ mit $\alpha_i \in K$ und $\alpha_i \neq \alpha_j$ für $i \neq j$.

   Bemerkung: Diese Definition ist unabhängig von der Wahl des Zerfällungskörpers. *Beweis:* Angenommen, $K(f)_1$ ist weiterer Zerfällungskörper, mit (2.7.1) existiert $\sigma : K(f) \to K(f)_1$ Isomorphismus über K, es gilt $f^{\bar{\sigma}} = f$ und nach (2.7.3) wird eine Nullstelle α_i von f in $K(f)$ durch σ auf die Nullstelle von f in $K(f)_1$ abgebildet; dabei ist $\alpha_i^\sigma \neq \alpha_j^\sigma$ für $i \neq j$.

2. Ein Polynom $f \in K[x]$ heißt separabel, wenn es Produkt irreduzibler separabler Polynome aus $K[x]$ ist.

3. Ein algebraisches Element $\alpha \in L$ heißt separabel über K, wenn $p_\alpha \in K[x]$ separabel ist.

   Bemerkung: Das ist äquivalent dazu, daß α Nullstelle eines separablen Polynoms aus $K[x]$ ist.

4. L heißt *separabel* über K, wenn L algebraisch über K ist und alle $\alpha \in L$ über K separabel sind.

LEMMA:

1. Sei $f \in K[x]$ mit $K \leq L$. Ist f separabel über K, so ist f separabel über L.

2. Für $K \leq M \leq L$ gilt: Ist L separabel über K, so ist L separabel über M.

BEWEIS:

1. Nach Definition ist $f = p_1 \cdot \ldots \cdot p_r$ mit separablen irreduziblen Polynomen $p_i \in K[x]$. Da $L[x]$ ZPE-Ring ist, ist $f = q_1 \cdot \ldots \cdot q_s$ mit $q_i \in L[x]$ irreduzibel. Da $q_i \mid f = p_1 \cdot \ldots \cdot p_r$ in $L[x]$ und q_i Primelement, existieren j mit $q_i \mid p_j$. Somit ist jede Nullstelle von q_i eine Nullstelle von p_j, da p_j separabel ist, sind alle Nullstellen von p_j (also auch von q_i) verschieden, damit ist q_i separabel (über L). Dann ist f separabel.

2. Da L algebraisch über K ist, ist L algebraisch über M. Sei $\alpha \in L$, seien $p_\alpha \in K[x]$ und $q_\alpha \in M[x]$ die zugehörigen Minimalpolynome von α. Es ist $p_\alpha \in M[x]$ mit $p_\alpha(\alpha) = 0$, d.h. $q_\alpha \mid p_\alpha$. Da p_α separabel ist, also lauter verschiedene Nullstellen hat, folgt wie eben q_α separabel. Somit ist α separabel über M, also ist L separabel über M.

3.9.2 Kriterium für inseparable Polynome

LEMMA: Ist f ein inseparables irreduzibles Polynom aus $K[x]$, so ist $f' = 0$.

BEWEIS: Sei $L = K(f)$. Da f inseparabel, existiert mehrfache Nullstelle α von f in L. Nach (2.8.6) ist also $f'(\alpha) = 0 = f(\alpha)$. Betrachte $p_\alpha \in K[x]$. Nach (2.4.4) gilt $p_\alpha \mid f$ und $p_\alpha \mid f' \in K[x]$. Da p_α und f irreduzibel, also $f \mid f'$, mit Gradformel folgt $f' = 0$, sonst $\operatorname{grad} f' < \operatorname{grad} f$.

SATZ: Sei K ein Körper.

1. Ist $\operatorname{char} K = 0$, so ist jedes (irreduzible) Polynom aus $K[x]$ separabel.
2. Ist $\operatorname{char} K = p > 0$, so ist ein irreduzibles Polynom $f \in K[x]$ genau dann inseparabel, wenn $f = g(x^p)$ für ein $g \in K[x]$ mit Grad $g \geq 1$.

BEWEIS:

1. Mit $f = \sum_{i=0}^n a_i x^i$, $a_n \neq 0$ folgt $f' = n a_n x^{n-1} + \ldots \neq 0$, mit Lemma ist also f separabel.
2. „$\Leftarrow$“ Sei $f = g(x^p)$, $f = \sum_{i=0}^k b_i x^i$, dann folgt $f = \sum_{i=0}^k b_i x^{ip}$, also $f' = \sum_{i=1}^k ip b_i x^{ip-1} = 0$. Somit ist jede Nullstelle α von f in $K(f)$ nach (2.8.6) eine mehrfache Nullstelle, also f inseparabel.

   „$\Rightarrow$“ Sei f inseparabel, mit Lemma ist $f' = 0$, also $f = \sum_{i=0}^n a_i x^i$ mit $f' = \sum_{i=1}^n i a_i x^{i-1}$. Damit ist $i a_i = 0$ für alle i, also $a_i = 0$ für alle i mit $p \nmid i$, d.h. $f = \sum_{j=0}^k a_{jp} x^{jp}$. Somit $f = g(x^p)$ für $g = \sum_{j=0}^k a_{jp} x^j$.

3.9.3 Beispiele inseparabler Polynome

Satz: Sei $\operatorname{char} K = p > 0$, $a \in K$.

(a) Ist $a = b^p$ mit $b \in K$, so ist $x^p - a = (x-b)^p$ reduzibel.

(b) Ist $a \neq b^p$ für alle $b \in K$, so ist $x^p - a$ irreduzibel und inseparabel.

(c) Ist α transzendent über einem Körper F und $K = F(\alpha)$, so ist $x^p - \alpha$ irreduzibel und inseparabel über K.

Beweis:

(a) $(x-b)^p = x^p - b^p = x^p - a$ (nach Aufgabe 8 in $K(x)$).

(b) Sei L ein Zerfällungskörper von $f = x^p - a$. Sei $\beta \in L$ eine Nullstelle von f, d.h. $\beta^p = a$. Nach (a) ist $f = x^p - a = (x-\beta)^p$. Zu zeigen: f irreduzibel in $K[x]$. Angenommen, $f = gh$ mit $1 \leq \operatorname{grad} g < p$ und $g, h \in K[x]$. Also $g \cdot h = f = (x-\beta)^p$ in $L[x]$. Somit ist $g = (x-\beta)^k = x^k - k\beta x^{k-1} + \ldots$ mit $1 \leq k < p$; da $g \in K[x]$ muß $k\beta \in K$ liegen. Damit liegt aber $\beta \in K$. Widerspruch, also f irreduzibel.

(c) Da $\beta \in K$ existiert mit $\beta^p = \alpha$, d.h. es existieren $f, g \in F[x]$ mit $\alpha = \beta^p = \frac{f(\alpha)^p}{g(\alpha)^p}$. Also ist $g(\alpha)^p \cdot \alpha = f(\alpha)^p$. Für die Grade gilt: $np + 1 = mp$ für $n = \operatorname{grad} g, m = \operatorname{grad} f$, das ist jedoch ein Widerspruch, da $p \nmid 1$.

3.9.4 Monomorphismus, Primkörper

Lemma: Sei K ein Körper mit $\operatorname{char} K = p > 0$.

1. Dann ist die Abbildung $\sigma : K \to K$ mit $a \mapsto a^p$ ein Monomorphismus. Die Menge der Fixpunkte unter σ ist der Primkörper $GF(p)$.
2. Ist K endlich, so ist σ Automorphismus, der *Frobeniusautomorphismus*.

Beweis:

1. Es gilt laut Aufgabe (8): $(a+b)^\sigma = (a+b)^p = a^p + b^p = a^\sigma + b^\sigma$ und $(ab)^\sigma = (ab)^p = a^p b^p = a^\sigma b^\sigma$. Weiter falls $a \in \operatorname{Kern} \sigma$, ist $0 = a^\sigma = a^p$, also $a = 0$.

   Fixpunkte der Abbildung sind diejenigen Elemente, für die gilt: $a^p = a$, also sind alle Elemente aus $P = \{0, 1, 1+1, 1+1+, \ldots\}$ Fixpunkte. Alle Fixpunkte sind Nullstellen von $x^p - x$, es gibt höchstens p Nullstellen, also ist P die Menge der Fixpunkte.

2. K endlich und σ injektiv, also ist σ surjektiv.

3.9.5 vollkommene Körper

DEFINITION: Der Körper K heißt *vollkommen*, wenn jedes (irreduzible) Polynom aus $K[x]$ separabel über K ist, also alle algebraische Erweiterungen von K separabel sind.

SATZ: Jeder Körper der Charakteristik 0 ist vollkommen. Ein Körper K mit Charakteristik $p > 0$ ist genau dann vollkommen, wenn die Abbildung $\sigma : K \to K, a \mapsto a^p$ ein Automorphismus von K ist.

KOROLLAR: Jeder endliche Körper ist vollkommen.

BEWEIS: Satz (3.9.2) impliziert: bei $\operatorname{char} K = 0$ ist K vollkommen. Sei also $\operatorname{char} K = p > 0$.

„$\Leftarrow$“ Sei K vollkommen. Angenommen σ ist kein Automorphismus. Dann folgt nach (3.9.4): σ nicht surjektiv, d.h. es existiert $a \in K$ mit $a \neq b^p$ für alle $b \in K$. Dann ist nach (3.9.3)(b) $x^p - a$ inseparabel, Widerspruch.

„$\Rightarrow$“ Sei nun σ ein Automorphismus. Angenommen $f \in K[x]$ irreduzibel und inseparabel. Nach (3.9.2) existiert $g \in K[x]$ mit $f = g(x^p)$. Sei $g = \sum_{i=0}^k b_i x^i$. Da σ surjektiv, existieren c_i mit $c_i^p = b_i (i = 1, \ldots, k)$, also

$$f = \sum_{i=0}^{k} b_i x^{pi} = \sum_{i=0}^{k} c_i^p (x^i)^p = \sum_{i=0}^{k} (c_i x^i)^p = \left(\sum_{i=0}^{k} c_i x^i \right)^p$$

Dies ist Widerspruch zu f irreduzibel.

3.9.6 Der Satz vom primitiven Element

SATZ: Jede endliche separable Erweiterung ist einfach.

BEMERKUNGEN:

1. Falls $K \leq L, [L : K] < \infty$ und separabel, so existiert $\alpha \in L$ mit $L = K(\alpha)$. Dieses α ist ein primitives Element nach (2.4.1).

2. Man kann gut rechnen in $K(\alpha)$.

3. Falls $\operatorname{char} K = 0$, so kann „separabel“ weggelassen werden.

LEMMA: Sei $K \leq L = K(\alpha, \beta)$ mit α algebraisch und β separabel über K. Dann existiert $\gamma \in L$ mit $L = K(\gamma)$.

BEWEIS:

Hilfssatz: Seien $a, b \in R \leq S$ Hauptidealringe. Ist $c \in \mathrm{ggT}_S(a, b)$, so existiert eine Einheit $s \in S$ mit $cs \in \mathrm{ggT}_R(a, b)$. *Beispiele:*

1. $R = \mathbb{Z}, S = \{a + bi \mid a, b \in \mathbb{Z}\}$ der Gaußsche Ring, $a = 4, b = 6$. $(2i)(-2i) = 4, (2i)(-3i) = 6$, daraus folgt: $2i \in \mathrm{ggT}_S(4, 6)$. Für $s = i$ ist $2is = -2 \in \mathrm{ggT}_R(4, 6)$.
2. Seien $K \leq L$ Körper, $R = K[x]$ und $S = L[x]$. Sei $f = (x^2 + 1)x$ und $g = (x^2 + 1)(x + 1)$. Dann gilt $\mathrm{ggT}_R(f, g) \ni (x^2 + 1) \in \mathrm{ggT}_S(f, g)$, kleinere Teiler in S (z.B. $x + i$) müssen nicht die Eigenschaft haben, mit Teilern in R assoziiert zu sein!

Beweis: Sei $d \in \mathrm{ggT}_R(a, b)$. Nach Satz (1.2.9) existiert $r_i, s_i \in S$ mit $c = s_1 a + s_2 b, d = r_1 a + r_2 b$. In S gilt: $c \mid a, b$, daraus folgt: $c \mid r_1 a + r_2 b = d$, genauso $d \mid c$. Damit $d \sim c$ in S, also existiert eine Einheit $s \in S$ mit $d = cs \in \mathrm{ggT}_R(a, b)$.

Ist K endlich, so ist $K(\alpha)$ endlich (da endlichdimensionaler Vektorraum über K), also auch $K(\alpha)(\beta) = L$ endlich. Daraus folgt mit (2.8.5): $L = F(\gamma)$ mit F Primkörper in L (für geeignetes γ) erst recht $L = K(\gamma)$.

Sei also K unendlich. Sei $p = p_\alpha, q = p_\beta$ Minimalpolynome von α bzw. β über K und sei $M = L(p \cdot q)$ ein Zerfällungskörper von $p \cdot q$ über L. Seien $\alpha_1, \ldots, \alpha_r$ die verschiedenen Nullstellen von p in M und $\beta_1, \ldots, \beta_s$ die verschiedenen Nullstellen von q in M. Sei $\alpha = \alpha_1, \beta = \beta_1$. Für $k \neq 1$ ist $\beta_k \neq \beta_1$ und somit $(\beta_1 - \beta_k)x + (\alpha_1 - \alpha_i) \in M[x]$ von Grad 1 (für alle $k > 1$ und alle i). Da K unendlich, existiert $c \in K$, das nicht Nullstelle ist für alle diese Polynome, also mit

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1 \text{ für alle } i = 1, \ldots, r, k = 2, \ldots, s \tag{$\star$}$$

Setze $\gamma = \alpha_1 + c\beta_1 = \alpha + c\beta \in K(\alpha, \beta)$. *Behauptung:* $K(\gamma) = L = K(\alpha, \beta)$. *Beweis:* betrachte die Polynome q und $f = p(\gamma - cx)$ (d.h. $\gamma - cx \in M[x]$ eingesetzt in p). Beides sind Polynome in $M[x]$; sei $g \in \mathrm{ggT}_{M[x]}(q, f)$. Da β, also q separabel und irreduzibel, hat q nur einfache Nullstellen in M und somit ist $q = (x - \beta_1) \ldots (x - \beta_s)$. Es folgt: g ist Produkt der $(x - \beta_i)$ mit $x - \beta_i \mid f$, also $f(\beta_i) = 0$. Offenbar gilt: $f(\beta_1) = p(\gamma - c\beta_1) = p(\alpha_1) = 0$. Für $k \geq 2$ ist

$$f(\beta_k) = p(\gamma - c\beta_k) = p(\alpha_1 + c\beta_1 - c\beta_k) \neq 0$$

da laut $(\star)$ $\alpha_1 + c\beta_i - c\beta_k \neq \alpha_i$ ist. Für alle i und $\alpha_1, \ldots, \alpha_r$ genau die Nullstellen von p sind. Somit $g = x - \beta_1$. Hilfssatz mit $a = q, b = f, R =$

$K(\gamma)[x] \leq M[x] = S$ liefert: es existiert $m \in M^*$ (= Einheit in $M[x]$) mit $mg = mx - m\beta_1 \in K(\gamma)[x]$. Dann $m \in K(\gamma), m\beta \in K(\gamma)$, also $\beta_1 = \beta \in K(\gamma)$. Weiter gilt: $\alpha = \gamma - c\beta \in K(\gamma)$, also $K(\alpha, \beta) \leq K(\gamma) \leq K(\alpha, \beta)$.

Beweis des Satzes: Sei $L = K(\alpha_1, \ldots, \alpha_n), \alpha_i$ separabel über K. Zu zeigen: L einfach. Induktion nach n. Verankerung für $n = 1$ trivial. Sei die Aussage also für $n - 1$ richtig, d.h. $K(\alpha_1, \ldots, \alpha_{n-1}) = K(\beta)$ mit geeignetem β. Nach dem Lemma ist $L = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\beta, \alpha_n) = K(\gamma)$ mit $\gamma \in L$.

Beispiel: Zu $\mathbb{Q}(\sqrt{2}, \sqrt{3})$: $p = x^2 - 2, q = x^2 - 3, \alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \beta_1 = \sqrt{3}, \beta_2 = -\sqrt{3}$. Da $c = 1$ die Eigenschaft $(\star)$ erfüllt, gilt $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + 1 \cdot \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

3.10 der Hauptsatz der Galoistheorie

3.10.1 die Galoiskorrespondenz

Sei L ein Körper, G eine Untergruppe der Gruppe $\operatorname{Aut} L$.

Definitionen:

1. Für $U \leq G$ sei $U\mathfrak{F} := \{a \in L \mid a^\sigma = a \text{ für alle } \sigma \in U\}$ Menge der Fixelemente unter U.
2. Für $K \leq L$ sei $K\mathfrak{G} := \{\sigma \in G \mid a^\sigma = a \text{ für alle } a \in K\}$.
3. $\mathfrak{V}(G) = \{U \mid U \leq G\}$ ist der Untergruppenverband von G
4. $\mathfrak{V}(L) = \{K \mid K \leq L\}$ ist der Teilkörperverband von L

Lemma: Für jede Teilmenge U von G ist $U\mathfrak{F} \leq L$ Teilkörper, für jede Teilmenge K von L ist $K\mathfrak{G} \leq G$ Untergruppe.

Beweis: Seien $a, b \in U\mathfrak{F}$, dann $(a + b)^\sigma = a^\sigma + b^\sigma = a + b$ für alle $\sigma \in U$, also $a + b \in U\mathfrak{F}$, genauso mit $-, \cdot, /$. Damit ist $U\mathfrak{F} \leq F$, da $1, 0 \in U\mathfrak{F}$.

Seien $\sigma, \tau \in K\mathfrak{G}$, d.h. $a^\sigma = a = a^\tau$ für alle $a \in K$. Dann ist $a^{\sigma\tau^{-1}} = (a^\sigma)^{\tau^{-1}} = a^{\tau^{-1}} = a$, also $\sigma\tau^{-1} \in K\mathfrak{G}$. Daraus folgt: $K\mathfrak{G} \leq G$, da $1 \in K\mathfrak{G}$.

Korollar: Ist P der Primkörper in L, so ist $a^\sigma = a$ für alle $a \in P$ und $\sigma \in \operatorname{Aut} L$.

Beweis: Da $\sigma \in \operatorname{Aut} L$, ist $P \leq \{\sigma\}\mathfrak{F} \leq L$, da P der Schnitt aller Teilkörper ist.

SATZ: Seien $\mathfrak{F}$ und $\mathfrak{G}$ wie oben auf $\mathfrak{V}(G)$ bzw. $\mathfrak{V}(L)$ definiert. Dann gilt für alle $U, U_1, U_2 \in \mathfrak{V}(G)$ und $K, K_1, K_2 \in \mathfrak{V}(L)$:

(a) $U_1 \leq U_2 \Rightarrow U_2\mathfrak{F} \leq U_1\mathfrak{F}$

(b) $K_1 \leq K_2 \Rightarrow K_2\mathfrak{G} \leq K_1\mathfrak{G}$

(c) $U \leq U\mathfrak{F}\mathfrak{G}$

(d) $K \leq K\mathfrak{G}\mathfrak{F}$

Aus (a) bis (d) folgt (allgemein):

(e) $U\mathfrak{F} = U\mathfrak{F}\mathfrak{G}\mathfrak{F}$

(f) $K\mathfrak{G} = K\mathfrak{G}\mathfrak{F}\mathfrak{G}$

BEMERKUNG: Eine Beziehung der Art $U = U\mathfrak{F}\mathfrak{G}$ heißt *Galoiskorrespondenz*.

BEWEIS:

(a) Aus $a \in U_2\mathfrak{F}$ folgt (Definition von $\mathfrak{F}$): $a^\sigma = a$ für alle $\sigma \in U_2$, dann folgt mit $U_1 \leq U_2$, daß $a^\sigma = a$ für alle $\sigma \in U_1$, also $a \in U_1\mathfrak{F}$

(b) Sei $\sigma \in K_2\mathfrak{G}$, mit Definition von $\mathfrak{G}$ folgt $a^\sigma = a$ für alle $a \in K_2$, da $K_1 \leq K_2$ gilt $a^\sigma = a$ für alle $a \in K_1$, also ist $\sigma \in K_1\mathfrak{G}$.

(c) Aus $\sigma \in U$ folgt mit der Definition von $\mathfrak{F}$: $a^\sigma = a$ für alle $a \in U\mathfrak{F}$, daraus folgt (Definition von $\mathfrak{G}$): $\sigma \in (U\mathfrak{F})\mathfrak{G} = U\mathfrak{F}\mathfrak{G}$.

(d) Aus $a \in K$ folgt mit der Definition von $\mathfrak{G}$: $a^\sigma = a$ für alle $\sigma \in K\mathfrak{G}$, daraus folgt (Definition von $\mathfrak{F}$): $a \in (K\mathfrak{G})\mathfrak{F} = K\mathfrak{G}\mathfrak{F}$.

(e) Nach (c) gilt: $U \leq U\mathfrak{F}\mathfrak{G}$, mit (a) gilt $U\mathfrak{F} \geq U\mathfrak{F}\mathfrak{G}\mathfrak{F}$. Aus (d) folgt zudem $U\mathfrak{F} \leq U\mathfrak{F}\mathfrak{G}\mathfrak{F}$.

(f) Symmetrisch zu (e).

BEISPIELE:

1. Sei $L = \mathbb{C}$ und $\sigma : a + bi \mapsto a - bi$, somit $U = \langle\sigma\rangle \leq \operatorname{Aut}\mathbb{C}$.

   - Für $a + bi \in U\mathfrak{F}$ ist $a + bi = (a + bi)^\sigma = a - bi$, also $b = 0$; somit: $U\mathfrak{F} = \mathbb{R}$
   - Für $\tau \in \mathbb{R}\mathfrak{G}$ ist $(a + bi)^\tau = a^\tau + b^\tau i^\tau = a + bi^\tau$; zudem gilt $(i^\tau)^2 = (i^2)^\tau = (-1)^\tau = -1$, also $i^\tau = \pm i$; somit ist $\tau = \mathrm{id}$ oder $\tau = \sigma$. Somit ist $\mathbb{R}\mathfrak{G} = U$.

2. Sei $L = \mathbb{Q}(\sqrt{2}, i) = \left\{ a + b\sqrt{2} + ci + di\sqrt{2} \;\middle|\; a,b,c,d \in \mathbb{Q} \right\}$ (Beispiel 5 aus (2.5)). Für $\sigma \in G = \operatorname{Aut} L$ ist

$$\begin{aligned}(a + b\sqrt{2} + ci + di\sqrt{2})^\sigma &= a^\sigma + b^\sigma(\sqrt{2})^\sigma + c^\sigma i^\sigma + d^\sigma i^\sigma(\sqrt{2})^\sigma \\ &= a + b(\sqrt{2})^\sigma + ci^\sigma + di^\sigma(\sqrt{2})^\sigma\end{aligned}$$

Frage: Was ist i^σ und $\sqrt{2}^\sigma$? Die Zahl $\sqrt{2}$ ist Nullstelle von $x^2 - 2$, mit (2.7.3) gilt: $(\sqrt{2})^\sigma$ ist Nullstelle von $x^2 - 2$, also ist $(\sqrt{2})^\sigma = \pm\sqrt{2}$. Entsprechend $i^\sigma = \pm i$. Also existieren die vier Möglichkeiten

$\sqrt{2} \mapsto \dots$	$i \mapsto \dots$		σ_j	$(a + b\sqrt{2} + ci + di\sqrt{2})^{\sigma_j}$
$\sqrt{2} \mapsto \sqrt{2}$	$i \mapsto i$	$\Rightarrow$	$\sigma = \mathrm{id}$	$a + b\sqrt{2} + ci + di\sqrt{2}$
$\sqrt{2} \mapsto \sqrt{2}$	$i \mapsto -i$	$\Rightarrow$	σ_1	$a + b\sqrt{2} - ci - di\sqrt{2}$
$\sqrt{2} \mapsto -\sqrt{2}$	$i \mapsto i$	$\Rightarrow$	σ_2	$a - b\sqrt{2} + ci - di\sqrt{2}$
$\sqrt{2} \mapsto -\sqrt{2}$	$i \mapsto -i$	$\Rightarrow$	σ_3	$a - b\sqrt{2} - ci + di\sqrt{2}$

Dann ist $G = \{1, \sigma_1, \sigma_2, \sigma_3\}$ und $U_i = \langle \sigma_i \rangle$ für $i = 1, 2, 3$.

Nun sind die $L_i := U_i\mathfrak{F}$ die folgenden: $L_1 = \mathbb{Q}(\sqrt{2})$ (mehr nicht wegen Gradsatz), $L_2 = \mathbb{Q}(i)$ und $L_3 = \mathbb{Q}(i\sqrt{2})$. Es gilt jeweils $L_i\mathfrak{G} = U_i$. Außerdem gilt: $G\mathfrak{F} \leq U_1\mathfrak{F} \cap U_2\mathfrak{F} = \mathbb{Q}$.

Behauptung: $L_1, L_2, L_3, \mathbb{Q}, L$ sind alle Teilkörper von L. *Beweis:* Angenommen, es existiert weiterer Teilkörper von K, dann ist $[K : \mathbb{Q}] = [L : K] = 2$; sei $\alpha \in L \setminus K$ und $p_\alpha \in K[x]$ zugehöriges Minimalpolynom. Nach Satz (2.5.1) ist Grad $p_\alpha = 2$. und die Erweiterung ist normal (2.7.1). Somit ist mit α auch die zweite Nullstelle β von p_α in L enthalten und $L = K(\alpha) = K(\beta)$. Nach (2.4.6) existiert ein Isomorphismus $\sigma : K(\alpha) \to K(\beta)$ mit $\alpha^\sigma = \beta$ und $a^\sigma = a$ für alle $a \in K$. Also ist $\alpha \in \operatorname{Aut} L = G$. Da K vollkommen, ist p_α separabel und somit $\alpha \neq \beta$, also $\sigma \neq \mathrm{id}$. Also $\sigma = \sigma_i$ für ein i und $K \leq \{\sigma_i\}\mathfrak{F} = L_i$, also $2 = [L_i : \mathbb{Q}] = [L_i : K] \cdot [K : \mathbb{Q}] = 2 \cdot [L_i : K]$, damit $L_i = K$.

3.10.2 Endliche Körper

Sei $L = GF(p^n)$ und $G = \operatorname{Aut} L$.

Satz:

1. $\operatorname{Aut} L$ ist zyklisch der Ordnung n und wird erzeugt vom Frobeniusautomorphismus $\sigma : L \to L$ mit $a \mapsto a^P$.

2. Für jeden Teiler d von n gilt: $GF(p^d)\mathfrak{G} = \left\langle \sigma^d \right\rangle$ und $\left\langle \sigma^d \right\rangle \mathfrak{F} = GF(p^d)$.

Beweis:

1. Nach Lemma (3.9.4) ist $\sigma \in \operatorname{Aut} L$. Sei $F = GF(p)$ und $\alpha \in GF(p^n)^*$ mit $GF(p^n) = F(\alpha)$ (existiert nach (2.8.5)). Offenbar gilt $\alpha^{\sigma^i} = \alpha^{p^i}$, und da $1, \alpha, \alpha^2, \ldots, \alpha^{p^n-1}$ genau die Elemente von L^* sind, sind $\alpha^{p^i} \neq \alpha^{p^j}$ für $i, j \in \{0, \ldots, n-1\}$ für $i \neq j$; also $1 = \sigma^0, \sigma, \sigma^2, \sigma^{n-1}$ paarweise verschieden. Ist p_α das Minimalpolynom von α über F, so ist $n = [F(\alpha) : F] \overset{(2.5.1)}{=} \operatorname{grad} p_\alpha$.

   Nach (2.7.3) ist aber für jeden Automorphismus τ von L das Element α^τ Nullstelle des Polynoms $p_\alpha^\tau \overset{(3.10.1)}{=} p_\alpha$, davon gibt es höchstens n, ferner ist wegen $L = F(\alpha)$ jeder Automorphismus durch α^τ festgelegt. Also $|\operatorname{Aut} L| \leq n$, somit $\operatorname{Aut} L = \{1, \sigma, \ldots, \sigma^{n-1}\}$ zyklisch von σ erzeugt.

2. Für $a \in L$ gilt: $a \in GF(p^d)$ genau dann, wenn (2.8.7) $a = a^{p^d} = a^{\sigma^d}$. Dies ist äquivalent zu $a \in \langle \sigma^d \rangle \mathfrak{F}$, d.h. $GF(p^d) = \langle \sigma^d \rangle \mathfrak{F}$.

   Für $GF(p^d) = F(\beta)$ und $1 \leq i \leq n$ gilt: $\sigma^i \in GF(p^d)\mathfrak{G}$ genau dann, wenn $\beta = \beta^{\sigma^i} = \beta^{p^i}$. Dies ist äquivalent zu $\beta^{p^i-1} = 1$, also $o(\beta) = p^d - 1 \mid p^i - 1$. Dies ist genau dann der Fall, wenn $d \mid i$ gilt, also $\sigma^i \in \langle \sigma^d \rangle$, also $GF(p^d)\mathfrak{G} = \langle \sigma^d \rangle$.

Beispiele:

3. $L = \mathbb{Q}(\sqrt[4]{5})$ (Aufgabe 27), dann ist $[L : \mathbb{Q}] = 4$, $f = x^4 - 5$, $\alpha = \sqrt[4]{5}, -\alpha \in L$. Dann ist $|\operatorname{Aut} L| = 2$, Sei $\sigma : \alpha \mapsto -\alpha$. Dann ist $\mathbb{Q}\mathfrak{G} = \operatorname{Aut} L$, $\mathbb{Q}\mathfrak{G}\mathfrak{F} = (\operatorname{Aut} L)\mathfrak{F} = \mathbb{Q}(\sqrt{5})$ (wegen $(\sqrt{5})^\sigma = (\alpha^2)^\sigma = (\alpha^\sigma)^2 = (-\alpha)^2 = \alpha^2 = \sqrt{5}$); also ist $\mathbb{Q} < \mathbb{Q}\mathfrak{G}\mathfrak{F}$, da L nicht normal über $\mathbb{Q}$ ist, gibt es zu wenige Automorphismen.

4. Beispiel (3.9.3)(c): $F = GF(p)$, $K = F(\alpha)$, α transzendent über F, dann ist $L = K(x^p - \alpha)$; sei β Nullstelle von $x^p - \alpha$, dann folgt $x^p - \alpha = (x - \beta)^p$, also ist $K\mathfrak{G} = 1$, also $K\mathfrak{G}\mathfrak{F} = L > K$; da L nicht separabel über K.

3.10.3 die Galoisgruppe

Definition: $\operatorname{Gal}(L/K) := \{\sigma \in \operatorname{Aut} L \mid a^\sigma = a \text{ für alle } a \in K\}$ $(= K\mathfrak{G})$ *Galoisgruppe* von L über K.

Satz: Seien $(K_1, L_1), (K_2, L_2)$ endliche Körpererweiterungen und sei $\sigma : K_1 \to K_2$ ein Isomorphismus.

1. Dann existieren höchstens $[L_1 : K_1]$ Fortsetzungen von σ zu Isomorphismen von L_1 auf L_2.

2. Ist $L_1 = K_1(f)$ mit einem separablen Polynom $f \in K_1[x]$ und ist $L_2 = K_2(f^{\bar{\sigma}})$, so existieren genau $[L_1 : K_1]$ Fortsetzungen von σ zu Isomorphismen von L_1 auf L_2.

Korollar: Sei L eine endliche Erweiterung von K. Dann gilt:

1. $|\mathrm{Gal}(L/K)| \leq [L : K]$

2. Ist $L = K(f)$ mit f separabel aus $K[x]$, so ist $|\mathrm{Gal}(L/K)| = [L : K]$

Beweis des Korollars: Folgt aus dem Satz mit $K_1 = K_2 = K, \sigma = \mathrm{id}, L_1 = L_2 = L$.

Beweis des Satzes:

1. Induktion über $[L_1 : K_1]$. Falls $[L_1 : K_1] = 1$, dann ist $L_1 = K_1$, also existiert höchstens eine Fortsetzung.

   Sei $[L_1 : K_1] > 1$. Sei $\alpha \in L_1 \setminus K_1$. Sei τ eine Fortsetzung von σ zu einem Isomorphismus von $K_1(\alpha)$ auf einen Teilkörper von L_2. Nach (2.5.2) ist α algebraisch über K_1, sei p_α das Minimalpolynom. Dann ist nach (2.7.3) α^τ eine Nullstelle von $p_\alpha^{\bar{\tau}} = p_\alpha^{\bar{\sigma}}$. Nach (1.3.9) hat p_α höchstens $\operatorname{grad} p_\alpha^{\bar{\sigma}} = \operatorname{grad} p_\alpha = [K_1(\alpha) : K]$ Nullstellen. Damit hat σ höchstens $[K_1(\alpha) : K]$ Fortsetzungen τ. Da nach (2.5.3) $[L_1 : K_1(\alpha)] = \frac{[L_1:K_1]}{[K_1(\alpha):K_1]} < [L_1 : K_1]$ existiert nach Induktionsannahme für jedes solche τ höchstens $[L_1 : K_1(\alpha)]$ Fortsetzungen zu Isomorphismen von L_1 auf L_2. Da jede Fortsetzung von σ so auftritt, existieren insgesamt höchstens $[K_1(\alpha) : K] \cdot [L_1 : K_1(\alpha)] = [L_1 : K_1]$ Fortsetzungen von σ.

2. Induktion über $[L_1 : K_1]$ Falls $[L_1 : K_1] = 1$, so ist $L_1 = K_1 = K_1(f)$, d.h. $K_2(f^{\bar{\sigma}}) = K_2 = L$, also ist σ die einzige Fortsetzung.

   Sei also $L_1 = K_1(f) > K_1$ und f separabel. Nach Definition (2.7.1) ist $f = p \cdot q$ mit p irreduzibel, $\operatorname{grad} p \geq 2$ und $q \in K_1(x)$ und p separabel. Da $L_1 = K_1(f)$, existieren $\alpha_i \in L$ mit $p = (x - \alpha_1) \ldots (x - \alpha_m), m = \operatorname{grad} p; \alpha_i \neq \alpha_j$ für $i \neq j$ (da p separabel). Sei $M_1 = K_1(\alpha_1, \ldots, \alpha_m) \leq L$.

   Da $\bar{\sigma}$ Homomorphismus, so ist $f^{\bar{\sigma}} = p^{\bar{\sigma}} \cdot q^{\bar{\sigma}}$, in L_2 zerfällt $p^{\bar{\sigma}} = (x -$

$\beta_1)\ldots(x-\beta_m)$. Sei $M_2 = K_2(\beta_1,\ldots,\beta_m)$. Da $M_1 = K_1(p)$ und $M_2 = K_2(p^{\bar\sigma})$, existiert nach (2.7.4) ein Isomorphismus $\tau : M_1 \to M_2$ mit $\tau|_{K_1} = \sigma$. Dann gilt

$$p^{\bar\sigma} = p^{\bar\tau} = (x-\alpha_1)^{\bar\tau}\ldots(x-\alpha_m)^{\bar\tau} = (x-\alpha_1^\tau)\ldots(x-\alpha_m^\tau)$$

Offenbar $\alpha_i^\tau \neq \alpha_j^\tau$ für $i \neq j$, d.h. $p^{\bar\sigma}$ hat m verschiedene Nullstellen. Sei $\alpha = \alpha_1$ fest. Nach Satz (2.4.6) existieren Fortsetzungen $\sigma_i : K_1(\alpha) \to K_2(\beta_i)$ von σ mit $\alpha^{\sigma_i} = \beta_i$ für $i = 1,\ldots,m$.

Da $L_1 = K_1(\alpha)(f)$ und nach Lemma (3.9.1) ist f separabel in $K_1(\alpha)$ und $L_2 = K_2(f^{\bar\sigma}) = K_1(\alpha)^{\sigma_i}(f^{\bar\sigma}) = K_1(\alpha)^{\sigma_i}(f^{\bar\sigma_i})$, existieren nach Induktionsvoraussetzung genau $[L_1 : K_1(\alpha)]$ Fortsetzungen von σ_i zu Isomorphismus von L_1 auf L_2. Da $\sigma_i \neq \sigma_j$ für $i \neq j$ erhalten wir insgesamt $m \cdot [L_1 : K_1(\alpha)]$ verschiedene Fortsetzungen von σ. Wegen $m = \operatorname{grad} p = [K_1(\alpha) : K]$ sind das $[L_1 : K_1]$ Stück. Nach (1) können es nicht mehr sein.

Bemerkungen:

1. Zu Beispiel (2): es folgt $|\operatorname{Aut} L| = 4 = |\operatorname{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$, da $L = \mathbb{Q}(x^2+1)(x^2-2)$. Analog für Beispiel (5).

2. $L = GF(p^n), d \mid n$ und $K = GF(p^d)$, dann ist $\operatorname{Gal}(L/K) = K\mathfrak{G} = \langle \sigma^d \rangle$, also $|\operatorname{Gal}(L/K)| = \frac{n}{d} = [L : K]$.

3.10.4 Satz von Artin

Satz von Artin (1898-1962): Ist G eine endliche Gruppe von Automorphismen des Körpers L, so ist $[L : G\mathfrak{F}] = |G|$.

Beweis: Zu zeigen: $[L : G\mathfrak{F}] = |G| := m$.

„$\geq$“ Ist L eine endliche Erweiterung von $G\mathfrak{F}$, so folgt aus $G \leq \operatorname{Gal}(L/G\mathfrak{F})$: $|G| \leq |\operatorname{Gal}(L/K)| \overset{(3.10.3)}{\leq} [L : G\mathfrak{F}]$.

„$\leq$“ Zu zeigen ist (für $\dim_K L \leq m$), dass je $m+1$ Elemente $\alpha_0,\ldots,\alpha_m \in L$ linear abhängig über K sind, also zu zeigen: es existieren $x_0,\ldots,x_m \in K$, nicht alle 0 mit

$$\alpha_0 x_0 + \ldots + \alpha_m x_m = 0 \tag{i}$$

Betrachte stattdessen das lineare Gleichungssystem:

$$\alpha_0^\sigma x_0 + \ldots + \alpha_m^\sigma x_m = 0 \;\forall\, \sigma \in G \tag{ii}$$

Sei

$$T = \left\{ (a_0, \ldots, a_m) \in L^{m+1} \;\middle|\; \alpha_0^\sigma a_0 + \ldots + \alpha_m^\sigma a_m = 0 \;\forall\, \sigma \in G \right\}$$

Dann ist $\{0\} \neq T \leq L^{m+1}$. *Behauptung:*

$$(a_0, \ldots, a_m) \in T,\ \tau \in G \Longrightarrow (a_0^\tau, \ldots, a_m^\tau) \in T \tag{iii}$$

Beweis: Sei $\sigma \in G$. Mit $\sigma, \tau \in G$ ist auch $\sigma\tau^{-1} \in G$. Somit gilt wegen $(a_0, \ldots, a_m) \in T$:

$$0 = 0^\tau = (\alpha_0^{\sigma\tau^{-1}} a_0 + \ldots + \alpha_m^{\sigma\tau^{-1}} a_m)^\tau = \alpha_0^\sigma a_0^\tau + \ldots + \alpha_m^\sigma a_m^\tau$$

Somit $(a_0^\tau, \ldots, a_m^\tau) \in T$. Sei $0 \neq (a_0, \ldots, a_k, 0, \ldots, 0)$ mit $a_i \neq 0 (0 \leq i \leq k)$ aus T mit höchstens vielen Nullen. Da T ein Teilraum von L^{m+1}, ist dann auch $a_k^{-1}(a_0, \ldots, a_k, 0, \ldots, 0) = (b_0, \ldots, b_{k-1}, 1, 0, \ldots, 0)$ aus T.

Behauptung: $(b_0, \ldots, b_{k-1}, 1, 0, \ldots, 0) \in K^{m+1}$. *Beweis:* Für $\tau \in G$ ist $(b_0^\tau, \ldots, b_{k-1}^\tau, 1, 0, \ldots, 0) \in T$ (nach (iii)), also auch $(b_0 - b_0^\tau, \ldots, b_{k-1} - b_{k-1}^\tau, 0, \ldots, 0) \in T$ mit mehr Nullen, also gleich 0 nach Wahl der a_i. Also ist $b_i = b_i^\tau$ für $i = 0, \ldots, k-1$ und für alle $\tau \in G$ und somit $b_i \in G\mathfrak{F}$ für alle $i = 0, \ldots, k-1$.

3.10.5 Galoissche Körpererweiterungen

Sei $K \leq L$ Körper.

Satz: Die folgenden Eigenschaften der Körpererweiterung (K, L) sind äquivalent:

(1) L ist normal und separabel über K

(2) $L = K(f)$ mit $f \in K[x]$, f separabel

(3) L ist endlich über K und $|\mathrm{Gal}(L/K)| = [L : K]$

(4) Es existiert eine endliche Untergruppe G von $\operatorname{Aut} L$ mit $K = G\mathfrak{F}$.

Definition: Die Körpererweiterung (K, L) heißt *galoissch*, wenn sie eine (und damit alle) der Eigenschaften (1) bis (4) hat. Beweis:

(1) $\Rightarrow$ (2) Sei L normal über K, $L = K(\alpha_1, \ldots, \alpha_n)$ mit $\alpha_i \in L$. Nach Satz (2.7.5) ist dann $L = K(f)$ mit $f = \prod_{i=1}^n p_{\alpha_i}$ (mit p_{α_i} Minimalpolynom $\in K[x]$). Da L separabel über K ist, ist mit (3.9.1) α_i separabel über K, dann sind die p_{α_i} separabel und somit auch f.

(2) $\Rightarrow$ (3) folgt aus (3.10.3)(b), da $[K(f) : K] < \infty$ nach (2.5.1)

(3) $\Rightarrow$ (4) Sei $G := \mathrm{Gal}(L/K)$. Dann ist nach Definition der Galoisgruppe $K \leq G\mathfrak{F}$ Dann ist

$$|G| = |\mathrm{Gal}(L/K)| \overset{\text{Vor}}{=} [L : K] \overset{K \leq G\mathfrak{F}}{\geq} [L : G\mathfrak{F}] \overset{(3.10.4)}{=} |G|$$

Damit folgt $[L : K] = [L : G\mathfrak{F}]$, also ist $K = G\mathfrak{F}$.

(4) $\Rightarrow$ (1) Nach (3.10.4) ist $[L : K] = |G|$ endlich. Wir zeigen:

$$\alpha \in L \Longrightarrow p_\alpha \text{ zerfällt in } L[x] \text{ in lauter verschiedene Linearfaktoren} \qquad (\star)$$

Aus $(\star)$ folgt:

- L normal: Ist $g \in K[x]$ irreduzibel und $\alpha \in L$ mit $g(\alpha) = 0$. Nach (2.4.4) gilt $p_\alpha \mid g$, da beide irreduzibel folgt $g \sim p_\alpha$, mit $(\star)$ folgt: g zerfällt in $L[x]$.
- L separabel: $\alpha \in L$, mit $(\star)$ ist p_α separabel, mit (3.9.1) ist damit α separabel und damit auch L separabel.

Beweis von $(\star)$: Seien $\alpha = \alpha_1, \dots, \alpha_n$ die paarweise verschiedenen Bilder von α unter Elementen aus G. Sei $f = \prod_{i=1}^n (x - \alpha_i)$. Für $\sigma \in G$ ist $f^{\bar{\sigma}} = \prod_{i=1}^n (x - \alpha_i^\sigma) = f$, da $\{\alpha_1, \dots, \alpha_n\} = \{\alpha_1^\sigma, \dots, \alpha_n^\sigma\}$ (Menge der verschiedenen Bilder von α unter G) ist (wegen $\alpha_i^\sigma = \alpha_j^\sigma \Rightarrow \alpha_i = \alpha_j$). Jeder Koeffizient von f ist unter G invariant, liegt also im Fixkörper $G\mathfrak{F} = K$. Damit ist $f \in K[x]$, mit $\alpha = \alpha_1$ folgt $f(\alpha) = 0$, also $p_\alpha \mid f$ in $K[x]$, damit gilt $p_\alpha \mid f$ auch in $L[x]$. Wegen der eindeutigen Zerlegung in Primelemente ist $p_\alpha = \prod_i (x - \alpha_i)$ für einige i.

3.10.6 Hauptsatz der Galoistheorie

Satz: Sei (K, L) eine galoissche Körpererweiterung, $G = \mathrm{Gal}(L/K)$ und $\mathfrak{V}(L/K) = \{R \mid K \leq R \leq L\}$ der Verband der K enthaltenden Teilkörper von L. Dann sind $\mathfrak{F} : \mathfrak{V}(G) \to \mathfrak{V}(L/K)$ und $\mathfrak{G} : \mathfrak{V}(L/K) \to \mathfrak{V}(G)$ zueinander inverse *Antiisomorphismen*, d.h. bijektiv und es gilt für alle $U, U_1, U_2 \leq G$ und $K \leq R, R_1, R_2 \leq L$:

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

(b) $R = R\mathfrak{G}\mathfrak{F}(= \mathrm{Gal}(L/R)\mathfrak{F})$

(c) $U_1 \leq U_2 \Leftrightarrow U_2\mathfrak{F} \leq U_1\mathfrak{F}$

(d) $R_1 \leq R_2 \Leftrightarrow R_2\mathfrak{G} \leq R_1\mathfrak{G}$

(e) $|U_2 : U_1| = [U_1\mathfrak{F} : U_2\mathfrak{F}]$ für $U_1 \leq U_2$.

(e') $|U| = [L : U\mathfrak{F}]$ und $|G : U| = [U\mathfrak{F} : K]$

(f) $|R_2 : R_1| = [R_1\mathfrak{G} : R_2\mathfrak{G}]$ für $R_1 \leq R_2$.

(f') $|R\mathfrak{G}| = [L : R]$ und $|R : K| = [G : R\mathfrak{G}]$

Beweis:

(a) Sei $U \leq G$, dann ist nach (3.10.1) bereits $U \leq U\mathfrak{F}\mathfrak{G} = \mathrm{Gal}(L/U\mathfrak{F})$. Dann ist[30]

$$|U| \leq |U\mathfrak{F}\mathfrak{G}| = |\mathrm{Gal}(L/U\mathfrak{F})| \overset{(3.10.3)}{\leq} [L : U\mathfrak{F}] \overset{(3.10.4)}{=} |U|$$

Damit ist insbesondere $U = U\mathfrak{F}\mathfrak{G}$.

Zusatz: Seien $K \leq L$ Körper und $U \leq \mathrm{Gal}(L/K)$. Ist $[L : K]$ oder U endlich, so gilt $U = U\mathfrak{F}\mathfrak{G}$.

(b) Sei $K \leq R \leq L$, mit (3.10.1) ist $R \leq R\mathfrak{G}\mathfrak{F} \overset{(3.10.3)}{=} \mathrm{Gal}(L/R)\mathfrak{F}$. Dann folgt:

$$[L : R] \geq [L : R\mathfrak{G}\mathfrak{F}] = [L : \mathrm{Gal}(L/R)\mathfrak{F}] \overset{(3.10.4)}{=} |\mathrm{Gal}(L/R)| \overset{(3.10.5)}{=} [L : R]$$

Die letzte Gleichheit folgt, da L galoissch über R ist (nach Lemma (3.9.1) und Korollar (2.7.6)). Somit $[L : R] = [L : R\mathfrak{G}\mathfrak{F}]$, also $R = R\mathfrak{G}\mathfrak{F}$.

[30] „…weil ja alles irgendwie endlich ist…“

(c) Mit $U_1 \leq U_2$ folgt (3.10.1) $U_2\mathfrak{F} \leq U_1\mathfrak{F}$, dann ist nach (3.10.1)

$$U_1 \overset{(a)}{=} U_1\mathfrak{F}\mathfrak{G} \leq U_2\mathfrak{F}\mathfrak{G} \overset{(a)}{=} U_2$$

(d) Mit $R_1 \leq R_2$ folgt (3.10.1) $R_2\mathfrak{G} \leq R_1\mathfrak{G}$, dann ist nach (3.10.1)

$$R_1 \overset{(b)}{=} R_1\mathfrak{G}\mathfrak{F} \leq R_2\mathfrak{G}\mathfrak{F} \overset{(b)}{=} R_2$$

(e) Aus $|U| \overset{(3.10.4)}{=} [L : U\mathfrak{F}]$ folgt:

$$|U_2 : U_1| \overset{(2.8.2)}{=} \frac{|U_2|}{|U_1|} = \frac{[L : U_2\mathfrak{F}]}{[L : U_1\mathfrak{F}]} \overset{(2.5.3)}{=} [U_1\mathfrak{F} : U_2\mathfrak{F}]$$

(f) Da L galoissch über R ist, gilt $|R\mathfrak{G}| = |\mathrm{Gal}(L/R)| = [L : R]$

$$[R_2 : R_1] = \frac{[L : R_1]}{[L : R_2]} = \frac{|R_1\mathfrak{G}|}{|R_2\mathfrak{G}|} = |R_1\mathfrak{G} : R_2\mathfrak{G}|$$

3.10.7 Zwischenkörper, Beispiel $\mathbb{Q}(x^4 - 5)$

Gegeben sei (G, L) galoissch, etwa $L = K(f)$ mit separablem Polynom $f \in K[x]$. Dann müssen wir bestimmen:

1. die Galoisgruppe $G = \mathrm{Gal}(L/K)$
2. den Untergruppenverband von G
3. die Fixkörper dieser Untergruppen

Das liefert nach (3.10.6) alle Zwischenkörper[31]. Wie macht man das?

1. (a) $L = K(\alpha_1, \ldots, \alpha_n)$ mit $f(\alpha_i) = 0$, jeder Automorphismus ist bestimmt durch die Bilder der α_i. Nach (2.7.3) sind diese Bilder Nullstellen von f; G ist also eine Permutationsgruppe auf $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ (Menge der Nullstellen von f).
   (b) $L = K(\beta_1, \ldots, \beta_r)$ und p_{β_i}. Bilder der β_i sind Nullstellen von p_{β_i}
   (c) $L = K(\alpha)$, betrachte p_α, für jede Nullstelle α_i von p existiert Automorphismus σ_i mit $\alpha \to \alpha_i$, das liefert $\mathrm{grad}_{p_\alpha} = [L : K]$ Automorphismen.
2. Siehe Satz von Sylow (3.11.2)

[31] „Wen interessieren schon Zwischenkörper?“

3. siehe Aufgabe 51

Beispiel:

(5) $L = \mathbb{Q}(f), f = x^4 - 5, K = \mathbb{Q}$.

1. Bestimmung der **Galoisgruppe**: Es gilt $[L : \mathbb{Q}] = 8, L = \mathbb{Q}(\alpha, i)$, die Nullstellen von f sind $\alpha = \sqrt[4]{5}$ (die positive reelle Wurzel) sowie $-\alpha, \alpha i, -\alpha i$. Es gilt $L = \mathbb{Q}(\alpha)(i)$. Nach (2.4.6) existiert $\sigma \in \operatorname{Aut} L$ mit $i^\sigma = -i, \alpha^\sigma = \alpha$. Genauso existiert $\delta \in \operatorname{Aut} L$ mit $i^\delta = i, \alpha^\delta = \alpha i$.

   Betrachte nun Potenzen und Produkte von σ und δ:

φ	δ^4	δ	δ^2	δ^3	σ	$\sigma\delta$	$\sigma\delta^2$	$\sigma\delta^3$
φ	σ^2					$\delta^3\sigma$	$\delta^2\sigma$	$\delta\sigma$
α^φ	α	αi	$-\alpha$	$-\alpha i$	α	αi	$-\alpha$	$-\alpha i$
i^φ	i	i	i	i	$-i$	$-i$	$-i$	$-i$
$\mathrm{o}(\varphi)$		4	2		2	2	2	2

   Damit hat $G = \langle \sigma, \delta \rangle$ acht Elemente, ist also Gruppe der Ordnung acht.

2. Bestimmung des **Untergruppenverbandes** von G: Es existieren (bis auf die trivialen) höchstens Untergruppen der Ordnung 2 und 4. Wie in der Tabelle zu sehen, existieren fünf Elemente der Ordnung 2, diese erzeugen alle Untergruppen der Ordnung 2. Für einige ist es offensichtlich (σ), für andere leicht nachzurechnen. Exemplarisch für $(\sigma\delta)^2$: Es gilt $i^{(\sigma\delta)^2} = i$ sowie

   $$(\alpha)^{(\sigma\delta)^2} = (\alpha^{\sigma\delta})^{\sigma\delta} = (\alpha i)^{\sigma\delta} = \alpha^{\sigma\delta} i^{\sigma\delta} = (\alpha i)(-i) = \alpha$$

   Da die Automorphismen $\mathbb{Q}$ ja ohnehin festlassen, ist $(\sigma\delta)^2 = \mathrm{id}$ und somit ist $\langle \sigma\delta \rangle$ eine Untergruppe der Ordnung 2.

   Die Untergruppen der Ordnung 4 sind $\langle \delta \rangle$ sowie $M_1 = \{1, \delta^2, \sigma\delta, \sigma\delta^3\}$

und $M_2 = \{1, \delta^2, \sigma, \sigma\delta^2\}$. Das ergibt insgesamt folgendes Schema:

$$
\begin{array}{ccccc}
 & & \langle \sigma, \delta \rangle & & \\
 & \nearrow & \uparrow & \nwarrow & \\
 & M_1 & \langle \delta \rangle & M_2 & \\
\nearrow & \uparrow & \nwarrow\uparrow\nearrow & \uparrow & \nwarrow \\
\langle \sigma\delta^3 \rangle & \langle \sigma\delta \rangle & \langle \delta^2 \rangle & \langle \sigma \rangle & \langle \sigma\delta^2 \rangle \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
 & & \{1\} & &
\end{array}
$$

3. Bestimmung der **Teilkörper** von L: Analog durch Anwendung von $\mathfrak{F}$:

$$
\begin{array}{ccccc}
 & & \{1\}\mathfrak{F} & & \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
\langle \sigma\delta^3 \rangle \mathfrak{F} & \langle \sigma\delta \rangle \mathfrak{F} & \langle \delta^2 \rangle \mathfrak{F} & \langle \sigma \rangle \mathfrak{F} & \langle \sigma\delta^2 \rangle \mathfrak{F} \\
\nwarrow & \uparrow & \nearrow\uparrow\nwarrow & \uparrow & \nearrow \\
 & M_1\mathfrak{F} & \langle \delta \rangle \mathfrak{F} & M_2\mathfrak{F} & \\
 & \nwarrow & \uparrow & \nearrow & \\
 & & \langle \sigma, \delta \rangle \mathfrak{F} & &
\end{array}
$$

Es fehlt noch die genauere Bestimmung der jeweiligen $(\ldots)\mathfrak{F}$. Wir kennen schon drei quadratische Erweiterungen: $\mathbb{Q}(i), \mathbb{Q}(\alpha^2)$ und $\mathbb{Q}(i\alpha^2)$. Damit gilt $\langle \delta \rangle \mathfrak{F} = \mathbb{Q}(i)$, $M_1\mathfrak{F} = \mathbb{Q}(i\alpha^2)$ sowie $M_2\mathfrak{F} = \mathbb{Q}(\alpha^2)$. Für $\langle \delta^2 \rangle$ findet man leicht durch Betrachtung der obigen Tabelle, daß $\langle \delta^2 \rangle \mathfrak{F} = \mathbb{Q}(i, \alpha^2)$ ist. Desweitern läßt σ das Element α fest, also $\langle \sigma \rangle \mathfrak{F} = \mathbb{Q}(\alpha)$ und $\langle \sigma\delta^2 \rangle \mathfrak{F} = \mathbb{Q}(i\alpha)$.

Schwer bleibt die Bestimmung von $\langle \sigma\delta^3 \rangle \mathfrak{F}$ und $\langle \sigma\delta \rangle \mathfrak{F}$. Es gibt mehrere Möglichkeiten:

(a) Methode von Stewart: Für alle Linearkombinationen der Basis testen, was invariant bleibt.

(b) $\alpha + i$ ist ein primitives Element, da es von keinem Automorphismus festgelassen wird (Aufgabe 50). Nach Aufgabe 51 ist

$$\begin{aligned} p &= (x - (\alpha + i))(x - (\alpha + i)^{\sigma\delta}) \\ &= (x - (\alpha + i))(x - (\alpha i - i)) \\ &= x^2 + x(i - \alpha i - \alpha - i) + (\alpha^2 i - \alpha i - \alpha + 1) \end{aligned}$$

Es folgt $a_1 = -\alpha(1 + i) \quad a_0 = -\alpha(1 + i) + \alpha^2 i + 1$ und damit (mit $\star$: $a_1^2 = 2\alpha^2 i$)

$$\langle \sigma\delta \rangle \mathfrak{F} = \mathbb{Q}(a_0, a_1) \overset{\star}{=} \mathbb{Q}(a_1) = \mathbb{Q}((1 + i)\alpha)$$

Ähnlich bestimmen wir $\langle \sigma\delta^2 \rangle \mathfrak{F}$.

Letztendlich kommt man auf:

$$\begin{array}{ccccc}
 & & L & & \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
\mathbb{Q}(\alpha - i\alpha) & \mathbb{Q}(\alpha + i\alpha) & \mathbb{Q}(i, \alpha^2) & \mathbb{Q}(\alpha) & \mathbb{Q}(i\alpha) \\
\nwarrow & \uparrow & \nearrow\uparrow\nwarrow & \uparrow & \nearrow \\
 & \mathbb{Q}(i\alpha^2) & \mathbb{Q}(i) & \mathbb{Q}(\alpha^2) & \\
 & \nwarrow & \uparrow & \nearrow & \\
 & & \mathbb{Q} & &
\end{array}$$

3.10.8 Konjugierte Untergruppen und Teilkörper

Sei G eine Gruppe, $x, g \in G, X \subseteq G$. Seien $K \leq R_1, R_2 \leq L$ Körper.

DEFINITIONEN:

- $x^g := g^{-1}xg$ das *zu x unter g konjugierte Element*.
- $X^g := \{x^g \mid x \in X\}$ das *zu X unter g konjugierte Teilmenge*.
- R_2 heißt *zu R_1 konjugiert*, wenn es ein $\sigma \in \mathrm{Gal}(L/K)$ gibt mit $R_2 = R_1^\sigma$.

EIGENSCHAFTEN: für alle $x, y, g, h \in G$ gilt

1. $(xy)^g = x^g \cdot y^g$

2. $x^{gh} = (x^g)^h$

Beweis:

1. $x^g \cdot y^g = g^{-1}xgg^{-1}yg = g^{-1}xyg = (xy)^g$

2. $x^{gh} = (gh)^{-1}xgh = h^{-1}g^{-1}xgh = (x^g)^h$

Bemerkung: Eigenschaft (1) zeigt, dass für $g \in G$ die Abbildung $\sigma_g : G \to G, x \mapsto x^g$ ein Homomorphismus ist, ferner ist sie bijektiv, denn aus (2) folgt:

$$\sigma_g \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_1 = \mathrm{id} = \sigma_{g^{-1}}\sigma_g$$

Damit ist σ ein Automorphismus, der von g bewirkte *innere Automorphismus*.

Satz: Sei (K, L) eine Körpererweiterung, $G = \mathrm{Gal}(L/K), \sigma \in G$. Dann gilt für alle $K \leq R \leq L$ und $U \leq G$:

1. $(R\mathfrak{G})^\sigma = R^\sigma\mathfrak{G}$ (konjugierte Körper werden auf konjugierte Untergruppen (durch $\mathfrak{G}$) abgebildet)

2. $(U^\sigma)\mathfrak{F} = (U\mathfrak{F})^\sigma$ (konjugierte Untergruppen werden auf konjugierte Teilkörper (durch $\mathfrak{F}$) abgebildet)

Beweis:

1. Für $\tau \in G$ gilt:

$$\begin{aligned}
\tau \in (R^\sigma)\mathfrak{G} &\Leftrightarrow (r^\sigma)^\tau = r^\sigma \forall r \in R \\
&\Leftrightarrow r^{\sigma\tau\sigma^{-1}} = r \forall r \in R \\
&\Leftrightarrow \sigma\tau\sigma^{-1} \in R\mathfrak{G} \\
&\Leftrightarrow \tau = \sigma^{-1}(\sigma\tau\sigma^{-1})\sigma \in (R\mathfrak{G})^\sigma
\end{aligned}$$

2. Für $a \in L$ gilt:

$$\begin{aligned}
f \in (U^\sigma)\mathfrak{F} &\Leftrightarrow a^{\sigma^{-1}\tau\sigma} = a \forall \tau \in U \\
&\Leftrightarrow (a^{\sigma^{-1}})^\tau = a^{\sigma^{-1}} \forall \tau \in U \\
&\Leftrightarrow a^{\sigma^{-1}} \in U\mathfrak{F} \\
&\Leftrightarrow a \in (U\mathfrak{F})^\sigma
\end{aligned}$$

3.10.9 Normalteiler und normale Zwischenkörper

Definition: Die Untergruppe N der Gruppe G heißt *Normalteiler von G* (in Zeichen $N \trianglelefteq G$) wenn $N^g = N$ für alle $g \in G$.

Bemerkung: Es reicht zu wissen, dass $N^g \leq N$ für alle $g \in G$, denn es folgt aus $N^{g^{-1}} \leq N$, dass $N = (N^{g^{-1}})^g \leq N^g$.

Satz: Sei (K, L) eine galoissche Körperweiterung, $G = \mathrm{Gal}(L/K)$. Für einen Zwischenkörper R zwischen K und L sind äquivalent:

1. R ist normal über K.
2. $R^\sigma = R$ für alle $\sigma \in G$
3. $R\mathfrak{G} \trianglelefteq G$

Bemerkung: Untergruppen vom Index zwei sind immer Normalteiler.

Beweis:

(2) $\Rightarrow$ (3) Für alle $\sigma \in G$ gilt: $(R\mathfrak{G})^\sigma \overset{(3.10.8)}{=} R^\sigma\mathfrak{G} \overset{(2)}{=} R\mathfrak{G}$. Damit ist $R\mathfrak{G} \trianglelefteq G$.

(3) $\Rightarrow$ (2) Für alle $\sigma \in G$ gilt: $R^\sigma \overset{(3.10.6)}{=} (R\mathfrak{G}\mathfrak{F})^\sigma \overset{(3.10.8)}{=} (R\mathfrak{G})^\sigma\mathfrak{F} \overset{(3)}{=} R\mathfrak{G}\mathfrak{F} \overset{(3.10.6)}{=} R$.

(1) $\Rightarrow$ (2) Wir zeigen $R^\sigma \leq R$ für alle $\sigma \in G$. Sei $\alpha \in R \setminus K$ (für $\alpha \in K$ ist $\alpha^\sigma = \alpha \in R$) und p_α das Minimalpolynom aus $K[x]$. Da $p_\alpha(\alpha) = 0$, so ist nach Definition (2.7.5) $p_\alpha = (x - \alpha_i) \ldots (x - \alpha_r)$ mit $\alpha_i \in R$. Nach (2.7.3) ist α_σ eine Nullstelle von $p_\alpha^{\bar{\sigma}} = p_\alpha$. Also $\alpha^\sigma = \alpha_i \in R$ (für ein i), also $\alpha^\sigma \in R$.

(2) $\Rightarrow$ (1) Verifiziere Definition (2.7.5). Es gilt $[R : K] < \infty$, da (K, L) galoissch. Sei $g \in K[x]$ (o.B.d.A. mit höchstem Koeffizient 1) irreduzibel und $\alpha \in R$ mit $g(\alpha) = 0$. Also $g = p_\alpha$. Da L normal über K, ist $g = (x - \alpha_1) \ldots (x - \alpha_r)$ mit $\alpha_i \in L$. Nach (2.4.6) und Korollar (2.7.9) existiert für jedes i ein $\sigma \in \mathrm{Gal}(L/K)$ mit $\alpha^\sigma = \alpha_i$. Da $R^\sigma = R$, folgt: $\alpha_i = \alpha^\sigma \in R$, also g zerfällt über R.

3.10.10 Faktorgruppen und Homomorphiesatz

Sei G eine Gruppe, $N \leq G$ und $X, Y, Z \subseteq G$.

Definition: $XY := \{xy \mid x \in X, y \in Y\}$, *Komplexmultiplikation*. Offenbar ist $(XY)Z = X(YZ)$. Falls $X = \{g\}$, so schreiben wir $NX = N\{g\} = Ng$.

Lemma: Folgende Eigenschaften der Untergruppe N von G sind äquivalent:

1. $N \trianglelefteq G$
2. $gN = Ng$ für alle $g \in G$.
3. $G/N := \{Ng \mid g \in G\}$ bildet mit der Verknüpfung $(Ng) \circ (Nh) = (Ng)(Nh)$ eine Gruppe.

Beweis:

(1)⇔(2) trivial:

$$N = N^g = g^{-1}Ng \Leftrightarrow gN = Ng$$

(2)⇒(3) $\circ$ ist wohldefiniert, da

$$(Ng)(Nh) = NgNh = NNgh = Ngh$$

- Assoziativität trivial
- Einselement ist N, denn

$$(Ng) \circ N = NgN = NNg = Ng$$

genauso mit Multiplikation von Links.

- Das Inverse zu Ng ist Ng^{-1}

$$(Ng) \circ (Ng^{-1}) = NgNg^{-1} = Ngg^{-1}N = N$$

und genauso

$$(Ng^{-1}) \circ (Ng) = N$$

(3)⇒(1) Ist $(G/N, \circ)$ Gruppe, so muß $(Ng) \circ N$ eine Rechtsrestklasse sein, die offenbar $1 \cdot g \cdot 1 = g$ enthält, also muss sie gleich Ng sein. Somit $NgN = Ng$ und es folgt $gN = 1 \cdot gN \leq Ng$, also $N \leq g^{-1}Ng = N^g$ für alle $g \in G$, also $N^g = N$ für alle $g \in G$.

Definition: Ist $N \trianglelefteq G$, so heißt $(G/N, \circ)$ *die Faktorgruppe* von G nach N, es gilt $(Ng) \circ (Nh) = Ngh$ für alle $g, h \in G$.

HOMOMORPHIESATZ: Seien G und H Gruppen.

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

2. Ist $\sigma : G \to H$ ein Homomorphismus, so ist $N := \operatorname{Kern} \sigma = \{g \in G \mid g^\sigma = 1\} \trianglelefteq G$ und $\sigma = \rho \circ \tau$ mit dem natürlichen Homomorphismus $\rho : G \to G/N$ und dem Monomorphismus $\tau : G/N \to H; Ng \mapsto g^\sigma$. Insbesondere ist $G^\sigma \simeq G/\operatorname{Kern} \sigma$.

BEWEIS:

1. ρ ist offenbar wohldefiniert und surjektiv;
$$(gh)^\rho = Ngh = (Ng) \circ (Nh) = g^\rho \circ g^\rho$$

2. Wie immer sind Bilder und vollständige Urbilder von Untergruppen wieder Untergruppen. Für $x \in \operatorname{Kern} \sigma; g \in G$ gilt
$$(g^{-1}xg)^\sigma \overset{\sigma \text{ Hom.}}{=} (g^{-1})^\sigma x^\sigma g^\sigma \overset{x \in \operatorname{Kern} \sigma}{=} (g^\sigma)^{-1} g^\sigma = 1$$
also $g^{-1}xg \in \operatorname{Kern} \sigma$, d.h. $(\operatorname{Kern} \sigma)^g \leq \operatorname{Kern} \sigma$. Also $\operatorname{Kern} \sigma \trianglelefteq G$. Weiter wörtlich wie in (1.1.8).

3.10.11 Homomorphismus in Galois-Gruppen

SATZ: Sei (K, L) galoissch, $K \leq R \leq L$. Ist R normal über K, so ist $\operatorname{Gal}(R/K) \simeq \operatorname{Gal}(L/K)/R\mathfrak{G}$.

BEMERKUNG: Bisher hatten wir:
$$|G : R\mathfrak{G}| \overset{(3.10.6)}{=} [R : K] \overset{(3.10.5)}{=} |\operatorname{Gal}(R/K)|$$

BEWEIS: Für $\sigma \in G = \operatorname{Gal}(L/K)$ ist $\sigma|_R : R \to R$ ein Isomorphismus über K, d.h. $\sigma|_R \in \operatorname{Gal}(R/K)$. Sei also $\varphi : G \to \operatorname{Gal}(R/K); \sigma \mapsto \sigma|_R$. Für $\sigma, \tau \in G$ gilt
$$(\sigma\tau)^\varphi = (\sigma\tau)|_R = \sigma|_R \cdot \tau|_R = \sigma^\varphi \cdot \tau^\varphi$$
Nach Satz (2.7.8) ist φ surjektiv. Es gilt: $\operatorname{Kern} \varphi = \{\sigma \in G \mid \sigma|_R = 1\} = R\mathfrak{G}$. Homomorphiesatz sagt: $\operatorname{Gal}(R/K) = G^\varphi \simeq G/\operatorname{Kern} \varphi = G/R\mathfrak{G}$.

3.11 der „Fundamentalsatz der Algebra“

3.11.1 der „Fundamentalsatz der Algebra“

SATZ: Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschloßen.

BEWEISE stammen von GAUSS (1799, 1816, 1816, 1849)[32]

3.11.2 Satz von SYLOW

Sei G eine Gruppe. Frage: Für welche Teiler von $|G|$ gibt es Untergruppen von G mit dieser Ordnung?

BEISPIELE:

1. G zyklisch der Ordnung n, dann ex. zu jedem Teiler d von n genau eine Untergruppe mit dieser Ordnung.
2. In $G = S_3, |G| = 6$ existieren Untergruppen zu allen Teilern.
3. Diedergruppe der Ordnung 8 hat alle Untergruppen.
4. (a) $G = S_4, |G| = 24$ hat alle Untergruppen.
   (b) $G = A_4$, die Gruppe der geraden Permutationen, $|G| = 12$, Die Untergruppe der Ordnung 6 ist nicht vorhanden.
5. Falls $n \geq 5, 2 < m < n$, so hat $G = S_n$ keine Untergruppe vom Index m.

SATZ (1872) von SYLOW (1832-1918): Ist G eine endliche Gruppe und p^n eine Primzahlpotenz, die die Ordnung von G teilt, so besitzt G eine Untergruppe der Ordnung p^n.

3.11.3 Beweis des „Fundamentalsatzes der Algebra“

(1) Zu $0 \leq a \in \mathbb{R}$ existiert $b \in \mathbb{R}$ mit $b^2 = a$.

(2) Jedes Polynom ungeraden Grades aus $\mathbb{R}[x]$ besitzt eine reelle Nullstelle.

(3) Sei $\mathbb{C} = \mathbb{R}(i)$ mit i Nullstelle von $x^2 + 1$. Zu jedem $a + bi \in \mathbb{C}$ existiert $u + iv \in \mathbb{C}$ mit $(u + iv)^2 = (a + bi)$.

[32] Buch mit historischen Hintergrundinformationen: Ebbinghaus et. al. „Zahlen“, Springer.

Beweis: Offenbar existiert $\sqrt{a^2+b^2} \geq |a|$, somit ist $\pm a + \sqrt{a^2+b^2} \geq 0 \in \mathbb{R}$, somit existieren

$$u = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \text{ und } v = \varepsilon\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

mit $\varepsilon = \operatorname{sgn} b \in \{+1,-1\}$. Dann gilt

$$\begin{aligned}
(u+iv)^2 &= u^2 - v^2 + 2iuv \\
&= \frac{a+\sqrt{a^2+b^2}+a-\sqrt{a^2+b^2}}{2} \\
&\quad +2i\varepsilon\frac{\sqrt{(a+\sqrt{a^2+b^2})(-a+\sqrt{a^2+b^2})}}{2} \\
&= a + i\varepsilon\sqrt{a^2+b^2-a^2} = a + i\varepsilon|b| = a + ib
\end{aligned}$$

(4) $\mathbb{C}$ besitzt keine Körpererweiterung vom Grad 2.

Beweis: Angenommen $[L:\mathbb{C}] = 2$; sei $\alpha \in L \setminus \mathbb{C}$ und $p_\alpha \in \mathbb{C}[x]$ das definierende Polynom. Dann folgt mit (2.5.1): $\operatorname{grad} p_\alpha = [\mathbb{C}(\alpha):\mathbb{C}] = [L:\mathbb{C}] = 2$, also $p_\alpha = x^2 + cx + d$ mit $c, d \in \mathbb{C}$. Nach (3) existiert $e \in \mathbb{C}$ mit $e^2 = \frac{c^4}{4} - d$. Dann gilt:

$$\begin{aligned}
\left(x - \left(-\frac{c}{2}+e\right)\right)\left(x - \left(-\frac{c}{2}-e\right)\right) &= \left(x + \left(\frac{c}{2}-e\right)\right)\left(x + \left(\frac{c}{2}+e\right)\right) \\
&= x^2 + cx + \frac{c^2}{4} - e^2 \\
&= x^2 + cx + d = p_\alpha
\end{aligned}$$

(5) $\mathbb{C}$ hat keine echte algebraische Erweiterung.

Beweis: Angenommen es existiert eine echte algebraische Erweiterung L von $\mathbb{C}$; sei $\alpha \in L \setminus \mathbb{C}$. Dann ist $\mathbb{C}(\alpha)$ endliche Erweiterung von $\mathbb{C}$ (nach (2.5.1)), also über $\mathbb{R}$ (nach (2.5.3)). Insbesondere ist α algebraisch über $\mathbb{R}$. Ist also $p \in \mathbb{R}[x]$ das definierende Polynom von α über $\mathbb{R}$ und $q = x^2+1$, so ist $\mathbb{R} \leq \mathbb{C}(\alpha) = \mathbb{R}(i,\alpha) \leq \mathbb{R}(p \cdot q) =: L$ und L ist galoissch über $\mathbb{R}$. Sei $G = \operatorname{Gal}(L/\mathbb{R})$ und $|G| = 2^n \cdot k$ mit $n \geq 0$ und k ungerade. Nach Sylow existiert $S \leq G$ mit $|S| = 2^n$, nach (3.10.6)(e') ist $[S\mathfrak{F}:\mathbb{R}] = |G:S| = k$ ungerade. Für $\beta \in S\mathfrak{F}$ ist dann $p_\beta \in \mathbb{R}[x]$ irreduzibel und $\operatorname{grad} p_\beta = [\mathbb{R}(\beta):\mathbb{R}]$, also gilt mit (2.5.3): $\operatorname{grad} p_\beta \mid [S\mathfrak{F}:\mathbb{R}] = k$ ungerade. Nach (2) besitzt p_β eine Nullstelle $d \in \mathbb{R}$, also $p_\beta = x - d$ (da irreduzibel), also $\beta = d \in \mathbb{R}$. Somit ist $S\mathfrak{F} = \mathbb{R}$, somit $S = S\mathfrak{F}\mathfrak{G} = \mathbb{R}\mathfrak{G} = G$, d.h. $|G| = 2^n$.

Nach (3.10.6)(f') ist $|G : \mathbb{C}\mathfrak{G}| = [\mathbb{C} : \mathbb{R}] = 2$, also $|\mathbb{C}\mathfrak{G}| = 2^{n-1}$. Nach Sylow existiert Untergruppe U von $\mathbb{C}\mathfrak{G}$ mit $|U| = 2^{n-2}$. Nach (3.10.6)(e) ist $[U\mathfrak{F} : \mathbb{C}] = |\mathbb{C}\mathfrak{G} : U\mathfrak{F}\mathfrak{G}| = |\mathbb{C}\mathfrak{G} : U| = 2$. Dies wäre also eine Körpererweiterung vom Grad 2, Widerspruch zu (4).

3.11.4 Algebraische Erweiterung der reellen Zahlen

SATZ: $\mathbb{C}$ ist bis auf Isomorphie über $\mathbb{R}$ die einzige echte algebraische Erweiterung von $\mathbb{R}$.

BEWEIS: Ist $\mathbb{R} < L$ mit L algebraisch über $\mathbb{R}$, so ist $\mathbb{R} < L(x^2+1)$ nach (2.5.6) algebraisch über $\mathbb{R}$, also auch über $\mathbb{R}(i) = \mathbb{C}$, mit (3.11.1) ist dann $L(x^2+1) = \mathbb{C}$.

3.11.5 Irreduzible reelle Polynome

SATZ: Jedes irreduzible Polynom $f \in \mathbb{R}[x]$ hat Grad 1 oder 2.

BEWEIS: Sei $R(\alpha)$ mit $f(\alpha) = 0$, dann ist $p_\alpha = [\mathbb{R}(\alpha) : \mathbb{R}]$.

3.12 Einheitswurzeln und Kreisteilungskörper

3.12.1 Einheitswurzeln

Sei K Körper, $n \in \mathbb{N}$.

DEFINITION: Ein Element ε eine Erweiterungskörpers L von K heißt n-te Einheitswurzel (Ew) über K, wenn ε Nullstelle des Polynoms $x^n - 1$ ist.

BEMERKUNG: Ist $\operatorname{char} K = p > 0$ und $n = p \cdot m$, so gilt $x^n - 1 = x^{pm} - 1 = (x^m - 1)^p$. Somit werden wir immer voraussetzen, daß $\operatorname{char} K \nmid n$ ist.

SATZ: Sei K Körper, $n \in \mathbb{N}$ und $\operatorname{char} K \nmid n$. Sei $L = K(x^n - 1)$ ein Zerfällungskörper von $x^n - 1$ über K und

$$E_n = E_n(K) = \{\varepsilon \in L \mid \varepsilon^n - 1 = 0\}$$

Dann ist E_n eine zyklische Untergruppe der Ordnung n von L^*.

BEWEIS: $(x^n - 1)' = nx^{n-1}$ hat 0 als einzige Nullstelle. Nach Satz (2.8.6) hat also $x^n - 1$ keine mehrfache Nullstelle. Somit ist $|E_n| = n$. Mit $\varepsilon_1, \varepsilon_2 \in E_n$ ist $(\varepsilon_1\varepsilon_2^{-1})^n = \varepsilon_1^n \cdot (\varepsilon_2^n)^{-1} = 1$, also $\varepsilon_1\varepsilon_2^{-1} \in E_n$. Somit ist E_n Untergruppe der Ordnung n von L^*. Nach Satz (2.8.4) ist E_n zyklisch.

3.12.2 Primitive Einheitswurzeln

Sei $n \in N$, K Körper mit $\operatorname{char} K \nmid n$ und E_n die Gruppe der n-ten Einheitswurzeln in $L = K(x^n - 1)$.

DEFINITIONEN:

(a) ε heißt primitive n-te Einheitswurzel genau dann, wenn $E_n = \langle \varepsilon \rangle$.

(b) $\varphi(n)$ sei die Anzahl der primitiven n-ten Einheitswurzeln über K.

Warum betrachten wir Einheitswurzeln?

- Konstruktion von ε liefert Konstruktion des regulären n-Ecks (wenn ε primitive n-te Einheitswurzel)
- $x^n - a$, α Nullstelle, ε n-te Einheitswurzel, dann ist $(\varepsilon\alpha)^n = \varepsilon^n \alpha^n = \alpha^n = a$

BEISPIELE:

1. Für $K = \mathbb{C}$ ist $\varepsilon^n = 1 \Rightarrow |\varepsilon|^n = 1 \Rightarrow |\varepsilon| = 1$, liegen also alle auf dem Einheitskreis; die n-ten Einheitswurzeln sind $\varepsilon = e^{\frac{2\pi i}{n} \cdot k}$.

LEMMA: Ist $1 \neq \varepsilon \in E_n$, so ist

$$1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{n-1} = \frac{\varepsilon^n - 1}{\varepsilon - 1} = 0$$

wobei $1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{n-1}$ nach Satz (2.8.1) die Summe der Elemente aus E_n, falls $\{\varepsilon\} = E_n$, insbesondere für ε primitive n-te Einheitswurzel ist die Summe aller n-ten Einheitswurzeln gleich 0.

3.12.3 Die Eulersche Phi-Funktion

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

DEFINITION: Sei $\varphi(n)$ die Anzahl der primitiven n-ten Einheitswurzeln.

LEMMA:

$$\begin{aligned}
\varphi(n) &= \text{Anzahl der primitiven } n\text{-ten Einheitswurzeln} \\
&= \text{Anzahl der Erzeugenden einer zyklischen Gruppe der Ordnung } n \\
&= \text{Anzahl der zu } n \text{ teilerfremden Zahlen zwischen 1 und } n \\
&= |E(\mathbb{Z}/n\mathbb{Z})| \text{ Ordnung der Einheitegruppe von } \mathbb{Z}/n\mathbb{Z}
\end{aligned}$$

Beweis: Die ersten Gleichheit folgt aus (3.12.1). $G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ falls G zyklisch der Ordnung n; $\mathbb{Z}/n\mathbb{Z} = \{1{+}n\mathbb{Z}, \ldots, (n-1){+}n\mathbb{Z}\}$.

Wir zeigen: *Behauptung:* Für $k \in \{0, \ldots, n-1\}$ sind äquivalent:

(a) $(k, n) = 1$, d.h. es existieren $c, d \in \mathbb{Z}$ mit $1 = kc + nd$

(b) $\langle g^k \rangle = \langle g \rangle$

(c) $k{+}n\mathbb{Z}$ ist Einheit in $\mathbb{Z}/n\mathbb{Z}$

Beweis:

(a) $\Rightarrow$ (b) $g^{kc} = g^{1-nd} = g \cdot (g^{nd})^{-1} = g \in \langle g^k \rangle \Rightarrow \langle g^k \rangle = \langle g \rangle$

(b) $\Rightarrow$ (c) $g \in \langle g^k \rangle \Rightarrow \exists c \in \mathbb{Z}$ mit $g = g^{kc} \Rightarrow g^{1-kc} = 1 \Rightarrow n \mid 1 - kc$, also existiert d mit $nd = 1 - kc$

(c) $\Rightarrow$ (a) $(k{+}n\mathbb{Z})(c{+}n\mathbb{Z}) = hc + n\mathbb{Z} = 1 + n\mathbb{Z}$

Satz: Seien $r, s, t \in \mathbb{N}$. Dann gilt:

(a) $(r, s) = 1 \Rightarrow \varphi(rs) = \varphi(r)\varphi(s)$ (φ ist *multiplikativ*)

(b) $\varphi(p^t) = p^t - p^{t-1} = p^t(1 - \frac{1}{p})$

(c) $\varphi(n) = n \cdot \prod_{p \in \mathbb{P}, p|n} (1 - \frac{1}{p})$

Beweis:

(a) Sei $A = \langle a \rangle$ zyklisch der Ordnung rs, $B = \langle a^s \rangle$ die Untergruppe der Ordnung r von A und $C = \langle a^r \rangle$ die der Ordnung s. Seien A^*, B^*, C^* jeweils die Mengen der Erzeugenden von A, B und C.

$$\sigma : B^* \times C^* \longrightarrow A^* \text{ mit } \sigma : (b, c) \mapsto bc$$

Nach Lemma (2.8.3) wohldefiniert (d.h. $bc \in A^*$, da $o(bc) = rs$), zudem surjektiv: $a_1 \in A^*$, $1 = rc + sd$, dann ist $a_1 = a_1^{rc+sd} = (a_1^s)^d (a_1^r)^c$ mit $(a_1^r)^c \in C^*$ und $(a_1^s)^d \in B^*$. Die Abbildung ist auch injektiv: Aus $b_1 c_1 = b_2 c_2$ folgt $b_2^{-1} b_1 = c_2 c_1^{-1} \in B \cap C = 1$ (Lagrange, da $|B| = r$, $|C| = s$ teilerfremd) Also σ bijektiv.

(b) Aufgabe 34: $a \in G$ erzeugt G genau dann, wenn a nicht in der Untergruppe der Ordnung p^{t-1} liegt, das sind $p^t - p^{t-1}$ Elemente

(c) Aus $n = p_1^{t_1} \cdot \ldots \cdot p_r^{t_r}$ folgt

$$\varphi(n) = \varphi(p_1^{t_1}) \cdot \ldots \cdot \varphi(p_r^{t_r}) = \prod_{i=1}^{r} p_i^{t_i}(1 - \frac{1}{p_i}) = n \cdot \prod_{i=1}^{r}(1 - \frac{1}{p_i})$$

BEISPIEL:

(2) $\varphi(12) = 12 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3}$

3.12.4 Kreisteilungspolynome

VORAUSSETZUNG: wie in (3.12.2) und $L = K(x^n - 1)$.

DEFINITION: Das *n-te Kreisteilungspolynom* sei

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

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

Für $P \leq K$ Primkörper und $\bar{L} = P(x^n - 1) \leq L$ folgt

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

LEMMA: Es gilt

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

BEWEIS: Auf beiden Seiten steht $\prod_{\varepsilon \in E_n}(x - \varepsilon)$, rechts nach der Ordnung der ε geordnet.

BEISPIELE:

(a) $\phi_1 = x - 1$

(b) p Primzahl, dann ist $x^p - 1 = \phi_1\phi_p = (x - 1)\phi_p$, es folgt $\phi_p = \frac{x^p-1}{x-1} = 1 + x + \ldots + x^{p-1}$

(c) Für $n = 4$ ist $x^4 - 1 = \phi_1\phi_2\phi_4 = (x-1)(x+1)\phi_4$, es folgt $\phi_4 = \frac{x^4-1}{x^2-1} = x^2 + 1$

(d) Für $n = 6$ ist $x^6 - 1 = \phi_1\phi_2\phi_3\phi_6 = (x^3-1)\phi_2\phi_6$, es folgt $\phi_6 = \frac{x^6-1}{(x^3-1)(x+1)} = x^2 - x + 1$

(e) Für $n = 12$ ist $x^{12} - 1 = \phi_1\phi_2\phi_3\phi_4\phi_6\phi_{12} = (x^6 - 1)\phi_4\phi_{12}$, es folgt $\phi_{12} = \frac{x^{12}-1}{(x^6-1)(x^2+1)} = x^4 - x^2 + 1$

SATZ: Die Koeffizienten der Kreisteilungspolynome $\phi_{n,K}$ liegen im Primkörper; ist $\operatorname{char} K = 0$, so ist $\phi_n \in \mathbb{Z}[x]$ mit höchstem Koeffizienten 1.

BEWEIS:

- Durch vollständige Induktion: Sei P der Primkörper in K. Für $n = 1$ ist $\phi_1 = x - 1$, Aussage ist also korrekt. Sei nun $n \in \mathbb{N}$ und die Aussage richtig für kleinere $m \in \mathbb{N}$. Das Lemma besagt, daß

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

  mit $f \in P[x]$. Nach Division mit Rest in $P[x]$ existieren $q, r \in P[x]$ mit $x^n - 1 = qf + r$ und $\operatorname{grad} r < \operatorname{grad} f$ oder $r = 0$.

  In $L[x]$ gilt also $q \cdot f + r = x^n - 1 = \phi_{n,K} \cdot f$, also $r = f(\phi_{n,K} - q)$. Aus Gradgründen folgt $r = 0$, und da $f \neq 0$ ist auch $\phi_{n,K} - q = 0$, also $\phi_{n,K} = q \in P[x]$.

- Für $\operatorname{char} K = 0$ ebenfalls Induktion: Für $n = 1$ ist $\phi_1 = x - 1$, Aussage korrekt. Sei die Aussage also richtig für $m < n$, dann ist $x^n - 1 = \phi_n \cdot f$ mit $f \in \mathbb{Z}[x]$ und höchstem Koeffizient 1 (wie eben). Also ist f primitiv. Nach Lemma (1.3.3)(a) ist $\phi_n = c \cdot g$ mit $c \in \mathbb{Q}, g \in \mathbb{Z}[x]$ primitiv (da $\phi_n \in \mathbb{Q}[x]$), also $x^n - 1 = c \cdot g \cdot f$ und nach Satz (1.3.3) ist $g \cdot f$ primitiv. Nach Lemma (1.3.3)(c) ist $c \in \mathbb{Z}$. Somit ist $\phi_n \in \mathbb{Z}[x]$; da f und $x^n - 1$ höchsten Koeffizienten 1 haben, hat auch ϕ_n höchsten Koeffizienten 1.

KOROLLAR: Sei p Primzahl mit $p \nmid n$. Ist $\sigma_p := \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = GF(p)$ der natürliche Homomorphismus und $\bar{\sigma}_p$ die Fortsetzung auf $\mathbb{Z}[x]$, so gilt $\phi_{n,p} = \phi^{\bar{\sigma}_p}$.

BEWEIS: Durch Induktion nach n: Für $n = 1$ ist $\phi_1 = x - 1$, Aussage korrekt. Sei $n \in \mathbb{N}$ und die Aussage richtig für alle $d \mid n$ mit $d < n$ (die werden von p

nicht geteilt). Dann gilt für $x^n - 1 \in GF(p)[x]$:

$$\begin{aligned} x^n - 1 &= (x^n-1)^{\bar\sigma_p} = \left(\phi_n \cdot \left(\prod_{\substack{d|n\\d<n}} \phi_d\right)\right)^{\bar\sigma_p} \\ &= \phi_n^{\bar\sigma_p} \cdot \prod_{\substack{d|n\\d<n}} \phi_d^{\bar\sigma_p} \overset{\text{IV}}{=} \phi_n^{\bar\sigma_p} \cdot \prod_{\substack{d|n\\d<n}} \phi_{d,p} \\ x^n - 1 &= \prod_{d|n} \phi_{d,p} = \phi_{n,p} \cdot \prod_{\substack{d|n\\d<n}} \phi_{d,p} \end{aligned}$$

Wegen der Nullteilerfreiheit ist $\phi_{n,p} = \phi_n^{\bar\sigma_p}$.

3.12.5 irreduzible Kreisteilungspolynome

SATZ (GAUSS): Alle Kreisteilungspolynome ϕ_n sind irreduzibel.

BEWEIS: Nach Satz (1.3.4) ist ein primitives Polynom ϕ_n aus $\mathbb{Z}[x]$ genau dann über $\mathbb{Q}$ irreduzibel, wenn es über $\mathbb{Z}$ irreduzibel ist. Zu zeigen also: ϕ_n über $\mathbb{Z}[x]$ irreduzibel. Angenommen, $\phi_n = h \cdot k$ mit $h, k \in \mathbb{Z}[x]$ und $\operatorname{grad} h \geq 1$ und h irreduzibel in $\mathbb{Z}[x]$. Will zeigen: Für $h = \pm\phi_n$ ist

$$\varepsilon \in \mathbb{Q}(x^n-1) \text{ mit } h(\varepsilon) = 0 \text{ und } p \in P \text{ mit } p \nmid n \Longrightarrow h(\varepsilon^p) = 0 \qquad (\star)$$

Dann sind wir fertig: Da $\phi_n = h \cdot k$, ist ε eine primitive n-te Einheitswurzel. Ist γ irgendeine primitive n-te Einheitswurzel, so ist $\langle\gamma\rangle = \langle\varepsilon\rangle$. Nach Lemma (3.12.3) existiert $k \in \{0, \ldots, n-1\}$ mit $\gamma = \varepsilon^k$ und $(k, n) = 1$. Sei $k = p_1 \cdot \ldots \cdot p_r$, so liefert $(\star)$ angewandt auf ε, p_1, daß $h(\varepsilon^{p_1}) = 0$. Wiederum $(\star)$ angewandt auf ε^{p_1}, p_2 ist $h(\varepsilon^{p_1 p_2}) = 0$. Mit trivialer Induktion ist $h(\varepsilon^{p_1 \cdot \ldots \cdot p_r}) = 0$, also $h(\gamma) = 0$. Somit hat h alle primitiven n-ten Einheitswurzeln als Nullstelle, d.h. aus $\phi_r \mid h$ folgt: $h = \pm\phi_n$, d.h. ϕ_n ist irreduzibel.

Zum Beweis von $(\star)$: Nach Lemma (3.12.3) ist mit ε auch ε^p eine primitive n-te Einheitswurzel. Angenommen, $h(\varepsilon^p) \neq 0$. Da $\phi_n(\varepsilon^p) = 0$, folgt $k(\varepsilon^p) = 0$ und somit ist ε eine Nullstelle von $k_1 := k(x^p)$ (denn $k_1(\varepsilon) = k(\varepsilon^p) = 0$). Da h irreduzibel in $\mathbb{Q}[x]$, ist h das Minimalpolynom von ε. Nach (2.4.4) gilt $h \mid k_1$, d.h.

$$k_1 = h \cdot l \text{ mit } l \in \mathbb{Z}[x] \qquad (1)$$

Dabei ist eigentlich $l \in \mathbb{Q}[x]$, aber es existieren $c \in \mathbb{Q}$ und $l_1 \in \mathbb{Z}[x]$ primitiv mit $l = c \cdot l_1$, also $k_1 = chl_1$, nach Satz (1.3.3) ist hl primitv und dann $c \in \mathbb{Z}$.

Sei wieder (nach Lemma (3.12.4))

$$h \cdot k \cdot f = x^n - 1 = \phi_n \cdot \prod_{\substack{d|n \\ d<n}} \phi_d = \phi_n \cdot f \text{ mit } f \in \mathbb{Z}[x]$$

Sei $\sigma := \bar{\sigma}_p$ aus Korollar (3.12.4). Dann gilt:

$$x^n - 1 = h^\sigma \cdot k^\sigma \cdot f^\sigma \tag{2}$$

$$h^\sigma \cdot l^\sigma \overset{(1)}{=} k_1^\sigma = (k(x^p))^\sigma = k^\sigma(x^p) = (k^\sigma)^p \tag{3}$$

Die letzte Gleichheit gilt, da für $k^\sigma = \sum_{i=0}^{r} a_i x^i$ gilt

$$(k^\sigma)^p = \left(\sum_{i=0}^{r} a_i x^i\right)^p \overset{\text{Aufg8}}{=} \sum_{i=0}^{r} a_i^p (x^p)^i = \sum_{i=0}^{r} a_i (x^p)^i = k^\sigma(x^p)$$

Da h höchsten Koeffizienten ± 1 hat, ist $\operatorname{grad} h^\sigma = \operatorname{grad} h \geq 1$. Somit besitzt h^σ in $GF(p)(h^\sigma)$ eine Nullstelle δ. Da $h^\sigma \cdot l^\sigma \overset{(3)}{=} (k^\sigma)^p$, ist dann δ auch Nullstelle von k^σ. Nach (2) ist dann δ mehrfache Nullstelle von $h^\sigma k^\sigma f^\sigma = x^n - 1$. Wegen $p \nmid n$ hat $x^n - 1$ über $GF(p)$ nach (3.12.1) nur einfache Nullstellen. Widerspruch zur Annahme.

Bemerkung: $\phi_{n,p}$ ist im Allgemeinen nicht irreduzibel:

$$\phi_{7,2} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$$

Es ist $GF(2)(x^7 - 1) = GF(8) = GF(2)(\varepsilon)$ mit $\operatorname{grad} \varepsilon = 3$, das Minimalpolynom von ε kann nur eines der beiden hinteren Faktoren sein. Da es keine mehrfachen Nullstellen gibt, müssen beide Polynome vorkommen

3.12.6 Kreisteilungskörper

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

Definition: $\mathbb{Q}_n := \mathbb{Q}(x^n - 1)$ ist der n-te *Kreisteilungskörper*.

Bemerkung: Es gilt $\mathbb{Q}_n = \mathbb{Q}(\varepsilon) = \mathbb{Q}(\phi_n)$ mit primitiver n-ter Einheitswurzel ε; somit

$$[\mathbb{Q}_n : \mathbb{Q}] = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] \overset{(3.12.5)}{=} \operatorname{grad} \phi_n \overset{(3.12.4)}{=} \varphi(n)$$

Satz: Sei $n \in \mathbb{N}$, K ein Körper mit Charakteristik $K \nmid n$ und $K_n := K(x^n - 1)$. Dann ist K_n galoissch über K und $\operatorname{Gal}(K_n/K)$ isomorph zu einer Untergruppe der Einheitengruppe $E(\mathbb{Z}/n\mathbb{Z})$. Insbesondere ist $\operatorname{Gal}(K_n/K)$ abelsch und somit sind alle Zwischenkörper zwischen K und K_n normal über K.

Beweis: Nach (3.12.1) hat $x^n - 1$ lauter verschiedene Nullstellen, ist also separabel, damit ist K_n galoissch über K. Sei $G = \mathrm{Gal}(K_n/K)$ und $\varepsilon \in K_n$ primitive n-te Einheitswurzel. Für $\sigma \in G$ ist ε^σ wieder eine primitive n-te Einheitswurzel (da $(\varepsilon^k)^\sigma = (\varepsilon^\sigma)^k$ uns somit die multiplikative Ordnung eines Elementes unter Automorphismen erhalten bleibt). Nach Lemma (3.12.3) existiert ein $r \in \{0, \ldots, n-1\}$ mit $\varepsilon^\sigma = \varepsilon^r$ und $(r, n) = 1$. Sei

$$\varphi : G \to E(\mathbb{Z}/n\mathbb{Z}); \sigma \mapsto r + n\mathbb{Z}$$

Da

$$\varepsilon^r = \varepsilon^s \overset{(2.8.1)}{\Leftrightarrow} \varepsilon^{r-s} = 1 \overset{(2.8.3)(3)}{\Leftrightarrow} n \mid r - s \overset{Def.}{\Leftrightarrow} r + n\mathbb{Z} = s + n\mathbb{Z}$$

ist die Abbildung φ wohldefiniert. Für $\sigma_1, \sigma_2 \in G$ und etwa $\varepsilon^{\sigma_1} = \varepsilon^{r_1}, \varepsilon^{\sigma_2} = \varepsilon^{r_2}$ gilt

$$\varepsilon^{\sigma_1\sigma_2} = (\varepsilon^{\sigma_1})^{\sigma_2} = (\varepsilon^{r_1})^{\sigma_2} = (\varepsilon^{\sigma_2})^{r_1} = (\varepsilon^{r_2})^{r_1} = \varepsilon^{r_1 r_2}$$

also

$$(\sigma_1\sigma_2)^\varphi = r_1 r_2 + n\mathbb{Z} = (r_1 + n\mathbb{Z})(r_2 + n\mathbb{Z}) = \sigma_1^\varphi \sigma_2^\varphi$$

Somit ist φ ein Homomorphismus. Es gilt weiter

$$\sigma \in \mathrm{Kern}\,\varphi \Leftrightarrow \sigma^\varphi = 1 + n\mathbb{Z} \Leftrightarrow \varepsilon^\sigma = \varepsilon \Leftrightarrow \sigma = 1$$

d.h. $\mathrm{Kern}\,\varphi = 1$. Mit Homomorphiesatz gilt:

$$G = G/\mathrm{Kern}\,\varphi \simeq \mathrm{Bild}\,\varphi \leq E(\mathbb{Z}/n\mathbb{Z})$$

Da $\mathbb{Z}$ kommutativ, ist $E(\mathbb{Z}/n\mathbb{Z})$ abelsch, also alle Untergruppen von G normal in G. Nach (3.10.6) + (3.10.9) sind alle Zwischenkörper normal.

Korollar:

(a) $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) = \mathrm{Aut}\,\mathbb{Q}_n \simeq E(\mathbb{Z}/n\mathbb{Z})$

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

Beweis:

(a) $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \overset{\simeq}{\leq} E(\mathbb{Z}/n\mathbb{Z})$. Laut Satz

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) &\overset{(3.10.5)}{=} [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) \overset{(3.12.3)}{=} |E(\mathbb{Z}/n\mathbb{Z})| \\ \Rightarrow \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) &\simeq E(\mathbb{Z}/n\mathbb{Z}) \end{aligned}$$

(b) $n = p \Rightarrow \mathbb{Z}/p\mathbb{Z} = GF(p) \Rightarrow E(\mathbb{Z}/p\mathbb{Z}) = GF(p)^*$ zyklisch der Ordnung $p - 1$. [33]

[33] Huppert, S.84, Kurzweil/Stellmacher 44-48

3.12.7 Konstruktion des regulären n-Ecks (mit Zirkel und Lineal)

Sei $n \in \mathbb{N}, n \geq 3$.

SATZ: (Gauß, 1801). Das reguläre n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^r \cdot p_1 \dots p_s$ mit ganzen Zahlen $r, s \geq 0$ und Primzahlen $p_i \neq p_j (i \neq j)$ der Form $p_i = 2^{2^{k_i}} + 1, k_i \geq 0$ (Fermatsche Primzahlen).

LEMMA: Genau dann ist das reguläre n-Eck mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine 2-Potenz ist.

BEWEIS des Lemmas:

Die Konstruktion des regulären n-Ecks mit Zirkel und Lineal ist äquivalent zur Konstruktion des Punktes $\left(\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n}\right)$ aus $\mathfrak{P} = \{(0,0),(1,0)\}$ oder des Punktes $\left(\cos \frac{2\pi}{n}, 0\right)$. Sei $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ (primitive n-te Einheitswurzel). Dann ist

$$\begin{aligned} \varepsilon^{-1} &= \cos \frac{2\pi}{n} - i \sin \frac{2\pi}{n}, \\ \text{da} \quad & \left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}\right)\left(\cos \frac{2\pi}{n} - i \sin \frac{2\pi}{n}\right) = \cos^2 \frac{2\pi}{n} + \sin^2 \frac{2\pi}{n} = 1 \end{aligned}$$

Ferner $\varepsilon + \varepsilon^{-1} = 2 \cos \frac{2\pi}{n}$, also $\mathbb{Q}\left(\cos \frac{2\pi}{n}\right) = \mathbb{Q}(\varepsilon + \varepsilon^{-1})$. Da

$$\varepsilon^2 - (\varepsilon + \varepsilon^{-1})\varepsilon + 1 = \varepsilon^2 - \varepsilon^2 - 1 + 1 = 0$$

ist ε Nullstelle des Polynoms $x^2 - (\varepsilon + \varepsilon^{-1})x + 1 \in \mathbb{Q}\left(\cos \frac{2\pi}{n}\right)[x]$. Somit $\left[\mathbb{Q}(\varepsilon) : \mathbb{Q}\left(\cos \frac{2\pi}{n}\right)\right] \leq 2$, da ε nicht reell, folgt: ist gleich 2. Da $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \varphi(n)$ nach Bemerkung (3.12.6), folgt:

$$\left[\mathbb{Q}\left(\cos \frac{2\pi}{n}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2} \tag{*}$$

Nun können wir das Lemma zeigen:

„$\Rightarrow$“ Sei n-Eck konstruierbar, also $\left(\cos \frac{2\pi}{n}, 0\right)$ konstruierbar (bei geeignetem Koordinatensystem). Dann existieren Körper $L_0 = \mathbb{Q} < L_1 < \ldots < L_k$ mit $[L_i : L_{i-1}] = 2$ und $\frac{\cos 2\pi}{n} \in L_k$. Daraus folgt

$$[L_k : \mathbb{Q}] = 2^k \Rightarrow \left[\mathbb{Q}\left(\cos \frac{2\pi}{n}\right) : \mathbb{Q}\right] = 2^r \text{ für ein } r \in \mathbb{N} \Rightarrow \varphi(n) = 2^{r+1}$$

„⇒“ Sei $\varphi(n)$ eine 2-Potenz, also $\frac{\varphi(n)}{2} = 2^r$. Nach Satz (3.12.6) ist $\mathbb{Q}\left(\cos\frac{2\pi}{n}\right)$ normal über $\mathbb{Q}$ (als Zwischenkörper zwischen $\mathbb{Q}$ und $\mathbb{Q}(\varepsilon)$), also galoissch; sei $G = \mathrm{Gal}\left(\mathbb{Q}\left(\cos\frac{2\pi}{n}\right)/\mathbb{Q}\right)$. Nach (3.10.6) ist $|G| = \left[\mathbb{Q}\left(\cos\frac{2\pi}{n}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2} = 2^r$. Mit Satz von Sylow existiert $U_1 \leq G$ mit $|U_1| = 2^{r-1}$, ferne $U_2 \leq U_1$ mit $|U_2| = 2^{r-2}$, erhalte Kette $G = U_0 > U_1 > \ldots > U_r = 1$ mit $|U_i : U_{i+1}| = 2$ für alle i. Mit (3.10.6) gilt für $L_i = U_i\mathfrak{F}$: $\mathbb{Q} < L_1 < \ldots < L_r = \mathbb{Q}\left(\cos\frac{2\pi}{n}\right)$ und $[L_i : L_{i-1}] = [U_{i-1} : U_i] = 2$, damit ist mit Satz (2.6.7) $\left(\cos\frac{2\pi}{n}, 0\right)$ konstruierbar.

Beweis des Satzes:

Wann ist $\varphi(n)$ eine 2-Potenz?

$$n = p_1^{\alpha_1}\ldots p_r^{\alpha_r} \overset{(3.12.3)}{\Longrightarrow} \varphi(n) = \varphi(p_1^{\alpha_1}))\ldots\varphi(p_r^{\alpha_r})$$

Genau dann ist $\varphi(n)$ eine 2-Potenz, wenn alle $\varphi(p_i^{\alpha_i})$ 2-Potenzen sind.

- $p = 2$: $\varphi(2^\alpha) = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1}$, immer 2-Potenz.
- $p \neq 2$: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$. Dies ist genau dann eine 2-Potenz, wenn $\alpha \leq 1$ und $p = 2^m + 1$. Für ungerades $r > 1$ ist

  $$(a^r + 1) = (a+1)(a^{r-1} - a^{r-2} + a^{r-3} - \ldots - a + 1) \text{ für } a \in \mathbb{Z}$$

  Ist m keine 2-Potenz, so $m = 2^k v$ mit $k \geq 0$, v ungerade und $v > 1$ und somit

  $$2^m + 1 = \left(2^{2^k}\right)^v + 1 = \left(2^{2^k} + 1\right)(\ldots) \text{ mit } a = 2^{2^k}$$

  p Primzahl impliziert $v = 1$, d.h. $m = 2^k$.

Fermatsche Primzahlen sind:

k	0	1	2	3	4
$2^{2^k}+1$	3	5	17	257	65537

Vermutung von Fermat (1640): alle Zahlen dieser Form sind Primzahlen. Euler zeigte aber im Jahre 1732: $2^{32} + 1 = 641 \cdot 6700417$. Die Idee:

$$\begin{aligned} 641 &= 2^4 + 5^4 = 5 \cdot 2^7 + 1 \\ 2^{32} &= 16 \cdot 2^{28} = (641 - 5^4)2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 = 641 \cdot m - 1 \end{aligned}$$

Es sind bis jetzt auch keine weiteren Primzahlen dieser Form bekannt und man vermutet inzwischen, daß es auch keine weiteren gibt.[34]

[34]Konstruktionen des 17-Ecks: Stewart, S.189, des 257-Ecks: Richelot, Crelle Journale Band 9, (1832), in Latein in der Bibliothek vorhanden!

Index