Skript zur Vorlesung

Algebra mit Elementen der Galoistheorie

(Sommersemester 2019)

Dieses Geheft enthält in kompakter Form die wesentlichen Inhalte, wie sie in der Vorlesung ,,Algebra mit Elementen der Galoistheorie" vorgestellt werden.

Es ist zum Gebrauch neben der Vorlesung gedacht und erhebt nicht den Anspruch, ,,in sich selbst verständlich" oder vollständig zu sein.

S. Hilger

Inhaltsverzeichnis

1 Ringe

1.1 Ringe und Ringhomomorphismen

1.1.1 Definition: Ring

(i) Eine Menge R, zusammen mit zwei Verknüpfungen

$$+ : R \times R \to R \qquad \text{und} \qquad \cdot : R \times R \to R,$$

heißt ein *Ring*, wenn die folgenden Eigenschaften erfüllt sind:

(A) $(R, +)$ ist eine abelsche Gruppe, das neutrale Element wird mit $0 = 0_R$ bezeichnet.

(B) Die Verknüpfung $\cdot$ ist assoziativ, d.h. es ist

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad \forall\ x, y, z \in R,$$

(C) Es gelten die beiden Distributivgesetze: Für beliebige x, y, z ist (Punkt-vor-Strich-Konvention)

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z \\ (y + z) \cdot x &= y \cdot x + z \cdot x. \end{aligned}$$

(ii) Ist außerdem

$$x \cdot y = y \cdot x \qquad \text{für alle } x, y \in R,$$

so heißt R ein *kommutativer Ring*.

(iii) Enthält R ein bzgl. der Multiplikation neutrales Element $1 = 1_R \in R$, d.h.

$$1 \cdot x = x \cdot 1 = x \qquad \forall\ x \in R,$$

so heißt der Ring *unitär*.

1.1.2 Vereinbarung

Wir werden zunächst nur unitäre kommutative Ringe betrachten, bei denen $1 \neq 0$ ist. Meistens werden wir nochmal durch das Kürzel uk darauf hinweisen.

1.1.3 Folgerungen

Für $x, y \in R$ ist

$$\begin{aligned} 0 \cdot x &= 0 \\ (-x) \cdot y &= -(x \cdot y) \\ (-x) \cdot (-y) &= x \cdot y. \end{aligned}$$

1.1.4 Beweis

Für $x, y \in R$ ist

$$\begin{aligned} 0 \cdot x &= (0+0) \cdot x = 0 \cdot x + 0 \cdot x \quad \Longrightarrow \quad 0 \cdot x = 0 \\ (-x) \cdot y + x \cdot y &= [(-x) + x] \cdot y = 0 \cdot y = 0 \quad \Longrightarrow \quad (-x) \cdot y = -(x \cdot y) \\ (-x) \cdot (-y) &= -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y. \end{aligned}$$

1.1.5 Beispiele von uk Ringen

1. Enthält $R = \{a\}$ genau ein Element, so kann man darauf eine (reichlich triviale) Ringstruktur durch $a + a = a$ und $a \cdot a = a$ definieren. Das Null- und Einselement ist a. Man spricht dann auch vom Nullring und schreibt statt a gleich 0.

2. Die klassischen Zahlenmengen mit den klassischen Verknüpfungen

   $$(\mathbb{Z}, +, \cdot), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot), \quad (\mathbb{C}, +, \cdot)$$

   sind uk Ringe.

3. Der Ring $\mathbb{R}[x]$ der Polynome mit reellen Koeffizienten ist ein uk Ring.

4. Es sei $n \in \mathbb{N}, n \geq 1$, fixiert. Die abelsche endliche Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ wird durch die beiden Abbildungen

   $$+ : \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to \quad \mathbb{Z}/n\mathbb{Z} \\ (x + n\mathbb{Z}, y + n\mathbb{Z}) & \mapsto \quad (x+y) + n\mathbb{Z} \end{cases} \qquad \cdot : \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to \quad \mathbb{Z}/n\mathbb{Z} \\ (x + n\mathbb{Z}, y + n\mathbb{Z}) & \mapsto \quad (x \cdot y) + n\mathbb{Z} \end{cases}$$

   zu einem uk Ring.

5. Sind R und S uk Ringe, so ist $R \times S$ mit den komponentenweisen Verknüpfungen ein uk Ring, der so genannte *Produktring*.

6. Sind R ein uk Ring und X eine beliebige Menge, so ist die Menge aller Funktionen $X \to R$ (unter komponentenweisen Verknüpfungen) ein uk Ring.

7. Ist X ein (offenes) Intervall, so sind die Mengen ...

   $\mathcal{C}^0(X, \mathbb{R})$ der auf X stetigen Funktionen ...

   $\mathcal{C}^1(X, \mathbb{R})$ der auf X stetig differenzierbaren Funktionen ...

   $\mathcal{C}^\infty(X, \mathbb{R})$ der auf X unendlich oft stetig differenzierbaren Funktionen

   $\mathcal{C}^\omega(X, \mathbb{R})$ der auf X analytischen Funktionen

   mit den stellenweisen Verknüpfungen uk Ringe.

8. Ist Ω ein Gebiet, so ist die Menge $\mathcal{H}(\Omega)$ der auf Ω holomorphen Funktionen ein uk Ring.

9. Es sei $d \in \mathbb{Z}$ quadratfrei, d.h. in der Primfaktorzerlegung von d tritt kein Primfaktor mehr als einmal auf. $\sqrt{d} \in \mathbb{C}$ sei eine Quadratwurzel von d. Dann bilden die Teilmengen von $\mathbb{C}$

$$\begin{aligned} \mathbb{Z} + \mathbb{Z}\sqrt{d} &= \{z \in \mathbb{C} \,|\, \exists\, u, v \in \mathbb{Z} \text{ mit } z = u + v\sqrt{d}\} \\ \mathbb{Q} + \mathbb{Q}\sqrt{d} &= \{z \in \mathbb{C} \,|\, \exists\, u, v \in \mathbb{Q} \text{ mit } z = u + v\sqrt{d}\} \end{aligned}$$

unter den von $\mathbb{C}$ her bekannten Verknüpfungen uk Ringe.

Im Fall $d = -1$ wählt man $\sqrt{d} = i$, der Ring $\mathbb{Z} + \mathbb{Z}\, i$ heißt dann der Ring der *gaußschen Zahlen*.

Im Fall $d = -5$ heißt der Ring $\mathbb{Z} + \mathbb{Z}\,\sqrt{-5}$ der *Kummerring*.

10. Die Teilmengen von $\mathbb{C}$

$$\begin{aligned} &\mathbb{Z} + \mathbb{Z}\,\sqrt{2} + \mathbb{Z}\,\sqrt{3} + \mathbb{Z}\,\sqrt{6} \\ &\qquad = \{z \in \mathbb{C} \,|\, \exists\, t, u, v, w \in \mathbb{Z} \text{ mit } z = t + u\sqrt{2} + v\sqrt{3} + w\sqrt{6}\} \\ &\mathbb{Q} + \mathbb{Q}\,\sqrt{2} + \mathbb{Q}\,\sqrt{3} + \mathbb{Q}\,\sqrt{6} \\ &\qquad = \{z \in \mathbb{C} \,|\, \exists\, t, u, v, w \in \mathbb{Q} \text{ mit } z = t + u\sqrt{2} + v\sqrt{3} + w\sqrt{6}\} \end{aligned}$$

bilden unter den von $\mathbb{C}$ her bekannten Verknüpfungen uk Ringe.

11. Ist p eine Primzahl, so bildet die Teilmenge von $\mathbb{Q}$

$$\mathbb{Z}_{(p)} = \{x = \tfrac{m}{n} \in \mathbb{Q} \mid p \not| \, n\}$$

einen uk Ring.

12. Ist $\ell \in \mathbb{N}$, so bildet die Teilmenge von $\mathbb{Q}$

$$\{x = \tfrac{m}{n} \in \mathbb{Q} \mid \exists\, k \in \mathbb{N}_0 : n = \ell^k\}$$

einen uk Ring.

13. Für $n \in \mathbb{N}$ bildet die Menge aller reellen quadratischen Matrizen der Form

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & \cdots & a_{n-1} & a_n \\ a_{-1} & a_0 & a_1 & & & & a_{n-1} \\ a_{-2} & a_{-1} & a_0 & \ddots & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & a_2 \\ a_{-n+1} & & & & \ddots & \ddots & a_1 \\ a_{-n} & a_{-n+1} & \cdots & \cdots & \cdots & a_{-1} & a_0 \end{pmatrix}$$

unter den bekannten Matrixverknüpfungen einen uk Ring. Wir bezeichnen ihn mit $\mathbb{R}^{n\times n}_{\text{käm}}$. Der Teilring $\mathbb{R}^{n\times n}_{\text{käm,obere}}$ der oberen Dreiecksmatrizen ist ebenfalls ein uk Ring.

1.1.6 Definition: Teilring

Es sei R ein uk Ring. Die folgenden Aussagen über eine Teilmenge $S \subseteq R$ sind äquivalent.

(A) S heißt *(uk) Teilring* von R.

(B) Es gilt

(i) $(S, +)$ ist eine Untergruppe von $(R, +)$.

(ii) S ist unter der von R vererbten Multiplikation abgeschlossen.

(iii) Das Eins-Element von R ist auch das Einselement von S.

(C) Es gilt

(i) Für $x, y \in S$ sind $x - y$ und $x \cdot y$ in S.

(ii) Das Einselement von R ist in S.

1.1.7 Bemerkung

Der Begriff „Teilring eines Rings" wird in der Literatur unterschiedlich definiert. Manche Autoren fordern, dass der Teilring das Einselement enthält (wie oben oder Vorlesung „Grundbegriffe der Algebra", WS 2018/19, Danz), andere verzichten darauf.

Leider ist das nicht nebensächlich, wie das Beispiel $2\mathbb{Z} \subseteq \mathbb{Z}$ zeigt.

1.1.8 Beispiele

1. Die einzigen Teilringe S von $\mathbb{Z}$ sind $\{0\}$ und $\mathbb{Z}$ selbst. Ist nämlich $1 \in S$, so ist auch $n = 1 + \ldots + 1 \in \mathbb{Z}$ und dann auch $-n \in \mathbb{Z}$.

2. Wir haben die Teilringe $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

3. Die Menge der differenzierbaren Funktionen auf einem offenen Intervall $I \subseteq \mathbb{R}$ bildet einen Teilring der Menge aller auf I stetigen Funktionen.

1.1.9 Definition: Ringhomomorphismus

Es seien R und $\widetilde{R}$ uk Ringe. Eine Abbildung $\varphi : R \to \widetilde{R}$ heißt (unitärer) Ringhomomorphismus, wenn für alle $x, y \in R$ gilt

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(x \cdot y) &= \varphi(x) \cdot \varphi(y) \\ \varphi(1) &= 1. \end{aligned}$$

In diesem Fall heißt

$$\ker \varphi := \varphi^{-1}(\{0\}) = \{x \in R \mid \varphi(x) = 0\}$$

der *Kern von* φ und

$$\operatorname{im} \varphi := \varphi(R) = \{y \in \widetilde{R} \mid \exists x \in R \text{ mit } \varphi(x) = y\}$$

das *Bild von* φ.

1.2 Einheiten, Assoziiertheit

1.2.1 Definition: Einheit

Es sei R ein uk Ring. Die folgenden Aussagen über ein Element x von R sind äquivalent:

(A) (def) x heißt Einheit.

(B) x ist Teiler von 1.

(C) x ist Teiler jedes Elements von R.

1.2.2 Beweis

(C) $\Rightarrow$ (B) ist trivial.

Zu (B) $\Rightarrow$ (C). Ist x Teiler von 1, so gibt es per definitionem ein $y \in R$ mit $x \cdot y = y \cdot x = 1$. Ist dann $z \in R$ beliebig, so gilt aber auch

$$x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z = 1 \cdot z = z,$$

also ist x Teiler von z.

1.2.3 Satz: Die Einheitengruppe

Es sei R ein uk Ring. Die Teilmenge

$$R^\times \;=\; \{x \in R \mid \exists\, y \in R \text{ mit } x \cdot y = y \cdot x = 1\}$$

der Einheiten bildet unter der von R vererbten Multiplikation eine abelsche Gruppe, die so genannte *Einheitengruppe von* R. Genauer:

(a) Es ist $1 \in R^\times$,

(b) Sind $x, y \in R^\times$, so ist auch $xy \in R^\times$.

(c) Ist $x \in R^\times$, so ist das Element $y \in R^\times$ mit $xy = yx = 1$ eindeutig bestimmt. Es wird mit x^{-1} bezeichnet.

Zusätzlich gilt sogar

(d) $x, y \in R^\times \iff xy \in R^\times$.

1.2.4 Beweis

(a) Wegen $1 \cdot 1 = 1$ ist das klar.

(b) Sind $x, y \in R^\times$, so ist $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = 1$. Also ist $xy \in R$ auch $xy \in R^\times$, da in diesem Fall $y^{-1}x^{-1}$ das inverse Element ist.

(c) Das ist eine Erkenntnis aus der Gruppentheorie.

(d) Ist $xy \in R^\times$, so ist

$$x \cdot [y \cdot (xy)^{-1}] \;=\; (xy) \cdot (xy)^{-1} \;=\; 1$$

und damit x eine Einheit. Dann ist auch $y = x^{-1}(xy)$ eine Einheit.

1.2.5 Beispiele

1. Im Ring $\mathbb{Z}$ sind genau ± 1 die Einheiten.
2. Im Ring $\mathbb{Z}/n\mathbb{Z}$ sind die Einheiten genau die Restklassen $\ell + n\mathbb{Z}$, wobei $\mathrm{ggT}(\ell, n) = 1$.
3. In den Ringen von Funktionen $X \to \mathbb{R}$ sind die Funktionen ohne Nullstellen die Einheiten.
4. Im Ring $\mathbb{R}^{n\times n}_{\text{gekämmt}}$ (vgl. 1.1.5 13.) sind die invertierbaren Matrizen die Einheiten.

1.2.6 Definition und Satz: Assoziiertheit

Es sei R ein uk Ring.

(i) Zwei Elemente $x, y \in R$ heißen *assoziiert zueinander*, wenn es eine Einheit $u \in R^\times$ gibt so, dass $x = u \cdot y$ (x und y sind „bis auf Einheit gleich"). Man schreibt dafür $x \sim y$.

(ii) Assoziiertheit ist eine Äquivalenzrelation auf ganz R.

(iii) Assoziiertheit ist mit der Multiplikation auf R verträglich:

$$x \sim \widetilde{x} \text{ und } y \sim \widetilde{y} \quad \Longrightarrow \quad x \cdot y \ \sim \ \widetilde{x} \cdot \widetilde{y}.$$

1.2.7 Beweis Nachrechnen!

1.2.8 Beispiele

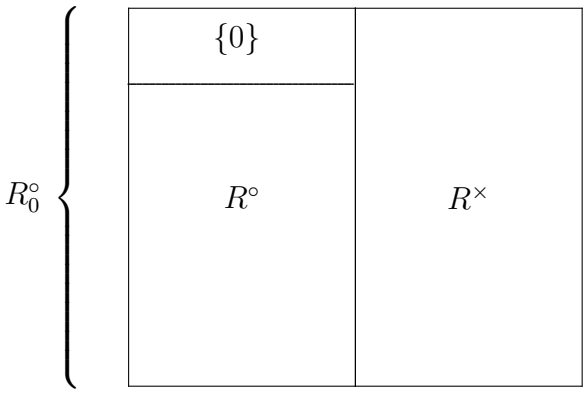
1. Die Einheiten eines uk Rings R sind alle zueinander assoziiert. In anderen Worten, $R^\times$ bildet eine Äquivalenzklasse.
2. Das Nullelement 0 ist nur zu sich selbst assoziiert. $\{0\}$ ist eine Äquivalenzklasse.
3. In $\mathbb{Z}$ sind zwei Elemente x, y genau dann assoziiert, wenn $x = y$ oder $x = -y$.
4. Zwei Polynome $f, g \in \mathbb{R}[X]$ sind genau dann assoziiert, wenn es eine Zahl $\alpha \in \mathbb{R}\setminus\{0\}$ gibt so, dass $f = \alpha\, g$.
5. In einem Körper $\mathbb{K}$ gibt es genau zwei Äquivalenzklassen, nämlich $\{0\}$ und $\mathbb{K}^\times$.

Als Grundsatz lässt sich schon jetzt festhalten, dass die Assoziiertheit **nicht** die wesentlichen Eigenschaften von Elementen oder Teilmengen eines Rings beeinflusst. Genaueres später.

1.3 Nichteinheiten

1.3.1 Zerlegung in drei Teilmengen

Eine triviale, aber lern-nachhaltige Beobachtung ist, dass ein uk Ring R sich in drei disjunkte Teilmengen zerlegen lässt, die Teilmenge $\{0\}$, die Teilmenge $R^\times$ der Einheiten, und die Teilmenge $R^\circ := R \setminus (R^\times \cup \{0\})$. Wir bezeichnen noch $R_0^\circ := R^\circ \cup \{0\} = R \setminus R^\times$.



$$\begin{aligned} R^\times \cdot R^\times &= R^\times \\ R^\times \cdot R_0^\circ &= R_0^\circ \\ R_0^\circ \cdot R_0^\circ &\subseteq R_0^\circ \end{aligned}$$

Die Teilmenge R_0° bildet den „eher interessanten" Teil eines Rings. Teilbarkeitslehre und Idealtheorie finden in R_0° statt.

1.3.2 Beobachtung

Die Negation der Aussagen in Satz 1.2.3 (d) führt auf die Äquivalenz

$$x \cdot y \in R_0^\circ \quad \Longleftrightarrow \quad x \in R_0^\circ \text{ oder } y \in R_0^\circ.$$

1.3.3 Definition: Die N Elemente in R_0°

Es sei R ein uk Ring. Ein Element $x \in R$ heißt ...

- *nilpotent*, wenn es ein $n \in \mathbb{N}$ gibt mit $x^n = 0$.
- *Nullteiler*, wenn ein Element $y \in R \setminus \{0\}$ existiert, so dass $x \cdot y = 0$.
- *Nichteinheit*, wenn $x \in R_0^\circ$.

1.3.4 Der 4N Satz

Es sei R ein uk Ring.

(i) Für $x \in R$ bestehen die folgenden Implikationen

$$x \text{ ist Null} \quad \Longrightarrow \quad x \text{ nilpotent} \quad \Longrightarrow \quad x \text{ Nullteiler} \quad \Longrightarrow \quad x \text{ Nichteinheit.}$$

(ii) Es seien $x, \widetilde{x} \in R$ mit $x \sim \widetilde{x}$. Dann

$$\begin{aligned} x = 0 &\iff \widetilde{x} = 0 \\ x \text{ nilpotent} &\iff \widetilde{x} \text{ nilpotent} \\ x \text{ Nullteiler} &\iff \widetilde{x} \text{ Nullteiler} \\ x \text{ Nichteinheit} &\iff \widetilde{x} \text{ Nichteinheit.} \end{aligned}$$

1.3.5 Beweis

(i) Die erste Implikation ist trivial.

Zur zweiten Implikation. Ist x nilpotent, so gibt es ein minimales $n \in \mathbb{N}$ mit $x^n = 0$. Ist $n = 1$, so ist $x = 0$ ein Nullteiler. Im Fall $n \geq 2$ ist $x \cdot x^{n-1} = 0$, wobei $x^{n-1} \neq 0$, und deshalb x ein Nullteiler.

Zur dritten Implikation. Es sei x ein Nullteiler, also ex. $y \in R \setminus \{0\}$ mit $x \cdot y = 0$. Wäre x eine Einheit, so würde $y = x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 = 0$ sein. Widerspruch.

(ii) Bitte Nachrechnen.

1.3.6 Beispiele, Bemerkung

1. $2 + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$ ist nilpotent.
2. Streng obere Dreiecksmatrizen

$$\begin{pmatrix} 0 & a_1 & a_2 & \cdots & \cdots & a_{n-1} & a_n \\ 0 & 0 & a_1 & & & & a_{n-1} \\ 0 & 0 & 0 & \ddots & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & a_2 \\ 0 & & & & \ddots & \ddots & a_1 \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

   sind nilpotent in $\mathbb{K}^{n\times n}_{\text{käm}}$.
3. $3 + 6\mathbb{Z} \in \mathbb{Z}/6\mathbb{Z}$ ist ein Nullteiler, aber nicht nilpotent.
4. $(0, 1), (1, 0) \in R \times R$ sind Nullteiler, aber nicht nilpotent.
5. $2 \in \mathbb{Z}$ ist eine Nichteinheit, aber kein Nullteiler.
6. $X - 2 \in \mathbb{R}[X]$ ist eine Nichteinheit, aber kein Nullteiler.
7. In endlichen uk Ringen gilt die Umkehrung der dritten Implikation:

   $$x \text{ Nullteiler} \quad \Longleftarrow \quad x \text{ Nichteinheit}.$$

   Vgl. Übungsaufgabe A4 bzw. F10 T3 A2.

1.4 Die Teilerrelation

Eine substantielle Teilbarkeitstheorie in einem uk Ring lässt sich eigentlich nur aufbauen, wenn man noch die Nullteilerfreiheit fordert, vgl. den Begriff des Integritätsrings, Kapitel 2.1. Die grundlegenden Definitionen und elementaren Einsichten können aber in allgemeinen uk Ringen angegeben werden.

1.4.1 Definition: Teilerrelation

Es sei R ein uk Ring. Dann sind für zwei Elemente $x, y \in R$ die folgenden Aussagen äquivalent:

(A) (def) x teilt y, x *teilt* y, symbolisch $x \mid y$.

Gleichbedeutend: x heißt *Teiler* von y.

Gleichbedeutend: y heißt *Vielfaches* von x.

(B) Es existiert ein $z \in R$ mit $x \cdot z = y$.

1.4.2 Lemma: Eigenschaften der Teilerrelation

Es seien R ein uk Ring und $x, y, \widetilde{x}, \widetilde{y}, z \in R$. Dann gilt

(i) Es gilt immer $\quad 1 \mid x, \;\; x \mid 0, \;\; x \mid x.$

(ii) Transitivität. Für $x, y, z \in R$ gilt die Implikation

$$x \mid y \text{ und } y \mid z \quad \Longrightarrow \quad x \mid z.$$

(iii) $x \mid y$ und $\widetilde{x} \mid \widetilde{y} \quad \Longrightarrow \quad x\widetilde{x} \mid y\widetilde{y}.$

(iv) $z \mid x$ und $z \mid \widetilde{x} \quad \Longrightarrow \quad z \mid (yx + \widetilde{y}\widetilde{x}).$

(v) Es seien $x \sim \widetilde{x}$ und $y \sim \widetilde{y}$. Dann

$$x \mid y \quad \Longleftrightarrow \quad \widetilde{x} \mid \widetilde{y}.$$

(vi) Es gilt

$$x \mid y \text{ und } y \mid x \quad \Longleftrightarrow \quad x \sim y.$$

1.4.3 Beweis

Nachprüfen! Beachte, dass so etwas wie die Existenz oder Eindeutigkeit einer Primfaktorzerlegung nicht geklärt ist.

Wir zeigen (vi)/$\Rightarrow$. Es ist

$$\begin{aligned} x \mid y &\implies \exists\, z \in R : xz = y \\ y \mid x &\implies \exists\, w \in R : yw = x. \end{aligned}$$

Daraus folgt

$$x \;=\; yw \;=\; xzw \;=\; x(zw),$$

also ist $zw = 1$, damit sind z und w Einheiten.

1.4.4 Beispiele

1. Die aus der Schule bekannte Teilerrelation für natürliche Zahlen kann auf der Menge $\mathbb{Z}$ betrachtet werden. Man berücksichtigt einfach die Vorzeichen nicht.

2. In einem beliebigen Körper ist die Teilerrelation reichlich uninteressant. Alle Elemente ungleich Null teilen sich gegenseitig und die Null. Die Null teilt nur sich selbst.

3. Im aus der Schule bekannten Ring der reellen Polynomfunktionen ist $(x-1) \mid (x^2-1)$, da $(x-1)(x+1) = x^2 - 1$.

4. Die im Lemma 1.4.2 angegebenen Regeln für die Teilbarkeit sind wohl vertraut. Wir werden aber sehen, dass andere ,,Regeln" aus der Teilbarkeitslehre ihre Tücken haben.

5. Zwei Einheiten eines uk Rings teilen sich immer gegenseitig.

1.4.5 Definition: Irreduzible und Primelemente in R°

Es sei R ein uk Ring. Ein Element $x \in R$ heißt ...

- *irreduzibel (= unzerlegbar)*, wenn

$$\begin{aligned} &x \in R^\circ \\ &x \;=\; y \cdot z \quad \Longrightarrow \quad y \in R^\times \text{ oder } z \in R^\times. \end{aligned}$$

  (Die Nichteinheit x kann nicht in zwei Nichteinheiten ,,zerlegt" werden.)

  Wir fassen alle irreduziblen Elemente eines Rings in der Menge $R^{\text{irr}} \subseteq R^o$ zusammen.

- *reduzibel*, wenn es nicht irreduzibel ist, d.h.

$$\begin{aligned} &x = 0 \text{ oder } x \in R^\times \text{ oder} \\ &\exists\, y, z \in R^\circ : x = y \cdot z. \end{aligned}$$

- ein *Primelement (=prim)*, wenn

$$\begin{aligned} &x \in R^\circ \\ &x \mid (y \cdot z) \quad \Longrightarrow \quad x \mid y \text{ oder } x \mid z. \end{aligned}$$

  (Teilt x ein Produkt, so teilt es bereits einen der Faktoren.)

  Wir fassen alle Primelemente eines Rings in der Menge $R^{\text{prm}} \subseteq R^o$ zusammen.

1.4.6 Satz: Irreduzible und Primelemente bei Assoziiertheit

Es sei R ein uk Ring. Es seien $x, \widetilde{x} \in R$ mit $x \sim \widetilde{x}$. Dann

$$\begin{aligned} x \text{ irreduzibel} &\iff \widetilde{x} \text{ irreduzibel} \\ x \text{ Primelement} &\iff \widetilde{x} \text{ Primelement.} \end{aligned}$$

1.4.7 Beweis Nachrechnen!

1.4.8 Aussagen

Im folgenden formulieren wir sechs Aussagen über einen uk Ring R.

($\mathrm{Ex}_{\mathrm{prm}}$) Jedes $a \in R^\circ$ lässt sich als (endliches) Produkt von Primelementen darstellen.

$$a = p_1 \cdot \ldots \cdot p_r.$$

($\mathrm{Ei}_{\mathrm{prm}}$) Gibt es für ein $a \in R^\circ$ eine Darstellung als (endliches) Produkt von Primelementen, so ist diese bis auf Reihenfolge und Assoziiertheit eindeutig, d.h. genauer:
Sind $r, s \in \mathbb{N}$, $p_1, \ldots, p_r, q_1, \ldots, q_s \in R$ Primelemente mit

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s,$$

so ist $r = s$ und $p_i \sim q_{\pi(i)}$, wobei π eine geeignete Permutation von $\{1, \ldots, r\}$ ist.

($\mathrm{Ex/Ei}_{\mathrm{prm}}$) $\iff$ ($\mathrm{Ex}_{\mathrm{prm}}$) und ($\mathrm{Ei}_{\mathrm{prm}}$).

($\mathrm{Ex}_{\mathrm{irr}}$) Jedes $a \in R^\circ$ lässt sich als (endliches) Produkt von irreduziblen Elementen darstellen.

$$a = p_1 \cdot \ldots \cdot p_r.$$

($\mathrm{Ei}_{\mathrm{irr}}$) Gibt es für ein $a \in R^\circ$ eine Darstellung als (endliches) Produkt von irreduziblen Elementen, so ist diese bis auf Reihenfolge und Assoziiertheit eindeutig, d.h. genauer:
Sind $r, s \in \mathbb{N}$, $p_1, \ldots, p_r, q_1, \ldots, q_s \in R$ irreduziblen Elemente mit

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s,$$

so ist $r = s$ und $p_i \sim q_{\pi(i)}$, wobei π eine geeignete Permutation von $\{1, \ldots, r\}$ ist.

($\mathrm{Ex/Ei}_{\mathrm{irr}}$) $\iff$ ($\mathrm{Ex}_{\mathrm{irr}}$) und ($\mathrm{Ei}_{\mathrm{irr}}$).

1.4.9 Definition: Gemeinsame Teiler und Vielfache

Es seien R ein uk Ring und $A \subseteq R \setminus \{0\}$.

1. Ein Element $x \in R \setminus \{0\}$ heißt *gemeinsamer Teiler von* A, wenn

   $$x \mid a \quad \text{für alle } a \in A.$$

   Wir fassen diese gemeinsamen Teiler in der Menge $\mathcal{M}_{\mathrm{gT}}(A)$ zusammen.

2. Ein Element $x \in R \setminus \{0\}$ heißt *gemeinsames Vielfaches von* A, wenn

   $$a \mid x \quad \text{für alle } a \in A.$$

   Wir fassen diese gemeinsamen Vielfache in der Menge $\mathcal{M}_{\mathrm{gV}}(A)$ zusammen.

3. Ein Element $x \in R \setminus \{0\}$ heißt *größter gemeinsamer Teiler (ggT) von* A, wenn x

   gemeinsamer Teiler von A und zusätzlich
   Vielfaches aller gemeinsamen Teiler von A

   ist. Die Menge der größten gemeinsamen Teiler von A ist also

   $$\mathcal{M}_{\mathrm{ggT}}(A) \;=\; \mathcal{M}_{\mathrm{gT}}(A) \;\cap\; \mathcal{M}_{\mathrm{gV}}(\mathcal{M}_{\mathrm{gT}}(A)).$$

4. Ein Element $x \in R \setminus \{0\}$ heißt *kleinstes gemeinsames Vielfaches (kgV) von* A, wenn x

   gemeinsames Vielfaches von A und zusätzlich
   Teiler aller gemeinsamen Vielfachen von A

   ist. Die Menge der kleinsten gemeinsamen Vielfachen von A ist also

   $$\mathcal{M}_{\mathrm{kgV}}(A) \;=\; \mathcal{M}_{\mathrm{gV}}(A) \;\cap\; \mathcal{M}_{\mathrm{gT}}(\mathcal{M}_{\mathrm{gV}}(A)).$$

1.4.10 Bemerkungen

1. Es geht fast ausschließlich um endliche Teilmengen $A = \{a_1, \ldots, a_m\}$. Man schreibt dann auch $\mathcal{M}_x(A) = \mathcal{M}_x(a_1, \ldots, a_m)$.

2. Die Begriffe ,,größtes" und ,,kleinstes" suggerieren, dass auf dem betrachteten Ring eine lineare Ordnung (= totale, antisymmetrische, transitive Relation) existieren würde. Die Begriffe beziehen sich aber nur auf die Teilerrelation.

3. In dem elementaren Ring $\mathbb{Z}$ sind 6 und -6 größte gemeinsame Teiler von 12 und 18 bzw. kleinste gemeinsame Vielfache von 2 und 3. Anders als in der Menge $\mathbb{N}$ der natürlichen Zahlen können sie also nicht als Verknüpfungen $R \times R \to R$ sinnvoll definiert werden.

4. Es gilt immer

   $$R^\times \subseteq \mathcal{M}_{\mathrm{gT}}(A)$$
   $$a_1 \cdot \ldots \cdot a_m \;\in\; \mathcal{M}_{\mathrm{gV}}(A), \quad \text{falls } A = \{a_1, \ldots, a_m\} \text{ endlich.}$$

5. Wir werden Beispiele dafür kennenlernen, dass $\mathcal{M}_{\mathrm{ggT}}(\{a_1, a_2\}) = \varnothing$ ist.

1.4.11 Gemeinsame Teiler und Vielfache bei Assoziiertheit

Es sei $A \subseteq R$ eine feste Teilmenge von R. Bezüglich Assoziiertheit haben die in Definition 1.4.9 beschriebenen Teilmengen die folgenden Eigenschaften. Für $x, y \in R \setminus \{0\}$ gilt

$$\begin{aligned}
y \sim x, \quad x \in \mathcal{M}_{\mathrm{gT}}(A) \quad &\Longrightarrow \quad y \in \mathcal{M}_{\mathrm{gT}}(A) \\
y \sim x, \quad x \in \mathcal{M}_{\mathrm{gV}}(A) \quad &\Longrightarrow \quad y \in \mathcal{M}_{\mathrm{gV}}(A) \\
y \sim x, \quad x \in \mathcal{M}_{\mathrm{ggT}}(A) \quad &\Longrightarrow \quad y \in \mathcal{M}_{\mathrm{ggT}}(A) \\
y \sim x, \quad x \in \mathcal{M}_{\mathrm{kgV}}(A) \quad &\Longrightarrow \quad y \in \mathcal{M}_{\mathrm{kgV}}(A)
\end{aligned}$$

$$\begin{aligned}
x, y \in \mathcal{M}_{\mathrm{ggT}}(A) \quad &\Longrightarrow \quad x \sim y \\
x, y \in \mathcal{M}_{\mathrm{kgV}}(A) \quad &\Longrightarrow \quad x \sim y.
\end{aligned}$$

1.4.12 Beweis

Wir zeigen beispielsweise die fünfte Zeile.

$$\begin{aligned}
& x, y \in \mathcal{M}_{\mathrm{ggT}}(A) \\
\Longrightarrow \quad & x \in \mathcal{M}_{\mathrm{gT}}(A),\ y \in \mathcal{M}_{\mathrm{gV}}(\mathcal{M}_{\mathrm{gT}}(A)) \\
\Longrightarrow \quad & x \mid y.
\end{aligned}$$

Umgekehrt gilt auch $y \mid x$ und damit $x \sim y$, siehe Lemma 1.4.2(vi).

1.5 Ideale

1.5.1 Satz und Definition: Ideal

Es seien R ein uk Ring und I eine (additive) Untergruppe der abelschen Gruppe $(R,+)$. Die folgenden Aussagen sind äquivalent.

(A) (def) I heißt Ideal in R.

(B) Für alle $x \in R$ und $a \in I$ sind $x \cdot a \in I$ (und $a \cdot x \in I$).
(R operiert multiplikativ auf I).

(C) Die Faktorgruppe $(R/I,+)$ ist wohldefiniert und wird bzgl. der wie folgt wohldefinierten Multiplikation zu einem uk Ring

$$\cdot : \left\{ \begin{array}{rcl} R/I \times R/I & \to & R/I \\ (x+I, y+I) & \mapsto & (x \cdot y) + I. \end{array} \right.$$

R/I heißt dann *Faktorring*, die kanonische Abbildung $\pi : R \to R/I$ weiterhin der *kanonische Epimorphismus*.

(D) Es existieren ein uk Ring S und ein (unitärer) Ringhomomorphismus $\varphi : R \to S$ so, dass $\ker \varphi = I$.

1.5.2 Beweis

(B) $\Rightarrow$ (C). Da $(R,+)$ abelsch ist, ist I ein Normalteiler und R/I ist wohldefiniert.

Sind $x, \widetilde{x}, y, \widetilde{y} \in R$ mit $x + I = \widetilde{x} + I$ und $y + I = \widetilde{y} + I$, so gibt es $a, b \in I$ mit $\widetilde{x} = x + a$ und $\widetilde{y} = y + b$, deswegen

$$(\widetilde{x} \cdot \widetilde{y}) + I \;=\; [(x+a)(y+b)] + I \;=\; [xy + \underbrace{xb + ay + ab}_{\in I}] + I \;=\; xy + I.$$

Für alle $x \in R$ ist

$$(1+I)(x+I) \;=\; (1 \cdot x) + I \;=\; x + I,$$

also ist $1 + I$ das Einselement in R/I.

Wir rechnen das Distributivgesetz nach. Für $x, y, z \in R$ ist

$$\begin{aligned} (x+I) \cdot [(y+I) + (z+I)] &= (x+I) \cdot [(y+z) + I] = [x \cdot (y+z)] + I \\ &= [x \cdot y + x \cdot z] + I = (x \cdot y) + I + (x \cdot z) + I \\ &= (x+I)(y+I) + (x+I)(z+I). \end{aligned}$$

Das Assoziativgesetz ist noch einfacher nachzuprüfen.

(C) $\Rightarrow$ (D). Man wähle einfach den Ring $S = R/I$ und als Ringhomomorphismus den kanonischen Epimorphismus

$$\pi : \left\{ \begin{array}{rcl} R & \to & R/I \\ x & \mapsto & x + I. \end{array} \right.$$

(D) $\Rightarrow$ (B). Sind $x \in R$ und $a \in I = \ker \varphi$, so ist

$$\varphi(x \cdot a) \;=\; \varphi(x) \cdot \varphi(a) \;=\; \varphi(x) \cdot 0 \;=\; 0,$$

also $x \cdot a \in \ker \varphi = I$.

1.5.3 Beispiele

(1) Ist $n \in \mathbb{Z}$, so ist die Vielfachenmenge $n\mathbb{Z} = \mathcal{M}_{\mathrm{gV}}(n)$ ein Ideal.

(2) Ist allgemeiner $A \subseteq R$, R ein Ring, so ist die Vielfachenmenge $\mathcal{M}_{\mathrm{gV}}(A)$ ein Ideal.

(3) Ist $R = \mathbb{R}[X, Y]$ der Ring der Polynome in zwei Variablen mit reellen Koeffizienten, das sind

$$f \;=\; f_{00} + f_{10}X + f_{01}Y + f_{11}XY + \ldots$$

Die Teilmenge der Polynome f mit $f_{00} = 0$ bildet ein Ideal. Für dieses Ideal gibt es kein Element in R so, dass es dazu Vielfachenmenge wäre.

(4) Ist R ein Ring von Funktionen $A \to \mathbb{R}$ und $N \subseteq A$ eine Teilmenge der Definitionsmenge, so ist die Teilmenge der Funktionen mit $N \subseteq f^{-1}(0)$ (auf N gleich Null) ein Ideal.

1.5.4 Bemerkungen: Ideale

(1) Enthält ein Ideal I eines uk Rings eine Einheit, so ist es gleich dem ganzen Ring.

(2) Ideale sind unter Assoziiertheit abgeschlossen.

(3) Ist eine Teilmenge X eines uk Rings R zugleich Ideal und Teilring, so ist $X = R$.

(4) Es gibt zahlreiche verschiedene Schreibweisen für die Restklassen in R/I:

$$x + I \;=\; x \bmod I \;=\; \overline{x} \;=\; [x].$$

1.5.5 Satz: Schnittmenge von Idealen

Es sei R ein uk Ring. Sind $(I_j)_{j\in\mathcal{J}}$ (endlich oder unendlich viele) Ideale in R, so ist auch

$$I \;:=\; \bigcap_{j\in\mathcal{J}} I_j$$

ein Ideal in R.

1.5.6 Beweis

Dass I eine abelsche Untergruppe von R ist, ist aus der Gruppentheorie (Prop. 3.5, Vorlesung ,,Grundbegriffe der Algebra", WS 2018/19, Danz) bekannt.

Es seien dann $x \in R$ und $a \in I$. Dann ist $a \in I_j$ für alle $j \in \mathcal{J}$, deswegen $x\,a \in I_j$ für alle $j \in \mathcal{J}$, und damit $x\,a \in I$.

1.5.7 Definition und Satz: Teilmenge erzeugt Ideal

Es sei R ein uk Ring und $A \subseteq R$ eine Teilmenge. Die folgenden Aussagen über eine weitere Teilmenge $(A) \subseteq R$ sind äquivalent.

(A) (def) (A) heißt das *von A in $\mathbb{R}$ erzeugte Ideal*.

(B) (A) ist unter allen Idealen $I \subseteq R$ mit $A \subseteq I$ minimal, d.h. genauer:

Existiert ein Ideal J mit $A \subseteq J \subseteq (A)$, so ist $J = (A)$.

(C) Es ist (A) der Schnitt aller Ideale in R, die A enthalten.

(D) Die Elemente von (A) sind genau die R-A-Linearkombinationen, d.h. genauer

$$(A) \;=\; \{x \in R \mid \exists\, \ell \in \mathbb{N},\, r_1, \ldots, r_\ell \in R,\, a_1, \ldots, a_\ell \in A : x = r_1 a_1 + \ldots + r_\ell a_\ell\}.$$

Im Fall $A = \varnothing$ ist naheliegend $(A) = \{0\}$.

1.5.8 Beweis

Fehlt bzw. leicht.

1.5.9 Definition: Hauptideal, endlich erzeugtes Ideal

Es sei R ein uk Ring und I ein Ideal in R.

(i) Das Ideal I heißt *Hauptideal*, wenn es ein einziges Element $a \in R$ gibt so, dass

$$I \;=\; \mathcal{M}_{\mathrm{gV}}(a) \;=\; (a) \;=\; aR \;=\; Ra.$$

Hauptideale umfassen also alle Vielfache von a.

(ii) Das Ideal I heißt *endlich erzeugt*, wenn es endlich viele Elemente $a_1, \ldots, a_n \in R$ gibt so, dass

$$I \;=\; (a_1, \ldots, a_n) \;=\; \{z \in R \mid \exists\, r_1, \ldots, r_n \in R : z = r_1 a_1 + \ldots + r_n a_n\}.$$

1.5.10 Teilbarkeit und Hauptideale

Es seien $x, y \in R$ Elemente eines uk Rings und $(x), (y)$ die von ihnen erzeugten Hauptideale. Dann

(i) $x \mid y \quad\Longleftrightarrow\quad (y) \;\subseteq\; (x)$.

(ii) $x \sim y \quad\Longleftrightarrow\quad (y) \;=\; (x)$.

1.5.11 Beweis

Fehlt bzw. leicht.

1.5.12 Satz: Verknüpfungen von Idealen

I, J, K seien Ideale in dem uk Ring R.

(i) Die folgenden drei Teilmengen sind ebenfalls Ideale in R.

$$\begin{aligned} I \cdot J \;=\; (I \cdot J) \quad &= \left\{ \textstyle\sum_{\text{endl.}} a_j b_j \in R \mid a_j \in I,\, b_j \in J \right\} \\ &\neq \left\{ ab \in R \mid a \in I,\, b \in J \right\} \quad \text{(Vorsicht: i.a.)} \\ I \cap J \;=\; (I \cap J) \quad &= \left\{ a \in R \mid a \in I,\, a \in J \right\} \\ I + J \;=\; (I \cup J) \quad &= \left\{ a + b \in R \mid a \in I,\, b \in J \right\} \\ &\neq I \cup J. \quad \text{(Vorsicht: i.a.)} \end{aligned}$$

(ii) Es gilt

$$I \cdot J \;\subseteq\; I \cap J \;\subseteq\; I \;\subseteq\; I + J.$$

Im allgemeinen ist an keiner Stelle Gleichheit gegeben.

(iii) Es gilt die Implikation

$$\underbrace{I + J \;=\; R}_{\overset{\text{def}}{\iff} \; I,\, J \text{ heißen koprim}} \qquad \Longrightarrow \qquad I \cdot J \;=\; I \cap J.$$

(iv) Rechenregeln für das Rechnen mit Idealen. Es ist

$$\begin{aligned} (I \cdot J) \cdot K \;&=\; I \cdot (J \cdot K) \\ I \cdot (J + K) \;&=\; I \cdot J + I \cdot K. \end{aligned}$$

(Ersetzt man in der zweiten Zeile den Malpunkt $\cdot$ durch das Schnittzeichen $\cap$, so stimmt dieses ,,Distributivgesetz" in allgemeinen Ringen nicht.)

1.5.13 Beweis

(i) Dass die drei angegebenen Teilmengen Ideale sind, ist schon in Satz 1.5.7 ausgesagt.

(Vorsicht)$_1$. Ist $R = \mathbb{R}[X, Y]$ der Ring der Polynome in zwei Variablen mit reellen Koeffizienten, so sind $I = (X)$ und $J = (Y)$ Ideale. Für das Polynom $X^2Y + XY^2$ gilt dann

$$X^2Y + XY^2 \;=\; (X + Y)\, XY \in I \cdot J,$$

es gibt aber nicht zwei Polynome $f \in I$ und $g \in J$ so, dass

$$X^2Y + XY^2 \;=\; f \cdot g.$$

(Vorsicht)$_2$. Für die beiden Ideale $I = (2)$ und $J = (3)$ in $\mathbb{Z}$ gilt

$$(2) + (3) \;=\; \{x \in \mathbb{Z} \mid \exists z_1, z_2 \in \mathbb{Z} : x = z_1 \cdot 2 + z_2 \cdot 3\} \;=\; \mathbb{Z}$$

und $5 \notin (2) \cup (3)$.

(ii) Aufgrund von

$$\begin{aligned} I \cdot J &\subseteq R \cdot J = J \\ I \cdot J &\subseteq I \cdot R = I \end{aligned}$$

ist $I \cdot J \subseteq I \cap J$. Die anderen Inklusionen sind noch einfacher einzusehen.

Für das Ideal $I = (2)$ in $\mathbb{Z}$ gilt $I \cdot I = (4) \subsetneq (2) = I \cap I$.

Für die beiden Ideale $I = (2)$ und $J = (3)$ in $\mathbb{Z}$ gilt

$$I \cap J \;=\; (6) \;\subsetneq\; (2) \;=\; I \;\subsetneq\; \mathbb{Z} \;=\; I + J.$$

(iii) Aufgrund der Voraussetzung ,,koprim" gibt es $a \in I$, $b \in J$ mit $1 = a + b$.

Ist $x \in I \cap J$, so sind $a \cdot x \in I \cdot J$ und $b \cdot x \in J \cdot I = I \cdot J$. Es gilt dann

$$x \;=\; 1 \cdot x \;=\; (a + b) \cdot x \;=\; a \cdot x + b \cdot x \;\in\; I \cdot J.$$

(iv) Selbst nachrechnen!

1.5.14 Beispiel: Hauptideale in $\mathbb{Z}$

Im Ring $\mathbb{Z}$, allgemeiner in einem ,,Hauptidealring" (siehe später), korrespondieren die Verknüpfungen von Idealen mit Verknüpfungen der sie erzeugenden Elemente.

Für $x, y \in \mathbb{Z}$ gelten die Beziehungen

$$\begin{array}{ccccccc} (x) \cdot (y) & \subseteq & (x) \cap (y) & \subseteq & (x) & \subseteq & (x) + (y) \\ \| & & \| & & \| & & \| \\ (x \cdot y) & \subseteq & (\mathrm{kgV}(x, y)) & \subseteq & (x) & \subseteq & (\mathrm{ggT}(x, y)). \end{array}$$

Für $x, y \in \mathbb{Z}$ gelten die Implikationen

$$\begin{aligned} & \mathrm{ggT}(x, y) = 1 \\ \iff\; & (x) + (y) = R \\ \iff\; & (x) \cdot (y) = (\mathrm{kgV}(x, y)) \\ & \mathrm{kgV}(x, y) = x \cdot y. \end{aligned}$$

1.5.15 Definition: Primideal, maximales Ideal

Es sei R ein uk Ring und $I \subseteq$ ein Ideal. Das Ideal heißt ...

- *Primideal*, wenn

$$\begin{aligned} &I \neq R \\ &a \cdot b \in I \quad \Longrightarrow \quad a \in I \text{ oder } b \in I. \end{aligned}$$

- *maximales Ideal*, wenn

$$\begin{aligned} &I \neq R \\ &\text{Ist } J \text{ ein Ideal mit } I \subseteq J \subseteq R, \text{ so ist } J = I \text{ oder } J = \mathbb{R}. \end{aligned}$$

1.5.16 Satz: Maximale Ideale und Primideale

In einem uk Ring R ist jedes maximale Ideal I ein Primideal.

1.5.17 Beweis

Es sei also $I \subseteq R$ ein maximales Ideal und $x, y \in R$ mit $xy \in I$, $x \notin I$. Dann ist (I, x) ein I echt umfassendes Ideal, also $(I, x) = R$ und weiter $1 \in (I, x)$.

Dann existieren Elemente $z \in R$ und $a \in I$ mit $zx + a = 1$. Deshalb ist $zx \in 1 + I$, das heißt aber $zx + I = 1 + I$. Dann ist

$$\begin{aligned} y + I &= (1 + I)(y + I) = (zx + I)(y + I) = zxy + I \\ &= (z + I)(xy + I) = (z + I)(0 + I) = 0 + I, \end{aligned}$$

also $y \in I$.

1.5.18 Beispiele

(1) In einem Integritätsring (s.u.), der kein Körper ist, ist $\{0\}$ ein Primideal, aber kein maximales Ideal.

(2) Im Ring $\mathbb{R}[X, Y]$ der reellen Polynome mit zwei Variablen ist (X) ein Primideal, aber kein maximales Ideal, da

$$(X) \subsetneqq (X, Y) \subsetneqq \mathbb{R}[X, Y].$$

(3) Im Ring $\mathbb{Z}[X]$ der Polynome in einer Variablen mit ganzzahligen Koeffizienten ist (X) ein Primideal, aber kein maximales Ideal, da

$$(X) \subsetneqq (2, X) \subsetneqq \mathbb{Z}[X].$$

1.6 Isomorphiesätze

1.6.1 Vorbemerkung

Die Namensgebung für die folgenden Sätze ist uneinheitlich.

Hilger	Danz	Fischer
Homomorphiesatz 1.6.2	Homomorphiesatz 10.17	Erster Isomorphiesatz S. 179
Erster Isomorphiesatz 1.6.4	Erster Isomorphiesatz 10.18	Zweiter Isomorphiesatz S. 192
Korrespondezsatz 1.6.6	? (Seite im Skript fehlt)	Korrespondenzsatz S. 179

1.6.2 Satz: Homomorphiesatz

Es sei $\varphi : R \to \widetilde{R}$ ein (unitärer) Ringhomomorphismus zwischen zwei uk Ringen R und $\widetilde{R}$. Dann ist

$$\Phi : \begin{cases} R/(\ker\varphi) & \to & \operatorname{im}\varphi \\ a + I & \mapsto & \varphi(a) \end{cases}$$

ein wohldefinierter Ring**iso**morphismus.

1.6.3 Beweis

Gemäß Satz 4.17 Vorlesung ,,Grundbegriffe der Algebra", WS 2018/19, Danz ist Φ ein Isomorphismus abelscher Gruppen.

Für $x + \ker\varphi, y + \ker\varphi \in R/(\ker\varphi)$ gilt weiter

$$\begin{aligned} \Phi((x+\ker\varphi)\cdot(y+\ker\varphi)) &= \Phi(xy+\ker\varphi) = \varphi(xy) \\ &= \varphi(x)\cdot\varphi(y) = \Phi(x+\ker\varphi)\cdot\Phi(y+\ker\varphi). \end{aligned}$$

Schließlich ist

$$\Phi(1+\ker\varphi) = \varphi(1) = 1.$$

1.6.4 Satz: Isomorphiesatz

Es seien R ein uk Ring, S ein Teilring und I ein Ideal in R. Dann gilt

(i) I ist ein Ideal im Teilring $S + I$ von R.

(ii) $S \cap I$ ist ein Ideal in S.

(iii) Es ex. ein Ring**iso**morphismus

$$(S+I)/I \cong S/(S\cap I).$$

1.6.5 Beweis

Vgl. Vorlesung Danz, ,,Erster Isomorphiesatz" 10.18

1.6.6 Satz: Korrespondenzsatz

Es seien R ein uk Ring und $I \subseteq R$ ein fixiertes Ideal. Es sei weiter $\widetilde{R} := R/I$ der Faktorring und $\pi : R \to \widetilde{R}$ der kanonische Ring**epi**morphismus.

(i) Dann korrespondieren die beiden Mengen

$$\begin{aligned} \mathcal{M} &:= \{J \subseteq R \mid J \text{ Ideal} \quad \text{und } I \subseteq J\} \\ \widetilde{\mathcal{M}} &:= \{\widetilde{J} \subseteq \widetilde{R} \mid \widetilde{J} \text{ Ideal}\} \end{aligned}$$

in dem Sinne, dass die Abbildungen

$$\Phi : \left\{ \begin{array}{rcl} \mathcal{M} & \to & \widetilde{\mathcal{M}} \\ J & \mapsto & \pi(J) \end{array} \right. \qquad \Psi : \left\{ \begin{array}{rcl} \widetilde{\mathcal{M}} & \to & \mathcal{M} \\ \widetilde{J} & \mapsto & \pi^{-1}(\widetilde{J}) \end{array} \right.$$

inklusionserhaltend, bijektiv und invers zueinander sind.

(ii) Ist J ein weiteres fixiertes Ideal mit $I \subseteq J$, so ist die Abbildung

$$\left\{ \begin{array}{rcl} (R/I)\,/\,(J/I) & \to & R/J \\ (x+I)+J/I & \mapsto & x+J \end{array} \right.$$

ein Ring**iso**morphismus.

1.6.7 Beweis

(i) Zunächst ist die ,,Inklusionserhaltung" trivial:

$$J_1 \subseteq J_2 \implies \pi(J_1) \subseteq \pi(J_2).$$

Es ist dann zu zeigen, dass

$$\begin{aligned} \Phi \circ \Psi &= \mathrm{id}_{\widetilde{\mathcal{M}}}, \qquad \text{d.h.} \quad \pi(\pi^{-1}(\widetilde{J})) = \widetilde{J} \quad \text{für alle } \widetilde{J} \in \widetilde{\mathcal{M}}, \\ \Psi \circ \Phi &= \mathrm{id}_{\mathcal{M}}, \qquad \text{d.h.} \quad \pi^{-1}(\pi(J)) = J \quad \text{für alle } J \in \mathcal{M}. \end{aligned}$$

Wir betrachten die vier Inklusionen

$$\begin{aligned} \pi(\pi^{-1}(\widetilde{J})) &\subseteq \widetilde{J} \quad \text{für alle } \widetilde{J} \in \widetilde{\mathcal{M}}, \\ \pi(\pi^{-1}(\widetilde{J})) &\supseteq \widetilde{J} \quad \text{für alle } \widetilde{J} \in \widetilde{\mathcal{M}}, \\ \pi^{-1}(\pi(J)) &\supseteq J \quad \text{für alle } J \in \mathcal{M}, \\ \pi^{-1}(\pi(J)) &\subseteq J \quad \text{für alle } J \in \mathcal{M}. \end{aligned}$$

Die erste und dritte sind ganz allgemein richtig bei Abbildungen. Die zweite folgt aus der Surjektivität von π.

Die vierte zeigen wir mit Hilfe einer Implikationskette wie folgt

$$\begin{aligned} & x \in \pi^{-1}(\pi(J)) \\ \implies & \pi(x) \in \pi(J) \\ \implies & \exists\, y \in J : \pi(x) = \pi(y) \\ \implies & \exists\, y \in J : x - y \in I \subseteq J \\ \implies & \exists\, y \in J : x = (x-y) + y \in J. \end{aligned}$$

(ii) Diese Aussage zeigt man genau so wie die entsprechende im ,,Dritten Isomorphiesatz" der Gruppentheorie.

1.6.8 Beispiel

Wir betrachten den Ring $\mathbb{Z}$ und darin das Ideal $I = 24\mathbb{Z}$. Die Menge $\mathcal{M}$ der „Oberideale" von I in $\mathbb{Z}$ enthält 8 Elemente. Die bijektive Abbildung Φ aus dem Satz ist konkret gegeben durch

$$\Phi : \begin{cases} \mathcal{M} & \to & \widetilde{\mathcal{M}} \\ J & \mapsto & \pi(J) \\ & & \\ 1\mathbb{Z} & \mapsto & \{\overline{0}, \overline{1}, \overline{2}, \overline{6}, \ldots, \overline{23}\} \\ 2\mathbb{Z} & \mapsto & \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \ldots, \overline{22}\} \\ 3\mathbb{Z} & \mapsto & \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \ldots, \overline{21}\} \\ 4\mathbb{Z} & \mapsto & \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \ldots, \overline{20}\} \\ 6\mathbb{Z} & \mapsto & \{\overline{0}, \overline{6}, \overline{12}, \overline{18}\} \\ 8\mathbb{Z} & \mapsto & \{\overline{0}, \overline{8}, \overline{16}\} \\ 12\mathbb{Z} & \mapsto & \{\overline{0}, \overline{12}\} \\ 24\mathbb{Z} & \mapsto & \{\overline{0}\}. \end{cases}$$

2 Besondere Ringe

2.1 Integritätsringe

2.1.1 Definition und Satz: Integritätsring

Es sei R ein uk Ring.

Dann sind die folgenden Aussagen äquivalent.

(A) (def) Der Ring R heißt *Integritätsring (= Integritätsbereich) (= nullteilerfrei).*

(B_1) $R \setminus \{0\}$ enthält keine Nullteiler. Für jedes $x \in R$ gilt die Implikation
$\Big(\exists\, z \in R \setminus \{0\} : x \cdot z = 0 \implies x = 0\Big)$

(B_2) Allgemeine Kürzungsregel. Für jedes $x, y \in R$ gilt die Implikation
$\Big(\exists\, z \in R \setminus \{0\} : x \cdot z = y \cdot z \implies x = y\Big)$

(C) $\{0\}$ ist ein Primideal in R.

2.1.2 Beweis

(B_1) $\Leftrightarrow$ (B_2). Für $x, y, w = x - y \in R$ haben wir die Äquivalenzkette

$$\begin{aligned}
& \Big(\exists\, z \in R \setminus \{0\} : w \cdot z = 0 \quad \Longrightarrow \quad w = 0\Big) && (B_1)\\
\overset{w = x - y}{\Longrightarrow} \quad & \Big(\exists\, z \in R \setminus \{0\} : (x - y) \cdot z = z \quad \Longrightarrow \quad x = y\Big) &&\\
\Longleftrightarrow \quad & \Big(\exists\, z \in R \setminus \{0\} : x \cdot z = y \cdot z \quad \Longrightarrow \quad x = y\Big) && (B_2)
\end{aligned}$$

(B_1) $\Leftrightarrow$ (C). Wir haben die Äquivalenzkette

$$\begin{aligned}
& R \setminus \{0\} \text{ enthält keine Nullteiler} &&\\
\Longleftrightarrow \quad & \Big(xy = 0 \quad \Longrightarrow \quad x = 0 \text{ oder } y = 0\Big) && \forall x, y \in R\\
\Longleftrightarrow \quad & \Big(xy \in \{0\} \quad \Longrightarrow \quad x \in \{0\} \text{ oder } y \in \{0\}\Big) && \forall x, y \in R\\
\Longleftrightarrow \quad & \{0\} \text{ ist Primideal.} &&
\end{aligned}$$

2.1.3 Beispiele

1. Der Ring $\mathbb{Z}$ ist selbstverständlich ein Integritätsring. Das Produkt zweier ganzer Zahlen ist nur dann Null, wenn (mindestens) eine der beiden Zahlen selbst Null ist.

2. Der Ring der reellen Polynome $\mathbb{R}[x]$ ist ein Integritätsring. Da dies aus der Schule nur ,,gefühlt bekannt" ist, werden wir das noch eigens beweisen.

3. Der Ring der auf einem Gebiet Ω holomorphen Funktionen ist ein Integritätsring. Das Produkt zweier solcher Funktionen kann nach dem Identitätsprinzip nur Null sein, wenn eine der beiden Faktor-Funktionen Null ist.

2.1.4 Satz:

Es sei R ein uk Ring und I ein Ideal in R. Es gilt

$$I \text{ ist ein Primideal} \quad \Longleftrightarrow \quad R/I \text{ ist Integritätsring.}$$

2.1.5 Beweis

$\Rightarrow$. Es seien $x+I$, $y+I$ Nullteiler in R/I. Dann folgern wir in einer Implikationskette

$$\begin{aligned} & (x+I)(y+I) = 0+I \\ \Longrightarrow \quad & xy+I = 0+I \\ \Longrightarrow \quad & xy \in I \\ \overset{I \text{ Primideal}}{\Longrightarrow} \quad & x \in I \text{ oder } y \in I \\ \Longrightarrow \quad & x+I = 0+I \text{ oder } y+I = 0+I \end{aligned}$$

und damit ist R nullteilerfrei.

$\Leftarrow$. Es seien $x, y \in R$. Dann folgern wir in einer Implikationskette

$$\begin{aligned} & xy \in I \\ \Longrightarrow \quad & xy+I \;=\; 0+I \\ \Longrightarrow \quad & (x+I)(y+I) \;=\; 0+I \\ \overset{R/I \text{ Integritätsring}}{\Longrightarrow} \quad & (x+I) \;=\; 0+I \text{ oder } (y+I) \;=\; 0+I \\ \Longrightarrow \quad & x \in I \text{ oder } y \in I. \end{aligned}$$

2.1.6 Teilbarkeit in Integritätsringen I

Es sei R ein Integritätsring und $p \in R \setminus \{0\}$. Es gelten die folgenden Implikationen.

$$\begin{aligned} & (p) \text{ ist maximales Ideal} \\ \Longrightarrow \quad & (p) \text{ ist Primideal} \\ \Longleftrightarrow \quad & p \text{ ist Primelement} \\ \Longrightarrow \quad & p \text{ ist irreduzibles Element} \\ \Longleftrightarrow \quad & (p) \text{ ist maximal unter den Hauptidealen} \end{aligned}$$

2.1.7 Beweis

Es seien die fünf Zeilen durchnummeriert.

(1) $\Rightarrow$ (2). Das ist Satz 1.5.16.

(2) $\Leftrightarrow$ (3). Es ist

$$\begin{aligned} & p \text{ prim} \\ \Longleftrightarrow \quad & \Big(p|xy \;\Rightarrow\; p|x \text{ oder } p|y\Big) \quad \text{und} \quad p \in R^\circ \\ \overset{R \text{ Integritätsring}}{\Longleftrightarrow} \quad & \Big(xy \in (p) \;\Rightarrow\; x \in (p) \text{ oder } y \in (p)\Big) \quad \text{und} \quad (p) \neq R \\ \Longleftrightarrow \quad & (p) \text{ Primideal.} \end{aligned}$$

(3) $\Rightarrow$ (4). Angenommen, $p \in R$ ist prim, aber nicht irreduzibel. Da $p \neq 0$ und $p \notin R^\times$, gibt es $r, s \in R^\circ$

$$p \;=\; r \cdot s, \quad \text{insbesondere} \quad p \mid (r \cdot s).$$

Da p prim ist, folgt

$$p \mid r \text{ oder } p \mid s, \qquad \text{O.B.d.A. ersteres}$$

Es gibt also $y \in R$ so, dass

$$p \cdot y \;=\; r.$$

Deswegen gilt

$$p \;=\; r \cdot s \;=\; p \cdot y \cdot s.$$

Es folgt wegen der Kürzungsregel (B_2) $y \cdot s = 1$, also ist s eine Einheit. Widerspruch.

(4) $\Rightarrow$ (5). Es seien p irreduzibel und (a) ein Hauptideal mit $(p) \subsetneqq (a) \subsetneqq R$. Dann sind da die Implikationen

$$\begin{aligned}
& (p) \subsetneqq (a) \subsetneqq R \\
\Longrightarrow\; & a \in R^\circ \text{ und } a \mid p \\
\Longrightarrow\; & a \in R^\circ \text{ und } \exists\, b \in R \text{ mit } ab = p \\
\Longrightarrow\; & \exists\, b \in R^\times \text{ mit } ab = p \\
\Longrightarrow\; & (a) = (p),
\end{aligned}$$

also ist (p) maximal unter den Hauptidealen.

(5) $\Rightarrow$ (4). Es sei (p) maximal unter den Hauptidealen. Wir nehmen an, dass $p = xy$ mit $x \notin R^\times$. Dann ist $(p) \subseteq (x) \neq R$ und somit $(p) = (x)$. Es folgt $xy = p = x\widetilde{y}$ mit $\widetilde{y} \in R^\times$. Die Kürzungsregel ($B_2$) liefert dann $y = \widetilde{y} \in R^\times$.

2.1.8 Beispiel: $R \times R$

Zu einem Integritätsring R betrachten wir das „kartesische Quadrat" $R \times R$ (komponentenweise Verknüpfungen). Wir zeigen, dass $(1,0) \in (R \times R)^{\mathrm{prm}} \setminus (R \times R)^{\mathrm{irr}}$.

Wegen der Zerlegung

$$(1,0) \;=\; (1,0) \cdot (1,0)$$

in zwei Nichteinheiten ist $(1,0)$ nicht irreduzibel.

Ist $(1,0) \mid (a,b) \cdot (c,d)$, so gilt $0 \mid bd$ und damit $bd = 0$. Da R Integritätsring ist, folgt $b = 0$ oder $d = 0$ und damit $(1,0) \mid (a,b)$ oder $(1,0) \mid (c,d)$. Also ist $(1,0)$ prim.

2.1.9 Satz: Teilbarkeit in Integritätsringen II

Es sei R ein Integritätsring.

(i) Es gilt $(\mathrm{Ei}_{\mathrm{prm}})$.

(ii) Es gilt die Implikation $(\mathrm{Ex}_{\mathrm{prm}}) \implies R^{\mathrm{prm}} = R^{\mathrm{irr}}$.

(iii) Es gilt die Implikation $(\mathrm{Ex/Ei}_{\mathrm{irr}}) \implies R^{\mathrm{prm}} = R^{\mathrm{irr}}$.

2.1.10 Beweis

(i) Es seien also

$$a \;=\; p_1 \cdot \ldots \cdot p_r \;=\; q_1 \cdot \ldots q_s,$$

zwei Prim-Produkt-Darstellungen des gleichen Elements $a \in R^\circ$. Wir führen eine Induktion nach der Anzahl r der Faktoren im linken Produkt durch.

$r = 1$. In diesem Fall ist

$$a \;=\; p_1 \;=\; q_1 \cdot \ldots \cdot q_s,$$

Da p_1 prim ist, folgt (O.B.d.A.) $p_1 \mid q_s$. Umgekehrt ist aber auch $q_s \mid p_1$, also $p_1 \sim q_s$. Deshalb ist $q_1 \cdot \ldots \cdot q_{s-1}$ Einheit. Das widerspricht der Irreduzibilität, wenn $s \geq 2$.

$r - 1 \mapsto r$. Wegen $p_r \mid (q_1 \cdot \ldots \cdot q_s)$ gilt, da p_r Primelement ist, (O.B.d.A.) $p_r \mid q_s$.

Gemäß Satz 2.1.6 ist q_s irreduzibel. Es folgt $p_r \sim q_s$ mit $q_s = p_r \cdot u$, $u \in R^\times$.

Weiter folgt

$$(p_1 \cdot \ldots \cdot p_{r-1} - q_1 \cdot \ldots \cdot q_{s-1}u) \cdot p_r \;=\; p_1 \cdot \ldots \cdot p_r - q_1 \cdot \ldots \cdot q_s \;=\; 0,$$

wegen der Nullteilerfreiheit von R und $p_r \neq 0$ ist

$$p_1 \cdot \ldots \cdot p_{r-1} \;=\; q_1 \cdot \ldots \cdot q_{s-2} \cdot (q_{s-1}u).$$

Mit q_{s-1} ist auch $q_{s-1}u$ Primelement.

Darauf wenden wir die Induktionsvoraussetzung an. Es gilt $r - 1 = s - 1$ und

$$\begin{aligned} p_i \;&\sim\; q_{\pi(i)} \quad \text{für} \quad i = 1, \ldots, s-2, \text{wobei } \pi \text{ eine Permutation von } \{1, \ldots, r-1\} \text{ ist.} \\ p_{r-1} \;&\sim\; q_{s-1}u \;\sim\; q_{s-1}. \end{aligned}$$

Daraus folgt $r = s$ und die Existenz einer Permutation von $\{1, \ldots, r\}$ mit der in $(\mathrm{Ei}_{\mathrm{prm}})$ dargestellten Eigenschaft.

(ii), (iii). Dem Satz 2.1.6 kann die Inklusion $R^{\mathrm{prm}} \subseteq R^{\mathrm{irr}}$ entnommen werden.

(ii) Es sei $a \in R$ irreduzibel. Es existieren gemäß $(\mathrm{Ex}_{\mathrm{prm}})$ Primelemente $p_1, \ldots, p_r \in R$ mit

$$a \;=\; p_1 \cdot \ldots \cdot p_r.$$

Da a selbst irreduzibel ist, muss $r = 1$ und $a \sim p_1$ sein. Damit ist a prim.

(iii) Es sei $a \in R$ irreduzibel. Weiter seien $x, y \in R \setminus \{0\}$ mit $a \mid xy$. Es ist zu zeigen, dass $a \mid x$ oder $a \mid y$.

Wir stellen fünf verschiedene Fälle zusammen:

$\boxed{x = 0}$ Es folgt $a \mid x$.

$\boxed{y = 0}$ Es folgt $a \mid y$.

$\boxed{x \in R^\times}$ Es folgt $a \mid y$.

$\boxed{y \in R^\times}$ Es folgt $a \mid x$.

$\boxed{x, y \in R^\circ}$ Es existiert $z \in R$ mit $az = xy$.
Es ist $z \neq 0$, da R Integritätsring, und $z \notin R^\times$, da a irreduzibel. Also $z \in R^\circ$.
Gemäß ($\mathrm{Ex}_{\mathrm{irr}}$) existieren $x_1, \ldots, x_r$, $y_1, \ldots, y_s$, $z_1, \ldots, z_t \in R^{\mathrm{irr}}$ mit

$$a \cdot \underbrace{z_1 \cdot \ldots z_t}_{=z} = \underbrace{x_1 \ldots \cdot x_r}_{=x} \cdot \underbrace{y_1 \cdot \ldots \cdot y_s}_{=y}$$

Gemäß ($\mathrm{Ei}_{\mathrm{irr}}$) ist dann

$$a \sim x_i \quad \text{oder} \quad a \sim y_j$$

für ein $i \in \{1, \ldots, r\}$ oder $j \in \{1, \ldots, s\}$. Damit gilt $a \mid x$ oder $a \mid y$.

2.2 Faktorielle Ringe

2.2.1 Definition und Satz: Faktorieller Ring

Es sei R ein Integritätsring. Die folgenden Aussagen sind äquivalent.

(A) (def) R heißt *faktoriell* (= *gaußsch* = *ZPE Ring* = *UFD*).

(B) Es gilt $(\mathrm{Ex}_{\mathrm{prm}})$.

(C) Es gilt $(\mathrm{Ex/Ei}_{\mathrm{irr}})$.

(D) Es gelten $R^{\mathrm{irr}} = R^{\mathrm{prm}}$ und $(\mathrm{Ex/Ei}_{\mathrm{irr}}) = (\mathrm{Ex/Ei}_{\mathrm{prm}})$.

2.2.2 Beweis

Der Beweis besteht darin, die Aussagen aus Satz 2.1.9 geeignet einzubeziehen.

Aus (B) oder (C) folgt gemäß (iii) bzw. (iv) dieses Satzes $R^{\mathrm{irr}} = R^{\mathrm{prm}}$.

Aus (B) folgt mit (i) dieses Satzes die Aussage $(\mathrm{Ex/Ei}_{\mathrm{prm}})$.

Die Implikationen (D) $\Rightarrow$ (B) und (D) $\Rightarrow$ (C) sind trivial.

2.2.3 Bemerkungen

1. Verwechsle nicht ,,faktorieller Ring" mit ,,Faktorring".
2. Man kann sich den Kopf darüber zerbrechen, ob man die Elemente in $R^{\mathrm{irr}} = R^{\mathrm{prm}}$ prim oder irreduzibel nennt.
   - Im Fall des Ringes $R = \mathbb{Z}$ spricht man von Primelementen.
   - Im Fall eines Ringes $\mathbb{K}[X]$, $\mathbb{K}$ Körper, nennt man die Elemente von $R^{\mathrm{irr}} = R^{\mathrm{prm}}$ irreduzible Polynome.

2.2.4 Nicht-Beispiele

1. Der Kummer-Ring aus Übungsaufgabe A9 (Blatt 3) $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ ist ein Integritätsring, aber nicht faktoriell.

   Die vier Faktoren in

   $$2 \cdot 3 \;=\; 6 \;=\; (1+i\sqrt{5})(1-i\sqrt{5}).$$

   sind alle irreduzibel, aber nicht prim. Die Zerlegung in irreduzible Faktoren ist nicht eindeutig.

   Wir haben weiter gesehen, dass $\mathcal{M}_{\mathrm{ggT}}(9, 6+3\sqrt{-5}) = \varnothing$.

2. Der Ring R der auf $\mathbb{C}$ holomorphen Funktionen ist ein Integritätsring (FTH1, Identitätssatz), aber nicht faktoriell. Die linearen Funktion $z - c$, $c \in \mathbb{C}$ sind genau die irreduziblen = primen Elemente.

   Die Funktion $\sin(z)$ hat jede lineare Funktion $z - k\pi$, $k \in \mathbb{Z}$, als Teiler, kann also nicht als Produkt von (endlich vielen) Primelementen dargestellt werden.

   Formal zusammengefasst, es gilt $R^{\mathrm{prm}} = R^{\mathrm{irr}}$, aber nicht $(\mathrm{Ex}_{\mathrm{prm}}) = (\mathrm{Ex}_{\mathrm{irr}})$.

2.2.5 Definition: Vertretersystem im faktoriellen Ring

Es sei R ein faktorieller Ring. Wir nennen eine Teilmenge $P \subseteq R^{\mathrm{prm}}$ kurz ein *Vertretersystem*, wenn es ein Vertretersystem der Äquivalenzklassen von Primelementen bzgl. der Assoziiertheit ist, d.h.

$$p \text{ Primelement} \quad \Longrightarrow \quad \text{Es ex. genau ein } \widetilde{p} \in P \text{ mit } p \sim \widetilde{p}.$$

Es ist ziemlich praktisch und leichter verständlich, in faktoriellen Ringen von vornherein ein Vertretersystem P zur Verfügung zu haben. Die Teilbarkeitstheorie lässt sich dann mehr auf einzelne Elemente als auf bestimmte Teilmengen gründen.

Im folgenden sei also in einem faktoriellen Ring R ein Vertretersystem P ausgewählt, wir werden aber immer wieder darauf hinweisen.

2.2.6 Beispiele

1. Im faktoriellen Ring $\mathbb{Z}$ kann die Menge der (positiven) Primzahlen als Vertretersystem P ausgewählt werden.
2. Im faktoriellen Ring $\mathbb{R}[X]$ der Polynome mit reellen Koeffizienten bilden die normierten irreduziblen Polynome ein Vertretersystem.
3. Im faktoriellen Ring $\mathbb{C}[X]$ der Polynome mit komplexen Koeffizienten bilden aufgrund des Fundamentalsatzes der Algebra die linearen normierten Polynome $x - c$, $c \in \mathbb{C}$, ein Vertretersystem.

2.2.7 Satz: Eindeutige Primfaktorzerlegung im faktoriellen Ring

Es sei R ein faktorieller Ring mit Vertretersystem P.

Es existiert zu jedem $a \in R \setminus \{0\}$ eine eindeutige *Primfaktorzerlegung (PFZ)*.
Das bedeutet, es existiert genaue eine Abbildung

$$\alpha : \left\{ \begin{array}{rcl} P & \to & \mathbb{N}_0 \\ p & \mapsto & \alpha(p), \end{array} \right. \qquad \text{(nur an endlich vielen Stellen ungleich Null)}$$

und genau ein $u \in R^\times$ so, dass

$$a \;=\; u \cdot \prod_{p \in P} p^{\alpha(p)}.$$

2.2.8 Beweis

Das sind direkte Konsequenzen der Eigenschaft ($\mathrm{Ex/Ei}_{\mathrm{prm}}$) eines faktoriellen Rings.

2.2.9 Definition und Satz: ggT und kgV in faktoriellen Ringen

Es sei R ein faktorieller Ring mit Vertretersystem P.

Zu jedem Element einer endlichen Teilmenge $A = \{a_1, \ldots, a_n\} \in R \setminus \{0\}$ betrachten wir die Primfaktorzerlegung wie oben

$$a_j \;=\; u_j \cdot \prod_{p \in P} p^{\alpha_j(p)}.$$

Es gelten die folgenden Aussagen

(i) Die Menge $\mathcal{M}_{\mathrm{ggT}}(A)$ ist nicht leer.

Das gemäß Satz 2.2.7 (i) eindeutige in ihr enthaltene Element nennen wir **den** *größten gemeinsamen Teiler von* A, es ist

$$\mathrm{ggT}(A) \;=\; \prod_{p \in P} p^{\min\{\alpha_j(p), j=1,\ldots,n\}} \;\in\; \mathcal{M}_{\mathrm{ggT}}(A).$$

(ii) Die Menge $\mathcal{M}_{\mathrm{kgV}}(A)$ ist nicht leer. Das gemäß Satz 2.2.7 (i) eindeutige in ihr enthaltene Element nennen wir **das** *kleinste gemeinsame Vielfache von* A, es ist

$$\mathrm{kgV}(A) \;=\; \prod_{p \in P} p^{\max\{\alpha_j(p), j=1,\ldots,n\}} \;\in\; \mathcal{M}_{\mathrm{kgV}}(A).$$

2.2.10 Satz: ggT und kgV zweier Elemente

Es sei R ein faktorieller Ring mit Vertretersystem P.

Zu zwei Elementen $a, b \in R \setminus \{0\}$ betrachten wir die Primfaktorzerlegungen

$$a \;=\; u \cdot \prod_{p \in P} p^{\alpha(p)}, \qquad b \;=\; v \cdot \prod_{p \in P} p^{\beta(p)}.$$

Dann gelten die folgenden Aussagen

(i) $a|b \quad\Longleftrightarrow\quad \alpha(p) \;\leq\; \beta(p)$ für alle $p \in P$.

(ii) $a \sim b \quad\Longleftrightarrow\quad \alpha(p) \;=\; \beta(p)$ für alle $p \in P$.

(iii) Für $a, b \in R \setminus \{0\}$ gilt

$$a \cdot b \;\sim\; \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b).$$

2.2.11 Teilbarkeit im faktoriellen Ring

Es sei R ein faktorieller Ring. Für $a, b, c \in R \setminus \{0\}$ gilt die Implikation

$$\left.\begin{array}{l} a, b \text{ teilerfremd} \\ a \mid c \\ b \mid c \end{array}\right\} \quad\Longrightarrow\quad (ab) \mid c.$$

Dabei heißen zwei Elemente $a, b \in R$ *teilerfremd*, wenn $\mathcal{M}_{\mathrm{ggT}}(a,b) = R^\times$.

2.2.12 Beweis

Wir wählen ein Vertretersystem P. Die Elemente a, b, c haben die eindeutigen PFZen

$$\begin{aligned} a &= u \cdot \prod_{p \in P} p^{\alpha(p)} \\ b &= v \cdot \prod_{p \in P} p^{\beta(p)} \\ c &= w \cdot \prod_{p \in P} p^{\gamma(p)}. \end{aligned}$$

Da a, b teilerfremd, ist $\alpha(p) = 0$ oder $\beta(p) = 0$ für alle $p \in P$.

Es ist dann weiter für alle $p \in P$

$$\left\{ \begin{array}{c} a, b \text{ teilerfremd} \\ a \mid c \\ b \mid c \end{array} \right\} \quad \Longrightarrow \quad \left\{ \begin{array}{c} \alpha(p) = 0 \text{ oder } \beta(p) = 0 \\ \alpha(p) \leq \gamma(p) \\ \beta(p) \leq \gamma(p) \end{array} \right\}$$

$$\Longrightarrow \quad \alpha(p) + \beta(p) \leq \gamma(p)$$

und deswegen $(ab) \mid c$.

2.2.13 ggT = kgV eines einzelnen Elements

Es sei R ein faktorieller Ring mit Vertretersystem P.

Eine nicht so wichtige und weniger gebräuchliche, aber nützliche Bemerkung ist noch, dass für ein einzelnes Element $a \in R \setminus \{0\}$

$$\operatorname{ggT}(a) \;=\; \operatorname{kgV}(a) \;=\; \prod_{p \in P} p^{\alpha_j(p)} \;\sim\; a.$$

Es wird also die Einheit von a ,,abgestreift", es bleibt nur die Darstellung als Produkt von Elementen aus P übrig.

Man überlege, dass

$$\begin{aligned} \operatorname{ggT}(a \cdot b) &= \operatorname{ggT}(a) \cdot \operatorname{ggT}(b) \\ \operatorname{kgV}(a \cdot b) &= \operatorname{kgV}(a) \cdot \operatorname{kgV}(b). \end{aligned}$$

2.3 Noethersche Ringe

2.3.1 Definition und Satz: Noetherscher Ring

Für einen uk Ring R sind die folgenden Aussagen äquivalent:

(A) R heißt *noetherscher Ring*

(B) Jedes Ideal I in R ist endlich erzeugt.

(C) Jede wachsende Kette

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

von Idealen in R wird irgendwann *stationär*, d.h. genauer, es existiert ein $n \in \mathbb{N}$ so, dass

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n = I_{n+1} = I_{n+2} = \dots$$

(D) In jeder nichtleeren Menge M von Idealen in R existiert ein maximales Element J, d.h. es gilt die Implikation

$$I \in M, \quad J \subseteq I \quad \Longrightarrow \quad J = I.$$

Beachte, dass ein **maximales Element** in einer solchen Menge nicht notwendig ein **maximales Ideal** ist. Das maximale Element kann durchaus gleich dem Nullideal oder gleich dem ganzen Ring sein.

2.3.2 Beweis

(B) $\Rightarrow$ (C). Es sei also eine wachsende Kette $(I_j)_{j\in\mathbb{N}}$ gemäß (C) vorgegeben. Die Vereinigung

$$I := \bigcup_{j=1}^{\infty} I_j$$

ist selbst ein Ideal. (Übung)

Dieses Ideal besitzt nach Voraussetzung (B) ein endliches Erzeugendensystem $\{a_1, \dots, a_m\}$.

Zu jedem $j \in \{1, \dots, m\}$ gibt es ein $n_j \in \mathbb{N}$ mit $a_j \in I_{n_j}$.

Ist nun $n := \max\{n_j \mid j \in \{1, \dots, m\}\}$, so ist $\{a_1, \dots, a_m\} \subseteq I_n$.

Für $k \geq n$ folgt

$$I_n \subseteq I_k \subseteq I = (a_1, \dots, a_m) \subseteq I_n,$$

also $I_k = I_n$. Die Kette wird bei n stationär.

(C) $\Rightarrow$ (D). Gäbe es eine nichtleere Menge M von Idealen ohne maximales Element, so könnte man darin eine wachsende Kette von Idealen rekursiv definieren, die nicht stationär wird.

(D) $\Rightarrow$ (B). Es sei I ein Ideal in R. Wir definieren die Menge aller endlich erzeugten Ideale, die in I enthalten sind,

$$M_{\subseteq I} \;:=\; \{J \subseteq R \mid J \text{ ist endlich erzeugtes Ideal mit } J \subseteq I\}.$$

M ist wegen $\{0\} \in M$ nichtleer, besitzt also nach (D) ein maximales Element $J_{\max} \subseteq I$. $J_{\max}$ ist selbst endlich erzeugt, es sei $J_{\max} = (a_1, \ldots, a_n)$.

Wäre $J_{\max} \subsetneq I$, so würde ein $b \in I \setminus J_{\max}$ existieren und dann wäre

$$(a_1, \ldots, a_n, b) \;=\; (J_{\max}, b) \;\subseteq\; I$$

ein Ideal in $M_{\subseteq I}$, das $J_{\max}$ echt umfasst. Widerspruch.

Damit ist $I = J_{\max}$ endlich erzeugt.

2.3.3 Bemerkung

Diese drei Charakterisierungen von noetherschen Ringen durch (innere und äußere) Eigenschaften von Idealen finden sich analog auch in der Topologie wieder. So gibt es auch noethersche topologischer Räume; hier ist die Rolle der Ideale durch die der offenen Teilmengen ersetzt.

2.4 Hauptidealringe

2.4.1 Definition: Hauptidealring

Ein uk Ring R heißt *Hauptidealring (HIR)*, wenn

- er ein Integritätsring ist und
- jedes Ideal I in R ein Hauptideal ist.

2.4.2 Teilbarkeit in Hauptidealringen

Es sei R ein Hauptidealring und $p \in R \setminus \{0\}$. Dann gelten die folgenden Äquivalenzen.

$$
\begin{aligned}
& (p) \text{ ist maximales Ideal} \\
\iff\ & (p) \text{ ist Primideal} \\
\iff\ & p \text{ ist Primelement} \\
\iff\ & p \text{ ist irreduzibles Element} \\
\iff\ & (p) \text{ ist maximal unter den Hauptidealen}
\end{aligned}
$$

2.4.3 Beweis

Die Abwärts-Implikationen wurden alle in Satz 2.1.6 gezeigt. Die Implikation (5. Zeile) $\Rightarrow$ (1. Zeile) ist trivial, da in einem Hauptidealring alle Ideale Hauptideale sind.

2.4.4 Satz: Hauptidealring ist faktoriell

Ein Hauptidealring R ist faktoriell.

2.4.5 Beweis

(1) Gemäß Definition 2.4.1 ist der Hauptidealring R ein Integritätsring.

(2) Dem Satz 2.4.2 ist zu entnehmen, dass $R^{\mathrm{prm}} = R^{\mathrm{irr}}$.

(3) Es sei

$$M \;:=\; \{x \in R^\circ \,|\, x \text{ lässt sich nicht als Produkt von Primelementen darstellen}\}.$$

(4) Wir definieren eine ,,Wähle-Teiler-Abbildung"

$$T : \left\{ \begin{array}{rcl} M & \to & M \\ x & \mapsto & \text{Echter Teiler von } x \end{array} \right.$$

Da x nicht prim und damit nicht irreduzibel ist, existiert ein solcher echter Teiler. Dieser muss wieder in M sein.

(5) Die Annahme ,,R nicht faktoriell" ist gleichbedeutend damit, dass ein $a \in M$ existiert.

(6) Es kommt eine aufsteigende Kette von nicht-leeren Idealen

$$(a) \;\subseteq\; (T(a)) \;\subseteq\; (T^2(a)) \;\subseteq\; (T^3(a)) \;\subseteq\; \ldots$$

zustande, die nach Satz 2.3.1 stationär wird. Es existiert also ein $n \in \mathbb{N}$ so, dass

$$(T^n(a)) \;=\; (T^{n+1}(a)).$$

(7) Nach Satz 1.5.10 (ii) bedeutet dies aber, dass

$$T^n(a) \;\sim\; T^{n+1}(a) \;=\; T(T^n(a)).$$

(8) Das Element $T^{n+1}(a)$ ist also gemäß Definition von T sowohl ein echter Teiler von $T^n(a)$ als auch assoziiert dazu. Widerspruch.

(9) Es ist also $M = \varnothing$ und jedes $x \in R^\circ$ lässt sich als Produkt von Primelementen darstellen. Das ist die Eigenschaft $(\mathrm{Ex}_{\mathrm{prm}})$ aus Definition und Satz 2.2.1.

2.4.6 Satz: Operationen mit Hauptidealen

Es seien R ein Hauptidealring mit Vertretersystem P der Primelemente und $a, b \in R$.

(i) Dann gilt

$$\begin{aligned}(a)\cdot(b) &= (a\cdot b)\\ (a)\cap(b) &= (\mathrm{kgV}(a,b))\\ (a)+(b) &= (\mathrm{ggT}(a,b)).\end{aligned}$$

(ii) Tatsächlich gilt die erste Aussage von (i) in allgemeinen uk Ringen, die zweite in allgemeinen faktoriellen Ringen.

(iii) Da die in (i) angegebenen Verknüpfungen für Ideale bzw. Elemente eines Hauptidealrings alle assoziativ sind, gelten die drei Aussagen auch für die Verknüpfungen von endlich vielen Idealen bzw. Elementen.

2.4.7 Beweis

(1) Es ist

$$\begin{aligned}(a)\cdot(b) &= \{\sum_{\text{endl.}} a_j b_j \mid a_j \in (a), b_j \in (b)\} = \{\sum_{\text{endl.}} (\ell_j a)(k_j b) \mid \ell_j, k_j \in R\}\\ &= \{(\sum_{\text{endl.}} \ell_j k_j) ab \mid \ell_j, k_j \in R\} \subseteq (a\cdot b) \subseteq (a)\cdot(b).\end{aligned}$$

(2) Sind

$$a = u\cdot\prod_{p\in P} p^{\alpha(p)}, \qquad b = v\cdot\prod_{p\in P} p^{\beta(p)},$$

die eindeutigen Primfaktorzerlegungen von a und b bzgl. des Vertretersystems P, so gilt

$$\begin{aligned}(a) &= \{w\cdot\prod_{p\in P} p^{\gamma_p} \mid w\in R^\times,\ \gamma_p\in\mathbb{N}_0 \text{ mit } \gamma_p \geq \alpha(p)\}\\ (b) &= \{w\cdot\prod_{p\in P} p^{\delta_p} \mid w\in R^\times,\ \delta_p\in\mathbb{N}_0 \text{ mit } \delta_p \geq \beta(p)\}\end{aligned}$$

und dann

$$\begin{aligned}(a)\cap(b) &= \{w\cdot\prod_{p\in P} p^{\varepsilon_p} \mid w\in R^\times,\ \varepsilon_p\in\mathbb{N}_0 \text{ mit } \varepsilon_p \geq \max\{\alpha(p),\beta(p)\}\}\\ &= (\mathrm{kgV}(a,b)).\end{aligned}$$

(3) Da R Hauptidealring ist, existiert $c\in R$ mit $(a)+(b)=(c)$.

Wir können dann folgern

$$\begin{aligned}(a)\subseteq(a)+(b)\subseteq(c) &\implies c\mid a\\ (b)\subseteq(a)+(b)\subseteq(c) &\implies c\mid b\end{aligned}$$

und damit $c\in\mathcal{M}_{\mathrm{gT}}(a,b)$.

Ist $x \in \mathcal{M}_{\mathrm{gT}}(a,b)$, so gibt es wegen $(c) \subseteq (a)+(b)$ Elemente $r_1, s_1, r_2, s_2 \in R$ mit

$$c \;=\; r_1 a + r_2 b \;=\; r_1 s_1 x + r_2 s_2 x \;=\; (r_1 s_1 + r_2 s_2)x,$$

also $x \mid c$ und damit $c \in \mathcal{M}_{\mathrm{gV}}(\mathcal{M}_{\mathrm{gT}}(a,b))$.

Insgesamt ist also $c \in \mathcal{M}_{\mathrm{ggT}}(a,b)$.

Damit ist $\mathrm{ggT}(a,b) \sim c$ und es gilt

$$(\mathrm{ggT}(a,b)) \;=\; (c) \;=\; (a)+(b).$$

2.4.8 Lemma von Bezout

Es sei R ein Hauptidealring, $A = \{a_1, \ldots, a_n\} \subseteq R$. Dann

(i) Betrachte die folgenden Aussagen über ein $d \in R$.

(G) $d \in \mathcal{M}_{\mathrm{ggT}}(A)$.

(E) $(A) = (d)$.

(L) Es existieren $r_1, \ldots, r_n \in R$ so, dass $d = r_1 a_1 + \ldots + r_n a_n$

Dann gelten die Implikationen

$$\text{(G)} \quad \Longleftrightarrow \quad \text{(E)} \quad \Longrightarrow \quad \text{(L)}.$$

(ii) Die folgenden Aussagen sind äquivalent.

(G) A ist teilerfremd.

(E) Es ist $(A) = R$.

(L) Es gibt $r_1, \ldots, r_n \in R$ so, dass $1 = r_1 a_1 + \ldots + r_n a_n$.

2.4.9 Beweis

(i) (G) $\Leftrightarrow$ (E). Aufgrund von 2.4.6 (i,iii) gilt

$$(A) = (a_1) + \ldots + (a_n) = (\mathrm{ggT}(A))$$

und es ist weiter für $d \in R$

$$(\mathrm{ggT}(A)) \;=\; (d) \quad \Longleftrightarrow \quad \mathrm{ggT}(A) \sim d \quad \Longleftrightarrow \quad d \in \mathcal{M}_{\mathrm{ggT}}(A).$$

(i) (E) $\Rightarrow$ (L). Aus (E) folgt $d \in (A)$. Wende dann die Definition von „A erzeugt (A)" an.

(ii) Setzt man in (i) $d = 1$, so erhält man die Implikationen (G) $\Leftrightarrow$ (E) $\Rightarrow$ (L) in (ii). Die Implikation (L) $\Rightarrow$ (E) ist klar, da aus (L) folgt: $R = (1) \subseteq (A)$.

2.4.10 Beispiele

1. Es sei $\mathbb{R}[X,Y]$ der Ring der Polynome in zwei Variablen mit reellen Koeffizienten. Die beiden Polynome X und Y sind teilerfremd, das Polynom $1 \in \mathcal{M}_{\mathrm{ggT}}(X,Y)$ lässt sich aber nicht wie in Aussage (iii)/(L) darstellen. Also kann $\mathbb{R}[X,Y]$ kein Hauptidealring sein.

2. Es sei $\mathbb{Z}[X]$ der Ring der Polynome in einer Variablen mit ganzzahligen Koeffizienten. Die beiden Polynome 2 und X sind teilerfremd, das Polynom $1 \in \mathcal{M}_{\mathrm{ggT}}(2,X)$ lässt sich aber nicht wie in Aussage (iii)/(L) darstellen. Also kann $\mathbb{Z}[X]$ kein Hauptidealring sein.

2.5 Euklidische Ringe

2.5.1 Definition und Satz: Euklidischer Ring

Ein uk Ring R heißt *euklidisch*, wenn er ein Integritätsring ist und es eine *euklidische Bewertung*

$$E : \left\{ \begin{array}{rcl} R \setminus \{0\} & \to & \mathbb{N}_0 \\ x & \mapsto & E(x) \end{array} \right.$$

gibt mit den folgenden beiden Eigenschaften:

- „Division-mit-Rest-Eigenschaft": Zu zwei Elementen $x \in R$, $y \in R \setminus \{0\}$ gibt es zwei Elemente $q, r \in R$ so, dass

$$x \;=\; q \cdot y + r \qquad \text{und} \qquad E(r) \;<\; E(y), \text{ falls } r \neq 0.$$

- Es ist für $x, y \in R \setminus \{0\}$

$$E(xy) \;\geq E(x).$$

2.5.2 Bemerkung

In der Literatur finden sich zahlreiche andere Bezeichnungen für die euklidische Bewertung: euklidische Funktion, euklidische Norm(-funktion), Grad-Abbildung oder Gradfunktion.

Teilweise weisen die Definitionen von euklidischem Ring bzw. Eukldischer Bewertung auch geringfügige Unterschiede auf, die sich in den unterschiedlichen Namen niederschlagen.

2.5.3 Beispiele

1. $\mathbb{Z}$ ist ein euklidischer Ring, wenn man als Abbildung $E(z) = |z|$ wählt. In diesem Fall kann die Division-mit-Rest-Gleichung auch „schulnäher" geschrieben werden als

$$x \;=\; q \cdot y + r \quad \Longleftrightarrow \quad x : y \;=\; q : y + r \quad \Longleftrightarrow \quad x : y \;=\; q \,\mathrm{R}\, r.$$

   Die bereits in der Grundschule erarbeitete Division-mit-Rest wird hier von den natürlichen Zahlen auf alle ganzen Zahlen erweitert.

   Beachte, dass die beiden Zahlen q, r nicht eindeutig sein müssen. So ist beispielsweise in $\mathbb{Z}$

$$11 \;=\; 3 \cdot 3 + 2 \;=\; 4 \cdot 3 + (-1).$$

   Hier liesse sich die Eindeutigkeit mit der Zusatzforderung $r \geq 0$ erzwingen. Beachte aber, dass in allgemeinen Ringen i.a. keine lineare Ordnung definiert ist.

2. Im Ring der reellen Polynome $\mathbb{R}[x]$ ist mit $E(p) = \operatorname{grad} p$ die Struktur eines euklidischen Rings gegeben. Die Division-mit-Rest entspricht der aus der Schule bekannten Polynomdivision.

3. Der Ring der gaußschen Zahlen ist mit $E(m+ni) = m^2 + n^2$ ein euklidischer Ring.

4. Die Ringe

$$\mathbb{Z} + \mathbb{Z}\sqrt{-2}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{-1}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{+2}, \qquad \mathbb{Z} + \mathbb{Z}\sqrt{+3}$$

   sind unter der Grad-Abbildung $E(x) = N(x)$ euklidische Ringe.

5. Der Teilring $R = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-19}}{2} \subseteq \mathbb{C}$ ist ein Hauptidealring, es gibt aber keine euklidische Bewertung so, dass R damit zu einem euklidischen Ring würde.

   Der Beweis dieser beiden Aussagen ist aufwändig.

6. Jeder Körper $\mathbb{K}$ ist ein euklidischer Ring. Wähle als euklidische Bewertung $E(x) = 1$ für alle $x \in \mathbb{K} \setminus \{0\}$.

2.5.4 Satz: Euklidischer Ring ist Hauptidealring

Ein euklidischer Ring ist ein Hauptidealring.

2.5.5 Beweis

(1) Per definitionem sind euklidische Ringe Integritätsringe.

(2) Es sei weiter $I \subseteq R$ ein nicht-leeres Ideal ungleich dem Nullideal.

(3) Wir betrachten die Bildmenge der euklidischen Funktion E auf $I \setminus \{0\}$

$$\{n \in \mathbb{N}_0 \mid \exists_{x \in I \setminus \{0\}} : n = E(x)\}$$

und wählen ein $a \in I \setminus \{0\}$ mit $E(a) \leq E(x)$ für alle $x \in I \setminus \{0\}$.

Wir betrachten das Hauptideal $(a) \subseteq I$.

(4) Ist nun $x \in I$, so existieren $q, r \in R$ mit

$$x \;=\; qa + r, \qquad \text{wobei } E(r) < E(a).$$

Es ist $r = x - qa \in I$, deswegen $E(r) \geq E(a)$ oder $r = 0$, ersteres bedeutet eine Widerspruch.

Es folgt $x = qa \in (a)$ und damit $I \subseteq (a)$. Insgesamt ist $I = (a)$ ein Hauptideal.

2.5.6 Der Euklidische Algorithmus

Ein euklidischer Ring R ist ein Hauptidealring und demzufolge faktoriell. Es sei P ein Vertretersystem der Primelemente von R.

In R kann der so genannte euklidische Algorithmus zur Bestimmung des $\mathrm{ggT}(a, b)$ von zwei Elementen aus $a, b \in R^\circ$ herangezogen werden.

Vergleiche dazu Kapitel XIII, Vorlesung Danz WS 2018/19.

Der euklidische Algorithmus stellt auch eine Methode bereit, die beiden Elemente $r, s \in R$ innerhalb der gemäß Lemma von Bezout 2.4.8 (i) existierenden Darstellung

$$\mathrm{ggT}(a, b) \;=\; r \cdot a + s \cdot b$$

zu ermitteln.

2.6 Körper

2.6.1 Definition und Satz: Körper

Es sei R ein uk Ring. Dann sind die folgenden Aussagen äquivalent.

(A) (def) Der Ring R heißt *Körper*.

(B) Jedes Element aus $R \setminus \{0\}$ ist eine Einheit.
Andere Sichtweise: Die Menge R° ist leer.

(C) $\{0\}$ ist ein maximales Ideal in R.
Andere Sichtweise: Die Ideale $\{0\}$ und R sind die einzigen Ideale in R.

2.6.2 Beweis

Die Äquivalenz $(B) \Leftrightarrow$ (C) erschließt sich aus den Definitionen in Abschnitt 1.3.1.

(B) $\Rightarrow$ (C). Ist $I \neq \{0\}$ ein Ideal in R, so enthält I ein Element ungleich Null, das gemäß (B) eine Einheit sein muss. Ein Ideal mit Einheit ist aber immer der ganze Ring.

(C) $\Rightarrow$ (B). Sei $x \in R \setminus \{0\}$. Dann ist $(x) = R$. Dann gibt es aufgrund der Definition von ,,Erzeugung" ein $y \in R$ mit $xy = 1$, also ist x Einheit.

2.6.3 Satz

Es seien S ein uk Ring und I ein Ideal in S. Dann gilt

$$I \text{ ist ein maximales Ideal in } S \quad \Longleftrightarrow \quad S/I \text{ ist ein Körper.}$$

2.6.4 Beweis

Der Beweis besteht in der folgenden Äquivalenzkette

$$\begin{aligned}
& I \text{ ist ein maximales Ideal in } S \\
\Longleftrightarrow\ & S \text{ und } I \text{ sind die einzigen Ideale in } S, \text{ die } I \text{ enthalten} \\
& \text{(Korrespondenzsatz 1.6.6)} \\
\Longleftrightarrow\ & S/I \text{ und } I/I = \{0\} \text{ sind die einzigen Ideale in } S/I \\
& \text{(Echte Ideale enthalten Elemente aus } R^\circ\text{)} \\
\Longleftrightarrow\ & S/I \text{ ist ein Körper.}
\end{aligned}$$

Zur Übung sei ein Beweis ohne Benutzung des Korrespondenzsatzes empfohlen.

2.6.5 Beobachtung

Mit Hilfe der Charakterisierung von Körpern und Integritätsringen als Faktorringen kann man die Aussage ,,in einem uk Ring R ist jedes maximale Ideal I ein Primideal" aus Satz 1.5.16 (i) erneut beweisen:

$$\begin{aligned}
& I \text{ maximales Ideal} \\
\Longleftrightarrow\ & R/I \text{ ist Körper} \\
\Longrightarrow\ & R/I \text{ ist Integritätsring} \\
\Longleftrightarrow\ & I \text{ ist Primideal.}
\end{aligned}$$

2.7 Quotientenkörper

2.7.1 Satz und Definition

Es sei R ein Integritätsring. Die Menge $\{0\}$ ist ein Primideal und deshalb die Menge $R \setminus \{0\}$ multiplikativ abgeschlossen.

(i) Es existiert ein Körper $\operatorname{Quot} R$, der den Ring enthält. Das heißt genauer, dass ein injektiver Ringhomomorphismus $\iota : R \to \operatorname{Quot} R$ existiert.

(ii) Der Körper und der Ringhomomorphismus sind bis auf Isomorphie durch die folgende Eigenschaft eindeutig bestimmt:

Sind K irgendein Körper und $\varphi : R \to K$ ein injektiver Ringhomomorphismus, so kann dieser wie folgt ,,gehoben" werden: Es existiert genau ein injektiver Ringhomomorphismus $\Phi : \operatorname{Quot} R \to K$ mit $\varphi = \Phi \circ \iota$.

Der Körper $\operatorname{Quot} R$ heißt *Quotientenkörper* zu R, der injektive Ringhomomorphismus ι heißt *kanonische Einbettung*.

2.7.2 Beweis

(i) Wir beschreiben hier, wie $\operatorname{Quot} R$ und ι definiert werden. Die elementaren Nachrechnungen bestimmter Eigenschaften werden weggelassen.

(0) Die Menge $\{0\}$ ist ein Primideal und deshalb die Menge $S = R \setminus \{0\}$ multiplikativ abgeschlossen.

(1) Auf dem kartesischen Produkt $R \times S$ wird wie folgt eine Relation definiert

$$(r, s) \sim (\widetilde{r}, \widetilde{s}) \quad \Longleftrightarrow \quad r \cdot \widetilde{s} = \widetilde{r} \cdot s.$$

(2) Durch Nachrechnen zeigt man, dass das eine Äquivalenzrelation ist.

Es sei dann $\operatorname{Quot} R$ die Menge der Äquivalenzklassen.

Wir bezeichnen die Äquivalenzklasse, in der (r, s) enthalten ist, mit $[r, s]$ oder (schulisch-anschaulicher) mit $\frac{r}{s}$.

(3) Auf $\operatorname{Quot} R$ definieren wir Addition und Multiplikation wie folgt:

$$\begin{aligned} [r, s] + [t, u] &:= [ru + ts, su] \\ [r, s] \cdot [t, u] &:= [rt, su]. \end{aligned}$$

Man überlege, dass diese Verknüpfungen wohldefiniert (also unabhängig von den verschiedenen Elementen in ein- und derselben Äquivalenzklasse) ist.

(4) Nullelement und Einselement sind gegeben durch $[0, 1]$ bzw. $[1, 1]$. Die inversen Elemente sind, wie man nachrechnen kann,

$$\begin{aligned} -[r, s] &= [-r, s] \qquad \forall r \in R, s \in S, \\ [r, s]^{-1} &= [s, r] \qquad \forall r, s \in S. \end{aligned}$$

(5) Der Ringhomomorphismus ι ist gegeben durch

$$\iota : \left\{ \begin{array}{rcl} R & \to & \operatorname{Quot} R \\ r & \mapsto & [r, 1] \end{array} \right.$$

Er ist injektiv, da

$$\Big((r,1)\in[0,1] \quad\Longrightarrow\quad r=0\Big) \quad\Longrightarrow\quad \varphi^{-1}([0,1])=\{0\}.$$

(ii)

(0) Wir definieren

$$\Phi:\left\{\begin{array}{rcl}\operatorname{Quot} R & \to & K\\ [r,s] & \mapsto & \varphi(r)\cdot\varphi(s)^{-1}.\end{array}\right.$$

(1) Sind $r,\widetilde{r}\in R$, $s,\widetilde{s}\in S$ mit $(r,s)\sim(\widetilde{r},\widetilde{s})$, so gilt

$$\widetilde{r}\cdot s \;=\; r\cdot\widetilde{s} \quad\Longrightarrow\quad \varphi(\widetilde{r})\cdot\varphi(s) \;=\; \varphi(r)\cdot\varphi(\widetilde{s})$$

und deshalb

$$\Phi([\widetilde{r},\widetilde{s}]) \;=\; \varphi(\widetilde{r})\cdot\varphi(\widetilde{s})^{-1} \;=\; \varphi(r)\cdot\varphi(s)^{-1} \;=\; \Phi([r,s]).$$

Das bedeutet, dass Φ wohldefiniert ist.

(2) Rechne nach, dass Φ ein Ringhomomorphismus ist.

(3) Aufgrund von $\Phi([1,1])=1$ ist $[1,1]\notin\ker\Phi$. Damit kann das Ideal $\ker\Phi$ im Körper $\operatorname{Quot} R$ nur das Null-Ideal sein. Also ist Φ injektiv.

(4) Wären Φ und Φ' zwei ,,Hebungen" von φ auf $\operatorname{Quot} R$, so würde für $r\in R$, $s\in S$ folgen:

$$\begin{aligned}\Phi'([r,s]) &= \Phi'([r,1]\cdot[1,s]) \;=\; \Phi'([r,1])\cdot\Phi'([1,s])\\ &= \varphi(r)\cdot\varphi(s)^{-1}\\ &= \Phi([r,1])\cdot\Phi([s,1])^{-1} \;=\; \Phi([r,1])\cdot\Phi([1,s]) \;=\; \Phi([r,1]\cdot[1,s])\\ &= \Phi([r,s]).\end{aligned}$$

2.7.3 Schreibweise mit Bruchstrichen

Die Äquivalenzklassen $[a,b]$ in dem Quotientenkörper $\operatorname{Quot} R$ werden wegen der Vertrautheit aus Schule und Alltagsleben viel suggestiver als geschrieben:

$$\frac{r}{s} \;:=\; [r,s], \qquad r\in R,\;\; s\in R\setminus\{0\},$$

Man arbeite den obigen Beweis noch einmal unter Benutzung dieser Schreibweise durch und mache sich dabei die folgenden Gesetze der Bruchrechnung bewusst. Für $r,\widetilde{r}\in R$ und $s,\widetilde{s}\in R\setminus\{0\}$ gelten die Implikationen und Rechengesetze

$$\begin{aligned}\frac{r}{s} \;=\; \frac{\widetilde{r}}{\widetilde{s}} \quad&\Longleftrightarrow\quad r\cdot\widetilde{s} \;=\; \widetilde{r}\cdot s\\ \frac{r}{s}\pm\frac{\widetilde{r}}{\widetilde{s}} \quad&=\quad \frac{r\cdot\widetilde{s}\pm\widetilde{r}\cdot s}{s\cdot\widetilde{s}}\\ \frac{r}{s}\cdot\frac{\widetilde{r}}{\widetilde{s}} \quad&=\quad \frac{r\cdot\widetilde{r}}{s\cdot\widetilde{s}}\\ \frac{r}{s}\cdot\left(\frac{\widetilde{r}}{\widetilde{s}}\right)^{-1} \quad&=\quad \frac{r\cdot\widetilde{s}}{\widetilde{r}\cdot s}.\end{aligned}$$

Eine lineare Ordnung ($\leq$) ist auf einem Integritätsring R — und damit auch auf dem Quotientenkörper Quot R — nicht definiert.

Beachte, dass Begriffe wie ,,Hauptnenner" oder ,,soweit wie möglich gekürzt" auf dem Begriff des ggT beruhen — und deshalb nur sinnvoll sind, wenn R ein faktorieller Ring (mit Vertretersystem P) ist. Vgl. weiter unten Abschnitt 2.7.5.

2.7.4 Beispiele

1. Es ist $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$ (Schule JGS 6).
2. Es ist $\mathrm{Quot}(\mathbb{R}[x])$ der ,,Körper der gebrochen-rationalen Funktionen mit reellen Koeffizienten" (Schule JGS 11).
3. Es ist $\mathrm{Quot}(\mathbb{Z} + i\mathbb{Z}) = \mathbb{Q} + i\mathbb{Q}$ der Körper der gaußschen Zahlen.
4. Ist R der Integritätsring der auf einem Gebiet $\Omega \subseteq \mathbb{C}$ holomorphen Funktionen, so kann man (mit Hilfe des Weierstrass-Produktsatzes) zeigen, dass Quot R der Körper der meromorphen Funktionen ist.

2.7.5 Primfaktorzerlegung im Quotientenkörper eines faktoriellen Rings

Es sei (R, P) ein faktorieller Ring mit Vertretersystem P.

Es existiert zu jedem $\frac{r}{s} \in \mathrm{Quot}\, R \backslash \{0\}$ eine eindeutige Primfaktorzerlegung, das ist genauer eine Abbildung

$$\alpha : \left\{ \begin{array}{rcll} P & \to & \mathbb{Z} & \\ p & \mapsto & \alpha(p), & \text{(nur an endlich vielen Stellen ungleich Null)} \end{array} \right.$$

und genau ein $u \in R^\times$ so, dass

$$\frac{r}{s} \;=\; u \cdot \prod_{p \in P} p^{\alpha(p)}.$$

2.7.6 Begründung, Kommentare

Gemäß Satz 2.2.7 existieren zu r und s eindeutige Primfaktorzerlegungen

$$r \;=\; u \cdot \prod_{p \in P} p^{\alpha(p)}, \qquad s \;=\; v \cdot \prod_{p \in P} p^{\beta(p)}.$$

Es ist dann

$$\frac{r}{s} \;=\; uv^{-1} \prod_{p \in P} p^{\alpha(p) - \beta(p)}$$

eine PFZ für $\frac{r}{s}$. Es ist klar, dass nicht eine zweite solche Abbildung das gleiche Element in Quot R repräsentieren kann.

2.7.7 Beispiel

Aufteilung in Zähler und Nenner, ,,Soweit wie möglich gekürzt".

2.8 Der Chinesische Restsatz — Simultane Kongruenzen ⊖

2.8.1 Definition: Koprime Ideale

Es seien I, J zwei Ideale in einem uk Ring R. Die folgenden Aussagen sind äquivalent:

(A) Es ist $I + J = R$ (I und J heißen dann *koprim*).

(B) Es existieren $a \in I$ und $b \in J$ so, dass $1 = a + b$.

(C) Zu jedem $x \in R$ existieren $a \in I$ und $b \in J$ so, dass $x = a + b$.

2.8.2 Beweis Nachrechnen.

2.8.3 Satz: Produkte paarweise koprimer Ideale

Es seien R ein uk Ring. Dann gilt

(i) Sind $I_1, \ldots, I_n$ paarweise koprime Ideale in R, so gilt

$$I_1 \cdot \ldots \cdot I_n \;=\; I_1 \cap \ldots \cap I_n.$$

(ii) Sind $I_1, \ldots, I_n$ und J Ideale in R, so dass I_k und J koprim sind für alle $k = 1, \ldots, n$, so sind auch $I_1 \cdot \ldots \cdot I_n$ und J koprim.

(iii) Sind $I_1, \ldots, I_n$ paarweise koprime Ideale in R, so sind für jedes $k \in \{1, \ldots, n\}$ das Ideal I_k und sein Komplementär-Ideal

$$\overline{I}_k \;:=\; I_1 \cdot \ldots \cdot I_{k-1} \cdot I_{k+1} \cdot \ldots \cdot I_n \qquad (I_k \text{ im Produkt weggelassen})$$

koprim.

2.8.4 Beweis

(i) Per Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Der Fall $n = 2$ wurde bereits in 1.5.12 (iii) abgehandelt.

Induktionsschluss. Sind $I_1, \ldots, I_n, I_{n+1}$ paarweise koprim, so ist nach Induktionsvoraussetzung

$$I_1 \cdot \ldots \cdot I_n \;=\; I_1 \cap \ldots \cap I_n$$

und dann aufgrund des Falls $n = 2$

$$\begin{aligned} I_1 \cdot \ldots \cdot I_n \cdot I_{n+1} &= (I_1 \cdot \ldots \cdot I_n) \cdot I_{n+1} \\ &= (I_1 \cap \ldots \cap I_n) \cap I_{n+1} \;=\; I_1 \cap \ldots \cap I_n \cap I_{n+1}. \end{aligned}$$

(ii) Wir wählen für alle $\ell \in \{1, \ldots, n\}$ ein $a_\ell \in I_\ell$ und $b_\ell \in J$ mit $a_\ell + b_\ell = 1$. Es gibt dann $c_j \in R$, $j = 1, \ldots, n$ so, dass

$$1 \;=\; \prod_{\ell=1}^{n} (a_\ell + b_\ell) \;=\; a_1 \cdot \ldots \cdot a_n + \sum_{j=1}^{n} b_j c_j \;\in\; I_1 \cdot \ldots \cdot I_n + J.$$

(iii) folgt sofort aus (i) und (ii).

2.8.5 Bemerkung

Im Kummerring sind einerseits die Ideale $(2), (3), (1+\sqrt{-5}), (1-\sqrt{-5})$ paarweise koprim. Wegen

$$(2)\cdot(3) \;=\; (6) \;=\; (1+\sqrt{-5})\cdot(1-\sqrt{-5})$$

sind aber die beiden Produktideale links und rechts nicht koprim.

2.8.6 Der Chinesische Restsatz

Es sei R ein uk Ring. Weiter seien $I_1,\ldots,I_n$ paarweise koprime Ideale in R. Dann ist der Restklassen-Ringhomomorphismus

$$\chi : \left\{ \begin{array}{rcl} R & \to & R/I_1 \times \ldots \times R/I_n \\ x & \mapsto & (x+I_1,\ldots,x+I_n) \end{array} \right.$$

surjektiv mit Kern $\ker\chi = I_1\cdot\ldots\cdot I_n$.

Der Kern von χ ist gegeben durch das Produkt der Ideale

$$\ker\chi \;=\; I_1\cdot\ldots\cdot I_n.$$

2.8.7 Beweis

(0) Wir wissen aus Satz 2.8.3 (iii), dass für jedes $k\in\{1,\ldots,n\}$ I_k und $\overline{I}_k$ koprim sind. Es existieren also $c_k\in I_k$ und $d_k\in\overline{I}_k$ so, dass $c_k+d_k=1$.

(1) Ist nun $(x_1+I_1,\ldots,x_n+I_n)\in R/I_1\times\ldots\times R/I_n$ vorgegeben, so setzen wir

$$x := x_1d_1+\ldots+x_nd_n.$$

(2) Es sei nun $k\in\{1,\ldots,n\}$ fixiert. Es gilt dann

$$c_k\in I_k, \qquad \text{also} \qquad x_kc_k\in I_k$$

und für $\ell\in\{1,\ldots,k-1,k+1,\ldots,n\}$

$$d_\ell \;\in\; \overline{I}_\ell \;=\; I_1\cdot\ldots\cdot I_{\ell-1}\cdot I_{\ell+1}\cdot\ldots\cdot I_n \;\subseteq\; I_k, \qquad \text{also} \qquad x_\ell d_\ell\in I_k.$$

(3) Es ist weiter

$$\begin{array}{rcl} x-x_k & = & x_1d_1+\ldots+x_{k-1}d_{k-1}+x_k(1-c_k)+x_{k+1}d_{k+1}+\ldots+x_nd_n-x_k \\ & = & x_1d_1+\ldots+x_{k-1}d_{k-1}-x_kc_k \qquad\quad +x_{k+1}d_{k+1}+\ldots+x_nd_n \\ & \in & I_k. \end{array}$$

also $x+I_k=x_k+I_k$. Das bedeutet insgesamt, dass

$$\delta(x) \;=\; (x+I_1,\ldots,x+I_n) \;=\; (x_1+I_1,\ldots,x_n+I_n)$$

damit ist die Surjektivität von χ bewiesen.

(4) Ist $x\in I_1\cdot\ldots\cdot I_n$, so gilt $x\in I_k$ für alle $k\in\{1,\ldots,n\}$ und deswegen $\chi(x)=(0+I_1,\ldots 0+I_n)$. Also $I_1\cdot\ldots\cdot I_n\subseteq\ker\chi$.

(5) Ist $x\in\ker\chi$, so gilt $(x+I_1,\ldots,x+I_n)=(0+I_1,\ldots 0+I_n)$, also $x\in I_k$ für alle k. Daraus folgt mit Satz 2.8.3 (i)

$$x \;\in\; I_1\cap\ldots\cap I_n \;=\; I_1\cdot\ldots\cdot I_n.$$

2.8.8 Folgerung: Simultane Kongruenzen

Es seien

paarweise teilerfremde Zahlen (Divisoren) $d_1, \ldots, d_m \in \mathbb{Z}$ und

beliebige Zahlen (Reste) $r_1, \ldots, r_m \in \mathbb{Z}$

gegeben.

(i) Dann gibt es eine Lösung $x \in \mathbb{Z}$ der simultanen Kongruenz-Gleichungen

$$\begin{aligned} x &= r_1 \bmod d_1 \\ x &= r_2 \bmod d_2 \\ &\vdots \\ x &= r_m \bmod d_m. \end{aligned}$$

Es sei noch an die Äquivalenz

$$x = r_j \bmod d_j \quad \Longleftrightarrow \quad \exists\, q_j \in \mathbb{Z} \quad \text{mit} \quad x = q_j \cdot d_j + r_j$$

erinnert.

(ii) Die Menge aller Lösungen ergibt sich durch Addition/Subtraktion von Vielfachen des Produkts aller Divisoren:

$$\mathcal{L} = \{x + k \cdot (d_1 \cdot \ldots \cdot d_m) \mid k \in \mathbb{Z}\}.$$

3 Polynome

3.1 Abstrakte Polynome

3.1.1 Finite Folgen

Es sei R ein uk Ring.

Zur Erinnerung: Eine Folge $f : \mathbb{N}_0 \to R$ heißt *finite Folge über R*, wenn es ein $N \in \mathbb{N}$ gibt, so dass

$$f_j \;=\; f(j) \;=\; 0 \quad \text{für alle } j > N.$$

Anders ausgedrückt: Die Folge enthält nur endlich viele Glieder ungleich Null.

3.1.2 Definition: Produkt zweier finiter Folgen

Sind nun zwei finite Folgen

$$f \;=\; (f_0, f_1, f_2, \ldots, f_m, 0, \ldots), \qquad g \;=\; (g_0, g_1, g_2, \ldots, g_n, 0, \ldots)$$

gegeben, so definieren wir ihr *Produkt (= Faltung)* durch

$$(f \cdot g)_j \;=\; f_0 \cdot g_j + f_1 \cdot g_{j-1} + \ldots + f_{j-1} \cdot g_1 + f_j \cdot g_0.$$

Das bedeutet, dass jeweils alle Glieder von f und g mit gleicher Summe j der Indices miteinander multipliziert werden und dann alle Produkte aufsummiert werden. Das Ergebnis steht an der Stelle j der Produktfolge.

Man mache sich klar, dass das Produkt wieder eine finite Folge ist.

3.1.3 Beispiel

$$\begin{aligned}
& (4, 2, -5, 3, 0, 0, 0 \ldots) \cdot (-1, 3, -4, 0, 0, 0 \ldots) \\
= \;& (4 \cdot (-1), 4 \cdot 3 + 2 \cdot (-1), 4 \cdot (-4) + 2 \cdot 3 + (-5) \cdot (-1), \\
& \qquad 2 \cdot (-4) + (-5) \cdot 3 + 3 \cdot (-1), (-5) \cdot (-4) + 3 \cdot 3, 3 \cdot (-4), 0, 0, \ldots) \\
= \;& (-4, 10, -5, -26, 29, -12, 0, 0, \ldots)
\end{aligned}$$

3.1.4 Definition: Polynom, Polynomring

Durch die gliedweise Addition und die Faltung ist die Struktur eines uk Rings auf der Menge aller finiten Folgen über $\mathbb{R}$ gegeben.

(1) Im Kontext dieser Ringstruktur heißt eine finite Folge $(f_j)_{j \in \mathbb{N}_0}$ in R auch *(abstraktes) Polynom über R* oder *(abstraktes) Polynom mit Koeffizienten aus R.*

(2) Die Menge aller Polynome wird deshalb *Polynomring (über R)* genannt und mit $R[X]$ (s.u.) bezeichnet.

(3) Die Elemente $f_0, f_1, \ldots \in R$ heißen in diesem Zusammenhang die *Koeffizienten* des Polynoms.

3.1.5 Die X-Darstellung

Es sei

$$X \;=\; (0,1,0,0,\ldots\ldots)$$

die finite Folge mit 1 an der Stelle 1.

Es stellt sich dann heraus, dass für $j \in \mathbb{N}_0$

$$X^j \;=\; (0,\ldots,0,1,0,\ldots\ldots), \quad \text{wobei die 1 an der } j\text{-ten Stelle.}$$

Das bedeutet, dass ein Polynom f geschrieben werden kann als

$$f \;=\; (f_0,f_1,f_2,\ldots,f_m,0,\ldots) \;=\; f_0+f_1X+f_2X^2+\ldots+f_mX^m.$$

Die X-Schreibweise eröffnet einen suggestiveren Zugang zur Multiplikation. Werden zwei Polynome f und g wie oben multipliziert, so wende man das Distributivgesetz und das Potenzgesetz an:

$$\begin{aligned} f\cdot g &= (f_0+f_1X+f_2X^2+\ldots+f_mX^m)\cdot \\ &\qquad\qquad (g_0+g_1X+g_2X^2+\ldots+g_nX^n) \\ &= f_0\cdot g_0+(f_0g_1+f_1g_0)X+\ldots+(f_mg_{n-1}+f_{m-1}g_n)X^{m+n-1}+f_mg_nX^{m+n}. \end{aligned}$$

3.1.6 Bemerkung

In der Algebra hat sich inzwischen das Symbol X (bei Bedarf auch Y oder Z) bei dieser Schreibweise etabliert. Beachte, dass es zunächst nicht die Bedeutung einer Variablen hat, für die ein Element aus R (oder aus einem anderen geeigneten Ring) eingesetzt werden soll.

3.1.7 Ring-Hom induziert Polynomring-Hom

Es seien $R, \widetilde{R}$ uk Ringe und $R[X]$, $\widetilde{R}[X]$ die zugehörigen Polynomringe.

Weiter sei $\varphi : R \to \widetilde{R}$ ein Ring-Homomorphismus zwischen den Ringen.

Dazu definieren wir wie folgt einen Homomorphismus der zugehörigen Polynomringe, indem wir einfach die Koeffizienten mit Hilfe von φ abbilden.

$$\varphi_* : \left\{ \begin{array}{rcl} R[X] & \to & \widetilde{R}[X] \\ f_0+f_1X+\ldots+f_mX^m & \mapsto & \varphi(f_0)+\varphi(f_1)X+\ldots+\varphi(f_m)X^m. \end{array} \right.$$

3.1.8 Weiterführung: Polynome mit mehreren Variablen

Setzt man den oben beschriebenen Prozess „Übergang vom Ring R zum Polynomring $R[X]$ rekursiv fort, so gelangt man zu den Polynomringen

$$R[X_1,X_2],\ R[X_1,X_2,X_3],\ \ldots\ ,R[X_1,\ldots,X_k]$$

in mehreren Variablen.

Wir wollen diese (hier noch) nicht voll ausbreiten.

3.1.9 Weiterführung: Formale Potenzreihen

Lässt man bei der Einführung des Begriffs des Polynoms die Bedingung „finit" beiseite, so bleiben Addition und insbesondere die Multiplikation sinnvoll. Auf diese Weise entsteht der so genannte Ring $R[[X]]$ der *formalen Potenzreihen.*

3.2 Der Grad eines Polynoms

3.2.1 Definitionen: Grad

(1) Ist f nicht das Nullpolynom, so heißt die eindeutig bestimmte Zahl $m \in \mathbb{N}_0$ mit

$$f_m \neq 0, \qquad f_j = 0 \text{ für alle } j > m,$$

der *Grad* des Polynoms. Das Nullpolynom hat per definitionem den Grad gleich $-\infty$.

Symbolisch wird dies durch $\deg f = m$ ausgedrückt.

(2) Ist m der Grad eines Polynoms f, so nennt man f_m den *Leitkoeffizienten*.

(3) Ein Polynom heißt *normiert*, wenn der Leitkoeffizient gleich 1 ist.

3.2.2 Gradformel

Es seien R ein uk Ring und $f, g \in R[X]$ zwei Polynome. Dann gilt:

(i) Ganz allgemein:

$$\begin{aligned} \deg(f \cdot g) &\leq \max\{\deg f, \deg g\} \\ \deg(f \cdot g) &\leq \deg f + \deg g. \end{aligned}$$

(ii) Ist einer der beiden Leitkoeffizienten kein Nullteiler, so gilt

$$\deg(f \cdot g) = \deg f + \deg g.$$

(iii) Die Bedingung in (ii) ist immer erfüllt, wenn R ein Integritätsring ist.

Der Fall des Nullpolynoms ist hier enthalten, wenn man Rechenregeln für $-\infty$ einbezieht.

3.2.3 Beispiel

Die Gradformel (ii) stimmt nicht mehr, wenn die Leitkoeffizienten Nullteiler sind.

Im uk Ring $\mathbb{Z}/6\mathbb{Z}$ ist

$$(3X - 1) \cdot (2X - 1) = 6X^2 - 5X + 1 = X + 1 \bmod 6.$$

3.3 Der Einsetzungshomomorphismus

3.3.1 Definition und Satz: Der Einsetzungshomomorphismus

Es seien R ein uk Ring und $R[X]$ der zugehörige Polynomring.

Für den so genannten Einsetzungshomomorphismus

$$\varepsilon_{\cdot}(\cdot) : \left\{ \begin{array}{rcl} R[X] \times R[X] & \to & R[X] \\ (f,g) & \mapsto & \varepsilon_g(f) = f(g) := f_0 + f_1 \cdot g + f_2 \cdot g^2 + \ldots + f_m \cdot g^m \end{array} \right.$$

gelten die folgenden Aussagen.

(i) „g fixiert". Der Einsetzhomomorphismus

$$\varepsilon_g(\cdot) : \left\{ \begin{array}{rcl} R[X] & \to & R[X] \\ f & \mapsto & \varepsilon_g(f) = f(g) := f_0 + f_1 \cdot g + f_2 \cdot g^2 + \ldots + f_m \cdot g^m \end{array} \right.$$

ist — wie der Name sagt — ein Ring**homo**morphismus.

(ii) „$g = g_1 X + g_0$ fixiert mit $g_1 \in R^\times$". In diesem Fall ist der Einsetzhomomorphismus

$$\varepsilon_g(\cdot) : \left\{ \begin{array}{rcl} R[X] & \to & R[X] \\ f & \mapsto & f(g) := f_0 + f_1 \cdot (g_1 X + g_0) + f_2 \cdot (g_1 X + g_0)^2 + f_m \cdot g^m \end{array} \right.$$

ein Ring**iso**morphismus. Der inverse Ringisomorphismus ist gegeben durch ε_h, wobei $h = g_1^{-1}(X - g_0)$.

(iii) „f fixiert und $g \in R$". Wir erhalten die Abbildung

$$\varepsilon_{\cdot}(f) : \left\{ \begin{array}{rcl} R & \to & R \\ \lambda & \mapsto & \varepsilon_\lambda(f) = f(\lambda) := f_0 + f_1 \cdot \lambda + f_2 \cdot \lambda^2 + \ldots + f_m \cdot \lambda^m \end{array} \right.$$

Wir erhalten daraus einen Operator

$$\left\{ \begin{array}{rcl} R[X] & \to & \mathcal{F}(R,R) \\ f & \mapsto & (\lambda \mapsto f(\lambda)), \end{array} \right.$$

der einem Polynom $f \in R[X]$ eine polynomiale Abbildung $R \to R$ zuordnet.

Beachte, dass dieser Operator im allgemeinen ...

- nicht injektiv ist. Zwei verschiedene Polynome können die gleiche Abbildung induzieren.
- kein Ringhomomorphismus ist.

(iv) Ist der Ring R ein Integritätsring mit unendlich vielen Elementen, so ist der Operator in (iii) injektiv.

3.3.2 Beweis

(i) und (iii) können leicht eingesehen werden. (ii) folgt daraus, dass die beiden genannten Polynome g und h invers bzgl. Einsetzung sind.

(iv) Ist

$$\begin{cases} R & \to & R \\ \lambda & \mapsto & f(\lambda), \end{cases}$$

die Nullabbildung, so hat das induzierende Polynom f unendlich viele Nullstellen. Das steht im Widerspruch zu der Aussage in Satz 3.5.2(iv), dass die Anzahl der Nullstellen von f durch $\deg(f)$ beschränkt ist, außer es ist $f = 0$. Das bedeutet, dass der Operator injektiv ist.

3.3.3 Beispiel

Ist beispielsweise $R = \mathbb{Z}/2\mathbb{Z}$ der Körper mit zwei Elementen, so sind die beiden konkreten Polynome

$$f(X) \;=\; X^2 + X + 1, \qquad g(X) \;=\; X^3 + X + 1$$

aufgrund von

$$f(0) \;=\; g(0) \;=\; 1, \qquad f(1) \;=\; g(1) \;=\; 1$$

als Abbildungen $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ gleich. Als abstrakte Polynome sind sie jedoch verschieden:

$$f \;=\; (1,1,1,0,0,\ldots) \;\neq\; (1,1,0,1,0,\ldots) \;=\; g.$$

Das Beispiel zeigt auch, dass der Grad einer Polynomfunktion nicht eindeutig definiert sein muss.

3.4 Polynomdivision

3.4.1 Satz: Polynomdivision

Es sei R ein uk Ring (nicht notwendig ein Integritätsring). Wir betrachten zwei Polynome

$$\begin{aligned} f &= f_m X^m + f_{m-1} X^{m-1} + \ldots + f_1 X + f_0 \quad \in R[X] \\ g &= g_n X^n + g_{n-1} X^{n-1} + \ldots + g_1 X + g_0 \quad \in R[X]. \end{aligned}$$

Ist der Leitkoeffizient von g eine Einheit, $g_n \in R^\times$, so gibt es Polynome $q, r \in R[X]$ mit

$$f = q \cdot g + r, \qquad \text{wobei } \deg r < \deg g \qquad (\leftarrow \text{Der Fall } r = 0 \text{ ist eingeschlossen}).$$

Die beiden Polynome q, r sind durch die Zusatzbedingung an den Grad von r eindeutig bestimmt.

3.4.2 Beweis

Existenz.

(0) Der Fall $\deg f < \deg g$ ist klar. Setze dann $q = 0$ und $r = f$.

(1) Der Fall $\deg g = 0$ ist auch klar. Setze dann $q = g_0^{-1} f$ und $r = 0$.

(2) Sei ansonsten $\deg f \geq \deg g \geq 1$. Induktion nach $m = \deg f \geq 0$.

Induktionsanfang. $\deg f = m = 1$. Dann ist auch $\deg g = 1$ und wir wählen q, r so:

$$f_1 X + f_0 = \underbrace{g_1^{-1} f_1}_{=:q} (g_1 X + g_0) + (\underbrace{f_0 - g_1^{-1} f_1 g_0}_{=:r}).$$

Wegen $\deg r \leq 0$ ist die Zusatzbedingung erfüllt.

(3) Induktionsschritt. Sei $\deg f = m \geq n \geq 1$.

Definiere

$$\widetilde{f} := f - g_n^{-1} f_m \cdot X^{m-n} \cdot g.$$

Es ist dann

$$\widetilde{f}_m = f_m - g_n^{-1} f_m g_n = 0, \quad \text{also } \deg \widetilde{f} < \deg f.$$

(4) Damit ist die Induktionsvoraussetzung auf $\widetilde{f}$ anwendbar, wir erhalten eindeutig bestimmte Polynome $\widetilde{q}, r$ mit

$$\widetilde{f} = \widetilde{q} \cdot g + r, \qquad \text{wobei } \deg r < \deg g.$$

(5) Setzen wir dies in die Definition von $\widetilde{f}$ in (3) ein, so erhalten wir

$$\begin{aligned} f &= \widetilde{f} + g_n^{-1} f_m \cdot X^{m-n} \cdot g = \widetilde{q} \cdot g + r + g_n^{-1} f_m \cdot X^{m-n} \cdot g \\ &= [\underbrace{\widetilde{q} + g_n^{-1} f_m \cdot X^{m-n}}_{=:q}] \cdot g + r. \end{aligned}$$

Eindeutigkeit.

(6) Angenommen, es gibt zwei verschiedene Ergebnisse der Division mit Rest

$$\begin{aligned} f &= q_1 g + r_1 \qquad \text{wobei } \deg r_1 < \deg g \\ &= q_2 g + r_2 \qquad \text{wobei } \deg r_2 < \deg g. \end{aligned}$$

Es folgt

$$(q_1 - q_2)g + (r_1 - r_2) = 0$$

(7) Die Annahme $r_1 \neq r_2$ führt auf $(q_1 - q_2)g \neq 0$ und damit $q_1 - q_2 \neq 0$.

Da der Leitkoeffizient von g eine Einheit und damit kein Nullteiler ist, folgt

$$\begin{aligned} \max\{\deg r_1, \deg r_2\} &\geq \deg(r_1 - r_2) = \deg[(q_1 - q_2)g] \\ &\overset{3.2.2(ii)}{=} \underbrace{\deg(q_1 - q_2)}_{\geq 0} + \deg g \geq \deg g. \end{aligned}$$

Widerspruch.

(8) Es muss also $r_1 = r_2$ sein. Dann muss aber, da der Leitkoeffizient von g eine Einheit und damit kein Nullteiler ist, auch $q_1 = q_2$ sein.

3.4.3 Beispiel: Polynomdivision

Die beiden Polynome g und r aus dem obigen Satz erhält man algorithmisch durch die aus der Schule bekannte Polynomdivision.

Man überzeuge sich mit Hilfe der Polynomdivision

$$(3X^5 - 4X^4 + 2X^3 - X + 8) : (X^3 + 7X^2 - 5)$$

von der Darstellung

$$\begin{aligned} & 3X^5 - 4X^4 + 2X^3 - X + 8 \\ = \; & (3X^2 - 25X + 177)(X^3 + 7X^2 - 5) - 1224X^2 - 126X + 893. \end{aligned}$$

3.5 Nullstellen und Linearfaktoren

3.5.1 Definition: Nullstelle

Es sei R ein uk Ring.

Eine Zahl $\lambda \in R$ heißt *Nullstelle* der Polynomfunktion f, wenn $\varepsilon_\lambda(f) = f(\lambda) = 0$.

3.5.2 Satz: Nullstellen und Linearfaktoren

Es seien R ein Integritätsring und ein Polynom $f \in R[X]$ mit $\deg f \geq 1$ gegeben. Weiter sei $\lambda \in R$.

(i) Die beiden folgenden Aussagen sind äquivalent:

(A) λ ist eine Nullstelle von f, d.h. es ist

$$f_m\lambda^m + f_{m-1}\lambda^{m-1} + \ldots + f_1\lambda + f_0 \;=\; 0.$$

(B) Es gibt ein eindeutig bestimmtes Polynom g mit $\deg g = \deg f - 1$ so, dass

$$f(X) \;=\; (X-\lambda)\cdot g(X).$$

Man spricht von der *Abspaltung eines Linearfaktors*.

(ii) Es gibt eine eine eindeutig festgelegte Zahl $k \in \mathbb{N}_0$ und ein Polynom g mit $\deg g = \deg f - k$ so, dass

$$f(X) \;=\; (X-\lambda)^k \cdot g(X), \qquad \text{wobei } g(\lambda) \neq 0.$$

Die Zahl k heißt die *Vielfachheit* der Nullstelle λ im Polynom f.

(iii) Das Polynom f hat höchstens $\deg f$ Nullstellen.

3.5.3 Beweis

(i) $\Rightarrow$ Die Richtung (B) $\Rightarrow$ (A) ist trivial.

(i) $\Leftarrow$ Für die Umkehrung machen wir eine Vorüberlegung: Es gilt für $m \in \mathbb{N}$

$$\begin{aligned}(X^m - \lambda^m) &= \Big[X^m + X^{m-1}\lambda + X^{m-2}\lambda^2 + \ldots + X^2\lambda^{m-2} + X\lambda^{m-1}\Big] \\ &\quad - \Big[X^{m-1}\lambda + X^{m-2}\lambda^2 + \ldots + X^2\lambda^{m-2} + X\lambda^{m-1} + \lambda^m\Big] \\ &= (X-\lambda)\cdot \underbrace{(X^{m-1} + X^{m-2}\lambda + \ldots + X\lambda^{m-2} + \lambda^{m-1})}_{=:\, Q_{m-1}(X,\lambda)}\end{aligned}$$

Jetzt können wir die Umkehrung zeigen:

$$\begin{aligned}f(X) &= f(X) - f(\lambda) \\ &= \Big(f_nX^n + f_{n-1}X^{n-1} + \ldots + f_1X + f_0\Big) - \Big(f_n\lambda^n + f_{n-1}\lambda^{n-1} + \ldots + f_1\lambda + f_0\Big) \\ &= f_n(X^n - \lambda^n) + f_{n-1}(X^{n-1} - \lambda^{n-1}) + \ldots + f_1(X-\lambda) \\ &= (X-\lambda)\cdot\Big(f_nQ_{n-1}(X,\lambda) + f_{n-1}Q_{n-2}(X,\lambda) + \ldots + f_1\Big) \\ &= (X-\lambda)\cdot g(X).\end{aligned}$$

Die Existenz lässt sich auch ohne die Voraussetzung „R Integritätsring" beweisen.

Die Eindeutigkeit von g ist gesichert, da R ein Integritätsring ist.

(ii) Aufgrund der Verminderung des Grads bei jeder Abspaltung der Linearfaktoren $(X - \lambda)$ muss irgendwann — nach k Schritten — $g(\lambda) \neq 0$ eintreten.

(iii) Anderenfalls würde ein Widerspruch zur Gradformel 3.2.2 (ii) entstehen.

3.5.4 Beispiele

1. Wir betrachten den uk Ring $\mathbb{Z}/6\mathbb{Z}$, der kein Integritätsring ist.

   Das Polynom $f = X^2 + X$ hat Grad 2, aber vier verschiedenen Nullstellen, nämlich

   $$0 + 6\mathbb{Z}, \qquad 2 + 6\mathbb{Z}, \qquad 3 + 6\mathbb{Z}, \qquad 5 + 6\mathbb{Z}.$$

2. Wir betrachten den uk Ring der Matrizen

   $$\begin{pmatrix} a & r \\ 0 & a \end{pmatrix}, \qquad a, r \in \mathbb{R}.$$

   Das Polynom X^2 hat alle Matrizen der Form $\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$, also unendlich viele, als Nullstellen.

3.5.5 Definition: Zerfall in Linearfaktoren

Es sei R ein uk Ring und $f \in R[X]$. Man sagt, das Polynom f *zerfällt (über R) in Linearfaktoren*, wenn es in der Form

$$f(X) \;=\; f_m \cdot (X - \lambda_1)^{k_1} \cdot (X - \lambda_2)^{k_2} \cdot \ldots \cdot (X - \lambda_m)^{k_m}$$

mit Elementen $\lambda_1, \ldots, \lambda_\ell \in R$ und $k_1, \ldots, k_\ell \in \mathbb{N}$ dargestellt werden kann.

3.5.6 Zusatz: Nullstellen im Quotientenkörper $^{\ominus}$

Es sei R ein faktorieller Ring und $\operatorname{Quot} R$ der zugehörige Quotientenkörper. Zu einem gegebenen Polynom $f \in R[X]$ mit $\deg f = m$ betrachten wir die Äquivalenzen von Polynomgleichungen

$$0 \;=\; f(X) \;=\; f_m X^m + f_{m-1} X^{m-1} + \ldots + f_1 X + f_0$$

(Substitution: $X = \frac{Y}{f_m}$)

$$0 \;=\; f_m (\tfrac{Y}{f_m})^m + f_{m-1} (\tfrac{Y}{f_m})^{m-1} + \ldots + f_1 (\tfrac{Y}{f_m}) + f_0$$

(Mulitplikation mit f_m^{m-1})

$$0 \;=\; g(Y) \;=\; Y^m + f_{m-1} Y^{m-1} + \ldots + f_1 f_m^{m-2} + f_0 f_m^{m-1}.$$

(i) Für ein $\lambda \in \operatorname{Quot} R$ sind äquivalent:

- λ ist Nullstelle von f.
- Es ist $\lambda = \frac{\mu}{f_m}$, wobei μ Nullstelle von g ist.

(ii) Ist $\lambda = \frac{\mu}{f_m} \in \operatorname{Quot} R$ Nullstelle von f, so gilt $\lambda \mid (f_0 f_m^{m-1})$.

3.6 Transfer von Eigenschaften zum Polynomring

3.6.1 Satz: Transfer von Eigenschaften

Es sei R ein uk Ring R. Dann gelten die folgenden Implikationen.

(i) R ist ein Integritätsring
$\iff$ $R[X]$ ist ein Integritätsring

(ii) R ist faktoriell
$\implies$ $R[X]$ ist faktoriell (Satz von Gauß)

(iii) R ist noethersch
$\implies$ $R[X]$ ist noethersch (Basissatz von Hilbert)

(iv) R ist ein Körper
$\iff$ $R[X]$ ist ein euklidischer Ring
$\iff$ $R[X]$ ist ein Hauptidealring

3.6.2 Beweis

(i) (A) $\Rightarrow$ (B). Sind f und g zwei Polynome über dem Integritätsring R, so sind ihre Leitkoeffizienten keine Nullteiler. Dann kann auch der Leitkoeffizient des Produktpolynoms $f \cdot g$ kein Nullteiler sein, ist also ungleich Null.

(ii) (B) $\Rightarrow$ (A). Da $R \subseteq R[X]$, ist die Aussage trivial.

(ii) (A) $\Rightarrow$ (B). Der Beweis dieser Implikation ist sehr aufwändig. Er wird später in Kapitel 3.9 geführt.

(iv) (A) $\Rightarrow$ (B). In einem Körper gilt $R^\times = R \setminus \{0\}$, also sind Leitkoeffizienten von Polynomen immer Einheiten. Die Behauptung ist dann in Satz 3.4.1 enthalten. Die euklidische Funktion ist der Polynomgrad.

(iv) (B) $\Rightarrow$ (C). Siehe Satz 2.5.4.

(iv) (C) $\Rightarrow$ (A). Es sei $R[X]$ ein Hauptidealring. Wir betrachten den Einsetzhomomorphismus

$$\varepsilon_0 : \left\{ \begin{array}{rcl} R[X] & \to & R \\ f & \mapsto & f_0 = f(0) \end{array} \right.$$

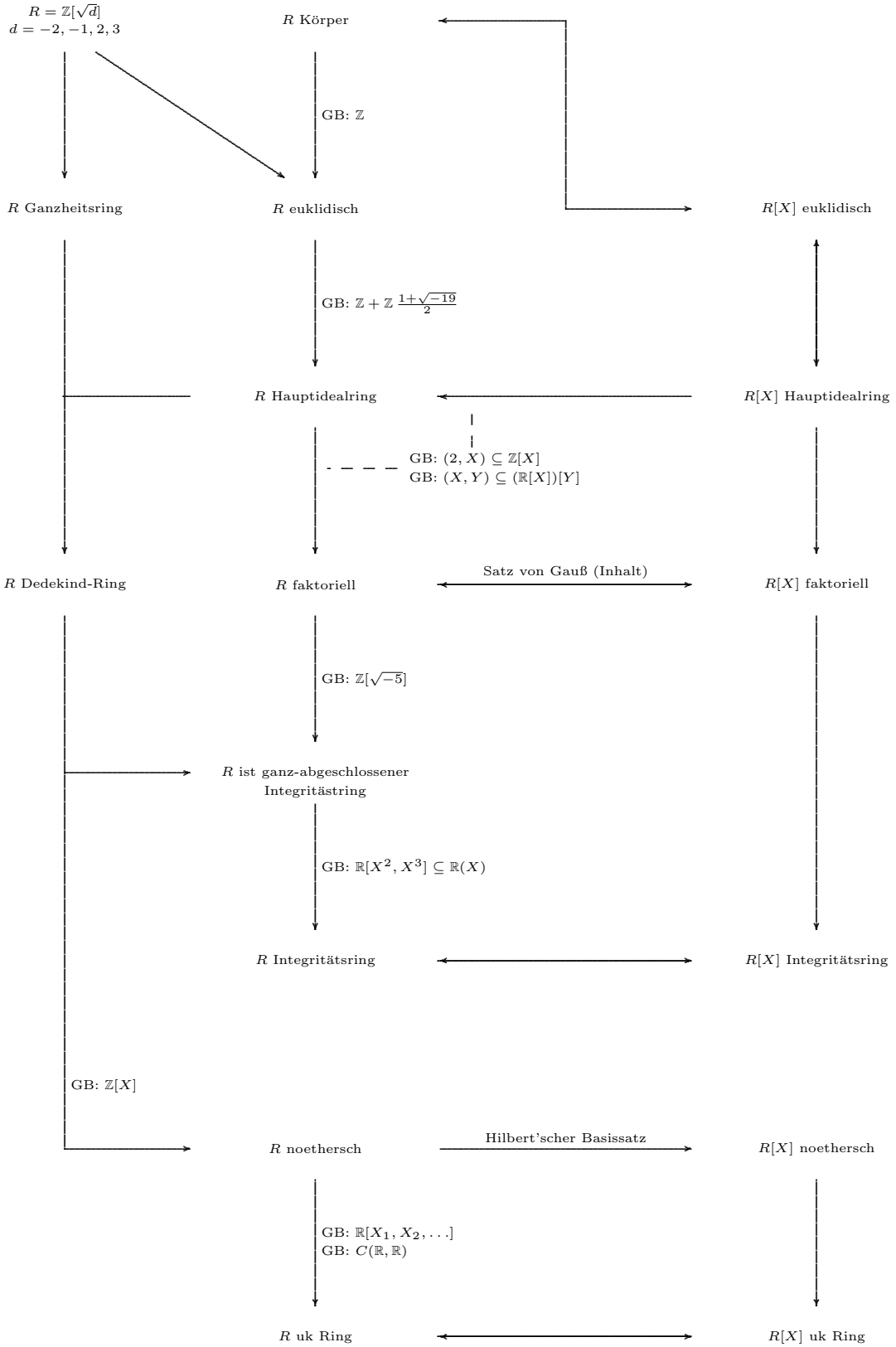
und dazu den Homomorphiesatz

$$R \simeq R[X]/(\ker \varepsilon_0).$$

Dann gilt die folgende Implikationskette.

$$\begin{array}{rl} & R[X] \text{ ist Hauptidealring} \\ \overset{\text{def}}{\Longrightarrow} & R[X] \text{ ist Integritätsring} \\ \Longrightarrow & R \text{ ist Integritätsring} \\ \overset{R \simeq R[X]/(\ker \varepsilon_0)}{\Longrightarrow} & R[X]/(\ker \varepsilon_0) \text{ ist Integritätsring} \\ \Longrightarrow & \ker \varepsilon_0 \text{ ist Primideal in } R[X] \\ \overset{\text{Satz 2.4.2}}{\Longrightarrow} & \ker \varepsilon_0 \text{ ist maximales Ideal in } R[X] \\ \overset{\text{Satz 2.6.1}}{\Longrightarrow} & R \text{ ist Körper.} \end{array}$$

3.6.3 Diagramm zu uk Ringen und ihren Polynomringen



3.7 Primitive Polynome und Inhalt eines Polynoms

In diesem gesamten Kapitel ist R ein faktorieller Ring mit Vertretersystem P. Das bedeutet, dass ggT und kgV Funktionen sind, die endlichen Teilmengen von R ,,eindeutig definierte" Elemente von R zuordnen.

3.7.1 Definition: Primitives Polynom

Es seien R ein faktorieller Ring mit Vertretersystem P der Primelemente. Weiter sei $f = f_0 + f_1 X + \ldots + f_m X^m \in R[X] \setminus \{0\}$ ein Polynom.

Das Polynom f heißt *primitiv*, wenn seine Koeffizienten teilerfremd sind, d.h. $\operatorname{ggT}(f_0, \ldots, f_m) = 1$.

3.7.2 Bemerkung

Irreduzible Polynome sind primitiv, das Polynom X^2 ist primitiv, aber nicht irreduzibel.

3.7.3 Definition: Inhalt-Primitiv-Zerlegung eines Polynoms

Es sei R ein faktorieller Ring mit Vertretersystem P und

$$f \;=\; f_0 + f_1 X + \ldots + f_m X^m \qquad \in \operatorname{Quot} R[X]$$

ein Polynom mit Koeffizienten im Quotientenkörper $\operatorname{Quot} R$.

Wir zerlegen in einer Abfolge von Schritten das Polynom in seinen *Inhalt* $\operatorname{inh} f$ und *primitiven Anteil* f^{prt}.

(1) Soweit wie möglich kürzen

Es existieren gemäß Satz 2.7.5 eindeutige Elemente $a_j \in R, b_j \in R \setminus \{0\}$ so, dass

$$f \;=\; \tfrac{a_0}{b_0} + \tfrac{a_1}{b_1} X + \ldots + \tfrac{a_m}{b_m} X^m, \qquad \forall_j \;\operatorname{ggT}(a_j, b_j) = 1.$$

(2) Extrahieren des kgV im Nenner

Wir extrahieren $B := \operatorname{kgV}(b_1, \ldots, b_m) \neq 0$ und erhalten

$$f \;=\; B^{-1} \cdot (c_0 + c_1 X + \ldots + c_m X^m), \qquad \text{wobei } c_j \;=\; \tfrac{B\, a_j}{b_j} \in R.$$

(3) Extrahieren des ggT

Wir extrahieren $C := \operatorname{ggT}(c_0, \ldots, c_m) \neq 0$ und erhalten

$$f \;=\; \underbrace{C\, B^{-1}}_{=:\operatorname{inh} f} \cdot \underbrace{(\, d_0 + d_1 X + \ldots + d_m X^m \,)}_{=:f^{\mathrm{prt}}}, \qquad \text{wobei } d_j \;=\; \tfrac{B\, a_j}{C\, b_j} \in R.$$

(4) Zerlegung

Es ist dann $\operatorname{ggT}(d_0, \ldots, d_m) = 1$. Wir haben also eine eindeutige Zerlegung

$$f \;=\; \operatorname{inh} f \cdot f^{\mathrm{prt}}$$

des Polynoms $f \in \operatorname{Quot} R[X]$ in zwei Faktoren $\operatorname{inh} f \in \operatorname{Quot} R$ und ein primitives Polynom $f^{\mathrm{prt}} \in R[X]$ erhalten.

Beachte, dass die Eindeutigkeit dieser Zerlegung auf der Eindeutigkeit von ggT und kgV beruht.

3.7.4 Eigenschaften der Inhalt-Primitiv-Zerlegung

Es seien R ein faktorieller Ring und P ein Vertretersystem der Primelemente von R. Weiter sei

$$f \;=\; f_0 + f_1 X + \ldots + f_m X^m \qquad \in \operatorname{Quot} R[X].$$

(i) Ist $f = a \cdot \widetilde{f}$ eine weitere Zerlegung von f mit $a \in \operatorname{Quot} R$ und primitivem $\widetilde{f}$, so gilt

$$\widetilde{f} \sim f^{\mathrm{prt}} \quad \text{ in } R[X].$$

(ii) Es gelten die Implikationen in dem folgenden Diagramm

$$\begin{array}{ccc}
f \in (\operatorname{Quot} R)[X] \setminus \{0\}, \text{ normiert} & \Longrightarrow & \operatorname{inh} f \;=\; \frac{1}{B},\ B \in R \setminus \{0\} \\
\Uparrow & & \\
f \in R[X] \setminus \{0\}, \text{ normiert} & & \\
\Downarrow & & \\
f \in R[X] \setminus \{0\}, \text{ primitiv} & \Longleftrightarrow & \operatorname{inh} f \;=\; 1 \\
\Downarrow & & \\
f \in R[X] \setminus \{0\} & \Longleftrightarrow & \operatorname{inh} f \in R \setminus \{0\} \\
\Downarrow & & \\
f \in (\operatorname{Quot} R)[X] \setminus \{0\} & \Longleftrightarrow & \operatorname{inh} f \in \operatorname{Quot} R \setminus \{0\}
\end{array}$$

3.7.5 Beweis $\ominus$

(i) Wir zeigen die etwas allgemeinere Aussage: Gilt

$$f \;=\; a \cdot g \;=\; b \cdot h \qquad \text{mit } a, b \in \operatorname{Quot} R \quad \text{und} \quad g, h \text{ primitiv},$$

so folgt

$$g \;\sim\; h \quad \in R[X].$$

(1) Da wir die Gleichung mit dem kgV der Nenner von a und b multiplizieren können, kann von vornherein $a, b \in R$ angenommen werden.

(2) Der Koeffizientenvergleich liefert

$$a \cdot g_j \;=\; b \cdot h_j \qquad j \in \{0, 1 \ldots, m\}. \qquad (*)$$

(3) Da g und h primitiv sind, gilt

$$\begin{aligned}
\operatorname{ggT}(g_0, \ldots, g_m) &= 1 \qquad (**) \\
\operatorname{ggT}(h_0, \ldots, h_m) &= 1 \qquad (***)
\end{aligned}$$

(4) Es gilt dann

$$a \overset{(**)}{\sim} \operatorname{ggT}(ag_0, \ldots, ag_m) \overset{(*)}{=} \operatorname{ggT}(bh_0, \ldots, bh_m) \overset{(***)}{\sim} b,$$

also $a \sim b$.

(5) Es existiert also $u \in R^\times$ mit $b = u\,a$ und dann

$$ag = bh = u\,ah,$$

nach Anwenden der Kürzungsregel $g = u\,h$. qed.

(ii) Dritte Zeile. Diese Äquivalenz ist eine direkte Folgerung der Definition des Inhalts.

(ii) Vierte Zeile $\Rightarrow$

Betrachte die Schrittfolge in der Definition 3.7.3. Es ist $b_0 = \ldots = b_m = 1$, deshalb $B = 1$ und dann $\operatorname{inh} f = C = \operatorname{ggT}(c_0, \ldots, c_m) = \operatorname{ggT}(f_0, \ldots, f_m) \in R$.

(ii) Vierte Zeile $\Leftarrow$

Wegen $f^{\mathrm{prt}} \in R[X]$ ist dann auch $f = \operatorname{inh} f \cdot f^{\mathrm{prt}} \in R[X]$.

(ii) Erste Zeile. Wie in Schritt (2) von 3.7.3 beschrieben, sei $B \in R \setminus \{0\}$ das kgV der Nenner der gekürzten Koeffizienten von f.

Wir betrachten das Polynom

$$g := Bf = BX^m + Bf_{m-1}X^{m-1} + \ldots + Bf_1X + Bf_0.$$

und zeigen, dass es primitiv ist.

Angenommen es gibt ein $p \in P$ mit $p \mid g_j$ für alle $j \in \{0, \ldots, m\}$.

Da f normiert und damit primitiv ist, muss $p \mid B$ gelten. Gemäß Definition des kgV muss die höchste Potenz p^k im kgV auch bei mindestens einem der Nenner b_j des Polynoms f auftreten, wir erhalten

$$\begin{aligned} B &= p^k \cdot \widetilde{B} \quad \text{mit} \quad p \nmid \widetilde{B} \\ b_j &= p^k \cdot \widetilde{b}_j \quad \text{mit} \quad p \nmid \widetilde{b}_j. \end{aligned}$$

Weiter ist wegen $\operatorname{ggT}(a_j, b_j) = 1$ auch $p \nmid a_j$.

Es gilt dann

$$g_j = \frac{Ba_j}{b_j} = \frac{p^k \cdot \widetilde{B}a_j}{p^k \cdot \widetilde{b}_j} = \frac{\widetilde{B}a_j}{\widetilde{b}_j},$$

woraus $p \nmid g_j$ folgt. Also ist g primitiv und es folgt mit der Implikation der dritten Zeile

$$1 = \operatorname{inh} g = \operatorname{inh}(Bf) = B \cdot \operatorname{inh} f.$$

3.7.6 Lemma von Gauß

Es seien R ein faktorieller Ring und $g, h \in R[X] \setminus \{0\}$ Polynome.

Primitivität und die Inhalt-Primitiv-Zerlegung verhalten sich multiplikativ, d.h. genauer

(i) Sind g, h primitiv, so ist auch $g \cdot h$ primitiv.

(ii) Es ist $\operatorname{inh}(g \cdot h) \;=\; \operatorname{inh} g \cdot \operatorname{inh} h$.

(iii) Es ist $(g \cdot h)^{\mathrm{prt}} \;=\; g^{\mathrm{prt}} \cdot h^{\mathrm{prt}}$.

3.7.7 Beweis $\ominus$

(i) Es seien

$$\begin{array}{rcrcl} g & = & g_m X^m & + \ldots + & g_1 X + g_0 \\ h & = & h_n X^n & + \ldots + & h_1 X + h_0 \\ f = g \cdot h & = & f_{m+n} X^{m+n} & + \ldots + & f_1 X + f_0. \end{array}$$

Angenommen, f ist nicht primitiv. Dann gibt es ein Primelement $p \in \mathcal{M}_{\mathrm{gT}}(f_0, \ldots, f_{m+n})$.

Da h und g primitiv sind, gibt es $j \in \{0, \ldots, m\}$ und $k \in \{0, \ldots, n\}$ so, dass

$$\begin{aligned} &p \mid h_0, \;\ldots,\; p \mid h_{j-1}, \qquad p \nmid h_j \\ &p \mid g_0, \;\ldots,\; p \mid g_{k-1}, \qquad p \nmid g_k. \end{aligned}$$

Es ist dann

$$f_{j+k} \;=\; \underbrace{h_0 g_{j+k} + h_1 g_{j+k-1} + \ldots + h_{j-1} g_{k+1}} + h_j g_k + \underbrace{h_{j+1} g_{k-1} + \ldots + h_{j+k-1} g_1 + h_{j+k} g_0}.$$

Da p alle Summanden in der Unterklammerung und die linke Seite f_{j+k} teilt, teilt p auch $h_j g_k$. Da p ein Primelement ist, folgt $p \mid h_j$ oder $p \mid g_k$. Widerspruch.

(ii) Wir wenden die Inhalt-Primitiv-Zerlegung auf das Produkt gh und auf die Faktoren g und h an, d.h.

$$\operatorname{inh}(g \cdot h) \cdot (g \cdot h)^{\mathrm{prt}} \;=\; g \cdot h \;=\; \operatorname{inh}(g) g^{\mathrm{prt}} \cdot \operatorname{inh}(h) h^{\mathrm{prt}} \;=\; \operatorname{inh}(g) \operatorname{inh}(h) \cdot g^{\mathrm{prt}} h^{\mathrm{prt}}.$$

Nach (i) dieses Satzes ist das Produkt $g^{\mathrm{prt}} h^{\mathrm{prt}}$ ganz rechts primitiv. Mit Satz 3.7.4(i) erhalten wir

$$g^{\mathrm{prt}} h^{\mathrm{prt}} \;\sim\; (g \cdot h)^{\mathrm{prt}}.$$

Nach Satz 3.7.4(ii) sind die Inhalte in R, es folgt zunächst

$$\operatorname{inh}(g \cdot h) \;\sim\; \operatorname{inh}(g) \operatorname{inh}(h)$$

und dann, da die Inhalte als ggTs nur Produkte von Elementen aus P sind, dass

$$\operatorname{inh}(g \cdot h) \;=\; \operatorname{inh}(g) \operatorname{inh}(h).$$

Die erste Gleichung in (ii) zeigt dann sofort auch die Aussage (iii) auf.

3.7.8 Folgerungen aus dem Lemma von Gauß

Es seien R ein faktorieller Ring und P ein Vertretersystem der Primelemente von R. Es gelten die folgenden (technischen) Implikationen

$$\left.\begin{aligned} f, g \in R[X] \setminus \{0\},\ g \text{ primitiv} \\ h \in (\operatorname{Quot} R)[X] \setminus \{0\} \\ g \cdot h = f \quad \text{in } (\operatorname{Quot} R)[X] \end{aligned}\right\} \quad \Longrightarrow \quad h \in R[X].$$

$$\left.\begin{aligned} f, g \in R[X] \setminus \{0\},\ g \text{ primitiv} \\ g \mid f \quad \text{in } (\operatorname{Quot} R)[X] \end{aligned}\right\} \quad \Longrightarrow \quad g \mid f \quad \text{in } R[X].$$

$$\left.\begin{aligned} f, g \in R[X] \setminus \{0\},\ f, g \text{ primitiv} \\ f \sim g \quad \text{in } (\operatorname{Quot} R)[X] \end{aligned}\right\} \quad \Longrightarrow \quad f \sim g \quad \text{in } R[X].$$

$$\left.\begin{aligned} f, g, h \in (\operatorname{Quot} R)[X] \setminus \{0\}, \quad \text{normiert} \\ f = g \cdot h \in R[X] \end{aligned}\right\} \quad \Longrightarrow \quad g, h \in R[X].$$

3.7.9 Beweis ⊖

(1) Unter Beachtung der dritten und vierten Zeile des Diagramms in 3.7.4 (ii) und des Lemmas von Gauß (ii) folgt

$$\operatorname{inh} h \;=\; \operatorname{inh} g \cdot \operatorname{inh} h \;=\; \operatorname{inh}(f) \;\in\; R$$

und damit $h \in R[X]$.

(2) Die zweite Impliktation ist nur eine Umformulierung der ersten.

(3) Unter Beachtung von $f \sim g \iff f \mid g$ und $g \mid f$ lässt sich die dritte Implikation auf die zweite zurückführen.

(4) Gemäß erster Zeile im Diagramm in 3.7.4 (ii) gibt es $B_g, B_h \in R \setminus \{0\}$ mit $\operatorname{inh} g = \frac{1}{B_g}$ und $\operatorname{inh} h = \frac{1}{B_h}$. Wegen

$$1 \;=\; \operatorname{inh} f \;=\; \operatorname{inh} g \cdot \operatorname{inh} h \;=\; \tfrac{1}{B_g} \cdot \tfrac{1}{B_h}$$

sind $B_h, B_h \in R^\times$ und damit $\operatorname{inh} g, \operatorname{inh} h \in R$. Es folgt $g, h \in R[X]$.

3.8 Irreduzibilitätskriterien

3.8.1 Satz: Irreduzibilität beim Wechsel zwischen Ring und Quotientenkörper
Es seien R ein faktorieller Ring und $\operatorname{Quot} R$ sein Quotientenkörper.

Wir betrachten ein Polynom

$$f \;=\; f_0 + f_1 X + \ldots + f_m X^m \qquad \in R[X] \setminus \{0\}.$$

Dann gelten die folgenden Implikationen

$$f \text{ irreduzibel } \in (\operatorname{Quot} R)[X] \quad \begin{array}{c} \overset{f \text{ primitiv}}{\Longrightarrow} \\ \underset{\deg f \geq 1}{\Longleftarrow} \end{array} \qquad f \text{ irreduzibel } \in R[X].$$

3.8.2 Beispiele

Die Polynome $2X$ oder $24X^2 - 18X + 36$ sind irreduzibel in $(\operatorname{Quot} R)[X]$, aber nicht in $R[X]$.

Die Polynome 2 oder -5 sind irreduzibel in $R[X]$, aber nicht in $(\operatorname{Quot} R)[X]$.

Das heißt, die beiden Implikationen des Satzes sind ,,Äquivalenzen bis auf Sonderfälle".

3.8.3 Beweis

$\Rightarrow$. Angenommen, es wäre $f = g \cdot h$ eine Zerlegung in $R[X]$. Wegen der Irreduzibilität von f in $\operatorname{Quot}(R)[X]$ ist (O.B.d.A.)

$$g \in ((\operatorname{Quot} R)[X])^\times \cap R[X] \;=\; (\operatorname{Quot} R)^\times \cap R[X] \;\subseteq\; R.$$

Wäre $g \notin R^\times$, so wäre $f = g \cdot h$ nicht primitiv.

$\Leftarrow$. Angenommen, es wäre $f = g \cdot h$ eine Zerlegung in $(\operatorname{Quot} R)[X]$. Es gilt dann $\deg g \geq 1$ und $\deg h \geq 1$. Weiter ist dann

$$f \;=\; g \cdot h \;=\; \operatorname{inh} g \cdot \operatorname{inh} h \cdot g^{\mathrm{prt}} \cdot h^{\mathrm{prt}} \;=\; \underbrace{\operatorname{inh} f}_{\in R} \cdot \underbrace{g^{\mathrm{prt}}}_{\in R[X]} \cdot \underbrace{h^{\mathrm{prt}}}_{\in R[X]}$$

eine Zerlegung in $R[X]$. Widerspruch.

3.8.4 Nullstellen von normierten Polynomen

Es sei R ein faktorieller Ring.

(i) Ist $\lambda \in (\operatorname{Quot} R)[X]$ eine Nullstelle des normierten Polynoms $f \in R[X]$, so gilt $\lambda \in R$ und dann weiter $\lambda \mid f_0$.

(ii) Ist f normiert und reduzibel in $(\operatorname{Quot} R)[X]$ mit $\deg f \in \{1, 2, 3\}$, so gibt es eine Nullstelle $\lambda \in R$.

3.8.5 Beweis

(i) In diesem Fall kann in $(\operatorname{Quot} R)[X]$ der zugehörige Linearfaktor abgespalten werden, also

$$f(X) \;=\; (X-\lambda)\cdot g(X).$$

Es muss auch g normiert sein. Gemäß der vierten Implikation in Folgerung 3.7.8 ist $X-\lambda \in R[X]$, also $\lambda \in R$.

(ii) In diesem Fall gibt es in der Zerlegung von f einen Linearfaktor, der eine Nullstelle in $\operatorname{Quot} R$ nach sich zieht. Man wende Aussage (i) an.

3.8.6 Satz: Das Schönemann-Eisenstein-Kriterium

Es seien R ein faktorieller Ring und

$$f \;=\; \underbrace{f_0}_{p\mid\ p^2\nmid} + \underbrace{f_1}_{p\mid} X + \underbrace{f_2}_{p\mid} X^2 + \ldots + \underbrace{f_{m-1}}_{p\mid} X^{m-1} + \underbrace{f_m}_{p\nmid} X^m \in R[X]$$

ein primitives Polynom mit $\deg f \geq 1$.

Wenn es ein Primelement $p \in R$ gibt so, dass die Teilbarkeitsbedingungen wie oben in der zweiten Zeile erfüllt sind, so ist f irreduzibel in $R[X]$ und dann auch in $(\operatorname{Quot} R)[X]$.

3.8.7 Beweis

(1) Wegen $\deg f \geq 1$ ist $f \in R^\circ$.

(2) Wir nehmen an, f sei nicht irreduzibel, d.h. es existiert ein Zerlegung $f = g\cdot h$, wobei

$$\begin{aligned} g &= g_0 + g_1X + B_2X^2 + \ldots + g_{k-1}X^{k-1} + g_kX^k, && g_k \neq 0,\\ h &= h_0 + h_1X + B_2X^2 + \ldots + h_{\ell-1}X^{\ell-1} + h_\ell X^\ell, && h_\ell \neq 0. \end{aligned}$$

(3) Es ist

$$\left.\begin{array}{c} p \mid f_0 \\ p^2 \nmid f_0 \end{array}\right\} \;\Longrightarrow\; \left\{\begin{array}{c} p \mid g_0h_0 \\ p^2 \nmid g_0h_0 \end{array}\right\} \overset{\text{O.B.d.A.}}{\Longrightarrow} \left\{\begin{array}{c} p \mid g_0 \\ p \nmid h_0 \end{array}\right.$$

$$p \nmid f_m \;\Longrightarrow\; p \nmid g_kh_\ell \;\Longrightarrow\; p \nmid g_k$$

Also gibt es ein $j \in \{1,\ldots,k\}$ so, dass

$$p \mid g_0, \qquad p \mid g_1, \qquad \ldots\ldots \qquad p \mid g_j, \qquad p \nmid g_{j+1} \qquad (*)$$

(4) Es ist

$$f_{j+1} \;=\; g_{j+1}h_0 + g_jh_1 + \ldots + g_0h_{j+1}, \qquad \text{wobei } h_k := 0 \text{ für } k > \ell.$$

(5) Weiter

$$\left.\begin{array}{c} p \nmid g_{j+1} \\ p \nmid h_0 \end{array}\right\} \;\Longrightarrow\; \left.\begin{array}{c} p \nmid g_{j+1}h_0 \\ p \mid (g_jh_1 + \ldots + g_0h_{j+1}) \end{array}\right\} \;\Longrightarrow\; p \nmid f_{j+1} \;\Longrightarrow\; j+1 = m.$$

(6) In $(*)$ steht dann also $p \nmid g_m$. Es folgt $g_m \neq 0$ und damit $\deg g = m = \deg f$. Dann ist $\ell = 0$, also $h \in R$.

(7) Da f als primitiv vorausgesetzt wurde, folgt $h \in R^\times$.

(8) Die zweite Aussage folgt mit dem Irreduzibilitätssatz 3.8.1

3.8.8 Beispiel

Das Polynom

$$f \;=\; 3X^5 - 91X^4 + 126X^3 - 77X + 35$$

ist gemäß dem Kriterium von Schönemann-Eisenstein bei Wahl von $p = 7$ irreduzibel.

3.8.9 Beispiel

Es seien $m \in \mathbb{N}$, p eine Primzahl und $f(X) = X^m - p \in \mathbb{Z}[X]$. Das Schönemann-Eisenstein-Kriterium zeigt sofort, dass f irreduzibel in $\mathbb{Z}[X]$ und $(\operatorname{Quot}\mathbb{Z})[X] = \mathbb{Q}[X]$.

Fast genau so leicht ist zu sehen, dass $f(X) = X^m - q \in \mathbb{Z}[X]$ irreduzibel ist, wenn q Produkt von paarweise verschiedenen Primzahlen ist.

Insbesondere ist $\sqrt[m]{q}$ irrational.

3.8.10 Beispiel: Das p-Kreisteilungspolynom

Es seien p eine Primzahl und

$$f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1 \qquad \in \mathbb{Z}[X]$$

das so genannte p-te Kreisteilungspolynom, vgl. später Kapitel **??**.

Es ist, wie man mit Hilfe des Schönemann-Eisenstein-Kriteriums zeigen kann, irreduzibel. (Übung)

3.8.11 Reduktionssatz

Es sei R ein faktorieller Ring und

$$f = f_m X^m + \ldots + f_1 X + f_0 \qquad \in R[X]$$

ein primitives Polynom. I sei Primideal in R und dann

$$\overline{f} = \overline{f_m} X^m + \ldots + \overline{f_1} X + \overline{f_0} \qquad \in (R/I)[X]$$

das projizierte Polynom, vgl. 3.1.7.

Ist

$$f_m \notin I, \qquad \text{d.h.} \quad \overline{f_m} \neq \overline{0},$$

so gilt

$$\begin{array}{rll} & \overline{f} & \text{irreduzibel in } (R/I)[X] \\ \Longrightarrow & f & \text{irreduzibel in } R[X] \\ \Longrightarrow & f & \text{irreduzibel in } (\operatorname{Quot} R)[X]. \end{array}$$

3.8.12 Beweis

Angenommen, das gegebene Polynom f ist in $R[X]$ nicht irreduzibel, es gibt also eine Zerlegung

$$f = g \cdot h \qquad \text{mit } \deg g \geq 1, \quad \deg h \geq 1.$$

in $R[X]$, die sich nach $(R/I)[X]$ vererbt

$$\overline{f} = \overline{g} \cdot \overline{h}.$$

Sind g_k und h_ℓ die Leitkoeffizienten von g und h, so gilt, da R/I Integritätsring, dass

$$0 \neq \overline{f_m} = \overline{g_k} \cdot \overline{h_\ell} \implies \left\{ \begin{array}{rcl} \overline{g_k} & \neq & 0 \\ \overline{h_\ell} & \neq & 0 \end{array} \right. \implies \left\{ \begin{array}{rcl} \deg \overline{g} & = & \deg g \geq 1 \\ \deg \overline{h} & = & \deg h \geq 1, \end{array} \right.$$

also ist $\overline{f}$ nicht irreduzibel in $(R/I)[X]$.

Die zweite Implikation ist wieder eine Konsequenz aus dem Irreduzibilitätssatz 3.8.1.

3.8.13 Beispiel

Das Polynom $2X + 4$ ist reduzibel in $\mathbb{Z}[X]$, das $\bmod 3$ projizierte Polynom $2X + 1$ ist aber irreduzibel in $\mathbb{F}_3[X] = \mathbb{Z}/3\mathbb{Z}$. Es kann also nicht auf die Voraussetzung ,,primitiv" im Reduktionssatz 3.8.11 verzichtet werden.

3.8.14 Beispiel

Das Polynom

$$f(X) \;=\; 5X^3 - 4X^2 + 3X - 9 \qquad \in \mathbb{Z}[X]$$

ist irreduzibel. Das bei Reduktion mod 2 entstehende Polynom

$$\overline{f}(X) \;=\; X^3 + X + 1 \qquad \in (\mathbb{Z}/2\mathbb{Z})[X]$$

ist irreduzibel, da es als Polynom dritten Grades eine Nullstelle in $\mathbb{Z}/2\mathbb{Z}$ haben müsste, aber keine der beiden Zahlen $\overline{0}, \overline{1}$ Nullstelle ist.

Man kann hier elementarer argumentieren: Das Polynom f müsste bei Reduzibilität eine Nullstelle in $\mathbb{Z}$ haben. Setzt man aber eine ungerade bzw. gerade Zahl ein, so ist der Wert immer ungerade, kann niemals Null sein.

3.8.15 Beispiel

Das Polynom

$$f(X) \;=\; X^4 + 12X^3 + 13X^2 - 11X + 10 \qquad \in \mathbb{Z}[X]$$

wird bei Reduktion mod 2 zu dem reduziblen Polynom

$$X^4 + X^2 + X$$

Selbstverständlich kann man nicht schließen, dass auch f reduzibel wäre. Tatsächlich wird es mod 3 zu

$$\overline{f}(X) \;=\; X^4 + X^2 + X + 1 \qquad \in (\mathbb{Z}/3\mathbb{Z})[X]$$

Dieses Polynom hat keine Nullstelle in $\mathbb{Z}/3\mathbb{Z}$, es könnte also höchstens eine Zerlegung in zwei quadratische Polynome haben:

$$f(X) \;=\; (X^2 + aX + b) \cdot (X^2 + cX + d), \qquad (*).$$

Testet man die neun normierten Polynome in $(\mathbb{Z}/3\mathbb{Z})[X]$ durch, so stellt man fest, dass davon nur

$$X^2 + 1, \qquad X^2 + X + 2, \qquad X^2 + 2X + 2$$

irreduzibel sind. Setzt man sie paarweise in $(*)$ ein, so geht das in keinem Fall auf.

Somit ist $\overline{f}$ irreduzibel in $(\mathbb{Z}/3\mathbb{Z})[X]$ und dann f irreduzibel in $\mathbb{Z}[X]$.

3.9 Beweis des Satzes von Gauß

3.9.1 Satz von Gauß

Ist ein Ring R faktoriell, so ist auch der zugehörige Polynomring $R[X]$ faktoriell.

3.9.2 Beweis

(0) Wir zeigen gemäß Definition und Satz 2.2.1 die beiden Eigenschaften ($\mathrm{Ex}_{\mathrm{irr}}$) und ($\mathrm{Ei}_{\mathrm{irr}}$) für $R[X]$. Es sei $f \in R[X] \setminus \{0\}$.

($\mathrm{Ex}_{\mathrm{irr}}$). Per Induktion über $m = \deg f$.

Für $m = 0$ ist ($\mathrm{Ex}_{\mathrm{irr}}$) klar, da R selbst faktoriell ist.

Induktionsschritt. Sei ($\mathrm{Ex}_{\mathrm{irr}}$) für Polynome g mit $\deg g \leq m-1$ gezeigt.

Es ist

$$f \;=\; \operatorname{inh} f \cdot f^{\mathrm{prt}}$$

Da R faktoriell ist, besitzt $\operatorname{inh} f$ eine Zerlegung in irreduzible Elemente.

Das Polynom f^{prt} ist wegen der Primitivität selbst irreduzibel oder es besitzt eine Zerlegung $f^{\mathrm{prt}} = g \cdot h$ in zwei Polynome g, h mit $\deg g \leq m-1$ und $\deg h \leq m-1$. Nach Induktionsvoraussetzung gibt es für g und h Zerlegungen in irreduzible Elemente, damit hat man auch eine für f.

($\mathrm{Ei}_{\mathrm{irr}}$).

(1) Wir nehmen an, es gäbe zwei Zerlegungen

$$\begin{aligned} f &= \underbrace{r_1 \cdot \ldots \cdot r_k}_{=r} \cdot \underbrace{g_1 \cdot \ldots \cdot g_\ell}_{=g} \\ f &= \underbrace{\widetilde{r}_1 \cdot \ldots \cdot \widetilde{r}_{\widetilde{k}}}_{=\widetilde{r}} \cdot \underbrace{\widetilde{g}_1 \cdot \ldots \cdot \widetilde{g}_{\widetilde{\ell}}}_{=\widetilde{g}} \end{aligned}$$

mit irreduziblen Elementen $r_j, \widetilde{r}_j \in R$ und $g_j, \widetilde{g}_j \in R[X] \setminus R$.

(2) Die Polynome $g_j, \widetilde{g}_j \in R[X] \setminus R$ sind irreduzibel und deshalb primitiv. Damit sind gemäß dem Lemma von Gauß 3.7.6 auch die Produkte g und $\widetilde{g}$ primitiv.

(3) Mit Satz 3.7.4 (i) folgt $g \sim \widetilde{g}$ in $R[X]$ und dann $r \sim \widetilde{r}$ in R, also

$$r_1 \cdot \ldots \cdot r_k \;\sim\; \widetilde{r}_1 \cdot \ldots \cdot \widetilde{r}_{\widetilde{k}}$$

(4) Da R faktoriell ist, ist diese Zerlegung (bis auf Assoziiertheit und Reihenfolge der Faktoren) eindeutig, d.h. es ist $k = \widetilde{k}$ und (nach Umnummerierung) $r_j \sim \widetilde{r}_j$ für $j = 1, \ldots, k$.

(5) Wir wechseln jetzt in den Ring $(\operatorname{Quot} R)[X]$ und stellen fest, dass

> der Polynomring $(\operatorname{Quot} R)[X]$ über einem Körper ja bereits als faktoriell erwiesen ist,
>
> die Polynome g_j und $\widetilde{g}_j$ wegen deg ≥ 1 gemäß dem Irreduzibilitätssatz 3.8.1 auch in $(\operatorname{Quot} R)[X]$ irreduzibel sind,

die Assoziiertheit

$$g_1 \cdot \ldots \cdot g_\ell \ \sim \ \widetilde{g}_1 \cdot \ldots \cdot \widetilde{g}_{\widetilde{\ell}}$$

aus Schritt (3) auch in $(\operatorname{Quot} R)[X]$ gilt.

(6) Wegen $(\mathrm{Ei}_{\mathrm{irr}})$ in $(\operatorname{Quot} R)[X]$ gilt $\ell = \widetilde{\ell}$ und dann (nach Umnummerierung) $g_j \sim \widetilde{g}_j$ in $(\operatorname{Quot} R)[X]$, dann gemäß der dritten Implikation in Satz 3.7.8 (iii) auch in $R[X]$.

4 Körpererweiterungen

4.1 Charakteristik und Primkörper

4.1.1 Definition: Charakteristik und Primkörper eines Körpers

1. Für jeden uk Ring R ist die Abbildung

$$\iota : \begin{cases} \mathbb{Z} & \to & R \\ n & \mapsto & \begin{cases} \underbrace{1+\ldots+1}_{n \text{ Summanden}}, & \text{falls } n \geq 1, \\ 0, & \text{falls } n = 0, \\ \underbrace{-(1+\ldots+1)}_{-n \text{ Summanden}}, & \text{falls } n \leq 1, \end{cases} \end{cases}$$

ein Ringhomomorphismus, da sie die Addition erhält und für $j, k \in \mathbb{N}$ gilt

$$\begin{aligned} \iota(jk) &= \underbrace{1+\ldots+1}_{jk \text{ Summanden}} = \underbrace{\underbrace{(1+\ldots+1)}_{j \text{ Summanden}} + \ldots\ldots + \underbrace{(1+\ldots+1)}_{j \text{ Summanden}}}_{k \text{ Klammern}} \\ &= \underbrace{\iota(j) + \ldots\ldots + \iota(j)}_{k \text{ Summanden}} = \iota(j) \cdot \underbrace{(1+\ldots\ldots+1)}_{k \text{ Summanden}} \\ &= \iota(j) \cdot \iota(k). \end{aligned}$$

Auf sie kann der erste Homomorphiesatz 1.6.2 angewandt werden, es existiert ein $m \in \mathbb{Z}$ so, dass

$$\iota(Z) \simeq \mathbb{Z}/\ker(\iota) = \begin{cases} \mathbb{Z}, & \text{falls } \ker(\iota) = \{0\}, \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } \ker(\iota) = m\mathbb{Z}. \end{cases}$$

2. Diese Zahl m heißt die *Charakteristik* $\operatorname{char}(R)$ des Rings.

3. Ist K ein Körper (oder allgemeiner ein Integritätsring), so folgt im Falle $\operatorname{char}(K) = j \cdot k$, dass

$$0 = \iota(jk) = \iota(j) \cdot \iota(k),$$

also wegen der Nullteilerfreiheit $\iota(j) = 0$ oder $\iota(k) = 0$.

Das bedeutet insgesamt, dass ein Körper nur die Charakteristiken 0 oder Primzahl haben kann.

4. Ist $\operatorname{char}(K) = 0$, so ist ι injektiv. Der Ring $\mathbb{Z}$ der ganzen Zahlen kann als in K eingebettet angesehen werden. Dann ist aber auch der Quotientenkörper $\mathbb{Q}$ von $\mathbb{Z}$ in K enthalten.

5. Ist $\mathrm{char}(K) = p$, Primzahl, so ist das Bild $\iota(\mathbb{Z})$ isomorph zum endlichen Körper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Mittels ι kann $\mathbb{F}_p$ als in K enthalten angesehen werden.

6. Der in dem gegebenen Körper K enthaltende Teilkörper

$$\begin{cases} \mathbb{Q}, & \text{falls } \mathrm{char}(K) = 0, \\ \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, & \text{falls } \mathrm{char}(K) = p, \end{cases}$$

heißt der *Primkörper* von K.

4.1.2 Satz und Definition: Monomorphismen von Körpern

Es seien K und $\widetilde{K}$ Körper und

$$\varphi : \begin{cases} K & \to & \widetilde{K} \\ x & \mapsto & \varphi(x) \end{cases}$$

ein (unitärer) Ringhomomorphismus.

(i) Es gilt dann auch $\varphi(x^{-1}) = \varphi(x)^{-1}$ für alle $x \in K^\times$.

(ii) φ ist injektiv.

(iii) Die Charakteristiken von K und $\widetilde{K}$ stimmen überein.

(iv) Die Einschränkung von φ auf den (gemeinsamen) Primkörper ist die Identität.

Wir nennen deshalb eine solche Abbildung einen *Monomorphismus der Körper*.

4.1.3 Beweis

(i) Es ist

$$\varphi(x) \cdot \varphi(x^{-1}) \;=\; \varphi(x \cdot x^{-1}) \;=\; \varphi(1) \;=\; 1.$$

(ii) Ist $x \in K^\times$, so gilt

$$1 \;=\; \varphi(1) \;=\; \varphi(x \cdot x^{-1}) \;=\; \varphi(x) \cdot \varphi(x^{-1}),$$

also $\varphi(x) \in \widetilde{K}^\times$. Es folgt $\ker \varphi = \{0\}$.

(iii) Wegen $\iota : \mathbb{Z} \to K \to \widetilde{K}$ ist $\ker(\mathbb{Z} \to \widetilde{K}) \subseteq \ker(\mathbb{Z} \to K)$. Diese beiden Mengen sind $\{0\}$ oder $p\mathbb{Z}$. Eine Inklusion lässt sich nur herstellen, wenn die beiden Kerne gleich sind oder im Falle $\mathrm{char}\, K = p$ und $\mathrm{char}\, \widetilde{K} = 0$.

Dieser zweite Fall würde aber bedeuten, dass auch der Primkörper $\mathbb{F}_p$ von K in $\widetilde{K}$ eingebettet werden kann. Wegen

$$\underbrace{1 + \ldots + 1}_{p \text{ Sdn.}} \;=\; 0 \qquad \in \mathbb{F}_p$$

folgt

$$p \;=\; \varphi(1) + \ldots + \varphi(1) \;=\; \varphi(1 + \ldots + 1) \;=\; \varphi(0) \;=\; 0 \qquad \in \widetilde{K}$$

und das ist ein Widerspruch.

(iv) Der Primkörper wird von dem Element $1 \in K$ erzeugt. Wegen $\varphi(1) = 1$ folgt die Behauptung.

4.2 Körpererweiterungen und Zwischenkörper

4.2.1 Definition: Körpererweiterung und Zwischenkörper

Es seien zwei Körper K und L gegeben, so dass K ein Unterkörper von L ist. Man spricht dann von einer *Körpererweiterung*, symbolisch schreibt man $L : K$.

Ist M ein weiterer Körper mit $K \subseteq M \subseteq L$, so heißt M ein *Zwischenkörper* der Körpererweiterung $L : K$.

Durch M entstehen die Körpererweiterungen $L : M$ und $M : K$. Wir schreiben diese Situation auch kurz als $L : M : K$.

Da eine Körpererweiterung die Existenz einer Einbettung $K \to L$ bedeutet, müssen K und L gemäß Satz 4.1.2 (iii) gleich Charakteristik haben.

4.2.2 Bemerkung

Das Programm bei Körpererweiterungen unterliegt dann den zwei folgenden Gesichtspunkten.

- Es ist ein ,,großer" Körper L gegeben. Man will einen Überblick über die Unterkörper M gewinnen.
- Es ist ein ,,kleiner" Körper K gegeben. Man sucht Oberkörper M, die in ,,gewisser Weise bessere Eigenschaften" haben.

4.2.3 Definition: Monomorphismen von Körpererweiterungen

1. Sind $L : K$ und $\widetilde{L} : K$ Körpererweiterungen, so heißt ein Monomorphismus von Körpern $\varphi : L \to \widetilde{L}$ ein *Monomorphismus von Körpererweiterungen* oder besser, ein *K-Monomorphismus*, wenn die Einschränkung auf K die Identität ist,

   $$\varphi|_K \;=\; \mathrm{id}_K.$$

   Wir schreiben dann auch $\varphi : \quad L : K \to \widetilde{L} : K$.

2. Entsprechend gibt es wieder die Begriffe Isomorphismus und Automorphismus von Körpererweiterungen.

4.3 Erzeugung von Zwischenringen und Zwischenkörpern

4.3.1 Definition: Erzeugung von Zwischenringen und Zwischenkörpern

Es sei $L : K$ eine Körpererweiterung.

1. Ist A eine beliebige Zwischen**menge**, $K \subseteq A \subseteq L$, so ist der Schnitt aller uk Ringe, die die Teilmenge A enthalten,

$$\bigcap_{K \cup A \subseteq R \subseteq L,\, R \text{ uk Ring}} R$$

   ein uk Zwischen**ring**. Wir nennen ihn den *(von A) erzeugten Zwischenring*. Symbolisch schreibt man dafür $K[A]$.

2. Ist A eine beliebige Zwischen**menge**, $K \subseteq A \subseteq L$, so ist der Schnitt aller Zwischenkörper M, die die Teilmenge A enthalten,

$$\bigcap_{K \cup A \subseteq M \subseteq L,\, M \text{ Körper}} M$$

   ebenfalls ein Zwischen**körper**. Wir nennen ihn den *(von A) erzeugten Zwischenkörper*. Symbolisch schreibt man dafür $K(A)$.

3. Man spricht auch davon, dass der uk Ring $K[A]$ bzw. der Körper $K(A)$ durch *(innere) Adjunktion* von A an K entstanden sind.

   Leider wird in den Symbolen $K[A]$ und $K(A)$ und beim Begriff ,,Adjunktion von A an K" unterschlagen, dass auch der Oberkörper L maßgeblich ist.

4. Ist $A = \{a_1, \ldots, a_n\} \subseteq L$ eine endliche Menge, so schreibt man auch

$$K[A] \;=\; K[a_1, \ldots, a_n] \qquad \text{bzw.} \qquad K(A) \;=\; K(a_1, \ldots, a_n).$$

5. Enthält $A = \{a\} \subseteq L$ nur ein einziges Element, so schreibt man auch

$$K[A] \;=\; K[a] \qquad \text{bzw.} \qquad K(A) \;=\; K(a).$$

6. Gibt es zu einem Zwischenkörper M eine endliche Teilmenge $A \subseteq M$ mit $M = K(A)$, so heißt M *endlich erzeugt*.

7. Gibt es zu einem Zwischenkörper M ein $a \in L$ mit $M = K(a)$, so heißt R *einfach* und a heißt ein *primitives Element*.

8. Es sei als Erinnerung (und Anlehnung an die Schulmathematik) darauf hingewiesen, dass

   - $K[a]$ alle ,,polynomialen Ausdrücke" mit Polynomen
   - $K(a)$ alle ,,rationalen Ausdrücke" mit Quotienten von Polynomen

   enthält, die Elemente aus K als Koeffizienten haben und bei denen a anstelle der Variablen X eingesetzt ist.

4.4 Der Grad einer Körpererweiterung

4.4.1 Definition: Grad einer Körpererweiterung

Es ist leicht einzusehen, dass (durch die Multiplikation von K auf der abelschen Gruppe L) auf L die Struktur eines K-Vektorraums gegeben ist.

Aus der linearen Algebra ist bekannt, dass dann gleichmächtige Basen dieses K-Vektorraums existieren.

Man nennt die Dimension, also die Mächtigkeit einer solchen Basis, den *Grad (der Körpererweiterung)* $L : K$, symbolisch

$$[L : K] \quad = \quad \dim_K(L).$$

4.4.2 Satz: Gradformel

Ist M ein Zwischenkörper der Körpererweiterung $L : K$, so gilt

$$[L : K] \quad = \quad [L : M] \cdot [M : K].$$

4.4.3 Beweis

(0) Es ist nur der Fall beweisbedürftig, dass alle drei Zahlen endlich sind. Dieser Beweis lässt sich allein mit linearer Algebra führen.

(1) Wir werden zeigen: Ist

$$\begin{array}{ll} (u_1, \ldots, u_m) & \text{eine Basis des } K\text{-Vektorraums } M \quad \text{und} \\ (v_1, \ldots, v_\ell) & \text{eine Basis des } M\text{-Vektorraums } L, \end{array}$$

so bilden die Produkte

$$(u_1v_1, u_1v_2, \ldots, u_mv_{\ell_1}, u_mv_\ell) \text{ eine Basis des } K\text{-Vektorraums } L.$$

(2) Zu jedem Basisvektor $v_k \in M$ existieren $\alpha_{jk} \in K$ so, dass

$$v_k \quad = \quad \alpha_{1,k}u_1 + \ldots + \alpha_{m,k}u_m.$$

(3) Ist $x \in L$ beliebig, so existieren $\beta_k \in M$ so, dass

$$x \quad = \quad \beta_1v_1 + \ldots + \beta_\ell v_\ell.$$

Jedes β_k wiederum lässt sich mit $\gamma_{j,k} \in K$ darstellen als

$$\beta_k \quad = \quad \gamma_{1,k}u_1 + \ldots + \gamma_{m,k}u_m.$$

Dann gilt

$$\begin{aligned} x \quad &= \quad \beta_1v_1 + \ldots + \beta_\ell v_\ell \\ &= \quad (\gamma_{1,1}u_1 + \ldots + \gamma_{m,1}u_m)v_1 + \ldots + (\gamma_{1,\ell}u_1 + \ldots + \gamma_{m,\ell}u_m)v_\ell \\ &= \quad \gamma_{1,1}u_1v_1 + \ldots + \gamma_{m,\ell}u_mv_\ell. \end{aligned}$$

also lässt sich x als Linearkombination der Produkte $u_j \cdot v_k$ darstellen.

(4) Die Produkte sind linear unabhängig, denn es gilt

$$\begin{aligned}
& \gamma_{1,1}u_1v_1 + \ldots + \gamma_{m,\ell}u_mv_\ell \;=\; 0 \\
\Longrightarrow\; & (\gamma_{1,1}u_1 + \ldots + \gamma_{m,1}u_m)v_1 + \ldots + (\gamma_{1,\ell}u_1 + \ldots + \gamma_{m,\ell}u_m)v_\ell \;=\; 0 \\
& \text{(Linearkombination in } L \text{ mit Koeffizienten aus } M) \\
\Longrightarrow\; & \gamma_{1,j}u_1 + \ldots + \gamma_{m,j}u_m \;=\; 0 \qquad \forall\, j \in \{1, \ldots, \ell\} \\
& \text{(Linearkombinationen in } M \text{ mit Koeffizienten aus } K) \\
\Longrightarrow\; & \gamma_{j,k} \;=\; 0 \qquad \forall\, j, k.
\end{aligned}$$

4.4.4 Folgerung: Existenz und Eindeutigkeit von Zwischenkörpern

Es seien $M\widetilde{M}$ Zwischenkörper der endlichen Körpererweiterung $L : K$ mit $M \subseteq \widetilde{M}$.

(i) Ist $[L : M] = [L : \widetilde{M}]$, so folgt $M = \widetilde{M}$.

(ii) Ist $[M : K] = [\widetilde{M} : K]$, so folgt $M = \widetilde{M}$.

(iii) Ist $[L : K]$ eine Primzahl, so folgt $M = K$ oder $M = L$.

4.4.5 Beispiele

1. Die quadratischen Zahlkörpererweiterungen $(\mathbb{Q} + \mathbb{Q}\sqrt{d}) : \mathbb{Q}$ haben Grad 2 und können deshalb keine echten Zwischenkörper haben.

2. Die Körpererweiterung $\mathbb{C} : \mathbb{R}$ hat Grad 2 und kann deshalb keinen echten Zwischenkörper haben.

4.5 Transzendente Elemente

4.5.1 Definition und Satz: Transzendentes Element

Es sei $L : K$ eine Körpererweiterung. Für ein Element $a \in L$ sind die folgenden Aussagen äquivalent.

(A) (def) a heißt *transzendent (über K).*

(B) Es gibt kein Polynom $f \in K[X] \setminus \{0\}$ so, dass a Nullstelle von f wäre.

(C) Der Einsetz-Homomorphismus

$$\varepsilon_a : \left\{ \begin{array}{rcl} K[X] & \to & L \\ f & \mapsto & f(a) \end{array} \right.$$

ist injektiv. Anders ausgedrückt: Zwei polynomiale Ausdrücke in a sind verschieden, wenn die beiden Polynome verschieden sind.

(D) Es gibt eine unendliche streng absteigende Kette von Körpern zwischen $K(a)$ und K wie folgt

$$K(a) \supsetneqq K(a^2) \supsetneqq K(a^4) \supsetneqq \ldots\ldots \supsetneqq K.$$

(E) Es ist $[K(a) : K] = \infty$.

4.5.2 Beweis

Die Äquivalenz (B) $\Leftrightarrow$ (C) ist nur eine konkret-abstrakte Umformulierung.

(C) $\Rightarrow$ (D). Zunächst ist $K(a^{2^{n+1}}) \subset K(a^{2^n})$ klar. Wäre $a^{2^n} \in K(a^{2^{n+1}})$, so gäbe es zwei normierte Polynome $f, g \in K[X] \setminus \{0\}$ so, dass

$$a^{2^n} = \frac{f(a^{2^{n+1}})}{g(a^{2^{n+1}})}.$$

Daraus folgt aber

$$a^{2^n} \cdot g(a^{2^{n+1}}) - f(a^{2^{n+1}}) = 0.$$

Das Polynom

$$X \cdot g(X^2) - f(X^2)$$

ist Differenz eines ungeraden und geraden Anteils, damit ungleich Null. Es hat a^{2^n} als Nullstelle. Damit gibt es ein Polynom mit a als Nullstelle. Widerspruch.

(D) $\Rightarrow$ (E) ist wegen der Gradformel trivial.

(E) $\Rightarrow$ (B). Diese Implikation stimmt mit der Implikation (B) $\Rightarrow$ (E) in Satz 5.1.1 überein und wird dort bewiesen.

4.5.3 Definition: Transzendente Körpererweiterung

Eine Körpererweiterung $L : K$ heißt *transzendent*, wenn L mindestens ein über K transzendentes Element enthält.

5 Endliche und algebraische Körpererweiterungen

5.1 Algebraische Elemente

5.1.1 Definition und Satz: Algebraisches Element und Minimalpolynom

Es sei $L : K$ eine Körpererweiterung. Weiter seien $a \in L$ und $n \in \mathbb{N}$.

(i) Die folgenden Aussagen sind äquivalent.

(A) (def) a heißt *algebraisch (über K mit Grad n).*

(B) Es gibt ein Polynom $f \in K[X] \setminus \{0\}$ so, dass a Nullstelle von f ist.

Es gibt dann auch ein normiertes irreduzibles Polynom $\mu_a \in K[X]$ mit $\deg \mu_a = n$ so, dass a Nullstelle von μ_a ist.

(C) Die Folge $(1, a, a^2, \ldots, a^{n-1})$ ist eine Basis des K-Vektorraums $K[a]$.

(D) Der Einsetzungshomomorphismus

$$\varepsilon_a : \left\{ \begin{array}{rcl} K[X] & \to & L \\ g & \mapsto & g(a) \end{array} \right.$$

ist nicht injektiv. Der K-Vektorraum

$$K[a] \;=\; \operatorname{im} \varepsilon_a \;\simeq\; K[X]/\ker \varepsilon_a$$

hat die Dimension n.

(E) Der Ring $K[a]$ stimmt bereits mit dem Körper $K(a)$ überein und es gilt

$$[K(a) : K] \;=\; n.$$

(ii) Das in (i)/(B) beschriebene Polynom μ_a ist durch jede der folgenden äquivalenten Eigenschaften eindeutig festgelegt.

- μ_a heißt das *Minimalpolynom (von $a \in L$).*
- $\mu_a = \mathrm{ggT}(\ker \varepsilon_a)$.
- μ_a ist enthalten in $\ker \varepsilon_a$, normiert und irreduzibel (= prim).
- μ_a ist enthalten in $\ker \varepsilon_a$, normiert und hat minimalen Grad in $\ker \varepsilon_a$.

5.1.2 Beweis

Die innerhalb von (i)/(B) angegebene Aussage und die in (ii) konstatierten Äquivalenzen sind ringtheoretischer Natur. Der Hintergrund ist im wesentlichen, dass $K[X]$ ein euklidischer Ring mit euklidischer Bewertung $E(f) = \deg f$ und damit ein Hauptidealring ist.

Das eindeutige normierte irreduzible Polynom, das das Ideal $\ker \varepsilon_a$, siehe (C), erzeugt, ist eben das Minimalpolynom.

Zu (i).

(B) $\Rightarrow$ (C). Da a Nullstelle von μ_a ist, gilt in L

$$(\mu_a)_0 + (\mu_a)_1 \cdot a + \ldots + (\mu_a)_{n-1} \cdot a^{n-1} + a^n \;=\; 0,$$

und damit

$$a^n \;=\; -\Big((\mu_a)_0 + (\mu_a)_1 \cdot a + \ldots + (\mu_a)_{n-1} \cdot a^{n-1}\Big).$$

Damit ist jede Potenz a^j, $j \geq n$, eine K-Linearkombination von $(1, a, a^2, \ldots, a^{n-1})$ in $K[a]$.

Angenommen, die Folge $(1, a, a^2, \ldots, a^{n-1})$ sei linear abhängig in L. Dann existieren $f_j \in K$ mit

$$f_0 \cdot 1 + f_1 \cdot a + f_2 \cdot a^2 + \ldots + f_{n-1} \cdot a^{n-1} \;=\; 0.$$

Das ist aber ein Polynom ungleich Null vom Grad $n-1$, das a als Nullstelle hat. Das ist ein Widerspruch zum minimalen Grad von μ_a.

(C) $\Rightarrow$ (B). Da die Menge $\{1, a, \ldots, a^n\}$ linear abhängig ist, gibt es $f_0, \ldots, f_n \in K$, nicht alle gleich Null, so dass

$$f_0 + f_1 a + \ldots + f_n a^n \;=\; 0.$$

Damit ist ein Polynom mit a als Nullstelle gefunden.

(D) ist eine abstrakte Umformulierung der in (B) und (C) getätigten Aussagen.

(D) $\Rightarrow$ (E). Es ist

$$K[a] \;=\; \operatorname{im} \varepsilon_a \;\simeq\; K[X]/\ker \varepsilon_a \;=\; K[X]/(\mu_a).$$

Das Hauptideal $(\mu_a) \subseteq K[X]$ wir von dem irreduziblen Element μ_a erzeugt, ist also ein maximales Ideal. Deshalb ist $K[a]$ bereits ein Körper und es gilt $K(a) = K[a]$.

Evtl. blickt man dabei nochmal auf die Definitionen von $K(a)$ und $K[a]$ in Abschnitt 4.3.1.

(E) $\Rightarrow$ (B) Die Teilmenge $\{1, a, \ldots, a^n\} \subseteq K(a)$ muss linear abhängig sein, es gibt also ein Polynom $f \neq 0$ mit $\deg f = n$ und $f(a) = 0$. Normierung liefert die Aussage über den Grad des Minimalpolynoms.

5.1.3 Beispiel

Innerhalb der Körpererweiterung $\mathbb{C} : \mathbb{R}$ ist $i \in \mathbb{C} \setminus \mathbb{R}$ algebraisch mit Minimalpolynom $\mu_i = X^2 + 1$ und dann $[\mathbb{C} : \mathbb{R}] = 2$.

5.1.4 Beispiel

Innerhalb der Körpererweiterung $\mathbb{C} : \mathbb{Q}$ sei $a \in \mathbb{C} \setminus \mathbb{Q}$ mit $b = a^2 \in \mathbb{Q}$.

Dann ist $\mathbb{Q}[a] = \mathbb{Q}(a)$ mit Minimalpolynom $X^2 - b \in \mathbb{Q}[X]$.

Ist $a = d \in \mathbb{Z}$ quadratfrei, so ergeben sich die schon mehrfach betrachteten Körper

$$\mathbb{Q}(d) \;=\; \mathbb{Q} + \mathbb{Q}\sqrt{d}$$

mit $[\mathbb{Q}(d) : \mathbb{Q}] = 2$. Wir hatten dabei schon festgestellt, dass die linearen Polynome $u + v\sqrt{d} \neq 0$ invertierbar sind, also $\mathbb{Q}[d] = \mathbb{Q}(d)$ gilt.

5.1.5 Beispiel

In Übung A22. hatten wir gesehen, dass das p-te Kreisteilungspolynom

$$f(X) = X^{p-1} + X^{p-2} + \ldots + X + 1 \qquad \in \mathbb{Z}[X], \qquad p \text{ Primzahl}$$

irreduzibel ist. Es hat $\zeta_p := e^{\frac{2\pi i}{p}} \in \mathbb{C}$ als Nullstelle.

Damit ist ζ_p algebraisch über $\mathbb{Q}$, es gilt $\mathbb{Q}(\zeta_p) = \mathbb{Q}[\zeta_p]$ mit $[\mathbb{Q}(\zeta_p); \mathbb{Q}] = p - 1$.

5.1.6 Beispiel

Wir betrachten den uk Ring

$$Q \;=\; \mathbb{Q} + \mathbb{Q}\sqrt{2} + \mathbb{Q}\sqrt{3} + \mathbb{Q}\sqrt{6}$$

aus Beispiel 1.1.5/10 und Übung A3.

Der Teilaufgabe A3(a) lässt sich entnehmen, dass für $a := \sqrt{2} + \sqrt{3}$ gilt

$$a^4 - 10a^2 + 1 \;=\; 0$$

und dann, dass

$$\mu_a(X) \;=\; X^4 - 10X^2 + 1$$

das Minimalpolynom von a ist, da es kein Polynom f kleineren Grades gibt mit $f(a) = 0$.

Der Satz 5.1.1 sagt nun aus, dass $Q = \mathbb{Q}[a] = \mathbb{Q}(a)$ ein Körper ist mit $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

Es stellt sich die Frage, wie inverse Elemente berechnet werden.

5.2 Endliche Körpererweiterungen

5.2.1 Definitionen: Endliche und algebraische Körpererweiterungen

Eine Körpererweiterung $L : K$ heißt ...

1. *endlich*, wenn der Grad $[L : K]$ endlich ist.
2. *algebraisch-endlich-erzeugt*, wenn $L : K$ endlich-erzeugt ist und dabei die erzeugenden Elemente $a_1, \ldots, a_n \in L = K(a_1, \ldots, a_n)$ algebraisch über K sind.
3. *algebraisch-einfach*, wenn es ein algebraisches Element $a \in L$ gibt so, dass $L = K(a)$.
4. *algebraisch*, wenn alle Elemente $a \in L$ algebraisch über K sind.

5.2.2 Bemerkungen

Beachte, dass das Wort ,,endlich" hier in zwei wohl zu unterscheidenden Bedeutungen auftritt.

Gemäß der Definition (A) $\Leftrightarrow$ (B) bedeutet ,,endliche Körpererweiterung" $L : K$ nichts anderes, als dass L ein endlich-dimensionaler K-Vektorraum ist. Eigentlich wäre hier die Benutzung des Wortes ,,endlich-dimensional" anstelle von ,,endlich" günstiger.

Das Wort ,,endlich-erzeugt" nimmt Bezug auf die Definition in 4.3.1. und meint eben ,,endlich viele Elemente erzeugen L".

5.2.3 Hauptsatz über endliche Körpererweiterungen

Für eine Körpererweiterung $L : K$ sind die folgenden Aussagen äquivalent.

(A) $L : K$ ist algebraisch-endlich-erzeugt.

(B) $L : K$ ist endlich.

(C) $L : K$ ist endlich und algebraisch.

5.2.4 Bemerkung

Die Implikation (A) $\Rightarrow$ (C) ist trotz der ähnlichen Wörter alles andere als trivial oder ,,direkt-in-ein-zwei-zeilen-beweisbar". Tatsächlich ist zu ihrem Beweis der ,,Umweg" über die Aussage (B) entscheidend. Dabei sind die Beweise der Implikationen (A) $\Rightarrow$ (B) $\Rightarrow$ (C) letztlich linear-algebraisch.

5.2.5 Beweis

(A) $\Rightarrow$ (B). Es sei $L = K(a_1, \ldots, a_n)$ mit algebraischen Elementen $a_j \in L$. Wir zeigen die Behauptung mit Induktion über n.

$n = 1$. Das ist die Implikation (A) $\Rightarrow$ (E) aus Satz 5.1.1.

$n - 1 \to n$. Nach Voraussetzung ist a_n algebraisch über K, also erst recht über $K(a_1, \ldots, a_{n-1})$.

Gemäß Gradformel ist

$$[K(a_1,\ldots,a_n):K] \;=\; [K(a_1,\ldots,a_n):K(a_1,\ldots,a_{n-1})]\cdot[K(a_1,\ldots,a_{n-1}):K]$$

und die rechte Seite ist wegen Induktionsanfang und Induktionsvoraussetzung endlich.

(B) $\Rightarrow$ (C). Es seien $[L:K]=d$ und $a\in L\setminus K$. Die $d+1$ Elemente $1,a,a^2,\ldots,a^d$ sind als Vektoren im d-dimensionalen K-Vektorraum L linear abhängig. Es gibt also Koeffizienten $f_j\in K$, nicht alle Null, mit

$$f_0+f_1a+f_2\,a^2+\ldots+f_d\,a^d \;=\; 0.$$

Damit hat man ein Polynom $f\in K[X]\setminus\{0\}$ gefunden, das a als Nullstelle hat, also ist a algebraisch über K.

(C) $\Rightarrow$ (A). Eine endliche Basis $\{a_1,\ldots,a_d\}$ des K-Vektorraums L ist eine Teilmenge von L, die L algebraisch-endlich-erzeugt.

5.2.6 Beispiel

Die Körpererweiterung $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ über $\mathbb{Q}$ ist algebraisch-endlich erzeugt. Aufgrund der Implikation (A) $\Rightarrow$ (C) gibt es auch zu den Zahlen

$$\sqrt{2}+\sqrt{3},\qquad \sqrt{2}-\sqrt{3},\qquad \sqrt{2}\cdot\sqrt{3},\qquad \sqrt{2}:\sqrt{3},$$

$$\frac{[3(\sqrt{2})^5+8(\sqrt{3})^7]\cdot[3(\sqrt{2})^9-11(\sqrt{3})^{23}]-(\sqrt{2})^{17}\cdot(\sqrt{3})^{23}}{[7\sqrt{2}-15\sqrt{3}]^{23}\cdot[13\sqrt{2}+19\sqrt{3}]^{-47}}$$

Polynome in $K[X]$, die sie als Nullstellen haben.

5.3 Algebraische Körpererweiterungen

5.3.1 Satz: Übertragung der Algebraizität

Es sei $L : K$ eine Körpererweiterung mit Zwischenkörper M. Dann gilt

$$\left.\begin{array}{l} L : M \text{ algebraisch} \\ M : K \text{ algebraisch} \end{array}\right\} \iff L : K \text{ algebraisch.}$$

5.3.2 Beweis

Die Richtung $\Leftarrow$ ist trivial.

$\Rightarrow$. Hier wenden wir dreimal den Hauptsatz über endliche Körpererweiterungen 5.2.3 an.

Es sei also $a \in L$. Da a algebraisch über M ist, gibt es ein Polynom

$$f \;=\; f_0 + f_1 X + \ldots + f_m X^m \qquad \in M[X]$$

mit $f(a) = 0$. Es sei $F := \{f_0, \ldots, f_m\} \subseteq M$. Betrachte nun das Diagramm von Körpererweiterungen

$$L \;:\; \begin{array}{c} M \\ K(a,F) \end{array} \;:\; K(F) \;:\; K.$$

Da $M : K$ algebraisch, ist auch $K(F) : K$ algebraisch, also algebraisch-endlich-erzeugt. Gemäß dem Hauptsatz ist $[K(F) : K] < \infty$.

Auch $K(a, F) : K(F)$ algebraisch-endlich-erzeugt, also gemäß Hauptsatz $[K(a, F) : K(F)] < \infty$.

Mit der Gradformel folgt

$$[K(a,F) : K] \;=\; [K(a,F) : K(F)] \cdot [K(F) : K] \;<\; \infty.$$

Gemäß Hauptsatz ist $K(a, F) : K$ algebraisch und damit a algebraisch über K.

5.3.3 Beispiele

1. Die Körpererweiterungen $(\mathbb{Q} + \mathbb{Q}\sqrt{d}) : Q$ sind algebraisch. Jedes einzelne Element $u + v\sqrt{d}$ ist Nullstelle des quadratischen Polynoms

   $$X^2 - 2uX + (u^2 - dv^2) \quad \in \mathbb{Q}[X],$$

   wie man leicht nachrechnen kann.

2. Eine beliebige komplexe Zahl $u + iv$ ist Nullstelle des Polynoms

   $$X^2 - (u^2 + v^2) \quad \in \mathbb{R}[X],$$

   also ist die Körpererweiterung $\mathbb{C} : \mathbb{R}$ algebraisch.

3. $\mathbb{R} : \mathbb{Q}$ ist nicht algebraisch, da es beispielsweise für die beiden Zahlen e und π keine Polynome mit rationalen Koeffizienten gibt, die e bzw. π als Nullstellen haben.

4. Die Körpererweiterung $(\mathbb{Q}+\mathbb{Q}\sqrt{2}+\mathbb{Q}\sqrt{3}+\mathbb{Q}\sqrt{6}) : \mathbb{Q}$ ist algebraisch. Jedes Element ist Nullstelle eines rationalen Polynoms höchstens vierten Grades.

5.3.4 Satz: Zwischenkörper der algebraischen Elemente

In einer Körpererweiterung $L : K$ definieren wir die Teilmenge

$$M_{\text{alg}} := \{a \in L \mid a \text{ algebraisch über } K\}.$$

Dann gilt

(i) M_{alg} ist ein Zwischenkörper, wir erhalten die zwei Körpererweiterungen

$$L : M_{\text{alg}} : K.$$

(ii) $M_{\text{alg}} : K$ ist algebraisch.

(iii) Die Teilmenge der algebraischen Elemente in $L : M_{\text{alg}}$ ist M_{alg} selbst.

5.3.5 Beweis

(i) Wir betrachten zu $a, b \in M_{\text{alg}}$ die algebraisch-endlich-erzeugte Körpererweiterung $K(a, b) : K$. Gemäß dem Hauptsatz 5.2.3 ist sie algebraisch. Es gilt also $K(a, b) \subseteq M_{\text{alg}}$, demzufolge sind $a + b, a - b, a \cdot b \in M_{\text{alg}}$ und $ab^{-1} \in M_{\text{alg}}$, falls $b \neq 0$.

(ii) ist klar nach Definition von ,,algebraischer Erweiterung".

(iii) Ist $a \in L$ algebraisch über M_{alg}, so ist $M_{\text{alg}}(a) : M_{\text{alg}}$ gemäß dem Hauptsatz 5.2.3 algebraisch.

Da $M_{\text{alg}} : K$ algebraisch ist, ist gemäß Satz 5.3.1 auch $M_{\text{alg}}(a) : K$ algebraisch, also a algebraisch über K.

5.3.6 Zusatz

Es sei $L : K$ eine algebraische Körpererweiterung und $C \in \mathbb{N}$.

Ist für jeden Zwischenkörper M mit $[M : K] < \infty$ sogar

$$[M : K] \leq C,$$

so gilt auch

$$[L : K] \leq C.$$

5.3.7 Beweis

Angenommen, es wäre $[L : K] > C$. Definiere dann rekursiv eine Folge $a_1, a_2, \ldots$ in L so, dass

$$a_j \in L \setminus K(a_1, \ldots, a_{j-1}).$$

Es gilt dann für alle j

$$\begin{aligned} [K(a_1, \ldots, a_j) : K] &= [K(a_1, \ldots, a_j) : K(a_1, \ldots, a_{j-1})] \cdot [K(a_1, \ldots, a_{j-1}) : K] \\ &> [K(a_1, \ldots, a_{j-1}) : K]. \end{aligned}$$

Es liesse sich also eine streng monoton wachsende Folge von Körpererweiterungen in $L : K$ konstruieren, die dann irgendwann im Widerspruch zur Voraussetzung $[M : K] \leq C$ steht.

5.4 Algebraisch abgeschlossene Körper, algebraischer Abschluss

5.4.1 Definition

Für einen Körper K sind die folgenden Aussagen äquivalent.

(A) (def) K heißt *algebraisch abgeschlossen*.

(B) Jedes Polynom $f \in K[X] \setminus \{0\}$ hat mindestens eine Nullstelle in K.

(C) Zu jedem Polynom $f \in K[X] \setminus \{0\}$ mit $\deg f = m$ gibt es $a_1 \ldots, a_m \in K$ so, dass

$$f(X) \;=\; f_m \cdot (X - a_1) \cdot \ldots \cdot (X - a_m).$$

(D) Ein Polynom $f \in K[X] \setminus \{0\}$ ist genau dann irreduzibel, wenn $\deg f = 1$.

(E) Ist $L : K$ eine algebraische Körpererweiterung, so gilt $L = K$.

5.4.2 Beweis

Die Äquivalenz der Aussagen (B) bis (D) entstammt der Theorie der Polynomringe über Körpern.

(E) $\Rightarrow$ (B) ist trivial.

(C) $\Rightarrow$ (E). Sei $a \in L$. Da a algebraisch ist, gibt es ein $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$. Gemäß (C) sind aber alle Nullstellen in K, also auch $a \in K$.

5.4.3 Definition: Algebraischer Abschluss

Für eine Körpererweiterung $L : K$ sind die folgenden Aussagen äquivalent.

(A) (def) $L : K$ heißt *algebraischer Abschluss*

oder auch: L heißt *algebraischer Abschluss* von K.

(B) $L : K$ ist algebraisch und L ist algebraisch abgeschlossen.

(C) $L : K$ ist eine maximale algebraische Erweiterung, d.h.:

Ist $\widetilde{L} : K$ eine algebraische Erweiterung mit Zwischenkörper L, so ist $\widetilde{L} = L$.

5.4.4 Beweis

(B) $\Rightarrow$ (C). Ist $a \in \widetilde{L}$, so ist das Element a algebraisch über K. Es ist dann Nullstelle eines Polynoms $f \in K[X] \setminus \{0\} \subseteq L[X] \setminus \{0\}$. Da L algebraisch abgeschlossen ist, gilt $a \in L$.

(C) $\Rightarrow$ (B). Da L Zwischenkörper der algebraischen Erweiterung $\widetilde{L} : K$ ist, ist $L : K$ algebraisch.

Sei a eine Nullstelle des Polynoms $f \in L[X]\setminus\{0\}$. Wir setzen $\widetilde{L} := L(a)$. Dann ist $L(a) : K$ gemäß Satz 5.3.1 algebraisch, mit der Aussage in (C) folgt $L(a) = L$, also $a \in L$.

5.4.5 Satz

Ist in der Körpererweiterung $L : K$ der Körper L algebraisch abgeschlossen, so ist die Teilmenge

$$\overline{K} := M_{\text{alg}} \;=\; \{a \in L \mid a \text{ algebraisch über } K\}.$$

ein algebraischer Abschluss von K.

5.4.6 Beweis

Die beiden in 5.4.3(B) genannten Eigenschaften sind gerade die in Satz 5.3.4 (ii) und (iii) erwähnten.

5.4.7 Beispiel

Wir betrachten die Körpererweiterung $\mathbb{C} : \mathbb{Q}$. Der Körper

$$\overline{\mathbb{Q}} \;=\; \{a \in \mathbb{C} \mid a \text{ algebraisch über } \mathbb{Q}\}.$$

ist der algebraische Abschluss von $\mathbb{Q}$. Seine Elemente heißen *algebraische Zahlen*.

Wie man mit Mitteln der Analysis zeigen kann, sind die Zahlen e (Hermite, 1873) und π (Lindemann, 1882) nicht algebraisch, sie sind also *transzendente Zahlen*. Es gilt also $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$.

Diese echte Inklusion kann man auch dadurch nachweisen, dass man die Abzählbarkeit von $\overline{\mathbb{Q}}$ zeigt.

5.4.8 Satz: Es gibt immer einen algebraischer Abschluss

Zu jedem Körper existiert ein algebraischer Abschluss $\overline{K}$ des Körpers K.

5.4.9 Bemerkungen

1. Dieser Satz lässt sich mit abstrakt-algebraisch-mengentheoretischen Mitteln, insbesondere mit dem Lemma von Zorn beweisen. Erstmals wurde dies von Steinitz (1910) mit Hilfe der so genannten ,,transfiniten Induktion" durchgeführt, ein Beweis nach Emil Artin (mit Hilfe des Lemmas von Zorn) ist in Fischer, Kap. III 2.5, zu finden.

2. Tatsächlich ist ein solcher algebraischer Abschluss bis auf Isomorphie eindeutig.

3. Ist K ein Unterkörper von $\mathbb{C}$, so lässt sich der Satz leicht auf der Grundlage des Fundamentalsatzes der Algebra beweisen.

4. Ist K ein endlicher Körper, so lässt sich der Satz vergleichsweise einfach mit vollständiger Induktion nachweisen. Siehe später.

5. Die Existenz eine algebraischen Abschlusses für beliebige K ist eine ziemlich starke und praktisch verwertbare Aussage.

6. Für die noch zu entwickelnde Theorie werden wir den Satz nicht verwenden, es genügt die Existenz eines so genannten Zerfällungskörpers für ein einziges Polynoms $f \in K[X]$ — und eben nicht alle — zu beweisen.

7. Die Situation ist ähnlich zu einer in der Linearen Algebra. Dort wird per Axiom die Existenz einer Basis für beliebige Vektorräume konstatiert. Bei endlichdimensionalen Vektorräumen weiß man das a priori.

6 Normale Körpererweiterungen

6.1 Einstieg

6.1.1 Definition: Zerfällungskörper

Betrachte zu der Körpererweiterung $L : K$ und der Familie von Polynomen $\mathcal{F} \subseteq K[X]$ die folgenden Aussagen.

(Z) Zerfällung. Jedes Polynom aus $\mathcal{F}$ als Polynom in $L[X]$ in Linearfaktoren zerfällt,

$$f(X) \;=\; f_m \cdot (X - a_1) \cdot \ldots \cdot (X - a_m), \qquad a_j \in L,$$

(M) Minimalität. Ist $\widetilde{L}$ ein weiterer Körper mit $K \subseteq \widetilde{L} \subseteq L$ und der Eigenschaft (Z), so ist $\widetilde{L} = L$.

(E) Erzeugnis. Ist $A \subseteq L$ die Teilmenge aller Nullstellen aller Polynome aus $\mathcal{F}$, so gilt $L = K(A)$.

1. Die beiden Aussagen (M) und (E) sind äquivalent.
2. L heißt ein *Zerfällungskörper für* $\mathcal{F}$ bzw. $L : K$ heißt eine *Zerfällungskörpererweiterung für* $\mathcal{F}$, wenn (Z) und (M) bzw. (Z) und (E) erfüllt sind.

6.1.2 Definition: Normale Körpererweiterung

Eine Körpererweiterung $L : K$ heißt *normal*, wenn die folgende Aussage erfüllt ist.

Ist $g \in K[X]$ irreduzibel und existiert **eine** Nullstelle von g in L,

so existieren **alle** Nullstellen von g in L.

(„Alle Nullstellen oder keine").

6.1.3 Beispiel

Ist $\overline{K}$ ein algebraischer Abschluss eines Körpers K, so ist $\overline{K} : K$ normal.

6.1.4 Hauptsatz über normale Körpererweiterungen $^{\ominus}$

Die folgenden Aussagen über eine Körpererweiterung $L : K$ sind äquivalent.

(A) Es gibt eine Familie $\mathcal{F}$ von Polynomen so, dass L Zerfällungskörper für $\mathcal{F}$ ist.

(B) Ist $\widetilde{L} : L$ eine Körpererweiterung und $\varphi : L \to \widetilde{L}$ ein K-Körpermonomorphismus, so gilt $\varphi(L) \subseteq L$.

(C) $L : K$ ist normal.

6.1.5 Beweis

Der Beweis macht Gebrauch von der Existenz eines algebraischen Abschlusses von L. Deshalb verzichten wir darauf, ihn zu präsentieren.

Wir wenden uns stattdessen den endlichen normalen Körpererweiterungen zu und beweisen später den für uns eigentlich wichtigeren Hauptsatz über endliche normale Körpererweiterungen 6.4.1.

6.1.6 Beobachtung

Ist $\mathcal{F}$ eine **endliche** Familie von Polynomen aus $K[X]$, so ist ein Körper L genau dann Zerfällungskörper für $\mathcal{F}$, wenn er Zerfällungskörper des Produkts dieser endlich vielen Polynome ist.

Deshalb studieren wir in den nächsten Abschnitten Zerfällungskörper für ein einziges Polynom f.

6.1.7 Beispiel

Jede Körpererweiterung $L : K$ mit $[L : K] = 2$ ist normal. (Übung)

6.1.8 Beispiel

Innerhalb von $\mathbb{C} : \mathbb{Q}$ betrachten wir die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. Das Minimalpolynom des erzeugenden Elements $a = \sqrt[3]{2}$ ist $f(X) = X^3 - 2$.

Die drei Nullstellen von f sind a, $a\zeta_3$ und $a\zeta_3^2$, wobei $\zeta_3 = \exp(\frac{2\pi i}{3})$.

Die beiden Nullstellen $a\zeta_3$ und $a\zeta_3^2$ sind echt komplex, also nicht in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ enthalten.

Deshalb kann $L : K$ nicht normal sein.

6.1.9 Beispiel

Innerhalb von $\mathbb{C} : \mathbb{Q}$ betrachten wir die Körpererweiterung $\mathbb{Q}(\zeta_p) : \mathbb{Q}$, wobei $\zeta_p = \exp(\frac{2\pi i}{p})$, p Primzahl.

Das Minimalpolynom des erzeugenden Elements ζ_p ist $f(X) = X^{p-1} + \ldots + X + 1$.

Die Nullstellen von f sind $\zeta_p^k \in \mathbb{Q}(\zeta_p)$, $k \in \{1, \ldots, p-1\}$.

Also ist $\mathbb{Q}(\zeta_p)$ Zerfällungskörper für f. Der obige unbewiesene Hauptsatz sagt dann aus, dass $\mathbb{Q}(\zeta_p) : \mathbb{Q}$ normal ist. Das werden wir noch unabhängig davon beweisen.

6.2 Fortsetzung von Körperisomorphismen

Den folgenden Satz (mit Folgerung) hätten wir schon in Kapitel 5.1 über algebraische Elemente unterbringen können.

6.2.1 Satz: Fortsetzung von Körperisomorphismen

Es seien $L : K$ und $\widetilde{L} : \widetilde{K}$ zwei Körpererweiterungen.

Es sei weiter $\varphi : K \to \widetilde{K}$ ein Körperisomorphismus.

Es seien weiter $f \in K[X]$ und $\widetilde{f} = \varphi_*(f) \in \widetilde{K}[X]$ irreduzible Polynome, die über den φ-Koeffizientenaustausch in Zusammenhang stehen.

Es seien weiter $a \in L$ mit $f(a) = 0$ und $\widetilde{a} \in \widetilde{L}$ mit $\widetilde{f}(\widetilde{a}) = 0$.

(i) Dann gibt es einen Körperisomorphismus $\varphi^{\text{ext}} : K(a) \to \widetilde{K}(\widetilde{a})$ mit

$$\varphi^{\text{ext}}|_K \;=\; \varphi \qquad \text{und} \qquad \varphi^{\text{ext}}(a) \;=\; \widetilde{a},$$

der durch diese beiden Eigenschaften eindeutig bestimmt ist.

(ii) Dieser Körperisomorphismus ist explizit gegeben durch

$$\varphi^{\text{ext}} : \left\{ \begin{array}{rcl} K(a) & \to & \widetilde{K}(\widetilde{a}) \\ \alpha_0 + \alpha_1 a + \ldots + \alpha_{m-1} a^{m-1} & \mapsto & \varphi(\alpha_0) + \varphi(\alpha_1)\widetilde{a} + \ldots + \varphi(\alpha_{m-1})\widetilde{a}^{m-1} \end{array} \right.$$

(In dem polynomialen Ausdruck werden also die Koeffizienten aus K durch ihre Bilder unter φ, die Nullstelle $a \in L$ durch die Nullstelle $\widetilde{a} \in \widetilde{L}$ ersetzt.)

6.2.2 Beweis

(1) Es gilt $K(a) = K[a] = \operatorname{im} \varepsilon_a$, also lässt sich jedes $x \in K(a)$ schreiben als polynomialer Ausdruck in a wie in (ii) bereits angegeben:

$$x \;=\; \alpha_0 + \alpha_1 a + \ldots + \alpha_{m-1} a^{m-1}$$

(2) Wir definieren φ^{ext} wie in (ii) angegeben. Da φ ein Körperisomorphismus ist, ist φ^{ext} surjektiv, dann als lineare Abbildung zwischen gleich-dimensionalen K-Vektorräumen auch bijektiv.

(3) Die beiden in (i) angegebenen Eigenschaften

$$\varphi^{\text{ext}}|_K \;=\; \varphi \qquad \text{und} \qquad \varphi^{\text{ext}}(a) \;=\; \widetilde{a},$$

sind klar.

(4) Es seien

$$\begin{aligned} x &= g(a) \\ y &= h(a) \end{aligned}$$

mit Polynomen $g, h \in K[X]$ mit $\deg g, h \leq m - 1$.

(5) Dann gibt es Polynome $q, r \in K[X]$ mit

$$g \cdot h \;=\; q \cdot f + r \qquad \text{mit } \deg r < \deg f \leq m-1.$$

(6) Es folgt

$$x \cdot y \;=\; g(a) \cdot h(a) \;=\; q(a) \cdot f(a) + r(a) \;=\; r(a)$$

und dann

$$\begin{aligned} \varphi^{\text{ext}}(x \cdot y) &= \varphi^{\text{ext}}(r(a)) = \varphi_*(r)(\widetilde{a}) = \varphi_*(g \cdot h - q \cdot f)(\widetilde{a}) \\ &= [\varphi_*(g) \cdot \varphi_*(h) - \varphi_*(q) \cdot \varphi_*(f)](\widetilde{a}) \\ &= \varphi_*(g)(\widetilde{a}) \cdot \varphi_*(h)(\widetilde{a}) - \varphi_*(q)(\widetilde{a}) \cdot \varphi_*(f)(\widetilde{a}) \\ &= [\varphi_*(g)(\widetilde{a}) \cdot \varphi_*(h)(\widetilde{a}) \\ &= \varphi^{\text{ext}}(x) \cdot \varphi^{\text{ext}}(y). \end{aligned}$$

(7) Also ist φ^{ext} auch multiplikativ, ein unitärer Ringisomorphismus, damit ein Körperisomorphismus.

6.2.3 Satz: Fortsetzung von Isomorphismen auf Zerfällungskörper

Es sei $\varphi : K \to \widetilde{K}$ ein Körperisomorphismus.

Es seien weiter $f \in K[X]$ und $\widetilde{f} = \varphi_*(f) \in \widetilde{K}[X]$ Polynome mit $m = \deg f = \deg \widetilde{f} \geq 1$, die über den φ-Koeffizientenaustausch in Zusammenhang stehen.

$L : K$ und $\widetilde{L} : \widetilde{K}$ seien die Zerfällungskörpererweiterungen für f bzw. $\widetilde{f}$.

(i) Es gibt einen Isomorphismus $\varphi^{\text{ext}} : L \to \widetilde{L}$, der φ fortsetzt.

(ii) Die Aussage aus (i) lässt sich wie folgt erweitern und präzisieren.

> Ist a eine Nullstelle eines (einzigen) irreduziblen Teilers g von f mit $\deg g \geq 2$ und ist $\widetilde{a}$ Nullstelle von $\widetilde{g} := \varphi_*(g)$, so gibt es einen Isomorphismus $\varphi^{\text{ext}} : L \to \widetilde{L}$ mit
>
> $$\varphi^{\text{ext}}|_K \;=\; \varphi \text{ und } \varphi^{\text{ext}}(a) \;=\; \widetilde{a}.$$

6.2.4 Bemerkung

Im Falle $\deg g = 1$ in (ii) impliziert die linke Forderung $\varphi^{\text{ext}}|_K = \varphi$ die rechte Forderung $\varphi^{\text{ext}}(a) \;=\; \widetilde{a}$.

Es ist dann auch $\deg \widetilde{g} = 1$. Zwischen den eindeutig festgelegten Nullstellen $a \in K$ von g und $\widetilde{a} \in \widetilde{K}$ von $\widetilde{g}$ besteht dann der Zusammenhang

$$\varphi^{\text{ext}}(a) \;=\; \varphi(a) \;=\; \varphi(-g_1^{-1} g_0) \;=\; -\varphi(g_1)^{-1} \cdot \varphi(g_0) \;=\; -(\widetilde{g}_1)^{-1} \cdot \widetilde{g}_0 \;=\; \widetilde{a}.$$

6.2.5 Beweis

(1) Der Beweis geschieht durch Induktion über $d = [L : K]$.

(2) Induktionsanfang $[L : K] = 1$. Dann ist $L = K$ und f zerfällt bereits über K in Linearfaktoren

$$f(X) \;=\; f_m \cdot (X - a_1) \cdot \ldots \cdot (X - a_m), \qquad a_j \in K.$$

Es ist dann mit $\widetilde{a}_j := \varphi(a_j)$

$$\widetilde{f}(X) \;=\; \varphi_*(f)(X) \;=\; \varphi(f_m) \cdot (X - \varphi(a_1)) \cdot \ldots \cdot (X - \varphi(a_m)), \quad \varphi(a_j) \in \widetilde{K},$$

also zerfällt auch $\widetilde{f}$ über $\widetilde{K}$ in Linearfaktoren, es folgt $\widetilde{L} = \widetilde{K}$. Es muss dann $\varphi^{\text{ext}} = \varphi$ sein. Es gilt dann auch $\deg g = 1$ und die Bemerkung 6.2.4 greift.

(3) Induktionsschluss. Es sei $[L : K] = d > 1$. Da g und $\widetilde{g}$ irreduzibel sind, existiert gemäß Satz 6.2.1(i) ein Körperisomorphismus $\varphi' : K(a) \to \widetilde{K}(\widetilde{a})$ mit

$$\varphi'|_K \;=\; \varphi \qquad \text{und} \qquad \varphi'(a) \;=\; \widetilde{a}.$$

Dann sind $L : K(a)$ und $\widetilde{L} : \widetilde{K}(\widetilde{a})$ auch Zerfällungskörpererweiterungen.

(4) Die Gradformel zeigt

$$[L : K(a)] \;=\; \tfrac{[L:K]}{[K(a):K]} \;=\; \tfrac{d}{\deg g} \;<\; d.$$

(5) Gemäß Induktionsvoraussetzung kann φ' zu einem Körperisomorphismus $\varphi^{\text{ext}} : L \to \widetilde{L}$ mit

$$\varphi^{\text{ext}}|_{K(a)} \;=\; \varphi' \qquad \text{und} \qquad \varphi^{\text{ext}}(a) \;=\; \widetilde{a}.$$

fortgesetzt werden.

(6) Es gilt dann auch

$$\varphi^{\text{ext}}|_K \;=\; \varphi'|_K \;=\; \varphi \qquad \text{und} \qquad \varphi^{\text{ext}}(a) \;=\; \widetilde{a}.$$

6.3 Existenz und Eindeutigkeit von Zerfällungskörpern

6.3.1 Satz (Kronecker)

Es seien K ein Körper und $f \in K[X]$ mit $m = \deg f \geq 1$ irreduzibel.

Dann gibt es

eine Körpererweiterung $L : K$ mit

$[L : K] = m$ und

ein $a \in L$ mit $f(a) = 0$.

6.3.2 Beweis

(0) Die Konstruktion des Körpers L ist ein Musterbeispiel für die enorme Kraft abstrakter Theorie.

(1) Da f irreduzibel ist, ist (f) im Hauptidealring $K[X]$ maximal, also $L := K[X]/(f)$ ein Körper.

(2) Wir betrachten die Nacheinanderausführungen der beiden Ringhomomorphismen

$$\iota : \left\{ \begin{array}{ccccc} K & \to & K[X] & \to & K[X]/(f) \\ x & \mapsto & x & \mapsto & x + (f) \end{array} \right.$$

(3) ι ist ein (unitärer) Ringhomomorphismus, deshalb ein Körpermonomorphismus. K kann als eingebettet in L aufgefasst werden, $L : K$ ist also eine Körpererweiterung.

(4) Es sei nun $a := X + (f) \in L$, also die Projektion des Monoms $X \in K[X]$.

(5) Ist $f(X) = f_0 + f_1 X + \ldots + f_m X^m$, so gilt in L (super ausführlich)

$$\begin{aligned} f(a) &= f_0 + f_1 a + f_2 a^2 + \ldots + f_m a^m \\ &= f_0 + f_1[X + (f)] + f_2[X + (f)]^2 + \ldots + f_m[X + (f)]^m \\ &= f_0 + f_1[X + (f)] + f_2[X^2 + (f)] + \ldots + f_m[X^m + (f)] \\ &= f_0 + f_1 X + f_1(f) + f_2 X^2 + f_2(f) + \ldots + f_m X^m + f_m(f) \\ &= f_0 + f_1 X + (f) + f_2 X^2 + (f) + \ldots + f_m X^m + (f) \\ &= f_0 + f_1 X + f_2 X^2 + \ldots + f_m X^m + (f) \\ &= f + (f) \;=\; (f) \;\equiv\; 0. \end{aligned}$$

(6) Das Minimalpolynom von a ist $\mu_a = f_m^{-1} f$, da f irreduzibel ist. Es folgt

$$[L : K] \;=\; \deg \mu_a \;=\; \deg f.$$

6.3.3 Satz: Existenz und Eindeutigkeit eines Zerfällungskörpers

Es seien K ein Körper und $f \in K[X]$, nicht notwendig irreduzibel, mit $m = \deg f \geq 1$.

(i) Dann gibt es

$$\begin{aligned} &\text{einen Zerfällungskörper } L \text{ für } f \quad \text{mit} \\ &[L : K] \;\leq\; m! \end{aligned}$$

(ii) Dieser Zerfällungskörper L ist bis auf Isomorphie eindeutig.

(iii) Genauer gilt:

Sind L und $\widetilde{L}$ Zerfällungskörper für $f \in K[X]$ und sind $a \in L$ und $\widetilde{a} \in \widetilde{L}$ Nullstellen von f, so gibt es einen K-Körperisomorphismus $L \to \widetilde{L}$ mit $\varphi(a) = \widetilde{a}$.

6.3.4 Bemerkung

Weiß man, dass K einen algebraischen Abschluss $\overline{K}$ hat, so folgt daraus ganz einfach die Existenz-Behauptung. Es existieren in $\overline{K}$ Elemente $a_1, \ldots, a_m$, so dass

$$f(X) \;=\; f_m \cdot (X - a_1) \cdot \ldots \cdot (X - a_m).$$

Definiere einfach

$$L \;:=\; K(a_1, \ldots, a_m) \;=\; \bigcap_{K \cup \{a_1, \ldots, a_m\} \subseteq M \subseteq \overline{K},\, M \text{ Körper}} M.$$

Wir wollen davon keinen Gebrauch machen und präsentieren den folgenden direkten konstruktiven Beweis.

6.3.5 Beweis

Zu (i).

(0) Induktion über $m = \deg f$.

(1) Induktionsanfang. In diesem Fall ist $f(X) = f_1 X + f_0$ mit $f_1 \in K^\times$. Dann ist $L = K$ mit $[L : K] = 1$. f ist bereits selbst ein Linearfaktor.

(2) Induktionsschluss. Es sei $f \in K[X]$ mit $\deg f = m + 1$ und g ein irreduzibler Teiler von f.

(3) Gemäß dem Satz 6.3.1 von Kronecker gibt es eine Körpererweiterung $M : K$ mit $[M : K] = \deg g \leq \deg f = m + 1$ und ein $a \in M$ mit $g(a) = 0$, also auch $f(a) = 0$.

(4) Wir spalten von f in $M[X]$ den Linearfaktor $X - a$ ab und erhalten ein Polynom $\widetilde{f} \in M[X]$ mit

$$f(X) \;=\; \widetilde{f}(X) \cdot (X - a),$$

deshalb $\deg \widetilde{f} = m$ und $\widetilde{f}_m = f_m$.

(5) Gemäß Induktionsvoraussetzung existiert eine Körpererweiterung $L : M$ so, dass L Zerfällungskörper für $\widetilde{f} \in M[X]$ ist. Genauer gilt $[L : M] \leq m!$ und es existieren $a_1, \ldots, a_m \in M$ mit

$$\widetilde{f}(X) \;=\; f_m \cdot (X - a_1) \cdot \ldots \cdot (X - a_m).$$

(6) Es gilt dann

$$[L : K] \;=\; [L : M] \cdot [M : K] \;\leq\; m! \cdot (m + 1) \;=\; (m + 1)!$$

und

$$f(X) \;=\; \widetilde{f}(X) \cdot (X - a) \;=\; f_m \cdot (X - a_1) \cdot \ldots \cdot (X - a_m) \cdot (X - a).$$

Zu (iii). Setze in Satz 6.2.3 $\widetilde{K} = K$ und $\varphi = \mathrm{id}_K$. Es folgt $\widetilde{f} = f$. Als irreduziblen Teiler g von f wähle einen, der in L die vorgegebene Nullstelle a von f als Nullstelle hat.

6.3.6 Bemerkung

Es entsteht dann wieder die Frage, ob man von **einem** Zerfällungskörper oder **dem** Zerfällungskörper sprechen soll.

Akzeptiert und verinnerlicht man die Eindeutigkeitsaussage, so bietet sich die Bezeichnung $L = \mathrm{Zerf}(f) = \mathrm{Zerf}(f, K)$ an.

6.4 Endliche normale Körpererweiterungen

6.4.1 Hauptsatz über endliche normale Körpererweiterungen

Die folgenden Aussagen über eine Körpererweiterung $L : K$ sind äquivalent.

(A) Es gibt ein Polynom $f \in K[X]$ so, dass L Zerfällungskörper für f ist.

(B) Es ist $L : K$ endlich. Ist weiter $\widetilde{L} : L$ eine Körpererweiterung und $\varphi : L \to \widetilde{L}$ ein K-Körpermonomorphismus, so gilt $\varphi(L) \subseteq L$.

(C) $L : K$ ist endlich und normal.

6.4.2 Beweis

(A) $\Rightarrow$ (B). Es seien $\widetilde{L}$ und φ wie in (B) angegeben.

Die Menge $\{a_1, \ldots, a_m\} \subseteq L$ der Nullstellen von f in L ist invariant unter φ, da

$$\begin{aligned} f(\varphi(a_j)) &= f_0 + f_1\varphi(a_j) + \ldots + f_m[\varphi(a_j)]^m \\ &= \varphi(f_0) + \varphi(f_1)\varphi(a_j) + \ldots + \varphi(f_m)[\varphi(a_j)]^m \\ &= \varphi(f_0 + f_1 a_j + \ldots + f_m a_j^m) \\ &= \varphi(0) \;=\; 0. \end{aligned}$$

Also ist

$$\begin{aligned} \varphi(L) &= \varphi(K(a_1, \ldots, a_m)) \;\subseteq\; \varphi(K)(\varphi(a_1), \ldots, \varphi(a_m)) \\ &\subseteq K(a_1, \ldots, a_m) \;=\; L. \end{aligned}$$

(B) $\Rightarrow$ (C).

(1) Es sei $a_1 \in L$ eine gemäß Definition 6.1.2 vorgegebene Nullstelle eines irreduziblen Polynoms $g \in K[X]$. Gemäß dem Hauptsatz über endliche Körpererweiterungen 5.2.3 gibt es über K algebraische Elemente $a_2, \ldots, a_n \in L$ so, dass $L = K(a_1, \ldots, a_n)$.

(2) Es ist $g_1, g_2, \ldots, g_n \in K[X]$ die Minimalpolynome von $a_1, a_2, \ldots, a_n$. Es gilt dann $g_1 \sim g$.

(3) Es sei $\widetilde{L} \;:=\; \operatorname{Zerf} h$ der Zerfällungskörper des Produktpolynoms

$$h \;:=\; g_1 \cdot g_2 \cdot \ldots \cdot g_n \qquad \in K[X].$$

Es ist dann L ein Zwischenkörper von $\widetilde{L} : K$.

(4) Es sei nun $\widetilde{a} \in \operatorname{Zerf}(g) \subseteq \widetilde{L}$ eine beliebige Nullstelle von g.

Gemäß Satz 6.2.3(ii) existiert ein K-Körperisomorphismus

$$\varphi : \widetilde{L} \to \widetilde{L} \quad \text{mit} \quad \varphi(a_1) = \widetilde{a}.$$

(5) Durch Einschränkung auf L erhalten wir einen K-Körpermonomorphismus

$$\varphi|_L : L \to \widetilde{L} \quad \text{mit} \quad \varphi|_L(a_1) = \widetilde{a}.$$

(6) Gemäß Aussage (B) ist $\varphi|_L(L) \subseteq L$ und deshalb

$$\widetilde{a} \;\in\; \varphi|_L(L) \;\subseteq\; L.$$

Damit sind alle Nullstellen von g in L, was zu beweisen war.

(C) $\Rightarrow$ (A). Gemäß dem Hauptsatz über endliche Körpererweiterungen 5.2.3 gibt es über K algebraische Elemente $a_1, \ldots, a_n \in L$ so, dass $L = K(a_1, \ldots, a_n)$.

Sind dann $g_1, \ldots, g_n \in K[X]$ die zugehörigen Minimalpolynome, so enthält L aufgrund der Normalität alle Nullstellen von $f = g_1 \cdot \ldots \cdot g_n \in K[X]$.

Wäre bereits ein Körper $M \subsetneqq L = K(a_1, \ldots, a_n)$ ein Zerfällungskörper, so gäbe es ein $a_j \in L \setminus M$. Dann kann aber der Faktor g_j im Polynom f nicht über M zerfallen.

6.4.3 Beispiel

Es sei M ein Zwischenkörper von $\mathbb{C} : \mathbb{Q}$, der Zerfällungskörper eines rationalen Polynoms.

Die Komplex-Konjugation

$$\left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array} \right.$$

ist ein Körperautomorphismus. Wird sie auf M eingeschränkt, so ist sie gemäß (B) des obigen Hauptsatzes 6.4.1 sogar ein $\mathbb{Q}$-Körpermonomorphismus $\kappa : M \to M$, wegen $\kappa^2 = \mathrm{id}_M$ ein $\mathbb{Q}$-Körperautomorphismus von M.

Ist $M \subseteq \mathbb{R}$, so ist $\kappa = \mathrm{id}_M$ trivial. Im Falle $M \cap (\mathbb{C} \setminus \mathbb{R}) \neq \varnothing$ ist κ ein nichttrivialer $\mathbb{Q}$-Körperautomorphismus.

7 Separable Körpererweiterungen

7.1 Formale Ableitung

7.1.1 Definition: Formale Ableitung

Es sei K ein Körper und

$$f(X) = \sum_{j=0}^{m} f_j X^j \qquad \in K[X]$$

ein Polynom. Dann heißt das Polynom

$$f'(X) = \sum_{j=1}^{m} j \cdot f_j X^j \qquad \in K[X]$$

die *formale Ableitung von* f.

7.1.2 Bemerkung

Beachte, dass die in der formalen Ableitung auftretenden Elemente $j \in K$ definiert sind als die Summen von j vielen Eins-Elementen.

7.1.3 Beispiele

1. Bei $\operatorname{char} K = 0$ ist die formale Ableitung aus der Analysis wohlbekannt. Beachte, dass hier zur Definition keinerlei Grenzwertprozesse herangezogen wurden.

2. Ist $\operatorname{char} K = p$, p Primzahl, so ist

   $$(X^p - a)' = 0.$$

3. Ist $g \in K[X]$ bei $\operatorname{char} K = p$, so „enthält" das Polynom

   $$f(X) := g(X^p)$$

   nur Exponenten, die Vielfache von p sind. Es folgt $f' = 0$.

4. So hat beispielsweise bei Charakteristik 3 das Polynom

   $$f(X) = 2X^6 - X^4 + X^3 - X^2 + 2X + 2$$

   die Ableitung

   $$f'(X) = 12X^5 - 4X^3 + 3X^2 - 2X + 2 = 2X^3 + 2X + X + 2$$

7.1.4 Satz: Rechenregeln

Sind $f, g \in K[X]$ und $\alpha, \beta \in K$, so gilt

$$\begin{aligned}(\alpha f + \beta g)' &= \alpha f' + \beta g' \\ (f \cdot g)' &= f' \cdot g + f \cdot g'.\end{aligned}$$

7.1.5 Beweis

Einfaches Nachrechnen.

7.1.6 Satz: Mehrfache Nullstellen

Ist $f \in K[X]$ ein Polynom, so sind die folgenden beiden Aussagen über ein $a \in K$ und $j \in \mathbb{N}$ äquivalent.

(A) a ist Nullstelle von f mit Vielfachheit j, vgl. die Definition in 3.5.2.

(B) Es ist $f(a) = f'(a) = \ldots = f^{(j-1)}(a) = 0$ und $f^{(j)}(a) \neq 0$.

7.1.7 Beweis

Einfaches Nachrechnen.

7.2 Separabilität

7.2.1 Satz: Einfache Nullstellen

Es seien K ein Körper und $f \in K[X]$ mit $\deg f \geq 1$. Betrachte die folgenden Aussagen.

(A) f hat in einem (bis auf Isomorphie eindeutigen) Zerfällungskörper nur einfache Nullstellen.

(B) f und f' haben in $K[X]$ keinen gemeinsamen Teiler g mit $\deg g \geq 1$, d.h. es ist $\mathrm{ggT}(f, f') = 1$.

(C) Es ist $f' \neq 0$.

(D) In f existiert ein Monom $f_j X^j$ mit Exponent $j \notin p\,\mathbb{Z}$ und Koeffizient $f_j \neq 0$.

Es gilt dann

$$\text{(A)} \quad \Longleftrightarrow \quad \text{(B)} \quad \Longrightarrow \quad \text{(C)} \quad \Longleftrightarrow \quad \text{(D)}$$

Ist f irreduzibel, so gilt auch

$$\text{(B)} \quad \Longleftrightarrow \quad \text{(C)}$$

7.2.2 Beweis

(A) $\Rightarrow$ (B). Hätten die Polynome f und f' einen gemeinsamen Teiler g mit $\deg g \geq 1$, so hätten sie im Zerfällungskörper einen gemeinsamen Linearfaktor, dann auch eine gemeinsame Nullstelle a. Diese Nullstelle wäre dann gemäß Satz 7.1.6 eine (mindestens) doppelte Nullstelle von f.

(B) $\Rightarrow$ (A). Wäre $a \in K$ eine mehrfache Nullstelle von f, so wäre $f(a) = f'(a) = 0$. Dann gilt für das Minimalpolynom μ_a

$$\mu_a \mid f \quad \text{und} \quad \mu_a \mid f',$$

also ist μ_a ein gemeinsamer Teiler mit $\deg \mu_a \geq 1$.

(B) $\Rightarrow$ (C). Wäre $f' = 0$, so wäre $\mathrm{ggT}(f, f') = f \neq 1$.

(C) $\Rightarrow$ (B), falls f irreduzibel. Da dann die Teiler von f assoziiert zu 1 oder f sind, muss $\mathrm{ggT}(f, f') \in \{1, f_m^{-1} f\}$ sein. Es kann aber $f_m^{-1} f$ kein Teiler von $f' \neq 0$ sein.

7.2.3 Definition: Separabilität

Es sei $L : K$ eine Körpererweiterung.

1. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn jeder irreduzible Teiler g von f in dem zugehörigen Zerfällungskörper Zerf_g nur einfache Nullstellen hat.

2. Ein Element $a \in L$ heißt *separabel (über K)*, wenn a algebraisch ist und das zugehörige Minimalpolynom μ_a separabel ist.

3. $L : K$ heißt *separabel*, wenn jedes Element $a \in L$ separabel über K ist.

4. K heißt *vollkommen*, wenn jedes irreduzible Polynom $f \in K[X]$ separabel ist.

7.2.4 Direkte Folgerungen

(i) Ein irreduzibles Polynom ist genau dann separabel, wenn die vier äquivalenten Eigenschaften aus Satz 7.2.1 erfüllt sind.

(ii) Eine separable Erweiterung ist immer algebraisch.

(iii) Eine algebraische Erweiterung eines vollkommenen Körpers ist separabel.

7.2.5 Satz: Hinreichende Bedingungen für Vollkommenheit

Es sei K ein Körper.

(i) Ist $\operatorname{char} K = 0$, so ist K vollkommen.

(ii) Ist $\operatorname{char} K = p$, so ist K vollkommen genau dann, wenn der Frobenius-Monomorphismus

$$\Phi : \left\{ \begin{array}{ccc} K & \to & K \\ x & \mapsto & x^p \end{array} \right.$$

surjektiv ist.

(iii) Ist K endlich, so ist K vollkommen.

7.2.6 Beweis

(i) Ist g ein irreduzibler Faktor von f, so gilt

$$\deg g' \;=\; \deg g - 1 \;\geq\; 0, \qquad \text{also} \qquad g' \neq 0.$$

Wende dann die Implikation (C) $\Rightarrow$ (A) aus Satz 7.2.1 an.

(ii) $\Rightarrow$. (1) Angenommen, Φ wäre nicht surjektiv, d.h. es gibt ein $a \in K$ so, dass das Polynom $f(X) = X^p - a$ keine Nullstelle hat.

(2) Es sei $L : K$ Zerfällungskörpererweiterung von f und $b \in L$ Nullstelle von f, also $b^p = a$, es folgt

$$f(X) \;=\; X^p - a \;=\; X^p - b^p \;=\; (X-b)^p.$$

(3) Ist g ein normierter irreduzibler Faktor von f, so folgt, da $L[X]$ faktoriell ist, dass

$$g(X) \;=\; (X-b)^j \qquad \text{mit } j \in \{2, \ldots, p\}.$$

$j = 1$ ist unmöglich wegen $g \in K[X]$ und $b \notin K$.

Also hat das irreduzible Polynom $g \in K[X]$ mehrfache Nullstellen, ist demnach nicht separabel. Schließlich kann K deshalb nicht vollkommen sein.

(ii) $\Leftarrow$. Es sei $f \in K[X]$ irreduzibel.

Hätte das Polynom $f \in K[X]$ eine mehrfache Wurzel in Zerf_f, so hätte es gemäß der Äquivalenz (A) $\Leftrightarrow$ (D) aus Satz 7.2.1 die Form

$$f(X) \;=\; f_0 + f_p X^p + f_{2p} X^{2p} + \ldots + f_{kp} X^{kp}.$$

Da Φ surjektiv ist, gibt es zu jedem Koeffizienten $f_j \in K$ ein $g_j \in K$ mit $g_j^p = f_j$.

Dann gilt aber

$$\begin{aligned} f(X) &= g_0^p + g_p^p X^p + g_{2p}^p X^{2p} + \ldots + g_{kp}^p X^{kp} \\ &= (g_0 + g_p X + g_{2p} X^2 + \ldots + g_{kp} X^k)^p \end{aligned}$$

und das ist ein Widerspruch zur Irreduzibilität von f.

(iii) Ist K endlich, so folgt aus der Injektivität des Frobenius-Monomorphismus die Surjektivität.

7.3 Der Satz vom primitiven Element

7.3.1 Satz: Endliche multiplikative Untergruppen eines Körpers

Es sei K ein Körper.

Dann ist eine endliche Untergruppe $U \subseteq (K^\times, \cdot\,)$ zyklisch.

7.3.2 Beweis

(0) U ist abelsch und damit direktes Produkt der p-Sylowgruppen

$$U \;\simeq\; U_{p_1} \times \ldots \times U_{p_\ell}.$$

(1) Da die Ordnungen der Faktoren teilerfremd sind, ist U zyklisch genau dann, wenn die Faktoren U_{p_j} zyklisch sind.

Wir können also annehmen, dass U eine Primzahlpotenz als Ordnung hat.

(2) Es sei $g \in U$ mit maximaler Ordnung p^m, d.g. es existiert kein Element $\widetilde{g} \in U$ mit $\operatorname{ord}(\widetilde{g}) > m$.

(3) Dann ist $\operatorname{ord}(U) \geq m$.

(4) Andererseits, da alle Elemente von U unter den höchstens m Nullstellen des Polynoms $X^m - 1 \in K[X]$ sind, ist $\operatorname{ord}(U) \leq m$.

(5) Damit gilt $\operatorname{ord} U = m$, deshalb $U = \langle g \rangle$, also ist U zyklisch.

7.3.3 Vorbereitung: ggT bei Körpererweiterung

Es seien $L : K$ eine Körpererweiterung und $f, g \in K[X]$. Dann gilt

$$\operatorname{ggT}_{L[X]}(f,g) \;=\; \operatorname{ggT}_{K[X]}(f,g) \quad \in K[X].$$

7.3.4 Beweis

Es gilt zunächst

$$\begin{array}{rl} & \left.\begin{array}{l} \operatorname{ggT}_{K[X]}(f,g) \mid f \text{ in } K[X] \\ \operatorname{ggT}_{K[X]}(f,g) \mid g \text{ in } K[X] \end{array}\right. \quad\Longrightarrow\quad \left.\begin{array}{l} \operatorname{ggT}_{K[X]}(f,g) \mid f \text{ in } L[X] \\ \operatorname{ggT}_{K[X]}(f,g) \mid g \text{ in } L[X] \end{array}\right. \\ \Longrightarrow & \operatorname{ggT}_{K[X]}(f,g) \mid \operatorname{ggT}_{L[X]}(f,g) \text{ in } L[X]. \end{array}$$

Gemäß Lemma von Bezout im Hauptidealring $K[X]$ existieren Polynome $h, k \in K[X]$ mit

$$\operatorname*{ggT}_{K[X]}(f,g) \;=\; h \cdot f + k \cdot g.$$

Da diese Relation auch in $L[X]$ gültig ist, folgern wir weiter

$$\left.\begin{array}{l} \operatorname{ggT}_{L[X]}(f,g) \mid f \text{ in } L[X] \\ \operatorname{ggT}_{L[X]}(f,g) \mid g \text{ in } L[X] \end{array}\right. \quad\Longrightarrow\quad \operatorname{ggT}_{L[X]}(f,g) \mid \operatorname{ggT}_{K[X]}(f,g) \text{ in } L[X].$$

Also sind $\operatorname{ggT}_{K[X]}(f,g)$ und $\operatorname{ggT}_{L[X]}(f,g)$ assoziiert in $L[X]$. Da diese beiden Polynome normiert sind, folgt Gleichheit.

7.3.5 Der Satz vom primitiven Element

Es sei $L : K$ mit $L = K(a_1, a_2, \ldots, a_n)$ eine algebraisch-endliche-erzeugte Körpererweiterung, vgl. Satz 5.2.3.

(i) Sind die Elemente $a_2, \ldots, a_n$ separabel über K. so gibt es ein primitives Element c in L, d.h. es ist $L = K(c)$.

(ii) Die Voraussetzung in (i) ist insbesondere erfüllt, wenn $L : K$ separabel ist.

(iii) Die Voraussetzung in (i) ist insbesondere erfüllt, wenn K vollkommen ist.

7.3.6 Beweis

(0) Ist der Körper K endlich, so zeigt der Satz 7.3.1 die Behauptung.

Es sei also O.B.d.A. $|K| = \infty$.

(1) Wir betrachten zunächst den Fall, dass L durch zwei Elemente erzeugt wird. Aus ,,beweisdidaktischen" Gründen nennen wir diese beiden Elemente a_1 und b_1, es ist also $L = K(a_1, b_1)$ mit $a_1, b_1 \in L$.

(2) Es seien $f \in K[X]$ und $g \in K[X]$ die Minimalpolynome von a_1 bzw. b_1. Es gibt einen Zerfällungskörper M mit $K \subseteq L \subseteq M$ so, dass

$$\begin{aligned} f &= (X - a_1)(X - a_2) \cdot \ldots \cdot (X - a_m), \quad a_j \in M,\ j = 1, \ldots, m, \\ g &= (X - b_1)(X - b_2) \cdot \ldots \cdot (X - b_n), \quad b_k \in M,\ k = 1, \ldots, n. \end{aligned}$$

(3) Da b_1 separabel ist, sind die Elemente $b_1, b_2, \ldots, b_n$ paarweise verschieden.

(4) Da $|K| = \infty$, gibt es ein

$$\lambda \in K \setminus \underbrace{\left\{ \tfrac{a_j - a}{b_1 - b_k} \mid j = 1, \ldots, m,\ k = 2, \ldots, n \right\}}_{\text{endlich}}.$$

(5) Wir setzen jetzt

$$c = a_1 + \lambda\, b_1.$$

Damit erhalten wir eine Kette von Körpererweiterungen

$$K \subseteq K(c) \subseteq K(a_1, b_1) = L \subseteq M$$

(6) Wir zeigen nun $b_1 \in K(c)$. Dazu definieren wir das Polynom

$$h = f(c - \lambda X) \in (K(c))[X].$$

(7) Es ist

$$\begin{aligned} h(b_1) &= f(c - \lambda b_1) = f(a) = 0 \\ h(b_k) &= f(c - \lambda b_k) \neq 0, \qquad k = 2, \ldots, n. \end{aligned}$$

Die zweite Zeile folgt daraus, dass

$$c - \lambda b_k = a_1 + \lambda(b_1 - b_k) \overset{(2),(3)}{\neq} a_1 + \tfrac{a_j - a_1}{b_1 - b_k}(b_1 - b_k) = a_j,\ \forall j = 1, \ldots, m.$$

(8) Demzufolge ist der größte gemeinsame Teiler in $M[X]$

$$\mathrm{ggT}(g,h) \;=\; X - b_1 \;\in\; M[X],$$

gemäß Satz 7.3.3 sogar in $(K(c))[X]$

$$\mathrm{ggT}(g,h) \;=\; X - b_1 \in (K(c))[X].$$

Also ist $b_1 \in K(c)$.

(9) Dann ist aber auch $a_1 = c - \lambda b_1 \in K(c)$.

7.3.7 Beispiele

1. In Übungsaufgabe A3 (Blatt 1) haben wir nachgewiesen, dass

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \;=\; \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

2. In Übungsaufgabe A30 (Blatt 10) haben wir nachgewiesen, dass für zwei verschiedene Primzahlen p, q

$$\mathbb{Q}(\sqrt{p},\sqrt[3]{q}) \;=\; \mathbb{Q}(\sqrt{p}\cdot\sqrt[3]{q}).$$

8 Endliche Körper

8.0.8 Satz und Definition: Der Frobenius-Monomorphismus

Es sei L ein Körper der Charakteristik p, Primzahl.

(i) Die Abbildung

$$\Phi : \left\{ \begin{array}{ccc} L & \to & L \\ x & \mapsto & x^p \end{array} \right.$$

ist ein Körpermonomorphismus. Man nennt sie den *Frobenius-Monomorphismus*, kurz den *Frobenius*.

(ii) Ist L endlich, so ist Φ bijektiv.

(iii) Der Primkörper $\mathbb{F}_p$ von L ist invariant unter Φ, d.h.

$$\Phi|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}.$$

8.0.9 Beweis

(i) Es ist leicht zu sehen, dass Φ ein unitärer Ringhomomorphismus ist:

$$\begin{aligned} \Phi(1) &= 1^p = 1 \\ \Phi(x \cdot \widetilde{x}) &= (x \cdot \widetilde{x})^p = x^p \cdot \widetilde{x}^p = \Phi(x) \cdot \Phi(\widetilde{x}) \\ \Phi(x + \widetilde{x}) &= (x + \widetilde{x})^p = \sum_{j=0}^{p} \binom{p}{j} x^j \cdot \widetilde{x}^{p-j} \\ &\qquad \text{(Für } j = 1, \ldots, p-1 \text{ gilt } p \mid \tbinom{p}{j}\text{, deshalb } \tbinom{p}{j} = 0 \bmod p.\text{)} \\ &= \sum_{j \in \{0,p\}} \binom{p}{j} x^j \cdot \widetilde{x}^{p-j} \\ &= \widetilde{x}^p + x^p = \Phi(x) + \Phi(\widetilde{x}). \end{aligned}$$

Deshalb ist Φ auch ein Körpermonomorphismus.

(ii) Als injektive Selbstabbildung auf einer endlichen Menge ist Φ automatisch surjektiv.

(iii) Der Primkörper $\mathbb{F}_p$ wird von $1 \in L$ erzeugt. Die Aussage folgt dann aus $\Phi(1) = 1$.

8.0.10 Satz: Charakterisierung endlicher Körper

Es sei L ein Körper.

(i) Ist L endlich, so existieren eine Primzahlpotenz p^n so, dass

$$[L : \mathbb{F}_p] \;=\; n \quad \text{und damit} \quad |L| \;=\; p^n.$$

(ii) Es sei jetzt $q := p^n$ eine solche Primzahlpotenz. Weiter seien $f(X) = X^q - X \in \mathbb{F}_p[X]$ und

$$N_f \;\subseteq\; \{a \in L \mid a^q - a = 0\}$$

die Teilmenge der Nullstellen von f in L. Dann sind die folgenden Aussagen äquivalent.

(E) Es ist $|L| = q$.
(Z′) Es ist $N_f \;=\; L \;\simeq\; \mathrm{Zerf}(f, \mathbb{F}_p)$.
(Z) Es ist $L \;\simeq\; \mathrm{Zerf}(f, \mathbb{F}_p)$.

(iii) Ist p^n eine Primzahlpotenz, so gibt es einen Körper L mit $|L| = p^n$, er ist bis auf Isomorphie eindeutig bestimmt. Deshalb ist auch die Bezeichnung $L = \mathbb{F}_{p^n}$ üblich.

(iv) Ist $g \in \mathbb{F}_p[X]$ irreduzibel mit $\deg g = n$, so hat der per Satz von Kronecker konstruierte Körper $\mathbb{F}_p[X]/(g)$ genau p^n Elemente. Es ist also (ii) anwendbar.

Dabei ist jede Nullstelle von g ein primitives Element der Körpererweiterung $\mathbb{F}_p[X]/(g) : \mathbb{F}_p$.

8.0.11 Beweis

(i) Vgl. Übungsaufgabe A29 (b).

Da L endlich ist, ist die Körpererweiterung $[L : \mathbb{F}_p] = n$, endlich.

Aus der linearen Algebra ist bekannt, dass $L \simeq (\mathbb{F}_p)^{\times n}$, also $|L| = p^n$.

(ii) (Z′) $\Rightarrow$ (Z) ist trivial.

(E) $\Rightarrow$ (Z′). Die multiplikative Gruppe $L^\times$ ist gemäß Satz 7.3.1 zyklisch mit Ordnung $q - 1$. Also gilt für jedes Element $a \in L^\times$, dass $a^{q-1} = 1$, dann $a^q - a = 0$ für alle $a \in L$.

Es folgt $L \subseteq N_f$ und dann

$$q \;=\; |L| \;\leq\; |N_f| \;\leq\; q,$$

also $N_f = L$.

Das aber bedeutet, dass das Polynom f über L zerfällt und es keinen Teilkörper von L mit dieser Eigenschaft geben kann. Wir haben $L \simeq \mathrm{Zerf}(f)$.

(Z′) $\Rightarrow$ (E). Es ist $f'(X) = qX^{q-1} - 1 = -1$, weshalb f und f' keinen gemeinsamen Teiler g mit $\deg g \geq 1$ haben können. Aufgrund der Implikation (B) $\Rightarrow$ (A) aus Satz 7.2.1 hat f nur einfache Nullstellen in L, es folgt

$$|L| \;=\; |N_f| \;=\; q.$$

(Z) $\Rightarrow$ (Z′). Vgl. auch Übungsaufgabe A29. (a),(b),(c).

(1) Wir betrachten die Nullstellenmenge von f in L

$$N \;:=\; \{a \in L \mid a^q - a = 0\}.$$

(2) Wir bezeichnen die k-fache Nacheinanderausführung des *Frobenius-Isomorphismus* mit

$$\Phi^{\circ k} : \left\{ \begin{array}{ccc} L & \to & L \\ x & \mapsto & x^{(p^k)}. \end{array} \right.$$

(3) Es ist $N_f = \ker(\Phi^{\circ n} - \mathrm{id}_L)$. Die Abbildung $\Phi^{\circ n} - \mathrm{id}_L : x \mapsto x^q - x$ ist ein Homomorphismus abelscher Gruppen, also ist N_f eine abelsche Untergruppe von L. Sind $x, y \in N_f$, so folgt

$$\begin{array}{rcl} (x \cdot y)^q & = & x^q \cdot y^q \;=\; x \cdot y \\ (x^{-1})^q & = & (x^q)^{-1} \;=\; x^{-1}, \qquad \text{falls } x \neq 0. \end{array}$$

Also ist N_f abgeschlossen bzgl. Multiplikation und Inversenbildung. Die Körpergesetze werden von L auf die Teilmenge N_f vererbt. N_f ist also ein Unterkörper von L, der alle Nullstellen von $X^q - X$ enthält. Da $L \simeq \mathrm{Zerf}(f)$, folgt $N_f = L$.

(iii) Das folgt sofort aus der Äquivalenz (E) $\Leftrightarrow$ (Z) in (ii) und dem Satz 6.3.3 über Existenz und Eindeutigkeit von Zerfällungskörpern.

(iv) Gemäß Satz von Kronecker ist

$$[\,\mathbb{F}_p[X]/(g) : \mathbb{F}_p\,] \;=\; \deg g = n, \qquad \text{also} \qquad |\,\mathbb{F}_p[X]/(g)\,| \;=\; p^n.$$

8.0.12 Hinweis

Ein Körper der Charakteristik p, Primzahl, muss keineswegs endlich sein.

Beispielsweise ist der Körper $\mathbb{F}_p(X) = \mathrm{Quot}(\mathbb{F}_p[X])$ der rationalen Ausdrücke mit Koeffizienten in $\mathbb{F}_p$ ein unendlicher Körper mit Charakteristik p.

9 Galois-Erweiterungen

9.1 Automorphismengruppe und Galoiskorrespondenz

9.1.1 Definition: Automorphismengruppe

Es sei $L : K$ eine Körpererweiterung. Die Menge der K-Körperautomorphismen $L \to L$ bildet unter Nacheinanderausführung eine (i.a. nicht abelsche) Gruppe.

Sie heißt die *Automorphismengruppe* von $L : K$ und wird mit

$$\operatorname{Aut}(L : K) \;=\; \{\sigma : L \to L \mid \text{ Körperautomorphismus mit } \sigma|_K = \mathrm{id}_K\}$$

bezeichnet.

Oft, aber nicht immer, wird die Automorphismengruppe auch Galoisgruppe genannt, dann auch mit $\operatorname{Gal}(L : K) = \operatorname{Aut}(L : K)$ bezeichnet.

Durchgängige Übereinstimmung in der Begriffsbildung besteht dann, wenn $L : K$ eine Galois-Erweiterung ist, vgl. nächstes Kapitel.

9.1.2 Definition: Galoiskorrespondenz

Es sei $L : K$ eine fixierte Körpererweiterung. Es seien dann

$$\begin{aligned} \mathcal{G} \;&:=\; \mathcal{G}(L : K) \;=\; \{U \mid \text{ Untergruppe von } \operatorname{Aut}(L : K)\} \\ \mathcal{F} \;&:=\; \mathcal{F}(L : K) \;=\; \{M \mid \text{ Zwischenkörper von } L : K\}. \end{aligned}$$

die ,,Verbände" der Untergruppen von $\operatorname{Aut}(L : K)$ bzw. der Zwischenkörper von $L : K$.

Wir definieren weiter die Operatoren

$$\Phi : \left\{ \begin{array}{lcl} \mathcal{G} & \to & \mathcal{F} \\ U & \mapsto & M := \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in U\} \end{array} \right.$$

$$\Gamma : \left\{ \begin{array}{lcl} \mathcal{F} & \to & \mathcal{G} \\ M & \mapsto & U := \{\sigma \in G \mid \sigma(x) = x \text{ für alle } x \in M\} \end{array} \right.$$

Φ ordnet also einer Untergruppe U von $\operatorname{Aut}(L : K)$ den Zwischenkörper M der Elemente zu, der unter allen Automorphismen aus U fixiert bleiben.

Γ ordnet einem Zwischenkörper M die Untergruppe von $\operatorname{Aut}(L : K)$ zu, die die Elemente dieses Zwischenkörpers fest lassen, also die Untergruppe $\operatorname{Aut}(L : M)$.

Man nennt dieses Zusammenspiel zweier Operatoren auch *Galoiskorrespondenz*.

9.1.3 Satz: Erste Eigenschaften der Galoiskorrespondenz

(i) Die beiden Operatoren sind inklusionsumkehrend, d.h.

$$\begin{array}{rcl} U \subseteq \widetilde{U} & \Longrightarrow & \Phi(U) \supseteq \Phi(\widetilde{U}) \\ M \subseteq \widetilde{M} & \Longrightarrow & \Gamma(M) \supseteq \Gamma(\widetilde{M}). \end{array}$$

(ii) Es gilt

$$\begin{array}{rcll} U & \subseteq & \Gamma(\Phi(U)) & \text{für } U \in \mathcal{G} \\ M & \subseteq & \Phi(\Gamma(M)) & \text{für } M \in \mathcal{F}. \end{array}$$

(iii) Für $\sigma \in \operatorname{Aut}(L:K)$ und $M \in \mathcal{F}$ gilt

$$\operatorname{Aut}(L:\sigma(M)) = \sigma \cdot \operatorname{Aut}(L:M) \cdot \sigma^{-1}.$$

9.1.4 Beweis

(i) ist sofort klar aus den Definitionen.

(ii) Man stellt sorgfältig die Definitionen zusammen.

$$\begin{array}{ll} & \sigma \in U \\ \Longrightarrow & \sigma(x) = x \text{ für alle } x \in \Phi(M) \\ \Longrightarrow & \sigma \in \Gamma(\Phi(U)) \end{array} \qquad \begin{array}{ll} & x \in M \\ \Longrightarrow & \sigma(x) = x \text{ für alle } \sigma \in \Gamma(M) \\ \Longrightarrow & x \in \Phi(\Gamma(M)). \end{array}$$

(iii) Überlege einfach die folgende Kette von Äquivalenzen für $\sigma \in \operatorname{Aut}(L:K)$

$$\begin{array}{ll} & \varphi \in \operatorname{Aut}(L:\sigma(M)) \\ \Longleftrightarrow & \varphi(x) = x \quad \text{für alle } x \in \sigma(M) \\ \Longleftrightarrow & \varphi(\sigma(y)) = \sigma(y) \quad \text{für alle } y \in M \\ \Longleftrightarrow & \sigma^{-1} \circ \varphi \circ \sigma = \mathrm{id}_M \\ \Longleftrightarrow & \sigma^{-1} \circ \varphi \circ \sigma \in \operatorname{Aut}(L:M) \\ \Longleftrightarrow & \varphi \in \sigma \cdot \operatorname{Aut}(L:M) \cdot \sigma^{-1}. \end{array}$$

9.1.5 Sammlung von „Kennzahlen"

Es sei $L : K$ eine Körpererweiterung und $f \in K[X]$ mit $\deg f \geq 1$. Wir betrachten dazu die Menge $\mathcal{N}$ der Nullstellen von f in L

$$\mathcal{N} \;=\; \{a \in L \mid f(a) = 0\}.$$

In diesem Kontext definieren wir die folgenden natürlichen Zahlen.

$$\begin{aligned} m &:= \deg f \\ \ell &:= |\mathcal{N}| \\ d &:= [L : K] \\ g &:= \operatorname{ord}(\operatorname{Aut}(L : K)). \end{aligned}$$

9.1.6 Satz: Beziehungen zwischen m, ℓ, d

Wir können einige Erkenntnisse aus Polynom- und Körpertheorie über die Zahlen m, ℓ, d zusammentragen.

(i) Es gilt ganz allgemein $\ell \leq m$.

(ii) Ist f irreduzibel, separabel und zerfällt f in L, so gilt $\ell = m$.

(iii) Ist $L : K$ ein Zerfällungskörper für f, so gilt $d \leq m!$

(iv) Ist f das Minimalpolynom eines Elements von L, so gilt $m \leq d$.

(v) Ist f das Minimalpolynom eines primitiven Elements von $L : K$, so gilt $m = d$.

(vi) Ist f separabel und das Minimalpolynom eines primitiven Elements von $L : K$, so gilt $\ell = m = d$.

Die Zahl $g = \operatorname{ord}(\operatorname{Aut}(L : K))$ trat hier noch nicht in Erscheinung, dies geschieht in dem folgenden Satz.

9.1.7 Begründungen

Alle diese Aussagen sind schon im Laufe dieser Vorlesung aufgetreten.

(i) Ein Polynom f mit Koeffizienten in einem Körper hat höchstens $\deg f$ Nullstellen.

(ii) Das entnimmt man der Definition von Separabilität eines Polynoms, vgl. 7.2.3.

(iii) Das wurde in Satz 6.3.3 (i) konstatiert.

(iv) Ist a ein solches Element, so gilt gemäß Satz 5.1.1 und Gradformel

$$m \;\leq\; [L : K(a)] \cdot \underbrace{[K(a) : K]}_{=m} \;=\; [L : K] \;=\; d.$$

(v) Ist a ein solches Element, so gilt $L = K(a)$ und dann gemäß Satz 5.1.1

$$m \;=\; [K(a) : K] \;=\; [L : K] \;=\; d.$$

(vi) ist eine Kombination von (ii) und (v).

9.1.8 Satz: Automorphismengruppe eines Zerfällungskörpers, Beziehungen zwischen g, ℓ

Es sei $L : K$ der Zerfällungskörper eines Polynoms $f \in K[X]$ mit $\deg f \geq 1$.

(i) Für alle $\sigma \in \mathrm{Aut}(L : K)$ ist $\sigma(\mathcal{N}) = \mathcal{N}$.

Die Automorphismengruppe operiert also auf der Nullstellenmenge $\mathcal{N}$.

(ii) Der zu der Gruppenoperation aus (i) gehörende Gruppenhomomorphismus

$$\left\{ \begin{array}{rcl} \mathrm{Aut}(L : K) & \to & S_{\mathcal{N}} \\ \sigma & \mapsto & \sigma|_{\mathcal{N}} \end{array} \right.$$

ist injektiv.

Deshalb gilt $g \mid \ell$!

(iii) Ist f irreduzibel, so ist die Operation von $\mathrm{Aut}(L : K)$ auf $\mathcal{N}$ transitiv.

Deshalb gilt $\ell \mid g$.

(iv) Ist f das Minimalpolynom eines primitiven Elements von $L : K$, so ist die Operation von $\mathrm{Aut}(L : K)$ auf $\mathcal{N}$ einfach transitiv.

Deshalb gilt $\ell = g$.

9.1.9 Beweis

(i) Sind $\sigma \in \mathrm{Aut}(L : K)$ und $a \in \mathcal{N}$, so gilt (ähnlich wie im Beweis von Satz 6.4.1)

$$\begin{array}{rcl} f(\sigma(a)) & = & f_0 + f_1\sigma(a) + \ldots + f_m[\sigma(a)]^m \\ & = & \sigma(f_0) + \sigma(f_1)\sigma(a) + \ldots + \sigma(f_m)[\sigma(a)]^m \\ & = & \sigma(f_0 + f_1 a + \ldots + f_m a^m) \\ & = & \sigma(0) \ = \ 0 \end{array}$$

und damit $\sigma(\mathcal{N}) \subseteq \mathcal{N}$. Da σ bijektiv ist, gilt Gleichheit.

(ii) Dass $L : K$ Zerfällungskörper ist, bedeutet $L = K(\mathcal{N})$. Ist $\sigma|_{\mathcal{N}} = \mathrm{id}_{\mathcal{N}}$, so folgt $\sigma = \mathrm{id}_L$.

(iii) (1) Sind $a, \widetilde{a} \in \mathcal{N}$, so existiert gemäß Satz 6.2.1 ein K-Körperautomorphismus

$$\sigma : \left\{ \begin{array}{rcl} K(a) & \to & K(\widetilde{a}) \\ \alpha_0 + \alpha_1 a + \ldots + \alpha_{m-1}a^{m-1} & \mapsto & \alpha_0 + \alpha_1\widetilde{a} + \ldots + \alpha_{m-1}\widetilde{a}^{m-1}, \end{array} \right.$$

mit $\sigma(a) \ = \ \widetilde{a}$.

(2) Dies ist auch ein Körperisomorphismus $K(a) \to K(\widetilde{a})$ „innerhalb der Körpererweiterungen $L : K(a)$ und $L : K(\widetilde{a})$", der gemäß Satz 6.2.3 zu einem K-Körperautomorphismus

$$\sigma^{\mathrm{ext}} : \quad L \ \to \ L$$

fortgesetzt werden kann.

(3) Dieser fortgesetzte Körperisomorphismus ist dann ein K-Körperautomorphismus

$$\sigma^{\text{ext}} : L \to L,$$

der a auf $\widetilde{a}$ abbildet.

(4) Gemäß ,,Bahn-Lemma" ist für ein $a \in \mathcal{N}$

$$\begin{aligned} g &= \operatorname{ord}(\operatorname{Aut}(L:K)) = \operatorname{ord}(\underbrace{\operatorname{Aut}(L:K)(a)}_{\text{Bahn von } a \text{ in } \mathcal{N}}) \cdot \operatorname{ord}(\operatorname{Stab}_{\operatorname{Aut}(L:K)}(a)) \\ &\overset{\text{transitiv}}{=} \ell \cdot \operatorname{ord}(\operatorname{Stab}_{\operatorname{Aut}(L:K)}(a)). \end{aligned}$$

(iv) In diesem Fall ist der K-Körperautomorphismus

$$\sigma^{\text{ext}} = \sigma$$

aus Schritt (iii)/(3) gemäß Schritt (iii)/(2) eindeutig, also ist die Operation einfach transitiv. In Schritt (iii)/(4) ist dann $\operatorname{Stab}_{\operatorname{Aut}(L:K)}(a) = \{1\}$, es folgt $g = \ell$.

9.1.10 Satz: Endliche Untergruppe induziert einfache Körpererweiterungen

Es sei L ein Körper. Es seien weiter eine endliche Untergruppe U von $\mathrm{Aut}(L)$ und ihr Fixkörper

$$M \ := \ \Phi(U) \ = \ \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in U\}.$$

vorgegeben.

In Abhängigkeit von $a \in L$ ist

$$U(a) \ = \ \{a_1, a_2, \ldots, a_m\}, \qquad \text{wobei } a_1 := a, \text{ alle } a_j \text{ paarweise verschieden},$$

die Bahn von a in L unter U. Abhängig von dieser Bahn definieren wird das normierte Polynom

$$f \ := \ (X - a_1) \cdot (X - a_2) \cdot \ldots \cdot (X - a_m) \qquad \in L[X].$$

Dann gelten die folgenden Aussagen.

(i) Es ist $f \in M[X]$.

(ii) Es ist a algebraisch über M mit Minimalpolynom f, wobei

$$[M(a) : M] \ = \ \mathrm{ord}(U(a)).$$

(iii) Es gilt weiter

$$[M(a) : M] \ \mid \ \mathrm{ord}(U).$$

9.1.11 Beweis

(i) Ein $\sigma \in U$ ist bijektiv auf $U(a_1)$, lässt also das Polynom f invariant. Damit sind auch die Koeffizienten von f invariant unter σ, d.h. $f \in M[X]$.

(ii) Wegen $f(a_1) = 0$ ist a_1 algebraisch über M, es sei g das Minimalpolynom von a_1 über M.

Ist a_j eine Nullstelle von f, so gibt es $\sigma \in U$ mit $\sigma(a_1) = a_j$ und deshalb ist

$$g(a_j) \ = \ g(\sigma(a_1)) \ = \ \sigma(g(a_1)) \ = \ 0.$$

Damit ist $f \mid g$, wegen der Irreduzibilität und Normiertheit von g ist $f = g$.

Die Begründung für die zweite Aussage ist

$$[M(a) : M] \ \overset{5.1.1(\mathrm{i})}{=} \ \deg f \ = \ m \ = \ \mathrm{ord}(U(a)).$$

(iii) Das ist eine Konsequenz aus (ii) und dem Bahn-Lemma

$$\mathrm{ord}(U(a)) \ \mid \ \mathrm{ord}(U).$$

9.1.12 Satz: Zwei Endlichkeitssätze

Es sei $L : K$ eine Körpererweiterung.

(i) Ist U eine endliche Untergruppe von $\mathrm{Aut}(L : K)$ und $\Phi(U)$ der zugehörige Fixkörper, so ist $L : \Phi(U)$ endlich mit

$$[L : \Phi(U)] \;=\; \mathrm{ord}(U).$$

(ii) Es sei $L : K$ endlich.

Ist M ein Zwischenkörper von $L : K$ und $\Gamma(M)$ die zugehörige Automorphismengruppe, so ist $\Gamma(M)$ endlich mit

$$\mathrm{ord}(\Gamma(M)) \;\mid\; [L : M].$$

9.1.13 Beweis

Zur Vereinfachung des Beweises setzen wir voraus, dass $L : K$ separabel ist. Wir können dann ohne weiteres — zweimal — den Satz 7.3.5 vom primitiven Element verwenden.

(0) Wir setzen $M := \Phi(U) \;=\; \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in U\}$.

(1) Gemäß Satz 9.1.10 (ii) ist $L : M$ algebraisch. Es ist für jede endliche Körpererweiterung $\widetilde{M} : M$ innerhalb $L : M$

$$[\widetilde{M} : M] \;\leq\; \mathrm{ord}(U),$$

da gemäß Satz 7.3.5 ein primitives Element $c \in L$ mit $\widetilde{M} = M(c)$ existiert, und dann Satz 9.1.10 (iii) verwendet werden kann.

(2) Gemäß dem Zusatz 5.3.6 ist dann auch

$$[L : M] \;\leq\; \mathrm{ord}(U).$$

(3) Es sei jetzt wieder gemäß Satz 7.3.5 $\widetilde{c} \in L$ ein primitives Element mit $L = M(\widetilde{c})$. Es gilt dann

$$\mathrm{Stab}(U)(\widetilde{c}) \;=\; \{\mathrm{id}_L\},$$

denn für beliebiges $\sigma \in U$ gilt die Implikation

$$\sigma(\widetilde{c}) \;=\; \widetilde{c} \quad\Longrightarrow\quad \sigma(x) \;=\; x \text{ für alle } x \in L = M(\widetilde{c}).$$

(4) Gemäß 9.1.10 (ii) und Bahn-Lemma ist schließlich

$$[L : M] \;=\; [M(\widetilde{c}) : M] \;=\; \mathrm{ord}(U(\widetilde{c})) \;=\; \mathrm{ord}(\mathrm{Stab}(U)(\widetilde{c})) \cdot \mathrm{ord}(U) \;=\; \mathrm{ord}(U).$$

(ii) Wir setzen $U := \Gamma(M) = \{\sigma \in \mathrm{Aut}(L:K) \mid \sigma(x) = x \text{ für alle } x \in M\}$.

Wir ziehen wieder ein primitives Element $\widehat{c}$ heran mit $L = K(\widehat{c})$. $f \in K[X]$ sei das Minimalpolynom von $\widehat{c}$.

Wie schon mehrfach argumentiert, ist für $\sigma \in \mathrm{Aut}(L:K)$ auch

$$f(\sigma(\widehat{c})) = 0.$$

Da $\mathrm{Aut}(L:K)$ einfach transitiv auf der Menge der Nullstellen $\mathcal{N}$ von f operiert, gilt

$$\mathrm{ord}(\mathrm{Aut}(L:K)) \leq |\mathcal{N}| \leq \deg f = [L:K] < \infty,$$

deshalb auch $\mathrm{ord}(U) < \infty$.

Es ist dann weiter mit 9.1.3 (ii)

$$\widetilde{M} := \Phi(U) = \Phi(\Gamma(M)) \supseteq M,$$

und gemäß Gradformel 4.4.2 und Aussage (i)

$$[L:M] = [L:\widetilde{M}] \cdot [\widetilde{M}:M] = \mathrm{ord}(U) \cdot [\widetilde{M}:M].$$

9.2 Galois-Erweiterungen

In den beiden Aussagen der Endlichkeitssätze tritt eine merkwürdige Unsymmetrie in Erscheinung, die wir jetzt beseitigen.

9.2.1 Satz und Definition: Galois-Erweiterungen

Die Körpererweiterung $L : K$ sei endlich.

Die folgenden Aussagen sind äquivalent.

(A) $L : K$ heißt eine *Galois-Erweiterung*.

(B) $L : K$ ist eine normale und separable Körpererweiterung.

(C) L ist Zerfällungskörper eines separablen Polynoms $f \in K[X]$.

(D) Es ist $\operatorname{ord}(\operatorname{Aut}(L : K)) = [L : K]$.

(E) Es gibt eine endliche Untergruppe U von $\operatorname{Aut}(L : K)$ mit

$$K \;=\; \Phi(U) \;=\; \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in U\}.$$

9.2.2 Beweis

Die Äquivalenz (B) $\Leftrightarrow$ (C) ist Satz 6.4.1 zu entnehmen.

(C) $\Rightarrow$ (D). Es sei c ein primitives Element der Zerfällungskörpererweiterung $L : K$ und μ_c das Minimalpolynom von c.

Es ist dann

$$\operatorname{ord}(\operatorname{Aut}(L : K)) \;=\; g \overset{9.1.8}{=} \ell \overset{9.1.6(\text{ii})}{=} m \overset{5.1.1}{=} d \;=\; [L : K].$$

(D) $\Rightarrow$ (E). Setzt man $U := \operatorname{Aut}(L : K)$, so folgt mit dem Endlichkeitssatz 9.1.12(i)

$$[L : \Phi(U)] \;=\; \operatorname{ord}(U) \overset{\text{Vor.(D)}}{=} [L : K].$$

Wegen $K \subseteq \Phi(U)$ folgt die Behauptung $\Phi(U) = K$.

(E) $\Rightarrow$ (C). Es sei c ein primitives Element der Körpererweiterung $L : K$.

Nach Voraussetzung ist $K = \Phi(U)$, U endliche Untergruppe von $\operatorname{Aut}(L : K)$, so dass wir 9.1.10 (ii) anwenden können. Es ist c algebraisch über K mit Minimalpolynom

$$\mu_c(X) \;=\; (X - a_1) \cdot \ldots \cdot (X - a_n), \qquad a_1 = c,$$

also ist $L = K(a_1, \ldots, a_n)$ Zerfällungskörper von μ_c.

9.2.3 Bemerkung

Beachte bzgl. des Beweises (E) $\Rightarrow$ (C), dass eine separable Körpererweiterung $L : K$ zwar ein primitives Element und dann ein zugehöriges Minimalpolynom hat, der Körper L aber nicht Zerfällungskörper des Minimalpolynoms sein muss. Das wird klar an folgendem Beispiel.

9.2.4 Beispiel

Wir betrachten die Körpererweiterung $L : K = : \mathbb{Q}$, $d \in \mathbb{Z}$, keine Quadratzahl.

Es ist $f(X) = X^2 - d$ das Minimalpolynom des primitiven Elements $\sqrt{d}$.

Es ist, wie man leicht überprüfen kann

$$\tau : \left\{ \begin{array}{rcl} \mathbb{Q}(\sqrt{d}) & \to & \mathbb{Q}(\sqrt{d}) \\ u + v\sqrt{d} & \mapsto & u - v\sqrt{d} \end{array} \right.$$

ein $\mathbb{Q}$-Körperautomorphismus. Es muss also $\{\mathrm{id}_L, \tau\} \subseteq \mathrm{Aut}(L : K)$ sein.

Wegen $|\mathrm{Aut}(L : K)| \mid [L : K]$, vgl. 9.1.12(ii)/$M = K$ ist

$$\mathrm{Aut}(L : K) = \{\mathrm{id}_L, \tau\}.$$

Diese Körpererweiterung ist galoissch, tatsächlich ist jede einzelne Aussage aus Satz 9.2.1 erfüllt.

(B) $\mathbb{Q}(\sqrt{d}) : \mathbb{Q}$ hat Grad 2 und ist deshalb normal (Übungsaufgabe 34, Blatt 11). Da $\mathbb{Q}$ vollkommen ist, ist $\mathbb{Q}(\sqrt{d}) : \mathbb{Q}$ separabel.

(C) $\mathbb{Q}(\sqrt{d}) : \mathbb{Q}$ ist Zerfällungskörper des separablen Polynoms $X^2 - d$.

(D) Es ist $\mathrm{ord}\,\mathrm{Aut}(L : K) = 2 = [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}]$.

(E) Mit $U = \mathrm{Aut}(L : K) = \{\mathrm{id}_L, \tau\}$ ist

$$\begin{array}{rcl} \Phi(U) & = & \{x \in \mathbb{Q}(\sqrt{d}) \mid \sigma(x) = x \text{ für alle } \sigma \in U\} \\ & = & \{x \in \mathbb{Q}(\sqrt{d}) \mid \tau(x) = x\} = \mathbb{Q}. \end{array}$$

9.2.5 Beispiel

Wir betrachten die Körpererweiterung $L : K = \mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$.

Es ist $f(X) = X^3 - 2$ das Minimalpolynom des primitiven Elements $\sqrt[3]{2}$.

Da $\mathcal{N}_f \cap \mathbb{Q}(\sqrt[3]{2}) = \{\sqrt[3]{2}\}$ und $\sigma(\mathcal{N}_f) = \mathcal{N}_f$ für alle $\sigma \in \mathrm{Aut}(L : K)$, muss $\mathrm{Aut}(L : K) = \{1\}$ sein.

Jede einzelne der Aussagen aus dem Satz ist nicht erfüllt.

(B) $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ ist nicht normal. $\sqrt[3]{2}$ ist Nullstelle des irreduziblen Polynoms $X^3 - 2$, die anderen Nullstellen $\sqrt[3]{2} \cdot \zeta_3$ und $\sqrt[3]{2} \cdot \zeta_3^2$ sind nicht in $\mathbb{Q}(\sqrt[3]{2})$ enthalten.

(C) $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ ist nicht Zerfällungskörper des separablen Polynoms $X^3 - 2$ und auch nicht eines anderen irreduziblen Polynoms $f \in \mathbb{Q}[X]$.

(D) Es ist $\mathrm{ord}\,\mathrm{Aut}(L : K) = 1 \neq 3 = [L : K]$.

(E) Es ist

$$\begin{array}{rcl} \Phi(U) & = & \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in U\} = \{x \in L \mid x = x\} \\ & = & L \neq K. \end{array}$$

Der Zerfällungskörper von $f(X) = X^3 - 2$ über $\mathbb{Q}$ ist $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ mit $\zeta_3 = \exp(\frac{2\pi i}{3})$. Wir werden ihn in Kapitel 9.4 ausführlich betrachten.

9.2.6 Folgerungen: Galois-Erweiterungen

(i) Ist $L : K$ eine endliche Körpererweiterung, so gibt es eine Galois-Erweiterung $\widetilde{L} : K$ mit L als Zwischenkörper.

(ii) Ist $L : K$ eine Galois-Erweiterung, so ist für jeden Zwischenkörper M auch $L : M$ eine Galois-Erweiterung.

(iii) Ist $L : K$ eine Galois-Erweiterung, so muss für einen Zwischenkörper M die Körpererweiterung $M : K$ nicht notwendig eine Galois-Erweiterung sein.

9.2.7 Beweis

(i) Es ist $L : K$ algebraisch-endlich-erzeugt, also $L = K(a_1, \ldots, a_n)$ mit algebraischen Elementen $a_j \in L$.

Es sei nun für alle $j = 1, \ldots, n$ $f^{(j)} \in K[X]$ das Minimalpolynom von a_j, dann

$$f \;=\; f^{(1)} \cdot \ldots \cdot f^{(n)}$$

das Produkt.

Dann hat

$$\widetilde{L} \;=\; \mathrm{Zerf}_f(K)$$

die geforderten Eigenschaften.

(ii) Folgerungskette

$$\begin{aligned} & L : K \text{ Galois-Erweiterung} \\ \Longrightarrow\; & L : K \text{ ist Zerfällungskörper eines } f \in K[X] \\ \Longrightarrow\; & L : M \text{ ist Zerfällungskörper von } f \in M[X] \\ \Longrightarrow\; & L : M \text{ Galois-Erweiterung} \end{aligned}$$

(iii) Als Gegenbeispiel dient wieder $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$.

9.3 Hauptsatz der Galois-Theorie

9.3.1 Hauptsatz der Galois-Theorie

Es sei $L : K$ eine Galois-Erweiterung. Wir betrachten die Operatoren

$$\Phi : \left\{ \begin{array}{rcl} \mathcal{G} & \to & \mathcal{F} \\ U & \mapsto & \{x \in L \mid \sigma(x) = x \text{ für alle } \sigma \in U\} \end{array} \right.$$

$$\Gamma : \left\{ \begin{array}{rcl} \mathcal{F} & \to & \mathcal{G} \\ M & \mapsto & \{\sigma \in G \mid \sigma(x) = x \text{ für alle } x \in M\} \end{array} \right.$$

aus 9.1.2. Dann gelten die folgenden Aussagen.

(i) Die beiden Operatoren Φ und Γ sind bijektiv, invers zueinander.

(ii) Ist M ein Zwischenkörper von $L : K$, so ist auch $L : M$ eine Galois-Erweiterung. Es folgt

$$\begin{array}{rcl} [L : M] & = & \operatorname{ord}(\operatorname{Aut}(L : M)) \\ [M : K] & = & \operatorname{ind}(\operatorname{Aut}(L : K) : \operatorname{Aut}(L : M)) \end{array}$$

(iii) Ist M ein Zwischenkörper von $L : K$, so ist $M : K$ genau dann eine Galois-Erweiterung, wenn $\operatorname{Aut}(L : M)$ Normalteiler in $\operatorname{Aut}(L : K)$.

In diesem Fall gibt es einen Gruppenhomomorphismus

$$\left\{ \begin{array}{rcl} \operatorname{Aut}(L : K) & \to & \operatorname{Aut}(M : K) \\ \sigma & \mapsto & \sigma|_M \end{array} \right.$$

und einen Gruppenisomorphismus

$$\left\{ \begin{array}{rcl} \operatorname{Aut}(M : K) & \to & \operatorname{Aut}(L : K)/\operatorname{Aut}(L : M) \\ \sigma & \mapsto & \sigma \operatorname{Aut}(L : M) = \operatorname{Aut}(L : M)\sigma. \end{array} \right.$$

9.3.2 Beweis

(i) Wir zeigen $\Phi \circ \Gamma = \mathrm{id}|_{\mathcal{F}}$. Es sei also $M \in \mathcal{F}$ ein Zwischenkörper von $L : K$. Setze $U := \Gamma(M) = \operatorname{Aut}(L : M)$. Dann haben wir mit Satz 9.1.3(ii)

$$K \subseteq M \subseteq \Phi(\Gamma(M)) \subseteq L.$$

Gemäß Folgerung 9.2.6(ii) ist auch $L : M$ eine Galois-Erweiterung, deshalb

$$[L : M] \overset{9.1.12\,(i)}{=} \operatorname{ord} U \overset{9.1.12\,(i)}{=} [L : \Phi(U)] = [L : \Phi(\Gamma(M))]$$

und damit $M = \Phi(\Gamma(M))$.

Wir zeigen als nächstes $\Gamma \circ \Phi = \mathrm{id}|_{\mathcal{G}}$. Es ist dann $U \subseteq \Gamma(\Phi(U))$ Untergruppe.

Da gemäß Folgerung 9.2.6(ii) $L : M$ eine Galois-Erweiterung ist, folgt

$$\operatorname{ord}(\Gamma(\Phi(U))) \overset{9.2.6(ii)}{=} [L : \Phi(U)] \overset{9.1.12\,(i)}{=} \operatorname{ord}(U).$$

und damit $U = \Gamma(\Phi(U))$.

(ii) Die erste Aussage wurde in Folgerung 9.2.6(ii) bereits angegeben. Es folgt

$$[L : M] \;=\; \operatorname{ord}(\operatorname{Aut}(L : K))$$

und dann mit Gradformel und Indexformel der Gruppentheorie (= Satz von Lagrange)

$$[M : K] \;=\; \tfrac{[L:K]}{[L:M]} \;=\; \tfrac{\operatorname{ord}(\operatorname{Aut}(L:K))}{\operatorname{ord}(\operatorname{Aut}(L:M))} \;=\; \operatorname{ind}(\operatorname{Aut}(L : K) : \operatorname{Aut}(L : M)).$$

(iii) $\Rightarrow$. Es sei also $L : K$ eine Galoiserweiterung, d.h. Zerfällungskörper eines Polynoms $f \in K[X]$. Weiter sei $\sigma \in \operatorname{Aut}(L : K)$ beliebig, fixiert.

(1) Gemäß der Implikation (A) $\Rightarrow$ (B) in Satz **??** ist $\sigma(M) \subseteq M$.

(2) Es ist weiter $[M : K] = [\sigma(M) : K] < \infty$, deswegen $M = \sigma(M)$.

(3) Schließlich folgt mit Satz 9.1.3(iii), dass

$$\operatorname{Aut}(L : M) \;=\; \operatorname{Aut}(L : \sigma(M)) \;=\; \sigma \cdot \operatorname{Aut}(L : M) \cdot \sigma^{-1},$$

d.h. $\operatorname{Aut}(L : M)$ ist Normalteiler in $\operatorname{Aut}(L : K)$.

$\Leftarrow$ (1) Ist $\operatorname{Aut}(L : M)$ Normalteiler in $\operatorname{Aut}(L : K)$, so folgt mit 9.1.3(iii) für ein beliebiges $\sigma \in \operatorname{Aut}(L : K)$

$$\operatorname{Aut}(L : \sigma(M)) \;=\; \sigma \cdot \operatorname{Aut}(L : M) \cdot \sigma^{-1} \;=\; \operatorname{Aut}(L : M).$$

(2) Gemäß (i) gibt es eine ein-eindeutige Zuordnung der Automorphismengruppen zu den Fixkörpern, es folgt

$$M \;=\; \sigma(M)$$

(3) Dadurch ist der Gruppenhomomorphismus

$$\epsilon : \left\{ \begin{array}{rcl} \operatorname{Aut}(L : K) & \to & \operatorname{Aut}(M : K) \\ \sigma & \mapsto & \sigma|_M \end{array} \right.$$

wohldefiniert.

(4) Es ist $\ker \epsilon := \operatorname{Aut}(L : M)$ und dann mit dem Homomorphiesatz der Gruppentheorie

$$\operatorname{Aut}(L : K)/\operatorname{Aut}(L : M) \;\simeq\; \operatorname{im} \epsilon \;\subseteq\; \operatorname{Aut}(M : K).$$

(5) Mit dem Endlichkeitssatz 9.1.12(ii) und (ii) dieses Satzes folgt

$$\begin{array}{rcl} [M : K] & \overset{9.1.12(ii)}{\geq} & \operatorname{ord}(\operatorname{Aut}(M : K)) \;\geq\; \operatorname{ord}(\operatorname{im} \epsilon) \\ & \overset{(ii)}{=} & \operatorname{ind}(\operatorname{Aut}(L : K) : \operatorname{Aut}(L : M)) \;=\; [M : K], \end{array}$$

also

$$[M : K] \;=\; \operatorname{ord}(\operatorname{Aut}(M : K)).$$

Damit ist $M : K$ eine Galois-Erweiterung. Die Inklusion in (4) ist dann wegen

$$\operatorname{ord}(\operatorname{Aut}(M : K)) \;=\; \operatorname{ind}(\operatorname{Aut}(L : K) : \operatorname{Aut}(L : M))$$

eine Gleichheit und wir erhalten den im Satz angegebenen Isomorphismus.

9.4 Der Zerfällungskörper von $X^3 - 2$

9.4.1 Beispiel: Der Zerfällungskörper von $X^3 - 2$

Das Polynom

$$f(X) \;=\; X^3 - 2 \qquad \in \mathbb{Q}[X]$$

ist gemäß Eisenstein irreduzibel, die Nullstellen in $\mathbb{C}$ sind

$$z_1 = \omega, \qquad z_2 = \omega\zeta, \qquad z_3 = \omega\zeta^2,$$

wobei zur Abkürzung

$$\omega = \sqrt[3]{2}, \qquad \zeta = e^{\frac{2\pi i}{3}}$$

gesetzt wurde.

Der Zerfällungskörper von f ist

$$L \;=\; \mathbb{Q}(z_1, z_2, z_3) \;=\; \mathbb{Q}(z_1, z_2) \;=\; \mathbb{Q}(\omega, \zeta) \;=\; \mathbb{Q}(\omega + \zeta).$$

Zwei mögliche geordnete Basen von $L : \mathbb{Q}$ sind

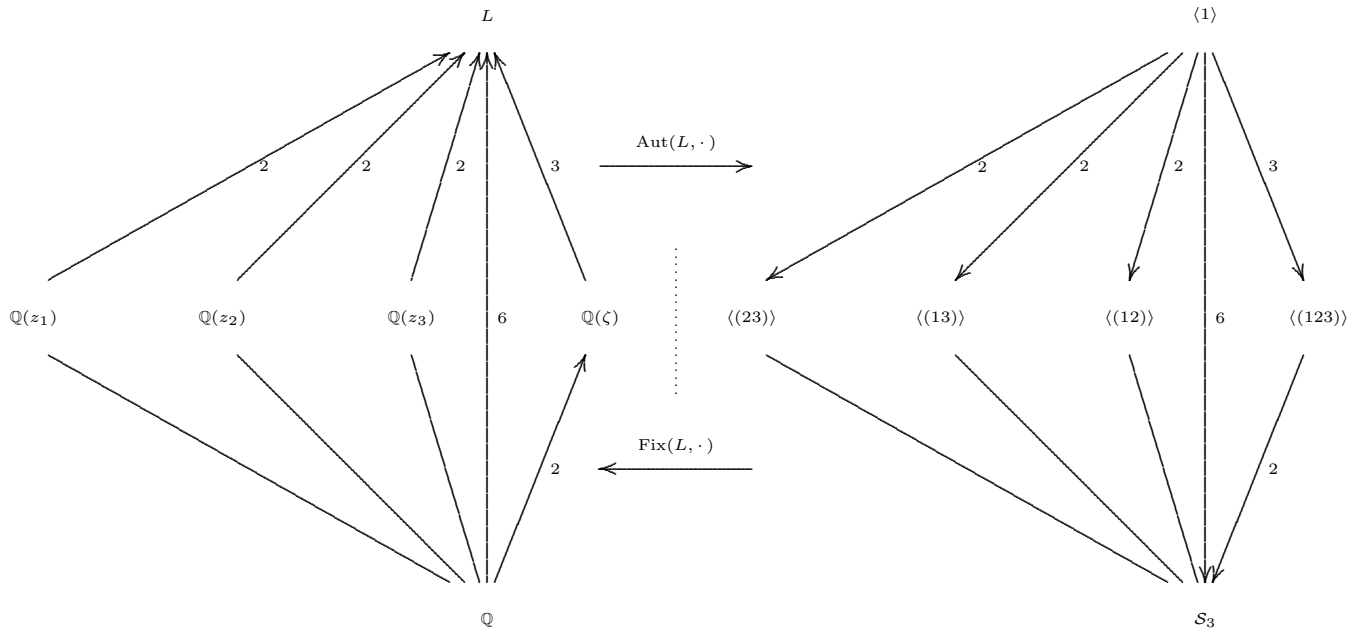
$$B_1 \;=\; (\omega, \quad \omega^2, \quad \omega\zeta, \quad \omega^2\zeta, \quad \omega\zeta^2, \quad \omega^2\zeta^2)$$

$$B_2 \;=\; (1, \quad \zeta, \quad \omega, \quad \omega\zeta, \quad \omega^2, \quad \omega^2\zeta).$$

Es gilt also $[L : K] = 3! = 6$.

Die Tabelle auf der nächsten Seite zeigt auf, dass $\mathrm{Aut}(L : K) \simeq S_3$.

9.4.2 Diagramm zur Galoiskorrespondenz



Pfeil bedeutet: galoissche Erweiterung
Zahl bedeutet: Grad der Erweiterung

Pfeil bedeutet: Normalteiler
Zahl bedeutet: Index der Untergruppe

9.4.3 Tabelle: Wie operiert die Galoisgruppe S_3 auf $\mathbb{Q}(\omega,\zeta)$?

Es seien

$$\omega = \sqrt[3]{2}, \qquad \zeta = e^{\frac{2\pi i}{3}}.$$

	$\pi \in \mathcal{S}_3$	Nullstellen	$\{\omega,\zeta\}$	prim. Element	Basis B_1	Basis B_2
σ_1	(1)	$z_1 \mapsto z_1$ $z_2 \mapsto z_2$ $z_3 \mapsto z_3$	$\omega \mapsto \omega$ $\zeta \mapsto \zeta$	$\omega+\zeta \mapsto \omega+\zeta$	$\omega \mapsto \omega$ $\omega^2 \mapsto \omega^2$ $\omega\zeta \mapsto \omega\zeta$ $\omega^2\zeta \mapsto \omega^2\zeta$ $\omega\zeta^2 \mapsto \omega\zeta^2$ $\omega^2\zeta^2 \mapsto \omega^2\zeta^2$	$1 \mapsto 1$ $\zeta \mapsto \zeta$ $\omega \mapsto \omega$ $\omega\zeta \mapsto \omega\zeta$ $\omega^2 \mapsto \omega^2$ $\omega^2\zeta \mapsto \omega^2\zeta$
σ_2	(12)	$z_1 \mapsto z_2$ $z_2 \mapsto z_1$ $z_3 \mapsto z_3$	$\omega \mapsto \omega\zeta$ $\zeta \mapsto \zeta^2$	$\omega+\zeta \mapsto \omega\zeta+\zeta^2$	$\omega \mapsto \omega\zeta$ $\omega^2 \mapsto \omega^2\zeta^2$ $\omega\zeta \mapsto \omega$ $\omega^2\zeta \mapsto \omega^2\zeta$ $\omega\zeta^2 \mapsto \omega\zeta^2$ $\omega^2\zeta^2 \mapsto \omega^2$	$1 \mapsto 1$ $\zeta \mapsto \zeta^2$ $\omega \mapsto \omega\zeta$ $\omega\zeta \mapsto \omega$ $\omega^2 \mapsto -\omega^2-\omega^2\zeta$ $\omega^2\zeta \mapsto \omega^2\zeta$
σ_3	(13)	$z_1 \mapsto z_3$ $z_2 \mapsto z_2$ $z_3 \mapsto z_1$	$\omega \mapsto \omega\zeta^2$ $\zeta \mapsto \zeta^2$	$\omega+\zeta \mapsto \omega\zeta^2+\zeta^2$	$\omega \mapsto \omega\zeta^2$ $\omega^2 \mapsto \omega^2\zeta$ $\omega\zeta \mapsto \omega\zeta$ $\omega^2\zeta \mapsto \omega^2$ $\omega\zeta^2 \mapsto \omega$ $\omega^2\zeta^2 \mapsto \omega^2\zeta^2$	$1 \mapsto 1$ $\zeta \mapsto \zeta^2$ $\omega \mapsto -\omega-\omega\zeta$ $\omega\zeta \mapsto \omega\zeta$ $\omega^2 \mapsto \omega^2\zeta$ $\omega^2\zeta \mapsto \omega^2$
σ_4	(23)	$z_1 \mapsto z_1$ $z_2 \mapsto z_3$ $z_3 \mapsto z_2$	$\omega \mapsto \omega$ $\zeta \mapsto \zeta^2$	$\omega+\zeta \mapsto \omega+\zeta^2$	$\omega \mapsto \omega$ $\omega^2 \mapsto \omega^2$ $\omega\zeta \mapsto \omega\zeta^2$ $\omega^2\zeta \mapsto \omega^2\zeta^2$ $\omega\zeta^2 \mapsto \omega\zeta$ $\omega^2\zeta^2 \mapsto \omega^2\zeta$	$1 \mapsto 1$ $\zeta \mapsto \zeta^2$ $\omega \mapsto \omega$ $\omega\zeta \mapsto -\omega-\omega\zeta$ $\omega^2 \mapsto \omega^2$ $\omega^2\zeta \mapsto -\omega^2-\omega^2\zeta$
σ_5	(123)	$z_1 \mapsto z_2$ $z_2 \mapsto z_3$ $z_3 \mapsto z_1$	$\omega \mapsto \omega\zeta$ $\zeta \mapsto \zeta$	$\omega+\zeta \mapsto \omega\zeta+\zeta$	$\omega \mapsto \omega\zeta$ $\omega^2 \mapsto \omega^2\zeta^2$ $\omega\zeta \mapsto \omega\zeta^2$ $\omega^2\zeta \mapsto \omega^2$ $\omega\zeta^2 \mapsto \omega$ $\omega^2\zeta^2 \mapsto \omega^2\zeta$	$1 \mapsto 1$ $\zeta \mapsto \zeta$ $\omega \mapsto \omega\zeta$ $\omega\zeta \mapsto -\omega-\omega\zeta$ $\omega^2 \mapsto -\omega^2-\omega^2\zeta$ $\omega^2\zeta \mapsto \omega^2$
σ_6	(132)	$z_1 \mapsto z_3$ $z_2 \mapsto z_1$ $z_3 \mapsto z_2$	$\omega \mapsto \omega\zeta^2$ $\zeta \mapsto \zeta$	$\omega+\zeta \mapsto \omega\zeta^2+\zeta$	$\omega \mapsto \omega\zeta^2$ $\omega^2 \mapsto \omega^2\zeta$ $\omega\zeta \mapsto \omega$ $\omega^2\zeta \mapsto \omega^2\zeta^2$ $\omega\zeta^2 \mapsto \omega\zeta$ $\omega^2\zeta^2 \mapsto \omega^2$	$1 \mapsto 1$ $\zeta \mapsto \zeta$ $\omega \mapsto -\omega-\omega\zeta$ $\omega\zeta \mapsto \omega$ $\omega^2 \mapsto \omega^2\zeta$ $\omega^2\zeta \mapsto -\omega^2-\omega^2\zeta$

9.5 Galoistheorie für endliche Körper

9.5.1 Satz: Galoistheorie für endliche Körper

Wir betrachten eine Körpererweiterung $L : K$ mit Körpern der Mächtigkeit $|L| = p^\ell$ und $|K| = p^k$. Es ist dann $n = \frac{\ell}{k} \in \mathbb{N}$.

(i) Die Körpererweiterung $L : K$ ist galoissch mit

$$\operatorname{ord}(\operatorname{Aut}(L : K)) \;=\; [L : K] \;=\; n.$$

(ii) Die Automorphismengruppe $\operatorname{Aut}(L : K)$ ist zyklisch, sie wird erzeugt von der k-fach-Nacheinanderausführung des Frobenius-Automorphismus

$$\Phi^{\circ k} : \left\{ \begin{array}{lcl} L & \to & L \\ x & \mapsto & x^{(p^k)}. \end{array} \right.$$

(iii) Zu jedem $m \in \mathbb{N}$ mit $k \mid m$ und $m \mid \ell$ gibt es genau einen Zwischenkörper M von $L : K$ mit $|M| = p^m$. Die Galoiskorrespondenz kann man dem folgenden Diagramm entnehmen.

$$\begin{array}{ccc} L \simeq \mathbb{F}_{p^\ell} & & \langle \Phi^{\circ \ell} \rangle = \langle \mathrm{id}_L \rangle \simeq \mathbb{Z}/\mathbb{Z} \\ \Big\uparrow \frac{\ell}{m} & & \Big\downarrow \frac{\ell}{m} \\ M \simeq \mathbb{F}_{p^m} & & \langle \Phi^{\circ m} \rangle \simeq \mathbb{Z}/(\frac{\ell}{m}\mathbb{Z}) \\ \Big\uparrow \frac{m}{k} & & \Big\downarrow \frac{m}{k} \\ K \simeq \mathbb{F}_{p^k} & & \langle \Phi^{\circ k} \rangle \simeq \mathbb{Z}/(\frac{\ell}{k}\mathbb{Z}) \end{array}$$

9.5.2 Beweis

(i) Gemäß Satz 8.0.10(ii) ist L Zerfällungskörper des (über dem vollkommenen Körper $\mathbb{F}_p$, vgl. Satz 7.2.5) separablen Polynoms $X^q - X \in \mathbb{F}_p[X]$. Gemäß Definition 9.2.1 ist $L : \mathbb{F}_p$ galoissch.

Gemäß Folgerung 9.2.6 (ii) ist dann auch $L : K$ galoissch und es ist $\operatorname{ord}(\operatorname{Aut}(L : K)) = [L : K] = n$.

(ii) Gemäß 8.0.10 (ii) stimmt K mit der Nullstellenmenge

$$\mathcal{N}_f \;=\; \{x \in K \mid x^{(p^k)} - x = 0\}$$

überein. Deshalb ist für alle $x \in K$

$$\Phi^{\circ k}|_K(x) \;=\; x^{(p^k)} \;=\; x,$$

also $\Phi^{\circ k}|_K = \mathrm{id}_K$ und damit $\Phi^{\circ k} \in \mathrm{Aut}(L:K)$.

Die gleiche Argumentation mir ℓ anstelle von k zeigt, dass für alle $x \in L$

$$(\Phi^{\circ k})^{\circ n}(x) \;=\; \Phi^{\circ \ell}(x) \;=\; x^{(p^\ell)} \;=\; x,$$

also $(\Phi^{\circ k})^{\circ n} = \mathrm{id}_L$.

Wäre $(\Phi^{\circ k})^{\circ j} = \mathrm{id}_L$ für ein $j \in \{1, \ldots, n-1\}$, so wäre für alle $x \in L^\times$

$$x^{(p^{jk}-1)} \;=\; x^{(p^{jk})} \cdot x^{-1} \;=\; x \cdot x^{-1} \;=\; 1.$$

Das würde bedeuten, dass $L^\times$ kein Element der Ordnung $\ell - 1 = p^\ell - 1 = p^{jn} - 1$ enthalten würde im Widerspruch zu Satz 7.3.1, der aussagt, dass L^x mit $|L^\times| = \ell - 1$ zyklisch ist.

Damit ist $\mathrm{ord}(\Phi^{\circ k}) = n$ als Element von $\mathrm{Aut}(L:K)$. Aufgrund von $|\mathrm{Aut}(L:K)| = n$ ist $\mathrm{Aut}(L:K)$ zyklisch.

(iii) Das ergibt sich sofort aus dem Hauptsatz der Galoistheorie und der Tatsache, dass die Untergruppen der zyklischen Gruppe $\mathrm{Aut}(L:K) \simeq \mathbb{Z}/n\mathbb{Z}$ genau die zyklischen Gruppen sind, deren Ordnung ein Teiler von n ist.

10 Kreisteilung

10.1 Vorbereitung: Die Eulersche φ-Funktion

10.1.1 Definition und Satz: Die Eulersche φ-Funktion

Die *Eulersche φ-Funktion* ist definiert durch

$$\varphi : \left\{ \begin{array}{rcl} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & |\,(\mathbb{Z}/n\mathbb{Z})^\times\,| \;=\; |\,\{d \in \mathbb{N} \mid d \leq n \text{ und } \operatorname{ggT}(d,n) = 1\}\,| \,. \end{array} \right.$$

Es ergibt sich aus dem Lemma von Bezout oder dem Umfeld des Erweiterten Euklidischen Algorithmus, dass für $n, d \in \mathbb{N}$ und $d < n$

$$\overline{d} \in (\mathbb{Z}/n\mathbb{Z})^\times \quad \Longleftrightarrow \quad \operatorname{ggT}(d,n) = 1.$$

10.1.2 Satz: Formeln zur Berechnung der φ-Funktion

(i) Es gilt

$$\varphi(n) \cdot \varphi(m) \;=\; \varphi(n \cdot m), \qquad \text{falls } n, m \in \mathbb{N},\ \operatorname{ggT}(n,m) = 1.$$

(ii) Ist p^k eine Primzahlpotenz, so gilt

$$\varphi(p^k) \;=\; p^{k-1} \cdot (p-1)$$

(iii) Ist $n \in \mathbb{N}$ beliebig, so gilt

$$\begin{array}{rcl} n & = & p_1^{k_1} \cdot \ldots \cdot p_\ell^{k_\ell} \\ \Longrightarrow \quad \varphi(n) & = & p_1^{k_1-1} \cdot \ldots \cdot p_\ell^{k_\ell-1} \cdot (p_1-1) \cdot \ldots \cdot (p_\ell - 1). \end{array}$$

10.1.3 Beweis

(i) Wegen $\operatorname{ggT}(m,n) = 1$ besteht gemäß chinesischem Restsatz ein Isomorphismus von uk Ringen

$$\mathbb{Z}/(mn\mathbb{Z}) \;\simeq\; \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Deshalb gilt

$$(\mathbb{Z}/(mn\mathbb{Z}))^\times \;\simeq\; (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times \;=\; (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

(ii) In der Zahlenmenge $\{1, \ldots, p^k\}$ gilt für jede p-te Zahl a, dass $\operatorname{ggT}(a, p^k) \neq 1$. Demzufolge ist

$$\varphi(p^k) \;=\; p^k - \tfrac{p^k}{p} \;=\; p^k - p^{k-1} \;=\; p^{k-1} \cdot (p-1).$$

(iii) ist eine Folgerung aus (i) und (ii).

10.2 Kreisteilungskörper und Einheitswurzeln

10.2.1 Definition: Kreisteilungskörper und Einheitswurzeln

Es sei $p = 0$ oder p eine Primzahl. Es sei dazu K der Primkörper mit $\mathrm{char}(K) = p$.

Es sei weiter eine Zahl $n \in \mathbb{N}$ fixiert und dann $X^n - 1 \in K[X]$.

1. Der (bis auf Isomorphie eindeutige) Zerfällungskörper $K_n := \mathrm{Zerf}(X^n - 1, K)$ von $X^n - 1 \in K[X]$ heißt der *n-te Kreisteilungskörper (über K)*.

2. Eine Nullstelle $\xi \in K_n$ von $f(X) = X^n - 1 \in K[X]$ heißt *n-te Einheitswurzel (über K)*. Wegen $\deg X^n - 1 = n$ gibt es höchstens n solche n-ten Einheitswurzeln in K_n.

3. Die Teilmenge K_n^{EW} der n-ten Einheitswurzeln in K_n bildet eine endliche multiplikative Untergruppe von $K_n^\times$, ist also gemäß Satz 7.3.1 zyklisch.

4. Eine n-te Einheitswurzel in K_n, die diese zyklische Gruppe K_n^{EW} erzeugt, heißt eine *primitive n-te Einheitswurzel*. Die Theorie der (multiplikativ geschriebenen) zyklischen Gruppen zeigt, dass die Teilmenge der primitiven Einheitswurzeln gegeben ist durch

$$\begin{aligned} K_n^{\mathrm{prEW}} &= \{\zeta \in K_n^{\mathrm{EW}} \mid \langle\zeta\rangle = K_n^{\mathrm{EW}}\} \\ &= \{\zeta \in K_n^{\mathrm{EW}} \mid \mathrm{ord}(\zeta) = n\} \\ &= \{\hat{\zeta}^k \in K_n^{\mathrm{EW}} \mid 1 \le k \le n,\ \mathrm{ggT}(k,n) = 1\}, \text{ wobei } \hat{\zeta} \in K_n^{\mathrm{prEW}} \text{ fixiert.} \\ &\simeq \mathrm{Aut}(K_n^{\mathrm{EW}}). \end{aligned}$$

10.2.2 Bemerkung

Der Begriff „Kreisteilungskörper" ist eigentlich nur sinnvoll im Fall $K = \mathbb{Q}$, da dann die adjungierten n-ten Einheitswurzeln $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ genau die Eckpunkte des regelmäßigen n-Ecks mit Eckpunkt 1 auf dem Einheitskreis in der komplexen Ebene sind.

Es hat sich jedoch eingebürgert, dass man auch im allgemeinen Fall von Kreisteilungskörpern spricht.

10.2.3 Beispiele: Kreisteilungskörper für kleine n

1. $n = 1$. Das Polynom $X - 1$ hat die Nullstelle $1 \in K$. Der „erste" Kreisteilungskörper über K stimmt mit K überein.

2. $n = 2$. Das Polynom $X^2 - 1 = (X - 1)(X + 1)$ zerfällt über K in Linearfaktoren. Der zweite Kreisteilungskörper über K stimmt ebenfalls mit K überein.

3. $n = 3$. Das Polynom $X^3 - 1 = (X - 1)(X^2 + X + 1)$ enthält als Faktor das Polynom $X^2 + X + 1$, die beiden Nullstellen ζ und ζ^{-1} sind multiplikativ invers zueinander.

   Der dritte Kreisteilungskörper $K_3 = K(\zeta)$ wird von einer dieser beiden Nullstellen erzeugt. Ist $X^2 + X + 1$ irreduzibel über K, so gilt $[K_3 : K] = 2$.

4. $n = 4$. Das Polynom $X^4 - 1 = (X-1)(X+1)(X^2+1)$ enthält als Faktor das Polynom $X^2 + 1$, die beiden Nullstellen ζ und $-\zeta$ sind additiv invers zueinander.

   Der vierte Kreisteilungskörper $K_4 = K(\zeta)$ wird von einer dieser beiden Nullstellen erzeugt. Ist $X^2 + 1$ irreduzibel über K, so gilt $[K_4 : K] = 2$.

10.2.4 Sonderfall: $\operatorname{char}(K) \mid n$

Es sei $\operatorname{char}(K) = p$ und $n = m \cdot p \in \mathbb{N}$.

Dann ist

$$X^n - 1 \;=\; X^{mp} - 1 \;=\; (X^m - 1)^p$$

und die zyklische Gruppe der n-ten Einheitswurzeln ist gegeben durch

$$K_n^{\mathrm{EW}} \;=\; K_m^{\mathrm{EW}}.$$

Das heißt, alle Überlegungen im Zusammenhang mit n-ten (primitiven) Einheitswurzeln und den darauf beruhenden n-ten Kreisteilungspolynomen lassen sich vom Fall n auf den Fall m zurückspielen.

Man kann O.B.d.A. annehmen, dass $\operatorname{char}(K) \nmid n$.

10.3 Kreisteilungspolynome

10.3.1 Definition: Kreisteilungspolynom

Es sei K_n der n-te Kreisteilungskörper über K mit $\operatorname{char}(K) \nmid n$.

Das Polynom

$$\Phi_n(X) \ := \prod_{\zeta \in K_n^{\mathrm{prEW}}} (X - \zeta) \quad \in K_n[X]$$

heißt das *n-te Kreisteilungspolynom (über K).*

10.3.2 Satz: Kreisteilungspolynome

Es sei K_n der n-te Kreisteilungskörper über K mit $\operatorname{char}(K) \nmid n$.

(i) Das Polynom $X^n - 1$ ist separabel über K. Deshalb ist $|K_n^{\mathrm{EW}}| \ = \ n$ und

$$X^n - 1 \ = \prod_{\xi \in K_n^{\mathrm{EW}}} (X - \xi).$$

(ii) Es ist $|K_n^{\mathrm{prEW}}| \ = \ \deg \Phi_n \ = \ \varphi(n)$ und

$$\begin{aligned} \Phi_n(X) \ &= \prod_{\zeta \in K_n^{\mathrm{prEW}}} (X - \zeta) \\ &= \prod_{\substack{1 \le k \le n \\ \mathrm{ggT}(k,n) = 1}} (X - \hat{\zeta}^k), \qquad \text{wobei } \hat{\zeta} \in K_n^{\mathrm{prEW}}, \text{ fixiert.} \end{aligned}$$

(iii) Es ist

$$K_n^{\mathrm{EW}} \ = \bigcup_{\substack{1 \le d \le n \\ d \mid n}} K_d^{\mathrm{prEW}} \qquad \text{(disjunkte Vereinigung)} \ ,$$

wobei wir hier die Abhängigkeit der Teilmenge K_n^{EW} von n durch den zusätzlichen Index n zum Ausdruck bringen. Deshalb gelten dann die Rekursionsformeln

$$\begin{aligned} \Phi_1(X) \ &= \ X - 1 \\ \Phi_n(X) \cdot \prod_{\substack{1 \le d < n \\ d \mid n}} \Phi_d(X) \ &= \ X^n - 1. \end{aligned}$$

10.3.3 Beweis

(i) Aufgrund von $\mathrm{char}(K) \not| n$ ist

$$\begin{aligned} \mathrm{ggT}(X^n - 1, nX^{n-1}) &= \mathrm{ggT}(X^n - 1 - n^{-1}XnX^{n-1}, nX^{n-1}) \\ &= \mathrm{ggT}(-1, nX^{n-1}) = 1. \end{aligned}$$

Gemäß der Implikation (B) $\Rightarrow$ (A) in Satz 7.2.1 hat $X^n - 1$ in K_n nur einfache Nullstellen, also genau n Nullstellen.

(ii) Das ist eine Aussage aus der Gruppentheorie über die Erzeuger von zyklischen Gruppen.

(iii) Die erste Teilaussage ist wieder der Gruppentheorie von zyklischen Gruppen entnommen. Die zweite ergibt sich dann direkt aus der Definition der Kreisteilungspolynome.

10.3.4 Illustration

Wir illustrieren die Aussage (C) anhand der ersten 10 Kreisteilungspolynome.

	$\Phi_1(X)$	$\Phi_2(X)$	$\Phi_3(X)$	$\Phi_4(X)$	$\Phi_5(X)$	$\Phi_6(X)$	$\Phi_7(X)$	$\Phi_8(X)$	$\Phi_9(X)$	$\Phi_{10}(X)$
$X-1$	$(X-1)$									
X^2-1	$(X-1)$	$(X+1)$								
X^3-1	$(X-1)$		(X^2+X+1)							
X^4-1	$(X-1)$	$(X+1)$		(X^2+1)						
X^5-1	$(X-1)$				$(X^4+X^3+X^2+X+1)$					
X^6-1	$(X-1)$	$(X+1)$	(X^2+X+1)			(X^2-X+1)				
X^7-1	$(X-1)$						$(X^6+\ldots+1)$			
X^8-1	$(X-1)$	$(X+1)$		(X^2+1)				(X^4+1)		
X^9-1	$(X-1)$		(X^2+X+1)						(X^6+X^3+1)	
$X^{10}-1$	$(X-1)$	$(X+1)$			$(X^4+X^3+X^2+X+1)$					$(X^4-X^3+X^2-X+1)$

Die dann folgenden sechs Kreisteilungspolynome sind

$$\begin{aligned} \Phi_{11}(X) &= X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1 \\ \Phi_{12}(X) &= X^4-X^2+1 \\ \Phi_{13}(X) &= X^{12}+X^{11}+X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1 \\ \Phi_{14}(X) &= X^6-X^5+X^4-X^3+X^2-X+1 \\ \Phi_{15}(X) &= X^8-X^7+X^5-X^4+X^3-X+1 \\ \Phi_{16}(X) &= X^8+1. \end{aligned}$$

10.3.5 Beispiel

Ist n eine Primzahl, so kann schnell bestätigt werden, dass

$$\Phi_n(X) = X^{n-1} + X^{n-2} + \ldots + X + 1.$$

10.3.6 Satz: Koeffizienten der Kreisteilungspolynome

Es sei K_n der n-te Kreisteilungskörper über K mit $\mathrm{char}(K) \not| n$.

Für die Kreisteilungspolynome Φ_n gelten die folgenden Aussagen.

(i) Es ist $\Phi_n \in K[X]$ und normiert.

(ii) Im Fall $\mathrm{char}(K) = 0$ gilt sogar $\Phi_n \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$.

(iii) Das n-te Kreisteilungspolynom $\Phi_n^{(p)}$ bei Charakteristik p entsteht aus dem n-ten Kreisteilungspolynom $\Phi_n^{(0)}$ bei Charakteristik 0 durch Reduktion der Koeffizienten $\bmod p$.

10.3.7 Beweis

(i),(ii) Aufgrund der Aussage (iii) in Satz 10.3.2 ergibt sich Φ_n durch Polynomdivision aus den Vorgänger-Polynomen durch

$$\Phi_n(X) \;=\; (X^n - 1) \cdot \Big[\prod_{\substack{1 \le d < n \\ d|n}} \Phi_d(X) \Big]^{-1}.$$

Der Satz 3.4.1 über die Polynomdivision in uk Ringen bei ,,Divisor-Leitkoeffizient ist Einheit" liefert die Aussage, dass $\Phi_n \in K[X]$ und im Fall $\mathrm{char}(K) = 0$ sogar $\Phi_n \in \mathbb{Z}[X]$. Die Normiertheit ist dann eine einfache Folgerung.

(iii) Da die Polynomdivision und Reduktion der Koeffizienten $\bmod p$ vertauschbar sind, ergibt sich auch die Aussage (iii).

10.4 Kreisteilung bei Charakteristik 0

10.4.1 Satz: Kreisteilung bei Charakteristik 0

Wir betrachten die Kreisteilung über $\mathbb{Q}$. Es sei $n \in \mathbb{N}$ fixiert.

(i) Es ist $\Phi_n \in \mathbb{Z}[X]$ irreduzibel in $\mathbb{Z}[X]$ und damit auch in $\mathbb{Q}[X]$.

(ii) Die Körpererweiterung $\mathbb{Q}_n : \mathbb{Q}$ mit dem n-ten Kreisteilungskörper $\mathbb{Q}_n$ über $\mathbb{Q}$ ist galoissch mit

$$|\operatorname{Aut}(\mathbb{Q}_n : \mathbb{Q})| \;=\; [\mathbb{Q}_n : \mathbb{Q}] \;=\; \varphi(n).$$

(iii) Es bestehen Gruppenisomorphismen wie folgt

$$\psi : \left\{ \begin{array}{rcccc} (\mathbb{Z}/n\mathbb{Z})^\times & \to & \operatorname{Aut}(\mathbb{Q}_n^{\mathrm{EW}}) & \to & \operatorname{Aut}(\mathbb{Q}_n : \mathbb{Q}) \\ \overline{j} & \mapsto & (\xi \mapsto \xi^j) & \mapsto & \sigma_j. \end{array} \right.$$

Insbesondere ist $\operatorname{Aut}(\mathbb{Q}_n : \mathbb{Q})$ abelsch.

10.4.2 Beweis

Für den Fall, dass n Primzahl ist, wurde der Beweis schon in Übungsaufgabe 22/Blatt 8 erbracht. Der folgende Beweis für den allgemeinen Fall $n \in \mathbb{N}$ stammt von Dedekind, 1857.

(1) Es sei $\hat{\zeta}$ eine fixierte primitive Einheitswurzel. Dann ist gemäß 10.2.1 die Menge aller primitiven Einheitswurzeln gegeben durch

$$\begin{aligned} \mathbb{Q}_n^{\mathrm{prEW}} &= \{\hat{\zeta}^k \in \mathbb{Q}_n^{\mathrm{EW}} \mid 1 \le k \le n,\ \mathrm{ggT}(k,n) = 1\} \\ &= \{\hat{\zeta}^{p_1 \cdot \ldots \cdot p_\ell} \in \mathbb{Q}_n^{\mathrm{EW}} \mid p_j \text{ Primzahl mit } p_j \nmid n \text{ für alle } j = 1, \ldots, \ell\}. \end{aligned}$$

(2) Wir zeigen nun: Ist μ das Minimalpolynom von $\zeta \in \mathbb{Q}_n^{\mathrm{prEW}}$ und p Primzahl mit $p \nmid n$, so gilt auch $\mu(\zeta^p) = 0$. Damit ist μ auch das Minimalpolynom von ζ^p.

(3) Wegen $\zeta^n - 1 = 0$ gibt es ein normiertes Polynom

$$f \;=\; f_0 + f_1 X + \ldots + f_{m-1} X^{m-1} + X^m \quad \in \mathbb{Q}[X]$$

so, dass

$$X^n - 1 \;=\; \mu(X) \cdot f(X).$$

(4) Da die drei Polynome in dieser Gleichung normiert sind, erhalten wir mit der Folgerung 3.7.8 (iv), dass

$$\mu, f \in \mathbb{Z}[X].$$

(5) Angenommen, $\mu(\zeta^p) \neq 0$. Dann ist $f(\zeta^p) = 0$ und damit

$$\mu(X) \mid [f_0 + f_1 X^p + \ldots + f_{m-1}(X^p)^{m-1} + (X^p)^m],$$

das heißt, es existiert — wieder nach Folgerung 3.7.8 (iv) — ein $g \in \mathbb{Z}[X]$, normiert, mit

$$f_0 + f_1 X^p + \ldots + f_m (X^p)^m \;=\; \mu(X) \cdot g(X).$$

(6) Wir reduzieren diese Gleichung $\bmod p$ und erhalten

$$\overline{f_0} + \overline{f_1} X^p + \ldots + \overline{f_m} (X^p)^m \;=\; \overline{\mu}(X) \cdot \overline{g}(X).$$

Beachte, dass $\overline{\mu}$ nicht notwendig die Irreduzibilität von μ erbt.

(7) Wir wenden dann den Frobenius-Monomorphismus auf diese Gleichung an und erhalten, da der Frobenius-Monomorphismus gleich der Identität in $\mathbb{F}_p$ ist,

$$(\overline{f_0} + \overline{f_1} X + \ldots + \overline{f_m} X^m)^p \;=\; \overline{\mu}(X) \cdot \overline{g}(X).$$

(8) Ist nun $\overline{h}$ ein irreduzibler Teiler von $\overline{\mu}$, so ist $\overline{h}$ auch Teiler von

$$\overline{f}(X) \;=\; \overline{f_0} + \overline{f_1} X + \ldots + \overline{f_m} X^m.$$

(9) Reduziert man nun die Gleichung aus (3) $\bmod p$, so folgt, dass

$$(\overline{h}(X))^2 \mid (X^n - \overline{1}).$$

(10) Gemäß Satz 10.3.2(i) ist $X^n - \overline{1}$ separabel, hat also nur einfache Nullstellen, beachte dabei, dass $p \not| n$.

(11) Ein irreduzibler Teiler kann also nicht doppelt auftreten. Aufgrund dieses Widerspruchs muss die Annahme $\mu(\zeta^p) \neq 0$ aus Schritt (5) verworfen werden.

(12) Damit ist nachgewiesen, dass das Minimalpolynom für $\zeta \in \mathbb{Q}_n^{\mathrm{prEW}}$ und das Kreisteilungspolynom Φ_n übereinstimmen. Damit ist Φ_n irreduzibel in $\mathbb{Z}[X]$, gemäß Satz von Gauß dann auch in $\mathbb{Q}[X]$.

(ii) Ist $\widehat{\zeta}$ eine n-te Einheitswurzel über $\mathbb{Q}$, also Nullstelle des irreduziblen Polynoms Φ_n, so gilt

$$\mathbb{Q}_n \;=\; \mathbb{Q}(\widehat{\zeta})$$

und deshalb

$$[\mathbb{Q}_n : \mathbb{Q}] \;=\; \deg \Phi_n \;=\; \varphi(n).$$

(iii) Der zweite Isomorphismus ist einfach durch die Fortsetzung der Abbildung $(\xi \mapsto \xi^j) \in \mathrm{Aut}(\mathbb{Q}_n^{\mathrm{EW}})$ auf $\mathbb{Q}_n$ gegeben, siehe dazu Satz 6.3.3.

10.4.3 Liste der Einheitswurzeln in $\mathbb{C}$

Die Nullstellen des n-ten Kreisteilungspolynoms in $\mathbb{Q}_n \subseteq \mathbb{C}$ sind wie folgt.

$\Phi_n(X)$	Primitiv	Weitere außer 1
$\Phi_1(X)$	$\zeta_1 = +1$	
$\Phi_2(X)$	$\zeta_2 = -1$	
$\Phi_3(X)$	$\zeta_3 = \frac{-1+\sqrt{-3}}{2}$	$\zeta_3^2 = \frac{-1-\sqrt{-3}}{2}$
$\Phi_4(X)$	$\zeta_4 + i$	$\zeta_4^3 = -i$
$\Phi_5(X)$	$\zeta_5 = (-\frac{1}{4} + \frac{\sqrt{5}}{4}) + i\sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}$	$\zeta_5^2, \zeta_5^3, \zeta_5^4$
$\Phi_6(X)$	$\zeta_6 = \frac{1+\sqrt{-3}}{2}$	$\zeta_6^5 = \frac{1-\sqrt{-3}}{2}$
$\Phi_7(X)$	ζ_7	$\zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6$
$\Phi_8(X)$	$\zeta_8 = \frac{1+i}{\sqrt{2}}$	$\zeta_8^3 = \frac{-1+i}{\sqrt{2}}, \zeta_8^5 = \frac{-1-i}{\sqrt{2}}, \zeta_8^7 = \frac{1-i}{\sqrt{2}}$
$\Phi_9(X)$	ζ_9	$\zeta_9^2, \zeta_9^4, \zeta_9^5, \zeta_9^7, \zeta_9^8$
$\Phi_{10}(X)$	$\zeta_{10} = (\frac{1}{4} + \frac{\sqrt{5}}{4}) + i\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}$	$\zeta_{10}^3, \zeta_{10}^7, \zeta_{10}^9$

10.5 Kreisteilung bei Charakteristik p

10.5.1 Satz: Kreisteilung bei Charakteristik p

Wir betrachten die Kreisteilung über $\mathbb{F}_p$.

Es seien $n \in \mathbb{N}$ und die Primzahl p fixiert mit $p \nmid n$. Dazu sei

$$m \;=\; \operatorname{ord}(\overline{p}) \quad \text{in der Gruppe } (\mathbb{Z}/n\mathbb{Z})^\times.$$

(i) Φ_n zerfällt in $\mathbb{F}_p[X]$ in $\frac{\varphi(n)}{m}$ paarweise nicht assoziierte irreduzible Faktoren vom Grad m.

(ii) Es ist

$$(\mathbb{F}_p)_n \;\simeq\; \mathbb{F}_{p^m}.$$

Damit sind alle weiteren Eigenschaften der Körpererweiterung $(\mathbb{F}_p)_n : \mathbb{F}_p$ durch Satz 9.5.1 erschlossen.

(iii) Es ist

$$\Phi_n \in \mathbb{F}_p[X] \text{ irreduzibel} \quad \text{und} \quad [(\mathbb{F}_p)_n : \mathbb{F}_p] \;=\; \varphi(n)$$

genau dann, wenn

$$\operatorname{ord}(\overline{p}) \;=\; \varphi(n) \quad \text{in der Gruppe } (\mathbb{Z}/n\mathbb{Z})^\times,$$

also wenn $\overline{p}$ erzeugendes Element der (dann zyklischen) Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.

10.5.2 Beweis

(i) Es sei $f \in \mathbb{F}_p[X]$ ein irreduzibler Faktor von Φ_n.

(1) Wir stellen eine Liste von Aussagen über eine Zahl $\ell \in \mathbb{N}$ zusammen.

(A) Es gilt $m \mid \ell$.

(B) Es ist $\overline{p}^\ell = \overline{1} \mod n$.

(C) Es ist $n \mid (p^\ell - 1)$.

(D) Φ_n zerfällt vollständig in $\mathbb{F}_{p^\ell}[X]$.

(E) f zerfällt vollständig in $\mathbb{F}_{p^\ell}[X]$.

(F) f hat eine Nullstelle in $\mathbb{F}_{p^\ell}$.

(G) Φ_n hat eine Nullstelle in $\mathbb{F}_{p^\ell}$.

(H) Es gilt $(\deg f) \mid \ell$.

Wir zeigen im folgenden, dass alle Aussagen äquivalent sind.

(2) Die Äquivalenz (A) $\Leftrightarrow$ (B) folgt leicht aus der Definition von m.

Die Äquivalenz (B) $\Leftrightarrow$ (C) ist offensichtlich.

(C) $\Rightarrow$ (D). Wende den Satz 10.3.2 (iii) mit $n = p^\ell - 1$ an. Dann ist

$$X^{(p^\ell-1)} - 1 \;=\; \prod_{\substack{1 \le d \le (p^\ell-1)\\ d \mid (p^\ell-1)}} \Phi_d(X) \;=\; \Phi_n(X) \cdot \prod_{\substack{1 \le d \le (p^\ell-1)\\ d \mid (p^\ell-1)\\ d \neq n}} \Phi_d(X).$$

Da $X^{(p^\ell-1)} - 1$ in $\mathbb{F}_{p^\ell}[X]$ vollständig zerfällt, gilt dies auch für Φ_n.

Die Implikationen (D) $\Rightarrow$ (E) $\Rightarrow$ (F) $\Rightarrow$ (G) sind wegen $f \mid \Phi_n$ trivial.

(G) $\Rightarrow$ (C). Ist $\zeta \in \mathbb{F}_{p^\ell}$ Nullstelle von Φ_n, dann auch von $X^n - 1$, also ist $\zeta^n = 1$.

Wegen $|\mathbb{F}_{p^\ell}^\times| = p^\ell - 1$ folgt $n \mid (p^\ell - 1)$.

(F) $\Leftrightarrow$ (H). Ist ζ eine Nullstelle von f (in einem Zerfällungskörper über $\mathbb{F}_p$), so gilt

$$\deg f \;=\; [\mathbb{F}_p(\zeta) : \mathbb{F}_p]$$

und weiter gemäß Satz 8.0.10 über die Charakterisierung endlicher Körper, dass

$$\mathbb{F}_p(\zeta) \;\simeq\; \mathbb{F}_{p^{\deg f}}.$$

Weiter ist dann aufgrund von Satz 9.5.1 über Galoistheorie bei endlichen Körpern

$$\begin{aligned} & \zeta \;\in\; \mathbb{F}_{p^\ell} \\ \Longleftrightarrow\quad & \mathbb{F}_p(\zeta) \;\subseteq\; \mathbb{F}_{p^\ell} \\ \Longleftrightarrow\quad & \deg f \mid \ell. \end{aligned}$$

(3) Es sind also die beiden Aussagen

$$m \mid \ell \qquad (\deg f) \mid \ell$$

für beliebiges $\ell \in \mathbb{N}$ äquivalent. Daraus folgt unmittelbar $m = \deg f$, was zu beweisen war.

(4) Da Φ_n paarweise verschiedene Nullstellen im Zerfällungskörper hat, können nicht zwei verschiedene Teiler f und $\widetilde{f}$ von Φ_n assoziiert sein.

(ii) Ist $\widehat{\zeta}$ eine n-te Einheitswurzel über $\mathbb{F}_p$, also Nullstelle des irreduziblen Polynoms Φ_n, so ist $\widehat{\zeta}$ auch Nullstelle eines der irreduziblen Teiler f wie in (i). Wegen

$$(\mathbb{F}_p)_n = \mathbb{F}_p(\widehat{\zeta})$$

gilt

$$[(\mathbb{F}_p)_n : \mathbb{F}_p] \;=\; \deg f \;=\; m,$$

also $(\mathbb{F}_p)_n \simeq \mathbb{F}_{p^m}$.

(iii) Das ist der Fall $m = \varphi(n)$ aus (i) und (ii).

10.5.3 Beispiel

Wir ziehen als Beispiel den Fall $q = 5$ und $n = 12$ im Kontext von (ii) heran. Es ist dann, da $5^2 = 25 = 1 \bmod 12$, also

$$m := \operatorname{ord}(\overline{5}) = 2.$$

Tatsächlich zerfällt das Kreisteilungspolynom Φ_{12} über $\mathbb{F}_5$ in zwei nicht assoziierte irreduzible Faktoren:

$$\Phi_{12}(X) = X^4 - X^2 + \overline{1} = (X^2 - \overline{2}X - \overline{1}) \cdot (X^2 + \overline{2}X - \overline{1}).$$

10.5.4 Beispiel

Wir ziehen als Beispiel den Fall $q = 2$ und $n = 15$ im Kontext von (ii) heran. Es ist dann, da $2^4 = 16 = 1 \bmod 15$, also

$$m := \operatorname{ord}(\overline{2}) = 4.$$

Tatsächlich zerfällt das Kreisteilungspolynom

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

nach Reduktion $\bmod 2$ in zwei nicht assoziierte irreduzible Faktoren vom Grad 4.

$$\Phi_{15}(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1 = (X^4 + X^3 + 1) \cdot (X^4 + X + 1).$$

11 Konstruieren mit Zirkel und Lineal

11.1 Einstieg

11.1.1 Ebene geometrische Objekte

Wir wollen hier zur Vereinfachung Teilmengen der Zeichenebene *(ebene geometrische) Objekte* nennen, wenn es sich um

- Punkte, Geraden, Halbgeraden, Strecken, Kreislinien und Kreisbögen, Winkel, Pfeile oder
- deren Vereinigung oder Schnitte

handelt.

11.1.2 Kommentare

- Man könnte in dieser ,,Definition" auf die Erwähnung von Geraden, Strecken oder Winkeln verzichten, da sich diese Objekte als Vereinigungs- oder Schnittmengen der anderen ergeben.
- Ein Pfeil ist die Zusammenstellung einer Halbgerade und einer in ihr enthaltenen Strecke.
- Wird die Zeichenebene mit einem Koordinatensystem versehen, so werden die erwähnten Objekte durch lineare oder quadratische Gleichungen und Ungleichungen beschrieben.
- Umgekehrt umfasst die Liste oben nicht alle Objekte, die durch quadratische Gleichungen beschrieben werden, beispielsweise Ellipsen, Parabeln oder Hyperbeln.

11.1.3 Definition: Konstruieren

Die folgenden Möglichkeiten beschreiben, wie man — ausgehend von gegebenen Objekten — neue Objekte ,,erstellen" kann. Wir wollen sie *elementare Schritte* nennen.

- Zu zwei gegebenen Punkten können erstellt werden
  - die Verbindungsstrecke
  - die Halbgerade mit einem der beiden Punkte als Anfangspunkt
  - die Gerade durch die zwei Punkte
- Zu einem gegebenen Punkt und einer gegebenen Strecke kann der Kreis erstellt werden, der den vorgegebenen Punkt als Mittelpunkt und die Länge der vorgegebenen Strecke als Radius hat.
- Sind zwei Geraden und/oder Kreise gegeben, so können der oder die Schnittpunkte dieser beiden Objekte erstellt werden.

Jede Abfolge von solchen elementaren Schritten wird als *Konstruktion* bezeichnet. Die zugehörige Tätigkeit heißt *Konstruieren*.

11.2 Algebraisierung der Konstruierbarkeit

11.2.1 Einstieg

Die klassischen Fragen, welche Objekte konstruiert werden können, können durch Algebraisierung genauer gestellt — und dann auch beantwortet — werden.

11.2.2 Modellierung durch kartesisches Koordinatensystem

Mit Hilfe eines Koordinatensystems (Zwei senkrecht zueinander stehende Achsen, mit Längenskalen) können die Punkte der Zeichenebene eineindeutig reellen Zahlenpaaren oder komplexen Zahlen zugeordnet werden.

$$\begin{array}{ccccc} \text{Zeichenebene} & \longleftrightarrow & \mathbb{R}^2 & \longleftrightarrow & \mathbb{C} \\ \text{Punkt} & \longleftrightarrow & \underbrace{\text{reelles Zahlenpaar} \quad \longleftrightarrow \quad \text{komplexe Zahl}}_{\text{kurz: Zahl}} & & \end{array}$$

Bezogen auf diese Korrespondenz seien zwei Punkte $\triangleq$ Zahlen fest vorgegeben:

$$\begin{array}{ccccc} O & \longleftrightarrow & (0,0) & \longleftrightarrow & 0 \\ E & \longleftrightarrow & (1,0) & \longleftrightarrow & 1 \end{array}$$

11.2.3 Satz: Die Menge der konstruierbaren Zahlen

Für einen Punkt C der Zeichenebene und die zugehörige komplexe Zahl c sind die folgenden Aussagen äquivalent.

(K) Der Punkt C ist — ausgehend von O und E — in endlich vielen Schritten mit Zirkel und Lineal konstruierbar.

(R) Die Zahl c ergibt sich — ausgehend von den Zahlen 0 und 1 — durch eine endliche Abfolge von Grundrechenarten und Ziehen von Quadratwurzeln.

(A) Die Zahl c ist enthalten in einem Körper K_n, der sich mit einer endlichen Abfolge von Körpererweiterungen vom Grad 2 aus dem Körper $\mathbb{Q}$ der rationalen Zahlen ergibt:

$$\begin{aligned} \mathbb{Q} =: K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots\ldots \subseteq K_n \subsetneq \mathbb{C} \\ [K_i : K_{i-1}] = 2 \qquad \text{für alle } i = 1, \ldots, n. \end{aligned}$$

11.2.4 Begründung

(K) $\Rightarrow$ (R)

Es sei C ein Punkt, der — ausgehend von bereits konstruierten Punkten — konstruiert werden kann. Das bedeutet, dass sich C als Schnittpunkt von zwei Geraden und/oder Kreisen ergibt, die durch bereits konstruierte Punkte definiert sind.

Die zugehörige Zahl c ist demzufolge Lösung eines Systems von zwei linearen oder quadratischen Gleichungen, deren Koeffizienten sich aus denen der bereits konstruierten Punkte

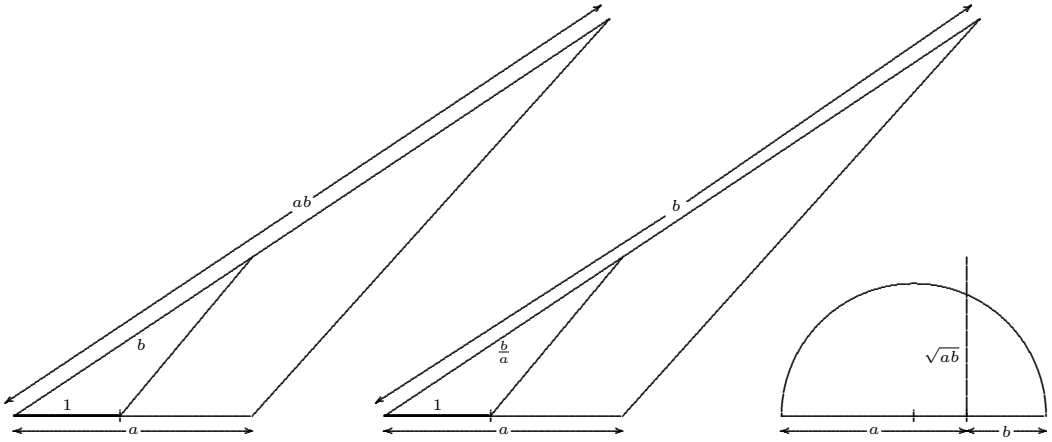
ergeben. Diese Koeffizienten sind also selbst mit Grundrechenarten und Quadratwurzelziehen herstellbar.

Die Lösungen dieses Gleichungssystems sind wiederum mit Grundrechenarten und Quadratwurzelziehen herstellbar. Es gilt also (R).

(R) $\Rightarrow$ (K)

(1) Summe und Differenz von zwei Zahlen können geometrisch mittels Aneinandersetzen der Ursprungs-Verbindungsstrahlen (= Ortsvektoren) konstruiert werden.

(2) Dass auch Produkte, Quotienten und Quadratwurzeln von Zahlen geometrisch konstruiert werden können, zeigen wir zunächst für vorgegebene reell-positive Zahlen auf. Man kann dies anhand der folgenden Konstruktionen einsehen, die auf den Strahlensätzen bzw. auf dem Höhensatz beruhen.



Vorgegeben: a, b
Zu konstruieren: $a \cdot b$

Vorgegeben: a, b
Zu konstruieren: $\frac{b}{a}$

Vorgegeben: a, b
Zu konstruieren: $\sqrt{a \cdot b}$

(3) Sind dann a und b beliebige komplexe Zahlen, so können Produkt, Quotient und Quadratwurzeln mit Hilfe von Polarkoordinaten auf

- Produkt, Quotient und Quadratwurzel der Beträge sowie
- Winkeladdition, -subtraktion und -halbierung der Argumente

zurückgeführt werden.

(R) $\Leftrightarrow$ (A).

Die Abgeschlossenheit der Menge der ,,konstruierbaren Zahlen" unter den Grundrechenarten entspricht genau der Tatsache, dass alle komplexen Zahlen mit rationalen Koordinaten konstruiert werden können. Es können also alle Zahlen des Zwischenkörpers $\mathbb{Q}(i)$ von $\mathbb{C} : \mathbb{Q}$ mit $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ konstruiert werden.

Das Ziehen von Quadratwurzeln bedeutet algebraisch, dass Nullstellen von beliebigen quadratischen Polynomen adjungiert werden können. Das entspricht aber genau den Körpererweiterungen vom Grad 2.

11.3 Klassische Fragen der Konstruierbarkeit

In Zeiten, in denen die Mathematikdidaktik Begriffe wie ,,Anwendung, Konkretisierung, Veranschaulichung" als alleinige Prinzipien eines gelingenden Mathematikunterrichts darstellt, erscheint die Formulierung dieser Aussage als ,,schwer, abstrakt, absurd".

Tatsächlich ermöglicht sie auf dann ,,einfache" Weise, klassische Fragen der Konstruierbarkeit zu beantworten.

11.3.1 Verdoppelung des Würfelvolumens

Es sei die Kantenlänge eines Würfels in der Zeichenebene vorgegeben. Kann die Kantenlänge des Würfels mit doppeltem Volumen konstruiert werden?

NEIN. Sieht man man die gegebene Kantenlänge als ,,gleich 1" an, so ist die Frage auf die nach der Konstruierbarkeit des Punktes mit Koordinaten $(0, \sqrt[3]{2})$ reduziert.

Als Nullstelle des irreduziblen Polynoms $x \mapsto x^3 - 2$ ist die Zahl $\sqrt[3]{2}$ sie in einem Erweiterungskörper K mit $[K : \mathbb{Q}] = 3$ enthalten. Damit kann sie nicht in einem Körper des Typs wie in Aussage 11.2.3 (A) enthalten sein.

11.3.2 Konstruktion des regelmäßigen n-Ecks

Es sei ein Kreis vorgegeben. Kann das ihm einbeschriebene regelmäßige n-Eck konstruiert werden?

Diese Frage lässt sich auf die nach der Konstruierbarkeit einer n-ten primitiven Einheitswurzel $\zeta_n \in \mathbb{C}$ zurückführen. Mit algebraischen Methoden zeigt man die folgende Kette von Äquivalenzen (Carl Friedrich Gauss, 1796)

Das regelmäßige n-Eck ist konstruierbar.

$\Leftrightarrow$ Eine primitive n-te Einheitswurzel $\zeta_n \in \mathbb{C}$ ist konstruierbar.

$\Leftrightarrow$ ζ_n ist in einem Körper wie 11.2.3 (A) enthalten.

$\Leftrightarrow$ Das Minimalpolynom Φ_n von ζ_n (= n-tes Kreisteilungspolynom) hat eine Zweierpotenz als Grad.

$\Leftrightarrow$ Es ist $\varphi(n) = 2^j$ für ein $j \in \mathbb{N}_0$.

$\Leftrightarrow$ Die Zahl n hat eine Primfaktorzerlegung der Form $n = 2^k \cdot p_1 \cdot \ldots \cdot p_r$, wobei $k \in \mathbb{N}_0$ und $p_1, \ldots, p_r$ paarweise verschiedene Fermatsche Primzahlen sind. Dabei heißt eine Primzahl Fermatsch, wenn sie eine Primfaktorzerlegung der Form $p = 2^{(2^\ell)} + 1$ mit $\ell \in \mathbb{N}_0$, hat.

Die heute bekannten fünf Fermatschen Primzahlen sind in der Tabelle aufgelistet. Man

vermutet, dass es keine weiteren gibt.

ℓ	0	1	2	3	4		5
2^ℓ	1	2	4	8	16		32
$2^{(2^\ell)}+1$	2^1+1 $=3$	2^2+1 $=5$	2^4+1 $=17$	2^8+1 $=257$	$2^{16}+1$ $=65\,537$		$2^{32}+1$ $=4\,294\,967\,297$
Fermat'sch?	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$		$=641\cdot 6\,700\,417$

11.3.3 Dreiteilung des Winkels

Kann ein beliebiger vorgegebener Winkel gedrittelt werden?

NEIN.

Anderenfalls würde beispielsweise der konstruierbare Winkel mit Maß 60° gedrittelt werden können. Mit Hilfe des Winkels mit Maß 20° könnte dann ein regelmäßiges 18-Eck konstruiert werden, was aber gemäß Abschnitt 11.3.2 unmöglich ist.

11.3.4 Die Quadratur des Kreises

Es sei ein Kreis vorgegeben. Kann die Seitenlänge des Quadrats mit gleichem Flächeninhalt konstruiert werden?

NEIN.

Sieht man man den gegebenen Radius als ,,gleich 1" an, so ist die Frage auf die nach der Konstruierbarkeit der Zahl $\sqrt{\pi}$ reduziert.

Die Frage wurde endgültig im Jahr 1882 von Ferdinand von Lindemann (1852 – 1939) negativ beschieden: Er bewies, dass π transzendent ist, d.h. nicht als Nullstelle eines Polynoms mit rationalen Koeffizienten auftritt. Dann kann aber π und demzufolge auch $\sqrt{\pi}$ nicht in einem Körper wie in Aussage 11.2.3 (A) enthalten sein.

12 Auflösbarkeit von polynomialen Gleichungen

12.1 Zwei vorbereitende Sätze

12.1.1 Satz: Galois-Eigenschaft bei Adjunktion einer primitiven n-ten Einheitswurzel

Es sei $L : K$ eine Galoiserweiterung und ζ eine primitive n-te Einheitswurzel.

(i) Dann ist auch $L(\zeta) : K(\zeta)$ eine Galoiserweiterung.

(ii) Zwischen den Automorphismengruppen gibt es einen Gruppenmonomorphismus

$$\mathrm{Aut}(L(\zeta) : K(\zeta)) \quad \hookrightarrow \quad \mathrm{Aut}(L : K).$$

12.1.2 Beweis

(i) Es ist

L Zerfällungskörper eines Polynoms $f \in K(\zeta)[X]$,

$L(\zeta)$ Zerfällungskörper des Polynoms $X^n - 1 \in L[X]$,

$K(\zeta)$ Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$.

Folglich ist auch

$L(\zeta)$ Zerfällungskörper des Polynoms $f(X) \cdot (X^n - 1) \in K[X]$,

also $L(\zeta) : K$ galoissch. Weiter ist dann gemäß Satz 9.2.6 (ii)

$L(\zeta) : K(\zeta)$ galoissch $f(X) \cdot (X^n - 1) \in K[X]$.

(ii) Die beiden Körpererweiterungen $L(\zeta) : L$ und $L : K$ sind galoissch. Gemäß dem Hauptsatz über normale Körpererweiterungen 6.1.4 ist

$$\sigma(L) \quad = \quad L \qquad \text{für alle} \quad \sigma \in \mathrm{Aut}(L(\zeta) : K).$$

Es folgen die Implikationen

$$\sigma \in \mathrm{Aut}(L(\zeta) : K(\zeta)) \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}(L(\zeta) : K) \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}(L : K).$$

12.1.3 Lemma von Artin

Es seien K ein Körper und $\sigma_1, \ldots, \sigma_k \in \mathrm{Aut}(K)$.

Die beiden folgenden Aussagen sind äquivalent.

(A) $\sigma_1, \ldots, \sigma_k$ sind paarweise verschieden.

(B) $\sigma_1, \ldots, \sigma_k$ sind linear unabhängig im K-Vektorraum $\mathrm{Abb}(K^\times, K)$.

12.1.4 Bemerkung

In dem Satz (und Beweis) kann anstelle von $K^\times$ als Definitionsmenge für den Abbildungsvektorraum in (B) eine beliebige Halbgruppe H gewählt werden. In diesem Fall muss an die Abbildungen $\sigma_1, \ldots, \sigma_k$ die Forderung gestellt werden, dass sie Halbgruppenhomomorphismen $H \to K^\times$ sind.

12.1.5 Beweis

(B) $\Rightarrow$ (A) ist trivial.

(A) $\Rightarrow$ (B). Induktion über k. Der Fall $k = 1$ ist trivial, da σ_1 nicht die Nullabbildung sein kann.

Sei die Behauptung für $k - 1 \in \mathbb{N}$ gezeigt.

(1) Wir setzen an, dass

$$\alpha_1\sigma_1 + \alpha_2\sigma_2 + \ldots + \alpha_k\sigma_k \;=\; 0 \qquad (*).$$

(2) Da $\sigma_1 \neq \sigma_k$, gibt es ein $a \in K^\times$ mit

$$\sigma_1(a) \;\neq\; \sigma_k(a).$$

(3) Mit beliebigem $x \in K^\times$ setzen wir in die Gleichung $(*)$ einerseits die Stelle $a \cdot x$ ein, andererseits setzen wir die Stelle x ein und multiplizieren die Gleichung mit $\sigma_k(a)$.

$$\begin{aligned} &\alpha_1\sigma_1(a)\sigma_1(x) \;+\; \ldots \;+\; \alpha_{k-1}\sigma_{k-1}(a)\sigma_2(x) \;+\; \alpha_k\sigma_k(a)\sigma_k(x) \;=\; 0 \\ &\alpha_1\sigma_k(a)\sigma_1(x) \;+\; \ldots \;+\; \alpha_{k-1}\;\sigma_k(a)\sigma_2(x) \;+\; \alpha_k\sigma_k(a)\sigma_k(x) \;=\; 0. \end{aligned}$$

(4) Subtraktion der beiden Gleichungen ergibt

$$\alpha_1[\sigma_1(a) - \sigma_k(a)]\sigma_1(x) \;+\; \ldots \;+\; \alpha_{k-1}[\sigma_{k-1}(a) - \sigma_k(a)]\sigma_{k-1}(x) \;=\; 0.$$

für alle $x \in K^\times$.

(5) Gemäß Induktionsvoraussetzung folgt

$$\alpha_j[\sigma_j(a) - \sigma_k(a)] \;=\; 0 \qquad \text{für alle } j \in \{1, \ldots, k-1\}.$$

Mit Schritt (2) folgt $\alpha_1 = 0$.

(6) Die Gleichung $(*)$ lautet nun

$$\alpha_2\sigma_2 + \ldots + \alpha_k\sigma_k \;=\; 0.$$

Gemäß Induktionsvoraussetzung sind auch

$$\alpha_2 \;=\; \alpha_3 \;=\; \ldots \;=\; \alpha_k \;=\; 0.$$

12.2 Zyklische Erweiterungen

12.2.1 Formel für reine Polynome

Es seien $n \in \mathbb{N}$ und M ein Körper mit $\operatorname{char} M \not| n$.

Enthält der Körper M eine primitive n-te Einheitswurzel, so gilt in $M[X,Y]$ die Formel

$$X^n - Y^n \;=\; (X-Y)\cdot(X-\zeta Y)\cdot\ldots\cdot(X-\zeta^{n-1}Y).$$

12.2.2 Beweis

Als Elemente in $(M[Y])[X]$ haben die Polynome links und rechts die n verschiedenen Nullstellen

$$Y,\ \zeta Y,\ \zeta^2 Y,\ldots,\zeta^{n-1}Y.$$

und stimmen deshalb überein.

12.2.3 Satz: Zyklische Erweiterungen

Es sei $n \in \mathbb{N}$. Wir betrachten einen Körper K mit $\operatorname{char} K = 0$ und die Körpererweiterung $M = K(\zeta)$ mit einer primitiven n-ten Einheitswurzel ζ.

Die folgenden Aussagen über eine Körpererweiterung $L : M$ sind äquivalent.

(A) $L : M$ ist eine *zyklische* Körpererweiterung mit Grad n, d.h. sie ist galoissch mit einem Gruppenmonomorphismus $\operatorname{Aut}(L:M) \cong \mathbb{Z}/n\mathbb{Z}$.

(B) Es gibt ein $a \in L$ mit den Eigenschaften

$$\begin{aligned} &a^n \in M,\\ &X^n - a^n \in M[X] \quad \text{ist das Minimalpolynom von } a \text{ über } M,\\ &L \;=\; M(a). \end{aligned}$$

(C) Es gibt ein $a \in L$ so, dass L Zerfällungskörper des reinen irreduziblen Polynoms $X^n - a^n$ ist. Es gilt dabei

$$X^n - a^n \;=\; (X-a)\cdot(X-\zeta a)\cdot\ldots\cdot(X-\zeta^{n-1}a).$$

12.2.4 Beweis

(A) $\Rightarrow$ (B).

(1) Gemäß der Voraussetzung existiert ein erzeugendes Element $\sigma \in \operatorname{Aut}(L:M)$ der Ordnung n, also ist

$$\operatorname{Aut}(L:M) \;=\; \{\mathrm{id}_M, \sigma, \ldots, \sigma^{n-1}\}.$$

(2) Wir betrachten die Linearkombination von Abbildungen in $\operatorname{Abb}(L^\times, L)$

$$\tau \;:=\; 1\cdot \mathrm{id}_{L^\times} + \zeta^{-1}\sigma + \zeta^{-2}\sigma^2 + \ldots + \zeta^{-(n-1)}\sigma^{n-1}.$$

Nach dem Lemma von Artin 12.1.3 kann dies nicht die Nullabbildung sein, es gibt also ein $c \in L^\times$ mit

$$a \;:=\; \tau(c) \;=\; c + \zeta^{-1}\sigma(c) + \zeta^{-2}\sigma^2(c) + \ldots + \zeta^{-(n-1)}\sigma^{n-1}(c) \quad \in L^\times.$$

(3) Wir wenden auf diese Gleichung die Abbildung $\zeta^{-1}\sigma$ an und erhalten, da $\zeta^n = 1$ und $\sigma^n = \mathrm{id}_L$

$$\zeta^{-1}\sigma(a) \;=\; \zeta^{-1}\sigma(c) + \zeta^{-2}\sigma^2(c) + \ldots + \zeta^{-(n-1)}\sigma^{n-1}(c) + \underbrace{\zeta^{-n}\sigma^n(c)}_{=c} \;=\; a,$$

umgekehrt

$$\sigma(a) \;=\; \zeta \cdot a.$$

(4) Daraus folgt

$$\sigma(a^n) \;=\; \sigma(a)^n \;=\; (\zeta \cdot a)^n \;=\; a^n, \qquad \text{also } a^n \in \Phi(\mathrm{Aut}(L:M)) \;=\; M.$$

(5) Ist $\mu \in M[X]$ das Minimalpolynom von a, so gilt für alle $j \in \{0, \ldots, n-1\}$

$$0 \;=\; \mu(\sigma^j(a)) \;=\; \mu(\zeta^j \cdot a),$$

es hat μ also mindestens n verschiedene Nullstellen, damit $\deg \mu \geq n$.

(6) Wegen $a \in L$ ist $M(a) \subseteq L$ und aufgrund von

$$[M(a):M] \;=\; \deg \mu \;\geq\; n \;=\; [L:M]$$

folgt $L = M(a)$.

(B) $\Rightarrow$ (C). Mit der Formel für reine Polynome 12.2.1 folgt

$$X^n - a^n \;=\; (X-a)\cdot(X-\zeta a)\cdot \ldots \cdot (X - \zeta^{n-1}a).$$

Also zerfällt das reine Polynom $X^n - a^n$ in L. Da $X^n - a^n$ irreduzibel in $M[X]$ ist, ist $L = M(a)$ Zerfällungskörper.

(C) $\Rightarrow$ (A). L enthält die n verschiedenen Nullstellen $\zeta^j a$, $j \in \{0, \ldots, n-1\}$. Der M-Automorphismus

$$\sigma : \left\{ \begin{array}{ccc} L & \to & L \\ a & \mapsto & \zeta \cdot a \end{array} \right.$$

erzeugt also die Automorphismengruppe $\mathrm{Aut}(L:M)$ mit n Elementen.

12.3 Zerfällungskörper von reinen Polynomen

12.3.1 Definition: Reines Polynom

Ist K ein Körper (oder allgemeiner ein uk Ring), so heißt ein Polynom der Form

$$X^n - b \qquad \text{mit } b \in K$$

ein *reines Polynom (über K mit Grad n und konstantem Glied b).*

12.3.2 Satz: Zerfällungskörper eines reinen Polynoms

Es sei K ein Körper mit $\operatorname{char} K = 0$ und $f(X) = X^n - b$ ein (nicht notwendig irreduzibles) reines Polynom über K.

Dazu definieren wir die beiden Körpererweiterungen

$M := K(\zeta)$, wobei ζ eine primitive n-te Einheitswurzel ist.

$L := \operatorname{Zerf}(X^n - b, K)$.

Es sei $a \in L$ eine Nullstelle von $X^n - b$, also $a^n = b$.

Dann gilt

(i) M ist ein Zwischenkörper von $L : K$.

(ii) Es gilt in $L[X]$

$$X^n - b \;=\; (X - a) \cdot (X - \zeta a) \cdot \ldots \cdot (X - \zeta^{n-1} a).$$

Insbesondere ist $L = K(\zeta, a) = M(a)$.

(iii) Es gibt $m, \ell \in \mathbb{N}$ mit $m \cdot \ell = n$ so, dass die drei folgenden Aussagen äquivalent sind.

(A) Es ist $\operatorname{Aut}(L : M) \cong \mathbb{Z}/m\mathbb{Z}$ zyklisch.

(B) $L \;=\; M(a)$ ist Zerfällungskörper des irreduziblen Polynoms $X^m - a^m \in M[X]$.

(C) Das reine Polynom $f(X) = X^n - b$ zerfällt in $M[X]$ wie folgt in ℓ irreduzible Faktoren mit Grad m

$$X^n - b \;=\; (X^m - a^m) \cdot (X^m - \zeta^m a^m) \cdot (X^m - \zeta^{2m} a^m) \cdot \ldots \cdot (X^m - \zeta^{(\ell-1)m} a^m).$$

Die irreduziblen Faktoren wiederum zerfallen wie folgt in $L[X]$.

$$X^m - \zeta^{jm} a^m \;=\; (X - \zeta^j a) \cdot (X - \zeta^{j+\ell} a) \cdot \ldots \cdot (X - \zeta^{j+(m-1)\ell} a).$$

(x) Beachte, dass $\operatorname{Aut}(L : K)$ i.a. nicht einmal abelsch ist, wie das Beispiel des reinen Polynoms $X^3 - 2$ aus Kapitel 9.4 zeigt.

12.3.3 Beispiel

Man mache sich die Aussage (iii) klar an dem folgenden Beispiel eines reinen Polynoms

$$X^6 - 125 \quad \in \quad \mathbb{Q}[X].$$

Ist $\zeta \in \mathbb{C}$ eine primitive 6-te Einheitswurzel, so gilt

$$\begin{aligned} & X^6 - 125 \\ = \; & (X^2 - 5) \cdot (X^2 - \zeta^2 5) \cdot (X^2 - \zeta^4 5) \\ = \; & [(X - \sqrt{5})(X - \zeta^3\sqrt{5})] \cdot [(X - \zeta\sqrt{5})(X - \zeta^4\sqrt{5})] \cdot [(X - \zeta^2\sqrt{5})(X - \zeta^5\sqrt{5})], \end{aligned}$$

Die zweite Zeile bringt zum Ausdruck, dass das Polynom reduzibel über $M = \mathbb{Q}(\zeta)$ ist.

Die dritte Zeile gibt die vollständige Zerfällung in $L = M(\sqrt{5}) = \mathbb{Q}(\zeta, \sqrt{5})$ an.

Es ist $[L : M] = 2$ und $[M : \mathbb{Q}] = 2$, also $[L : \mathbb{Q}] = 4$.

12.3.4 Beweis

(i) O.B.d.A. ist $n \geq 2$. Gemäß der Implikation (B) $\Rightarrow$ (A) aus Satz 7.2.1 hat das reine Polynom $X^n - b$ die paarweise verschiedenen Nullstellen $a_1, \ldots, a_n \in L^\times$. Es sind dann auch die n Elemente

$$\tfrac{a_1}{a_1},\ \tfrac{a_2}{a_1},\ \ldots\ \tfrac{a_n}{a_1}$$

paarweise verschieden und n-te Einheitswurzeln, da

$$(\tfrac{a_j}{a_1})^n \quad = \quad \tfrac{a_j^n}{a_1^n} \quad = \quad \tfrac{b}{b} \quad = \quad 1.$$

(ii) Als Zerfällungskörper von $X^n - b$ enthält L eine Nullstelle a. Die Zerlegung in lineare Faktoren ist durch die Formel 12.2.1 gegeben.

(iii)

(A) $\Rightarrow$ (B). Ist g das Minimalpolynom von a über M, so gilt $\deg g = m$.

Wegen $g \mid (X^n - a^n)$ und (ii) muss g die Form

$$g(X) \quad = \quad (X - a) \cdot (X - \zeta^{j_2} a) \cdot \ldots \cdot (X - \zeta^{j_m} a)$$

haben. Das konstante Glied ist dann

$$g_0 \quad = \quad (-1)^m \cdot \zeta^{j_2 + \ldots + j_m} \cdot a^m \quad \in M,$$

also $a^m \in M$. Dann ist aber $g(X) = X^m - a^m \in M[X]$ das Minimalpolynom und es gilt $L = \mathrm{Zerf}(g, M)$.

(B) $\Rightarrow$ (C). ζ^m ist eine primitive ℓ-te Einheitswurzel. Deshalb gilt mit der Formel 12.2.1

$$\begin{aligned} X^n - b \quad &= \quad (X^m)^\ell - (a^m)^\ell \\ &= \quad (X^m - a^m) \cdot (X^m - \zeta^m a^m) \cdot (X^m - \zeta^{2m} a^m) \cdot \ldots \cdot (X^m - \zeta^{(\ell-1)m} a^m). \end{aligned}$$

Für $j \in \{0, \ldots, \ell - 1\}$ gilt

$$X^m - \zeta^{jm} a^m \quad = \quad \zeta^m \cdot ((\tfrac{X}{\zeta})^m - a^m),$$

also sind alle Faktoren irreduzibel.

ζ^ℓ ist eine primitive m-te Einheitswurzel. Deshalb gilt mit der Formel 12.2.1

$$X^m - \zeta^{jm} a^m \;=\; X^m - (\zeta^j a)^m \;=\; (X - \zeta^j a) \cdot (X - \zeta^{j+\ell} a) \cdot \ldots \cdot (X - \zeta^{j+(m-1)\ell} a).$$

(C) $\Rightarrow$ (A). Gemäß der Aussage (C) ist

$$L \;=\; \operatorname{Zerf}(X^n - b, M) \;=\; \operatorname{Zerf}(X^m - a^m, M).$$

Das Polynom $X^m - a^m \in M[X]$ ist ein reines irreduzibles Polynom. Die Implikation (C) $\Rightarrow$ (A) aus Satz 12.2.3 liefert die aktuelle Implikation (C) $\Rightarrow$ (A).

12.3.5 Satz: Zerfällungskörper eines irreduziblen reinen Polynoms

Es sei K ein Körper mit $\operatorname{char} K = 0$ und $f(X) = X^n - b$ ein irreduzibles reines Polynom über K.

Dazu definieren wir die beiden Körpererweiterungen

$M := K(\zeta)$, wobei ζ eine primitive n-te Einheitswurzel ist.

$L := \operatorname{Zerf}(X^n - b, K)$.

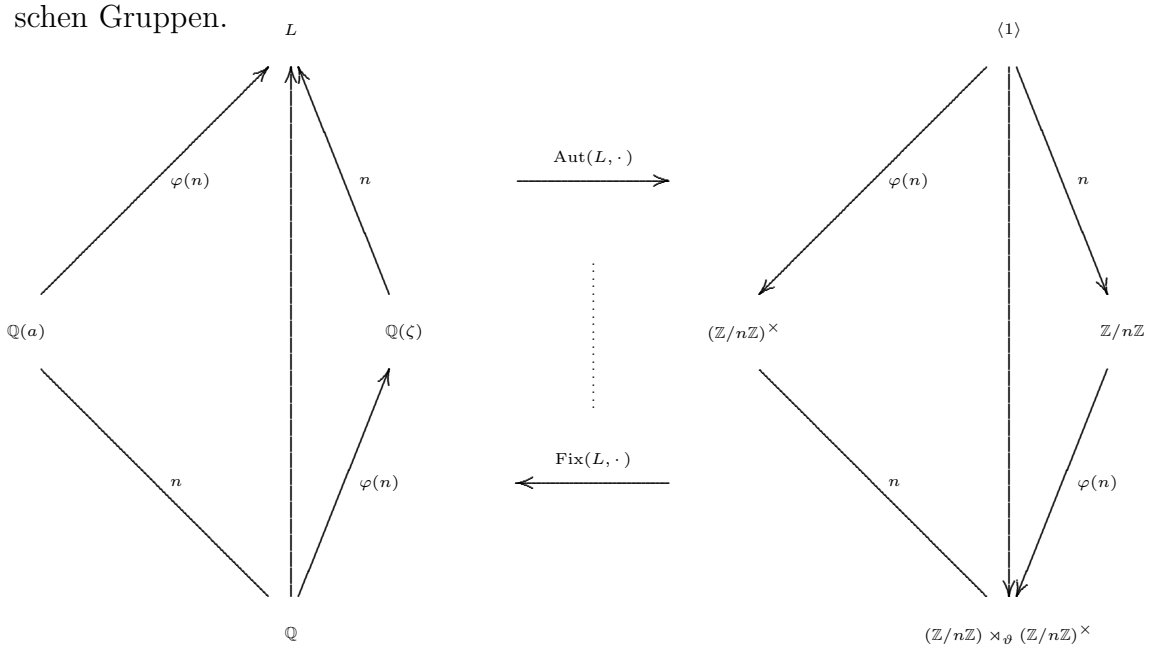
Dann gilt

(i) Es gibt einen Gruppenisomorphismus $\operatorname{Aut}(L : M) \cong \mathbb{Z}/n\mathbb{Z}$.

(ii) Ist $K = \mathbb{Q}$ und $X^n - b$ irreduzibel, so existiert ein Gruppenisomorphismus

$$\operatorname{Aut}(L : \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z}) \rtimes_\vartheta (\mathbb{Z}/n\mathbb{Z})^\times,$$

wobei innerhalb des semidirekten Produkts die Operation von ϑ gegeben ist durch den kanonischen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$. Vgl. Theorie der zyklischen Gruppen.



Pfeil bedeutet: galoissche Erweiterung
Zahl bedeutet: Grad der Erweiterung

Pfeil bedeutet: Normalteiler
Zahl bedeutet: Index der Untergruppe

12.3.6 Beweis

(i) Das ist die Implikation (C) $\Rightarrow$ (A) aus Satz 12.2.3.

(ii) Sind $\sigma, \widetilde{\sigma} \in \mathrm{Aut}(L:\mathbb{Q})$, so gibt es $\ell, \widetilde{\ell} \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $j, \widetilde{j} \in \mathbb{Z}/n\mathbb{Z}$ so, dass

$$\sigma : \left\{ \begin{array}{lcl} L & \to & L \\ \zeta & \mapsto & \zeta^{\ell} \\ a & \mapsto & \zeta^{j} \cdot a \end{array} \right. \qquad \widetilde{\sigma} : \left\{ \begin{array}{lcl} L & \to & L \\ \zeta & \mapsto & \zeta^{\widetilde{\ell}} \\ a & \mapsto & \zeta^{\widetilde{j}} \cdot a \end{array} \right.$$

Es gilt dann

$$\begin{aligned} (\widetilde{\sigma} \circ \sigma)(\zeta) &= \widetilde{\sigma}(\zeta^{\ell}) = (\zeta^{\ell})^{\widetilde{\ell}} = \zeta^{\widetilde{\ell} \cdot \ell} \\ (\widetilde{\sigma} \circ \sigma)(a) &= \widetilde{\sigma}(\zeta^{j} \cdot a) = \widetilde{\sigma}(\zeta^{j}) \cdot \widetilde{\sigma}(\cdot a) = (\zeta^{j})^{\widetilde{\ell}} \cdot \zeta^{\widetilde{j}} \cdot a = \zeta^{\widetilde{\ell} \cdot j + \widetilde{j}} \cdot a. \end{aligned}$$

Zu der Verknüpfung von σ und $\widetilde{\sigma}$ korrespondiert also die Verknüpfung

$$\left\{ \begin{array}{lcl} [(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^\times]^2, & \to & (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^\times \\ \qquad ((\widetilde{j}, \widetilde{\ell}), (j, \ell)) & \mapsto & (\widetilde{\ell} \cdot j + \widetilde{j}, \widetilde{\ell} \cdot \ell) = (\widetilde{j}, \widetilde{\ell}) *_\vartheta (j, \ell), \end{array} \right.$$

wobei ϑ die Aktion von $(\mathbb{Z}/n\mathbb{Z})^\times$ auf $\mathbb{Z}/n\mathbb{Z}$ mit $\vartheta_{\widetilde{\ell}}(j) = \widetilde{\ell} \cdot j$ bedeutet.

12.4 Radikalerweiterungen

12.4.1 Definition: Radikalerweiterung

Eine Körpererweiterung $L : K$ heißt *Radikalerweiterung*, wenn es eine endliche Folge $M_0, M_1, \ldots, M_\ell$ von Zwischenkörpern gibt so, dass

$$K \;=\; M_0 \subseteq M_1 \subseteq \ldots \subseteq M_\ell \;=\; L$$

und

$$M_j \;=\; M_{j-1}(a_j), \quad \text{wobei} \quad a_j^{n_j} \in M_{j-1}.$$

Der Zwischenkörper M_j entsteht also aus seinem Vorgänger-Zwischenkörper M_{j-1} dadurch, dass die Nullstelle a_j eines reinen Polynoms

$$X^{n_j} - \underbrace{a_j^{n_j}}_{\in M_{j-1}} \;\in\; M_{j-1}[X]$$

adjungiert wird. Anders ausgedrückt, es wird die n_j-te Wurzel eines Elements aus M_{j-1} adjungiert, um M_j zu erhalten.

12.4.2 Bemerkung

Es ist unmittelbar klar aus der Definition, dass die Eigenschaft „Radikalerweiterung" transitiv ist.

12.4.3 Satz: Einheitswurzeln zuerst

Es sei eine Radikalerweiterung

$$K \;=\; M_0 \subseteq M_1 \subseteq \ldots \subseteq M_\ell \;=\; L$$

mit $\operatorname{char}(K) = 0$ gegeben. Dazu existiert eine modifizierte Radikalerweiterung gemäß der unteren Zeile in dem folgenden Diagramm

$$\begin{array}{ccccccccccc}
K & = & M_0 & \subseteq & M_1 & \subseteq & \ldots & \subseteq & M_{\ell-1} & \subseteq & M_\ell & = & L \\
\cap\!| & & \cap\!| & & \cap\!| & & & & \cap\!| & & \cap\!| & & \cap\!| \\
\widetilde{K} & = & \widetilde{M}_0 & \subseteq & \widetilde{M}_1 & \subseteq & \ldots & \subseteq & \widetilde{M}_{\ell-1} & \subseteq & \widetilde{M}_\ell & = & \widetilde{L}
\end{array}$$

mit folgenden Eigenschaften

(A) Es ist $\widetilde{M}_0 = M_0(\zeta)$ mit einer primitiven Einheitswurzel ζ.

(B) Für alle $j \in \{1, \ldots, \ell\}$ ist $\widetilde{M}_j : \widetilde{M}_{j-1}$ eine galoissche Körpererweiterung mit zyklischer Automorphismengruppe $\operatorname{Aut}(\widetilde{M}_j : \widetilde{M}_{j-1})$.

(C) Für alle $j \in \{0, \ldots, \ell\}$ ist $\widetilde{M}_j : K$ eine galoissche Radikalerweiterung.

Insbesondere ist $\widetilde{L} : K$ eine galoissche Radikalerweiterung.

12.4.4 Beweis

(1) Wir definieren

$$n \;:=\; n_1 \cdot \ldots \cdot n_\ell,$$

wobei die Faktoren n_j der originalen Radikalerweiterung gemäß Definition 12.4.1 entnommen sind.

Es gibt dann eine primitive n-te Einheitswurzel ζ so, dass

$$\widetilde{M}_0 \;:=\; M_0(\zeta) \;=\; \mathrm{Zerf}(X^n-1, M_0),$$

also (A). $\widetilde{M}_0 : K$ ist Radikalerweiterung.

(2) Wir führen nun Induktion über die Länge $j = 0, \ldots, \ell$ der originalen Radikalerweiterung durch.

Für $j = 0$ ist $\widetilde{M}_0 : K = M_0(\zeta) : K$ eine galoissche Radikalerweiterung.

(3) Die Aussage sei jetzt für eine Radikalerweiterung der Länge $j-1$ bereits gezeigt.

Wir betrachten das Diagramm der bereits erstellen modifizierten Radikalerweiterung Es muss in dem Diagramm

$$\begin{array}{ccccccccc}
K & = & M_0 & \subseteq & M_1 & \subseteq & \ldots & \subseteq & M_{j-1} & \subseteq & M_j \\
\cap| & & \cap| & & \cap| & & & & \cap| & & \cap| \\
\widetilde{K} & = & \widetilde{M}_0 & \subseteq & \widetilde{M}_1 & \subseteq & \ldots & \subseteq & \widetilde{M}_{j-1} & \subseteq & \widetilde{M}_j
\end{array}$$

der Körper $\widetilde{M}_j$ mit den angeforderten Eigenschaften konstruiert werden.

(4) Nach Induktionsvoraussetzung ist $\widetilde{M}_{j-1} : K$ galoissch, also Zerfällungskörper eines Polynoms $f_{j-1}(X) \in K[X]$.

(5) Nach Voraussetzung des Satzes ist $M_j = M_{j-1}(a_j)$ mit $a_j^{n_j} \in M_{j-1}$. Wir definieren das Polynom

$$g_{j-1}(X) \;:=\; \prod_{\sigma \in \mathrm{Aut}(\widetilde{M}_{j-1}, K)} (X^{n_j} - \sigma(a_j^{n_j})) \quad \in \widetilde{M}_{j-1}[X].$$

Das Polynom ist invariant unter der Operation von $\mathrm{Aut}(\widetilde{M}_{j-1}, K)$ auf den Koeffizienten, also gilt

$$g_{j-1}(X) \;\in\; K[X].$$

(6) Wir definieren nun $\widetilde{M}_j$ als Zerfällungskörper des Polynoms

$$f_j(X) \;:=\; f_{j-1}(X) \cdot g_{j-1}(X) \in K[X]$$

und überlegen die angeforderten Eigenschaften.

(7) Es ist zunächst

$$\widetilde{M}_{j-1} \;\subseteq\; \widetilde{M}_j,$$

da $f_{j-1} \mid f_j$.

(8) Weiter ist nach Induktionsvoraussetzung

$$M_{j-1} \subseteq \widetilde{M}_{j-1} \subseteq \widetilde{M}_j$$

und $a_j \in \widetilde{M}_j$, da

$$g_{j-1}(a_j) = 0 \qquad \text{und} \qquad g_{j-1} \mid f_j.$$

Daraus folgt

$$M_j = M_{j-1}(a_j) \subseteq \widetilde{M}_j.$$

(9) Der Definition von $\widetilde{M}_j$ als Zerfällungskörper von $f_{j-1} \cdot g_{j-1}$ ist zu entnehmen, dass $\widetilde{M}_j = \widetilde{M}_{j-1}(a_j)$. Also $\widetilde{M}_j : \widetilde{M}_{j-1}$ eine Radikalerweiterung. Somit ist auch $\widetilde{M}_j : K$ eine Radikalerweiterung.

(10) Als Zerfällungskörper-Erweiterung eines Polynoms aus $K[X]$ ist $\widetilde{M}_j : K$ galoissch. Damit ist (C) gezeigt.

(11) Schließlich ist $\widetilde{M}_j = \widetilde{M}_{j-1}(a_j)$ mit $a_j^{n_j} \in \widetilde{M}_{j-1}$. Wegen $n_j \mid n$ gilt auch $a_j^n \in \widetilde{M}_{j-1}$.

Also enthält $\widetilde{M}_{j-1}$ alle n_j-ten Einheitswurzeln. Es folgt mit Satz **??**(iii), dass $\widetilde{M}_j : \widetilde{M}_{j-1}$ galoissch ist mit zyklischer Automorphismengruppe.

12.4.5 Hauptsatz über Auflösbarkeit

Es seien K ein Körper mit $\operatorname{char} K = 0$ und $f \in K[X]$ ein Polynom. Es sei L der Zerfällungskörper f über K. Dann sind die folgenden beiden Aussagen äquivalent.

(A) Die Automorphismengruppe $\operatorname{Aut}(L : K)$ ist auflösbar.

(B) f ist durch Radikale lösbar, d.h. es existiert eine Radikalerweiterung $\widehat{L} : K$ mit $L \subseteq \widehat{L}$.

12.4.6 Beweis

(A) $\Rightarrow$ (B).

(1) Nach Voraussetzung gibt es eine Normalreihe

$$\operatorname{Aut}(L : K) = N_0 \supseteq \ldots \supseteq N_\ell = \operatorname{Aut}(L : L) = \{\mathrm{id}_L\},$$

deren Faktoren N_{j-1}/N_j (nicht nur abelsch, sondern sogar) zyklisch sind. Vgl. den diesbezüglichen Satz in ALG1.

(2) Gemäß Hauptsatz der Galoistheorie korrespondiert dazu eine Körperkette

$$K = M_0 \subseteq \ldots \subseteq M_\ell = L,$$

mit $M_j := \Phi(L : N_j)$ so, dass $M_j : M_{j-1}$ galoissch ist

$$\operatorname{Aut}(M_j : M_{j-1}) \cong N_{j-1}/N_j \qquad \text{(zyklisch)}.$$

(3) Mit $n := \operatorname{ord}(\operatorname{Aut}(L : K))$ sei ζ eine n-te primitive Einheitswurzel. Gemäß Satz 12.1.1 ist $M_j(\zeta) : M_{j-1}(\zeta)$ galoissch mit

$$\operatorname{Aut}(M_j(\zeta) : M_{j-1}(\zeta)) \hookrightarrow \operatorname{Aut}(M_j : M_{j-1}) \qquad \text{(zyklisch)}.$$

(4) Gemäß Satz 12.2.3 gibt es ein $a_j \in M_j(\zeta)$ und ein $n_j \in \mathbb{N}$ mit $n_j \mid n$ so, dass

$$a_j^{n_j} \in M_{j-1}(\zeta) \qquad \text{und} \qquad M_j \;=\; M_{j-1}(a_j).$$

(5) Wir erhalten eine Kette von Körpererweiterungen

$$K \;\subseteq\; K(\zeta) \;=\; M_0(\zeta)\ldots \;\subseteq\; M_\ell(\zeta) \;=\; L(\zeta),$$

Wegen $\zeta^n = 1$ ist $K(\zeta) : K$ eine Radikalerweiterung. Da alle anderen Erweiterungen auch Radikalerweiterungen sind, ist insgesamt $L(\zeta) : K$ eine Radikalerweiterung. Mit $\widehat{L} := L(\zeta)$ folgt die Behauptung (B).

(B) $\Rightarrow$ (A).

(1) Gemäß Voraussetzung sei zu dem Zerfällungskörper L eine Radikalerweiterung $\widehat{L} : K$ mit $L \subseteq \widehat{L}$ gegeben. Wir betrachten dazu die modifizierte Radikalerweiterung $\widetilde{L} : K$ gemäß Satz 12.4.3

$$\begin{array}{ccccccccccc}
K & = & M_0 & \subseteq & M_1 & \subseteq & \ldots & \subseteq & M_{\ell-1} & \subseteq & M_\ell & = & \widehat{L} \\
\cap\!| & & \cap\!| & & \cap\!| & & & & \cap\!| & & \cap\!| & & \cap\!| \\
\widetilde{K} & = & \widetilde{M_0} & \subseteq & \widetilde{M_1} & \subseteq & \ldots & \subseteq & \widetilde{M_{\ell-1}} & \subseteq & \widetilde{M_\ell} & = & \widetilde{L}.
\end{array}$$

(2) (3) Wir zeigen nun, dass die Faktoren

$$\mathrm{Aut}(\widetilde{L} : \widetilde{M_{j-1}})/\,\mathrm{Aut}(\widetilde{L} : \widetilde{M_j}) \qquad \text{und} \qquad \mathrm{Aut}(\widetilde{L} : K)/\,\mathrm{Aut}(\widetilde{L} : \widetilde{K})$$

in dieser Normalreihe abelsch sind.

(3a) Aufgrund des Isomorphismus aus dem Hauptsatz der Galoistheorie

$$\mathrm{Aut}(\widetilde{L} : \widetilde{M_{j-1}})/\,\mathrm{Aut}(\widetilde{L} : \widetilde{M_j}) \;\cong\; \mathrm{Aut}(\widetilde{M_j} : \widetilde{M_{j-1}}), \quad j \in \{1, \ldots, n\}$$

und Aussage (B) in Satz 12.4.3 ist diese Faktorgruppe zyklisch.

(3b) Die Faktorgruppe

$$\mathrm{Aut}(\widetilde{L} : K)/\,\mathrm{Aut}(\widetilde{L} : \widetilde{K}) \;\cong\; \mathrm{Aut}(\widetilde{K} : K)$$

ist gemäß Satz 10.4.1 (iii) abelsch.

(4) Gemäß der Definition von ,,Auflösbarkeit einer Gruppe" auflösbar ist $\mathrm{Aut}(\widetilde{L} : K)$

(5) Es ist $L : K$ als Zerfällungskörper galoissch. Die Automorphismengruppe

$$\mathrm{Aut}(L : K) \;\cong\; \mathrm{Aut}(\widetilde{L} : K)/\,\mathrm{Aut}(\widetilde{L} : L)$$

ist als Faktorgruppe einer auflösbaren Gruppe dann selbst auflösbar.

12.5 Auflösbarkeit von Polynomen

12.5.1 Satz: Untergruppe der symmetrischen Gruppe

Es sei p eine Primzahl und $U \subseteq \mathcal{S}_p$ eine Untergruppe. Gilt für U

$p \mid \operatorname{ord}(U)$ und

U enthält eine Transposition,

so ist $U = \mathcal{S}_p$.

12.5.2 Beweis

(1) Gemäß Satz von Cauchy enthält U eine Element σ der Ordnung p. Die Bahn von 1 unter der von σ erzeugten Untergruppe muss als Ordnung ein Teiler von p sein, damit kann sie nur gleich p sein. Damit ist σ ein p-Zyklus. O.B.d.A. ist $\sigma = \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix}$.

(2) Wir können weiter (nach evtl. zyklischer Permutation der Elemente) annehmen, dass die Transposition gleich $\begin{pmatrix} 1 & 2 \end{pmatrix}$ ist.

Dann enthält U auch alle Transpositionen der Form

$$\begin{pmatrix} j-1 & j \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix}^{j-1} \circ \tau \circ \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix}^{-(j-1)}, \qquad j > 1$$

und dann (rekursiv)

$$\begin{pmatrix} 1 & j \end{pmatrix} = \begin{pmatrix} 1 & j-1 \end{pmatrix} \circ \begin{pmatrix} j-1 & j \end{pmatrix} \circ \begin{pmatrix} 1 & j-1 \end{pmatrix},$$

schließlich

$$\begin{pmatrix} j & k \end{pmatrix} = \begin{pmatrix} 1 & j \end{pmatrix} \circ \begin{pmatrix} 1 & k \end{pmatrix} \circ \begin{pmatrix} 1 & j \end{pmatrix}.$$

U enthält also alle Transpositionen und ist, da jede Permutation als Produkt von Transpositionen dargestellt werden kann, gleich $\mathcal{S}_p$.

12.5.3 Satz: Polynom nicht auflösbar

Es sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit $\deg f = 5$ und Zerfällungskörper $L \subseteq \mathbb{C}$.

Hat f genau drei reelle (und damit zwei echt komplexe) Nullstellen, so gilt

$$\operatorname{Aut}(L : \mathbb{Q}) \cong \mathcal{S}_5.$$

12.5.4 Beweis

Ist $a \in L$ eine Nullstelle von f, so gilt aufgrund der Irreduzibilität von f

$$[\mathbb{Q}(a) : \mathbb{Q}] = 5$$

und damit

$$\operatorname{ord}(\operatorname{Aut}(L : \mathbb{Q})) = [L : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}] = 5 \cdot [L : \mathbb{Q}(a)].$$

Die Konjugiert-Komplex-Abbildung κ ist ein Element von $\operatorname{Aut}(L : \mathbb{Q})$ mit $\operatorname{ord}(\kappa) = 2$.

Gemäß Satz 12.5.1 ist $\operatorname{Aut}(L : \mathbb{Q}) \cong \mathcal{S}_5$.

12.5.5 Beispiel

Wir betrachten das Polynom

$$f(X) \;=\; X^5 - 4X + 2 \;=\; X \cdot (X^4 - 4) + 2$$

Es ist gemäß Eisenstein irreduzibel. Die Ableitung $f'(X) = 5X^4 - 4$ hat die beiden Nullstellen $-\sqrt{\frac{4}{5}}$ und $+\sqrt{\frac{4}{5}}$. An diesen beiden Stellen ist

$$\begin{aligned} f(-\sqrt{\tfrac{4}{5}}) &= -\sqrt{\tfrac{4}{5}} \cdot (-\tfrac{84}{25}) + 2 > 0 \\ f(\sqrt{\tfrac{4}{5}}) &= \sqrt{\tfrac{4}{5}} \cdot (-\tfrac{84}{25}) + 2 < 0. \end{aligned}$$

Also hat f genau drei reelle Nullstellen.

Die fünf Nullstellen des Polynoms können also nicht — ausgehend von der Zahl $1 \in \mathbb{Q}$ — mit Hilfe von Grundrechenarten und Ziehen beliebiger Wurzeln dargestellt werden.