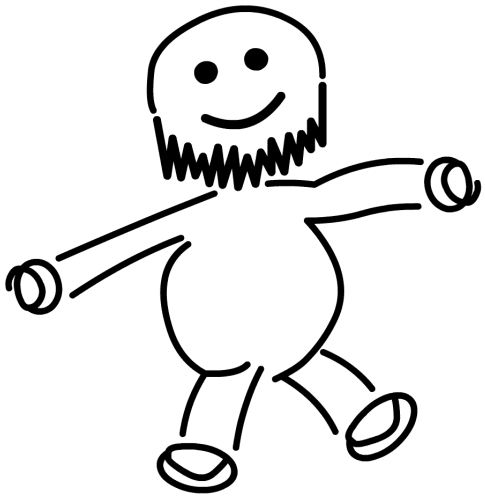
Algebra



Daniel Scholz im Winter 2004/2005

Überarbeitete Version vom 18. September 2005.

Inhaltsverzeichnis

1 Ringe und Ideale

1.1 Ringe und Ideale

1.1.1 Definition

Eine ***kommutativer Ring*** $(R, +, \cdot)$ mit 1 ist eine Menge R, auf der zwei Verknüpfungen (Addition und Multiplikation) definiert sind, so dass gilt:

(1) $(R, +)$ ist eine abelsche Gruppe

(2) Assoziativgesetz bezüglich Multiplikation

(3) Kommutativgesetz bezüglich Multiplikation

(4) Dristributivgesetze

(5) Es gibt ein Einselement 1, so dass für alle $a \in R$ gilt: $a \cdot 1 = 1 \cdot a = a$

1.1.2 Definition

Ein kommutativer Ring heißt ***Integritätsring***, wenn für alle $a, b \in R$ mit $a \cdot b = 0$ gilt:

$$a = 0 \quad \text{oder} \quad b = 0$$

1.1.3 Beispiele

(1) $R = (\mathbb{Z}, +, \cdot)$ ist ein Integritätsring.

(2) Der Polynomring $K[x]$ über dem Körper K ist ein Integritätsring.

(3) Jeder Körper ist auch ein Integritätsring.

(4) Seien R, S zwei kommutative Ringe mit 1. Dann ist auch

$$R \times S \;=\; \{(r, s) \mid r \in R,\; s \in S\}$$

ein Ring, aber kein Integritätsring, denn es gilt:

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

1.1.4 Satz 1

Ein endlicher Integritätsring ist sogar ein Körper.

1.1.5 Definition und Satz

Sei $(R, +, \cdot)$ ein kommutativer Ring mit 1.

$$\boxed{R^\times \;=\; \{a \in R \mid \exists\; b \in R \text{ mit } a \cdot b = b \cdot a = 1\}}$$

ist die Menge der so genannten ***Einheiten*** in R.

$(R^\times, \cdot)$ bildet eine abelsche Gruppe.

1.1.6 Beispiele

(1) Sei $R = (\mathbb{Z}, +, \cdot)$ der Ring der ganzen Zahlen. Dann gilt $R^\times = \{-1, 1\}$.

(2) Sei $R = K[x]$ der Polynomring über K. Dann gilt $R^\times = K^\times$.

(3) Sei $R = K$ ein Körper. Dann gilt $R^\times = K \setminus \{0\}$.

1.1.7 Definition

Sei $(R, +, \cdot)$ ein kommutativer Ring.

Ein ***Ideal*** $I \subset R$ ist eine Teilmene von R, für die gilt:

(1) $(I, +)$ ist eine Untergruppe von $(R, +)$

(2) $\forall\; r \in R,\; x \in I$ gilt: $r \cdot x = x \cdot r \in I$

1.1.8 Beispiele

(1) Sei $R = (\mathbb{Z}, +, \cdot)$ der Ring der ganzen Zahlen. Dann ist jedes Ideal I von der Form

$$I \;=\; n\mathbb{Z} \;=\; \{n \cdot x \mid x \in \mathbb{Z}\} \quad \text{mit} \quad n \in \mathbb{N}.$$

(2) Sei $R = K[x]$ der Polynomring über dem Körper K. Dann ist jedes Ideal I von der Form

$$I \;=\; f \cdot K[x] \;=\; \{f \cdot g \mid g \in K[x]\} \quad \text{mit} \quad f \in K[x].$$

(3) Sei

$$R \;=\; K[x, y] \;=\; \left\{ \sum_{i,j=0}^{n} a_{ij} x^i y^j \;\middle|\; n \in \mathbb{N},\; a_{ij} \in K \right\}$$

der Polynomring über dem Körper K mit zwei Unbekannten. Dann ist

$$I \;=\; x \cdot R + y \cdot R \;=\; \{x \cdot f(x, y) + y \cdot g(x, y) \mid f, g \in K[x, y]\}$$

ein Ideal in $K[x, y]$.

1.1.9 Definition

Seien R, S zwei kommutative Ringe.

Die Abbildung $\varphi : R \to S$ heißt ***Homomorphismus*** von Ringen, wenn für alle $a, b \in R$ gilt:

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$

(2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

1.1.10 Satz 2

Seien R, S zwei kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus.

Dann ist

$$\ker(\varphi) \;=\; \{r \in R \mid \varphi(r) = 0\}$$

ein Ideal in R.

1.1.11 Homomorphisatz

Sei R ein kommutativer Ring und sei $I \subset R$ ein Ideal.

Dann gilt:

(1) Die Gruppe $(R/I, +)$ der Nebenklassen

$$R/I \;=\; \{r + I \mid r \in R\}$$

bildet mit der Multiplikation

$$(a + I) \cdot (b + I) \;=\; a \cdot b + I$$

einen Ring.

(2) Die Abbildung

$$\begin{array}{rcl} p : R & \to & R/I \\ r & \mapsto & r + I \end{array}$$

ist ein Ringhomomorphismus mit $\ker(p) = I$.

(3) Sei S ein weiterer kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus mit $I \subset \ker(\varphi)$.

Dann gibt es genau einen Ringhomomorphismus $\overline{\varphi} : R/I \to S$, so dass das Diagramm

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ p \searrow & & \nearrow \overline{\varphi} \\ & \mathrm{R/I} & \end{array}$$

kommutiert.

Folgerung und Anwendung

Seien R und S zwei kommutative Ringe und sei $I \subset R$ ein Ideal von R.

Wenn nun gezeigt werden soll, dass R/I isomorph ist zu S, so muss eine Abbildung $\varphi : R \to S$ gefunden werden, für die gilt:

(1) φ ist ein Ringhomormorphismus.

(2) φ ist surjektiv.

(3) Es ist $\ker(\varphi) = I$.

Genau dann folgt aus dem Homomorphisatz, dass R/I isomorph ist zu S.

Dieser Satz gilt des Weiteren auch für Gruppen und Normalteiler statt Ringen und Idealen.

1.1.12 Definition

Sei R ein kommutativer Ring und sei $I \subset R$ ein Ideal von R.

I heißt ein ***maximales Ideal*** $:\Leftrightarrow$ I ist ein echtes Ideal von R und mit dieser Eigenschaft maximal.

I heißt ein ***Primideal*** $:\Leftrightarrow$ für alle $a, b \in R$ mit $a \cdot b \in I$ gilt $a \in I$ oder $b \in I$.

1.1.13 Beispiele

(1) Sei $R = (\mathbb{Z}, +, \cdot)$ der Ring der ganzen Zahlen und sei p eine Primzahl. Dann ist $I = p\mathbb{Z}$ ein Primideal.

(2) Sei $R = K[x, y]$ der Polynomring über dem Körper K. Dann ist

$$I \;=\; (x, y) \;=\; x \cdot R + y \cdot R \;=\; \{f \in K[x, y] \mid f(0, 0) = 0\}$$

ein maximales Ideal.

(3) Sei $R = K[x, y]$ der Polynomring über dem Körper K. Dann ist

$$I \;=\; x \cdot K[x, y]$$

ein Primideal, aber kein maximales Ideal.

1.1.14 Satz 3

Sei R ein kommutativer Ring und sei $I \subset R$ ein echtes Ideal von R.

Dann gilt:

(1) I ist ein maximales Ideal $\Leftrightarrow$ R/I ist ein Körper.

(2) I ist ein Primideal $\Leftrightarrow$ R/I ist ein Integritätsring.

Jedes maximale Ideal ist also auch ein Primideal.

1.1.15 Satz 4

Jeder kommutativer Ring mit 1 hat mindestens ein maximales Ideal.

1.2 Quotientenkörper

Es ist nun das Ziel, aus einem Integritätsring einen möglichst einfachen Körper zu definieren, den so genannten ***Quotientenkörper***. So wird zum Beispiel aus dem Ring der ganzen Zahlen der Körper $\mathbb{Q}$ erzeugt.

1.2.1 Definition des Quotientenkörper

Sei R ein beliebiger Integritätsring.

Betrachtet wird die Menge

$$\boxed{(R \times R)' \;=\; \{(a,b) \in R \times R \mid a,b \in R,\; b \neq 0\}.}$$

Seien $(a,b),(c,d) \in (R \times R)'$. Dann wird durch

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad ad = bc$$

eine Äquivalenzrelation in R beschrieben.

Betrachtet wird nun die Menge

$$M \;=\; (R \times R)'/\sim$$

und es wird für $\overline{(a,b)}, \overline{(c,d)} \in M$ definiert:

$$\begin{aligned}
\overline{(a,b)} + \overline{(c,d)} &:= \overline{(ad+bc, bd)} \\
\overline{(a,b)} \cdot \overline{(c,d)} &:= \overline{(ac, bd)} \\
\overline{0} &:= \overline{(0,1)} \\
\overline{1} &:= \overline{(1,1)} \\
\overline{(a,b)}^{-1} &:= \overline{(b,a)}
\end{aligned}$$

Durch diese Definitionen zeigt man leicht, dass

$$K \;=\; M \;=\; (R \times R)'/\sim$$

einen Körper bildet.

Quot$(R) = K$ heißt der ***Quotientenkörper*** von R.

Schreibweise

Sei $\overline{(a,b)} \in \text{Quot}(R)$. Dann schreibt man auch (mit $b^{-1} = \overline{(1,b)}$):

$$\overline{(a,b)} \;=\; a/b \;=\; \frac{a}{b} \;=\; a \cdot b^{-1}$$

1.2.2 Beispiele

(1) Sei $R = \mathbb{Z}$. Dann ist $\text{Quot}(R) = \mathbb{Q}$ der Quotientenkörper von R.

(2) Sei $R = K[x]$. Dann ist $\text{Quot}(R) = K(x)$ der Körper der rationalen Funktionene über K.

1.2.3 Satz 1

Sei R ein Integritätsring und sei $K = \text{Quot}(R)$.

Dann ist die Abbildung

$$\begin{array}{rcl} i : R & \to & K \\ a & \mapsto & (a,1) \end{array}$$

ein Ringhomomorphismus.

Sei weiter L ein Körper und $\varphi : R \to L$ ein injektiver Ringhomomorphismus.

Dann gibt es genau einen Ringhomomorphismus $\overline{\varphi} : K \to L$, so dass das Diagramm

$$\begin{array}{ccc} R & \overset{i}{\longrightarrow} & K \\ {\scriptstyle\varphi}\searrow & & \swarrow{\scriptstyle\overline{\varphi}} \\ & \text{L} & \end{array}$$

kommutiert.

1.3 Charakteristik eines Körpers

1.3.1 Definition der Charakteristik

Sei K ein beliebiger Körper.

Dann ist

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & K \\ n & \mapsto & n \cdot 1 \end{array}$$

ein Ringhomomorphismus.

$\ker(\varphi)$ ist demnach ein Ideal in $\mathbb{Z}$, also ist $\mathbb{Z}/\ker(\varphi)$ ein Integritätsring und somit ist $\ker(\varphi)$ ein Primideal in $\mathbb{Z}$ und von der Form $p\mathbb{Z}$.

Für die ***Charakteristik*** $\mathrm{char}(K)$ des Körpers K gilt nun:

$$\mathrm{char}(K) \;=\; \begin{cases} 0 & \text{falls} \quad \ker(\varphi) = \{0\} \\ p & \text{falls} \quad \ker(\varphi) = p\mathbb{Z} \end{cases}$$

1.3.2 Beispiele

(1) Für $K = \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl p gilt

$$\mathrm{char}(K) = p,$$

denn für $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ gilt $\ker(\varphi) = p\mathbb{Z}$.

(2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben die Charakteristik 0, denn $\varphi : \mathbb{Z} \to K$ ist für $K = \mathbb{Q}$ usw. injektiv, also gilt $\ker(\varphi) = \{0\}$.

1.3.3 Satz 1

Jeder Körper K mit $\mathrm{char}(K) = 0$ enthält den Körper $\mathbb{Q}$ (oder einen Körper, der zu $\mathbb{Q}$ isomorph ist).

Jeder Körper K mit $\mathrm{char}(K) > 0$ enthält den Körper $\mathbb{Z}/p\mathbb{Z}$ (oder einen Körper, der zu $\mathbb{Z}/p\mathbb{Z}$ isomorph ist).

1.4 Hauptidealringe

1.4.1 Definition

Sei R ein kommutativer Ring und sei $I \subset R$ ein Ideal von R.

I heißt ***Hauptideal***, wenn I von einem Element a erzeugt wird, d.h. es gilt

$$I \;=\; \{r \cdot a \mid r \in R\}$$

mit $a \in R$.

Schreibweise: $I = (a)$.

1.4.2 Definition

Ein Ring R heißt ***Hauptidealring***, wenn gilt:

(1) R ist ein Integritätsring.

(2) Jedes Ideal I von R ist ein Hauptideal.

1.4.3 Beispiele

(1) $(\mathbb{Z}, +, \cdot)$ ist ein Hauptidealring, denn jedes Ideal I ist von der Form

$$I \;=\; n\mathbb{Z} \;=\; (n).$$

(2) $K[x]$ ist ein Hauptidealring, denn jedes Ideal I ist von der Form

$$I \;=\; f \cdot K[x] \;=\; (f).$$

(3) Der Polynomring $K[x, y]$ ist ein Integritätsring, aber kein Hauptidealring. Es ist zum Beispiel

$$x \cdot K[x, y] + y \cdot K[x, y] \;=\; (x, y)$$

ein Ideal aber kein Hauptideal von $K[x, y]$.

1.4.4 Satz 1

Sei $R = (\mathbb{Z}, +, \cdot)$ der Ring der ganzen Zahlen und seien $a, b \in R$ mit $b \neq 0$.

Dann gibt es ganze Zahlen $r, s \in R$ mit

$$a \;=\; s \cdot b + r,$$

dabei $0 \leq r < b$.

1.4.5 Satz 2

Sei $R = K[x]$ der Polynomring über K und seien $a, b \in R$ mit $b \neq 0$.

Dann gibt es Polynome $r, s \in R$ mit

$$a \;=\; s \cdot b + r,$$

dabei $\text{grad}(r) < \text{grad}(b)$.

1.5 Teilbarkeit von Ringen

1.5.1 Satz 1

Sei $R = K[x]$ der Polynomring über K, sei $p(x) \in K[x]$ und sei $a \in K$ mit $p(a) = 0$.

Dann gibt es ein $p_1(x) \in K[x]$, so dass gilt:

$$p(x) \;=\; (x - a) \cdot p_1(x)$$

1.5.2 Definition

Sei R ein beliebiger Integritätsring, sei $p \in R$ mit $p \notin R^\times$.

Dann gilt:

(1) p heißt ***primes Element***, wenn $pR = (p)$ ein Primideal ist.

(2) p heißt ***irreduzibles Element***, wenn für jede Zerlegung der Form

$$p \;=\; a \cdot b$$

mit $a, b \in R$ gilt: $a \in R^\times$ oder $b \in R^\times$.

(3) Zwei irreduzieble Elemente p, q heißen ***assoziiert***, wenn es ein $r \in R^\times$ gibt, so dass gilt:

$$p \;=\; r \cdot q$$

Ist $a \in R$ ein primes Element, dann schreibt man auch: a ist prim.

1.5.3 Beispiele

(1) In $(\mathbb{Z}, +, \cdot)$ sind also

$$\{\pm 2,\, \pm 3,\, \pm 5,\, \pm 7,\, \pm 11,\, \pm 13,\, \pm 17,\, \pm 19, \ldots\}$$

primes Elemente.

(2) In $K[x]$ sind primes Elemente unzerlegbare Polynome.

(3) In $(\mathbb{Z}, +, \cdot)$ gilt $\mathbb{Z}^\times = \{-1, 1\}$.

Demnach sind alle Paare

$$\{-n, n\} \qquad \text{mit} \qquad n \in \mathbb{N}$$

assoziiert in $\mathbb{Z}$.

1.5.4 Satz 2

Jedes primes Element ist auch irreduzibel.

1.5.5 Satz von Euklid

Sei R ein Hauptidealring und seien $a, b \in R$.

Dann gilt:

(1) $p \in R$ ist irreduzibel $\Leftrightarrow$ p ist prim.

(2) $p \in R$ ist irreduzibel und p teilt $a \cdot b$ $\Leftrightarrow$ p teilt a oder p teilt b.

Für p teilt a schreibt man auch: $p \mid a$.

Folgerung

In den Hauptidealringen $(\mathbb{Z}, +, \cdot)$ und $K[x]$ sind irreduzible und primes Elemente dasselbe.

1.5.6 Satz 3

Sei R ein beliebiger Hauptidealring.

Dann besitzt jedes Element $x \in R$ eine (bis auf Permutationen und Assoziiertheit) eindeutig bestimmte Primfaktorzerlegung, d.h. jedes $x \in R$ läßt sich als Produkt von primes Elementen darstellen.

1.6 Faktorielle Ringe

1.6.1 Definition

Ein Integritätsring R heißt ein ***faktorieller Ring***, wenn jedes Element aus R eine eindeutige Zerlegung in irreduzible Elemente besitzt.

1.6.2 Beispiele

(1) Jeder Hauptidealring ist faktoriell.

(2) Sei R ein faktorieller Ring. Dann ist auch $R[x]$ faktoriell.

(3) Sei K ein Körper. Dann ist $K[x_1, .., x_n]$ faktoriell.

1.6.3 Satz 1

Sei R ein faktorieller Ring.

Dann ist jedes irreduzible Element $p \in R$ auch ein primes Element.

1.6.4 Definition

Sei R ein faktorieller Ring und seien $a_1, .., a_n \in R$.

Der ***größte gemeinsame Teiler*** von $a_1, .., a_n$ ist ein Element

$$\text{ggT}(a_1, .., a_n) \; = \; a \; \in \; R,$$

für das gilt:

(1) $a \mid a_i$ für $i = 1, .., n$ und

(2) a ist mit dieser Eigenschaft maximal (d.h.: $\forall\, a' \in R : \; a' \mid a_i \; \Rightarrow \; a' \mid a$).

Das ***kleinste gemeinsame Vielfache*** von $a_1, .., a_n$ ist ein Element

$$\text{kgV}(a_1, .., a_n) \; = \; b \; \in \; R,$$

für das gilt:

(1) $a_i \mid b$ für $i = 1, .., n$ und

(2) b ist mit dieser Eigenschaft minimal (d.h.: $\forall\, b' \in R : \; a_i \mid b' \; \Rightarrow \; b \mid b'$).

1.6.5 Satz 2

Der ggT und das kgV von n Elementen aus einem faktoriellen Ring existieren stets und sind eindeutig bestimmt.

1.6.6 Satz 3

Im Restklassenring der ganzen Zahlen gilt:

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \;\; = \;\; \{a + n\mathbb{Z} \mid a \in \mathbb{Z} \text{ mit } \text{ggT}(a, n) = 1\}$$

1.6.7 Satz 4

Sei p eine Primzahl.

Dann ist

$$(\mathbb{Z}/p\mathbb{Z})^{\times}$$

(bezüglich Multiplikation) eine zyklische Gruppe.

1.7 Chinesischer Restsatz

1.7.1 Chinesischer Restsatz

Sei R ein beliebiger kommutativer Ring mit 1 und seien

$$I_1, \ldots, I_n \subset R$$

n paarweise teilerfremde Ideale, d.h. es gelte

$$I_i + I_j = \{a + b \mid a \in I_i, b \in I_j\} = R \quad \forall\, 1 \leq i, j \leq n,\ i \neq j.$$

Dann ist der Homomorphismus

$$\begin{aligned} \varphi : R &\to R/I_1 \times \ldots \times R/I_n \\ r &\mapsto (r + I_1, \ldots, r + I_n) \end{aligned}$$

surjektiv, d.h. es gibt zu beliebigen $r_1, .., r_n \in R$ ein $x \in R$ mit

$$x \equiv r_i \,(\mathrm{mod}\ I_i) \quad \forall\, 1 \leq i \leq n.$$

Weiter gilt

$$\ker(\varphi) = \bigcap_{i=1}^{n} I_i.$$

1.7.2 Satz 1

Sei R ein Hauptidealring und sei $(a, b) = aR + bR$ ein Ideal in R.

Dann gilt:

$$(a, b) = (a) + (b) = aR + bR = \mathrm{ggT}(a, b) \cdot R$$

(Dieser Satz gilt im Allgemeinen nicht bei faktoriellen Ringen.)

1.7.3 Folgerung aus dem Chinesischen Restsatz

Sei R ein Hauptidealring und seien $a_1, .., a_n \in R$ paarweise teilerfremd, d.h. es gelte $\mathrm{ggT}(a_i, a_j) = 1\ \forall\ 1 \leq i, j \leq n,\ i \neq j$.

Dann gilt:

Die Abbildung

$$\begin{aligned} \varphi : R/(a_1 \cdot .. \cdot a_n) &\to R/(a_1) \times \ldots \times R/(a_n) \\ r &\mapsto (r + (a_1), \ldots, r + (a_n)) \end{aligned}$$

ist ein Isomorphismus.

1.7.4 Satz 2

Sei $\mathbb{Z}$ der Hauptidealring der ganzen Zahlen und sei

$$a \;=\; \pm\prod_{i=1}^{m} p_i^{n_i} \;\in\; \mathbb{Z}$$

die Primfaktorzerlegung von $a \in \mathbb{Z}$.

Dann ist $\mathbb{Z}/a\mathbb{Z}$ isomorph zu $\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{n_m}\mathbb{Z}$.

Schreibweise:

$$\mathbb{Z}/a\mathbb{Z} \quad \xrightarrow{\sim} \quad \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{n_m}\mathbb{Z}$$

Beispiel

Die Abbildung

$$\begin{aligned} \varphi : \mathbb{Z}/105\mathbb{Z} &\;\to\; \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ a &\;\mapsto\; (a+\mathbb{Z}/3\mathbb{Z},\, a+\mathbb{Z}/5\mathbb{Z},\, a+\mathbb{Z}/7\mathbb{Z}) \end{aligned}$$

ist also ein Isomorphismus.

1.7.5 Folgerung

Sei $a = \pm\prod_{i=1}^{m} p_i^{n_i}$ die Primfaktorzerlegung von $a \in \mathbb{Z}$.

Dann gilt für die Einheitengruppe:

$$(\mathbb{Z}/a\mathbb{Z})^\times \quad \xrightarrow{\sim} \quad (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_n^{n_m}\mathbb{Z})^\times$$

Beispiel

Es gilt:

$$\begin{aligned} \big((\mathbb{Z}/15\mathbb{Z})^\times,\ \cdot\ \big) \quad &\xrightarrow{\sim} \quad \big((\mathbb{Z}/3\mathbb{Z})^\times,\ \cdot\ \big) \times \big((\mathbb{Z}/5\mathbb{Z})^\times,\ \cdot\ \big) \\ &\xrightarrow{\sim} \quad ((\mathbb{Z}/2\mathbb{Z}),+) \times ((\mathbb{Z}/4\mathbb{Z}),+) \end{aligned}$$

1.8 Endlich erzeugte abelsche Gruppen

1.8.1 Satz 1

Jede endlich erzeugte abelsche Gruppe ist isomorph zu einer Gruppe der Form

$$\boxed{\mathbb{Z}^n \times \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.}$$

Dabei ist $n \in \mathbb{N} \cup \{0\}$, $p_1, .., p_r$ sind Primzahlen und $\alpha_1, .., \alpha_r \in \mathbb{N}$.

Bemerkung

Der Chinesische Restsatz ist also ein Spezialfall dieses Satzes.

1.9 Eulersche φ-Funktion

1.9.1 Definition

Die Abbildung

$$\begin{aligned} \varphi : \mathbb{N} &\to \mathbb{N} \\ N &\mapsto |(\mathbb{Z}/N\mathbb{Z})^\times| \end{aligned}$$

ist die ***Eulersche φ-Funktion***.

1.9.2 Satz 1

Sei

$$N \;=\; p_1^{n_1} \cdot \ldots \cdot p_m^{n_m} \;=\; \prod_{i=1}^{m} p_i^{n_i}$$

die Primfaktorzerlegung von $N \in \mathbb{N}$.

Dann gilt für die Eulersche φ-Funktion:

$$\varphi(N) \;=\; \prod_{i=1}^{m} \varphi(p_i^{n_i}) \;=\; \prod_{i=1}^{m} \left(p_i^{n_i} - p_i^{n_i-1} \right) \;=\; N \cdot \prod_{i=1}^{m} \left(1 - \frac{1}{p_i} \right)$$

Es gilt also für ein $N \in \mathbb{N}$:

$$\boxed{\varphi(N) \;=\; N \cdot \prod_{\substack{p \mid N \\ p \text{ prim}}} \left(1 - \tfrac{1}{p} \right)}$$

Beispiel

Es gilt $9 = 3^2$. Also folgt

$$\varphi(9) \;=\; 9 \cdot \left(1 - \frac{1}{3} \right) \;=\; 6.$$

Die Einheitengruppe $(\mathbb{Z}/9\mathbb{Z})^\times$ besteht daher aus genau 6 Elementen:

$$(\mathbb{Z}/9\mathbb{Z})^\times \;=\; \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$$

1.9.3 Satz 2

Sei $N \in \mathbb{Z}$ und sei φ die Eulersche φ-Funktion.

Dann gilt:

$$\sum_{d \mid N} \varphi(x) \;=\; N$$

1.10 Gaußsches Lemma und Irreduziblekriterium

1.10.1 Definition

Sei R ein faktoreller Ring und $K = \text{Quot}(R)$ der Quotientenkörper von R.

(1) Sei

$$f(x) \;=\; \sum_{i=0}^{n} a_i x^i \;\in\; R[x].$$

Dann ist

$$I(f) \;=\; \text{ggT}(a_0, .., a_n) \;\in\; R$$

der ***Inhalt*** von f.

(2) Sei $c \in R$ mit $c \neq 0$ und sei $f \in K[x]$ mit $c \cdot f \in R[x]$.

Dann ist

$$I(f) \;=\; \frac{1}{c} \cdot I(c \cdot f) \;\in\; K$$

der ***Inhalt*** von f.

Beispiel

Sei

$$f(x) \;=\; \frac{1}{7}x^2 + \frac{1}{5}x + 3 \;\in\; \mathbb{Q}[x].$$

Für $c = 35$ gilt:

$$c \cdot f(x) \;=\; 5x^2 + 7x + 105 \;\in\; \mathbb{Z}[x]$$

Demnach gilt:

$$I(f) \;=\; \frac{1}{35} \cdot \text{ggT}(5, 7, 105) \;=\; \frac{1}{35}$$

1.10.2 Gaußsches Lemma

Sei R ein faktorieller Ring.

Dann ist auch $R[x]$ faktoriell und die irreduziblen Elemente von $R[x]$ sind:

(1) Die irreduziblen Elemente $p \in R$ und

(2) alle Polynome $f \in R[x]$ mit $I(f) = 1$.

Folgerung 1

Sei R ein faktorieller Ring. Dann ist auch $R[x_1, .., x_n]$ faktoriell.

Folgerung 2

Sei $R[x]$ ein faktorieller Ring. Dann ist auch R faktoriell.

1.10.3 Eisensteinsches Irreduzibelkriterium

Sei R ein faktoreller Ring, $K = \text{Quot}(R)$ der Quotientenkörper von R, $p \in R$ irreduzibel und sei

$$\boxed{f(x) \;=\; x^n + \sum_{i=0}^{n-1} a_i x^i \;\in\; R[x].}$$

Es gelte:

(1) $p \mid a_i$ für alle $1 \leq i \leq n-1$

(2) $p^2 \nmid a_0$

Dann ist $f(x)$ irredizibel in $K[x]$ (also auch in $R[x]$).

1.10.4 Beispiel 1

Sei

$$f(x) \;=\; x^{13} + 24x^7 + 9x^2 + 24$$

gegeben.

Es gilt $3 \mid a_i$ für $i = 0, .., 12$ und $3^2 \nmid a_0 = 24$, somit ist $f(x)$ nach Einstein irreduzibel in $\mathbb{Z}[x]$ und nach dem Gaußschen Lemma auch in $\mathbb{Q}[x]$.

1.10.5 Beispiel 2

Sei p ein Primzahl und sei

$$\Phi_p(x) \;=\; x^{p-1} + x^{p-2} + \ldots + x + 1 \;=\; \frac{x^p - 1}{x - 1} \;\in\; \mathbb{Z}[x].$$

Dann ist $\Phi_p(x)$ irreduzibel in $\mathbb{Z}[x]$ und in $\mathbb{Q}[x]$.

Die Polynome $\Phi_p(x)$ heißen ***Kreisteilungspolynome***, da alle p Nullstellen in der komplexen Zahlenebene auf dem Einheitskreis liegen. Die Nullstellen sind dann genau

$$\left\{ \left(e^{\frac{2\pi i}{p}} \right)^k \;\middle|\; k = 0, \ldots, p-1 \right\}$$

und heißen auch ***primitive n-ten Einheitswurzeln***.

1.11 Gruppen der primes Resten

1.11.1 Definition und Satz

Sei p eine Primzahl und sei $a \in \mathbb{Z}$.

a heißt ***Primitivwurzel*** mod p, wenn $\overline{a}$ in $\mathbb{Z}/p\mathbb{Z}$ die genaue Ordnung $p-1$ hat.

Davon gibt es $\varphi(p-1)$ verschiedene.

Beispiel

Sei $p = 7$. Es gilt

$$\begin{array}{lll} \mathrm{ord}(1) = 1, & \mathrm{ord}(2) = 3, & \mathrm{ord}(3) = 6, \\ \mathrm{ord}(4) = 3, & \mathrm{ord}(5) = 6, & \mathrm{ord}(6) = 2. \end{array}$$

Demnach sind 3 und 5 Primitivwurzeln mod 7.

Das Ergebnis stimmt auch mit $\varphi(6) = 2$ überein.

1.11.2 Satz 1

Sei p eine Primzahl, sei $a \in \mathbb{Z}$ und es gelte $a \not\equiv 0 \pmod{p}$.

Dann hat

$$\overline{(1+ap)} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$$

die genaue Ordnung p^{n-1}.

1.11.3 Satz 2

Sei $p > 2$ ein Primzahl.

Dann gilt:

$$\big((\mathbb{Z}/p^n\mathbb{Z})^\times,\ \cdot\ \big) \quad \xrightarrow{\sim} \quad \big((\mathbb{Z}/(p-1)\mathbb{Z})^\times, +\big) \times \big((\mathbb{Z}/p^{n-1}\mathbb{Z})^\times, +\big)$$

1.11.4 Satz 3

Sei $p > 2$ ein Primzahl.

Dann ist

$$(\mathbb{Z}/p^n\mathbb{Z})^\times$$

zyklisch und von der Ordnung

$$\varphi(p^n) \ = \ (p-1) \cdot p^{n-1}.$$

Beispiel 1

Es gilt:

$$(\mathbb{Z}/3^2\mathbb{Z})^\times \ = \ (\mathbb{Z}/9\mathbb{Z})^\times \ = \ \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$$

Für die Ordnung gilt:

$$\varphi(p) \ = \ 2 \cdot 3^1 \ = \ 6$$

Beispiel 2

Es gilt:

$$(\mathbb{Z}/2^3\mathbb{Z})^\times \ = \ (\mathbb{Z}/8\mathbb{Z})^\times \ = \ \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

Diese Gruppe ist aber nicht zyklisch.

1.12 Quadratische Gleichungen

1.12.1 Satz 1

Sei K ein Körper und sei $f \in K[x]$ mit $\text{grad}(f) = d$.

Dann hat f höchstens d Nullstellen.

Folgerung

Sei $p \in \mathbb{Z}$ eine Primzahl.

Dann hat die Gleichung

$$x^d - 1 \;=\; 0$$

in $\mathbb{Z}/p\mathbb{Z}$ höchstens d Nullstellen.

1.12.2 Definition

Sei $p \in \mathbb{Z}$ ein Primzahl und sei $R = \mathbb{Z}/p\mathbb{Z}$ ein Ring.

$a \in \mathbb{Z}/p\mathbb{Z}$ heißt ***quadratischer Rest*** modulo p :$\Leftrightarrow$

$$x^2 \;\equiv\; a \;(\text{mod}\;\; p\,)$$

ist lösbar.

$a \in \mathbb{Z}/p\mathbb{Z}$ heißt ***quadratischer Nichtrest*** modulo p :$\Leftrightarrow$

$$x^2 \;\equiv\; a \;(\text{mod}\;\; p\,)$$

ist nicht lösbar.

Schreibweisen:

$$\begin{array}{ll} a \text{ quadratischer Rest:} & \left(\frac{a}{p}\right) = 1 \\ a \text{ quadratischer Nichtrest:} & \left(\frac{a}{p}\right) = -1 \end{array}$$

1.12.3 Satz 2

Sei $p \in \mathbb{Z}$ eine Primzahl.

Dann ist die Abbildung

$$\begin{array}{rcl} \varphi : (\mathbb{Z}/p\mathbb{Z})^\times & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \mapsto & x^2 \end{array}$$

ein Gruppenhomomorphismus. Weiter gilt

$$\ker(\varphi) \;=\; \{-1, 1\} \qquad \text{und} \qquad \text{Im}(\varphi) \;=\; \left\{ a \in (\mathbb{Z}/p\mathbb{Z})^\times \;\middle|\; \left(\frac{a}{p}\right) = 1 \right\},$$

somit folgt $|\mathrm{Im}(\varphi)| = \frac{p-1}{2}$.

Für $p \neq 2$ gilt:

(1) Es gibt $\frac{p-1}{2}$ quadratische Nichtreste.

(2) Es gilt: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

1.13 Der Ring der Gaußschen Zahlen

1.13.1 Definition und Satz

Seien folgende Mengen gegeben:

$$\begin{array}{lcll} \mathbb{Q}(i) & := & \{a+bi \mid a+bi \in \mathbb{C},\ a,b \in \mathbb{Q}\} & \subset \quad \mathbb{C} \\ \mathbb{Z}[i] & := & \{a+bi \mid a+bi \in \mathbb{C},\ a,b \in \mathbb{Z}\} & \subset \quad \mathbb{Q}(i) \end{array}$$

$\mathbb{Z}[i]$ ist der Ring der ***Gaußschen Zahlen*** und es gilt

$$\mathbb{Q}(i) \ = \ \mathrm{Quot}(\mathbb{Z}[i]).$$

Weiter sei folgende Abbildung gegeben:

$$\overline{(\ )} : \mathbb{Z}[i] \to \mathbb{Z}[i], \quad a+bi \mapsto a-bi$$

Dann gilt:

(1) Die Abbildung $\overline{(\ )}$ ist ein Automorphismus.

(2) $\overline{z \cdot y} = \overline{z} \cdot \overline{y}$

(3) $\overline{z+y} = \overline{z} + \overline{y}$

(4) $|z|^2 = a^2 + b^2 = z \cdot \overline{z}$

(5) $|z \cdot y| = |z| \cdot |y|$

1.13.2 Satz 1

Die Einzeitengruppe von $\mathbb{Z}[i]$ ist zyklisch und es gilt

$$(\mathbb{Z}[i])^{\times} \ = \ \{\pm 1, \pm i\}.$$

1.13.3 Satz 2

$\mathbb{Z}[i]$ ist ein Integritätsring und besitzt eine Division mit Rest.

D.h. zu je zwei $x, y \in \mathbb{Z}[i],\ y \neq 0$ gibt es zwei $s, r \in \mathbb{Z}[i]$ mit

$$x \ = \ s \cdot y + r,$$

dabei $|r|^2 < |y|^2$.

1.13.4 Satz 3

$\mathbb{Z}[i]$ ist sogar ein Hauptidealring.

1.13.5 Primes Elemente im Ring der Gaußschen Zahlen

Sei p eine Primzahl in $\mathbb{Z}$.

Dann lassen sich zu dieser Primzahl p ein oder zwei primes Elemente im Ring der Gaußschen Zahlen finden. Es ist bekannt, dass für $p \neq 2$

$$p \,(\bmod\ 4) = 1 \qquad \text{oder} \qquad p \,(\bmod\ 4) = 3$$

gilt, da jede Primzahl ungerade ist.

Es gilt nun für jede gegeben Primzahl p in $\mathbb{Z}$:

(1) Aus $p = 2$ folgt, dass

$$(1+i) \qquad \text{und} \qquad (1-i)$$

primes Elemente in $\mathbb{Z}[i]$ sind (es gilt $(1+i)(1-i) = 2$).

(2) Aus allen p mit

$$p \,(\bmod\ 4) \ = \ 3$$

folgt, dass p auch in $\mathbb{Z}[i]$ ein primes Element ist.

(3) Aus allen p mit

$$p \,(\bmod\ 4) \ = \ 1$$

folgt, dass es eine Zerlegung

$$p \ = \ (a+bi) \cdot (a-bi)$$

von p gibt, so dass $(a+bi)$ und $(a-bi)$ primes Elemente in $\mathbb{Z}[i]$ sind.

Beispiel 1

Für die Primzahl $p = 19$ gilt

$$19 \,(\bmod\ 4) \ = \ 3,$$

daher ist $19 = 19 + 0 \cdot i$ auch ein primes Element in $\mathbb{Z}[i]$.

Beispiel 2

Für die Primzahl $p = 97$ gilt

$$97 \,(\bmod\ 4) \ = \ 1$$

und es gilt

$$(9+4i) \cdot (9-4i) \ = \ 81 + 16 \ = \ 97.$$

Somit sind $(9+4i)$ und $(9-4i)$ primes Elemente in $\mathbb{Z}[i]$.

Beispiel 3

Ist das Element $91 \in \mathbb{Z}[i]$ in Primfaktoren zu zerlegen, so gilt:

$$91 \;=\; 7 \cdot 13 \;\in\; \mathbb{Z} \quad \Rightarrow \quad 91 \;=\; 7 \cdot (3+2i) \cdot (3-2i) \;\in\; \mathbb{Z}[i],$$

da $7 \;(\bmod\; 4) = 3$ und $13 \;(\bmod\; 4) = 1$ und $(3+2i) \cdot (3-2i) = 13$.

1.13.6 Satz 4

(1) Sei p eine Primzahl mit $p \equiv 1 \;(\bmod\; 4)$.

Dann gilt:

$$\mathbb{Z}[i]/p\mathbb{Z}[i] \quad \xrightarrow{\sim} \quad \mathbb{Z}/p\mathbb{Z} \;\times\; \mathbb{Z}/p\mathbb{Z}$$

(2) Sei p eine Primzahl mit $p \equiv 3 \;(\bmod\; 4)$.

Dann ist $\mathbb{Z}[i]/p\mathbb{Z}[i]$ ein Körper aus p^2 Elementen.

1.13.7 Ausblick

Betrachtet man ähnliche Ringe der Form

$$\mathbb{Z}[\sqrt{d}] \;=\; \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\},$$

so ist bekannt, dass es für $d < 0$ endlich viele weitere Hauptidealringe gibt.

Über Ringe dieser Form mit $d > 0$ ist bislang noch nicht sehr viel bekannt, es wird aber vermutet, dass es unendliche viele Hauptidealringe gibt.

1.14 Euklidische Ringe

1.14.1 Definition

Ein Integritätsring R heißt ein ***euklidischer Ring***, wenn es eine Abbildung

$$d : R \;\rightarrow\; \mathbb{N} \cup \{0\} \cup \{-\infty\}$$

gibt, für die gilt:

(1) $\forall\; a, b \in R,\; b \neq 0,\; \exists\; s, r \in R :\; a = sb + r$ mit $d(r) < d(b)$

(2) $d^{-1}(-\infty) = 0$

Schreibweise: (R, d)

1.14.2 Beispiele

(1) Sei $R = \mathbb{Z}$. Dann wird R durch die Abbildung

$$d(x) \;=\; \begin{cases} |x| & \text{für} \quad x \neq 0 \\ -\infty & \text{für} \quad x = 0 \end{cases}$$

ein euklidischer Ring.

(2) Sei $R = \mathbb{Z}[i]$. Dann wird R durch die Abbildung

$$d(z) \;=\; d(a+bi) \;=\; \begin{cases} a^2+b^2 & \text{für} \quad z \neq 0 \\ -\infty & \text{für} \quad z = 0 \end{cases}$$

ein euklidischer Ring.

(3) Sei K ein Körper und $R = K[x]$. Dann wird R durch die Abbildung

$$d(f) \;=\; \begin{cases} \text{grad}(f) & \text{für} \quad f \neq 0 \\ -\infty & \text{für} \quad f = 0 \end{cases}$$

ein euklidischer Ring.

1.14.3 Satz 1

Jeder euklidische Ring (R, d) ist ein Hauptidealring.

1.14.4 Euklidischer Algorithmus

Sei (R, d) ein euklidischer Ring und seien $a, b \in R$.

Dann kann man das Ideal

$$R \cdot a + R \cdot b \;=\; (a, b),$$

also den ggT von a und b, durch den Euklidischen Algorithmus berechnen:

$$\begin{aligned} a &= s \cdot b + r \\ b &= s_1 \cdot r_1 + r_2 \qquad \text{dabei } r_1 = r \\ r_1 &= s_2 \cdot r_2 + r_3 \qquad \text{dabei } 0 \leq r_2 < r_1 \\ &\vdots \\ r_{k-1} &= s_k \cdot r_k + r_{k+1} \qquad \text{dabei } 0 \leq r_k < r_{k-1} \\ r_k &= s_{k+1} \cdot r_{k+1} \qquad \text{dabei } 0 \leq r_{k+1} < r_k \end{aligned}$$

Insgesammt gilt dabei also

$$d(b) > d(r) = d(r_1) > d(r_2) \ldots > d(r_k).$$

Es folgt nun:

$$R \cdot a + R \cdot b \;=\; (a, b) \;=\; R \cdot r_{k+1} \;=\; (r_{k+1})$$

Beispiel

Der Euklidische Algorithmus verläuft bei zwei aufeinanderfolgenden Zahlen der ***Fibouacci Folge***

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

besonders langsam:

$$\begin{aligned} 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Es gilt $s, s_1, s_2, .., s_k = 1$, daher verläuft der Algorithmus hier gerade so langsam.

1.15 Aufgaben

1.15.1 Aufgabe 1

Sei $R = \mathbb{Z}/15\mathbb{Z}$. Berechne $R^\times$.

Lösung

Es gilt

$$R = \{\overline{0}, \overline{1}, \ldots, \overline{14}\}.$$

Gesucht sind alle Elemente aus R, die (bzgl. Multiplikation) invertierbar sind.

$\overline{0}, \overline{3}, \overline{5}$ sind Nullteiler von R, daher sind diese Element sowie Vielfaches davon nicht in $R^\times$.

Es gilt:

$$\begin{aligned} \overline{1} \cdot \overline{1} &= \overline{1}, & \overline{2} \cdot \overline{8} &= \overline{1}, & \overline{4} \cdot \overline{4} &= \overline{1}, \\ \overline{7} \cdot \overline{13} &= \overline{1}, & \overline{11} \cdot \overline{11} &= \overline{1}, & \overline{14} \cdot \overline{14} &= \overline{1}. \end{aligned}$$

Daher folgt

$$R^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}.$$

1.15.2 Aufgabe 2

Bestimme mit Hilfe des Euklidischen Algorithmus den ggT von 102 und 27 in $\mathbb{Z}$.

Lösung

Es gilt

$$\begin{aligned} 102 &= 3 \cdot 27 + 21 \\ 27 &= 1 \cdot 21 + 6 \\ 21 &= 3 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Somit ist $\mathrm{ggT}(27, 102) = 3$.

1.15.3 Aufgabe 3

Bestimme mit Hilfe des Euklidischen Algorithmus den ggT von

$$f(x) = x^9 + x^7 - x^2 - 1 \quad \text{und} \quad g(x) = x^8 + x^6 - x^2 - 1$$

in $\mathbb{Q}[x]$.

Lösung

Durch zweimalige Polynomdivision erhält man

$$\begin{aligned} (x^9 + x^7 - x^2 - 1) &= (x) \cdot (x^8 + x^6 - x^2 - 1) \; + \; (x^3 - x^2 + x - 1) \\ (x^8 + x^6 - x^2 - 1) &= (x^5 + x^4 + x^3 + x^2 + x + 1) \cdot (x^3 - x^2 + x - 1). \end{aligned}$$

Somit ist $\mathrm{ggT}(f(x), g(x)) = x^3 - x^2 + x - 1 \in \mathbb{Q}[x]$.

1.15.4 Aufgabe 4

Sei

$$R \; = \; \{(a, b) = a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

der Ring der so genannten ***Gaußschen Zahlen***.

(1) Zeige, dass $\varphi : R \to R, \; a + bi \mapsto a - bi$ ein Automorphismus von R ist.

(2) Berechne $R^\times$.

Lösung Teil 1

Seien $x = (a, b), y = (c, d) \in R$. Dann gilt:

(1) $\varphi(1) \;=\; \varphi(1,0) \;=\; 1 - 0 \;=\; 1$

(2) Es gilt für die Addition:

$$\begin{aligned} \varphi(x+y) &= \varphi(a+c, b+d) \\ &= (a+c, -b-d) \\ &= (a,-b) + (c,-d) \;=\; \varphi(x) + \varphi(y) \end{aligned}$$

(3) Es gilt für die Multiplikation:

$$\begin{aligned} \varphi(x \cdot y) &= \varphi(ac - bd, ad + bc) \\ &= (ac - bd, -ad - bc) \\ &= (a,-b) \cdot (c,-d) \;=\; \varphi(x) \cdot \varphi(y) \end{aligned}$$

(4) φ ist bijektiv, da φ linear ist und $\ker(\varphi) = \{(0,0)\}$ gilt.

Lösung Teil 2

Angenommen $R^\times$ ist nicht leer, dann gibt es $(a, b), (c, d) \in R$ mit

$$(a,b) \cdot (c,d) \;=\; (1,0).$$

Demnach gilt

$$ac - bd \;=\; 1 \qquad \text{sowie} \qquad ad + bc \;=\; 0$$

und es folgt

$$a = \frac{c}{c^2 + d^2} \qquad \text{und} \qquad b = \frac{-d}{c^2 + d^2}.$$

Da $a, b \in \mathbb{Z}$ ist es also notwendig, dass gilt:

$$(c,d) \;=\; (\pm 1, 0) \qquad \text{oder} \qquad (c,d) \;=\; (0, \pm 1)$$

Man sieht sofort:

$$\begin{aligned} (1,0) \cdot (1,0) &\;=\; (1,0), & (-1,0) \cdot (-1,0) &\;=\; (1,0), \\ (0,1) \cdot (0,-1) &\;=\; (1,0), & (0,-1) \cdot (0,1) &\;=\; (1,0). \end{aligned}$$

Somit gilt

$$R^\times \;=\; \{(1,0), (-1,0), (0,1), (0,-1)\} \;=\; \{\pm 1, \pm i\}.$$

Für jeden Automorphismus von Ringen gilt sogar:

Das Bild einer Einheit ist wieder eine Einheit.

1.15.5 Aufgabe 5

Zeige, dass die Einheitengruppen der beiden Körper

$$K_1 = \mathbb{Z}/5\mathbb{Z} \qquad \text{und} \qquad K_2 = \mathbb{Z}/11\mathbb{Z}$$

zyklisch sind.

Lösung

$(\mathbb{Z}/p\mathbb{Z})^\times$ ist genau dann zyklisch, wenn es ein Element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ gibt, so dass jedes Element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ von der Form

$$g^m \qquad \text{mit} \qquad m \in \mathbb{Z}$$

ist.

Man schreibt dann: $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$

Es gilt:

$$(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} \quad \text{und} \quad (\mathbb{Z}/11\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{10}\}.$$

(1) Für $\overline{2} \in (\mathbb{Z}/5\mathbb{Z})^\times$ gilt:

$$\{\overline{2}^0 = \overline{1},\ \overline{2}^1 = \overline{2},\ \overline{2}^2 = \overline{4},\ \overline{2}^3 = \overline{3}\} = \langle \overline{2} \rangle = (\mathbb{Z}/5\mathbb{Z})^\times$$

(2) Für $\overline{6} \in (\mathbb{Z}/11\mathbb{Z})^\times$ gilt:

$$\{\overline{6}^0 = \overline{1},\ \overline{6}^1 = \overline{6},\ \overline{6}^2 = \overline{3},\ \overline{6}^3 = \overline{7}, \ldots\} = \langle \overline{6} \rangle = (\mathbb{Z}/11\mathbb{Z})^\times$$

Für eine Primzahl p ist sogar jeder Körper der Form $\mathbb{Z}/p\mathbb{Z}$ zyklisch.

1.15.6 Aufgabe 6

Sei

$$\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} \mid x = a + b\sqrt{2} \text{ mit } a, b \in \mathbb{Q}\}.$$

(1) Zeige, dass $\mathbb{Q}[\sqrt{2}]$ ein Unterkörper von $\mathbb{R}$ ist.

(2) Berechne $(7 + \sqrt{2})^{-1}$ und $(11 - \sqrt{2})^{-1}$ in $\mathbb{Q}[\sqrt{2}]$.

Lösung Teil 1

Es gilt:

(1) $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$

(2) $0 + 0\sqrt{2} = 0 \in \mathbb{Q}[\sqrt{2}]$

(3) $1 + 0\sqrt{2} = 1 \in \mathbb{Q}[\sqrt{2}]$

(4) Seien $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ beliebig. Dann gilt:

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\ &= (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]\end{aligned}$$

(5) Sei $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ beliebig. Dann gilt:

$$-(a + b\sqrt{2}) = -a - b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

(6) Sei $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$ beliebig. Dann gilt:

$$\begin{aligned}(a + b\sqrt{2})^{-1} &= \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]\end{aligned}$$

Somit ist $\mathbb{Q}[\sqrt{2}]$ ein Unterkörper von $\mathbb{R}$.

Lösung Teil 2

Es gilt

$$(7 + \sqrt{2})^{-1} = \frac{1}{7 + \sqrt{2}} = \frac{7 - \sqrt{2}}{49 - 2} = \frac{7}{47} - \frac{1}{47}\sqrt{2}$$

sowie

$$(11 - \sqrt{2})^{-1} = \frac{1}{11 - \sqrt{2}} = \frac{11 + \sqrt{2}}{121 - 2} = \frac{11}{119} + \frac{1}{119}\sqrt{2}.$$

1.15.7 Aufgabe 7

Berechene $|(\mathbb{Z}/5040\mathbb{Z})^\times|$.

Lösung

Sei $N = 5040 \in \mathbb{N}$. Dann gilt:

$$5040 = 7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 5 \cdot 2 \cdot 3 \cdot 5 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$$

Also folgt:

$$\varphi(5040) = 5040 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = 1152$$

1.15.8 Aufgabe 8

Sei K ein Körper von der Primzahlcharakteristik $p > 0$ und sei

$$\begin{array}{rcl} F : K & \to & K \\ x & \mapsto & x^p \end{array}$$

eine Abbildung.

(1) Zeige, dass F ein injektiver Homomorphismus ist.

(2) Zeige, dass für $K = \mathbb{Z}/p\mathbb{Z}$ die Abbildung F genau die Identität ist.

Die Abbildung F ist der so genannte ***Frobeniushomomorphismus***.

Lösung Teil 1

Es gilt:

(1) $F(1) = 1^p = 1$

(2) Seien $x, y \in K$ beliebig. Dann gilt:

$$\begin{aligned} F(x+y) &= (x+y)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \\ &= x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} + y^p \\ &= x^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} x^k y^{p-k} + y^p \\ &= x^p + \sum_{k=1}^{p-1} \frac{(k+1)(k+2)\ldots(p-1)p}{1 \cdot 2 \cdot \ldots \cdot (p-k)} x^k y^{p-k} + y^p \\ &= x^p + \sum_{k=1}^{p-1} \frac{(k+1)(k+2)\ldots(p-1) \cdot x^k \cdot y^{p-k}}{1 \cdot 2 \cdot \ldots \cdot (p-k)} \cdot p + y^p \\ &= x^p + y^p + \sum_{k=1}^{p-1} \underbrace{\frac{\binom{p}{k}}{p}}_{\in \mathbb{Z}} \cdot x^k \cdot y^{p-k} \cdot p \\ &= x^p + y^p = F(x) + F(y) \end{aligned}$$

(3) Seien $x, y \in K$ beliebig. Dann gilt:

$$F(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = F(x) \cdot F(y)$$

Es bleibt nun noch die Injektivität zu zeigen:

Seien $x, y \in K$ mit $F(x) = F(y)$. Dann folgt:

$$x^p = y^p \quad \Leftrightarrow \quad x^p - y^p = 0 \quad \Leftrightarrow \quad (x-y)^p = 0$$

Es muss also $x = y$ gelten und somit ist F injektiv.

Lösung Teil 2

Sei $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ mit $n \in \mathbb{Z}$.

Es ist zu zeigen, dass $F(\overline{n}) = \overline{n}$ für alle $0 \leq n \leq p-1$ gilt:

Induktionsvorausetzung

$$F(\overline{n}) \;=\; \overline{n}$$

Induktionsanfang $(n = 0)$

$$F(\overline{0}) \;=\; \overline{0}^{\,p} \;=\; \overline{0}$$

Induktionsschritt

$$F(\overline{n+1}) \;=\; F(\overline{n}+\overline{1}) \;=\; F(\overline{n}) + F(\overline{1}) \;=\; \overline{n}^{\,p} + \overline{1}^{\,p} \;=\; \overline{n} + \overline{1} \;=\; \overline{n+1}$$

Es gilt also für alle $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$

$$F(\overline{n}) \;=\; \overline{n}.$$

Demnach ist F die Identität von $\mathbb{Z}/p\mathbb{Z}$.

1.15.9 Aufgabe 9

Zeige, dass die Menge

$$I \;=\; \{f(x) \cdot 6 + g(x) \cdot (x^2+1) \mid f(x), g(x) \in \mathbb{Z}[x]\}$$

ein Ideal in $\mathbb{Z}[x]$ ist und bestimme die Ordnung des Restklassenringes $\mathbb{Z}[x]/I$.

Lösung

Zunächst muss gezeigt werden, dass I eine additive Untergruppe von $\mathbb{Z}[x]$ ist:

(1) Mit $f(x) = g(x) = 0$ gilt $e = 0 \in I$.

(2) Mit $f(x), g(x), \overline{f}(x), \overline{g}(x) \in \mathbb{Z}[x]$ gilt

$$\begin{aligned} & \big(f(x) \cdot 6 + g(x) \cdot (x^2+1)\big) + \big((\overline{f}(x) \cdot 6 + \overline{g}(x) \cdot (x^2+1)\big) \\ = \;& \big(f(x) + \overline{f}(x)\big) \cdot 6 + (g(x) + \overline{g}(x)) \cdot (x^2+1) \quad \in \quad I. \end{aligned}$$

(3) Mit $f(x), g(x) \in \mathbb{Z}[x]$ ist auch $-f(x) \cdot 6 - g(x) \cdot (x^2+1) \in I$.

Es ist nun noch die Idealeigenschaft zu zeigen. Sei dazu $p(x) \in \mathbb{Z}[x]$ beliebig, dann gilt

$$\begin{aligned} & p(x) \cdot \big(f(x) \cdot 6 + g(x) \cdot (x^2+1)\big) \\ = \quad & (p(x) \cdot f(x)) \cdot 6 + (p(x) \cdot g(x)) \cdot (x^2+1) \quad \in \quad I. \end{aligned}$$

Damit ist gezeigt, dass I ein Ideal in $\mathbb{Z}[x]$ ist und es kann nun die Ordnung von $\mathbb{Z}[x]/I$ bestimmt werden:

Mit $f(x) = 0$ und $g(x) = 1$ erhält man $x^2 + 1 \in I$, somit sind alle Polynome in $\mathbb{Z}[x]/I$ vom Grad < 2, also von der Form

$$ax + b \quad \in \quad \mathbb{Z}[x].$$

Mit $f(x) = 1$ und $g(x) = 0$ erhält man $6 \in I$, also kommen auch nur Polynome $ax + b$ mit $b \in \{0, .., 5\}$ in $\mathbb{Z}[x]/I$ vor.

Analog erhält man mit $f(x) = x$ und $g(x) = 0$ das Polynom $6x \in I$ und es kommen nur Polynome $ax + b$ mit $a \in \{0, .., 5\}$ in $\mathbb{Z}[x]/I$ vor. Man erhält insgesamt

$$\mathbb{Z}[x]/I \;=\; \Big\{ ax + b \in \mathbb{Z}[x] \;\Big|\; a, b \in \{0, 1, 2, 3, 4, 5\} \Big\}$$

und somit $|\mathbb{Z}[x]/I| = 36$.

1.15.10 Aufgabe 10

Zeige, dass folgende Polynome (bis auf Assoziiertheit) in $\mathbb{R}[x]$ irreduzibel sind:

(1) Alle linearen Polynome $f(x) = (x + a)$ mit $a \in \mathbb{R}$.

(2) Quadratische Polynome $g(x) = x^2 + ax + b$ mit $a, b \in \mathbb{R}$ und $a^2 - 4b < 0$.

Lösung Teil 1

Sei $f(x) = a(x) \cdot b(x)$ eine beliebige Zerlegung von $f(x)$.

Es gilt

$$\operatorname{grad}(f) \;=\; \operatorname{grad}(a) + \operatorname{grad}(b) \;=\; 1.$$

Sei also o.B.d.A. $\operatorname{grad}(a) = 1$ und $\operatorname{grad}(b) = 0$.

Demnach ist $b(x) = k \neq 0$ ein konstantes Polynom und somit gehört $b(x)$ zur Einheitengruppe von $(\mathbb{R}[x])^\times$.

Lösung Teil 2

Sei $g(x) = x^2 + ax + b$. Dann gilt nach der p,q-Formel:

$$\alpha_{1,2} \;=\; -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$$

Wenn

$$\frac{a^2}{4} - b \geq 0 \qquad \Leftrightarrow \qquad a^2 - 4b \geq 0$$

gilt, dann ist

$$g(x) \;=\; x^2 + ax + b \;=\; (x - \alpha_1)(x - \alpha_2)$$

ein Zerlegung von $g(x)$. Da aber weder $(x - \alpha_1)$ noch $(x - \alpha_2)$ ein Element der Einheitengruppe von $(\mathbb{R}[x])^\times$ ist, kann ein derartiges Polynom $g(x)$ auch nicht irreduzibel sein.

Sei nun $a^2 - 4b < 0$. Dann gilt für jeder Zerlegung von $g(x) \in \mathbb{R}[x]$

$$g(x) \;=\; a(x) \cdot b(x)$$

mit $\text{grad}(b) = 0$ (o.B.d.A.). Somit ist $b(x) = k \neq 0$ ein konstantes Polynom und somit gilt $b(x) \in (\mathbb{R}[x])^\times$.

1.15.11 Aufgabe 11

Sei $\mathbb{F}_2$ der Körper aus zwei Elementen und sei $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

(1) Zeige, dass $p(x)$ irreduzibel in $\mathbb{F}_2[x]$ ist.

(2) Finde die Gruppe $(\mathbb{F}_2[x]/p(x))^\times$ und zeige, dass diese zyklisch ist.

Lösung Teil 1

Es gilt $\text{grad}(p) = 3$. Somit gilt für eine (echte) Zerlegung der Form

$$p(x) \;=\; a(x) \cdot b(x)$$

$\text{grad}(a) = 1$ und $\text{grad}(b) = 2$ (bzw. umgekehrt).

Es gilt aber $p(0) = 1$ und $p(1) = 1$, d.h. $p(x)$ hat in $\mathbb{F}_2[x]$ keine Nullstellen und somit gibt es kein solches Polynom $a(x) \in \mathbb{F}_2[x]$.

Demnach ist

$$p(x) \;=\; 1 \cdot (x^3 + x + 1)$$

die einzigst mögliche Zerlegung für $p(x)$.

$p(x)$ ist also irreduzibel, da 1 Element der Einheitengruppe $(\mathbb{F}_2[x])^\times$ ist.

Lösung Teil 2

Es ist

$$\mathbb{F}_2[x]/(x^3+x+1) \;=\; \left\{\overline{0},\,\overline{1},\,\overline{x},\,\overline{x+1},\,\overline{x^2},\,\overline{x^2+1},\,\overline{x^2+x},\,\overline{x^2+x+1}\right\}$$

und es gilt:

$$\begin{aligned}
\overline{1}\cdot\overline{1} &= \overline{1},\\
\overline{x}\cdot\overline{x^2+1} &= \overline{x^3+x} \;=\; \overline{x^3+x+1+1} \;=\; \overline{1},\\
\overline{x+1}\cdot\overline{x^2+x} &= \overline{x^3+x} \;=\; \overline{1},\\
\overline{x^2}\cdot\overline{x^2+x+1} &= \overline{x^4+x^3+x^2} \;=\; \overline{1},
\end{aligned}$$

also ist

$$(\mathbb{F}_2[x]/(x^3+x+1))^\times \;=\; \left\{\overline{1},\,\overline{x},\,\overline{x+1},\,\overline{x^2},\,\overline{x^2+1},\,\overline{x^2+x},\,\overline{x^2+x+1}\right\}.$$

Weiter gilt

$$\begin{aligned}
\overline{x+1}^0 &= \overline{1},\\
\overline{x+1}^1 &= \overline{x+1},\\
\overline{x+1}^2 &= \overline{x^2+1},\\
\overline{x+1}^3 &= \overline{x^3+x^2+x+1} \;=\; \overline{x^2},\\
\overline{x+1}^4 &= \overline{x+1}^3\cdot\overline{x+1} \;=\; \overline{x^2}\cdot\overline{x+1} \;=\; \overline{x^3+x^2} \;=\; \overline{x^2+x+1},\\
\overline{x+1}^5 &= \overline{x+1}^3\cdot\overline{x+1}^2 \;=\; \overline{x^2}\cdot\overline{x^2+1} \;=\; \overline{x^4+x^2} \;=\; \overline{x},\\
\overline{x+1}^6 &= \overline{x+1}^5\cdot\overline{x+1} \;=\; \overline{x}\cdot\overline{x+1} \;=\; \overline{x^2+x},
\end{aligned}$$

also folgt

$$(\mathbb{F}_2[x]/(x^3+x+1))^\times \;=\; \langle\,\overline{x+1}\,\rangle \;=\; \left\{\overline{x+1}^{\,i} \;\middle|\; 0\le i\le 6\right\}.$$

(Ein weiterer Lösungsweg ist die Polynomdivision.)

1.15.12 Aufgabe 12

Löse folgende ***simultanen Kongruenzen***:

(1) $x\equiv 2\ (\mathrm{mod}\ 7),\ \ x\equiv 6\ (\mathrm{mod}\ 13),\ \ x\equiv 1\ (\mathrm{mod}\ 3)$

(2) $x\equiv 4\ (\mathrm{mod}\ 5),\ \ x\equiv 1\ (\mathrm{mod}\ 7),\ \ x\equiv 1\ (\mathrm{mod}\ 52)$

Lösung

Da $\mathbb{Z}$ ein Hauptidealring ist und jeweils $\{3, 7, 13\}$ bzw. $\{5, 7, 52\}$ in $\mathbb{Z}$ paarweise teilerfremd sind, ist die Abbildung

$$\begin{aligned} \varphi : \mathbb{Z}/(a_1a_2a_3) &\rightarrow \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \mathbb{Z}/(a_3) \\ x &\mapsto (x + (a_1),\ x + (a_2),\ x + (a_3)) \end{aligned}$$

mit $\{a_1, a_2, a_3\} = \{3, 7, 13\}$ bzw. $\{a_1, a_2, a_3\} = \{5, 7, 52\}$ ein Isomorphismus (Folgerung aus dem Chinesischen Restsatz).

Daher gibt es jeweils eine Lösung $\overline{x}$ der simultanen Kongruenz in $\mathbb{Z}/(a_1a_2a_3)$, also ist die gesammte Lösungsmenge jeweils

$$\{x + (a_1a_2a_3)k \mid k \in \mathbb{Z}\}.$$

Teil 1

Es gilt

$$\begin{aligned} 58 \ (\mathrm{mod}\ 7) &= 2, \\ 58 \ (\mathrm{mod}\ 13) &= 6, \\ 58 \ (\mathrm{mod}\ 3) &= 1. \end{aligned}$$

Somit gilt für die Lösungsmenge der simultanen Kongruenz:

$$\{58 + (3 \cdot 7 \cdot 13)k \mid k \in \mathbb{Z}\} = \{58 + 273k \mid k \in \mathbb{Z}\}$$

Teil 2

Es gilt

$$\begin{aligned} 729 \ (\mathrm{mod}\ 5) &= 4, \\ 729 \ (\mathrm{mod}\ 7) &= 1, \\ 729 \ (\mathrm{mod}\ 52) &= 1. \end{aligned}$$

Somit gilt für die Lösungsmenge der simultanen Kongruenz:

$$\{729 + (5 \cdot 7 \cdot 52)k \mid k \in \mathbb{Z}\} = \{729 + 1820k \mid k \in \mathbb{Z}\}$$

1.15.13 Aufgabe 13

Zerlege die Elemente $\{80,\ 81 \,..\, 100\} \in \mathbb{Z}[i]$ im Ring der Gaußschen Zahlen in Primfaktoren.

Lösung

Es gilt für jede gegeben Primzahl p in $\mathbb{Z}$:

(1) Aus $p = 2$ folgt, dass

$$(1+i) \qquad \text{und} \qquad (1-i)$$

primes Elemente in $\mathbb{Z}[i]$ sind (es gilt $(1+i)(1-i) = 2$).

(2) Aus allen p mit

$$p \,(\bmod\ 4) \;=\; 3$$

folgt, dass p auch in $\mathbb{Z}[i]$ ein primes Element ist.

(3) Aus allen p mit

$$p \,(\bmod\ 4) \;=\; 1$$

folgt, dass es eine Zerlegung

$$p \;=\; (a+bi)\cdot(a-bi)$$

von p gibt, so dass $(a+bi)$ und $(a-bi)$ primes Elemente in $\mathbb{Z}[i]$ sind.

Es gilt demnach für die Primfaktorenzerlegung in $\mathbb{Z}[i]$:

$$\begin{array}{rcll}
80 &=& 2^4\cdot 5 & \Rightarrow \quad 80 = (1+i)^4\cdot(1-i)^4\cdot(2+i)\cdot(2-i) \in \mathbb{Z}[i] \\
81 &=& 3^4 & \Rightarrow \quad 81 = 3^4 \in \mathbb{Z}[i] \\
82 &=& 2\cdot 41 & \Rightarrow \quad 82 = (1+i)\cdot(1-i)\cdot(5+4i)\cdot(5-4i) \in \mathbb{Z}[i] \\
83 &=& 83 & \Rightarrow \quad 83 = 83 \in \mathbb{Z}[i] \\
84 &=& 2^2\cdot 3\cdot 7 & \Rightarrow \quad 84 = (1+i)^2\cdot(1-i)^2\cdot 3\cdot 7 \in \mathbb{Z}[i] \\
85 &=& 5\cdot 17 & \Rightarrow \quad 85 = (2+i)\cdot(2-i)\cdot(4+i)\cdot(4-i) \in \mathbb{Z}[i] \\
86 &=& 2\cdot 43 & \Rightarrow \quad 86 = (1+i)\cdot(1-i)\cdot 43 \in \mathbb{Z}[i] \\
87 &=& 3\cdot 29 & \Rightarrow \quad 87 = 3\cdot(5+2i)\cdot(5-2i) \in \mathbb{Z}[i] \\
88 &=& 2^3\cdot 11 & \Rightarrow \quad 88 = (1+i)^3\cdot(1-i)^3\cdot 11 \in \mathbb{Z}[i] \\
89 &=& 89 & \Rightarrow \quad 89 = (8+5i)\cdot(8-5i) \in \mathbb{Z}[i] \\
90 &=& 2\cdot 3^2\cdot 5 & \Rightarrow \quad 90 = (1+i)\cdot(1-i)\cdot 3^2\cdot(2+i)\cdot(2-1) \in \mathbb{Z}[i] \\
91 &=& 7\cdot 13 & \Rightarrow \quad 91 = 7\cdot(3+2i)\cdot(3-2i) \in \mathbb{Z}[i] \\
92 &=& 2^2\cdot 23 & \Rightarrow \quad 92 = (1+i)^2\cdot(1-i)^2\cdot 23 \in \mathbb{Z}[i] \\
93 &=& 3\cdot 31 & \Rightarrow \quad 93 = 3\cdot 31 \in \mathbb{Z}[i]
\end{array}$$

$$
\begin{array}{lcll}
94 & = & 2 \cdot 47 & \Rightarrow \quad 94 = (1+i) \cdot (1-i) \cdot 47 \in \mathbb{Z}[i] \\
95 & = & 5 \cdot 19 & \Rightarrow \quad 95 = (2+i) \cdot (2-i) \cdot 19 \in \mathbb{Z}[i] \\
96 & = & 2^5 \cdot 3 & \Rightarrow \quad 96 = (1+i)^5 \cdot (1-i)^5 \cdot 3 \in \mathbb{Z}[i] \\
97 & = & 97 & \Rightarrow \quad 97 = (9+4i) \cdot (9-4i) \in \mathbb{Z}[i] \\
98 & = & 2 \cdot 7^2 & \Rightarrow \quad 98 = (1+i) \cdot (1-i) \cdot 7^2 \in \mathbb{Z}[i] \\
99 & = & 3^2 \cdot 11 & \Rightarrow \quad 99 = 3^2 \cdot 11 \in \mathbb{Z}[i] \\
100 & = & 2^2 \cdot 5^5 & \Rightarrow \quad 100 = (1+i)^2 \cdot (1-i)^2 \cdot (2+i)^2 \cdot (2-i)^2 \in \mathbb{Z}[i]
\end{array}
$$

Bemerkung

$(-i)$ ist eine Einheit in $\mathbb{Z}[i]$ und es gilt

$$(-i) \cdot (1+i) \; = \; (1-i).$$

Somit sind $(1-i)$ und $(1+i)$ assoziierte Primelemente in $\mathbb{Z}[i]$, daher schreibt man auch

$$(1+i)^8 \qquad \text{für} \qquad (1+i)^4 \cdot (1-i)^4.$$

1.15.14 Aufgabe 14

Sei $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$. Dann ist $\left(x^3 + x + 1\right)$ ein maximales Ideal, da $f(x)$ irreduzibel über $\mathbb{Q}$ ist. Demnach ist

$$K \; = \; \mathbb{Q}[x]/(x^3 + x + 1)$$

ein Körper.

Bestimme $(x^2 + x + 1)^{-1}$ in K.

Lösung

In K gilt

$$x^3 \; = \; -x - 1 \qquad \text{und} \qquad x^4 \; = \; x^3 \cdot x \; = \; -x^2 - x.$$

Das gesuchte Element $(x^2 + x + 1)^{-1}$ ist höchstens vom Grad 2, daher gilt

$$(x^2 + x + 1) \cdot (ax^2 + bx + c) \; = \; 1$$

mit $a, b, c \in \mathbb{Q}$. Es folgt

$$
\begin{array}{rl}
 & ax^4 + bx^3 + cx^2 + ax^3 + bx^2 + cx + ax^2 + bx + c \\
= & a(-x^2 - x) + (b+a)(-x-1) + (c+b+a)x^2 + (c+b)x + c \\
= & -bx - b - ax - a + (c+b)x^2 + (c+b-a)x + c \\
= & (c+b)x^2 + (c-2a)x + (c-b-a) \quad = \quad 1
\end{array}
$$

Es ergibt sich durch Koeffizientenvergleich das Gleichungssystem

$$\begin{aligned} c+b &= 0 \\ c-2a &= 0 \\ c-b-a &= 1. \end{aligned}$$

Man erhält die Lösungen $a=\frac{1}{3}$, $b=-\frac{2}{3}$ und $c=\frac{2}{3}$.

Die Probe zeigt, dass auch wirklich

$$(x^2+x+1)^{-1} = \frac{1}{3}\left(x^2-2x+2\right)$$

gilt.

1.15.15 Aufgabe 15

Zeige am Beispiel von $\mathbb{Z}$, das jeder euklidische Ring auch ein Hauptidealring ist.

Lösung

Durch die Abbildung

$$d(x) = \begin{cases} |x| & \text{für} \quad x \neq 0 \\ -\infty & \text{für} \quad x = 0 \end{cases}$$

wird der Integritätsring $\mathbb{Z}$ zu einem euklidischen Ring.

Sei nun $(0) \neq I \in \mathbb{Z}$ ein beliebiges Ideal und sei $a \in I$ minimal mit $a > 0$.

Sei $b \in I$ beliebig. Es muss gezeigt werden, dass es ein $s \in I$ gibt mit $b = a \cdot s$, denn dann gilt gerade $I = (a)$.

In einem euklidischen Ring gibt es eine Division mit Rest, das heißt es gibt $r, s \in I$ mit

$$\begin{aligned} & b = a \cdot s + r \qquad \text{wobei} \qquad |r| < |a| \\ \Leftrightarrow \quad & r = b - a \cdot s. \end{aligned}$$

Da b und $a \cdot s$ Elemente von I sind, folgt $r \in I$ und da $|r| < |a|$ muss $r = 0$ gelten, denn a war minimal gewählt.

Demnach ist $b = a \cdot s \in I = (a)$ und es ist gezeigt, dass $\mathbb{Z}$ ein Hauptidealring ist.

2 Körpererweiterung

In diesem Kapitel geht es um die Theorie der Polynomgleichungen.

2.1 Algebraische Körpererweiterung

2.1.1 Definition

Seien K, L zwei Körper mit $K \subset L$ und sei

$$i : K \hookrightarrow L$$

ein Ringhomomorphismus mit $i(1) = 1$.

Dann heißt $K \overset{i}{\hookrightarrow} L$ ***Körpererweiterung***.

L heißt ***Erweiterungskörper*** oder ***Oberkörper*** von K und K ist der ***Teilkörper*** oder ***Unterkörper*** von L.

2.1.2 Satz 1

Sei $K \overset{i}{\hookrightarrow} L$ ein Körpererweiterung.

Dann ist L ein K-Vektorraum.

2.1.3 Definition

Sei $K \overset{i}{\hookrightarrow} L$ ein Körpererweiterung.

Dann heißt

$$(L : K) \;=\; \dim_K(L)$$

der ***Grad*** der Körpererweiterung.

Beispiele

(1) Es gilt

$$\dim_{\mathbb{R}}(\mathbb{C}) \;=\; (\mathbb{C} : \mathbb{R}) \;=\; 2.$$

(2) Sei K ein Körper und sei $L = K(x) = \text{Quot}(K[x])$. Es gilt

$$\dim_K(L) \;=\; \dim_K(K(x)) \;\geq\; \dim_K(K[x]),$$

und da $1, x, x^2, x^3, .. \in K[x]$ linear unabhängig sind, folgt

$$\dim_K(K(x)) \;= (L : K) \;=\; \infty.$$

(3) Es gilt

$$\dim_{\mathbb{Q}}(\mathbb{R}) \;=\; (\mathbb{R} : \mathbb{Q}) \;=\; \infty.$$

2.1.4 Definition

Sei $K \overset{i}{\hookrightarrow} L$ ein Körpererweiterung.

L heißt eine ***endliche Körpererweiterung***, wenn $(L : K) < \infty$ gilt.

2.1.5 Definition und Satz

Seien $K \overset{i}{\hookrightarrow} M \overset{j}{\hookrightarrow} L$ zwei endliche Körpererweiterungen.

Dann heißt M ein ***Zwischenkörper*** von K und L und es gilt

$$\boxed{(L : K) \;=\; (L : M) \cdot (M : K).}$$

Ist eine der beiden Körpererweiterungen nicht endlich, so gilt $(L : K) = \infty$.

2.1.6 Definition

Sei $K \overset{i}{\hookrightarrow} L$ ein Körpererweiterung und sei $\alpha \in L$.

α heißt ***algebraisch*** über K, wenn es $\lambda_0, .., \lambda_n \in K$ gibt, so dass gilt:

$$\lambda_n \alpha^n + \ldots + \lambda_1 \alpha + \lambda_0 \;=\; 0$$

mit nicht alle $\lambda_0, .., \lambda_n = 0$. Ist α nicht algebraisch, so heißt α ***transzendent***.

Beispiel

Es ist $\mathbb{Q} \overset{i}{\hookrightarrow} \mathbb{R}$ eine Körpererweiterung mit $(\mathbb{R} : \mathbb{Q}) = \infty$.

$e, \pi \in \mathbb{R}$ sind transzendent über $\mathbb{Q}$.

2.1.7 Satz 2

Sei $K \overset{i}{\hookrightarrow} L$ ein endliche Körpererweiterung.

Dann sind alle $\alpha \in L$ algebraisch über K.

2.1.8 Satz 3

Sei $K \overset{i}{\hookrightarrow} L$ eine Körpererweiterung und seien $\alpha, \beta \in L$ algebraisch über K.

Dann sind auch

$$(\alpha + \beta),\ (\alpha \cdot \beta),\ \left(\frac{\alpha}{\beta}\right)\ \in\ L$$

algebraisch über K.

2.2 Einfache Körpererweiterung

2.2.1 Definition

Eine Körpererweiterung $K \overset{i}{\hookrightarrow} L$ heißt ***einfache Körpererweiterung***, wenn es ein $\alpha \in L$ gibt mit

$$L\ =\ K(\alpha)\ :=\ \left\{ \frac{p(\alpha)}{q(\alpha)}\ \middle|\ p(x), q(x) \in K[x],\ q(x) \neq 0 \right\}.$$

L wird also von einem Element α erzeugt.

$K \overset{i}{\hookrightarrow} L$ ist eine ***einfach algebraische Körpererweiterung***, wenn $L = K(\alpha)$ gilt und α algebraisch in K ist.

Beispiel

Sei $K = \mathbb{R}$. Dann ist

$$\mathbb{R}(i)\ =\ \mathbb{C}$$

eine einfach algebraische Körpererweiterung.

2.2.2 Satz 1

Sei $K \overset{i}{\hookrightarrow} L$ ein Körpererweiterung und sei $\alpha \in L$ algebraisch über K.

Dann ist die einfach algebraische Körpererweiterung $K \overset{j}{\hookrightarrow} K(\alpha)$ endlich, d.h. es gilt

$$\dim_K(K(\alpha))\ <\ \infty.$$

2.2.3 Satz 2

Sei K ein Körper.

Ist R ein Integritätsring und ein endlich dimensionaler K-Vektorraum, dann ist $K \overset{i}{\hookrightarrow} R$ eine endliche Körpererweiterung.

2.2.4 Satz 3

Sei $K \overset{i}{\hookrightarrow} L$ eine Körpererweiterung und sei $\alpha \in L$ algebraisch über K.

Dann gilt

$$K[\alpha] \;=\; K(\alpha).$$

2.2.5 Definition und Satz

Sei $K \overset{i}{\hookrightarrow} L = K(\alpha)$ eine einfach algebraische Körpererweiterung und sei $p(x)$ irreduzibel in $K[x]$ mit $p(\alpha) = 0$.

Dann gilt

$$K[x]/\left(p(x)\right) \quad \overset{\sim}{\longrightarrow} \quad L = K(\alpha).$$

$p(x)$ ist das bis auf Assoziiertheit eindeutig bestimmte ***Minimalpolynom*** von α über K (bzw. in $K[x]$) und es gilt

$$(K(\alpha) : K) \;=\; \operatorname{grad}(p(x)).$$

Ist $f(x) \in K[x]$ mit $f(\alpha) = 0$ dann gilt

$$p(x) \mid f(x).$$

Ein Minimalpolynom ist also ein normiertes Polynom mit Koeffizienten aus K, dass α als Nullstelle hat und irreduzibel in $K[x]$ ist.

2.2.6 Beispiele

(1) Sei $K = \mathbb{Q}$ und $\alpha = \sqrt{2} + 3 \in \mathbb{Q}(x) = \mathbb{R}$. Es gilt

$$\begin{aligned} \alpha - 3 &= \sqrt{2} \\ \alpha^2 - 6\alpha + 9 &= 2 \\ \alpha^2 - 6\alpha + 7 &= 0. \end{aligned}$$

Das Polynom $p(x) = x^2 - 6x + 7$ ist irreduzibel in $\mathbb{Q}[x]$, da die einzig mögliche Zerlegung $p(x) = (x - \alpha)(x - \beta)$ ist mit $\alpha, \beta \notin \mathbb{Q}$.

Da $p(x)$ eine Nullstelle bei $\alpha \in \mathbb{R}$ hat, ist $p(x)$ das Minimalpolynom von α über $\mathbb{Q}$.

(2) Es ist $p(x) = x^2 + 1$ irreduzibel über $\mathbb{Q}$, also gilt

$$\mathbb{Q}[x]/\left(x^2 + 1\right) \quad \overset{\sim}{\longrightarrow} \quad \mathbb{Q}(i).$$

(3) Sei $K = \mathbb{Q}$ und $\alpha = \sqrt{2 + \sqrt[3]{2}} \in \mathbb{Q}(x) = \mathbb{R}$. Es gilt

$$\begin{aligned} \alpha^2 &= 2 + \sqrt[3]{2} \\ \alpha^2 - 2 &= \sqrt[3]{2} \\ (\alpha^2 - 2)^3 &= 2 \\ \alpha^6 - 6\alpha^4 + 12\alpha^2 - 10 &= 0. \end{aligned}$$

Das Polynom $p(x) = x^6 - 6x^4 + 12x^2 - 10$ ist irreduzibel in $\mathbb{Q}[x]$ und hat eine Nullstelle bei α. Demnach ist $p(x)$ das Minimalpolynom von α über $\mathbb{Q}$.

Weiter gilt $(\mathbb{Q}(\alpha) : \mathbb{Q}) = \text{grad}(p(x)) = 6$.

2.2.7 Satz 4

Sei K ein Körper und $p(x) \in K[x]$ irreduzibel.

Dann ist $K \overset{i}{\hookrightarrow} K[x]/(p(x)) = L$ eine einfach algebraische Körpererweiterung und

$$\overline{x} \;=\; x + (p(x)) \;\in\; L$$

ist eine Nullstelle von $p(x)$ in L.

Beispiel

Sei $K = \mathbb{R}$ und $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Dann ist

$$\mathbb{C} \;=\; \mathbb{R}[i] \;=\; \mathbb{R}[x]/(x^2+1) \;=\; L$$

eine einfach algebraische Körpererweiterung und es gilt

$$p(\overline{x}) \;=\; \overline{x}^2 + 1 \;=\; \overline{x^2+1} \;=\; \overline{0}.$$

2.2.8 Satz von Kronecker

Sei K ein Körper und sei $f(x) \in K[x]$ beliebig, aber nicht konstant.

Dann existiert eine endlich algebraische Körpererweiterung $K \overset{i}{\hookrightarrow} L$, so dass $f(x)$ eine Nullstelle in L hat.

2.2.9 Satz 5

Sei $K \overset{i}{\hookrightarrow} L$ eine Körpererweiterung und seien $\alpha_1, .., \alpha_n \in L$ alle algebraisch über K.

Dann gilt induktiv:

(1) $K(\alpha_1, .., \alpha_n)$ ist endlich algebraisch über K.

(2) Es ist

$$\begin{aligned}\Big(K(\alpha_1, .., \alpha_n) \,:\, K\Big) \;&=\; \prod_{i=2}^{r} \Big(K(\alpha_1, .., \alpha_i) \,:\, K(\alpha_1, .., \alpha_{i-1})\Big) \\ &\leq\; \prod_{i=1}^{r} \Big(K(\alpha_i) \,:\, K\Big).\end{aligned}$$

(3) Alle $\beta \in K(\alpha_1, .., \alpha_n)$ sind algebraisch über K.

(4) Es ist $K(\alpha_1, .., \alpha_n) = K[\alpha_1, .., \alpha_n]$.

2.2.10 Definition und Satz

Sei K ein Körper und sei $f(x) \in K[x]$ beliebig, aber nicht konstant.

Eine Körpererweiterung $K \overset{i}{\hookrightarrow} L$ heißt ***minimaler Zerfällungskörper*** von $f(x)$ über K, wenn es $\alpha_1, .., \alpha_n \in L$ und ein $c \in L^\times$ gibt, so dass gilt:

(1) $f(x) \;=\; c \cdot \prod_{i=1}^{n} (x - \alpha_i)$

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

Die $\alpha_1, .., \alpha_n$ sind also alles Nullstellen von $f(x)$ und L ist der kleinste Körper, der K und alle Nullstellen enthält.

Es gilt $(L : K) \leq \text{grad}(f(x))$!.

2.2.11 Beispiele

(1) Sei $K = \mathbb{R}$ und $f(x) = x^2 + 1 \in \mathbb{R}[x]$.

Es ist $f(\pm i) = 0$ und für den minimalen Zerfallskörper L von $f(x)$ gilt

$$\begin{aligned} L \;=\; \mathbb{R}(-i, i) \;=\; \mathbb{R}(i) \;&=\; \{a_n i^n + \ldots + a_1 i + a_0 \mid a_k \in \mathbb{R}\} \\ &=\; \{a + bi \mid a, b \in \mathbb{R}\} \;=\; \mathbb{C}. \end{aligned}$$

(2) Sei $K = \mathbb{Q}$ und $f(x) = x^2 - 2 \in \mathbb{Q}[x]$.

Es gilt $f(\pm\sqrt{2}) = 0$, somit folgt für den minimalen Zerfallskörper L von $f(x)$

$$\begin{aligned} L \;=\; \mathbb{Q}(-\sqrt{2}, \sqrt{2}) \;&=\; \mathbb{Q}(\sqrt{2}) \\ &=\; \{a_n \sqrt{2}^n + \ldots + a_1 \sqrt{2} + a_0 \mid a_k \in \mathbb{Q}\} \\ &=\; \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}. \end{aligned}$$

$\mathbb{Q}(\sqrt{2})$ ist also der kleinste Körper (vgl. Seite 29), der $\mathbb{Q}$ sowie $\pm\sqrt{2}$ enthält.

(3) Sei $K = \mathbb{Q}$ und $f(x) = x^3 - 6x^2 + 11x - 6 \in \mathbb{Q}[x]$. Dann gilt

$$f(x) \;=\; (x - 1)(x - 2)(x - 3),$$

somit sind $1, 2, 3$ alle Nullstellen von $f(x)$.

Der minimaler Zerfällungskörper L von $f(x)$ ist somit

$$L \;=\; \mathbb{Q}(1, 2, 3) \;=\; \mathbb{Q} \;=\; K,$$

also der Körper K selber, da alle Nullstellen von $f(x)$ Elemente aus K sind.

2.2.12 Satz 6

Sei $\varphi : K \to \tilde{K}$ ein Körperisomorphismus.

Sei weiter L ein minimaler Zerfällungskörper von $f(x) \in K[x]$ über K und sei $\tilde{L}$ ein minimaler Zerfällungskörper von $\tilde{f}(x) \in \tilde{K}[x]$ über $\tilde{K}$.

Dann gibt es einen Körperisomorphismus $\psi : L \to \tilde{L}$, so dass das Diagramm

$$\begin{array}{ccc} L & \xrightarrow{\psi} & \tilde{L} \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & \tilde{K} \end{array}$$

kommutiert.

2.3 Rechnen mit Zerfällungskörpern

2.3.1 Beispiel

Berechnung von $(K : \mathbb{Q})$ für den Körper $K = \mathbb{Q}(\sqrt{5}, \sqrt[3]{7})$.

Betrachtet man die irreduziblen Minimalpolynome

$$x^2 - 5 \qquad \text{und} \qquad x^3 - 7,$$

so erkennt man, dass $\sqrt{5}$ und $\sqrt[3]{7}$ albebraisch über $\mathbb{Q}$ sind. Daher gilt

$$\mathbb{Q}(\sqrt{5}, \sqrt[3]{7}) \;=\; \mathbb{Q}[\sqrt{5}, \sqrt[3]{7}].$$

Weiter ist

$$\mathbb{Q}[\sqrt{5}, \sqrt[3]{7}] \;=\; \left\{ \sum_{i,j=0}^{n} a_{ij} \sqrt{5}^{\,i} \sqrt[3]{7}^{\,j} \;\middle|\; a_{ij} \in \mathbb{Q} \right\}$$

$$= \; \left\{ x_1 + x_2\sqrt{5} + x_3\sqrt[3]{7} + x_4\sqrt[3]{7}^2 + x_5\sqrt{5}\sqrt[3]{7} + x_6\sqrt{5}\sqrt[3]{7}^2 \mid x_{1,..,6} \in \mathbb{Q} \right\},$$

somit muss $(K : \mathbb{Q}) \leq 6$ gelten.

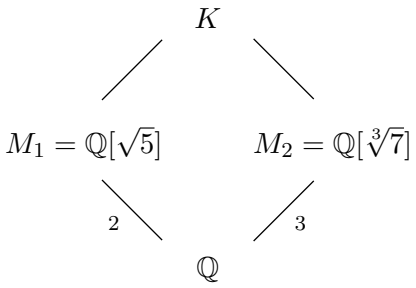
Es sind

$$M_1 \;=\; \mathbb{Q}[\sqrt{5}] \qquad \text{und} \qquad M_2 \;=\; \mathbb{Q}[\sqrt[3]{7}]$$

zwei Zwischenkörper von $\mathbb{Q}$ und K und es gilt

$$\begin{aligned} \mathbb{Q}[\sqrt{5}] &= \left\{ a + b\sqrt{5} \mid a, b \in \mathbb{Q} \right\} \\ \mathbb{Q}[\sqrt[3]{7}] &= \left\{ a + b\sqrt[3]{7} + c\sqrt[3]{7}^2 \mid a, b, c \in \mathbb{Q} \right\}. \end{aligned}$$

Demnach folgt $(M_1 : \mathbb{Q}) = 2$ und $(M_2 : \mathbb{Q}) = 3$. Man schreibt dafür auch folgendes Diagramm:



Wir wissen aber, dass die beiden Zahlen $(M_1 : \mathbb{Q})$ und $(M_2 : \mathbb{Q})$ gerade $(K : \mathbb{Q})$ teilen müssen, da M_1 und M_2 Zwischenkörper sind. Demnach gilt

$$2 \mid (K : \mathbb{Q}) \qquad \text{und} \qquad 3 \mid (K : \mathbb{Q}).$$

Also folgt $(K : \mathbb{Q}) = n \cdot 6$ mit $n \in \mathbb{N}$. Nach der Feststellung oben gilt also genau

$$(K : \mathbb{Q}) \; = \; 6.$$

2.3.2 Rechenregeln

Sei K ein Körper. Dann gilt:

(1) $K[a] = K$, falls $a \in K$

(2) $K[a, b] \; = \; K[a]$, falls $b \in K$

(3) $K[c + a] \; = \; K[a]$, falls $c \in K$

(4) $K[c \cdot a] \; = \; K[a]$, falls $c \in K$

(5) $K[a, a] \; = \; K[a]$

(6) $K[a, b] \; = \; K[a, b/a]$

(7) $K[a, b] \; = \; K[a]$, falls $b = c \cdot a$ mit $c \in K$

Beispiele

Es gilt:

(1) $\mathbb{Q}[-\sqrt{3}, \sqrt{3}] \; = \; \mathbb{Q}[\sqrt{3}] \; = \; \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$

(2) $\mathbb{Q}[1, 2, 3] \; = \; \mathbb{Q} \; = \; \{a \mid a \in \mathbb{Q}\}$

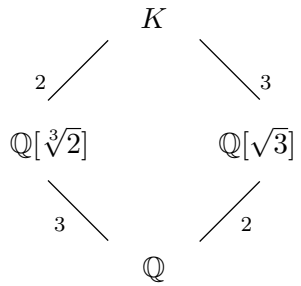
(3) $\mathbb{Q}[5 + \sqrt{7}] \; = \; \mathbb{Q}[\sqrt{7}] \; = \; \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$

(4) $\mathbb{Q}[i, -i] \; = \; \mathbb{Q}[i] \; = \; \{a + bi \mid a, b \in \mathbb{Q}\}$

(5) $\mathbb{Q}[1/2(5 - \sqrt{2})] \; = \; \mathbb{Q}[\sqrt{2}] \; = \; \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

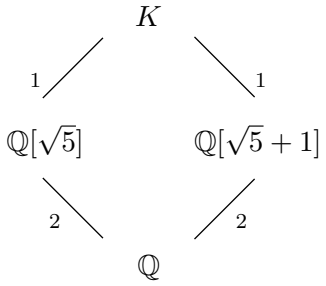
2.3.3 Beispiele für Diagramme

(1) Sei $K = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}]$. Den Grad von K über $\mathbb{Q}$ erkennt man aus folgendem Diagramm:



Es gilt also $(K : \mathbb{Q}) = 2 \cdot 3 = 3 \cdot 2 = 6$.

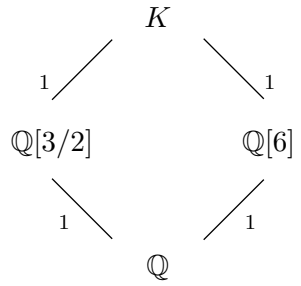
(2) Sei $K = \mathbb{Q}[\sqrt{5}, \sqrt{5}+1]$.



Es ist $(K : \mathbb{Q}[\sqrt{5}]) = (K : \mathbb{Q}[\sqrt{5}+1]) = 1$, also gilt

$$\mathbb{Q}[\sqrt{5}] \;=\; \mathbb{Q}[\sqrt{5}+1] \;=\; \mathbb{Q}[\sqrt{5}, \sqrt{5}+1].$$

(3) Es gilt $K = \mathbb{Q}[3/2, 6] = \mathbb{Q}$:



2.4 Aufgaben

2.4.1 Aufgabe 1

Sei $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ und sei $\alpha = \overline{x} \in \mathbb{Q}[x]/f(x)$.

Zeige, dass $f(x)$ irreduzibel über $\mathbb{Q}$ ist und brechne das Minimalpolynome von $(\alpha + 1)$ über $\mathbb{Q}$.

Lösung

Sei $f(x) = \sum_{i=0}^{2} a_i x^i = x^3 - 2$. In $\mathbb{Z}$ ist 2 ein primes Element und es gilt

$$2 \mid a_i \text{ für } i = 0, 1, 2 \qquad \text{und} \qquad 2 \nmid a_3 = 1 \qquad \text{und} \qquad 4 = 2^2 \nmid a_0.$$

Somit ist $f(x)$ nach Eisenstein irreduzibel über $\mathbb{Z}[x]$ und nach dem Gaußschen Lemma auch irreduzibel über $\mathbb{Q}[x]$.

Teillösung 1

Es sei $\alpha = \overline{x} = x + (f(x))$, also gilt

$$\alpha^3 - 2 \;=\; \overline{x^3} - 2 \;=\; \overline{x^3 - 2} \;\equiv\; \overline{0} \;=\; 0.$$

Daher ist nun bekannt, dass $\alpha^3 = 2$ gilt. Es folgt

$$\begin{aligned} T &= (\alpha + 1) \\ T - 1 &= \alpha \\ (T-1)^3 &= \alpha^3 \\ T^3 - 3T^2 + 3T - 1 &= 2 \\ T^3 - 3T^2 + 3T - 3 &= 0. \end{aligned}$$

Das Polynom $m(x) = x^3 - 3x^3 + 3x - 3 \in \mathbb{Q}[x]$ ist irreduzibel nach Eisenstein (mit $p = 3$) und hat eine Nullstelle bei $(\alpha + 1)$, also ist es das gesuchte Minimalpolynom.

Teillösung 2

Es sei wieder $\alpha = \overline{x} = x + (f(x))$. Da wir den Restklassenring $\mathbb{Q}[x]/f(x)$ betrachten und $f(x)$ den Grad 3 hat, kann auch das gesuchte Minimalpolynom maximal vom Grad 3 sein.

Gesucht sind demnach $a, b, c \in \mathbb{Q}$ mit

$$(\alpha + 1)^3 + a(\alpha + 1)^2 + b(\alpha + 1) + c \;=\; 0.$$

Da $\alpha^3 = 2$ gilt, folgt durch Ausmultiplizieren und Zusammenfassen

$$\begin{aligned} & \alpha^3 + 3\alpha^2 + 3\alpha + 1 + a\alpha^2 + 2a\alpha + a + b\alpha + b + c \\ = \; & 2 + (3+a)\alpha^2 + (3 + 2a + b)\alpha + (1 + a + b + c) \\ = \; & (3+a)\alpha^2 + (3 + 2a + b)\alpha + (3 + a + b + c) \;=\; 0. \end{aligned}$$

Man erhält durch Koeffizientenvergleich die drei Gleichungen

$$\begin{aligned} 3 + a &= 0, \\ 3 + 2a + b &= 0, \\ 3 + a + b + c &= 0. \end{aligned}$$

Es folgt $a = -3$, $b = 3$ und $c = -3$, somit erhält man wieder

$$m(x) \;=\; x^3 - 3x^3 + 3x - 3 \;\in\; \mathbb{Q}[x].$$

Dieses Polynom ist irreduzibel nach Eisenstein (mit $p = 3$) und hat eine Nullstelle bei $(\alpha + 1)$, also ist es das gesuchte Minimalpolynom.

2.4.2 Aufgabe 2

Sei $f(x) = x^5 - 1 \in \mathbb{Q}[x]$.

Berechne den minimalen Zerfällungskörper von $f(x)$ über $\mathbb{Q}$.

Lösung

Es ist $\text{grad}(f(x)) = 5$, somit müssen zunächst die 5 (zum Teil komplexen) Nullstellen gefunden werden.

Es gilt $f(1) = 0$ und da $f(x)$ gerade ein Kreisteilungspolynom ist, folgen die weiteren Nullstellen über die Eulerformel (mit $\varphi = 2\pi/5$):

$$\begin{aligned} \alpha_1 &= 1 \\ \alpha_2 &= e^{i\varphi} \;=\; e^{\frac{2\pi i}{5}} \\ \alpha_3 &= (\alpha_2)^2 \;=\; e^{\frac{4\pi i}{5}} \\ \alpha_4 &= (\alpha_2)^3 \;=\; e^{\frac{6\pi i}{5}} \\ \alpha_5 &= (\alpha_2)^4 \;=\; e^{\frac{8\pi i}{5}} \end{aligned}$$

Demnach folgt für den gesuchten minimalen Zerfällungskörper:

$$\begin{aligned} \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) &= \mathbb{Q}(\alpha_2, \alpha_3, \alpha_4, \alpha_5) \qquad \text{da } \alpha_1 \in \mathbb{Q} \\ &= \mathbb{Q}(\alpha_2, \alpha_2^2, \alpha_2^3, \alpha_2^4) \\ &= \mathbb{Q}(\alpha_2) \\ &= \mathbb{Q}[\alpha_2] \end{aligned}$$

2.4.3 Aufgabe 3

Es sei K ein minimaler Zerfällungskörper der Gleichung

$$x^3 - 2 \;=\; 0$$

über $\mathbb{Q}$.

Finde ein Element $\alpha \in K$ mit $\mathbb{Q}(\alpha) = K$.

Lösung

Gesucht ist zunächst ein Zerfällungskörper von $x^3 - 2$ über $\mathbb{Q}$.

Es ist $\sqrt[3]{2}$ eine Nullstelle der gegebenen Gleichung und durch Polynomdivision folgt

$$(x^3 - 2) \,:\, (x - \sqrt[3]{2}) \;=\; x^2 + \sqrt[3]{2}x + \left(\sqrt[3]{2}\right)^2 .$$

Man erhält somit die drei Nullstellen

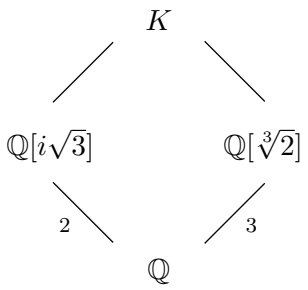
$$\sqrt[3]{2} \qquad \text{und} \qquad -\frac{\sqrt[3]{2} \pm \sqrt[3]{2}\sqrt{-3}}{2}$$

und es folgt für den minimaler Zerfällungskörper:

$$\begin{aligned} K &= \mathbb{Q}\left(\sqrt[3]{2}, -\frac{\sqrt[3]{2} \pm \sqrt[3]{2}\sqrt{-3}}{2}\right) \\ &= \mathbb{Q}\left(\sqrt[3]{2},\, \sqrt[3]{2}\sqrt{-3}\right) \\ &= \mathbb{Q}\left(\sqrt[3]{2},\, \sqrt{-3}\right) \\ &= \mathbb{Q}\left(\sqrt[3]{2},\, i\sqrt{3}\right) \\ &= \{a_0 + a_1\sqrt[3]{2} + \ldots + a_4\sqrt[3]{2}^2 + a_5\sqrt[3]{2}^2 i\sqrt{3} \mid a_0, .., a_5 \in \mathbb{Q}\} \end{aligned}$$

Demach ist $(K : \mathbb{Q}) \leq 6$.

Weiter gilt:



Also gilt $2 \mid (K:\mathbb{Q})$ und $3 \mid (K:\mathbb{Q})$ und somit folgt $(K:\mathbb{Q}) = 6$.

Sei nun $\alpha = \sqrt[3]{2}i\sqrt{3} \in K$. Dann ist $\mathbb{Q}(\alpha)$ ein Erweiterungskörper von $\mathbb{Q}$ und da $\mathbb{Q}(\alpha) \neq \mathbb{Q}$ gilt $(\mathbb{Q}(\alpha):\mathbb{Q}) = d \in \{2,3,6\}$, da d ein Teiler von 6 sein muss.

Annahme: $d = 2$. Dann gibt es ein normiertes Polynom vom Grad 2 in $\mathbb{Q}[x]$, das α als Nullstelle hat:

$$\begin{aligned} f(x) &= x^2 + \lambda x + \mu \\ \Rightarrow\ f(\alpha) &= -3\left(\sqrt[3]{2}\right)^2 + \lambda \cdot (\sqrt[3]{2}i\sqrt{3}) + \mu \cdot 1 \ = \ 0 \end{aligned}$$

Da $\{\sqrt[3]{2}^2, \sqrt[3]{2}i\sqrt{3}, 1\}$ aber linear unabhängig über $\mathbb{Q}$ sind, folgt $-3 = \lambda = \mu = 0$. Dieser Widerspruch zeigt, dass die Annahme falsch ist.

Annahme: $d = 3$. Ganz analog folgt auch das diese Annahme falsch ist.

Somit muss $d = 6$ gelten, also $(K:\mathbb{Q}(\alpha)) = 1$ und somit folgt $K = \mathbb{Q}(\alpha)$.

2.4.4 Aufgabe 4

Sei $K = \mathbb{Q}(\sqrt{5}, \sqrt{7}) \subset \mathbb{R}$.

(1) Berechene $(\sqrt{5} + \sqrt{7})^{-1}$ als Ausdruck in K.

(2) Berechne $(K:\mathbb{Q})$.

(3) Finde ein Elemente $\alpha \in K$ mit $K = \mathbb{Q}(\alpha)$.

(4) Berechne das Minimalpolynom von α über $\mathbb{Q}$.

Lösung Teil 1

Es gilt:

$$(\sqrt{5} + \sqrt{7})^{-1} \ = \ \frac{1}{(\sqrt{5} + \sqrt{7})} \ = \ \frac{\sqrt{5} - \sqrt{7}}{5 - 7} \ = \ -\frac{1}{2}\sqrt{5} + \frac{1}{2}\sqrt{7} \ \in \ K$$

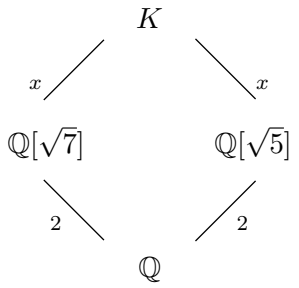
Lösung Teil 2

Es ist

$$\begin{aligned} \mathbb{Q}(\sqrt{5}, \sqrt{7}) &= \left\{ \sum_{i,j=0}^{n} a_{ij}\sqrt{5}^i\sqrt{7}^j \;\middle|\; a_{ij} \in \mathbb{Q} \right\} \\ &= \{a\sqrt{35} + b\sqrt{7} + c\sqrt{5} + d \mid a,b,c,d \in \mathbb{Q}\} \end{aligned}$$

Es folgt also $(K:\mathbb{Q}) \leq 4$.

Weiter gilt



und da 2 ein Teiler von 4 ist, muss auch $x \mid 2$ gelten.

Da $\mathbb{Q}[\sqrt{7}] \neq \mathbb{Q}[\sqrt{5}]$ gilt, folgt $x = 2$ und somit ist $(K : \mathbb{Q}) = 4$.

Lösung Teil 3

Sei $\alpha = \sqrt{5} + \sqrt{7} \in K$. Dann ist $\mathbb{Q}(\alpha)$ ein echter Erweiterungskörper von $\mathbb{Q}$ und somit ist $(\mathbb{Q}(\alpha) : \mathbb{Q}) = d \in \{2, 4\}$. Da es aber kein normiertes Polynom vom Grad 2 in $\mathbb{Q}[x]$ gibt, das α als Nullstellt hat, gilt $d = 4$ und somit ist $\mathbb{Q}(\alpha) = K$.

Lösung Teil 4

Berechnung des Minimalpolynoms von α über $\mathbb{Q}$:

$$\begin{aligned} \sqrt{5} + \sqrt{7} &= T \\ 5 + 2\sqrt{35} + 7 &= T^2 \\ 2\sqrt{35} &= T^2 - 12 \\ T^4 - 24T^2 + 4 &= 0 \end{aligned}$$

Das Polynom $p(x) = x^4 - 24x^2 + 4 \in \mathbb{Q}[x]$ hat also eine Nullstelle bei α und da $\operatorname{grad}(p(x)) = (\mathbb{Q}(\alpha) : \mathbb{Q}) = 4$ gilt, ist $p(x)$ auch irreduzibel über $\mathbb{Q}$.

Somit ist $p(x)$ das gesuchte Minimalpolynom.

2.4.5 Aufgabe 5

Sei $f(x) = x^3 - 1 \in \mathbb{Q}[x]$.

Bestimme den minimalen Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ und dessen Grad über $\mathbb{Q}$.

Lösung

$f(x)$ ist ein Kreisteilungspolynom und hat eine Nullstelle bei 1. Es gilt

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1$$

(siehe Seite 19). Sei $\zeta^3 = 1$ und $\zeta \neq 1$, also die eindeutig bestimmte dritte Einheitswurzel. Dann sind ζ und ζ^2 die beiden weiteren Nullstellen von $f(x)$ und es folgt

$$\mathbb{Q}(\zeta, \zeta^2, 1 = \zeta^3) \;=\; \mathbb{Q}(\zeta, \zeta^2) \;=\; \mathbb{Q}(\zeta).$$

Da ζ und ζ^2 die Nullstellen von $x^2 + x + 1$ sind, gilt $\zeta^2 = -\zeta - 1$. Demnach gilt

$$\mathbb{Q}(\zeta) \;=\; \{a + b\zeta \mid a, b \in \mathbb{Q}\}.$$

Der Grad von $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$ ist also 2.

2.4.6 Aufgabe 6

Sei $f(x) = x^5 - 1 \in \mathbb{Q}[x]$.

Bestimme den minimalen Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ und dessen Grad über $\mathbb{Q}$.

Lösung

$f(x)$ ist ein Kreisteilungspolynom und hat eine Nullstelle bei 1. Es gilt

$$\frac{x^5 - 1}{x - 1} \;=\; x^4 + x^3 + x^2 + x + 1.$$

Sei $\zeta^5 = 1$ und $\zeta \neq 1$, also die eindeutig bestimmte fünfte Einheitswurzel. Es sind also $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4\}$ alle Nullstellen von $f(x)$ und es folgt somit

$$\mathbb{Q}(1, \zeta, \zeta^2, \zeta^3, \zeta^4) \;=\; \mathbb{Q}(\zeta).$$

Weiter gilt $\zeta^4 = -\zeta^3 - \zeta^2 - \zeta - 1$. Demnach ist

$$\mathbb{Q}(\zeta) \;=\; \{a + b\zeta + c\zeta^2 + d\zeta^3 \mid a, b, c, d \in \mathbb{Q}\}.$$

und der Grad von $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$ ist 4 (vergleiche Seite 59).

3 Galoistheorie

3.1 Galoiserweiterungen

3.1.1 Definition

Sei K ein Körper.

Ein Polynom $f(x) \in K[x]$ heißt ***separabel*** über K, wenn jeder Faktor in der irreduziblen Zerlegung von $f(x)$ über K nur einfache Nullstellen in einem minimalen Zerfällungskörper von $f(x)$ besitzt.

Eine Körpererweiterung L von K heißt ***separabel***, wenn jedes Polynom aus $L[x]$ separabel über K ist.

3.1.2 Satz 1

Sei K ein Körper mit $\text{char}(K) = 0$.

Dann sind alle Polynome $f(x) \in K[x]$ separabel über K.

3.1.3 Definition

Sei K ein Körper.

Ein minimaler Zerfällungskörper L eines beliegiben Polynoms $f(x) \in K[x]$ ist eine ***normale Erweiterung*** von K.

Beispiele

(1) Sei $\zeta^3 = 1$ mit $\zeta \neq 1$, also die dritte primitive Einheitswurzel.

$\mathbb{Q}(\zeta)$ ist eine normale Erweiterung von $\mathbb{Q}$, da ζ und ζ^2 Nullstellen von

$$f(x) \;=\; x^2 + x + 1 \;\in\; \mathbb{Q}[x]$$

sind und somit $\mathbb{Q}(\zeta)$ ein minimaler Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ ist.

(2) Sei $\zeta^3 = 1$ mit $\zeta \neq 1$, also die dritte primitive Einheitswurzel.

$\mathbb{Q}(\sqrt[3]{2})$ ist keine normale Erweiterung von $\mathbb{Q}$. Betrachtet man zum Beispiel das Polynom

$$f(x) \;=\; x^3 - 2 \;\in\; \mathbb{Q}[x],$$

so ist $f(x)$ irreduzibel über $\mathbb{Q}$ und $\sqrt[3]{2}$ ist eine Nullstelle von $f(x)$. Da aber $\{\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2\}$ alle Nullstellen von $f(x)$ sind, ist $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ ein minimaler Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ und die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})$ enthält nicht alle Nullstellen von $f(x)$.

Es gibt kein Polynom in $\mathbb{Q}[x]$, dass nur $\sqrt[3]{2}$ oder Vielfache davon als Nullstellen hat.

3.1.4 Definition und Satz

Sei L ein Körper.

Die Menge aller Automorphismen von L bildet die Gruppe $\mathrm{Aut}(L)$.

Für eine Untergruppe $H \subset \mathrm{Aut}(L)$ ist die Menge

$$\boxed{L^H \;:=\; \{x \in L \mid \varphi(x) = x \;\forall\; \varphi \in H\}}$$

ein Unterkörper von L und heißt ***Fixkörper***.

3.1.5 Satz 2

Sei L ein Körper und $H \subset \mathrm{Aut}(L)$ eine endliche Gruppe von Automorphismen.

Dann gilt für den Fixkörper L^H

$$\big(L : L^H\big) \;=\; |H|.$$

3.1.6 Definition und Satz

Sei K ein Körper und sei L ein minimaler Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$.

Dann heißt L eine ***galoissche Erweiterung*** von K.

Die Gruppe

$$\mathrm{Aut}_K(L) \;:=\; \{\varphi : L \to L \mid \varphi \in \mathrm{Aut}(L) \text{ mit } \varphi|_K = id\}$$

von Automorphismen heißt ***Galoisgruppe***.

$$\begin{array}{ccc} L & \xrightarrow{\varphi} & L \\ \cup & & \cup \\ K & \xrightarrow{id} & K \end{array}$$

Schreibweise:

$$\mathrm{Gal}(L/K) \;:=\; \mathrm{Aut}(L/K) \;:=\; \mathrm{Aut}_K(L)$$

Ist L über K endlich, so ist auch $\mathrm{Gal}(L/K)$ endlich und es gilt

$$|\mathrm{Gal}(L/K)| \;=\; |\mathrm{Aut}_K(L)| \;=\; (L:K).$$

Beispiel

Es ist $f(x) = x^2 + 1 \in \mathbb{R}[x]$ ein separables Polynom, denn $\{i, -i\}$ sind einfache Nullstellen von $f(x)$ in dem minimalen Zerfällungskörper $\mathbb{C}$.

Demnach ist $\mathbb{C}$ galoissch über $\mathbb{R}$ und es gilt

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \;=\; \{id, \varphi\}$$

mit $\varphi(a + bi) = a - bi$.

Dieses Ergebnis stimmt auch mit $(\mathbb{C}:\mathbb{R}) = |\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$ überein.

3.1.7 Satz 3

Sei K ein Körper, sei $f(x) \in K[x]$ ein separables Polynom vom Grad r und sei L ein minimaler Zerfällungskörper von $f(x)$ über K.

Dann ist L galoissch über K und es gibt einen injektiven Homomorphismus

$$\sigma : \mathrm{Gal}(L/K) \;\to\; S_r.$$

Dabei ist S_r die Permutationengruppe aus r Elementen.

3.1.8 Satz 4

Sei L eine endliche Körpererweiterung eines Körpers K.

Dann sind äquivalent:

(1) L ist galoissch über K

(2) $L^G = K$ mit $G = \mathrm{Gal}(L/K)$

(3) L ist ein Zerfällungskörper eines sparablen Polynoms $f(x) \in K[x]$

3.2 Galoisgruppen und Zwischenkörper

3.2.1 Satz 1

Sei L galoissch über K und seien $K \subset M_1 \subset M_2 \subset L$ zwei Zwischenkörper von K und L.

Dann gilt

$$\mathrm{Gal}(L/L) \;\subset\; \mathrm{Gal}(L/M_2) \;\subset\; \mathrm{Gal}(L/M_1) \;\subset\; \mathrm{Gal}(L/K).$$

3.2.2 Satz 2

Seien $H_2 = \mathrm{Gal}(L/M_2) \subset H_1 = \mathrm{Gal}(L/M_1) \subset \mathrm{Gal}(L/K)$ zwei Untergruppen von $\mathrm{Gal}(L/K)$.

Dann gilt

$$K \ \subset \ L^{H_1} \ \subset \ L^{H_2} \ \subset \ L.$$

3.2.3 Folgerung

Sei L galoissch über K.

Dann ist jeder Zwischenkörper $K \subset M \subset L$ von der Form

$$M \ = \ L^H$$

mit passender Untergruppe $H = \mathrm{Aut}_M(L) = \mathrm{Gal}(L/M)$.

D.h. es gibt nur endlich viele Zwischenkörper M, da es nur endlich viele Untergruppen $H \subset G$ gibt.

3.3 Hauptsatz der Galoistheorie

Der Hauptsatz der Galoistheorie fasst noch einmal alle wichtigen Erkenntnisse zusammen und liefert eine Übersicht über alle Zwischenkörper einer Galoiserweiterung.

3.3.1 Hauptsatz der Galoistheorie

Sei K ein Körper und sei L ein minimaler Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$.

Dann ist L galois über K, $G = \mathrm{Gal}(L/K)$ ist die zugehörige Galoisgruppe und es besteht folgende Bijektion von Mengen:

$$\begin{array}{rcl} \varphi : \{M \mid K \subset M \subset L,\ M \text{ Körper}\} & \to & \{H \mid H \subset G \text{ Untergruppe}\} \\ M & \mapsto & \mathrm{Gal}(L/M) \end{array}$$

mit der Umkehrabbildung

$$\begin{array}{rcl} \psi : \{H \mid H \subset G \text{ Untergruppe}\} & \to & \{M \mid K \subset M \subset L,\ M \text{ Körper}\} \\ H & \mapsto & L^H \end{array}$$

Dabei gilt:

(1) φ und ψ sind inklusionsumkehrend (siehe Seite 57).

(2) $|\mathrm{Gal}(L/M)| = (L : M)$

(3) $(M : K) = |G| \,/\, |\mathrm{Gal}(L/M)|$

(4) Sind H_1 und H_2 konjugierte Untergruppen von G, d.h. es gibt ein $g \in \mathrm{Gal}(L/K)$ mit $gH_1g^{-1} = H_2$, dann ist L^{H_1} über K isomorph zu L^{H_2}.

(5) Sind M_1 und M_2 zwei über K isomorphe Zwischenkörper von K und L, dann sind $H_1 = \mathrm{Gal}(L/M_1)$ und $H_2 = \mathrm{Gal}(L/M_1)$ konjugierte Untergruppen von G.

(6) Ist $H = N$ ein Normalteiler in G, dann ist L^H eine galoissche Erweiterung von K. Die Galoisgruppe ist dann G/H.

(7) Ist M mit $K \subset M \subset L$ ein Zwischenkörper und ist M eine galoissche Erweiterung von K, dann ist $H = \mathrm{Gal}(L/M)$ ein Normalteiler von G und $\mathrm{Gal}(M/K)$ ist isomorph zu G/H.

(8) Sind M_1 und M_2 zwei über K isomorphe Zwischenkörper von K und L, dann gibt es ein $u \in \mathrm{Gal}(L/K)$, so dass für die Gruppe der Isomophismen zwischen M_1 und M_2 gilt:

$$\mathrm{Iso}_K(M_1, M_2) \;=\; u \cdot \mathrm{Gal}(L/M_1)$$

3.3.2 Beispiel

Berechne die Galoisgruppe eines minimalen Zerfällungskörpers K der Gleichung

$$f(x) \;=\; x^5 - 1 \;=\; 0$$

über $\mathbb{Q}$ und bestimme alle Zwischenkörper M mit $\mathbb{Q} \subset M \subset K$.

Lösung

Um den minimalen Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ zu berechnen, müssen zunächst die Nullstellen von $f(x)$ berechnet werden.

Sei dazu $\zeta^5 = 1$ und $\zeta \neq 1$. Damit ist ζ die endeutich bestimmte fünfte primitive Einheitswurzel $\left(\text{es ist somit } \zeta = e^{\frac{2\pi i}{5}}\right)$.

Somit sind $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ Nullstellen des (irreduziblen) Kreisteilungspolynoms

$$\frac{x^5 - 1}{x - 1} \;=\; x^4 + x^3 + x^2 + x + 1.$$

Damit sind $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4\}$ alle Nullstellen von $f(x)$ und es folgt für den gesuchten Zerfällungskörper

$$\begin{aligned} K &= \mathbb{Q}[1, \zeta, \zeta^2, \zeta^3, \zeta^4] \\ &= \mathbb{Q}[\zeta] \\ &= \left\{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \mid a_0, .., a_3 \in \mathbb{Q}\right\}. \end{aligned}$$

Da $\text{char}(\mathbb{Q}) = 0$ gilt, ist K separabel und somit ist eine galoissche Erweiterung über K. Es gilt

$$(K : \mathbb{Q}) \;=\; 4 \qquad \Leftrightarrow \qquad |\text{Gal}(K/\mathbb{Q})| \;=\; 4.$$

Um die Galoisgruppe zu bestimmen sind nun 4 Automorphismen $\varphi : K \to K$ gesucht mit $\varphi|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Die Abbildungen müssen so definiert sein, dass $\varphi(\zeta)$ eine Nullstelle von $f(x)$ ist, denn es gilt

$$\varphi(\zeta)^4 + \varphi(\zeta)^3 + \varphi(\zeta)^2 + \varphi(\zeta) + 1 \;=\; \varphi(\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) \;=\; \varphi(0) \;=\; 0.$$

Erfüllt wird diese Bedingung von folgenden Abbildungen:

$$\begin{aligned} \varphi_1 : K \to K \quad &\text{mit} \quad \varphi_1(\zeta) = \zeta^2 \\ \varphi_1^2 = \varphi_2 : K \to K \quad &\text{also} \quad \varphi_2(\zeta) = \zeta^4 \\ \varphi_1^3 = \varphi_3 : K \to K \quad &\text{also} \quad \varphi_3(\zeta) = \zeta^3 \\ id = \varphi_2^4 = \varphi_4 : K \to K \quad &\text{also} \quad \varphi_4(\zeta) = \zeta \end{aligned}$$

Die gesuchte Galoisgruppe ist somit

$$\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \;=\; \{id, \varphi_1, \varphi_1^2, \varphi_1^3\}.$$

$\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ ist isomorph zu $\mathbb{Z}/4\mathbb{Z}$ und da $\mathbb{Z}/4\mathbb{Z}$ drei Untergruppen besitzt, hat auch $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ genau drei Untergruppen, nämlich

$$H_1 \;=\; \{id, \varphi_1, \varphi_1^2, \varphi_1^3\} \qquad \text{und} \qquad H_2 \;=\; \{id\} \qquad \text{und} \qquad H_3 \;=\; \{id, \varphi_1^2\}.$$

Somit gibt es drei gesuchte Zwischenkörper:

$$\begin{aligned} \mathbb{Q}[\zeta]^{H_1} &= \mathbb{Q} \\ \mathbb{Q}[\zeta]^{H_2} &= \mathbb{Q}[\zeta] \\ \mathbb{Q}[\zeta]^{H_3} &= \mathbb{Q}[\zeta + \zeta^3] \end{aligned}$$

Den letzten Zwischenkörper erhält man aus der Betrachtung heraus, dass für alle $a_0, .., a_3 \in \mathbb{Q}$

$$\varphi_1^2(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3) \;=\; a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$$

gelten muss.

3.3.3 Bemerkung

Ist eine Galoisgruppe $\text{Gal}(L/K)$ zyklisch und von der Ordnung n, so wird diese Gruppe von einem Element φ erzeugt.

$\text{Gal}(L/K)$ ist daher isomorph zu $(\mathbb{Z}/n\mathbb{Z})^\times$. Durch diese Betrachtung können zunächst sehr viel einfacher die Untergruppen von $(\mathbb{Z}/n\mathbb{Z})^\times$ bestimmt werden um somit auf die Untergruppen von $\text{Gal}(L/K)$ zu schließen. Folglich können nun nach dem Hauptsatz der Galoistheorie alle Zwischenkörver von K und L bestimmen werden.

3.4 Ergänzungen

3.4.1 Satz 1

Sei L eine galoissche Erweiterung von K und sei $f(x) \in K[x]$ ein irreduzibles Polynom.

Dann zerlegt sich $f(x)$ in L in

$$f(x) \;=\; f_1(x) \cdot \ldots \cdot f_r(x),$$

wobei die Polynome $f_1(x), .., f_r(x)$ alle denselben Grad haben.

3.4.2 Satz 2

Sei L eine galoissche Erweiterung von K und sei $f(x) \in K[x]$ ein irreduzibles Polynom mit einer Nullstelle in L.

Dann hat $f(x)$ alle Nullstellen in L, d.h. $f(x)$ zerfällt in Linearfaktoren.

3.4.3 Satz 3

Sei L ein Körper und sei

$$G \;\subset\; \mathrm{Aut}(L) \;=\; \{\varphi : L \to L \mid \varphi \text{ ist ein Automorphismus}\}$$

eine endliche Untergruppe von $\mathrm{Aut}(L)$.

Dann ist L galoissch über K mit

$$K \;:=\; L^G \;=\; \{x \in L \mid \varphi(x) = x \;\forall\; \varphi \in G\}.$$

Es gilt $\mathrm{Gal}(L/K) = G$, also $(L : K) = |G|$.

3.5 Aufgaben

3.5.1 Aufgabe 1

Berechne die Galoisgruppe eines minimalen Zerfällungskörpers K der Gleichung

$$f(x) \;=\; (x^2 - 3)(x^2 - 5) \;=\; 0$$

über $\mathbb{Q}$ und bestimme alle Zwischenkörper M mit $\mathbb{Q} \subset M \subset K$.

Lösung

Es ist $f(x) = (x^2-3)(x^2-5) \in \mathbb{Q}[x]$ und $\{\pm\sqrt{3}, \pm\sqrt{5}\}$ sind die vier Nullstellen von $f(x)$. Somit gilt für den minimalen Zerfällungskörper K von $f(x)$ über $\mathbb{Q}$

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{3}, -\sqrt{3}, \sqrt{5}, -\sqrt{5}) \\ &= \mathbb{Q}(\sqrt{3}, \sqrt{5}) \\ &= \mathbb{Q}[\sqrt{3}, \sqrt{5}] \\ &= \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{3}\sqrt{5} \mid a, b, c, d \in \mathbb{Q}\}. \end{aligned}$$

Da K ein minimaler Zerfällungskörper von $f(x)$ ist und $f(x)$ keine mehrfachen Nullstellen besitzt (und somit insbesondere separabel ist), ist K galoissch über $\mathbb{Q}$. Es gilt $(K : \mathbb{Q}) = 4$, also bestehe auch die gesuchte Galoisgruppe aus vier Elementen.

Für die gesuchten Automorphismen φ gilt nun für alle $a, b, c, d \in \mathbb{Q}$

$$\varphi(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{3}\sqrt{5}) \;=\; a + b\varphi(\sqrt{3}) + c\varphi(\sqrt{5}) + d\varphi(\sqrt{3})\varphi(\sqrt{5}),$$

da $\varphi|_{\mathbb{Q}}$ die Identität sein soll.

Es muss also untersucht werden, worauf jeweils $\sqrt{3}$ und $\sqrt{5}$ abgebildet wird.

Es gilt $\varphi(\sqrt{3})^2 = \varphi(\sqrt{3}^2) = \varphi(3) = 3$, daher folgt $\varphi(\sqrt{3}) = \pm 3$ und analog $\varphi(\sqrt{5}) = \pm 5$. Durch diese Einschränkung kann es also nur noch 4 gesuchte Abbildungen geben.

Seien nun $\varphi_1, .., \varphi_4 : K \to K$ mit $\varphi_{1,..,4}|_{\mathbb{Q}} = id_{\mathbb{Q}}$ und

$$\begin{array}{rclcrcl} \varphi_1(\sqrt{3}) &=& \sqrt{3} & \text{und} & \varphi_1(\sqrt{5}) &=& \sqrt{5} \\ \varphi_2(\sqrt{3}) &=& \sqrt{3} & \text{und} & \varphi_2(\sqrt{5}) &=& -\sqrt{5} \\ \varphi_3(\sqrt{3}) &=& -\sqrt{3} & \text{und} & \varphi_3(\sqrt{5}) &=& \sqrt{5} \\ \varphi_4(\sqrt{3}) &=& -\sqrt{3} & \text{und} & \varphi_4(\sqrt{5}) &=& -\sqrt{5}. \end{array}$$

Da es wegen $(K : \mathbb{Q}) = 4$ auch vier Automorphismen geben muss, sind die Abbildungen $\varphi_1, .., \varphi_4$ auch tatsächlich bijektiv.

Daraus ergibt sich nun die gesuchte Galoisgruppe

$$\mathrm{Gal}(K/\mathbb{Q}) \;=\; \{\varphi_1 = id,\, \varphi_2,\, \varphi_3,\, \varphi_4\},$$

welche isomorph ist zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Die Galoisgruppe hat also genau 5 Untergruppen:

$$\begin{aligned} H_1 &= \{id,\, \varphi_2,\, \varphi_3,\, \varphi_4\} \\ H_2 &= \{id\} \\ H_3 &= \{id,\, \varphi_2\} \\ H_4 &= \{id,\, \varphi_3\} \\ H_5 &= \{id,\, \varphi_4\} \end{aligned}$$

Ist H eine beliebige Untergruppe einer Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$, so ist der zugehörige Zwischenkörper von der Form

$$K^H \;=\; \{x \in K \mid \varphi(x) = x \;\forall\; \varphi \in H\}.$$

Nach dem Hauptsatz der Galoistheorie gibt es nun auch genau fünf gesuchte Zwischenkörper:

$$\begin{array}{rcccl} M_1 & = & K^{H_1} & = & \mathbb{Q} \\ M_2 & = & K^{H_2} & = & \mathbb{Q}(\sqrt{3},\sqrt{5}) \;=\; K \\ M_3 & = & K^{H_3} & = & \mathbb{Q}(\sqrt{3}) \\ M_4 & = & K^{H_4} & = & \mathbb{Q}(\sqrt{5}) \\ M_5 & = & K^{H_5} & = & \mathbb{Q}(\sqrt{3}\sqrt{5}) \end{array}$$

Dabei ist zum Beispiel $K^{H_3} = \mathbb{Q}(\sqrt{3})$, da $\varphi(\sqrt{3}) = \sqrt{3}$ für alle $\varphi \in H_3$ gilt und für $\varphi_2 \in H_3$ gerade $\varphi(\sqrt{5}) \neq \sqrt{5}$ ist.

3.5.2 Aufgabe 2

Berechne die Galoisgruppe der Gleichung $x^3 - 2 = 0$ über $\mathbb{Q}$ und bestimme alle Zwischenkörper M mit $\mathbb{Q} \subset M \subset K$.

Betrachte dasselber über den reellen Zahlen $\mathbb{R}$.

Lösung

Sei $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ und sei $\zeta^3 = 1$ und $\zeta \neq 1$ (somit ist ζ die dritte primitive Einheitswurzel).

Dann sind $\alpha = \sqrt[3]{2}$, $\alpha\zeta$ und $\alpha\zeta^2$ die drei Nullstellen von $f(x)$.

Für den minimalen Zerfällungskörper von $f(x)$ über $\mathbb{Q}$ gilt also

$$\begin{array}{rcl} K & = & \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2) \\ & = & \mathbb{Q}(\alpha, \zeta) \\ & = & \mathbb{Q}[\alpha, \zeta]. \end{array}$$

Da $f(x)$ keine mehrfachen Nullstellen in $\mathbb{Q}$ besitzt, ist $f(x)$ separable und somit ist der minimale Zerfällungskörper K von $f(x)$ galoissch über $\mathbb{Q}$.

Es gilt $(K : \mathbb{Q}) = 6$, somit besteht auch die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ aus sechs Elementen.

Für die gesuchten Automorphismen muss nun untersucht werden, worauf α und ζ abgebildet werden.

Seien dazu $\varphi, \psi : K \to K$ mit

$$\begin{array}{rclcrcl} \varphi(\alpha) & = & \alpha\zeta & \text{und} & \varphi(\zeta) & = & \zeta \\ \psi(\alpha) & = & \alpha & \text{und} & \psi(\zeta) & = & \zeta^2. \end{array}$$

Daraus ergibt sich die gesuchte Galoisgruppe aus sechs Automorphismen:

$$\mathrm{Gal}(K/\mathbb{Q}) \;=\; \{id = \varphi^3 = \psi^2,\ \varphi,\ \varphi^2,\ \psi,\ \varphi\psi,\ \varphi^2\psi\}$$

Da $\mathrm{Gal}(K/\mathbb{Q})$ isomorph zur Permutationengruppe S_3 ist und S_3 genau sechs Untergruppen hat, erhält man auch genau sechs Zwischenkörper, nämlich

$$K, \qquad \mathbb{Q}(\zeta), \qquad \mathbb{Q}(\alpha), \qquad \mathbb{Q}(\alpha\zeta), \qquad \mathbb{Q}(\alpha\zeta^2) \quad \text{und} \quad \mathbb{Q}.$$

Betrachtet man den minimalen Zerfällungskörper L von $f(x)$ über $\mathbb{R}$, so erhält man

$$L \;=\; \mathbb{R}(\zeta) \;=\; \mathbb{R}[\zeta] \;\subset\; \mathbb{C}.$$

Wiederum ist L galoissch über $\mathbb{R}$, es gilt $(L : \mathbb{R}) = 2$ und da auch $(\mathbb{C} : \mathbb{R}) = 2$ gilt folgt $(\mathbb{C} : L) = 1$, also $L = \mathbb{C}$. Somit besteht auch die Galoisgruppe $\mathrm{Gal}(L/\mathbb{R})$ aus zwei Elementen.

Sei $\varphi' : L \to L$ mit $\varphi'(\zeta) = \zeta^2$. Dann ist $\mathrm{Gal}(L/\mathbb{R}) = \{id, \varphi'\}$.

Die Körper L und $\mathbb{R}$ besitzten nur zwei Zwischenkörper, nämlich L und $\mathbb{R}$ selber, da $\{id\}$ und $\{id, \varphi'\}$ die einzigen Untergruppen von $\mathrm{Gal}(L/\mathbb{R})$ sind.

4 Anwendungen

4.1 Endliche Körper

Einleitung

Sei $\mathbb{F}_q$ ein Körper aus q Elementen.

Dann gilt $\text{char}(\mathbb{F}_q) = p > 0$. Demnach enhält $\mathbb{F}_q$ auch $\mathbb{F}_p$ und es ist $\mathbb{F}_p$ isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Somit ist $\mathbb{F}_q$ ein d dimensionaler Vektorraum über $\mathbb{F}_p$. Es folgt

$$\mathbb{F}_q \quad \xrightarrow{\sim} \quad (\mathbb{F}_p)^d, \qquad \text{also} \qquad |\mathbb{F}_q| \;=\; q \;=\; p^d.$$

Sei $(\mathbb{F}_q^\times, \cdot\,)$ die multiplikative Einheitengruppe von $\mathbb{F}_q$.

Dann gilt für alle $a \in \mathbb{F}_q^\times$

$$a^{q-1} \;=\; 1,$$

also gilt auch für alle $a \in \mathbb{F}_q^\times \cup \{0\} = \mathbb{F}_q$

$$a^q \;=\; a.$$

Betrachtet man andersherum die Gleichung

$$x^q - x \;=\; 0,$$

so hat diese in $\mathbb{F}_q$ höchstens q Lösungen.

Zusammengefasst ist $\mathbb{F}_q$ also ein minimaler Zerfällungskörper der Gleichung

$$\boxed{x^q - x = 0}$$

über $\mathbb{F}_p$.

Nach der Galoistheorie ist $\mathbb{F}_q$ nun ein bis auf Isomorphie eindeutig bestimmter Körper über $\mathbb{F}_p$ aus q Elementen.

Da die Gleichung $x^q - x = 0$ keine mehrfachen Nullstellen hat, ist $\mathbb{F}_q$ galoissch über $\mathbb{F}_p$.

Galoisgruppe

Es ist bereits bekannt, dass $(\mathbb{F}_q : \mathbb{F}_p) = d$ gilt, somit besteht auch die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ aus d Elementen.

Sei F der Frobeniushomomophismus (siehe Seite 31), also

$$\begin{aligned} F : \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto x^p. \end{aligned}$$

Dann gilt

$$\begin{aligned} F^d : \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto (F \circ .. \circ F)(x^p) = x^{p^d} = x^q = x. \end{aligned}$$

Somit ist F^d die Identität auf $\mathbb{F}_q$ und für die Galoisgruppe gilt

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \{id, F, F^2, \ldots, F^{d-1}\}.$$

Zwischenkörper

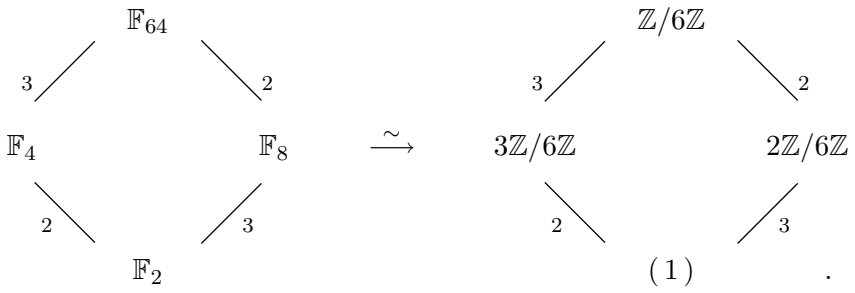
Die Galoisgruppe ist isomorph zu $\mathbb{Z}/d\mathbb{Z}$ und da es zu jedem Teiler d' von d eine Untergruppe H von $\mathbb{Z}/d\mathbb{Z}$ aus d' Elementen gibt, gibt es auch zu jedem Teiler von d auch genau einen Zwischenkörper M mit $\mathbb{F}_p \subset M \subset \mathbb{F}_q$.

4.1.1 Beispiel

Sei $\mathbb{F}_{64}$ ein Körper aus $64 = 2^6$ Elementen.

Es gilt $\mathrm{char}(\mathbb{F}_{64}) = 6$ und $\{1, 2, 3, 6\}$ ist die Menge der Teiler von 6.

Somit folgt für den Körper aus 64 Elementen



.

4.1.2 Zusammenfassung

Zu jeder Primzahlpotenz $q = p^d$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ aus q Elementen.

Dieser ist ein minimaler Zerfällungskörper des Polynoms

$$x^q - x = 0$$

über $\mathbb{F}_p$.

Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ ist zyklisch, von der Ordnung d und wird vom Frobeniushomomorphimus erzeugt.

Die Gruppe $(\mathbb{F}_q^{\times}, \cdot\,)$ ist zyklisch und von der Ordnung $q-1$.

4.2 Kreisteilungskörper

Einleitung

Sei $\zeta^n = 1$ und $\zeta \neq 1$. Demnach ist ζ die primitive n-te Einheitswurzel und es bezeichnet

$$\mathbb{Q}(\sqrt[n]{1}) \;=\; \mathbb{Q}(\zeta)$$

den minimalen Zerfällungskörper der Gleichung

$$\boxed{x^n - 1 \;=\; 0}$$

über $\mathbb{Q}$.

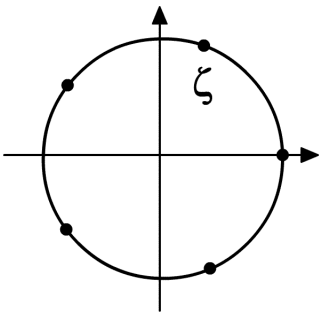


Abbildung 1

Die Lösungemenge μ_n der Gleichung $x^n - 1 = 0$ besteht aus n Elementen und ist

$$\mu_n \;=\; \{1, \zeta, \ldots, \zeta^{n-1}\} \;=\; \left\{ e^{\frac{2\pi i}{n} \cdot k} \;\middle|\; k = 0, \ldots, n-1 \right\}.$$

$(\mu_n, \cdot\,)$ bildet eine zyklische Gruppe der Ordnung $n-1$ und wird von dem Element $\zeta = e^{\frac{2\pi i}{n}}$ erzeugt, es gilt also

$$\mu_n \;=\; \langle\, \zeta \,\rangle \;=\; \langle\, e^{\frac{2\pi i}{n}} \,\rangle.$$

Weiter ist $\mathbb{Q}(\sqrt[n]{1})$ galoissch über $\mathbb{Q}$, da $\mathrm{char}(\mathbb{Q}) = 0$ gilt.

Galoisgruppe

Sei ζ die primitive n-te Einheitswurzel. Es gilt nun $\mu_n = \langle\, \zeta \,\rangle$.

Die Gruppe μ_n wird aber auch noch von anderen Einheitswurzeln erzeugt, nämlich von den Elementen ζ^a mit $\mathrm{ggT}(a, b) = 1$.

Für die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}\sqrt[n]{1}/\mathbb{Q})$ muss jeweils untersucht werden, worauf ζ abbildet wird. Da aber für ein $\varphi \in \mathrm{Gal}(\mathbb{Q}\sqrt[n]{1}/\mathbb{Q})$ auch $\varphi(\zeta)$ primitiv sein muss, sind die Elemente aus $\mathrm{Gal}(\mathbb{Q}\sqrt[n]{1}/\mathbb{Q})$ von der Form

$$\varphi_a : \mathbb{Q}\sqrt[n]{1} \to \mathbb{Q}\sqrt[n]{1} \qquad \text{mit} \qquad \varphi_a(\zeta) = \zeta^a,$$

dabei $\mathrm{ggT}(a, n) = 1$.

Die Abbildung

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}\sqrt[n]{1}/\mathbb{Q}) & \xrightarrow{\sim} & \big((\mathbb{Z}/n\mathbb{Z})^\times, \cdot\big) \\ \varphi_a & \mapsto & a \end{array}$$

ist sogar ein Gruppenisomorphismus.

$\mathrm{Gal}(\mathbb{Q}\sqrt[n]{1}/\mathbb{Q})$ ist also eine abelsche Gruppe und isomorph zu $(\mathbb{Z}/n\mathbb{Z})^\times$.

Zwischenkörper

Für einen Körper K der galoissch über $\mathbb{Q}$ ist und für den die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ abelsch ist, gibt es ein $n \in \mathbb{N}$, so dass

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt[n]{1})$$

gilt.

4.2.1 n-te Kreisteilungspolynome

Das n-te Kreisteilungspolynome wird definiert durch

$$\Phi_n(x) \;:=\; \prod_{\mathrm{ggT}(a,n)\,=\,1} (x - \zeta^a)\,,$$

dabei ist ζ die n-te primitive Einheitswurzel. Es gilt

$$x^n - 1 \;=\; \prod_{d|n} \Phi_d,$$

somit ergibt sich für die ersten Kreisteilungspolynome

$$\begin{aligned} \Phi_1 &= x - 1 \\ \Phi_2 &= x + 1 \\ \Phi_3 &= x^2 + x + 1 \\ \Phi_4 &= x^2 + 1 \\ \Phi_5 &= x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

(Für große n treten auch Koeffizienten $\neq \pm 1$ auf.)

4.2.2 Satz 1

Nach dem Gaußschen Lemma ist $\Phi_n(x) \in \mathbb{Q}[x]$ irreduzibel über $\mathbb{Q}$.

4.2.3 Satz 2

Sei p eine Primzahl.

Dann gilt

$$\Phi_p(x) \;=\; x^{p-1} + x^{p-1} + \ldots + x + 1.$$

4.2.4 Beispiel

Sei p eine Primzahl. Dann ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch und von der Ordnung $p-1$.

Demnach ist auch $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q})$ zyklisch und besteht aus $p-1$ Elementen.

Da p ein Primzahl ist, gilt $2 \mid (p-1)$ und somit gibt es einen Zwischenkörper M mit

$$\mathbb{Q} \subset M \subset \mathbb{Q}(\sqrt[p]{1})$$

und $(M : \mathbb{Q}) = 2$.

Für jeden weiteren Zwischenkörper K mit $(K : \mathbb{Q}) = d$ muss $d \mid p-1$ gelten.

4.3 Reine Gleichungen

Einleitung

Sei K ein beliebiger Körper, $a \in K$ und sei $n \in \mathbb{N}$.

Eine Gleichung der Form

$$\boxed{x^n - a \;=\; 0}$$

heißt eine ***reine Gleichung***. Die Nullstellen dieser Gleichung sind $\alpha = \sqrt[n]{a}$ sowie $\alpha\zeta, \ldots, \alpha\zeta^{n-1}$.

Ein minimaler Zerfällungskörper der Gleichung $x^n - a = 0$ über K ist

$$K(\alpha) \;=\; K(\sqrt[n]{a}).$$

Weiter ist $K(\sqrt[n]{a})$ galoissch über K.

Galoisgruppe

Gilt $\mathrm{char}(K) = n > 0$, so ist die Galoisgruppe $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ zyklisch und isomorph zu einer Untergruppe H von $(\mathbb{Z}/n\mathbb{Z}, +)$, also ist H von der Form $m\mathbb{Z}/n\mathbb{Z}$ mit $m \mid n$.

Ist p eine Primzahl und gilt $\mathrm{char}(K) = p$, dann ist $\mathrm{Gal}(K(\sqrt[p]{a})/K)$ also

isomorph zu $\mathbb{Z}/p\mathbb{Z}$ oder zu (1), $\mathrm{Gal}(K(\sqrt[p]{a})/K)$ ist demnach keine zyklische Gruppe.

Sei umgekehrt L galoisch über K und $\mathrm{Gal}(L/K)$ isomorph zu $\mathbb{Z}/n\mathbb{Z}$, also zyklisch und mit einem Erzeuger φ. Sei weiter $\zeta = \sqrt[n]{1} \in K$ die n-te primitive Einheitswurzel und sei $\tilde{\alpha} \in L$ mit $L = K(\tilde{\alpha})$. Setzte

$$\alpha \ := \ \sum_{i=1}^{n} \zeta^{-1} \varphi^i(\tilde{\alpha}),$$

dann gilt $\varphi(\alpha) = \zeta\alpha$ und es folgt $\alpha^n \in L^{\mathrm{Gal}(L/K)}$.

Sei weiter $a = \alpha^n$, so stellt man fest, dass $L = K(\sqrt[n]{a})$ gilt. Demnach wird L durch eine reine Gleichung gegeben.

4.4 Separable Körpererweiterungen

Sei K ein Körper und sei $f(x) \in K[x]$ ein irreduzibles Polynom.

Es ist bereits bekannt, dass $f(x)$ genau dann eine mehrfache Nullstelle hat, wenn $\mathrm{ggT}(f(x), f'(x)) \neq 1$ gilt. Auf diese Art und Weise läßt sich also insbesondere feststellen, ob $f(x)$ separabel ist oder nicht.

4.4.1 Definition

Sei L eine beliebige Körpererweiterung von K und sei $\alpha \in L$ algebraisch über K.

α heißt ***separabel*** über K, wenn das Minimalpolynom zu α über K separabel ist.

Es ist zu beachten, dass auch die folgenden Definitionen und Sätze nur für einen Körper K mit $\mathrm{char}(K) = p > 0$ gelten.

4.4.2 Definition

Sei K ein Körper und sei $L = K(\alpha)$ eine einfach algebraische Körpererweiterung von K.

Ein Polynom $p(x)$ vom Grad n heißt ***rein inseparabel*** über K, wenn es in L nur α als n fache Nullstelle gibt, wenn also gilt

$$p(x) \ = \ (x - \alpha)^n.$$

4.4.3 Definition und Satz

Sei K ein Körper mit $\mathrm{char}(K) = p > 0$, sei L eine endlich algebraische Körpererweiterung von K und sei $\alpha \in L$.

Dann gibt es eine Potenz p^l, so dass α^{p^l} ein separables Element über K ist.

Dabei heißt p^l der ***Inseparabilitätsgrad*** von α über K.

Ist $p(x)$ das Minimalpolynom von α^{p^l} über K, so heißt $\text{grad}(p(x))$ der ***Separabilitätsgrad*** von α über K.

4.4.4 Satz 1

Sei L eine algebraische Körpererweiterung von K und seien $\alpha, \beta \in L$.

Dann gilt:

(1) Sind α und β separabel über K, dann sind auch $\alpha + \beta$, $\alpha \cdot \beta$ und α/β separabel über K.

(2) Sind α und β rein inseparabel über K, dann sind auch $\alpha + \beta$, $\alpha \cdot \beta$ und α/β rein inseparabel über K.

4.4.5 Satz 2

Sei L eine Körpererweiterung von K, sei $X \subset L$ und sei $K(X)$ der von X in L erzeugte Teilkörper.

Dann gilt:

(1) Sind alle $\alpha \in X$ separabel über K, so ist $K(X)$ separabel über K.

(2) Sind alle $\alpha \in X$ rein inseparabel über K, so ist $K(X)$ rein inseparabel über K.

4.4.6 Satz 3

Sei L eine Körpererweiterung von K und M ein Zwischenkörper von K und L. Sei weiter $\alpha \in L$ separabel über M.

Dann gilt:

(1) Ist M separabel über K, dann ist α separabel über K.

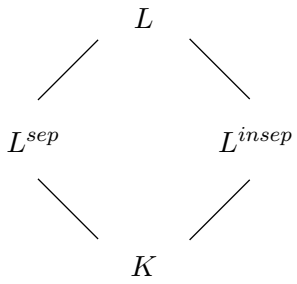
(2) Ist M rein inseparabel über K, dann ist α rein inseparabel über K.

4.4.7 Satz 4

Sei L eine endlich algebraische Körpererweiterung von K, und es seien

$$\begin{aligned} L^{sep} &:= \{\alpha \in L \mid \alpha \text{ ist separabel über } K\}, \\ L^{insep} &:= \{\alpha \in L \mid \alpha \text{ ist rein inseparabel über } K\}. \end{aligned}$$

Dann sind L^{sep} und L^{insep} Körper über K.



Weiter ist L^{sep} separabel über K und L^{insep} ins rein inseparabel über K. Zudem ist L separabel über L^{insep} und rein inseparabel über L^{sep}. Es gilt

$$L^{sep} \cap L^{insep} = K.$$

4.5 Konstruktionen mit Zirkel und Lineal

Es sollen nun geometrische Konstruktionen in der Ebene $E = \mathbb{R}^2$ vorgenommen werden.

Gegeben ist ein Nullpunkt $(0, 0) \in \mathbb{R}^2$. Zu einer beliebigen Gerade durch den Nullpunkt lässt sich eine senkrechte Gerae konstruieren und man erhält ein Koordinatensystem.

Nun kann man Einheiten und Geraden eintragen, um $\mathbb{Z}^2 \subset E$ zu erhalten:

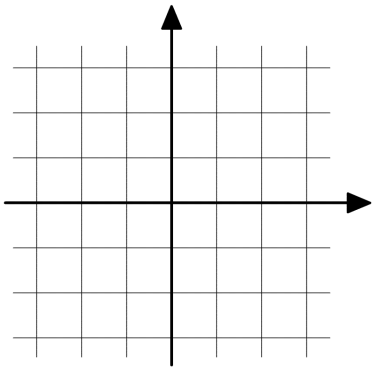


Abbildung 2

Mit Hilfe der Strahlensätze lässt sich sogar $\mathbb{Q}^2 \subset E$ konstruieren:

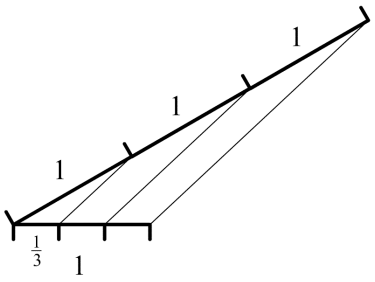


Abbildung 3

Sei nun $(a, b) \in \mathbb{Q}$, dann hat man auch die Strecke $x = \sqrt{a^2 + b^2}$ in einer geeigneten Körpererweiterung K^2, also $(a, b) \in \mathbb{R}$. Es können nun alle Punkte aus $K^2 \subset \mathbb{R}^2 = E$ konstruiert werden, wobei $K^2 \subset \mathbb{R}^2$ ein echter Unterkörper ist.

Sind nun g und h zwei verschieden nicht parallele Geraden über K, dann ist auch der Schnittpunkt $g \cap h \in K^2$.

Ist g eine Gerade und c ein Kreis über K, dann sind die Schnittpunkte $g \cap c \in L$, wobei L eine Körpererweiterung von K ist mit $(L : K) \leq 2$.

Genauso sind auch die Schnittpunkte $c \cap d$ von zwei Kreisen c und d über K Elemente einer Körpererweiterung L von K mit $(L : K) \leq 2$.

4.5.1 Zusammenfassung

Ein Punkt $(x, y) \in \mathbb{R}^2$ ist genau dann mit Zirkel und Lineal konstruierbar, wenn $(x, y) \in L^2$ gilt und L durch eine Reihe von Zwischenkörpern

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_{r-1} \subset K_r = L \subset \mathbb{R}^2$$

mit $(K_{i+1} : K_i) = 2$ gegeben wird. Insgesamt muss also $(L : \mathbb{Q}) = 2^n$ mit $n \in \mathbb{N} \cup \{0\}$ gelten.

4.5.2 Anwendungen

(1) ***Würfelverdoppelung***

Es soll also $(\sqrt[3]{2}, 0) \in \mathbb{R}^2$ mit Zirkel und Lineal konstruiert werden. Da $x^3 - 2 = 0$ irreduzibel ist, enthält man $(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = 3$, also nicht wie gefordert 2^n. Demnach ist eine derartige Konstruktion nicht möglich.

(2) ***Winkeldreiteilung***

Gegeben ist $\mathbb{R}^2 \xrightarrow{\sim} \mathbb{C}$ und $\alpha = (\cos(\varphi), \sin(\varphi)) = e^{i\varphi}$. Gesucht ist also $e^{\frac{i\varphi}{3}} = \big(\cos(\frac{\varphi}{3}), \sin(\frac{\varphi}{3})\big)$. Es ergibt sich die Gleichung $x^3 = \alpha$ und wiederrum $(K(\alpha) : K) = 3 \neq 2^n$. Demnach ist auch hier eine Konstruktion nicht möglich.

(3) ***Regelmäßiges n-Eck***

Dies bedeutet eine Konstruktion von $\mathbb{Q}(\sqrt[n]{1}) \in \mathbb{C} \xrightarrow{\sim} \mathbb{R}^2$ mit Zirkel und Lineal. Es gilt

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \quad \xrightarrow{\sim} \quad (\mathbb{Z}/n\mathbb{Z})^\times,$$

also gilt $(\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}) = \varphi(n)$, dabei ist φ die Eulersche φ-Funktion. Es muss also $\varphi(n) = 2^k$ gelten, damit ein regelmäßiges n-Eck konstruierbar ist. $\varphi(n) = 2^k$ gilt genau für $n = 2^{\left(2^l\right)} + 1$, also für

$$3,\ 5,\ 17,\ 257,\ 65537,\ \ldots.$$

4.6 Aufgaben

4.6.1 Aufgabe 1

Sei $K = \mathbb{Q}(\sqrt[7]{1})$, dabei $\sqrt[7]{1} \neq 1$.

Berechne $\mathrm{Gal}(K/\mathbb{Q})$ und bestimme alle Zwischenkörper $\mathbb{Q} \subset M \subset K$.

Lösung

$K = \mathbb{Q}(\sqrt[7]{1})$ ist ein minimaler Zerfällungskörper der Gleichung

$$x^7 - 1 \ = \ 0.$$

Sei $\zeta = \sqrt[7]{1}$ die 7-te primitive Einheitswurzel. Dann ist $\{1, \zeta, \zeta^2, .., \zeta^6\}$ die Menge der Lösungen dieser Gleichung. Es gilt

$$\zeta^6 \ = \ -\zeta^5 - \zeta^4 - \zeta^3 - \zeta^2 - \zeta - 1,$$

daher folgt

$$K \ = \ \mathbb{Q}(\sqrt[7]{1}) \ = \ \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 \mid a_0, .., a_5 \in \mathbb{Q}\}.$$

Und da $\Phi_6(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ irreduzible über $\mathbb{Q}$ ist, folgt sogar auch $(K : \mathbb{Q}) = 6$.

Für die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ muss nun nur wieder untersucht werden, worauf ζ abgebildet wird. Ein Element $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ ist jedoch von der Form

$$\varphi_a : K \to K \qquad \text{mit} \qquad \varphi_a(\zeta) = \zeta^a,$$

dabei $a \in \{1, .., 6\}$.

Da 7 eine Primzahl ist, sind die Abbildungen $\varphi_{1,..,6} : K \to K$ mit

$$\begin{aligned}\varphi_1(\zeta) &= \zeta \\ \varphi_2(\zeta) &= \zeta^2 \\ \varphi_3(\zeta) &= \zeta^3 \\ \varphi_4(\zeta) &= \zeta^4 \\ \varphi_5(\zeta) &= \zeta^5 \\ \varphi_6(\zeta) &= \zeta^6\end{aligned}$$

in der Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ enthalten.

Desweiteren ist $\mathrm{Gal}(K/\mathbb{Q})$ isomorph zu der zyklischen Gruppe $(\mathbb{Z}/7\mathbb{Z})^\times$, daher wird auch $\mathrm{Gal}(K/\mathbb{Q})$ von einem Element erzeugt. Für φ_3 (ebenso für φ_5) gilt:

$$\begin{aligned}\varphi_3(\zeta) &= \zeta^3 \\ \varphi_3^2(\zeta) &= \zeta^9 = \zeta^2 \\ \varphi_3^3(\zeta) &= \zeta^{27} = \zeta^6 \\ \varphi_3^4(\zeta) &= \zeta^{81} = \zeta^4 \\ \varphi_3^5(\zeta) &= \zeta^{243} = \zeta^5 \\ id = \varphi_3^6(\zeta) &= \zeta^{729} = \zeta\end{aligned}$$

Daher ist φ_3 ein Erzeuger der Galoisgruppe:

$$\mathrm{Gal}(K/\mathbb{Q}) = \{id, \varphi_3, \varphi_3^2, \varphi_3^3, \varphi_3^4, \varphi_3^5\}$$

Wie schon erwähnt, ist $\mathrm{Gal}(K/\mathbb{Q})$ isomorph zu $(\mathbb{Z}/7\mathbb{Z})^\times$, aber diese Gruppe ist isomorph zu $\mathbb{Z}/6\mathbb{Z}$, welche wiederum nach dem Chinesischen Restsatz isomorph ist zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Zu dieser Gruppe können wir nun einfach alle Untergruppen bestimmen. Dies sind neben den trivialen Untergruppen noch

$$\{0\} \times \mathbb{Z}/3\mathbb{Z} \qquad \text{und} \qquad \mathbb{Z}/2\mathbb{Z} \times \{0\}.$$

Daher hat auch $\mathrm{Gal}(K/\mathbb{Q})$ genau zwei nicht triviale Untergruppen, eine aus 2 Elementen und eine aus 3 Elementen.

Es gilt

$$\left(\varphi_3^3 \circ \varphi_3^3\right)(\zeta) = \varphi_3^3\left(\zeta^6\right) = \varphi_3^3\left(\zeta^{-1}\right) = \zeta.$$

Daher bildet $\{id, \varphi_3^3\}$ die Untergruppe von $\mathrm{Gal}(K/\mathbb{Q})$ aus 2 Elementen.

Weiter gilt

$$\begin{aligned}\left(\varphi_3^2 \circ \varphi_3^2\right)(\zeta) &= \zeta^4, \\ \left(\varphi_3^4 \circ \varphi_3^4\right)(\zeta) &= \zeta^{16} = \zeta^2, \\ \left(\varphi_3^2 \circ \varphi_3^4\right)(\zeta) &= \zeta^8 = \zeta \quad \text{und} \\ \left(\varphi_3^4 \circ \varphi_3^2\right)(\zeta) &= \zeta^8 = \zeta,\end{aligned}$$

daher bildet $\{id, \varphi_3^2, \varphi_3^4\}$ die Untergruppe von $\mathrm{Gal}(K/\mathbb{Q})$ aus 3 Elementen.
Neben den beiden trivialen Zwischenkörpern K und $\mathbb{Q}$ ergibt sich

$$M_1 \;=\; K^{\{id,\varphi_3^3\}} \;=\; \{a\zeta + b\zeta^6 \mid a, b \in \mathbb{Q}\} \;=\; \mathbb{Q}(\zeta + \zeta^6),$$

da $\varphi_3^3(\zeta) = \varphi_3^3(\zeta^3) = \varphi_3^3(\zeta^5) = \zeta^6$ und $\varphi_3^3(\zeta^2) = \varphi_3^3(\zeta^4) = \zeta$ gilt.
Ebenso erhält man

$$M_2 \;=\; K^{\{id,\varphi_3^2,\varphi_3^4\}} \;=\; \{a\zeta + b\zeta^2 + c\zeta^4 \mid a, b, c \in \mathbb{Q}\} \;=\; \mathbb{Q}(\zeta + \zeta^2 + \zeta^4),$$

da $\varphi_3^2(\zeta) = \varphi_3^2(\zeta^4) = \zeta^2$, $\varphi_3^2(\zeta^3) = \zeta$, $\varphi_3^2(\zeta^2) = \varphi_3^2(\zeta^5) = \zeta^4$ und $\varphi_3^4(\zeta) = \varphi_3^4(\zeta^4) = \zeta^4$, $\varphi_3^4(\zeta^2) = \varphi_3^4(\zeta^5) = \zeta^2$, $\varphi_3^4(\zeta^3) = \zeta$.

5 Gruppen

In diesem Kapitel wird davon ausgegangen, dass die grundlegen Definitionen wie zum Beispiel die Definitionen von Gruppen und Normalteiler bereits bekannt sind. Derartige Definitionen werden teilweise in den Sätzen angesprochen und noch einmal kurz wiederholt.

5.1 Auflösbare Gruppen

5.1.1 Definition

Sei G eine beliebige Gruppe.

$$G^{(1)} := \{[a,b] = aba^{-1}b^{-1} \mid a,b \in G\}$$

heißt die ***Kommutatorgruppe*** von G und ist die kleinste Untergruppe von G, die $[a,b]$ für alle $a,b \in G$ enthält.

5.1.2 Satz 1

Sei G eine Gruppe und sei $\varphi : G \to G$ ein beliebiger Gruppenautomorphismus.

Dann gilt

$$\varphi\left(G^{(1)}\right) = G^{(1)},$$

also ist $G^{(1)}$ eine ***charakteristische Gruppe*** von G. $G^{(1)}$ ist sogar ein Normalteiler von G.

Beweis

Es gilt für alle $a,b \in G$

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

Insbesondere gilt für den ***inneren Automorphismus***

$$\mathrm{Int}_g : G \to G, \qquad a \mapsto gag^{-1}$$

$\mathrm{Int}_g(G^{(1)}) = G^{(1)}$, also ist auch $gG^{(1)}g^{-1} = G^{(1)}$ mit $g \in G$ beliebig und somit ist die Normalteilereigenschaft gezeigt.

5.1.3 Beispiele

(1) Sei G eine abelsche Gruppe. Dann gilt

$$G^{(1)} \;=\; \{[a,b] = aba^{-1}b^{-1} \mid a,b \in G\} \;=\; \{1\}.$$

(2) Sei G eine ***einfache Gruppe***, d.h. G und $\{1\}$ sind alle Normalteiler von G.

Dann gilt $G^{(1)} = G$.

5.1.4 Definition

Sei G eine Gruppe. Dann definiert man induktiv

$$G^{(i+1)} \;:=\; \left(G^{(i)}\right)^{(1)}.$$

Beispiel

Seien $x = aba^{-1}b^{-1}$ und $y = cdc^{-1}d^{-1}$ in $G^{(1)}$. Dann gilt

$$[x,y] \;=\; (aba^{-1}b^{-1})(cdc^{-1}d^{-1})(bab^{-1}a^{-1})(dcd^{-1}c^{-1}) \;\in\; G^{(2)}.$$

5.1.5 Satz 2

Sei G eine Gruppe und sei $\varphi : G \to G$ ein beliebiger Gruppenautomorphismus.

Dann gilt

$$\varphi\left(G^{(i)}\right) \;=\; G^{(i)},$$

also sind alle $G^{(i)}$ auch charakteristische Gruppe von G.

Beispiel

Ist G eine einfache, nicht abelsche Gruppe. Dann gilt

$$G \;=\; G^{(1)} \;=\; G^{(2)} \;=\; G^{(3)} \;=\; \ldots.$$

5.1.6 Satz 3

Sei G eine beliebige und sei A eine abelsche Gruppe. Dann gilt:

(1) $G/G^{(1)}$ ist eine abelsche Gruppe.

(2) Ist $\varphi : G \to A$ ein Gruppenhomomorphismus, dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus $\overline{\varphi}$ mit $\varphi = \overline{\varphi} \circ p$, so dass das Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ p \searrow & & \nearrow \overline{\varphi} \\ & G/G^{(1)} & \end{array}$$

kommutiert.

(3) Entsprechen sind die Gruppen $G^{(i)}/G^{(i+1)}$ alle abelsch.

5.1.7 Definition

Sei G eine Gruppe.

G heißt ***auflösbar***, wenn es ein $n \in \mathbb{N} \cup \{0\}$ gibt, so dass $G^{(n)} = \{1\}$ gilt.

5.1.8 Beispiele

(1) Ist G abelsch, so gilt sofort $G^{(1)} = \{1\}$.

(2) Gilt $|G| = p^n$ mit einer Primzahl p, so ist G auflösbar.

(3) Die Gruppen S_4 und S_5 sind auflösbar.

(4) Die Gruppen S_n mit $n \geq 5$ sind nicht auflösbar.

5.1.9 Definition

Sei G eine Gruppe.

(1) Eine ***Normalreihe*** von G ist eine Folge von Untergruppen

$$G \;=\; G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r \;=\; \{1\},$$

so dass G_{i+1} jeweils ein Normalteiler von G_i ist.

(2) Eine ***Kompositionsreihe*** von G ist eine Normalreihe, wobei jeweils G_i/G_{i+1} eine einfache Gruppe ist.

Desweiteren gibt es zu jeder Normalreihe einer endlichen Gruppe eine Verfeinerung, so dass die Normalreihe zur Kompositionsreihe wird.

5.1.10 Beispiel

Betrachtet man die abelsche Gruppe $G = (\mathbb{Z}/p\mathbb{Z})^n$, so stellt man fest, dass G ein n dimensionaler Vektorraum über $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ist. Daher ist die Normalreihe von G eine endliche Folge von Untervektorräumen.

Die Kompositionsreihe ist demnach die Folge

$$G \;=\; V_n \supset V_{n-1} \supset V_{n-2} \supset \ldots \supset V_1 \supset V_0 \;=\; \{1\},$$

wobei V_i ein i dimensionaler Untervektorraum von G ist.

5.1.11 Satz von Jordan-Hoelder

Sei G eine endliche Gruppe und seien

$$G \;=\; G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r \;=\; \{1\},$$

$$G \;=\; G'_0 \supset G'_1 \supset G'_2 \supset \ldots \supset G'_r \;=\; \{1\}$$

zwei Kompositionsreihen von G.

Dann gibt es eine Bijektion $\varphi : \{0,..,r\} \to \{0,..,r\}$ mit

$$G_i/G_{i+1} \quad \xrightarrow{\sim} \quad G'_{\varphi(i)}/G'_{\varphi(i)+1}.$$

Beispiel

Sei $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Dann sind

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = G \;\supset\; \mathbb{Z}/2\mathbb{Z} = G_1 \;\supset\; \{1\} = G_2,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = G \;\supset\; \mathbb{Z}/3\mathbb{Z} = G'_1 \;\supset\; \{1\} = G'_2,$$

zwei Kompositionsreihen von G. Es gilt nun zum Beispiel

$$G/G_1 \quad \xrightarrow{\sim} \quad G'_1.$$

5.1.12 Satz 4

Sei G eine endliche Gruppe.

Dann sind folgende Aussagen äquivalent:

(1) G ist auflösbar.

(2) Es gibt eine Normalreihe $\{G_i\}$ von G, so dass G_i/G_{i+1} abelsch ist.

(3) Es gibt eine Normalreihe $\{G_i\}$ von G, so dass G_i/G_{i+1} zyklisch ist.

Beispiel

Sei $G = \mathbb{Z}$ und p eine Primzahl. Dann ist

$$\mathbb{Z} \supset p\mathbb{Z} \supset p^2\mathbb{Z} \supset \ldots \supset p^i\mathbb{Z} \supset \ldots \supset \{1\}$$

eine Normalreihe von $\mathbb{Z}$. Es gilt

$$p^i\mathbb{Z}/p^{i+1}\mathbb{Z} \quad \xrightarrow{\sim} \quad \mathbb{Z}/p\mathbb{Z}.$$

5.1.13 Auflösbarkeit durch Radikale

Jede Gleichung der Form $f(x) = 0$ über einem Körper K ist durch ***Radikale*** auflösbar, das heißt es gibt eine Folge von Erweiterungen

$$K = K_0 \ \subset \ K_1 \ \subset \ K_2 \ \subset \ \ldots \ \subset \ K_r = L,$$

so dass $f(x)$ in L vollständig in Linearfaktoren zerfällt und L galoissch über K ist.

5.1.14 Satz 5

Sei K ein Körper und sei $f(x) \in K[x]$ irreduzibel.

Dann sind äquivalent (mit char(K) geeignet):

(1) $f(x) = 0$ ist durch Radikale auflösbar.

(2) Die Galoisgruppe Gal(L/K) ist eine auflösbare Gruppe (dabei L ein minimaler Zerfällungskörper von $f(x)$ über K).

5.2 Allgemeine Gleichungen n-ten Grades

Einleitung

Sei K ein Körper und sei $K(t_1, .., t_n)$ der Körper der rationalen Funktionen mit n Unbekannten, also $K(t_1, .., t_n) = \text{Quot}(K[t_1, .., t_n])$.

Sei weiter

$$f(x) \ = \ x^n + t_1 x^{n-1} + \ldots + t_{n-1} x + t_n$$

ein Polynom vom Grad n. Sei nun L ein minimaler Zerfällungskörper von $f(x) = 0$ über $K(t_1, .., t_n)$ und seien $\alpha_1, .., \alpha_n$ die Nullstellen von $f(x)$ in L.

Dann gilt also

$$\prod_{i=1}^{n}(x - \alpha_i) \ = \ x^n + t_1 x^{n-1} + \ldots + t_{n-1} x + t_n$$

und man erhält durch Koeffizientenvergleich

$$\begin{aligned} t_1 &= -(\alpha_1 + \alpha_2 + \ldots + \alpha_n) \\ t_2 &= \sum_{i<j} \alpha_i \alpha_j \ = \ \alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n \\ &\vdots \\ t_n &= (-1)^n \prod_{i=1}^{n} \alpha_i \ = \ (-1)^n \alpha_1 \alpha_2 \ldots \alpha_n \end{aligned}$$

Galoisgruppe

Die Galoisgruppe von L über $K(t_1, .., t_n)$ ist isomorph zu der Permutationengruppe S_n:

$$\mathrm{Gal}(L/K(t_1, .., t_n)) \quad \xrightarrow{\sim} \quad S_n$$

5.2.1 Satz 1

Eine allgemeine Gleichung n-ten Grades ist genau dann durch Radikale auflösbar, wenn $n \leq 4$ gilt.

5.3 Sylowsche Sätze

5.3.1 Definition

Eine Gruppe G heißt ***p-Gruppe***, wenn $|G| = p^n$ gilt, wobei p eine Primzahl ist.

5.3.2 Satz 1

Sei G eine nicht triviale p-Gruppe.

Dann gilt für das Zentrum

$$|\,\mathrm{Zent}(G)\,| \;=\; |\,\{g \in G \mid gx = xg \text{ für alle } x \in G\}\,| \;>\; 1.$$

5.3.3 Satz 2

Jede endliche p-Gruppe ist auflösbar.

5.3.4 Erster Sylowsche Satz

Sei G eine endliche Gruppe der Ordnung $p^n \cdot m$ mit einer Primzahl p und mit $\mathrm{ggT}(p, m) = 1$.

Dann gibt es zu jedem $1 \leq s \leq n$ eine Untergruppe von G der Ordnung p^s.

Jede dieser Untergruppen heißt dann ***p-Sylowgruppe*** von G.

5.3.5 Satz 3

Sei wieder G eine endliche Gruppe der Ordnung $p^n \cdot m$ mit einer Primzahl p und mit $\mathrm{ggT}(p, m) = 1$.

Sei weiter N die Anzahl der p-Sylowgruppen von G, also

$$N \;=\; |\{S \subset G \mid S \text{ ist p-Sylowgruppe von G}\}|.$$

Dann teilt N die Gruppenordnung $|G|$ und es gilt

$$N \;\equiv\; 1 \;(\mathrm{mod}\; p\,).$$

5.3.6 Beispiel

Sei $G = S_4$. Dann gilt $|G| = 4! = 24 = 2^3 \cdot 3$.

Es gibt genau 4 mögliche 3-Sylowgruppen, nämlich

$$\{(1), (123), (132)\}, \quad \{(1), (124), (142)\},$$
$$\{(1), (134), (143)\}, \quad \{(1), (234), (243)\}.$$

Es gilt genau $4 \equiv 1 \pmod 3$ und $4 \mid 24$.

5.3.7 Zweiter Sylowsche Satz

Sei G eine endliche Gruppe der Ordnung $p^n \cdot m$ wie oben, sei H eine p-Sylowgruppe von G und sei S eine Untergruppe von G der Ordnung p^s mit $s \geq 0$.

Dann gibt es $g \in G$ mit

$$S \subset gHg^{-1}.$$

Folgerungen

(1) Ist S eine p-Gruppe, so ist S in einer p-Sylowgruppe von G enthalten.

(2) Je zwei p-Sylowgruppen sind konjugiert in G.

5.4 Gruppen spezieller Ordnung

5.4.1 Gruppen der Ordnung 4

Jede Gruppe der Ordnung 4 ist entweder isomorph ist zu der zyklischen Gruppe $\mathbb{Z}/4\mathbb{Z}$ oder zu der nicht zyklischen Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5.4.2 Gruppen der Ordnung 6

Jede Gruppe der Ordnung 6 ist entweder isomorph zu der abelschen Gruppe $\mathbb{Z}/6\mathbb{Z}$ oder zu der nicht abelschen Gruppe S_3.

5.4.3 Gruppen der Ordnung 15

Jede Gruppe der Ordnung 15 ist isomorph zu der additiven Gruppe $\mathbb{Z}/15\mathbb{Z}$.

5.4.4 Gruppen der Ordnung p

Jede Gruppe der Primzahlordnung p ist isomorph zu der additiven Gruppe $\mathbb{Z}/p\mathbb{Z}$.

5.5 Aufgaben

5.5.1 Aufgabe 1

Sei G eine Gruppe mit $|G| = p^n$, dabei p eine Primzahl. Die Gruppe G operiere auf einer endlichen Menge X. Es sei

$$X^G \;=\; \{x \in X \mid g \cdot x = x \text{ für alle } g \in G\} \;\subset\; X.$$

Zeige, dass die Kongruenz

$$|X| \;\equiv\; |X^G| \;(\mathrm{mod}\; p\,)$$

gilt.

Lösung

Die Bahn von $x \in X$ unter G ist

$$G \cdot x \;=\; \{y \in X \mid \exists\, g \in G :\; y = g \cdot x\} \;=\; \{g \cdot x \mid g \in G\} \;\subset\; X.$$

Es ist bekannt, dass gilt:

(1) Die Bahnen von allen $x \in X$ unter G bilden eine disjunkte Zerlegung von X.

(2) $|G \cdot x|$ teilt $|G|$.

(3) $x \in X^G \;\Leftrightarrow\; G \cdot x = \{x\} \;\Leftrightarrow\; |G \cdot x| = 1.$

Es gilt nun offenbar

$$|G \cdot x| \;=\; p^k \qquad \text{mit} \qquad k \in \{0, .., n\}.$$

Aufgrund der disjunkten Zerlegung von X in Bahnen gilt für die Summe über allen Bahnen

$$\sum |G \cdot x| \;=\; |X|.$$

Da alle $x \in X^G$ unter G fest bleiben, folgt

$$\begin{aligned} X \;&=\; \dot{\bigcup_{|G\cdot x|>1}} G \cdot x \;\;\cup\;\; \dot{\bigcup_{|G\cdot x|=1}} G \cdot x \\ \Leftrightarrow\quad |X| \;&=\; \sum_{|G\cdot x|>1} |G \cdot x| \;+\; |X^G|. \end{aligned}$$

Da wir bereits festgestellt haben, dass $|G \cdot x| = p^k$ gilt, folgt die Behauptung:

$$|X| \;\equiv\; \sum_{|G\cdot x|>1} 0 \;+\; |X^G| \;(\mathrm{mod}\; p\,) \;=\; |X^G| \;(\mathrm{mod}\; p\,)$$

5.5.2 Aufgabe 2

Zeige, dass jede Gruppe der Ordnung 4 entweder isomorph ist zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lösung

Zunächst einmal ist klar, dass jede Gruppe entweder zyklisch oder nicht zyklisch ist.

Sei zunächst G eine nicht zyklische Gruppe der Ordnung 4. Dann haben alle Elemente aus G die Ordnung 1, 2 oder 4, da dies genau die Teiler von 4 sind. Da das neutrale Element eindeutig bestimmt ist, gibt es genau ein Element der Ordnung 4. Da G nicht zyklisch ist, gibt es aber kein Element der Ordnung 4 und alle anderen Elemente müssen die Ordnung 2 haben. Dies zeigt, dass G isomorph ist zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Gruppe G	1	2	3	4
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
Ordnung	1	2	2	2

Sei nun H eine zyklische Gruppe der Ordnung 4. Auch hier haben wieder alle Elemente die Ordnung 1, 2 oder 4 und es gibt wieder nur das neutrale Element der Ordnung 1. Da H nun aber zyklisch ist, muss es mindestens ein Element der Ordnung 4 geben. Da es aber zu einem solchen Element auch ein Inveres in H gibt, hat auch das inverse Element die Ordnung 4. Es bleibt nun nur noch ein Element in H übrig, da aber auch dieses Element ein Inverses haben muss, ist es zu sich selber invers und somit hat es die Ordnung 2. Dies zeigt genau, dass H isomorph ist zu $\mathbb{Z}/4\mathbb{Z}$.

Gruppe H	1	2	3	4
$\mathbb{Z}/4\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
Ordnung	1	4	2	4

5.5.3 Aufgabe 3

Sei $\mathbb{F}_q$ ein Körper aus q Elementen, sei $n \in \mathbb{N}$ und sei $GL(n, \mathbb{F}_q)$ die Gruppe aller invertierbaren $n \times n$ Matrizen. Sei weiter $Z = \{kE \mid k \in \mathbb{F}_q^\times\}$ mit der $n \times n$ Einheitsmatrix E.

(1) Berechne die Ordnung der Gruppe $GL(n, \mathbb{F}_q)$.

(2) Berechne die Ordnung der Gruppe $PGL(n, \mathbb{F}_q) = GL(n, \mathbb{F}_q)/Z$.

Lösung Teil 1

Betrachtet man zunächst eine beliebige Matrix $A \in GL(n, \mathbb{F}_q)$, so ist A invertierbar und besteht aus n Spaltenvektoren $x_1, .., x_n \in \mathbb{F}_q^n$.

Da A invertierbar ist, sind die n Spaltenvektoren linear unabhängig.

Betrachtet man den ersten Spaltenvektor $x_1 = (x_{11}, .., x_{1n})$, so gilt $x_{1i} \in \mathbb{F}_q$ mit $i = 1, .., n$. Somit sind zunächst q^n unterschiedliche Vektoren x_1 gefunden in $\mathbb{F}_q^n$. Da A aber invertierbar ist, kann x_1 nicht der Nullvektor sein und es ergeben sich genau

$$q^n - 1$$

Möglichkeiten für die Wahl von x_1.

Nach gleicher Überlegung gibt es nun zunächst auch $q^n - 1$ Möglichkeiten für die Wahl des zweiten Spaltenvektors x_2. Da aber x_1 und x_2 linear unabhängig sein müssen, dürfen keine Vielfachen des ersten Spaltenvektors auftreten. Dies sind nach Abzug einer Möglichkeit durch die 0 genau $q - 1$. Es ergeben sich somit für den zweiten Spaltenvektor genau

$$q^n - 1 - (q - 1) \;=\; q^n - q$$

Möglichkeiten.

Für x_3 bleiben nun q^n Möglichkeiten abzüglich Vielfacher der beiden ersten Vektoren, dies sind genau q^2. Somit gibt es genau

$$q^n - q^2$$

Wahlmöglichkeiten für x_3.

Analog erhält man für den Spaltenvektor x_m mit $1 \leq m \leq n$ genau

$$q^n - q^{m-1}$$

Möglichkeiten der Wahl.

Die gesuchte Gruppenordnung ist das Produkt der Wahlmöglichkeiten der einzelnen Spaltenvektoren, also

$$\begin{aligned} |GL(n, \mathbb{F}_q)| &= (q^n - 1) \cdot (q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}) \\ &= \prod_{i=0}^{n-1} (q^n - q^i). \end{aligned}$$

Lösung Teil 2

Es gilt

$$|Z| \;=\; |\mathbb{F}_q| \;=\; q - 1.$$

Somit ergibt sich

$$|PGL(n,\mathbb{F}_q)| \;=\; |GL(n,\mathbb{F}_q)/Z| \;=\; |GL(n,\mathbb{F}_q)|/|Z| \;=\; \frac{\prod_{i=0}^{n-1}(q^n-q^i)}{q-1}.$$

Literaturverzeichnis

[1] Kersten, I. (2002): "Algebra". Skript zur Vorlesung im Wintersemester 2000/2001. Mathematisches Institut, Göttingen.

[2] Scholz, D. (2005): "Algebra". Vorlesungsmitschrift im Wintersemester 2004/2005 bei Prof. U. Stuhler, Universität Göttingen.

[3] Stuhler, U. (1999): "Analytische Geometrie und Lineare Algebra II". Skript zur Vorlesung im Sommersemester 2004. Unverändeter Nachdruck. Mathematisches Institut, Göttingen

Index