Galoistheorie

Matthias Künzer

Universität Koblenz-Landau

12. November 2015

Inhalt

Verzeichnis der Sätze

Vorwort

Wir folgen im wesentlichen Emil Artins Buch *Galoissche Theorie* [**1**], mit gelegentlichen Abweichungen. Eine davon gleich zu Beginn, wir betrachten den Polynomring und Ideale darin, was nützlich ist für die Konstruktion von Körpererweiterungen. Ferner schenken wir den endlichen Körpern etwas mehr Beachtung und führen auch die Berechnung von Galoisgruppen explizit aus (unter Zuhilfenahme von Magma [**2**] für Polynomfaktorisierungen). Auf der anderen Seite lassen wir gewisse Abschnitte aus Artins Buch hier weg, wie etwa Normalbasen, oder Kreisteilungskörper über $\mathbf{Q}$. Diese seien den Studenten zum weiteren Studium empfohlen.

Allgemein setzen wir Lineare Algebra voraus, nicht aber Algebra.

Die Aufgaben haben zweierlei Sinn. Zum einen dienen sie der Wiederholung und der Vertiefung von Beispielen. Zum anderen werden teils kleinere für die Vorlesung erforderliche Sachverhalte in die Übungen ausgelagert. Insofern sind Übungen und Lösungen Bestandteil des Skripts.

Für Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Koblenz, den 12.02.2009

Matthias Künzer

Konventionen.

(1) Für $a, b \in \mathbf{Z}$ schreiben wir $[a, b] := \{c \in \mathbf{Z} \ : \ a \leqslant c \leqslant b\}$ für das ganzzahlige Intervall. Ferner bezeichne $\mathbf{Z}_{\geqslant 0} := \{z \in \mathbf{Z} \ : \ z \geqslant 0\}$ etc.
Für $a, b, c \in \mathbf{Z}_{\geqslant 0}$ bedeutet $a^{b^c} := a^{(b^c)}$, wobei $0^0 = 1$.

(2) Ist $X \xrightarrow{f} Y$ eine Abbildung von Mengen, und sind $X' \subseteq X$ und $Y' \subseteq Y$ derart, daß $f(X') \subseteq Y'$, dann schreiben wir $f|_{X'}^{Y'} : X' \longrightarrow Y'$ für die im Urbild- und Bildbereich eingeschränkte Abbildung, die ein $x' \in X'$ nach $f(x') \in Y'$ schickt. Falls $Y' = Y$, dann schreiben wir auch $f|_{X'} := f|_{X'}^{Y}$. Falls $X' = X$, dann schreiben wir auch $f|^{Y'} = f|_{X}^{Y'}$.

(3) Es stehe "für $x \in X$" auch kurz statt "für alle $x \in X$". Dagegen wird "für ein $x \in X$" nicht abgekürzt.

(4) Die disjunkte Vereinigung von Mengen X und Y werde $X \sqcup Y$ geschrieben.

(5) Ist X eine endliche Menge, so bezeichnet $|X|$ ihre Kardinalität, d.h. die Anzahl ihrer Elemente. Ist X unendlich, so schreiben wir für diesen Sachverhalt $|X| = \infty$.

(6) Ist R ein kommutativer Ring, so schreiben wir auch $R^\times := R \smallsetminus \{0\}$.

(7) Gelegentlich wird eine injektive Abbildung $X \longrightarrow Y$ auch $X \hookrightarrow Y$ notiert.

Kapitel 1

Polynomringe und Ideale

1.1 Gruppen, Ringe, Körper

Erinnerung.

(1) Eine *Gruppe* ist eine Menge G, zusammen mit einer Abbildung (Multiplikation)

$$G \times G \quad \xrightarrow{(\cdot)} \quad G\,, \quad (g,h) \quad \longmapsto \quad g \cdot h = gh$$

derart, daß es ein $1 = 1_G \in G$ gibt mit $g \cdot 1 = 1 \cdot g = g$ für $g \in G$, daß es für jedes $g \in G$ ein $g^{-1} \in G$ gibt mit $g \cdot g^{-1} = g^{-1} \cdot g = 1$, und derart, daß $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ für g, h, $k \in G$. Wir schreiben oft kurz G für $(G, \cdot)$.

Ist $g \in G$ und $k \in \mathbf{Z}_{\geqslant 1}$, so schreibe $g^k := \underbrace{g \cdots g}_{k \text{ Faktoren}}$, $g^{-k} := \underbrace{g^{-1} \cdots g^{-1}}_{k \text{ Faktoren}}$ und $g^0 := 1$.

Zum Beispiel ist für gegebenes $n \geqslant 1$ die *symmetrische Gruppe* $\mathcal{S}_n$ eine Gruppe. Ihre Elemente sind *Permutationen* der Menge $[1,n] := \{1, \ldots, n\}$, d.h. Bijektionen von $[1,n]$ nach $[1,n]$. Die Multiplikation ist durch die Komposition von Bijektionen gegeben.

> Auf Gruppen in dieser Allgemeinheit kommen wir in einem späteren Abschnitt noch zu sprechen; vgl. §3.2.

(2) Eine *abelsche Gruppe* ist eine Menge A, zusammen mit einer Abbildung (Addition)

$$A \times A \quad \xrightarrow{(+)} \quad A\,, \quad (a,b) \quad \longmapsto \quad a + b$$

derart, daß $a + b = b + a$ für a, $b \in A$, daß es ein $0 = 0_A \in A$ gibt mit $a + 0 = a$ für $a \in A$, daß es für jedes $a \in A$ ein $-a \in A$ gibt mit $a + (-a) = 0$, und derart, daß $(a + b) + c = a + (b + c)$ für a, b, $c \in A$. Wir schreiben oft kurz A für $(A, +)$. Wir schreiben auch $a - b := a + (-b)$ etc.

Beachte, daß das Element 0 durch die Eigenschaft $a + 0 = a$ für $a \in A$ eindeutig festgelegt ist. Denn gibt es ein $0' \in A$ mit $a + 0' = a$ für $a \in A$, so folgt $0 = 0 + 0' = 0'$.

Beachte, daß für $a \in A$ das Element $-a$ durch die Eigenschaft $a+(-a) = 0$ eindeutig festgelegt ist. Denn gibt es ein $b \in A$ mit $a + b = 0$, so folgt $b = b + a + (-a) = -a$.

Ist $a \in A$ und $k \in \mathbf{Z}_{\geqslant 1}$, so schreibe $ka := \underbrace{a + \cdots + a}_{k \text{ Summanden}}$, $(-k)a := \underbrace{(-a) + \cdots + (-a)}_{k \text{ Summanden}}$ und $0 \cdot a := 0$.

Zum Beispiel bilden die ganzen Zahlen $\mathbf{Z}$ zusammen mit der üblichen Addition $(+)$ eine abelsche Gruppe.

Beachte, daß eine abelsche Gruppe auch multiplikativ geschrieben werden kann. Diesenfalls wird das neutrale Element mit 1 und das zu $a \in A$ inverse Element mit a^{-1} bezeichnet.

Eine Gruppe G wie in (1) ist abelsch, falls $gh = hg$ für $g, h \in G$.

(3) Ein *kommutativer Ring* ist eine Menge R, zusammen mit Abbildungen (Addition und Multiplikation)

$$\begin{array}{lcll} R \times R & \xrightarrow{(+)} & R\,, & (r,s) \longmapsto r+s \\ R \times R & \xrightarrow{(\cdot)} & R\,, & (r,s) \longmapsto r \cdot s = rs \end{array}$$

derart, daß $(R, +)$ eine abelsche Gruppe ist, mit Nullelement $0 = 0_R$, daß $r \cdot s = s \cdot r$ für $r, s \in R$, daß es ein Element $1 = 1_R$ gibt mit $r \cdot 1 = r$ für $r \in R$, und derart, daß $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ und $(r + s) \cdot t = r \cdot t + s \cdot t$ für $r, s, t \in R$.

Wir schreiben oft kurz R für $(R, +, \cdot)$.

Falls erforderlich, schreiben wir auch $(+_R) := (+)$ und $(\cdot_R) := (\cdot)$.

Es gelte die Regel "Punkt vor Strich", d.h. $a + b \cdot c := a + (b \cdot c)$ etc.

Beachte, daß das Element 1 durch die Eigenschaft $r \cdot 1 = r$ für $r \in R$ eindeutig festgelegt ist. Denn gibt es ein $1' \in R$ mit $r \cdot 1' = r$ für $r \in R$, so folgt $1 = 1 \cdot 1' = 1'$.

Beachte, daß $0 \cdot r = 0 \cdot r + 0 \cdot r - 0 \cdot r = (0+0) \cdot r - 0 \cdot r = 0 \cdot r - 0 \cdot r = 0$ für $r \in R$.

Beachte, daß $(-r) \cdot s = (-r) \cdot s + r \cdot s - r \cdot s = ((-r) + r) \cdot s - r \cdot s = 0 \cdot s - r \cdot s = -r \cdot s$ für $r, s \in R$.

Ist $r \in R$ und $k \in \mathbf{Z}_{\geqslant 1}$, so schreibe $r^k := \underbrace{r \cdots r}_{k \text{ Faktoren}}$ und $r^0 := 1$.

Zum Beispiel bilden die ganzen Zahlen $\mathbf{Z}$ zusammen mit der üblichen Addition $(+)$ und der üblichen Multiplikation $(\cdot)$ einen kommutativen Ring.

(4) Ein *Körper* ist ein kommutativer Ring K, für welchen $(K \smallsetminus \{0\}, \cdot)$ eine abelsche Gruppe ist.

Zum Beispiel ist $\mathbf{Z}$ kein Köper. Wohl aber sind $\mathbf{Q}$, $\mathbf{R}$ und $\mathbf{C}$ Körper. Wir werden noch weitere Beispiele kennenlernen. In der Tat dient dieses Kapitel §1 dazu, zur Konstruktion weiterer Beispiele das nötige Werkzeug bereitzustellen.

Beachte, daß es in einem kommutativen Ring für ein Element $r \in R$ höchstens ein r' mit $rr' = 1$ gibt. Denn ist dazuhin $rr'' = 1$, so folgt $r' = r''rr' = r''$. Das Element r heißt diesenfalls *invertierbar,* und wir schreiben $r^{-1} := r'$.

Bemerkung. *Ein kommutativer Ring R ist ein Körper genau dann, wenn $0_R \neq 1_R$ und jedes $r \in R \setminus \{0\}$ invertierbar ist.*

Beweis. Schreibe in diesem Beweis $R^\times := R \setminus \{0\}$.

($\Longrightarrow$). Ist R ein Körper, so halten wir zunächst fest, daß $1_R \in R^\times$. Denn wäre $1_R = 0_R$, so wäre $r = r \cdot 1_R = r \cdot 0_R = 0_R$ für $r \in R$, und also $R^\times = \emptyset$, und somit keine abelsche Gruppe, da diese wenigstens das Element $1_{R^\times}$ enthält.

Mit oben gesehener Eindeutigkeit ist also $1_R = 1_{R^\times}$. Somit gibt es zu $r \in R^\times$ ein r^{-1} mit $rr^{-1} = 1_{R^\times} = 1_R$, da $(R^\times, \cdot)$ eine abelsche Gruppe ist.

($\Longleftarrow$). Sei umgekehrt $0_R \neq 1_R$ und r^{-1} existent für alle $r \in R^\times$. Zunächst können wir auf $R^\times$ die Multiplikationsabbildung $(\cdot)|^{R^\times}_{(R^\times)\times(R^\times)}$ definieren. Denn *nehmen wir an,* es gibt $r,\, s \in R^\times$ mit $rs = 0$. Dann ist $s = r^{-1}rs = r^{-1} \cdot 0 = 0$, *Widerspruch.*

Ferner, ist $r \in R^\times$, so ist auch $r^{-1} \in R^\times$. Denn *wäre* $r^{-1} = 0_R$, so wäre $1_R = r^{-1} \cdot r = 0_R \cdot r = 0_R$, *Widerspruch.*

Nun gelten mit $1_{R^\times} := 1_R$ in $R^\times$ alle Gesetze einer multiplikativ geschriebenen abelschen Gruppe: es ist $r \cdot s = s \cdot r$ für $r,\, s \in R^\times$, es ist $r \cdot 1_{R^\times} = r$ für $r \in R^\times$, es ist $r \cdot r^{-1} = 1_{R^\times}$ für $r \in R^\times$ und es ist $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ für $r,\, s,\, t \in R^\times$, da dies jeweils in R gilt. ▫

1.2 Ideale

Definition. Sei R ein kommutativer Ring. Eine Teilmenge $I \subseteq R$ heißt *Ideal*, falls $0 \in I$, falls für alle $x,\, y \in I$ gilt, daß $x - y \in I$, und falls für alle $r \in R$ und alle $x \in I$ auch $rx \in I$ ist.

Bemerkung. *Ist $I \subseteq R$ ein Ideal, und sind $x,\, y \in R$, dann ist auch $-x = 0 - x \in I$, und damit auch $x + y = x - (-y) \in I$.*

Beispiel. Für $a \in \mathbf{Z}$ ist die Teilmenge $a\mathbf{Z} := \{az \,:\, z \in \mathbf{Z}\} \subseteq \mathbf{Z}$ ein Ideal.

Beispiel. Allgemeiner, ist R ein kommutativer Ring, und ist $r \in R$, so ist die Teilmenge $rR := \{rs \;:\; s \in R\} \subseteq R$ ein Ideal. Ideale von dieser Form heißen *Hauptideale.* Man spricht auch von r als vom *Erzeuger* von rR. Beachte, daß für $s \in R$ invertierbar gilt, daß $rR = srR$.

Beispiel. Sei R ein kommutativer Ring. Die Teilmengen $\{0\} = 0R \subseteq R$ und $R = 1R \subseteq R$ sind Ideale.

Bemerkung. Sei R ein kommutativer Ring. Sei $I \subseteq R$ ein Ideal. Es ist $I = R$ genau dann, wenn $1 \in I$.

Beweis. Ist $I = R$, so ist $1 \in I$. Ist umgekehrt $1 \in I$, dann auch $r = r \cdot 1 \in I$ für alle $r \in R$, woraus $I = R$ folgt. ▫

Bemerkung. *Sind I und J Ideale in R, so trifft dies auch auf $I \cap J$ und $I + J := \{x + y \,:\, x \in I,\, y \in J\}$ zu.*

Beweis. Zu $I \cap J$. Es ist $0 \in I \cap J$. Sind $x, y \in I \cap J$, so ist auch $x - y \in I \cap J$, da I und J unter Differenzbildung abgeschlossen sind. Ist dazuhin $r \in R$, so ist auch $rx \in I \cap J$, da I und J unter Multiplikation mit beliebigen Elementen aus R abgeschlossen sind.

Zu $I+J$. Es ist $0 = 0+0 \in I \cap J$. Sind $x, y \in I+J$, so können wir $x = x'+x''$ und $y = y'+y''$ mit $x', y' \in I$ und $x'', y'' \in J$ schreiben. Es wird $x - y = (x' - y') + (x'' - y'') \in I + J$. Ist dazuhin $r \in R$, so ist auch $rx = rx' + rx'' \in I + J$. ▫

Bemerkung. *Ein kommutativer Ring R ist ein Körper genau dann, wenn er zwei Ideale enthält. Diesenfalls sind dies $\{0\}$ und R.*

Beweis. ($\Longrightarrow$). Sei R ein Körper. Sei $I \subseteq R$ ein Ideal, und sei $I \neq \{0\}$. Wir wollen zeigen, daß $I = R$, und zeigen dazu, daß $R \subseteq I$. Sei $r \in R$. Wir wollen zeigen, daß $r \in I$. Nun gibt es ein $x \in I \setminus \{0\}$. Also ist $r = x(x^{-1}r) \in I$. Somit sind $\{0\}$ und R die einzigen Ideale von R.

Ferner ist $\{0\} \neq R$, da in einem Körper $0 \neq 1$, und somit $1 \in R$, aber $1 \notin \{0\}$. Also enthält R zwei Ideale, nämlich $\{0\}$ und R.

($\Longleftarrow$). Enthalte R zwei Ideale. Es enthält R die Ideale $\{0\}$ und R. *Wäre* $\{0\} = R$, so wäre $\{0\}$ mangels weiterer Teilmengen, die 0 enthalten, das einzige Ideal in R, *Widerspruch.* Also ist $\{0\} \neq R$, und dies sind die einzigen Ideale von R.

Es ist $1 \neq 0$, da sonst wegen $r = r \cdot 1 = r \cdot 0 = 0$ für $r \in R$ auch $R = \{0\}$ wäre.

Sei nun $r \in R \setminus \{0\}$. Wir bilden das Ideal rR. Da es r enthält, ist es ungleich $\{0\}$, und somit gleich R. Also gibt es ein $s \in R$ mit $rs = 1$. D.h., r istW invertierbar. ▫

1.3 Faktorringe

Sei I ein Ideal in einem kommutativen Ring R. Für $r, s \in R$ schreiben wir $r \equiv_I s$, gesprochen "r kongruent modulo I zu s", falls $r - s \in I$. Ist $I = tR$ für ein $t \in R$, so schreiben wir auch kurz $\equiv_t$ statt $\equiv_{tR}$.

Bemerkung. *Es ist $(\equiv_I)$ eine Äquivalenzrelation auf R.*

Beweis. Es ist $(\equiv_I)$ reflexiv, da $r \equiv_I r$ aus $r - r = 0 \in I$ folgt für $r \in R$. Es ist $(\equiv_I)$ symmetrisch, da für $r, s \in R$

$$r \equiv_I s \implies r - s \in I \implies s - r \in I \implies s \equiv_I r\,.$$

Es ist $(\equiv_I)$ transitiv, da für $r, s, t \in R$ aus $r \equiv_I s$ und $s \equiv_I t$ folgt, daß $r - t = (r - s) + (s - t) \in I$, und also $r \equiv_I t$. ▫

Sei mit $r + I$ die Äquivalenzklasse von $r \in R$ bezüglich $(\equiv_I)$ bezeichnet. In der Tat ist $r + I = \{r + x \,:\, x \in I\}$. Schreibe $R/I := R/\equiv_I$ für die Menge der Äquivalenzklassen.

Lemma. *Mittels $(r + I) + (s + I) := (r + s) + I$ und $(r + I) \cdot (s + I) := (r \cdot s) + I$ für $r, s \in R$ wird R/I zu einem kommutativen Ring, dem* Faktorring *von R modulo I.*

Beweis. Zunächst ein etwas heikler Punkt. Definiert man eine Abbildung auf Äquivalenzklassen unter Verwendung von gewählten Repräsentanten, wie eben für $(+)$ und $(\cdot)$ auf R/I geschehen, so hat man zunächst zu zeigen, daß das Bildelement nicht von der Wahl der Repräsentanten abhängt.

Allgemein nennt man die Aussage, daß eine gewisse Setzung in der Tat eine Abbildung definiert, auch die *Wohldefiniertheit* der betreffenden Abbildung. Wir zeigen also zunächst die Wohldefiniertheit von Addition und Multiplikation.

Seien also r, r', s, $s' \in R$ gegeben mit $r \equiv_I r'$ und $s \equiv_I s'$. Dann ist

$$r + s \ \equiv_I \ r + s + (r' - r) + (s' - s) \ = \ r' + s' \ ,$$

sowie

$$r \cdot s \ \equiv_I \ r \cdot s + (r' - r) \cdot s + r' \cdot (s' - s) \ = \ r' \cdot s' \ .$$

Nun zum Nachweis der Eigenschaften eines kommutativen Ringes. Seien $0_{R/I} := 0_R + I$ und $1_{R/I} := 1_R + I$ angesetzt. Sei ferner $-(r + I) := (-r) + I$ angesetzt, wobei $r \in R$.

Wir erhalten folgende Identitäten. Seien r, s, $t \in R$.

$$\begin{aligned}
&(r + I) + (s + I) \ = \ (r + s) + I \ = \ (s + r) + I \ = \ (s + I) + (r + I) \\
&(r + I) + (0 + I) \ = \ (r + 0) + I \ = \ r + I \\
&(r + I) + ((-r) + I) \ = \ (r + (-r)) + I \ = \ 0 + I \\
&((r + I) + (s + I)) + (t + I) \ = \ ((r + s) + t) + I \ = \ (r + (s + t)) + I \\
&\qquad\qquad = \ (r + I) + ((s + I) + (t + I)) \\
&(r + I) \cdot (s + I) \ = \ (r \cdot s) + I \ = \ (s \cdot r) + I \ = \ (s + I) \cdot (r + I) \\
&(r + I) \cdot (1 + I) \ = \ (r \cdot 1) + I \ = \ r + I \\
&((r + I) \cdot (s + I)) \cdot (t + I) \ = \ ((r \cdot s) \cdot t) + I \ = \ (r \cdot (s \cdot t)) + I \\
&\qquad\qquad = \ (r + I) \cdot ((s + I) \cdot (t + I)) \\
&((r + I) + (s + I)) \cdot (t + I) \ = \ ((r + s) \cdot t) + I \ = \ (r \cdot t + s \cdot t) + I \\
&\qquad\qquad = \ (r + I) \cdot (t + I) + (s + I) \cdot (t + I)
\end{aligned}$$

Kurz, die geforderten Eigenschaften für R/I vererben sich von denen für R. ▫

Beispiel. Es ist R/R ein Ring mit nur einem Element, $0 + R = 1 + R$.

Beispiel. Es ist für $n \geqslant 0$ der Ring $\mathbf{Z}/n\mathbf{Z}$ ein Ring mit n Elementen,

$$\mathbf{Z}/n\mathbf{Z} \ = \ \{0 + n\mathbf{Z}, \ldots, (n-1) + n\mathbf{Z}\} \ .$$

Sei nämlich $k \in \mathbf{Z}$ gegeben. Mit einer Division mit Rest können wir $k = nz + w$ schreiben, wobei $w \in [0, n-1]$. Also taucht $k + n\mathbf{Z} = w + n\mathbf{Z}$ in dieser Liste auf. Umgekehrt, ist $w + n\mathbf{Z} = w' + n\mathbf{Z}$ für $0 \leqslant w \leqslant w' \leqslant n-1$, so ist $w' - w \in n\mathbf{Z} \cap [0, n-1] = \{0\}$, und also $w = w'$.

Wir sind aber an diese Liste von Repräsentanten nicht gebunden. Zum Beispiel ist alternativ $-1 + n\mathbf{Z} = (n-1) + n\mathbf{Z}$. Beachte nun, daß es für Rechnungen oft einfacher ist, $-1 + n\mathbf{Z}$ zu verwenden. So etwa ist $(-1 + n\mathbf{Z})^2 = (-1)^2 + n\mathbf{Z} = 1 + n\mathbf{Z}$; oder aber auch $((n-1) + n\mathbf{Z})^2 = (n-1)^2 + n\mathbf{Z} = n^2 - 2n + 1 + n\mathbf{Z} = 1 + n\mathbf{Z}$.

Konvention. Ist aus dem Kontext ersichtlich, daß wir in $\mathbf{Z}/n\mathbf{Z}$ rechnen, so schreiben wir auch kurz x statt $x + n\mathbf{Z}$.

Diese Konvention ist praktisch unumgänglich, will man mit Polynomen mit Koeffizienten aus $\mathbf{Z}/n\mathbf{Z}$ rechnen; vgl. §1.6 unten.

1.4 Ringmorphismen

1.4.1 Definition und Schreibweise

Definition. Seien R und S kommutative Ringe. Eine Abbildung $R \xrightarrow{f} S$ heißt *Ringmorphismus* oder auch *Morphismus von Ringen,* falls $f(1_R) = 1_S$, $f(r + r') = f(r) + f(r')$ und $f(r \cdot r') = f(r) \cdot f(r')$ für alle r, $r' \in R$ ist. Beachte, daß dann auch

$$f(0_R) \;=\; f(0_R) + f(0_R) - f(0_R) \;=\; f(0_R + 0_R) - f(0_R) \;=\; f(0_R) - f(0_R) \;=\; 0_S$$

und

$$f(-r) \;=\; f(-r)+f(r)-f(r) \;=\; f(-r+r)-f(r) \;=\; f(0_R)-f(r) \;=\; 0_S-f(r) \;=\; -f(r)$$

für $r \in R$ ist.

Beispiel. Sei $I \subseteq R$ ein Ideal. Die Restklassenabbildung $R \xrightarrow{\rho} R/I$, $r \longmapsto r + I$ ist ein Ringmorphismus.

Ein bijektiver Ringmorphismus $R \xrightarrow{f} S$ heißt *Ringisomorphismus* oder auch *Isomorphismus von Ringen*, symbolisch geschrieben $R \xrightarrow[\sim]{f} S$. Gibt es einen Ringisomorphismus von R nach S, so heißen R und S isomorph, geschrieben $R \simeq S$.

Ein Isomorphismus $R \xrightarrow[\sim]{f} R$ von R nach R heißt auch *Ringautomorphismus* oder *Automorphismus von Ringen.*

Isomorphe kommutative Ringe sind "im wesentlichen gleich". Vorsicht, ein nichtidentischer Isomorphismus $R \xrightarrow{\sim} R$ ist von der Identität dagegen wesentlich verschieden. Man kann also nicht generell sagen, Isomorphismen seien quasi Gleichheiten.

Ein Ringmorphismus zwischen Körpern heißt auch *Körpermorphismus.* Etc.

Beispiel. Es ist $R \longrightarrow R/\{0\}$, $r \longmapsto r + \{0\}$ ein Ringisomorphismus. Insbesondere ist $R \simeq R/\{0\}$.

Beispiel. Es ist $\mathbf{C} \longrightarrow \mathbf{C}$, $z = u\mathrm{i} + v \longmapsto -u\mathrm{i} + v =: \bar{z}$ der Körperisomorphismus der komplexen Konjugation, wobei u, $v \in \mathbf{R}$. In der Tat ist

$$\begin{array}{lcll} \overline{1} & = & 1 & \\ \overline{(u\mathrm{i}+v)+(u'\mathrm{i}+v')} & = & -u\mathrm{i}-u'\mathrm{i}+v+v' & = \; \overline{(u\mathrm{i}+v)}+\overline{(u'\mathrm{i}+v')} \\ \overline{(u\mathrm{i}+v)\cdot(u'\mathrm{i}+v')} & = & -uu'-uv'\mathrm{i}-u'v\mathrm{i}+vv' & = \; \overline{(u\mathrm{i}+v)}\cdot\overline{(u'\mathrm{i}+v')} \end{array}$$

wobei u, u', v, $v' \in \mathbf{R}$. Und die komplexe Konjugation unterscheidet sich wesentlich von der Identität auf $\mathbf{C}$.

Bemerkung. *Ist $R \xrightarrow{f} S$ ein Ringisomorphismus zwischen kommutativen Ringen, so auch $S \xrightarrow{f^{-1}} R$.*

Beweis. Es ist $f^{-1}(1_S) = f^{-1}(f(1_R)) = 1_R$. Für s, $s' \in S$ ist

$$f^{-1}(s+s') = f^{-1}(f(f^{-1}(s))+f(f^{-1}(s'))) = f^{-1}(f(f^{-1}(s)+f^{-1}(s'))) = f^{-1}(s)+f^{-1}(s')$$

und

$$f^{-1}(s \cdot s') = f^{-1}(f(f^{-1}(s)) \cdot f(f^{-1}(s'))) = f^{-1}(f(f^{-1}(s) \cdot f^{-1}(s'))) = f^{-1}(s) \cdot f^{-1}(s') \,.$$

□

Bemerkung. *Sind $R \xrightarrow{f} S$ und $S \xrightarrow{g} T$ Ringmorphismen zwischen kommutativen Ringen, so auch $R \xrightarrow{g \circ f} T$.*

Beweis. Es ist $(g \circ f)(1_R) = g(1_S) = 1_T$. Für r, $r' \in R$ ist $(g \circ f)(r+r') = g(f(r)+f(r')) = (g \circ f)(r) + (g \circ f)(r')$ und $(g \circ f)(r \cdot r') = g(f(r) \cdot f(r')) = (g \circ f)(r) \cdot (g \circ f)(r')$. □

Bemerkung. *Sei $R \xrightarrow{f} S$ ein Ringmorphismus zwischen kommutativen Ringen. Sei $r \in R$ invertierbar. Dann ist $f(r)$ invertierbar, und es ist $f(r)^{-1} = f(r^{-1})$.*

Beweis. Es ist $f(r^{-1})f(r) = f(r^{-1}r) = f(1_R) = 1_S$. □

1.4.2 Teilringe

Definition. Sei $S = (S, +_S, \cdot_S)$ ein kommutativer Ring. Eine Teilmenge $T \subseteq S$ heißt *Teilring,* falls $1_S \in T$ und falls für alle t, $t' \in T$ auch $t - t' \in T$ und $tt' \in T$. Beachte, daß dann auch $0_S = 1_S - 1_S \in T$ und daß mit t, $t' \in T$ auch $-t = 0 - t \in T$ und $t + t' = t - (-t') \in T$.

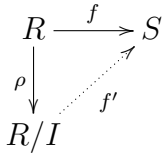
Mit $1_T := 1_S$ und $0_T := 0_S$, sowie $(+_T) := (+_S)|^T_{T \times T}$ und $(\cdot_T) := (\cdot_S)|^T_{T \times T}$ wird $(T, \cdot_T, +_T)$ ersichtlich ein kommutativer Ring – die verlangten Eigenschaften gelten alle bereits in S.

Diesenfalls ist die Inklusionsabbildung $T \longrightarrow S$, $t \longmapsto t$ ein Ringmorphismus.

Beispiel. Es ist $\mathbf{Z}$ ein Teilring von $\mathbf{Q}$. Dies zeigt, daß Teilringe von Körpern nicht notwendig Körper sind.

1.4.3 Gebrauchsanweisung für Faktorringe

Bemerkung. *Sei R ein kommutativer Ring, und sei $I \subseteq R$ ein Ideal. Sei S ein weiterer kommutativer Ring, und sei $R \xrightarrow{f} S$ ein Ringmorphismus mit $f(I) = \{0\}$. Dann gibt es genau einen Ringmorphismus $R/I \xrightarrow{f'} S$ derart, daß $f' \circ \rho = f$.*



Beweis. Die Eindeutigkeit von f' folgt aus der Surjektivität von $R \xrightarrow{\rho} R/I$. Wir müssen ein solches f' konstruieren. Wir setzen $f'(r+I) := f(r)$ für $r \in R$. Dies gibt eine wohldefinierte Abbildung $R/I \xrightarrow{f'} S$, da für $r, r' \in R$ mit $r \equiv_I r'$ auch

$$f(r) \;=\; f(r) + f(r'-r) \;=\; f(r+r'-r) = f(r')$$

ist. Nun ist $f'(1_{R/I}) = f'(1_R + I) = f(1_R)$. Für $r, r' \in R$ ist ferner

$$\begin{aligned} f'((r+I)+(r'+I)) \;&=\; f'((r+r')+I) \;=\; f(r+r') \;=\; f(r)+f(r') \\ &= f'(r+I)+f'(r'+I) \\ f'((r+I)\cdot(r'+I)) \;&=\; f'((r\cdot r')+I) \;=\; f(r\cdot r') \;=\; f(r)\cdot f(r') \\ &= f'(r+I)\cdot f'(r'+I)\,. \end{aligned}$$

Also ist f' auch ein Ringmorphismus. ▫

Sei $R \xrightarrow{f} S$ ein Ringmorphismus kommutativer Ringe. Seien *Kern* und *Bild* von f wie folgt definiert.

$$\begin{array}{lcccccl} \operatorname{Kern} f & := & f^{-1}(\{0\}) & = & \{r \in R \,:\, f(r) = 0_S\} & \subseteq & R \quad \text{(dt. Kern).} \\ \operatorname{Im} f & := & f(R) & = & \{f(r) \,:\, r \in R\} & \subseteq & S \quad \text{(engl. image).} \end{array}$$

Lemma.

(1) *Es ist* $\operatorname{Kern} f \subseteq R$ *ein Ideal.*

(2) *Es ist* $\operatorname{Im} f \subseteq S$ *ein Teilring.*

(3) *Es ist f injektiv genau dann, wenn* $\operatorname{Kern} f = \{0\}$.

(4) *Es ist die Abbildung* $R/\operatorname{Kern} f \xrightarrow{\tilde{f}} \operatorname{Im} f,\ r + \operatorname{Kern} f \longmapsto f(r)$ *ein Isomorphismus von Ringen.*

Beweis.

Ad (1). Es ist $0_R \in \operatorname{Kern} f$, da $f(0_R) = 0_S$. Sind $x, y \in \operatorname{Kern} f$, so ist auch $x-y \in \operatorname{Kern} f$, da $f(x-y) = f(x) - f(y) = 0_S - 0_S = 0_S$. Sind $r \in R$ und $x \in \operatorname{Kern} f$, so ist auch $rx \in \operatorname{Kern} f$, da $f(rx) = f(r)f(x) = f(r)\cdot 0_S = 0_S$.

Ad (2). Es ist $1_S = f(1_R) \in \operatorname{Im} f$. Ferner, sind $t, t' \in \operatorname{Im} f$, so können wir $t = f(r)$ und $t' = f(r')$ schreiben für gewisse $r, r' \in R$. Also sind $t - t' = f(r) - f(r') = f(r-r') \in \operatorname{Im} f$ und $tt' = f(r)f(r') = f(rr') \in \operatorname{Im} f$.

Ad (3). Allgemein ist $\operatorname{Kern} f = f^{-1}(\{0_S\}) \supseteq \{0_R\}$.

($\Longrightarrow$). Ist f injektiv, so ist also $f^{-1}(\{0_S\}) = \{0_R\}$.

($\Longleftarrow$). Ist umgekehrt $f^{-1}(\{0_S\}) = \{0_R\}$, und sind r, $r' \in R$ mit $f(r) = f(r')$ gegeben, so ist $0_S = f(r) - f(r') = f(r - r')$, und also $r - r' \in f^{-1}(\{0_S\}) = \{0_R\}$, d.h. $r = r'$.

Ad (4). Mit vorstehender Bemerkung, angewandt auf den Ringmorphismus $R \xrightarrow{f|^{\operatorname{Im} f}} \operatorname{Im} f$, erhalten wir die Wohldefiniertheit von $\tilde{f}$ und die Tatsache, daß es sich um einen Ringmorphismus handelt. Bleibt noch die Bijektivität von $\tilde{f}$ zu überprüfen. Nach Konstruktion ist $\tilde{f}$ surjektiv. Mit (3) bleibt also zu zeigen, daß der Kern von $\tilde{f}$ nur $0_{R/\operatorname{Kern} f} = 0 + \operatorname{Kern} f$ enthält. Sei $r \in R$ mit $\tilde{f}(r + \operatorname{Kern} f) = 0$ vorgegeben. Dann ist $f(r) = \tilde{f}(r + \operatorname{Kern} f) = 0$. Also ist $r \in \operatorname{Kern} f$, und somit $r + \operatorname{Kern} f = 0 + \operatorname{Kern} f$. ▫

Insgesamt gibt der Ringmorphismus $R \xrightarrow{f} S$ also Anlaß zu den Ringmorphismen

$$R \xrightarrow{\text{surj.}} R/\operatorname{Kern} f \xrightarrow[\sim]{\tilde{f}} \operatorname{Im} f \xrightarrow{\text{inj.}} S\,,$$

die komponiert auch wieder f ergeben.

1.5 Integritätsbereiche

Definition. Ein kommutativer Ring R heißt *Integritätsbereich,* falls $1_R \neq 0_R$ und falls für alle $x \in R \setminus \{0\}$ die Abbildung $R \longrightarrow R$, $r \longmapsto xr$ injektiv ist.

Bemerkung. *Ein kommutativer Ring R ist ein Integritätsbereich genau dann, wenn $1_R \neq 0_R$ und wenn für r, $s \in R \setminus \{0\}$ auch $r \cdot s \neq 0$ ist.*

Beweis. Ist $r \longmapsto xr$ injektiv für alle $x \in R \setminus \{0\}$, und sind r, $s \in R \setminus \{0\}$ gegeben, dann folgt aus $s \neq 0$, daß $rs \neq r0 = 0$. Ist umgekehrt für r, $s \in R \setminus \{0\}$ auch $r \cdot s \neq 0$, und sind $x \in R \setminus \{0\}$ sowie r, $r' \in R$ mit $xr = xr'$ gegeben, so folgt $x(r - r') = 0$, und daher, da $x \neq 0$, auch $r - r' = 0$, und also $r = r'$. Dies zeigt die Injektivität von $r \longmapsto xr$. ▫

Beispiel. Der Ring der ganzen Zahlen $\mathbf{Z}$ ist ein Integritätsbereich.

Beispiel. Der Ring $\mathbf{Z}/4\mathbf{Z}$ ist kein Integritätsbereich, da $(2 + 4\mathbf{Z})(2 + 4\mathbf{Z}) = 0$, aber $2 + 4\mathbf{Z} \neq 0$.

Beispiel. Jeder Körper ist ein Integritätsbereich. Allgemeiner, jeder Teilring eines Körpers ist ein Integritätsbereich. Allgemeiner, jeder Teilring eines Integritätsbereichts ist ein Integritätsbereich.

Bemerkung. *Sei R ein Integritätsbereich. Seien r, $s \in R \setminus \{0\}$. Es ist $rR = sR$ genau dann, wenn es ein invertierbares Element $x \in R$ gibt mit $rx = s$.*

Beweis. Ist $rx = s$ mit $x \in R$ invertierbar, so ist $rR = rxR = sR$, da $rxR \subseteq rR$ und $rR = (rx)x^{-1}R \subseteq (rx)R$.

Ist umgekehrt $rR = sR$, so gibt es ein $x \in R$ mit $rx = s$ und ein $y \in R$ mit $sy = x$. Es folgt $rxy = sy = r$, und also, da $r \neq 0$ und R Integritätsbereich, $xy = 1$. ▫

Bemerkung. *Ein endlicher Integritätsbereich R ist ein Körper.*

Beweis. Sei $x \in R \setminus \{0\}$. Wir müssen zeigen, daß x invertierbar ist. Nun ist $R \longrightarrow R$, $r \longmapsto xr$ injektiv. Da aber R endlich ist, ist diese Abbildung auch surjektiv. Mithin gibt es ein $r \in R$ mit $xr = 1$. ▫

Beispiel. Sei $p \in \mathbf{Z}$ prim. Verwendet man Primfaktorzerlegung in $\mathbf{Z}$, so sieht man, daß $\mathbf{Z}/p\mathbf{Z}$ ein Integritätsbereich ist. Denn sind $r,\ s \in \mathbf{Z}$ mit $r \not\equiv_p 0$ und $s \not\equiv_p 0$ gegeben, dann ist auch $rs \not\equiv_p 0$. Mit voriger Bemerkung ist

$$\mathbf{F}_p \ := \ \mathbf{Z}/p\mathbf{Z}$$

also ein Körper. Dieses Beispiel werden wir nochmals, und dann in größerer Allgemeinheit in §§ 1.8.2, 1.8.4 behandeln.

Hierbei steht $\mathbf{F}$ für engl. field. Beachte, daß $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ nur für p prim geschrieben wird. Unten in §1.8.5 werden wir $\mathbf{F}_4$ etc. kennenlernen, diese Körper sind aber anders definiert. Insbesondere wird, wie man nicht oft genug betonen kann, $\mathbf{F}_4 \not\simeq \mathbf{Z}/4\mathbf{Z}$ werden.

Beispiel. Die Multiplikationstafel von $\mathbf{F}_7$ hat folgende Gestalt.

$(\cdot)$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Daß jedes Element ungleich 0 ein multiplikativ Inverses besitzt, bedeutet, daß in jeder Zeile eine 1 zu finden ist. Oder, symmetrisch, in jeder Spalte. Die konkrete Bestimmung des Inversen kann mit dem Euklidschen Algorithmus aus den Übungen vorgenommen werden; vgl. Aufgabe 2.

1.6 Der Polynomring $R[X]$

Die beiden Integritätsbereiche, die uns hauptsächlich beschäftigen werden, sind der Ring $\mathbf{Z}$ der ganzen Zahlen, und der nun einzuführende Ring $K[X]$ der Polynome mit Koeffizienten in einem Körper K. Es wird sich herausstellen, daß sich $\mathbf{Z}$ und $K[X]$ ganz ähnlich verhalten. Zum Beispiel gibt es für beide einen Euklidschen Algorithmus, wie wir in den Übungen sehen; vgl. Aufgaben 2 und 8.

1.6.1 Definition und Schreibweise

Sei R ein kommutativer Ring. Sei $R[X]$ als Menge formaler Polynome mit Koeffizienten in R gegeben, i.e. als

$$R[X] \;:=\; \{\textstyle\sum_{i\geqslant 0} r_i X^i \;:\; r_i \in R, \text{ es gibt ein } m \geqslant 0 \text{ mit } r_i = 0 \text{ für alle } i \geqslant m\}\;.$$

Ihre Elemente heißen *Polynome* in der *Variablen* X mit *Koeffizienten* r_i in R.

Zwei Polynome $\sum_{i\geqslant 0} r_i X^i$ und $\sum_{i\geqslant 0} s_i X^i$ in $R[X]$ sind vereinbarungsgemäß genau dann gleich, wenn $r_i = s_i$ für alle $i \geqslant 0$.

> Begibt man sich auf einen formalen Standpunkt, so ist ein Polynom nichts anderes als die Folge seiner Koeffizienten. Insbesondere ist ein Polynom noch keine Abbildung. Man kann aber jedem Polynom in offensichtlicher Weise eine polynomiale Abbildung zuordnen, siehe §1.6.5 unten. Ist der Ring R ein unendlicher Körper wie $\mathbf{Q}$, $\mathbf{R}$ oder $\mathbf{C}$, so ergibt sich kein wirklicher Unterschied zwischen Polynom und zugehöriger polynomialer Abbildung. Ist R aber ein endlicher Körper, dann passiert es, daß verschiedene Polynome dieselbe polynomiale Abbildung liefern können; vgl. Beispiel in §1.6.5 unten. Um etwa Koeffizientenvergleich machen zu können, muß man sich hier mit dem Auswerten zurückhalten und Polynome als formale Ausdrücke auffassen.
>
> Die Rechenregeln von Polynomen sind von einem solchen feinen Unterschied aber nicht berührt, und sind die, die man erwartet.

Setze für $\sum_{i\geqslant 0} r_i X^i, \sum_{i\geqslant 0} s_i X^i \in R[X]$

$$\begin{array}{lcl} \sum_{i\geqslant 0} r_i X^i \;+\; \sum_{i\geqslant 0} s_i X^i & := & \sum_{i\geqslant 0} (r_i + s_i) X^i \\ \sum_{i\geqslant 0} r_i X^i \;\cdot\; \sum_{j\geqslant 0} s_j X^j & := & \sum_{k\geqslant 0} (\sum_{i\in[0,k]} r_i s_{k-i}) X^k \;=\; \sum_{k\geqslant 0} (\sum_{i,\,j\,\geqslant 0,\; i+j=k} r_i s_j) X^k\;. \end{array}$$

Wir zeigen, daß ein kommutativer Ring vorliegt. Setze $0_{R[X]} = 0_R \cdot X^0 = 0_R$, $1_{R[X]} = 1_R \cdot X^0 = 1_R$ und, für $\sum_{i\geqslant 0} r_i X^i \in R[X]$, das Negative $-\sum_{i\geqslant 0} r_i X^i = \sum_{i\geqslant 0} (-r_i) X^i$ an.

Es ist $(R[X], +)$ eine abelsche Gruppe, wie man koeffizientenweise auf die Tatsache zurückführt, daß $(R, +)$ eine abelsche Gruppe ist.

Seien $\sum_{i\geqslant 0} r_i X^i$, $\sum_{i\geqslant 0} s_i X^i$, $\sum_{i\geqslant 0} t_i X^i \in R[X]$ gegeben.

Es ist $(\sum_{i\geqslant 0} r_i X^i) \cdot 1_{R[X]} = \sum_{i\geqslant 0} r_i X^i$, da sich der Koeffizient für X^k, $k \geqslant 0$, zu $r_k \cdot 1 + r_{k-1} \cdot 0 + \cdots + r_0 \cdot 0 = r_k$ ergibt.

Ersichtlicherweise ist $(\sum_{i\geqslant 0} r_i X^i) \cdot (\sum_{j\geqslant 0} s_j X^j) = (\sum_{j\geqslant 0} s_j X^j) \cdot (\sum_{i\geqslant 0} r_i X^i)$.

Ferner wird

$$\begin{array}{lcl} \big((\sum_{i\geqslant 0} r_i X^i) \cdot (\sum_{j\geqslant 0} s_j X^j)\big) \cdot (\sum_{\ell\geqslant 0} t_\ell X^\ell) & = & (\sum_{k\geqslant 0} \sum_{i,\,j\,\geqslant 0,\; i+j=k} r_i s_j X^k) \cdot (\sum_{\ell\geqslant 0} t_\ell X^\ell) \\ & = & \sum_{m\geqslant 0} \sum_{k,\,\ell\,\geqslant 0,\, k+\ell=m} \sum_{i,\,j\,\geqslant 0,\; i+j=k} r_i s_j t_\ell X^m \\ & = & \sum_{m\geqslant 0} (\sum_{i,\,j,\,\ell\,\geqslant 0,\, i+j+\ell=m} r_i s_j t_\ell) X^m\;, \end{array}$$

und dies ist auch das Resultat von $(\sum_{i\geqslant 0} r_i X^i) \cdot \big((\sum_{j\geqslant 0} s_j X^j) \cdot (\sum_{\ell\geqslant 0} t_\ell X^\ell)\big)$. Desweiteren ist

$$\begin{aligned}
& \big((\textstyle\sum_{i\geqslant 0} r_i X^i) + (\sum_{i\geqslant 0} s_i X^i)\big) \cdot (\sum_{j\geqslant 0} t_j X^j) \\
= \;& (\textstyle\sum_{i\geqslant 0} (r_i + s_i) X^i) \cdot (\sum_{j\geqslant 0} t_j X^j) \\
= \;& \textstyle\sum_{k\geqslant 0} \sum_{i,\, j\,\geqslant 0,\, i+j=k} (r_i + s_i) t_j X^k \\
= \;& \textstyle\sum_{k\geqslant 0} \sum_{i,\, j\,\geqslant 0,\, i+j=k} (r_i t_j + s_i t_j) X^k \\
= \;& \big(\textstyle\sum_{k\geqslant 0} \sum_{i,\, j\,\geqslant 0,\, i+j=k} r_i t_j X^k\big) + \big(\sum_{k\geqslant 0} \sum_{i,\, j\,\geqslant 0,\, i+j=k} s_i t_j X^k\big) \\
= \;& (\textstyle\sum_{i\geqslant 0} r_i X^i) \cdot (\sum_{j\geqslant 0} t_j X^j) + (\sum_{i\geqslant 0} s_i X^i) \cdot (\sum_{j\geqslant 0} t_j X^j)
\end{aligned}$$

Somit ist $R[X] = (R[X], +, \cdot)$ ein kommutativer Ring, genannt der *Polynomring* (über R in einer Variablen X).

Der Tradition folgend, schreibt man auch oft z.B.

$$f \;=\; f(X) \;=\; \sum_{i\geqslant 0} f_i X^i$$

für ein Element von $R[X]$. Dies sei auch unsere Standardschreibweise.

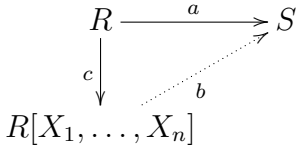
> Beachte, daß im nachhinein die Schreibweise $\sum_{i\geqslant 0} f_i X^i$ dadurch gerechtfertigt ist, daß mit der eben eingeführten Multiplikation und Addition hierbei in der Tat die Summe über alle Produkte $f_i \cdot X \cdots X$ (i Faktoren) vorliegt. Es ist also $\sum_{i\geqslant 0} f_i X^i$ nicht nur ein formaler, sondern in $R[X]$ auch ein regelgerecht aus den Polynomen $f_i = f_i \cdot X^0$ und aus dem Polynom $X = 1 \cdot X^1$ gebildeter Ausdruck.
>
> Vorsicht, diese Schreibweise impliziert nicht, daß $f(X)$ eine Funktion ist. Wohl aber kann man aus $f(X)$ eine Funktion gewinnen; vgl. §1.6.5 unten.

Wir behalten uns noch vor, andere Variablennamen statt X zu verwenden, in der Regel mit Großbuchstaben bezeichnet. So z.B. kann man $R[X,Y] := (R[X])[Y]$ definieren, etc. Ein Element von $R[X,Y]$ hat dann die Form $f(X,Y) = \sum_{i\geqslant 0,\, j\geqslant 0} f_{i,j} X^i Y^j$ mit $f_{i,j} \in R$. Etc.

1.6.2 Gebrauchsanweisung für Polynomringe

Sei $n \geqslant 1$. Schreibe $R \xrightarrow{c} R[X_1, \ldots, X_n]$, $r \longmapsto r$, wobei das Bild das konstante Polynom mit Wert r bedeute.

Bemerkung. *Sei S ein weiterer kommutativer Ring, und sei $R \xrightarrow{a} S$ ein Ringmorphismus. Seien $s_1, \ldots, s_n \in S$ gegeben. Dann gibt es genau einen Ringmorphismus $R[X_1, \ldots, X_n] \xrightarrow{b} S$ so, daß zum einen $b \circ c = a$, und so, daß zum anderen $b(X_i) = s_i$ für $i \in [1, n]$.*



Schreibe noch

$$f^a(s_1,\dots,s_n) \;:=\; \textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} a(f_{i_1,\dots,i_n}) s_1^{i_1}\cdots s_n^{i_n}$$

für das Bild von $f(X_1,\dots,X_n)$ unter b; vgl. Beweis.

Ist a die Einbettung eines Teilrings $R\subseteq S$, so schreibe auch

$$f(s_1,\dots,s_n) \;:=\; f^a(s_1,\dots,s_n) \;=\; \textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} f_{i_1,\dots,i_n} s_1^{i_1}\cdots s_n^{i_n}\ .$$

Merke: ein Ringmorphismus von einem Polynomring aus wird durch Einsetzen von Werten für die Variablen definiert.

Umgekehrt gesehen: Werte einsetzen in ein Polynom konnten wir immer schon, nur wissen wir nun, daß es sich bei der Prozedur des Einsetzens um einen Ringmorphismus handelt, auf welchen wir unseren Apparat anwenden können.

Beweis. Eindeutigkeit. Sei $\tilde b : R[X_1,\dots,X_n]\longrightarrow S$ ein weiterer solcher Ringmorphismus. Es wird

$$\begin{aligned}
\tilde b(f(X_1,\dots,X_n)) &= \tilde b\big(\textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} f_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}\big)\\
&= \textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} \tilde b(f_{i_1,\dots,i_n})\tilde b(X_1)^{i_1}\cdots \tilde b(X_n)^{i_n}\\
&= \textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} a(f_{i_1,\dots,i_n}) s_1^{i_1}\cdots s_n^{i_n}\\
&= b(f(X_1,\dots,X_n))
\end{aligned}$$

für $f(X_1,\dots,X_n)\in R[X_1,\dots,X_n]$, und mithin $\tilde b = b$.

Existenz. Setze

$$b(f(X_1,\dots,X_n)) \;=\; b\big(\textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} f_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}\big) \;:=\; \textstyle\sum_{i_k\geqslant 0,\ k\in[1,n]} a(f_{i_1,\dots,i_n}) s_1^{i_1}\cdots s_n^{i_n}\ .$$

Dann sind $b\circ c = a$ und $b(X_i) = s_i$ für $i\in[1,n]$ erfüllt. Zeigen wir, daß ein Ringmorphismus vorliegt. Es wird $1_{R[X_1,\dots,X_n]}$ auf 1_S geschickt. Ersichtlich ist das Bild der Summe zweier Polynome unter b gleich der Summe der Bilder. Um also nun noch zu zeigen, daß das Bild des Produktes zweier Polynome unter b gleich dem Produkt der Bilder ist, genügt es, das Produkt zweier Monome zu betrachten, also zweier Polynome, die aus je einem Summanden bestehen. Und in der Tat ist, mit $r,\ r'\in R$ und $i_k,\ i'_k\geqslant 0$ für $k\in[1,n]$,

$$\begin{aligned}
b\big((rX_1^{i_1}\cdots X_n^{i_n})\cdot(r'X_1^{i'_1}\cdots X_n^{i'_n})\big) &= b(rr'X_1^{i_1+i'_1}\cdots X_n^{i_n+i'_n})\\
&= a(rr')s_1^{i_1+i'_1}\cdots s_n^{i_n+i'_n}\\
&= a(r)s_1^{i_1}\cdots s_n^{i_n}\cdot a(r')s_1^{i'_1}\cdots s_n^{i'_n}\\
&= b(rX_1^{i_1}\cdots X_n^{i_n})\cdot b(r'X_1^{i'_1}\cdots X_n^{i'_n})\ .
\end{aligned}$$

□

Beispiel. Mit $n=1$, $R=S$, $a=\mathrm{id}$ und $x=s_1\in R$ erhalten wir den Ringmorphismus $R[X]\longrightarrow R$, $f(X)\longmapsto f(x)$. In Aufgabe 7.(2) war z.B. $x=0$.

Beispiel. Sei $R \xrightarrow{a} S$ ein Morphismus kommutativer Ringe. Wir erhalten mit der Setzung $b(X) := X$ das kommutative Viereck von Ringmorphismen

$$\begin{array}{ccc} R & \xrightarrow{\quad a \quad} & S \\ {\scriptstyle c}\downarrow & & \downarrow{\scriptstyle c} \\ R[X] & \xrightarrow{\quad b \quad} & S[X] \ , \end{array}$$

wobei b ein Polynom $f(X) \in R[X]$ schickt nach $f^a(X) = \sum_{i \geqslant 0} a(f_i) X^i$.

Beispiel. Sei $n = 1$, $R = \mathbf{R}$, $S = \mathbf{C}$ und a die Einbettung von $\mathbf{R}$ nach $\mathbf{C}$. Wir erhalten für $s_1 = \mathrm{i}$ den ersichtlich surjektiven Ringmorphismus $\mathbf{R}[X] \xrightarrow{b} \mathbf{C}$, $X \longmapsto i$. Wegen $\mathrm{i}^2 + 1 = 0$ liegt $X^2 + 1 \in \operatorname{Kern} b$, und damit

$$(X^2+1)\mathbf{R}[X] \quad \subseteq \quad \operatorname{Kern} b \ .$$

Wir haben also auch den Ringmorphismus

$$\begin{array}{rcl} \mathbf{R}[X]/(X^2+1)\mathbf{R}[X] & \xrightarrow{\quad b' \quad} & \mathbf{C} \\ X + (X^2+1)\mathbf{R}[X] & \longmapsto & \mathrm{i} \ , \end{array}$$

welcher ebenfalls surjektiv ist.

Zeigen wir, daß auch

$$(X^2+1)\mathbf{R}[X] \quad \overset{!}{\supseteq} \quad \operatorname{Kern} b \ .$$

Sei also $f(X) \in \mathbf{R}[X]$ mit $b(f(X)) = f(\mathrm{i}) = 0$ gegeben. Sei *angenommen,* es ist $f(X)$ kein Vielfaches von $X^2 + 1$. Division mit Rest liefert, unter Vorgriff auf §1.6.4, daß $f(X) = (X^2+1)q(X) + uX + v$ für gewisse u, $v \in \mathbf{R}$. Da $f(\mathrm{i}) = 0$ und $q(\mathrm{i}) = 0$, folgt $u\mathrm{i} + v = 0$. Da aber u, $v \in \mathbf{R}$, folgt hieraus $u = v = 0$. Also ist $f(X) = (X^2+1)q(X) \in (X^2+1)\mathbf{R}[X]$.

Somit ist insgesamt $(X^2+1)\mathbf{R}[X] = \operatorname{Kern} b$. Mit dem Lemma aus §1.4.3, Teil (4), ist also

$$\begin{array}{rcl} \mathbf{R}[X]/(X^2+1)\mathbf{R}[X] & \xrightarrow[\sim]{\quad b' \quad} & \mathbf{C} \\ X + (X^2+1)\mathbf{R}[X] & \longmapsto & \mathrm{i} \\ uX + v + (X^2+1)\mathbf{R}[X] & \longmapsfrom & u\mathrm{i} + v \ , \end{array}$$

wobei u, $v \in \mathbf{R}$.

Da nun auch $-\mathrm{i}$ eine Nullstelle von $X^2 + 1$ ist, erhalten wir mit genau denselben Argumenten den Isomorphismus

$$\begin{array}{rcl} \mathbf{R}[X]/(X^2+1)\mathbf{R}[X] & \xrightarrow[\sim]{\quad b'' \quad} & \mathbf{C} \\ X + (X^2+1)\mathbf{R}[X] & \longmapsto & -\mathrm{i} \\ -uX + v + (X^2+1)\mathbf{R}[X] & \longmapsfrom & u\mathrm{i} + v \ , \end{array}$$

Komposition liefert den Automorphismus

$$\begin{array}{rcccl} \mathbf{C} & \xrightarrow[\sim]{\quad b'^{-1} \quad} & \mathbf{R}[X]/(X^2+1)\mathbf{R}[X] & \xrightarrow[\sim]{\quad b'' \quad} & \mathbf{C} \\ u\mathrm{i} + v & \longmapsto & uX + v + (X^2+1)\mathbf{R}[X] & \longmapsto & -u\mathrm{i} + v \end{array}$$

der komplexen Konjugation.

Man kann hier vielleicht schon erahnen, daß das eben angewandte Konstruktionsprinzip in einer recht großen Allgemeinheit funktionieren wird. Ferner konnte man erkennen, daß das Polynom X^2+1 hier eine zentrale Rolle spielte. Später werden wir X^2+1 als Minimalpolynom von i über $\mathbf{R}$ bezeichnen.

1.6.3 Grad eines Polynoms

Ist $f = f(X) = \sum_{i\geqslant 0} f_i X^i \in R[X] \smallsetminus \{0\}$, so sei der *Grad* von f definiert durch

$$\deg f \;:=\; \max\{i \geqslant 0 \;:\; f_i \neq 0\} \qquad \text{(engl. degree)}\,.$$

Es heißt $\mathrm{L}(f) := f_{\deg f} \in R\smallsetminus\{0\}$ der *Leitkoeffizient* von f. Ein Polynom mit Leitkoeffizient 1 heißt *normiert.* Ein normiertes Polynom von Grad 1 heißt auch *linear* oder, wenn es in einem Produkt auftritt, *Linearfaktor.*

Wir vereinbaren nun, daß in $\mathbf{Z}\sqcup\{-\infty\}$ gelte, daß $-\infty < z$ und $(-\infty)+z = z+(-\infty) := -\infty$ für alle $z \in \mathbf{Z}$. Ferner sei $(-\infty)+(-\infty) = -\infty$. Wir setzen

$$\deg 0_{R[X]} \;:=\; -\infty\,.$$

Somit haben wir eine Abbildung $R[X] \xrightarrow{\deg} \mathbf{Z}_{\geqslant 0}\sqcup\{-\infty\}$. Das Nullpolynom hat keinen Leitkoeffizienten. Ein Polynom von Grad $\leqslant 0$ heißt auch *konstant.*

Sei R ein Integritätsbereich.

Bemerkung. *Seien $f(X)$, $g(X) \in R[X]\smallsetminus\{0\}$ mit $k := \deg f \geqslant 0$ und $\ell := \deg g \geqslant 0$ gegeben. Dann ist $\deg(f\cdot g) = k+\ell$. Der Leitkoeffizient von $f(X)g(X)$ ist das Produkt der Leitkoeffizienten von $f(X)$ und von $g(X)$.*

Insbesondere ist mit R auch $R[X]$ ein Integritätsbereich.

Beweis. Schreibe $k := \deg f \geqslant 0$ und $\ell = \deg g \geqslant 0$. Der $(k+\ell)$-te Koeffizient von $f(X)g(X)$ berechnet sich zu $f_k g_\ell$. Da f_k, $g_\ell \neq 0$, ist wegen R Integritätsbereich auch $f_k g_\ell \neq 0$. Ferner ist der j-te Koeffizient von $f(X)g(X)$ gleich 0 für $j > k+\ell$. Also ist $\deg(f\cdot g) = k+\ell$. ▫

Bemerkung. *Sind $f(X)$, $g(X) \in R[X]$, so ist*

$$\begin{array}{lcl} \deg(f+g) & \leqslant & \max\{\deg f, \deg g\} \\ \deg(f+g) & = & \max\{\deg f, \deg g\} \quad \textit{falls} \;\; \deg f \neq \deg g \\ \deg(f\cdot g) & = & \deg f + \deg g\,. \end{array}$$

Beweis. Da in $f(X)+g(X) = \sum_{i\geqslant 0}(f_i+g_i)X^i$ der j-te Koeffizient für alle $j > \max\{\deg f, \deg g\}$ verschwindet, folgt die erste Aussage. Ist nun $\deg f \neq \deg g$, so sei ohne Einschränkung $k := \deg f > \deg g$. Es ist der k-te Koeffizient von $f(X)+g(X)$ gleich $f_k \neq 0$, und also $\deg(f+g) = k$, woraus die zweite Aussage folgt.

Die dritte Aussage wurde für $\deg f, \deg g \geqslant 0$ bereits in der vorangehenden Bemerkung gezeigt. Für die verbleibenden Fälle $f = 0$ oder $g = 0$ ist sie aber auch richtig, da diesenfalls auf beiden Seiten der zu zeigenden Gleichung $-\infty$ steht. ▫

1.6.4 Polynomdivision mit Rest

Sei R ein kommutativer Ring. Seien $f(X) \in R[X]$ und $g(X) \in R[X] \smallsetminus \{0\}$ gegeben, und habe $g(X)$ einen invertierbaren Leitkoeffizienten $\mathrm{L}(g)$.

Lemma. *Es gibt Polynome* $q(X)$, $r(X) \in R[X]$ *mit* $\deg r < \deg g$ *und*

$$f(X) \;=\; q(X)g(X) + r(X)\;.$$

Beweis. Schreibe $f^{(0)}(X) := f(X)$.

Schreibe $d_0 := \deg f^{(0)} - \deg g$.

Ist $d_0 < 0$, so können wir $f(X) = 0 \cdot g(X) + f^{(0)}(X)$ schreiben und sind fertig.

Ist $d_0 \geqslant 0$, so schreiben wir $a_0 := \mathrm{L}(f^{(0)})\mathrm{L}(g)^{-1}$ und

$$f^{(0)}(X) \;=:\; a_0 X^{d_0} g(X) + f^{(1)}(X)\;.$$

Der Faktor $a_0 X^{d_0}$ ist hierbei so gewählt, daß die Leitkoeffizienten von $f^{(0)}(X)$ und von $a_0 X^{d_0} g(X)$ übereinstimmen, so daß $\deg f^{(1)} < \deg f^{(0)}$.

Schreibe $d_1 := \deg f^{(1)} - \deg g$.

Ist $d_1 < 0$, so können wir $f(X) = a_0 X^{d_0} g(X) + f^{(1)}(X)$ schreiben und sind fertig.

Ist $d_1 \geqslant 0$, so schreiben wir $a_1 := \mathrm{L}(f^{(1)})\mathrm{L}(g)^{-1}$ und

$$f^{(1)}(X) \;=:\; a_1 X^{d_1} g(X) + f^{(2)}(X)\;.$$

Der Faktor $a_1 X^{d_1}$ ist hierbei so gewählt, daß die Leitkoeffizienten von $f^{(1)}(X)$ und von $a_1 X^{d_1} g(X)$ übereinstimmen, so daß $\deg f^{(2)} < \deg f^{(1)}$.

Schreibe $d_2 := \deg f^{(2)} - \deg g$.

Ist $d_2 < 0$, so können wir $f(X) = (a_0 X^{d_0} + a_1 X^{d_1}) g(X) + f^{(2)}(X)$ schreiben und sind fertig.

Ist $d_2 \geqslant 0$, so schreiben wir $a_2 := \mathrm{L}(f^{(2)})\mathrm{L}(g)^{-1}$ und

$$f^{(2)}(X) \;=:\; a_2 X^{d_2} g(X) + f^{(3)}(X)\;.$$

Der Faktor $a_2 X^{d_2}$ ist hierbei so gewählt, daß die Leitkoeffizienten von $f^{(2)}(X)$ und von $a_2 X^{d_2} g(X)$ übereinstimmen, so daß $\deg f^{(3)} < \deg f^{(2)}$.

Und so fort. Da $\deg f^{(k+1)} < \deg f^{(k)}$ für alle $k \geqslant 0$ und es also ein $\ell \geqslant 0$ mit $d_\ell = \deg f^{(\ell)} - \deg g < 0$ geben muß, bricht der Prozeß nach endlich vielen Schritten erfolgreich ab. ▫

Beispiel. Sei $R = \mathbf{Z}$. Sei $f(X) = 2X^6 + X^3 + 1$, sei $g(X) = -X^2 + 2$. Wir erhalten

$$\underbrace{2X^6 + X^4 + 1}_{f^{(0)}} \;=\; \underbrace{-2}_{a_0} X^4 \cdot (-X^2 + 2) + \underbrace{(4X^4 + X^3 + 1)}_{f^{(1)}},$$

wobei $d_0 = 4$ im Exponent des ersten X auf der rechten Seite zu finden ist. Dann wird

$$\underbrace{(4X^4 + X^3 + 1)}_{f^{(1)}} \;=\; \underbrace{-4}_{a_1} X^2 \cdot (-X^2 + 2) + \underbrace{(X^3 + 8X^2 + 1)}_{f^{(2)}},$$

wobei $d_1 = 2$ im Exponent des ersten X auf der rechten Seite zu finden ist. Dann wird

$$\underbrace{(X^3 + 8X^2 + 1)}_{f^{(2)}} \;=\; \underbrace{-1}_{a_2} X^1 \cdot (-X^2 + 2) + \underbrace{(8X^2 + 2X + 1)}_{f^{(3)}},$$

wobei $d_2 = 1$ im Exponent des ersten X auf der rechten Seite zu finden ist. Schließlich wird

$$\underbrace{(8X^2 + 2X + 1)}_{f^{(3)}} \;=\; \underbrace{-8}_{a_3} X^0 \cdot (-X^2 + 2) + \underbrace{(2X + 17)}_{f^{(4)}},$$

wobei $d_3 = 0$ im Exponent des ersten X auf der rechten Seite zu finden ist. Das gibt nun $d_4 = -1$, so daß wir fertig sind und zu

$$2X^6 + X^3 + 1 \;=\; (-2X^4 - 4X^2 - X - 8)(-X^2 + 2) + (2X + 17)$$

zusammenfassen können.

> Ich hoffe, es ist nun deutlich geworden, daß es sich beim obigen Beweis des Lemmas um eine allgemeine Beschreibung des gewöhnlichen Polynomdivisionsalgorithmus handelt. Die übliche, aus der Schule bekannte Kurzschreibweise für dessen Durchführung sollte man beibehalten.

Beispiel. Sei $f(X) \in R[X]$, sei $x \in R$ derart, daß $f(x) = \sum_{i \geqslant 0} f_i x^i = 0$. Schreibe $f(X) = q(X)(X - x) + r(X)$ mit $\deg r < 1$. Somit ist $r(X) = r_0$. Nun aber ist $f(x) = q(x)(x-x)+r(x) = 0$, und somit auch $r_0 = 0$. Es folgt $f(X) = q(X)(X-x)$. Ist nun R ein Integritätsbereich, und ist $y \in R$, $y \neq x$, $f(y) = 0$, so kann man darüberhinaus folgern, daß auch $q(y) = 0$ ist; auf diese Weise kann man verschiedene Nullstellen sukzessive abdividieren.

1.6.5 Polynomiale Abbildungen

> Wir skizzieren kurz den Unterschied zwischen Polynomen und polynomialen Abbildungen.

Sei R ein kommutativer Ring. Sei $f(X) = \sum_{i \geqslant 0} f_i X^i \in R[X]$ ein Polynom. Sei

$$\begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & f(x) = \sum_{i \geqslant 0} f_i x^i \end{array}$$

die zu $f(X)$ gehörige *polynomiale Abbildung.* Beachte, daß nun $\sum_{i\geqslant 0} f_i x^i$ ein im Ring R zu bildender Term ist.

Nun kann es passieren, daß $f \neq 0$ (d.h. f_i nicht alle gleich null), aber $(x \longmapsto f(x)) = 0$ (d.h. $f(x) = 0$ für alle $x \in R$).

Beispiel. Sei $R = \mathbf{F}_5$. Sei $f(X) := X^5 - X$. Dann ist $f(x) = 0$ für $x \in \{-2, -1, 0, 1, 2\}$, da $f(0) = 0^5 - 0 = 0$, $f(1) = 1^5 - 1$ und $f(2) = 2^5 - 2 = 0$ (in $\mathbf{F}_5$); für die negativen Werte dann entsprechend. Also ist $f \neq 0$, aber $(x \longmapsto f(x)) = 0$. Vgl. Aufgabe 12.

Nichtsdestoweniger schreibt man oft ebenfalls f für die zu f gehörige polynomiale Abbildung. Das ist ein gefährlicher, aber doch üblicher Mißbrauch von Bezeichnungen.

Bemerkung. *Ist K ein unendlicher Körper, so ist für $f, g \in K[X]$ genau dann $f = g$, wenn $f(x) = g(x)$ für alle $x \in K$.*

Für einen unendlichen zugrundeliegenden Körper ist der angesprochene Mißbrauch von Bezeichnungen also ungefährlich. Hierzu gehören $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$.

Beweis. Mittels Differenzbildung können wir $g = 0$ annehmen. Sei $f(x) = 0$ für alle $x \in K$. Sei $n := \deg f$. *Angenommen*, es ist $f \neq 0$, i.e. $n \geqslant 0$. Seien $x_1, \ldots, x_{n+1} \in K$ paarweise verschiedene Elemente. Dann ist f, wie man durch sukzessives Abdividieren der zu den Nullstellen x_i gehörigen Faktoren $X - x_i$ erkennt, ein Vielfaches von $(X - x_1) \cdots (X - x_{n+1})$, und also von Grad $\geqslant n + 1$. Wir haben einen *Widerspruch* zu $\deg f = n$. ▫

1.7 Hauptidealbereiche

1.7.1 Definition

Definition. Ein Integritätsbereich heißt *Hauptidealbereich,* wenn alle seine Ideale Hauptideale sind.

Beispiel. Ein Körper ist ein Hauptidealbereich.

Weitere Beispiele sind $\mathbf{Z}$ und $K[X]$ für K ein Körper, wie wir sogleich verifizieren wollen.

Gegenbeispiel. Der Integritätsbereich $\mathbf{Z}[X]$ ist kein Hauptidealbereich. Denn es ist

$$I \;:=\; p\mathbf{Z}[X] + X\mathbf{Z}[X] \;=\; \{\textstyle\sum_{i\geqslant 0} a_i X^i \;:\; a_i \in \mathbf{Z},\; a_0 \in p\mathbf{Z}\}$$

kein Hauptideal, wobei p eine Primzahl sei. Denn *gäbe* es ein $f(X) \in \mathbf{Z}[X]$ mit $I = f(X)\mathbf{Z}[X]$, so gäbe es auch $u(X), v(X) \in \mathbf{Z}[X]$ mit $p = u(X)f(X)$ und $X = v(X)f(X)$. Aus der ersten Gleichung folgt aus Gradgründen, daß $f(X) = f_0$. Beachte, daß $f_0 \in p\mathbf{Z}$, da $f(X) \in I$. Aus der zweiten Gleichung folgt also durch Koeffizientenvergleich bei X^1, daß $1 = v_1 \cdot f_0 \in p\mathbf{Z}$, *Widerspruch.*

1.7.2 Der Hauptidealbereich Z

Lemma. *Es ist* $\mathbf{Z}$ *ein Hauptidealbereich.*

Beweis. Sei $I \subseteq \mathbf{Z}$ ein Ideal. Ohne Einschränkung ist $I \neq \{0\}$. Beachte, daß mit $z \in I$ auch immer $-z \in I$. Sei $x := \min(I \cap \mathbf{Z}_{>0})$. Es ist $x \in I$, also auch $x\mathbf{Z} \subseteq I$. Wir wollen zeigen, daß $x\mathbf{Z} = I$. Sei $y \in I$ vorgegeben. Wir wollen zeigen, daß $y \in x\mathbf{Z}$. Schreibe $y = qx + r$ mit $q,\ r \in \mathbf{Z}$ und $r \in [0, x-1]$. *Angenommen,* es ist $r \neq 0$. Dann ist $r = y - qx \in I \cap \mathbf{Z}_{>0}$. Aber $r < x$, und wir haben einen *Widerspruch* zur Wahl von x. Also ist $r = 0$, und also $y = qx \in x\mathbf{Z}$. ▫

Bemerkung. *Es ist* $z \in \mathbf{Z}$ *invertierbar genau dann, wenn* $z \in \{-1, +1\}$.

Bemerkung. *Es ist jedes Ideal in* $\mathbf{Z}$ *von der Form* $x\mathbf{Z}$ *für ein* $x \geqslant 0$*, und ein solches* x *liegt durch Vorgabe des Ideals auch eindeutig fest.*

Beweis. Der Beweis des vorigen Lemmas gab ein solches x. Nach der zweiten Bemerkung in §1.5 folgt aus $x\mathbf{Z} = x'\mathbf{Z}$ mit $x,\ x' \in \mathbf{Z}_{\geqslant 1}$, daß es ein invertierbares Element $u \in \mathbf{Z}$ mit $xu = x'$ gibt. Hier ist nun zwangsläufig $u = 1$. ▫

Beispiel. Seien $m,\ n \in \mathbf{Z}$. Dann ist $m\mathbf{Z} + n\mathbf{Z} = \mathrm{ggT}(m,n)\mathbf{Z}$. Denn mit vorstehender Bemerkung gibt es ein $g \in \mathbf{Z}_{\geqslant 0}$ mit $m\mathbf{Z} + n\mathbf{Z} = g\mathbf{Z}$. Schreibe demgemäß $g = ms + nt$ für gewisse $s,\ t \in \mathbf{Z}$. Nun sind m und n Vielfache von g. Ist umgekehrt $g' \in \mathbf{Z}_{\geqslant 0}$ so gegeben, daß m und n Vielfache von g' sind, so ist auch $g = ms + nt$ ein Vielfaches von g', und insbesondere ist $g \geqslant g'$. Folglich ist $g = \mathrm{ggT}(m,n)$. Vgl. auch Aufgabe 2.

1.7.3 Die Charakteristik eines kommutativen Rings

Bemerkung. *Sei* R *ein kommutativer Ring. Es gibt genau einen Ringmorphismus* $\mathbf{Z} \xrightarrow{\varepsilon_R} R$.

Ein vollständiger Beweis müßte auf die rekursiven Definitionen von Multiplikation und Addition in $\mathbf{Z}_{\geqslant 1}$ zurückgreifen. Wir skizzieren die wesentlichen Schritte.

Man schreibt auch oft $z := \varepsilon_R(z)$ und redet von "z, gesehen in R" etc., wobei $z \in \mathbf{Z}$.

"Beweis". Existenz. Um ε_R zu konstruieren, bilden wir zunächst 0 auf 0_R ab. Sei $z \in \mathbf{Z}_{\geqslant 1}$ gegeben. Wir bilden $z \in \mathbf{Z}_{\geqslant 1}$ ab auf die Summe $1_R + \cdots + 1_R$ aus z Summanden, und entsprechend $-z$ auf $-(1_R + \cdots + 1_R)$.

Dann ist $\varepsilon_R(1) = 1_R$. Für $z,\ w \in \mathbf{Z}_{\geqslant 1}$ ist $\varepsilon_R(z + w) = \varepsilon_R(z) + \varepsilon_R(w)$, $\varepsilon_R(z - w) = \varepsilon_R(z) - \varepsilon_R(w)$, sowie $\varepsilon_R(z \cdot w) = \varepsilon_R(z) \cdot \varepsilon_R(w)$, da das Distributivgesetz in R auf der rechten Seite eine Summe aus $z \cdot w$ Produkten $1_R \cdot 1_R$ liefert.

Daraus folgt wegen $\varepsilon_R(-z) = -\varepsilon_R(z)$ bereits, daß ε_R ein Morphismus von Ringen ist.

Eindeutigkeit. Da ein Ringmorphismus $\mathbf{Z} \longrightarrow R$ die 1 auf die 1_R schickt, und jedes Element von $\mathbf{Z}$ eine iterierte Summe von Einsen oder das Negative einer solchen ist, ist jeder Ringmorphismus von $\mathbf{Z}$ nach R bereits gleich ε_R. ▫

Definition. Sei R ein kommutativer Ring. Sei $\operatorname{Kern} f = c\mathbf{Z}$ mit $c \geqslant 0$. Dieses c ist eindeutig bestimmt und heißt die *Charakteristik* von R, geschrieben $\operatorname{char} R$.

Bemerkung. *Es ist* $\operatorname{char} R = 0$ *genau dann, wenn* $1_R + \cdots + 1_R$ *für* $\geqslant 1$ *Summanden nie null wird. Es ist* $\operatorname{char} R = n \in \mathbf{Z}_{\geqslant 1}$ *genau dann, wenn* $1_R + \cdots + 1_R$ *für minimal* n *Summanden gleich null wird.*

Beweis. Zunächst ist $\operatorname{char} R = 0$ genau dann, wenn $\operatorname{Kern} \varepsilon_R = \{0\}$, i.e. wenn $\operatorname{Kern} \varepsilon_R$ kein positives Element enthält. Ferner ist $\operatorname{char} R = n \geqslant 1$ genau dann, wenn $\operatorname{Kern} \varepsilon_R = n\mathbf{Z}$. Den positiven Erzeuger des Ideals $\operatorname{Kern} \varepsilon_R$ erhält man wie im Beweis des Lemmas in §1.7.2 als minimales positives Element darin. ▫

Beispiel. Es ist $\operatorname{char} \mathbf{Z} = \operatorname{char} \mathbf{Q} = \operatorname{char} \mathbf{R} = \operatorname{char} \mathbf{C} = 0$. Ist $n \in \mathbf{Z}$ gegeben, so ist $\operatorname{char}(\mathbf{Z}/n\mathbf{Z}) = |n|$. Insbesondere ist für p prim $\operatorname{char} \mathbf{F}_p = p$.

Bemerkung. *Ein kommutativer Ring* R *enthält einen Teilring isomorph zu* $\mathbf{Z}/(\operatorname{char} R)\mathbf{Z}$*, nämlich das Bild von* ε_R*. Insbesondere ist die Charakteristik eines Körpers gleich* 0 *oder prim.*

Beweis. Die Existenz des Teilrings ist eine Anwendung von Punkt (4) des Lemmas in §1.4.3 auf ε_R – es ist das Bild von ε_R isomorph zu $\mathbf{Z}/\operatorname{Kern} \varepsilon_R = \mathbf{Z}/(\operatorname{char} R)\mathbf{Z}$.

Da ein Teilring eines Körpers ein Integritätsbereich ist, kann die Charakteristik eines Körpers keine Nichtprimzahl $\geqslant 1$ sein; vgl. Aufgabe 16.(1). ▫

1.7.4 Der Hauptidealbereich $K[X]$

Sei K ein Körper.

Lemma. *Es ist* $K[X]$ *ein Hauptidealbereich.*

Beweis. Sei $I \subseteq K[X]$ ein Ideal. Ohne Einschränkung ist $I \neq \{0\}$. Sei $f(X)$ ein Polynom minimalen Grades in $I \smallsetminus \{0\}$. Es ist $f(X) \in I$, also auch $f(X)K[X] \subseteq I$. Wir wollen zeigen, daß $f(X)K[X] = I$. Sei $g(X) \in I$ vorgegeben. Wir wollen zeigen, daß $g(X) \in f(X)K[X]$. Schreibe $g(X) = q(X)f(X) + r(X)$ mit $q(X), r(X) \in K[X]$ und $\deg r < \deg f$. *Angenommen,* es ist $r(X) \neq 0$. Dann ist $r(X) = g(X) - q(X)f(X) \in I$. Aber $\deg r < \deg f$, und wir haben einen *Widerspruch* zur Wahl von $f(X)$. Also ist $r(X) = 0$, und also $g(X) = q(X)f(X) \in f(X)K[X]$. ▫

Bemerkung. *Es ist* $f(X) \in K[X]$ *invertierbar genau dann, wenn* $\deg f = 0$*, i.e. wenn* $f(X)$ *konstant und ungleich* 0 *ist.*

Bemerkung. *Es ist jedes Ideal in* $K[X]$ *ungleich* $\{0\}$ *von der Form* $f(X)K[X]$ *für ein normiertes Polynom* $f(X) \in K[X]$*, und ein solches* $f(X)$ *liegt durch Vorgabe des Ideals auch eindeutig fest.*

Beweis. Division des im vorstehenden Lemma gefundenen Erzeugers durch seinen Leitkoeffizienten gibt die Existenz eines normierten Erzeugers. Nach der zweiten Bemerkung in §1.5 folgt aus $f(X)K[X] = \tilde{f}(X)K[X]$ mit $f(X), \tilde{f}(X) \in K[X]$ normiert, daß es ein invertierbares Element $u(X) \in K[X]$ mit $f(X)u(X) = \tilde{f}(X)$ gibt. Da $u(X)$ nach vor-

angehender Bemerkung konstant ist, erzwingt die Normiertheit von $f(X)$ und von $\tilde{f}(X)$ vollends $u(X) = 1$. ▫

Beispiel. Seien $f(X)$, $h(X) \in K[X]$. Sei $g(X) \in K[X]$ das normierte Polynom, das das Ideal $f(X)K[X] + h(X)K[X]$ erzeugt, i.e.

$$g(X)K[X] := f(X)K[X] + h(X)K[X] \; .$$

Dann ist $g(X)$ der gemeinsame normierte Teiler größten Grades von $f(X)$ und $h(X)$, kurz,

$$\mathrm{ggT}(f(X), h(X)) \;:=\; g(X) \; .$$

Denn es sind zum einen sowohl $f(X)$ als auch $h(X)$ Vielfache von $g(X)$. Zum anderen, falls $\tilde{g}(X) \in K[X]$ ein normierter Teiler von $f(X)$ und von $h(X)$ ist, dann ist, da wir $g(X) = f(X)s(X) + h(X)t(X)$ mit $s(X)$, $t(X) \in K[X]$ schreiben können, auch $\tilde{g}(X)$ ein Teiler von $g(X)$, insbesondere ist $\deg \tilde{g} \leqslant \deg g$. Gilt hier Gleichheit, dann ist $\tilde{g}(X) = g(X)$ – dies zeigt, daß die Eigenschaft, gemeinsamer normierter Teiler maximalen Grades zu sein, das Polynom $g(X)$ auch eindeutig festlegt.

1.7.5 Der Faktorring $K[X]/f(X)K[X]$ als K-Vektorraum

Sei K ein Körper. Sei $f(X) \in K[X] \smallsetminus \{0\}$ normiert. Sei $n := \deg f$.

Bemerkung. *Sei R ein kommutativer Ring und $K \xrightarrow{a} R$ ein Ringmorphismus. Dann ist die abelsche Gruppe $(R, +)$ zusammen mit der skalaren Multiplikation $\lambda \cdot r := a(\lambda) \cdot r$ ein Vektorraum, wobei $\lambda \in K$ und $r \in R$.*

Beweis. Für λ, $\lambda' \in K$ und r, $r' \in R$ erhalten wir

$$\begin{array}{lllllllll}
1_K \cdot r & = & a(1_K) \cdot r & = & 1_R \cdot r & = & r & & \\
\lambda \cdot (\lambda' \cdot r) & = & a(\lambda) \cdot (a(\lambda') \cdot r) & = & (a(\lambda) \cdot a(\lambda')) \cdot r) & = & a(\lambda \cdot \lambda') \cdot r & = & (\lambda \cdot \lambda') \cdot r \\
\lambda \cdot (r + r') & = & a(\lambda) \cdot (r + r') & = & a(\lambda) \cdot r + a(\lambda) \cdot r' & = & \lambda \cdot r + \lambda \cdot r' & = & \\
(\lambda + \lambda') \cdot r & = & a(\lambda + \lambda') \cdot r & = & (a(\lambda) + a(\lambda')) \cdot r & = & a(\lambda) \cdot r + a(\lambda') \cdot r & = & \lambda \cdot r + \lambda' \cdot r \; .
\end{array}$$

▫

Beachte, daß diese Bemerkung via $K \longrightarrow K[X]$, $\lambda \longmapsto \lambda$ auf $K[X]$ anwendbar ist. Entsprechendes gilt für die Faktorringe von $K[X]$.

Lemma. *Sei $f(X) \in K[X] \smallsetminus \{0\}$. Sei $n := \deg f$. Schreibe*

$$\bar{X} \;:=\; X + f(X)K[X] \;\in\; K[X]/f(X)K[X] \; .$$

Eine K-lineare Basis von $K[X]/f(X)K[X]$ ist gegeben durch $(\bar{X}^0, \ldots, \bar{X}^{n-1})$. Insbesondere ist $\dim_K K[X]/f(X)K[X] = n = \deg f$.

Beweis. Die Aussage lautet, jedes Element von $K[X]/f(X)K[X]$ sei eindeutig als K-Linearkombination in dem angegebenen Tupel darstellbar, wobei Elemente aus K als konstante Polynome aufzufassen sind. In anderen Worten, wir müssen zeigen, daß jedes

Element von $K[X]/f(X)K[X]$ von genau einem Polynom von Grad $\leqslant n-1$ repräsentiert wird. Sei $g(X)+f(X)K[X]$ ein solches Element. Schreiben wir mittels Polynomdivision $g(X)=f(X)q(X)+r(X)$ mit $q(X)$, $r(X)\in K[X]$ und $\deg r(X)<\deg f$, i.e. $\deg r(X)\leqslant n-1$, so sehen wir, daß $g(X)+f(X)K[X]$ wegen $g(X)\equiv_f r(X)$ in der Tat von $r(X)$ repräsentiert wird. Es bleibt die Eindeutigkeit dieses repräsentierenden Elements zu zeigen. Sei $\tilde{r}(X)\in K[X]$ gegeben mit $\deg\tilde{r}(X)\leqslant n-1$ und $\tilde{r}(X)\equiv_f r(X)$. Dann ist $\tilde{r}(X)-r(X)=u(X)f(X)$ für ein $u(X)\in K[X]$. Es folgt

$$n-1\ \geqslant\ \deg(\tilde{r}-r)\ =\ \deg u+\deg f\ =\ \deg u+n\ ,$$

und also $\deg u<0$, i.e. $u(X)=0$, i.e. $\tilde{r}(X)=r(X)$. ▫

Beispiel. Im letzten Beispiel von §1.6.2 haben wir den Morphismus

$$\begin{array}{rcl}\mathbf{R}[X]/(X^2+1)\mathbf{R}[X] & \xrightarrow{\ b'\ } & \mathbf{C}\\ X+(X^2+1)\mathbf{R}[X] & \longmapsto & \mathrm{i}\ ,\end{array}$$

konstruiert und festgestellt, daß dieser surjektiv ist. Es ist b' auch $\mathbf{R}$-linear, da für $f(X)$, $g(X)\in\mathbf{R}[X]$ und λ, $\mu\in\mathbf{R}$ gilt, daß

$$\begin{array}{rl} & b'\big(\lambda(f(X)+(X^2+1)\mathbf{R}[X])+\mu(g(X)+(X^2+1)\mathbf{R}[X])\big)\\ & b'\big(\lambda f(X)+\mu g(X)+(X^2+1)\mathbf{R}[X])\big)\\ = & \lambda f(\mathrm{i})+\mu g(\mathrm{i})\\ = & \lambda b'\big(f(X)+(X^2+1)\mathbf{R}[X]\big)+\mu b'\big(g(X)+(X^2+1)\mathbf{R}[X]\big)\ .\end{array}$$

Da nun beide Seiten Dimension 2 über $\mathbf{R}$ haben und da eine surjektive lineare Abbildung zwischen zwei endlichdimensionalen Vektorräumen gleicher Dimension auch bijektiv ist, folgt, daß b' bijektiv ist, und somit ein Isomorphismus von Ringen – wie wir auf andere Weise auch schon in loc. cit. festgestellt hatten.

1.8 Maximale Ideale

1.8.1 Begriff

Definition. Sei R ein kommutativer Ring. Ein Ideal $I\subseteq R$ heiße *maximal*, falls I echt enthalten ist in R, und falls kein weiteres Ideal echt zwischen I und R liegt. Kurz, I ist maximal bezüglich Inklusion in der Menge der echt in R enthaltenen Ideale.

1.8.2 Maximale Ideale geben Körper

Lemma. *Sei I ein maximales Ideal in R. Dann ist R/I ein Körper.*

Beweis. Zunächst ist $0+I\neq 1+I$, da $I\subsetneq R$.

Sei $r\in R\smallsetminus I$. Wir müssen zeigen, daß es ein $r'\in R$ so gibt, daß $(r+I)(r'+I)=1+I$, i.e. daß $rr'\equiv_I 1$. Sei $J:=I+rR$. Da J ein Ideal ist, das das maximale Ideal I echt

enthält, ist $J = R$. Insbesondere ist $1 = x + rr'$ für gewisse $x \in I$ und $r' \in R$. Es folgt $rr' \equiv_I rr' + x = 1$. ▫

1.8.3 Maximalität in einem Hauptidealbereich

Sei R ein Hauptidealbereich. Ein Element $r \in R \smallsetminus \{0\}$ heiße *irreduzibel,* wenn r nicht invertierbar ist, aber aus $r = r'r''$ mit $r', r'' \in R$ folgt, daß r' invertierbar oder r'' invertierbar ist. Gibt es hingegen eine Produktdarstellung $r = r'r''$ mit $r', r'' \in R$ und weder r' noch r'' invertierbar, so heiße r *reduzibel.* Das Produkt eines irreduziblen mit einem invertierbaren Element ist irreduzibel.

Bemerkung. Sei $r \in R \smallsetminus \{0\}$. Es ist rR maximal genau dann, wenn r irreduzibel ist.

Beweis. ($\Longrightarrow$). Sei rR maximal. Sei $r = r'r''$ mit $r', r'' \in R$. Sei *angenommen,* daß weder r' noch r'' invertierbar sind, i.e. daß $r'R$ und $r''R$ echt in R enthalten sind. Da rR maximal ist, und da $rR \subseteq r'R$, folgt $rR = r'R$. Somit gibt es ein $s \in R$ mit $r' = rs$. Insgesamt ist $r = r'r'' = rsr''$, also $r(1 - sr'') = 0$, also $sr'' = 1$, also r'' invertierbar, *Widerspruch.*

($\Longleftarrow$). Sei $r \in R$ irreduzibel gegeben. Zunächst ist $rR \subsetneq R$, da r nicht invertierbar ist. Sei ferner $s \in R$ mit $rR \subseteq sR \subsetneq R$ gegeben. Wir haben $rR = sR$ zu zeigen. Es ist $r \in sR$, und also $r = st$ für ein $t \in R$. Da s nicht invertierbar ist, ist nach Voraussetzung t invertierbar. Also ist $rR = stR = sR$. ▫

1.8.4 Maximale Ideale in Z

Ist $m \in \mathbf{Z}_{\geqslant 1}$, so ist m genau dann irreduzibel wenn es eine Primzahl ist.

Lemma. *Ein Ideal in* $\mathbf{Z}$ *ist genau dann maximal, wenn es von der Form* $p\mathbf{Z}$ *ist für eine Primzahl* p*. Insbesondere ist für* p *prim*

$$\mathbf{F}_p \;=\; \mathbf{Z}/p\mathbf{Z}$$

ein Körper.

Vgl. das vorletzte Beispiel in §1.5.

Beweis. Das Nullideal in $\mathbf{Z}$ ist nicht maximal. Mit der Bemerkung aus §1.8.3 ist ferner ein Ideal in $\mathbf{Z}$ der Form $m\mathbf{Z}$ mit $m \in \mathbf{Z}_{\geqslant 1}$ genau dann maximal, wenn wenn m prim ist. ▫

Sei p prim. Wie kann man in $\mathbf{F}_p$ nun konkret ein nichtverschwindendes Element invertieren? Sei $x \in \mathbf{Z}$ mit $x + p\mathbf{Z} \neq 0 + p\mathbf{Z}$, i.e. $x \not\equiv_p 0$. Dann ist $\mathrm{ggT}(x, p) = 1$. Mithin gibt es $s, t \in \mathbf{Z}$ mit $xs + pt = 1$. Somit ist auch $xs \equiv_p xs + pt = 1$, also $s + p\mathbf{Z} = (x + p\mathbf{Z})^{-1}$. An diese Zahlen s und t kommt man rechnerisch mit dem Euklidschen Algorithmus, den wir in den Übungen betrachten; vgl. Aufgabe 2.

1.8.5 Maximale Ideale in $K[X]$

Sei K ein Körper. Ein Polynom $f(X) \in K[X]$ ist irreduzibel, wenn $\deg f \geqslant 1$ und wenn aus einer Produktzerlegung $f(X) = g(X)h(X)$ mit $g(X)$, $h(X) \in K[X]$ folgt, daß $\deg g = 0$ oder $\deg h = 0$.

Lemma. *Ein Ideal in $K[X]$ ist genau dann maximal, wenn es von der Form $p(X)K[X]$ ist für ein irreduzibles Polynom $p(X)$. Insbesondere ist für $p(X)$ irreduzibel der kommutative Ring $K[X]/p(X)K[X]$ ein Körper.*

Beweis. Das Nullideal in $K[X]$ ist nicht maximal. Mit der Bemerkung aus §1.8.3 ist ferner ein Ideal in $K[X]$ der Form $f(X)K[X]$ mit $f(X) \in K[X] \smallsetminus \{0\}$ genau dann maximal, wenn $f(X)$ irreduzibel ist. ▫

Sei $p(X) \in K[X]$ irreduzibel. Wie kann man in $K[X]/p(X)K[X]$ ein nichtverschwindendes Element invertieren? Sei $f(X) \in K[X]$ mit $f(X) \not\equiv_p 0$. Dann ist $f(X)K[X]+p(X)K[X] = K[X]$, da dieses Ideal echt über dem maximalen Ideal $p(X)K[X]$ liegt. Also gibt es $s(X)$, $t(X) \in K[X]$ mit $f(X)s(X) + p(X)t(X) = 1$. Folglich ist $f(X)s(X) \equiv_p 1$. An die Polynome $s(X)$ und $t(X)$ kommt man rechnerisch mit dem Euklidschen Algorithmus, den wir in den Übungen betrachten; vgl. Aufgabe 8.

Beispiel. Ein Polynom von Grad 2 oder 3 in $K[X]$ ist genau dann irreduzibel, wenn es in K keine Nullstelle besitzt. Denn Reduzibilität ist diesenfalls gleichbedeutend dazu, wenigstens einen Faktor von Grad 1 abzuspalten.

Vorsicht, ein Polynom in $K[X]$ kann durchaus reduzibel sein, ohne in K Nullstellen zu besitzen. Ist etwa $K = \mathbf{R}$, so ist $(X^2+1)^2$ reduzibel, hat aber in $\mathbf{R}$ keine Nullstellen.

Beispiel. Die Notation in den folgenden Beispielen $(2, 3, 4)$ sei unsere Standardnotation.

(1) Es ist $\mathbf{R}[X]/(X^2+1)\mathbf{R}[X] \xrightarrow{\sim} \mathbf{C}$, $X + (X^2+1)\mathbf{R}[X] \longmapsto \mathrm{i}$; vgl. das zweite Beispiel in §1.6.2, oder auch das Beispiel in §1.7.5.

Schreiben wir

$$\bar{X} \;:=\; X + (X^2+1)\mathbf{R}[X]\;,$$

so ist eine $\mathbf{R}$-lineare Basis von $\mathbf{R}[X]/(X^2+1)\mathbf{R}[X]$ gegeben durch

$$(1,\, \bar{X})\;,$$

dies entspricht, via obigen Isomorphismus, der $\mathbf{R}$-linearen Basis $(1, \mathrm{i})$ von $\mathbf{C}$.

(2) Es ist $X^2 + X + 1 \in \mathbf{F}_2[X]$ mangels Nullstelle irreduzibel. Also ist

$$\mathbf{F}_4 \;:=\; \mathbf{F}_2[X]/(X^2+X+1)\mathbf{F}_2[X].$$

ein Körper, welcher $\mathbf{F}_2 \subseteq \mathbf{F}_4$ als Teilkörper hat. Schreiben wir

$$\alpha \;:=\; X + (X^2+X+1)\mathbf{F}_2[X]\;,$$

so hat $\mathbf{F}_4$ die $\mathbf{F}_2$-lineare Basis $(1, \alpha)$. Ganz ausführlich geschrieben wird also

$$\mathbf{F}_4 \;=\; \{0,\, 1,\, \alpha,\, 1+\alpha\}\;.$$

Darin gilt nun $\alpha^2+\alpha+1 = X^2+X+1+(X^2+X+1)\mathbf{F}_2[X] = 0$, also $\alpha^2 = \alpha+1$. Beachte, daß darin auch $2=0$ ist, i.e. $\operatorname{char}\mathbf{F}_4 = 2$; vgl. Aufgabe 15.(2).

Zum Beispiel ist darin $\alpha\cdot(\alpha+1) = \alpha^2+\alpha = \alpha+1+\alpha = 1$, und somit $(\alpha+1)^{-1} = \alpha$.

Vorsicht, es ist $\boxed{\mathbf{F}_4 \not\cong \mathbf{Z}/4\mathbf{Z}}$. Denn $\mathbf{F}_4$ ist ein Körper, $\mathbf{Z}/4\mathbf{Z}$ nicht.

(3) Es ist $X^3+X+1 \in \mathbf{F}_2[X]$ mangels Nullstelle irreduzibel. Also ist

$$\mathbf{F}_8 \;:=\; \mathbf{F}_2[X]/(X^3+X+1)\mathbf{F}_2[X]$$

ein Körper, welcher $\mathbf{F}_2 \subseteq \mathbf{F}_8$ als Teilkörper hat.. Schreiben wir

$$\beta \;:=\; X+(X^3+X+1)\mathbf{F}_2[X]\;,$$

so hat $\mathbf{F}_8$ die $\mathbf{F}_2$-lineare Basis $(1,\beta,\beta^2)$. Ganz ausführlich geschrieben wird also

$$\mathbf{F}_8 \;=\; \{0,\,1,\,\beta\,,\beta+1\,,\beta^2\,,\beta^2+1\,,\beta^2+\beta\,,\beta^2+\beta+1\}\;.$$

Darin gilt nun $\beta^3+\beta+1 = 0$, also $\beta^3 = \beta+1$. Beachte, daß darin auch $2=0$ ist, i.e. $\operatorname{char}\mathbf{F}_8 = 2$.

Zum Beispiel ist darin $(\beta^2+\beta)\cdot(\beta^2+1) = \beta^4+\beta^3+\beta^2+\beta = (\beta^2+\beta)+(\beta+1)+\beta^2+\beta = \beta+1$.

(4) Es ist $X^2+1 \in \mathbf{F}_3[X]$ mangels Nullstelle irreduzibel. Also ist

$$\mathbf{F}_9 \;:=\; \mathbf{F}_3[X]/(X^2+1)\mathbf{F}_3[X]$$

ein Körper, welcher $\mathbf{F}_3 \subseteq \mathbf{F}_9$ als Teilkörper hat. Schreiben wir

$$\iota \;:=\; X+(X^2+1)\mathbf{F}_3[X]\;,$$

so hat $\mathbf{F}_9$ die $\mathbf{F}_3$-lineare Basis $(1,\iota)$. Ganz ausführlich geschrieben wird also

$$\mathbf{F}_9 \;=\; \{0,\,1,\,-1,\,\iota,\,\iota+1,\,\iota-1,\,-\iota,\,-\iota+1,\,-\iota-1\}\;.$$

Darin gilt nun $\iota^2+1 = 0$, also $\iota^2 = -1$. Beachte, daß darin natürlich auch $3=0$ ist, i.e. $\operatorname{char}\mathbf{F}_9 = 3$.

Zum Beispiel ist darin $(\iota+1)^4 = ((\iota+1)^2)^2 = (\iota^2+2\iota+1)^2 = (-\iota)^2 = -1$.

1.9 Eindeutige Zerlegung in irreduzible Elemente in einem Hauptidealbereich

Sei R ein Hauptidealbereich.

Bemerkung. *Für jede nichtleere Teilmenge von Idealen M in R gibt es ein $I \in M$ so, daß es kein $J \in M$ mit $I \subsetneq J$ gibt.*

Beweis. Angenommen, dies sei nicht der Fall. Dann können wir eine echt aufsteigende Kette $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ in M finden, da ja für jedes vorliegende Kettenglied noch ein echt dieses enthaltendes Ideal in M existiert.

Sei $I := \bigcup_{i \geqslant 0} I_i$. Dann ist I ein Ideal. Denn $0 \in I_0 \subseteq I$. Sind $x, y \in I$, so gibt es $i, j \geqslant 0$ mit $x \in I_i$ und $y \in I_j$. Es folgt $x - y \in I_{\max\{i,j\}} \subseteq I$. Ist ferner $x \in I$ und $r \in R$, so gibt es ein $i \geqslant 0$ mit $x \in I_i$. Es folgt $rx \in I_i \subseteq I$.

Da R ein Hauptidealbereich ist, gibt es ein $r \in R$ mit $I = Rr$. Insbesondere ist $r \in I = \bigcup_{i \geqslant 0} I_i$, es gibt also ein $i \geqslant 0$ mit $r \in I_i$. Dann aber ist

$$I \;=\; rR \;\subseteq\; I_i \;\subsetneq\; I_{i+1} \;\subseteq\; I\,,$$

insbesondere also $I \neq I$, und wir haben einen *Widerspruch.* ▫

Lemma. *Sei $r \in R \setminus \{0\}$ nicht invertierbar.*

(1) *Es gibt eine Produktzerlegung $r = r_1 \cdots r_k$ in irreduzible Elemente r_i, wobei $k \geqslant 1$ und $i \in [1, k]$.*

(2) *Sind $r = r_1 \cdots r_k = r'_1 \cdots r'_{k'}$ zwei Zerlegungen in irreduzible Elemente, so ist $k = k'$, und es gibt eine Permutation $\sigma \in \mathcal{S}_k$ mit $r_i R = r'_{\sigma(i)} R$.*

Beachte, daß dies e.g. auf $R = \mathbf{Z}$ oder auch auf $R = K[X]$ für K einen Körper angewandt werden kann. In diesen beiden Spezialfällen ist die Aussage (1) auch einfacher einzusehen.

Was (2) angeht, können wir z.B. $30 = \underbrace{2}_{r_1} \cdot \underbrace{3}_{r_2} \cdot \underbrace{5}_{r_3} = \underbrace{(-5)}_{r'_1} \cdot \underbrace{(-3)}_{r'_2} \cdot \underbrace{2}_{r'_3}$ in $\mathbf{Z}$ zerlegen. Mit $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$ wird in der Tat $r'_{\sigma(1)}\mathbf{Z} = 2\mathbf{Z} = r_1\mathbf{Z}$, sowie $r'_{\sigma(2)}\mathbf{Z} = (-3)\mathbf{Z} = 3\mathbf{Z} = r_2\mathbf{Z}$ und $r'_{\sigma(3)}\mathbf{Z} = (-5)\mathbf{Z} = 5\mathbf{Z} = r_3\mathbf{Z}$.

Beweis. Zu (1). Beachte zunächt, daß für $r, s \in R \setminus \{0\}$ mit $Rr = Rs \neq R$ das Element r eine Produktzerlegung in irreduzible Elemente genau dann besitzt, wenn dies für s zutrifft, wie mit der ersten Bemerkung aus §1.5 folgt.

Sei M die Menge aller Hauptideale ungleich $\{0\}$ und ungleich R in R, für die kein Erzeuger eine Produktzerlegung in irreduzible Elemente wie angegeben besitzt. Sei *angenommen,* es ist M nicht leer. Mit voriger Bemerkung gibt es ein $I \in M$, für welches gilt, daß jedes I echt enthaltende Ideal in R nicht mehr zu M gehört. Schreibe $I = sR$ für ein nicht invertierbares $s \in R \setminus \{0\}$. Dann ist s nicht irreduzibel, da sonst s eine einfaktorige Produktzerlegung in irreduzible Elemente besäße, was $sR = I \notin M$ nach sich zöge. Daher muß es eine Produktzerlegung $s = s's''$ mit weder s' noch s'' invertierbar geben. Nun ist $sR = s's''R \subseteq s'R$, wobei $sR \neq s'R$, da es sonst ein invertierbares $x \in R$ mit $s = s'x$ gäbe, was $s'x = s's''$ und somit wegen $s' \neq 0$ auch $x = s''$ zur Folge hätte, was nicht geht, da s'' nicht invertierbar ist. Also ist $I = sR \subsetneq s'R$. Genauso folgt $I = sR \subsetneq s''R$. Insbesondere ist weder $s'R$ noch $s''R$ in M. Also haben s' und s'' Produktzerlegungen in irreduzible Elemente. Somit hat auch $s = s's''$ eine Produktzerlegung in irreduzible Elemente, im *Widerspruch* zu $sR = I \in M$.

Zu (2). Seien $r = \prod_{i\in[1,k]} r_i = \prod_{i\in[1,k']} r'_i$ zwei Produktzerlegungen in irreduzible Elemente. Sei ohne Einschränkung $k \leqslant k'$.

Dann ist $\prod_{i\in[1,k']} r'_i \equiv_{r_1} 0$. Da $r_1R \subseteq R$ maximal und mithin R/r_1R ein Körper ist, folgt, daß bereits einer der Faktoren modulo r_1 verschwindet, sagen wir $r'_{\sigma(1)} \equiv_{r_1} 0$ für ein $\sigma(1) \in [1,k']$. Also ist $r'_{\sigma(1)} = r_1 \cdot x_1$ für ein $x_1 \in R$. Da nun $r'_{\sigma(1)}$ irreduzibel, aber r_1 nicht invertierbar ist, ist x_1 invertierbar, i.e. $Rr'_{\sigma(1)} = Rr_1$. Kürzen von r_1 gibt

$$\prod_{i\in[2,k]} r_i \;=\; x_1 \cdot \prod_{i\in[1,k']\smallsetminus\{\sigma(1)\}} r'_i \,.$$

Dann ist $x_1 \cdot \prod_{i\in[1,k']\smallsetminus\{\sigma(1)\}} r'_i \equiv_{r_2} 0$. Da $r_2R \subseteq R$ maximal und mithin R/r_2R ein Körper ist, folgt, daß bereits einer der Faktoren modulo r_2 verschwindet. Da x_1 in R invertierbar ist, ist auch seine Bild in R/r_2R invertierbar, und insbesondere ungleich 0. Sagen wir also, $r'_{\sigma(2)} \equiv_{r_2} 0$ für ein $\sigma(2) \in [1,k'] \smallsetminus \{\sigma(1)\}$. Also ist $r'_{\sigma(2)} = r_2 \cdot x_2$ für ein $x_2 \in R$. Da nun $r'_{\sigma(2)}$ irreduzibel, aber r_2 nicht invertierbar ist, ist x_2 invertierbar, i.e. $Rr'_{\sigma(2)} = Rr_2$. Kürzen von r_2 gibt

$$\prod_{i\in[3,k]} r_i \;=\; x_1 \cdot x_2 \cdot \prod_{i\in[1,k']\smallsetminus\{\sigma(1),\sigma(2)\}} r'_i \,.$$

Eine insgesamt k-fache Wiederholung dieses Arguments liefert

$$1 \;=\; x_1 \cdots x_k \cdot \prod_{i\in[1,k']\smallsetminus\{\sigma([1,k])\}} r'_i$$

für eine injektive Abbildung $[1,k] \xrightarrow{\sigma} [1,k']$, wobei $Rr'_{\sigma(i)} = Rr_i$ für alle $i \in [1,k]$. Da kein r'_i invertierbar ist, muß $[1,k'] \smallsetminus \sigma([1,k]) = \emptyset$ sein, d.h. σ muß auch surjektiv sein. Insgesamt ist in der Tat $\sigma \in \mathcal{S}_k$. ▫

1.10 Quotientenkörper eines Integritätsbereichs

Wir verallgemeinern die Konstruktion, um aus dem Integritätsbereich **Z** den Körper **Q** zu machen, auf beliebige Integritätsbereiche.

Sei R ein Integritätsbereich.

1.10.1 Definition und Schreibweise

Sei $\tilde{R} := \{(r,s) \in R \times R \;:\; r \in R,\; s \in R \smallsetminus \{0\}\}$. Definiere eine Äquivalenzrelation $(\sim)$ auf $\tilde{R}$ durch

$$(r,s) \sim (r',s') \qquad :\Longleftrightarrow \qquad rs' = r's \,.$$

Dies ist ersichtlich reflexiv und symmetrisch. Zeigen wir die Transitivität. Seien $(r,s) \sim (r',s') \sim (r'',s'')$. Dann ist $rs' = r's$ und $r's'' = r''s'$. Also ist $rs's'' = r'ss'' = r''ss'$, und somit, da $s' \neq 0$, $rs'' = r''s$.

Sei $\operatorname{frac} R := \tilde{R}/(\sim)$ die Menge der Äquivalenzklassen (engl. fraction field oder field of fractions). Schreibe $\frac{r}{s}$ für die Äquivalenzklasse von $(r,s) \in \tilde{R}$.

Beachte allgemein, daß für $s,\, s' \in R \smallsetminus \{0\}$ auch $ss' \neq 0$ ist.

Wir definieren eine Addition auf $\operatorname{frac} R$. Sei

$$\frac{r}{s} + \frac{r'}{s'} \;:=\; \frac{rs' + r's}{ss'} \;.$$

Dies ist wohldefiniert, da aus $(r,s) \sim (\tilde{r},\tilde{s})$, i.e. aus $r\tilde{s} = \tilde{r}s$, und aus $(r',s') \sim (\tilde{r}',\tilde{s}')$, i.e. aus $r'\tilde{s}' = \tilde{r}'s'$, folgt, daß

$$(rs' + r's)\tilde{s}\tilde{s}' \;=\; (\tilde{r}\tilde{s}' + \tilde{r}'\tilde{s})ss' \;,$$

i.e. daß $\frac{rs'+r's}{ss'} = \frac{\tilde{r}\tilde{s}'+\tilde{r}'\tilde{s}}{\tilde{s}\tilde{s}'}$, wobei $(r,s),\, (\tilde{r},\tilde{s}),\, (r',s'),\, (\tilde{r}',\tilde{s}') \in \tilde{R}$.

Wir definieren eine Multiplikation auf $\operatorname{frac} R$. Sei

$$\frac{r}{s} \cdot \frac{r'}{s'} \;:=\; \frac{rr'}{ss'} \;.$$

Dies ist wohldefiniert, da aus $(r,s) \sim (\tilde{r},\tilde{s})$, i.e. aus $r\tilde{s} = \tilde{r}s$, und aus $(r',s') \sim (\tilde{r}',\tilde{s}')$, i.e. aus $r'\tilde{s}' = \tilde{r}'s'$, folgt, daß

$$rr'\tilde{s}\tilde{s}' \;=\; \tilde{r}\tilde{r}'ss' \;,$$

i.e. daß $\frac{rr'}{ss'} = \frac{\tilde{r}\tilde{r}'}{\tilde{s}\tilde{s}'}$, wobei $(r,s),\, (\tilde{r},\tilde{s}),\, (r',s'),\, (\tilde{r}',\tilde{s}') \in \tilde{R}$.

Nachzuweisen, daß $\operatorname{frac} R = (\operatorname{frac} R, +, \cdot)$ nun einen Körper bildet, mit $0_{\operatorname{frac} R} = \frac{0}{1}$ und $1_{\operatorname{frac} R} = \frac{1}{1}$, sei eine Übungsaufgabe; vgl. Aufgabe 23. Es heißt $\operatorname{frac} R$ der *Quotientenkörper* von R.

Wir haben einen Ringmorphismus $R \xrightarrow{\lambda} \operatorname{frac} R$, $r \longmapsto \frac{r}{1}$. Dieser ist injektiv. Denn ist $\frac{r}{1} = \frac{0}{1}$, so ist $r \cdot 1 = 1 \cdot 0$, und also $r = 0$. Man schreibt auch oft r anstelle von $\frac{r}{1}$.

Beispiel. Es ist $\operatorname{frac} \mathbf{Z} = \mathbf{Q}$.

Beispiel. Ist K ein Körper, so ist $K \xrightarrow{\lambda}_{\sim} \operatorname{frac} K$. In der Tat ist $\frac{r}{s} = \frac{rs^{-1}}{1}$, und also λ auch surjektiv, insgesamt also bijektiv.

Beispiel. Sei K ein Körper. Wir schreiben $K(X) := \operatorname{frac} K[X]$, und analog $K(X_1, \ldots, X_n) := \operatorname{frac} K[X_1, \ldots, X_n]$ für $n \geqslant 1$. Die Elemente von $K(X_1, \ldots, X_n)$ haben die Form

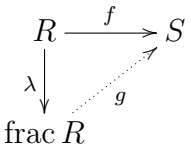
$$\frac{\sum_{i_k \geqslant 0,\, k \in [1,n]} r_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}}{\sum_{i_k \geqslant 0,\, k \in [1,n]} s_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}} \;,$$

wobei $r_{i_1,\ldots,i_n},\, s_{i_1,\ldots,i_n} \in K$, wobei diese Koeffizienten nur auf einer endlichen Teilmenge von $(\mathbf{Z}_{\geqslant 0})^n$ nicht verschwinden, und wobei das Polynom im Nenner nicht verschwinden darf.

1.10.2 Gebrauchsanweisung für Quotientenkörper

Bemerkung. *Sei $R \xrightarrow{f} T$ ein Ringmorphismus von unserem Integritätsbereich R in einen kommutativen Ring T so, daß $f(r)$ invertierbar ist für alle $r \in R \smallsetminus \{0\}$. Dann gibt es*

genau einen Ringmorphismus $\operatorname{frac} R \xrightarrow{g} S$ *so, daß* $f = g \circ \lambda$.



Beweis. Beachte allgemein, daß

$$f(ss')^{-1} \;=\; f(ss')^{-1}f(s)f(s')f(s)^{-1}f(s')^{-1} \;=\; f(ss')^{-1}f(ss')f(s)^{-1}f(s')^{-1} \;=\; f(s)^{-1}f(s')^{-1}\,.$$

Zeigen wir zunächst die *Existenz von g*. Setze $g(\frac{r}{s}) := f(r)f(s)^{-1}$, wobei $\frac{r}{s} \in \operatorname{frac} R$. Dies ist wohldefiniert, da für $r,\, r' \in R$ und $s,\, s' \in R \setminus \{0\}$ mit $rs' = r's$ gilt, daß

$$\begin{aligned} f(r)f(s)^{-1} &= f(r)f(s')f(s')^{-1}f(s)^{-1} \\ &= f(rs')f(s)^{-1}f(s')^{-1} \\ &= f(r's)f(s)^{-1}f(s')^{-1} \\ &= f(r')f(s)f(s)^{-1}f(s')^{-1} \\ &= f(r')f(s')^{-1}\,. \end{aligned}$$

Ersichtlich geht die Eins auf die Eins, und ebenso ersichtlich verträgt sich g mit der Multiplikation. Zeigen wir, daß sich g mit der Addition verträgt. Seien $\frac{r}{s},\, \frac{r'}{s'} \in \operatorname{frac} R$. Es wird

$$\begin{aligned} g(\tfrac{r}{s} + \tfrac{r'}{s'}) &= g(\tfrac{rs'+r's}{ss'}) \\ &= f(rs' + r's)f(ss')^{-1} \\ &= (f(r)f(s') + f(r')f(s))f(s)^{-1}f(s')^{-1} \\ &= f(r)f(s)^{-1} + f(r')f(s')^{-1} \\ &= g(\tfrac{r}{s}) + g(\tfrac{r'}{s'})\,. \end{aligned}$$

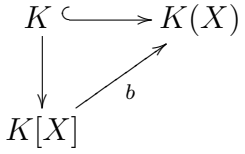
Schließlich ist $g \circ \lambda = f$, da $g(\lambda(r)) = g(\frac{r}{1}) = f(r)f(1)^{-1} = f(r)$ für $r \in R$.

Zeigen wir nun die *Eindeutigkeit von g*. Sei $\tilde{g} : \operatorname{frac} R \longrightarrow S$ ein zweiter Ringmorphismus mit derselben Eigenschaft, namentlich $\tilde{g} \circ \lambda = f$. Dann ist

$$\begin{aligned} \tilde{g}(\tfrac{r}{s}) &= \tilde{g}(\tfrac{r}{1} \cdot (\tfrac{s}{1})^{-1}) \\ &= \tilde{g}(\tfrac{r}{1}) \cdot \tilde{g}((\tfrac{s}{1})^{-1}) \\ &= \tilde{g}(\tfrac{r}{1}) \cdot \tilde{g}(\tfrac{s}{1})^{-1} \\ &= f(r) \cdot f(s)^{-1} \\ &= g(\tfrac{r}{s}) \end{aligned}$$

für $\frac{r}{s} \in \operatorname{frac} R$, und also $g = \tilde{g}$. ▫

Beispiel. Sei K ein Körper. Sei $f(X) \in K[X]$ mit $\deg f \geqslant 1$ gegeben. Wir erhalten zunächst unter Verwendung von §1.6.2



mit $b : g(X) \longmapsto g(f(X))$, also die Abbildung, die $f(X)$ für X substituiert. Es ist $\deg(g(f(X))) = (\deg g) \cdot (\deg f)$. Insbesondere bildet b jedes Polynom ungleich 0 auf ein invertierbares Element von $K(X)$ ab. Somit wird mit obiger Bemerkung

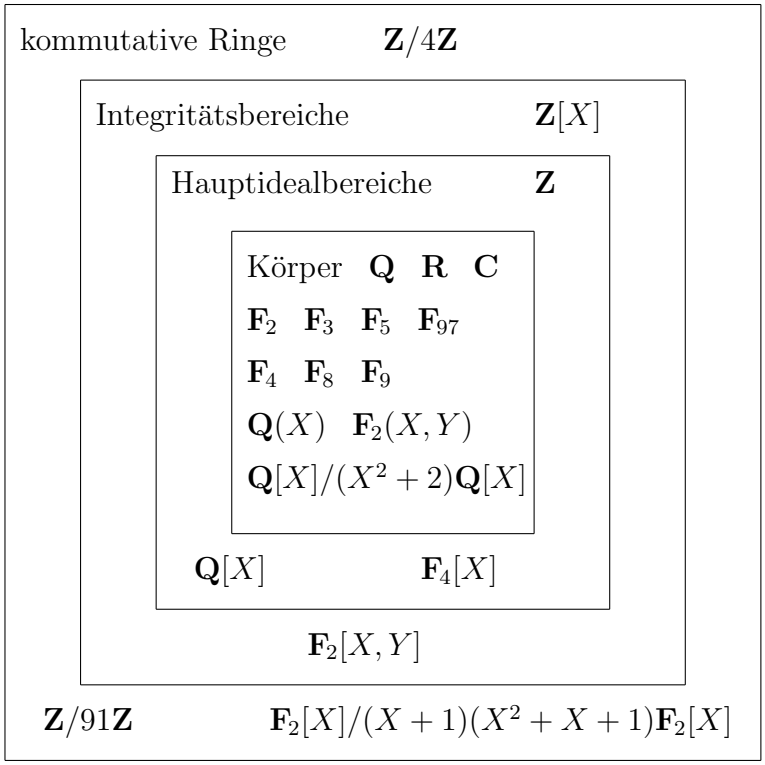
$$\begin{array}{ccc} K[X] & \xrightarrow{b} & K(X) \\ {\scriptstyle\lambda}\downarrow & \nearrow_{d} & \\ K(X) & & \end{array} ,$$

wobei d ein Element $\frac{g(X)}{h(X)}$ auf $\frac{g(f(X))}{h(f(X))}$ schickt.

Ist nun $\deg f = 1$, also $f(X) = uX+v$ mit $u,\ v \in K$ und $u \neq 0$, so zeigt die entsprechende Konstruktion ausgehend von $\tilde{f}(X) := u^{-1}X - u^{-1}v$, daß diesenfalls d ein Isomorphismus ist. In der Tat ist $f(\tilde{f}(X)) = u(u^{-1}X - u^{-1}v) + v = X$, und also $\frac{g(f(\tilde{f}(X)))}{h(f(\tilde{f}(X)))} = \frac{g(X)}{h(X)}$.

1.11 Ein paar kommutative Ringe

Stellen wir einmal ein paar typische Beispiele für kommutative Ringe in einem Bild zusammen. Ohne Anspruch auf Vollständigkeit!



(Die Information, daß $\mathbf{F}_2[X,Y]$ kein Hauptidealbereich ist, erfolgt ohne Beweis.)

Kapitel 2

Körpererweiterungen

Ein *Teilkörper* eines Körpers ist ein Teilring, der selbst wieder Körper ist.

Definition. Sei K ein Körper. Ein Körper L heißt *(Körper)erweiterung* von K, falls K ein Teilkörper von L ist. Geschrieben wird dies $L|K$, oder

$$\begin{array}{c} L \\ | \\ K \end{array},$$

oder auch, der Deutlichkeit halber,

$$\begin{array}{c} L \\ \uparrow \\ K \end{array}.$$

Beispiel.

(1) Es ist $\mathbf{C}$ eine Erweiterung von $\mathbf{R}$, also $\mathbf{C}|\mathbf{R}$.

(2) Es ist $\mathbf{F}_4|\mathbf{F}_2$.

(3) Es ist $\mathbf{F}_8|\mathbf{F}_2$.

(4) Es ist $\mathbf{F}_9|\mathbf{F}_3$.

(5) Es ist $\mathbf{R}|\mathbf{Q}$.

(6) Ist K ein Körper, so ist $K(X)|K$.

2.1 Primkörper

Wir zeigen, daß in jedem Körper ein minimaler Körper liegt, sein *Primkörper*. In anderen Worten, jeder Körper ist eine Erweiterung seines Primkörpers.

Bemerkung. *Sei K ein Körper von Charakteristik* $\operatorname{char} K = p > 0$.

(1) *Es enthält K genau einen Teilkörper isomorph zu $\mathbf{F}_p$, namentlich das Bild von ε_K.*

(2) *Ist σ ein Körpermorphismus von K nach K, und ist x im Bild von ε_K, so ist $\sigma(x) = x$.*

Der Teilkörper aus (1) heißt *Primkörper* von K. Man schreibt mißbräuchlich, aber unmißverständlich auch $\mathbf{F}_p = \operatorname{Im} \varepsilon_K \subseteq K$. Die Aussage (2) schreibt sich dann als $\sigma|^{\mathbf{F}_p}_{\mathbf{F}_p} = \mathrm{id}_{\mathbf{F}_p}$.

Beweis. Zu (1). Wir sahen schon in §1.7.3, daß K einen Teilkörper isomorph zu $\mathbf{F}_p$ enthält, namentlich $\operatorname{Im} \varepsilon_K$. Zeigen wir, daß dies der einzige solche ist. Sei $K_0 \subseteq K$ ein Teilkörper isomorph zu $\mathbf{F}_p$. Betrachte den zusammengesetzten Ringmorphismus

$$\mathbf{Z} \xrightarrow{\rho} \mathbf{F}_p \xrightarrow{\sim} K_0 \longrightarrow K \ .$$

Dieser ist nach der ersten Bemerkung in §1.7.3 gleich ε_K. Insbesondere ist sein Bild sowohl gleich $\operatorname{Im} \varepsilon_K$ als auch gleich K_0. ▫

Zu (2). Es ist ε_K der einzige Ringmorphismus von $\mathbf{Z}$ nach K. Insbesondere ist $\sigma \circ \varepsilon_K = \varepsilon_K$. Also ist $\sigma(\varepsilon_K(z)) = \varepsilon_K(z)$ für alle $z \in \mathbf{Z}$.

Bemerkung. *Sei K ein Körper von Charakteristik* $\operatorname{char} K = 0$.

(1) *Es enthält K genau einen Teilkörper isomorph zu $\mathbf{Q}$.*

(2) *Ist σ ein Körpermorphismus von K nach K, und ist x im in* (1) *beschriebenen Teilkörper, so ist $\sigma(x) = x$.*

Der Teilkörper aus (1) heißt *Primkörper* von K. Man schreibt mißbräuchlich, aber unmißverständlich auch $\mathbf{Q} \subseteq K$. Die Aussage (2) schreibt sich dann als $\sigma|^{\mathbf{Q}}_{\mathbf{Q}} = \mathrm{id}_{\mathbf{Q}}$.

Beweis. Zu (1). *Existenz.* Die Voraussetzung $\operatorname{char} K = 0$ bedeutet, daß der Kern von ε_K gleich $\{0\}$ ist, i.e. daß ε_K injektiv ist. Insbesondere werden alle Elemente von $\mathbf{Z} \smallsetminus \{0\}$ auf Elemente von $K \smallsetminus \{0\}$ abgebildet, d.h. auf invertierbare Elemente. Wenden wir die Bemerkung aus §1.10 auf $\varepsilon_K : \mathbf{Z} \longrightarrow K$ an, so erhalten wir genau einen Ringmorphismus $\mathbf{Q} \xrightarrow{\hat{\varepsilon}_K} K$ so, daß das Dreieck

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{\varepsilon_K} & K \\ {\scriptstyle\lambda}\downarrow & \nearrow_{\hat{\varepsilon}_K} & \\ \mathbf{Q} & & \end{array}$$

kommutiert, i.e. $\hat{\varepsilon}_K \circ \lambda = \varepsilon_K$. Da $\mathbf{Q}$ ein Körper ist, ist $\hat{\varepsilon}_K$ ist injektiv; vgl. Aufgabe 7. Also ist $\hat{\varepsilon}_K$ ein Isomorphismus von $\mathbf{Q}$ mit dem Teilkörper $\operatorname{Im} \hat{\varepsilon}_K$ von K.

Eindeutigkeit. Liege ein Teilkörper $Q \subseteq K$ und ein Isomorphismus $\mathbf{Q} \xrightarrow{\sim} Q$ vor. Nun ist der zusammengesetzte Ringmorphismus

$$\mathbf{Z} \xrightarrow{\lambda} \mathbf{Q} \xrightarrow{\sim} Q \longrightarrow K$$

nach der ersten Bemerkung in §1.7.3 gleich ε_K. Mit der Eindeutigkeitsaussage aus der Bemerkung aus §1.10 folgt nun, daß der zusammengesetzte Ringmorphismus

$$\mathbf{Q} \xrightarrow{\sim} Q \longrightarrow K$$

gleich $\hat{\varepsilon}_K$ ist. Insbesondere ist Q in der Tat das Bild von $\hat{\varepsilon}_K$.

Zu (2). Nach der ersten Bemerkung in §1.7.2 und mittels der Eindeutigkeit aus §1.10 gibt es genau einen Körpermorphismus von $\mathbf{Q}$ nach K, nämlich $\hat{\varepsilon}_K$. Insbesondere ist $\sigma \circ \hat{\varepsilon}_K = \hat{\varepsilon}_K$. Also ist $\sigma(\hat{\varepsilon}_K(x)) = \hat{\varepsilon}_K(x)$ für alle $x \in \mathbf{Q}$. ▫

Beispiel.

(1) Der Primkörper von $\mathbf{R}$ und von $\mathbf{C}$ ist $\mathbf{Q}$.

(2) Der Primkörper von $\mathbf{F}_4$ und von $\mathbf{F}_8$ ist $\mathbf{F}_2$.

(3) Der Primkörper von $\mathbf{F}_9$ ist $\mathbf{F}_3$.

(4) Der Primkörper von $\mathbf{F}_4(X)$ ist $\mathbf{F}_2$.

2.2 Der Gradsatz

Definition. Sei $L|K$ eine Körpererweiterung. Schreibe $[L : K] := \dim_K L$ für den *Grad* der Erweiterung $L|K$. Die Erweiterung $L|K$ heißt *endlich,* falls $[L : K]$ endlich ist, d.h., falls L ein endlichdimensionaler K-Vektorraum ist. Diesenfalls schreibt man auch

$$\begin{array}{c} L \\ {\scriptstyle [L:K]}\,\big| \\ K \end{array}$$

Beispiel.

(1) Es ist $[\mathbf{C} : \mathbf{R}] = 2$, also

$$\begin{array}{c} \mathbf{C} \\ {\scriptstyle 2}\,\big| \\ \mathbf{R}\,. \end{array}$$

(2) Es ist $[\mathbf{F}_4 : \mathbf{F}_2] = 2$.

(3) Es ist $[\mathbf{F}_8 : \mathbf{F}_2] = 3$.

(4) Es ist $[\mathbf{F}_9 : \mathbf{F}_3] = 2$.

(5) Es ist $[\mathbf{R} : \mathbf{Q}] = \infty$ (ohne Beweis).

(6) Ist K ein Körper, so ist $[K(X) : K] = \infty$. In der Tat ist e.g. $(X^0, X^1, \dots)$ ein unendliches linear unabhängiges Tupel.

Satz 1 (Gradsatz) *Seien $M|L$ und $L|K$ endliche Körpererweiterungen.*

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

Es ist

$$[M : K] \;=\; [M : L] \cdot [L : K] \; .$$

Beweis. Schreibe $\ell := [L : K]$ und $m := [M : L]$. Sei $(x_i)_{i\in[1,\ell]} = (x_1, \dots, x_\ell)$ eine Basis von L über K. Sei $(y_j)_{j\in[1,m]} = (y_1, \dots, y_m)$ eine Basis von M über L. Wir *behaupten,* daß

$$(x_i y_j)_{i\in[1,\ell],\, j\in[1,m]} \;=\; (x_1y_1, \dots, x_\ell y_1,\; x_1y_2, \dots, x_\ell y_2,\; \dots,\; x_1y_m, \dots, x_\ell y_m)$$

eine Basis von M über K ist.

Erzeugendensystem. Sei $z \in M$ gegeben. Schreibe

$$z \;=\; u_1y_1 + \cdots + u_my_m$$

mit $u_j \in L$ für $j \in [1, m]$. Schreibe

$$u_j \;=\; v_{j,1}x_1 + \cdots + v_{j,\ell}x_\ell$$

für $j \in [1, m]$, wobei $v_{j,i} \in K$ für $i \in [1, \ell]$. Insgesamt wird

$$\begin{array}{rcl} z & = & \sum_{j\in[1,m]} u_j y_j \\ & = & \sum_{j\in[1,m]} \sum_{i\in[1,\ell]} v_{j,i} x_i y_j \; . \end{array}$$

Also liegt z im K-linearen Erzeugnis der behaupteten Basis.

Lineare Unabhängigkeit. Seien $v_{j,i} \in K$ so gegeben, daß

$$\textstyle\sum_{j\in[1,m]} \sum_{i\in[1,\ell]} v_{j,i} x_i y_j \;=\; 0 \; .$$

Wir haben zu zeigen, daß $v_{j,i} = 0$ für $j \in [1, m]$ und $i \in [1, \ell]$. Da $(y_j)_{j\in[1,m]}$ linear unabhängig über L ist, und da

$$\textstyle\sum_{j\in[1,m]} \underbrace{\left(\sum_{i\in[1,\ell]} v_{j,i} x_i\right)}_{\in L} y_j \;=\; 0 \; ,$$

folgt $\sum_{i\in[1,\ell]} v_{j,i}x_i = 0$ für $j \in [1,m]$. Da $(x_i)_{i\in[1,\ell]}$ linear unabhängig über K ist, folgt $v_{j,i} = 0$ für $i \in [1,\ell]$ und $j \in [1,m]$.

Erzeugendensystem und lineare Unabhängigkeit gezeigt zu haben, zeigt insgesamt die *Behauptung,* es liege eine Basis vor.

Da die gefundene Basis von M über K nun $m \cdot \ell$ Elemente enthält, folgt

$$[M : K] \;=\; \dim_K M \;=\; m \cdot \ell \;=\; [M : L] \cdot [L : K] \,.$$

□

2.3 Algebraische Elemente

Sei $L|K$ eine Körpererweiterung.

2.3.1 Begriff

Definition. Ein Element $x \in L$ heißt *algebraisch* über K, falls es ein Polynom $f(X) \in K[X] \smallsetminus \{0\}$ gibt mit $f(x) = 0$.

Beispiel.

(1) Es ist $\mathrm{i} \in \mathbf{C}$ algebraisch über $\mathbf{R}$, da $\mathrm{i}^2 + 1 = 0$, da also mit $f(X) := X^2 + 1 \in \mathbf{R}[x] \smallsetminus \{0\}$ gilt, daß $f(\mathrm{i}) = 0$.

(2) Es ist $\alpha \in \mathbf{F}_4$ algebraisch über $\mathbf{F}_2$, da $\alpha^2 + \alpha + 1 = 0$.

(3) Jedes $x \in K \subseteq L$ ist algebraisch über K, da $f(x) = 0$ für $f(X) = X - x \in K[X] \smallsetminus \{0\}$.

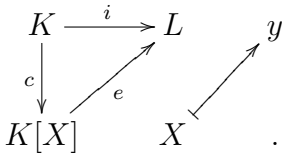
(4) Es ist $\mathrm{e} = \exp(1) \in \mathbf{R}$ nicht algebraisch über $\mathbf{Q}$ (ohne Beweis).

(5) Es ist $\sqrt{2} \in \mathbf{R}$ algebraisch über $\mathbf{Q}$, da $(\sqrt{2})^2 - 2 = 0$.

(6) Es ist $T^3+1 \in \mathbf{F}_2(T)$ nicht algebraisch über $\mathbf{F}_2$. In der Tat ist für $f(X) \in \mathbf{F}_2[X] \smallsetminus \{0\}$ der Grad von $f(T^3 + 1)$ gleich $3 \cdot \deg f$, und insbesondere ist $f(T^3 + 1) \neq 0$.

2.3.2 Endliche monogene Erweiterungen

Definition. Sei $y \in L$ algebraisch über K. Sei $K \xrightarrow{i} L$ die Einbettung. Mit der Bemerkung aus §1.6 haben wir ein kommutatives Dreieck von Ringmorphismen



.

Sei

$$K(y) \;:=\; \mathrm{Im}(K[X] \overset{e}{\longrightarrow} L) \;=\; \{f(y) \in L \;:\; f(X) \in K[X]\}$$

der von y *erzeugte* Teilring von L, gesprochen "K adjungiert y". Es heißt y ein Erzeuger von $K(y)$ über K.

Ein Teilring von L von der Form $K(z)$ für ein $z \in L$, das algebraisch über K ist, heißt auch *endliche monogene Erweiterung* von K ("monogen" = "von einem (Element) generiert").

Satz 2 (Minimalpolynom)

Wir betrachten die Körpererweiterung $L|K$. Sei $y \in L$ algebraisch über K.

(1) *Es ist $K(y)$ ein Teilkörper von L mit $n := [K(y) : K]$ endlich. Eine Basis von $K(y)$ über K ist gegeben durch $(y^0, y^1, \ldots, y^{n-1})$.*

(2) *Es gibt genau ein normiertes Polynom $\mu_{y,K}(X)$ von Grad $n = [K(y) : K]$ mit*

$$\mu_{y,K}(y) \;=\; 0\;.$$

Es teilt $\mu_{y,K}(X)$ ein Polynom in $K[X]$ genau dann, wenn dieses in L die Nullstelle y hat.

(3) *Es ist $\mu_{y,K}(X) \in K[X]$ irreduzibel.*

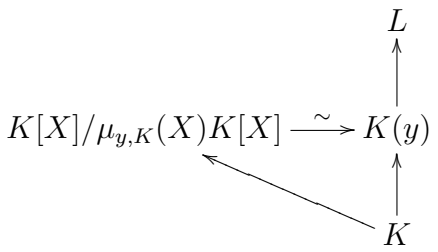
(4) *Es ist*

$$\begin{array}{rcl} K[X]/\mu_{y,K}(X)K[X] & \longrightarrow & K(y) \\ f(X) + \mu_{y,K}(X)K[X] & \longmapsto & f(y) \end{array}$$

ein Isomorphismus von Körpern, welcher den jeweiligen Teilkörper K identisch abbildet.

Das Polynom $\mu_{y,K}(X) \in K[X]$ aus (2) heißt auch das *Minimalpolynom* von y über K. Es ist wegen der Teilbarkeitseigenschaft aus (2) insbesondere das normierte Polynom kleinsten Grades in $K[X]$ mit Nullstelle y.

Mit Satz 2 stellt sich die Situation wie folgt dar.



Beweis. Es ist der Kern von $K[X] \overset{e}{\longrightarrow} L$ nach Voraussetzung an y, algebraisch über K zu sein, ungleich $\{0_{K[X]}\}$. Sei $\mu_{y,K}(X)$ der normierte Erzeuger des Kerns von $K[X] \overset{e}{\longrightarrow} L$; vgl. die erste Bemerkung in §1.7.4. Schreibe $\tilde{n} := \deg \mu_{y,K}$.

Zu (4). Dies folgt aus der Zerlegung eines Ringmorphismus wie am Ende von §1.4.3, angewandt auf $K[X] \xrightarrow{e} L$, namentlich

$$K[X] \xrightarrow{\rho} K[X]/\mu_{y,K}(X)K[X] \xrightarrow[\sim]{\tilde{e}} K(y) \longrightarrow L\ .$$

Für $\lambda \in K$ ist $\tilde{e}(\lambda) = \tilde{e}(\lambda X^0 + \mu_{y,K}(X)K[X]) = \lambda y^0 = \lambda$.

Zu (1). Mit dem Lemma aus §1.7.5 hat $K[X]/\mu_{y,K}(X)K[X]$ die Basis

$$(\bar{X}^0, \ldots, \bar{X}^{\tilde{n}-1})\ ,$$

wobei $\bar{X} := X + \mu_{y,K}(X)K[X]$. Der Isomorphismus $\tilde{e}$ aus (4) ist aber auch ein Isomorphismus von K-Vektorräumen, da

$$\tilde{e}(\lambda\xi + \nu\eta) \ = \ \tilde{e}(\lambda)\tilde{e}(\xi) + \tilde{e}(\nu)\tilde{e}(\eta) \ = \ \lambda\tilde{e}(\xi) + \nu\tilde{e}(\eta)$$

für $\lambda, \nu \in K$ und $\xi, \eta \in K[X]/\mu_{y,K}(X)K[X]$. Also ist das eintragsweise genommene Bild dieser Basis, nämlich

$$(y^0, \ldots, y^{\tilde{n}-1})\ ,$$

eine Basis von $K(y)$ über K. Insbesondere ist

$$\tilde{n} \ = \ [K(y) : K] \ = \ n\ .$$

Als endlichdimensionaler Integritätsbereich ist schließlich $K(y)$ in der Tat ein Teilkörper von L; vgl. Aufgabe 10.(1).

Zu (2). Nach Wahl von $\mu_{y,K}(X)$ als Erzeuger des Kerns von $e : K[X] \longrightarrow L$, $f(X) \longmapsto f(y)$ hat ein Polynom in $K[X]$ genau dann y als Nullstelle, wenn es von $\mu_{y,K}(X)$ geteilt wird.

Das einzige normierte Polynom von Grad $n = \deg \mu_{y,K} = [K(y) : K]$, welches y als Nullstelle hat, ist folglich $\mu_{y,K}(X)$ selbst.

Zu (3). *Nehmen* wir *an,* es sei $\mu_{y,K}(X) = f(X) \cdot g(X)$ mit $\deg f < n$ und $\deg g < n$. Dann aber ist $0 = \mu_{y,K}(y) = f(y) \cdot g(y)$, und folglich $f(y) = 0$ oder $g(y) = 0$, im *Widerspruch* zu (2), da $\mu_{y,K}(X)$ aus Gradgründen weder $f(X)$ noch $g(X)$ teilt. ▫

Beispiel. Sei $K = \mathbf{Q}$, sei $y = \sqrt{2} \in \mathbf{R}$. Es ist $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbf{Q}\}$. Eine Basis von $\mathbf{Q}(\sqrt{2})$ über $\mathbf{Q}$ ist gegeben durch $(1, \sqrt{2})$. Es ist $\mu_{\sqrt{2},\mathbf{Q}}(X) = X^2 - 2$. Es ist $\mathbf{Q}(\sqrt{2}) \simeq \mathbf{Q}[X]/(X^2 - 2)\mathbf{Q}[X]$.

Bemerkung. *Sei $f(X) \in K[X]$ irreduzibel und normiert. Sei $y \in L$ mit $f(y) = 0$ gegeben. Dann ist $f(X) = \mu_{y,K}(X)$.*

Beweis. Da $f(y) = 0$, ist $\mu_{y,K}(X)$ ein Teiler von $f(X)$. Da aber $f(X)$ irreduzibel und normiert ist, folgt $f(X) = \mu_{y,K}(X)$. ▫

Beispiel.

(1) Sei $K = \mathbf{R}$, $L = \mathbf{C}$ und $y = \mathrm{i}$. Es ist $\mu_{\mathrm{i},\mathbf{R}}(X) = X^2 + 1 \in \mathbf{R}[X]$. In der Tat ist dies ein irreduzibles normiertes Polynom in $\mathbf{R}[X]$ mit Nullstelle i. Siehe auch das zweite Beispiel in §1.6.2. Ferner ist $\mathbf{R}(\mathrm{i}) = \mathbf{C}$. Beachte noch, daß $\mu_{\mathrm{i},\mathbf{C}}(X) = X - \mathrm{i} \in \mathbf{C}[X]$.

(2) Sei $K = \mathbf{F}_2$, $L = \mathbf{F}_4$ und $y = \alpha$. Es ist $\mu_{\alpha,\mathbf{F}_2}(X) = X^2 + X + 1$. In der Tat ist dies ein irreduzibles normiertes Polynom in $\mathbf{F}_2[X]$ mit Nullstelle α. Ferner ist $\mathbf{F}_2(\alpha) = \mathbf{F}_4$.

(3) Sei $K = \mathbf{Q}$, $L = \mathbf{C}$ und $y = \sqrt[3]{2}$ – letzteres wollen wir als Abkürzung auch verwenden. Es ist $X^3 - 2$ mangels Nullstelle in $\mathbf{Q}$ ein irreduzibles Polynom. In der Tat sind die Nullstellen in $\mathbf{C}$ gegeben durch $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$ und $\zeta_3^2\sqrt[3]{2}$, wobei $\zeta_3 = \exp(2\pi\mathrm{i}/3) = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}$. Also ist $\mu_{y,\mathbf{Q}}(X) = X^3 - 2$, da dies ein irreduzibles normiertes Polynom in $\mathbf{Q}[X]$ mit Nullstelle y ist. Insbesondere ist $[\mathbf{Q}(y) : \mathbf{Q}] = \deg \mu_{y,\mathbf{Q}} = 3$.

Berechnen wir einmal $\mu_{y+1,\mathbf{Q}}(X)$. Dazu schreiben wir die Potenzen des fraglichen Elements in der Standardbasis (y^0, y^1, y^2) von $\mathbf{Q}(y)$ über $\mathbf{Q}$.

$$\begin{array}{rcrcrcr} (y+1)^0 & = & 1y^0 & + & 0y^1 & + & 0y^2 \\ (y+1)^1 & = & 1y^0 & + & 1y^1 & + & 0y^2 \\ (y+1)^2 & = & 1y^0 & + & 2y^1 & + & 1y^2 \\ (y+1)^3 & = & 3y^0 & + & 3y^1 & + & 3y^2 \end{array}$$

Die ersten drei Elemente bilden ein linear unabhängiges Tupel. Dahingegen ist

$$(y+1)^3 - 3(y+1)^2 + 3(y+1) - 3 \;=\; 0\,.$$

Also ist

$$\mu_{y+1,\mathbf{Q}}(X) \;=\; X^3 - 3X^2 + 3X - 3\,,$$

da dies das normierte irreduzible Polynom minimalen Grades in $\mathbf{Q}[X]$ mit Nullstelle $y + 1$ ist.

(4) Sei $K = \mathbf{F}_3$, $L = \mathbf{F}_9$ und $y = \iota - 1$. Berechnen wir einmal $\mu_{\iota-1,\mathbf{F}_3}$.

$$\begin{array}{rcrcr} (\iota-1)^0 & = & 1\iota^0 & + & 0\iota^1 \\ (\iota-1)^1 & = & -1\iota^0 & + & 1\iota^1 \\ (\iota-1)^2 & = & 0\iota^0 & + & 1\iota^1 \end{array}$$

Es ergibt sich

$$\mu_{\iota-1,\mathbf{F}_3}(X) \;=\; X^2 - X - 1\,.$$

(5) Die Einbettung von $\mathbf{F}_4$ in $\mathbf{F}_{16}$ in Aufgabe 24.(4) kann auch als Beispiel hierfür angeführt werden.

Bemerkung. Sei K ein Körper. Sei $f(X) \in K[X]$ ein normiertes irreduzibles Polynom. Dann ist $K[X]/f(X)K[X]$ ein Körper; vgl. Lemma in §1.8.5. Schreiben wir

$$\gamma \;:=\; X + f(X)K[X]\,,$$

so ist $K(\gamma) = K[X]/f(X)K[X]$. Darüberhinaus ist $f(X) = \mu_{\gamma,K}(X)$, da es sich um ein normiertes irreduzibles Polynom mit Nullstelle γ handelt. In der Tat ist

$$f(\gamma) \;=\; f(X+f(X)K[X]) \;=\; f(X)+f(X)K[X] \;=\; 0+K[X] \;=\; 0_{K[X]/f(X)K[X]} \;=\; 0_{K(\gamma)}\,.$$

Ist uns also ein normiertes irreduzibles Polynom $f(X)$ gegeben, so verfügen wir über eine zugehörige endliche monogene Erweiterung $K(\gamma)$ von K mit Minimalpolynom $\mu_{\gamma,K}(X) = f(X)$.

Beispiel. Es ist $\mathbf{F}_4 = \mathbf{F}_2(\alpha)$ durch $\mu_{\alpha,\mathbf{F}_2}(X) := X^2+X+1$ definierbar, da letzteres Polynom normiert und irreduzibel ist.

2.3.3 Endliche polygene Erweiterungen

Sei $k \geqslant 1$. Seien $y_1, \ldots, y_k \in L$ algebraisch über K. Sei die *endliche polygene Erweiterung*

$$K(y_1, y_2, \ldots, y_k) \ := \ K(y_1)(y_2)\cdots(y_k) \ \subseteq \ L$$

von K durch Iteration monogener Erweiterungen gewonnen. Es besteht $K(y_1, \ldots, y_k)$ also aus den polynomialen Ausdrücken in $(y_1, \ldots, y_k)$ mit Koeffizienten in K, d.h.

$$K(y_1, y_2, \ldots, y_k) \ = \ \{f(y_1, \ldots, y_k) \in L \ : \ f(X_1, \ldots, X_k) \in K[X_1, \ldots, X_k]\} \ .$$

Insbesondere kommt es auf die Reihenfolge der y_i nicht an, es ist also z.B. $K(y_2, y_3, y_1) = K(y_1, y_2, y_3)$. Mit Satz 1 (Gradsatz) wird

$$\begin{aligned}&[K(y_1, y_2, \ldots, y_k) : K] \ = \\ &[K(y_1, \ldots, y_{k-1}, y_k) : K(y_1, \ldots, y_{k-1})] \cdots [K(y_1, y_2) : K(y_1)][K(y_1) : K]\end{aligned}$$

Insbesondere ist $K(y_1, y_2, \ldots, y_k)|K$ endlich.

Beispiel. Wir bilden $\mathbf{Q}(\sqrt[3]{2}, \sqrt{3}) \subseteq \mathbf{C}$.

Es ist $\mu_{\sqrt[3]{2},\mathbf{Q}}(X) = X^3 - 2$ von Grad 3 und $\mu_{\sqrt{3},\mathbf{Q}(\sqrt[3]{2})}(X) = X^2 - 3$ von Grad 2. Also ist mit Satz 1 (Gradsatz) und Satz 2 (Minimalpolynom)

$$[\mathbf{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbf{Q}] \ = \ [\mathbf{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbf{Q}(\sqrt[3]{2})][\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] \ = \ 2 \cdot 3 \ = \ 6 \ .$$

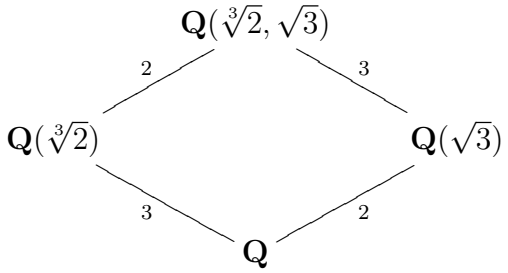
Eine aus dem Beweis des Gradsatzes resultierende Basis von $\mathbf{Q}(\sqrt[3]{2}, \sqrt{3})$ über $\mathbf{Q}$ ist gegeben durch

$$\Big(\underbrace{1, \sqrt{3}}, \underbrace{\sqrt[3]{2}, \sqrt{3}\sqrt[3]{2}}, \underbrace{(\sqrt[3]{2})^2, \sqrt{3}(\sqrt[3]{2})^2}\Big)$$

Alternativ ist $\mu_{\sqrt{3},\mathbf{Q}}(X) = X^2 - 3$ von Grad 2 und $\mu_{\sqrt[3]{2},\mathbf{Q}(\sqrt{3})}(X) = X^3 - 2$ von Grad 3. Also ist mit Satz 1 und Satz 2

$$[\mathbf{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbf{Q}] \ = \ [\mathbf{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{3})][\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \ = \ 3 \cdot 2 \ = \ 6 \ .$$

(Die Irreduzibilität der hier als Minimalpolynome angeführten Polynome kann mit dem Computeralgebrasystem Magma getestet werden, wie in §2.4 weiter unten dargelegt, oder mittels Aufgabe 55.(2) verifiziert werden. Allgemein werden wir, wegen der Komplexität dieses Problems, die Faktorisierung eines Polynoms in irreduzible als bekannt annehmen und ggf. via Magma bestimmen.)



Bemerkung. Eine endliche polygene Erweiterung kann durchaus auch monogen sein, so ein geeigneter Erzeuger existiert. So z.B. ist $\mathbf{R}(1+\mathrm{i}, 1-\mathrm{i}) = \mathbf{C} = \mathbf{R}(\mathrm{i})$.

2.3.4 Morphismen induziert von Nullstellen

Sei $K \xrightarrow[\sim]{a} \tilde{K}$ ein Isomorphismus von Körpern. Sei $\tilde{L}|\tilde{K}$ eine Körpererweiterung.

Sei $K(\gamma)$ eine endliche monogene Erweiterung mit Minimalpolynom

$$f(X) \;=\; \sum_{i\geqslant 0} f_i X^i \;:=\; \mu_{\gamma,K}(X) \in K[X]$$

von γ.

Wir erinnern an die Bezeichnung $f^a(X) = \sum_{i\geqslant 0} a(f_i)X^i \in \tilde{K}[X]$.

Bemerkung. *Sei*

$$\begin{array}{ccc} K(\gamma) & \xrightarrow{b} & \tilde{L} \\ \uparrow & & \uparrow \\ K & \xrightarrow[\sim]{a} & \tilde{K} \end{array}$$

ein kommutatives Viereck von Körpermorphismen, mit vertikalen Einbettungen.

Sei $\tilde{\gamma} := b(\gamma)$. *Dann ist* $f^a(\tilde{\gamma}) = 0$.

Beweis. Es ist

$$\begin{array}{rcl} f^a(\tilde{\gamma}) & = & \sum_{i\geqslant 0} a(f_i)\tilde{\gamma}^i \\ & = & \sum_{i\geqslant 0} a(f_i)b(\gamma)^i \\ & = & \sum_{i\geqslant 0} b(f_i)b(\gamma)^i \\ & = & b\left(\sum_{i\geqslant 0} f_i\gamma^i\right) \\ & = & b(f(\gamma)) \\ & = & b(0) \\ & = & 0\,. \end{array}$$

□

Wir wollen nun die Umkehrung dieser Bemerkung zeigen, in welcher wir $\tilde{\gamma}$ als Nullstelle von $f^a(X)$ gegeben voraussetzen und einen passenden Körpermorphismus b konstruieren.

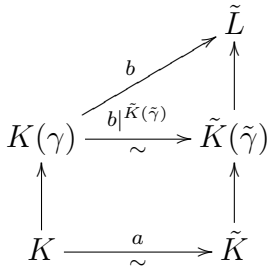
Satz 3 (Nullstelle induziert Morphismus)

Sei $\tilde{\gamma} \in \tilde{L}$ *gegeben mit* $\boxed{f^a(\tilde{\gamma}) = \sum_{i \geqslant 0} a(f_i)\tilde{\gamma}^i = 0_{\tilde{L}}}$.

Dann gibt es genau einen Morphismus von Körpern $K(\gamma) \xrightarrow{b} \tilde{L}$ *mit* $b(\gamma) = \tilde{\gamma}$ *und mit* $b|_K^{\tilde{K}} = a$.

Es ist $b(g(\tilde{\gamma})) = g^a(\tilde{\gamma})$ *für* $g(X) \in K[X]$.

Es ist $b|^{\tilde{K}(\tilde{\gamma})} : K(\gamma) \xrightarrow{\sim} \tilde{K}(\tilde{\gamma})$ *ein Isomorphismus.*



Beweis. Schreibe $\hat{a} : K \longrightarrow \tilde{L}$, $x \longmapsto a(x)$. D.h. es sei $\hat{a}$ der Isomorphismus a, gefolgt von der Einbettung $\tilde{K} \longrightarrow \tilde{L}$.

Es ist $K[X]/f(X)K(X) \xrightarrow{\sim} K(\gamma)$, $g(X) + f(X)K[X] \longmapsto g(\gamma)$; vgl. Satz 2.(4) aus §2.3.2.

Wir haben andererseits einen Morphismus von Ringen

$$\begin{array}{rcl} K[X] & \longrightarrow & \tilde{L} \\ g(X) & \longmapsto & g^a(\tilde{\gamma}) \ , \end{array}$$

welcher auf K zu $\hat{a}$ einschränkt; vgl. Bemerkung in §1.6.2. Dieser schickt $f(X)$ nach $f^a(\tilde{\gamma}) = 0_{\tilde{L}}$, und also $f(X)K[X]$ nach $\{0_{\tilde{L}}\}$. Also gibt es genau einen Morphismus von Ringen – nun genauer gesagt von Körpern –

$$\begin{array}{rcl} K[X]/f(X)K[X] & \longrightarrow & \tilde{L} \\ g(X) + f(X)K[X] & \longmapsto & g^a(\tilde{\gamma}) \ , \end{array}$$

welcher komponiert mit ρ vorstehenden Morphismus gibt; vgl. Bemerkung aus §1.4.3. Die Komposition des inversen Isomorphismus $K(\gamma) \xrightarrow{\sim} K[X]/f(X)K(X)$, $g(\gamma) \longmapsto g(X) + f(X)K[X]$ mit diesem liefert den Körpermorphismus

$$\begin{array}{rcl} K(\gamma) & \longrightarrow & \tilde{L} \\ g(\gamma) & \longmapsto & g(\tilde{\gamma}) \ , \end{array}$$

welcher auf K zu $\hat{a}$ einschränkt. Dies zeigt die Existenz von b und die behauptete Formel $b(g(\tilde{\gamma})) = g^a(\tilde{\gamma})$ für $g(X) \in K[X]$.

Zeigen wir die Eindeutigkeit von b. Sei $K(\gamma) \xrightarrow{b^*} \tilde{L}$ ein weiterer Körpermorphismus mit $b^*(\gamma) = \tilde{\gamma}$ und $b^*|_K^{\tilde{K}} = a$. Jedes Element in $K(\gamma)$ ist von der Form $g(\gamma)$ für ein $g(X) \in K[X]$.

Dafür wird nun

$$\begin{aligned} b^*(g(\gamma)) &= b^*(\textstyle\sum_{i\geqslant 0} g_i\gamma^i) \\ &= \textstyle\sum_{i\geqslant 0} b^*(g_i)b^*(\gamma)^i \\ &= \textstyle\sum_{i\geqslant 0} a(g_i)\tilde{\gamma}^i \\ &= \textstyle\sum_{i\geqslant 0} b(g_i)b(\gamma)^i \\ &= b(\textstyle\sum_{i\geqslant 0} g_i\gamma^i) \\ &= b(g(\gamma)) \ . \end{aligned}$$

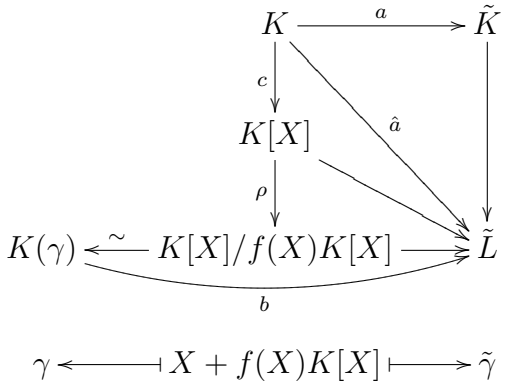
Also ist $b^* = b$.

Das Bild von b ist gleich

$$\operatorname{Im} b \ = \ \{g^a(\tilde{\gamma}) \ : \ g(X) \in K[X]\} \ = \ \{\tilde{g}(\tilde{\gamma}) \ : \ \tilde{g}(X) \in \tilde{K}[X]\} \ = \ \tilde{K}(\tilde{\gamma}) \ ,$$

wobei wir für die zweite Gleichheit verwendet haben, daß $K[X] \longrightarrow \tilde{K}[X]$, $f(X) \longmapsto f^a(X)$ bijektiv ist. Da Körpermorphismen injektiv sind, ist folglich $b|^{\tilde{K}(\tilde{\gamma})} : K(\gamma) \longrightarrow \tilde{K}(\tilde{\gamma})$ ein Isomorphismus.

Eine Konstruktionsskizze.



□

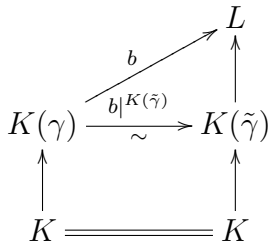
Betrachten wir den Spezialfall $a = \mathrm{id}_K$ explizit.

Folgerung. *Sei $L|K$ eine Körpererweiterung. Sei $K(\gamma)$ eine endliche monogene Erweiterung mit Minimalpolynom $f(X) = \sum_{i\geqslant 0} f_i X^i := \mu_{\gamma,K}(X) \in K[X]$ von γ.*

Sei $\tilde{\gamma} \in L$ gegeben mit $\boxed{f(\tilde{\gamma}) = 0_L}$.

Dann gibt es genau einen Morphismus von Körpern $K(\gamma) \xrightarrow{b} L$ mit $b(\gamma) = \tilde{\gamma}$ und mit $b|_K^K = \mathrm{id}_K$.

Es ist $K(\gamma) \xrightarrow{b|^{K(\tilde{\gamma})}} K(\tilde{\gamma})$ ein Isomorphismus.



Bemerkung. *In der Situation der Folgerung steht die Menge der Körpermorphismen von $K(\gamma)$ nach L, die auf K identisch einschränken, in Bijektion zur Menge der Nullstellen von $f(X)$ in L. Die Bijektion ist dadurch gegeben, daß solch ein Körpermorphismus b auf die Nullstelle $b(\gamma)$ von $f(X)$ abgebildet wird.*

Beweis. Die Injektivität folgt, da, wie im Beweis zu Satz 3 gesehen, ein Körpermorphismus von $K(\gamma)$ nach L durch seine Einschränkung auf $K \cup \{\gamma\}$ festgelegt ist. Die Surjektivität entnehmen wir vorangehender Folgerung. ▫

Beispiel.

(1) Betrachte $\mathbf{C}|\mathbf{R}$. Sei $\gamma = \mathrm{i}$. Hier ist nun $\mathbf{C} = \mathbf{R}(\mathrm{i})$. Es ist $f(X) = \mu_{\mathrm{i},\mathbf{R}}(X) = X^2 + 1 \in \mathbf{R}[X]$. Nun hat $f(X)$ die weitere Nullstelle $\tilde{\gamma} := -\mathrm{i}$ in $\mathbf{C}$. Daher gibt es genau einen Morphismus von Körpern

$$(\ \mathbf{C}\ =)\ \mathbf{R}(\mathrm{i})\ \longrightarrow\ \mathbf{C}\ (=\ \mathbf{R}(\mathrm{i})\ )\ ,$$

der $\gamma = \mathrm{i}$ auf $\tilde{\gamma} = -\mathrm{i}$ schickt, und der auf $\mathbf{R}$ identisch einschränkt. Dies ist die komplexe Konjugation.

(2) Betrachte $\mathbf{F}_4|\mathbf{F}_2$. Sei $\gamma = \alpha$. Hier ist nun $\mathbf{F}_4 = \mathbf{F}_2(\alpha)$. Es ist $f(X) = \mu_{\alpha,\mathbf{F}_2}(X) = X^2 + X + 1 \in \mathbf{F}_2[X]$. Nun hat $f(X)$ die weitere Nullstelle $\alpha + 1$ in $\mathbf{F}_4$. Daher gibt es genau einen Morphismus von Körpern

$$(\ \mathbf{F}_4\ =)\ \mathbf{F}_2(\alpha)\ \longrightarrow\ \mathbf{F}_4\ (=\ \mathbf{F}_2(\alpha)\ )\ ,$$

der $\gamma = \alpha$ auf $\tilde{\gamma} = \alpha + 1$ schickt, und der auf $\mathbf{F}_2$ identisch einschränkt. Dieser schickt dann $u\alpha + v$ auf $u(\alpha + 1) + v$, wobei $u,\ v\ \in\ \mathbf{F}_2$.

Da auch

$$\mathrm{Frob}_{\mathbf{F}_4}(u\alpha + v)\ =\ (u\alpha + v)^2\ =\ u^2\alpha^2 + v^2\ =\ u\alpha^2 + v\ =\ u(\alpha + 1) + v$$

ist, ist der gefundene Automorphismus von $\mathbf{F}_4$ gleich dem Frobenius $\mathrm{Frob}_{\mathbf{F}_4}$; vgl. Aufgabe 24. Dies folgt übrigens auch schon kürzer aus $\mathrm{Frob}_{\mathbf{F}_4}(\alpha) = \alpha^2 = \alpha + 1$.

2.4 Ein Taschenrechner zur Faktorisierung von Polynomen

Auf `http://magma.maths.usyd.edu.au/calc/` findet sich ein *Magma Calculator,* welchen wir als Taschenrechner zur Faktorisierung von Polynomen verwenden wollen.

Die folgenden Beispiele sind selbsterklärend – falls nicht, konsultiere man `http://magma.maths.usyd.edu.au/magma/htmlhelp/MAGMA.htm`.

Beispiel. Folgender Quelltext faktorisiert $X^4 + X^3 - X - 1 \in \mathbf{Q}[X]$ in irreduzible Polynome.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
f := X^4 + X^3 - X - 1;
Factorisation(f);
```

Dieser Quelltext ist in das orangene Feld einzugeben und der Knopf *Evaluate* zu drücken. Im grünen Feld erscheint das Ergebnis.

Beispiel. Folgender Quelltext konstruiert zunächst $K = \mathbf{Q}(\mathrm{i}\sqrt{2})$ durch Angabe des Minimalpolynoms $g(T) = T^2 + 2$ von $\alpha = \texttt{al} = \mathrm{i}\sqrt{2}$ und faktorisiert dann $X^4 + X + 1 \in K[X]$ in irreduzible Polynome. Mit der letzten Zeile überprüft man, daß $\alpha = \texttt{al}$ in der Tat eine Wurzel aus -2 ist.

```
Q := Rationals();
R<T> := PolynomialRing(Q);
g := T^2 + 2;
K<al> := ext<Q|g>;
S<X> := PolynomialRing(K);
f := X^4 + X + 1;
Factorisation(f);
al^2;
```

Das Ergebnis sieht etwas mager aus, sagt aber immerhin, daß $X^4 + X + 1 \in \mathbf{Q}(\mathrm{i}\sqrt{2})[X]$ irreduzibel ist.

Beispiel. Folgender Quelltext konstruiert zunächst $\texttt{K} = \mathbf{Q}(a)$, wobei

$$\mu_{a,\mathbf{Q}}(X) \;=\; X^4 + X + 1\,.$$

Dann wird $X^4 + X + 1 \in \texttt{K}[X]$ in irreduzible Polynome faktorisiert.

Sodann wird $\texttt{KK} = \mathbf{Q}(a, b)$ konstruiert, wobei

$$\mu_{b,\mathbf{Q}(a)}(X) = X^3 + aX^2 + a^2X + a^3 + 1$$

der zweite irreduzible Faktor der vorstehenden Faktorisierung ist.

> In Magma ist zu beachten, daß ein neuer Koeffizientenbereich für den Polynomring auch eine neue Variablenbezeichnung erfordert, hier `XX`. Variablennamen wie `XX`, `KK` dürfen mehr als einen Buchstaben lang sein.

Dann wird $X^4 + X + 1 \in \texttt{KK}[X]$ in irreduzible Polynome faktorisiert.

Schließlich wird $\texttt{KKK} = \mathbf{Q}(a, b, c)$ konstruiert, wobei

$$\mu_{\gamma,\mathbf{Q}(a,b)}(X) = X^2 + (a + b)X + b^2 + ab + a^2 \; .$$

Dann wird $X^4 + X + 1 \in \texttt{KKK}[X]$ in irreduzible Polynome faktorisiert.

Wir haben in $\texttt{KKK}[X] = \mathbf{Q}(a, b, c)[X]$ eine Zerlegung in vier Linearfaktoren erreicht, namentlich

$$X^4 + X + 1 \; = \; (X - a)(X - b)(X - c)(X + a + b + c) \; .$$

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + X + 1); // erster Durchlauf
KK<a> := ext<Q | X^4 + X + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^4 + XX + 1); // zweiter Durchlauf
KKK<b> := ext<KK | XX^3 + a*XX^2 + a^2*XX + a^3 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^4 + XXX + 1); // dritter Durchlauf
KKKK<c> := ext<KKK | XXX^2 + (a + b)*XXX + b^2 + a*b + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^4 + XXXX + 1); // vierter Durchlauf
```

Um den Magma Calculator sinnvoll zu verwenden, muß zunächst der Teil bis einschließlich "erster Durchlauf" eingegeben werden. Der Ausgabe entnimmt man das Polynom `X^4 + X + 1`, welches zur Definition von `KK` verwandt wird. Dann muß nochmals alles bis einschließlich "zweiter Durchlauf" eingegeben werden. Der Ausgabe entnimmt man das Polynom `XX^3 + a*XX^2 + a^2*XX + a^3 + 1`, welches zur Definition von `KKK` verwandt wird. Usf.

2.5 Zerfällungskörper

Ziel der Vorlesung ist es, ein Verfahren zu entwickeln, um für ein gegebenes irreduzibles Polynom die Galoisgruppe zu bestimmen (und aus dieser Folgerungen über die Form seiner Nullstellen zu gewinnen). Der erste Schritt hierfür ist die Berechnung seines Zerfällungskörpers; das ist der in einem gewissen Sinne kleinste Körper, in dem das Polynom in Linearfaktoren zerlegt werden kann. Die Galoisgruppe des gegebenen Polynoms wird dann die Gruppe der Automorphismen des Zerfällungskörpers sein, die identisch auf den Grundkörper einschränken.

Sei K ein Körper. Sei $f(X) \in K[X] \setminus \{0\}$ ein normiertes Polynom von Grad $n := \deg f$.

2.5.1 Begriff des Zerfällungskörpers

Definition. Es heißt L *Zerfällungskörper* (über K) von $f(X) \in K[X]$, falls $L|K$, falls es $\gamma_1, \ldots, \gamma_n \in L$ gibt mit

$$f(X) \;=\; (X-\gamma_1)(X-\gamma_2)\cdots(X-\gamma_n) \qquad \text{in } L[X]$$

und falls $K(\gamma_1, \ldots, \gamma_n) = L$.

Beispiel.

(1) Es ist $\mathbf{C}$ ein Zerfällungskörper von $X^2+1 \in \mathbf{R}[X]$, da $X^2+1 = (X+\mathrm{i})(X-\mathrm{i})$ und $\mathbf{R}(\mathrm{i}, -\mathrm{i}) = \mathbf{R}(\mathrm{i}) = \mathbf{C}$.

(2) Es ist $\mathbf{Q}(\sqrt[3]{2})$ kein Zerfällungskörper von $X^3-2 \in \mathbf{Q}[X]$, da

$$X^3-2 = (X-\sqrt[3]{2})(X^2+\sqrt[3]{2}\,X+(\sqrt[3]{2})^2) \;\in\; \mathbf{Q}(\sqrt[3]{2})[X]$$

und der Faktor $X^2+\sqrt[3]{2}\,X+(\sqrt[3]{2})^2$ in $\mathbf{Q}(\sqrt[3]{2})[X]$ irreduzibel ist, schon mangels Nullstelle in $\mathbf{R} \supseteq \mathbf{Q}(\sqrt[3]{2})$.

Wohl ist aber $\mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ mit $\zeta_3 := -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3} = \exp(2\pi\mathrm{i}/3)$ ein Zerfällungskörper von $X^3-2 \in \mathbf{Q}[X]$, da zum einen

$$X^3-2 = (X-\sqrt[3]{2})(X-\zeta_3\sqrt[3]{2})(X-\zeta_3^2\sqrt[3]{2}) \;\in\; \mathbf{Q}(\sqrt[3]{2},\, \zeta_3)[X]\,,$$

und da zum anderen $\mathbf{Q}(\sqrt[3]{2},\, \zeta_3\sqrt[3]{2},\, \zeta_3^2\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{2},\, \zeta_3)$.

(3) Es ist $\mathbf{F}_8$ ein Zerfällungskörper von $X^3+X+1 \in \mathbf{F}_2[X]$, da

$$X^3+X+1 \;=\; (X+\beta)(X+\beta^2)(X+(\beta^2+\beta)) \;\in\; \mathbf{F}_8[X]$$

und da $\mathbf{F}_2(\beta, \beta^2, \beta^2+\beta) = \mathbf{F}_2(\beta) = \mathbf{F}_8$.

Bemerkung. *Ist $M|L|K$, ist $f(X) \in K[X]$, und ist M ein Zerfällungskörper für $f(X)$ über K, so ist M auch ein Zerfällungskörper von $f(X)$ über L.*

Beweis. Es ist $f(X) = \prod_{i\in[1,n]}(X-\gamma_i) \in M[X]$ für gewisse $\gamma_i \in M$. Da ferner $M = K(\gamma_1, \ldots, \gamma_n)$, ist a fortiori auch $M = L(\gamma_1, \ldots, \gamma_n)$. ▫

Bemerkung. *Ist $L|K$ ein Zerfällungskörper für $f(X) \in K[X]$ über K, so ist $L|K$ als endliche polygene Erweiterung insbesondere endlich; cf.* §2.3.3.

2.5.2 Existenz des Zerfällungskörpers

Wir erinnern daran, daß K ein Körper ist und $f(X) \in K[X] \setminus \{0\}$ ein normiertes Polynom von Grad $n := \deg f$.

Satz 4 (Existenz Zerfällungskörper)

Es existiert ein Zerfällungskörper $L|K$ von $f(X) \in K[X]$ mit $[L : K] \leqslant n!$.

Beweis. Schreibe $K_0 := K$. Schreibe $f^{(1)}(X) := f(X) \in K[X]$. Es ist $\deg f^{(1)} = n$.

Schritt 1. Sei $g^{(1)}(X)$ ein irreduzibler Faktor von $f^{(1)}(X)$ in $K_0[X]$. Sei $K_1 := K_0(a_1)$ eine endliche monogene Erweiterung von K_0 mit $\mu_{a_1,K_0}(X) = g^{(1)}(X)$; vgl. die zweite Bemerkung in §2.3.2. Es wird

$$[K_1 : K_0] \;=\; \deg g^{(1)} \;\leqslant\; \deg f^{(1)} \;=\; n \;.$$

Beachte, daß aus $g^{(1)}(a_1) = 0$ folgt, daß $f^{(1)}(a_1) = 0$. Schreibe dementsprechend $f^{(1)}(X) = (X - a_1)f^{(2)}(X)$ in $K_1[X]$. Es ist $\deg f^{(2)} = n - 1$. Es ist

$$f(X) \;=\; (X - a_1)f^{(2)}(X) \;.$$

Schritt 2. Sei $g^{(2)}(X)$ ein irreduzibler Faktor von $f^{(2)}(X)$ in $K_1[X]$. Sei $K_2 := K_1(a_2)$ eine endliche monogene Erweiterung von K_1 mit $\mu_{a_2,K_1}(X) = g^{(2)}(X)$. Es wird

$$[K_2 : K_1] \;=\; \deg g^{(2)} \;\leqslant\; \deg f^{(2)} \;=\; n - 1 \;.$$

Beachte, daß aus $g^{(2)}(a_2) = 0$ folgt, daß $f^{(2)}(a_2) = 0$. Schreibe dementsprechend $f^{(2)}(X) = (X - a_2)f^{(3)}(X)$ in $K_2[X]$. Es ist $\deg f^{(3)} = n - 2$. Es ist

$$f(X) \;=\; (X - a_1)(X - a_2)f^{(3)}(X) \;.$$

Schritt 3. Sei $g^{(3)}(X)$ ein irreduzibler Faktor von $f^{(3)}(X)$ in $K_2[X]$. Sei $K_3 := K_2(a_3)$ eine endliche monogene Erweiterung von K_2 mit $\mu_{a_3,K_2}(X) = g^{(3)}(X)$. Es wird

$$[K_3 : K_2] \;=\; \deg g^{(3)} \;\leqslant\; \deg f^{(3)} \;=\; n - 2 \;.$$

Beachte, daß aus $g^{(3)}(a_3) = 0$ folgt, daß $f^{(3)}(a_3) = 0$. Schreibe dementsprechend $f^{(3)}(X) = (X - a_3)f^{(4)}(X)$ in $K_3[X]$. Es ist $\deg f^{(4)} = n - 3$. Es ist

$$f(X) \;=\; (X - a_1)(X - a_2)(X - a_3)f^{(4)}(X) \;.$$

Setze so fort bis *Schritt* n, woraus $f^{(n+1)}(X)$ mit $\deg f^{(n+1)} = 0$ hervorgeht. Wir haben also $f^{(n+1)}(X) = 1$.

Setze $L := K_n = K(a_1, \ldots, a_n)$, insbesondere $L|K$. Wir haben insgesamt erhalten

$$f(X) \;=\; (X - a_1)(X - a_2) \cdots (X - a_n) \;\in\; L[X] \;.$$

Somit erfüllt L alle drei Bedingungen an einen Zerfällungskörper.

Schließlich ist mit Satz 1 (Gradsatz)

$$[L : K] \;=\; [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1][K_1 : K_0] \;\leqslant\; 1 \cdot 2 \cdots (n-1) \cdot n \;=\; n! \;.$$

□

Bemerkung. In der Praxis muß der Prozeß aus dem Beweis zu Satz 4 nur bis zu der Stelle fortgesetzt werden, an der $f^{(i)}(X)$ in $K_i[X]$ in Linearfaktoren zerfällt. Denn dann sind alle weiteren Polynome $g^{(j)}(X)$ mit $j \geqslant i$ von Grad 1, und damit findet keine echte Körpererweiterung mehr statt.

Beispiel. Das letzte Beispiel in §2.4 war die Berechnung eines Zerfällungskörpers von $X^4 + X + 1 \in \mathbf{Q}[X]$ via Magma. In den Bezeichnungen des Existenzbeweises liest sich dies wie folgt.

Es ist $K_0 = \mathbf{Q}$ und $f^{(1)}(X) = X^4 + X + 1$.

Schritt 1. Es ist $f^{(1)}(X) \in \mathbf{Q}[X]$ irreduzibel, also $g^{(1)}(X) = X^4 + X + 1$ die einzig mögliche Wahl. Sei $K_1 := \mathbf{Q}(a)$ mit $a^4 + a + 1 = 0$; will sagen, mit $\mu_{a,\mathbf{Q}}(X) = X^4 + X + 1$. Zerlege

$$X^4 + X + 1 \;=\; (X - a)\underbrace{(X^3 + aX^2 + a^2X + a^3 + 1)}_{= f^{(2)}(X)} \;\in\; \mathbf{Q}(a)[X] \,.$$

Schritt 2. Es ist $f^{(2)}(X) \in \mathbf{Q}(a)[X]$ irreduzibel, also $g^{(2)}(X) = f^{(2)}(X)$. Sei $K_2 := \mathbf{Q}(a, b)$ mit $b^3 + ab^2 + a^2b + a^3 + 1 = 0$. Zerlege

$$X^3 + aX^2 + a^2X + a^3 + 1 \;=\; (X - b)\underbrace{(X^2 + (a + b)X + (a^2 + ab + b^2))}_{= f^{(3)}(X)} \;\in\; \mathbf{Q}(a, b)[X] \,.$$

Schritt 2. Es ist $f^{(3)}(X) \in \mathbf{Q}(a, b)[X]$ irreduzibel, also $g^{(3)}(X) = f^{(3)}(X)$. Sei $K_3 := \mathbf{Q}(a, b, c)$ mit $c^2 + (a + b)c + (a^2 + ab + b^2) = 0$. Zerlege

$$X^3 + aX^2 + a^2X + a^3 + 1 \;=\; (X - b)\underbrace{(X^2 + (a + b)X + (a^2 + ab + b^2))}_{= f^{(3)}(X)} \;\in\; \mathbf{Q}(a, b)[X] \,.$$

Die weiteren Schritte können bereits unterbleiben, da mit $L := K_2 = \mathbf{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2})$ wir bereits die Faktorisierung

$$(X^2 + (a + b)X + (a^2 + ab + b^2)) \;=\; (X - c)(X + a + b + c) \;\in\; \mathbf{Q}(a, b, c)[X] \,.$$

in Linearfaktoren haben. Hier können wir nun abbrechen, denn wir haben insgesamt

$$X^4 + X + 1 \;=\; (X - a)(X - b)(X - c)(X + a + b + c) \;\in\; \mathbf{Q}(a, b, c)[X]$$

erreicht. Ferner ist $\mathbf{Q}(a, b, c, -a - b - c) = \mathbf{Q}(a, b, c)$. Es ist also $\mathbf{Q}(a, b, c)$ ein Zerfällungskörper von $X^4 + X + 1 \in \mathbf{Q}[X]$. Sein Grad über $\mathbf{Q}$ berechnet sich zu

$$[\mathbf{Q}(a, b, c) : \mathbf{Q}] \;=\; [\mathbf{Q}(a, b, c) : \mathbf{Q}(a, b)][\mathbf{Q}(a, b) : \mathbf{Q}(b)][\mathbf{Q}(b) : \mathbf{Q}] \;=\; 2 \cdot 3 \cdot 4 \;=\; 24 \,.$$

Die gefundenen Minimalpolynome besagen hierbei, daß beim Rechnen in $\mathbf{Q}(a, b, c)$ die Regeln

$$\begin{aligned} 0 &= a^4 + a + 1 \\ 0 &= b^3 + ab^2 + a^2b + a^3 + 1 \\ 0 &= c^2 + (a + b)c + (b^2 + ab + a^2) \end{aligned}$$

zu beachten sind – und nur diese.

Im vorstehenden Beispiel war für $g^{(i)}(X)$ stets nur eine Wahl möglich, da $f^{(i)}(X)$ nie "freiwillig" zerfiel. Dieser Fall ist recht typisch – fängt man mit einem beliebigen Polynom an, so ist die Wahrscheinlichkeit groß, daß das Verfahren so ausgeht. Falls aber "mit etwas Glück" ein $f^{(i)}(X)$ "freiwillig" zerfällt, so passieren interessante Dinge (um vorzugreifen: dann ist die Galoisgruppe eine echte Untergruppe der symmetrischen Gruppe).

2.5.3 Eindeutigkeit des Zerfällungskörpers

Wir erinnern daran, daß K ein Körper ist und $f(X) \in K[X] \setminus \{0\}$ ein normiertes Polynom von Grad $n := \deg f$.

Satz 5 (Eindeutigkeit Zerfällungskörper) *Seien $L|K$ und $\tilde{L}|K$ Zerfällungskörper von $f(X) \in K[X]$ über K. Dann gibt es einen Körperisomorphismus $L \xrightarrow[\sim]{\sigma} \tilde{L}$ mit $\sigma|_K^K = \mathrm{id}_K$.*

$$\begin{array}{ccc} L & \xrightarrow[\sim]{\sigma} & \tilde{L} \\ \uparrow & & \uparrow \\ K & = & K \end{array}$$

Unter impliziter Bezugnahme auf Satz 5 werden wir auch von dem Zerfällungskörper von $f(X) \in K[X]$ reden.

Beweis. Um die Aussage per Induktion zeigen zu können, verallgemeinern wir sie ein kleines bißchen. Sei $K \xrightarrow[\sim]{\rho} \tilde{K}$ ein Körperisomorphismus. Sei $L|K$ ein Zerfällungskörper von $f(X) \in K[X]$ über K. Sei $\tilde{L}|\tilde{K}$ ein Zerfällungskörper von $f^\rho(X) \in \tilde{K}[X]$ über $\tilde{K}$. Dann, so *behaupten* wir, gibt es einen Körperisomorphismus $L \xrightarrow[\sim]{\sigma} \tilde{L}$ mit $\sigma|_K^{\tilde{K}} = \rho$.

$$\begin{array}{ccc} L & \xrightarrow[\sim]{\sigma} & \tilde{L} \\ \uparrow & & \uparrow \\ K & \xrightarrow[\sim]{\rho} & \tilde{K} \end{array}$$

(Die für den Satz zu zeigende Aussage ist hiervon der Spezialfall $\rho = \mathrm{id}_K$.)

Schreibe zunächst

$$\begin{array}{rcccl} f(X) & = & \prod_{i\in[1,n]}(X-\gamma_i) & \in & L[X] \\ f^\rho(X) & = & \prod_{i\in[1,n]}(X-\tilde{\gamma}_i) & \in & \tilde{L}[X]\,. \end{array}$$

Beachte, daß $L = K(\gamma_1, \ldots, \gamma_n)$ und $\tilde{L} = \tilde{K}(\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n)$.

Wir führen eine Induktion nach $[L : K]$.

Ist $[L : K] = 1$, so ist $L = K$, und also

$$f(X) \;=\; \prod_{i\in[1,n]} (X-\gamma_i) \;\in\; K[X]\,.$$

Somit ist

$$f^\rho(X) \;=\; \prod_{i\in[1,n]} (X-\rho(\gamma_i)) \;=\; \prod_{i\in[1,n]} (X-\tilde{\gamma}_i) \;\in\; \tilde{K}[X]\,,$$

und also $\tilde{L} = \tilde{K}(\rho(\gamma_1),\ldots,\rho(\gamma_n)) = \tilde{K}$. Wir können $\sigma = \rho$ wählen.

Ist $[L:K] > 1$, so gibt es ein $s \in [1,n]$ mit $\gamma_s \notin K$, insbesondere also $[K(\gamma_s):K] > 1$. Halten wir fest, daß aus $[L:K] = [L:K(\gamma_s)][K(\gamma_s):K]$ daher folgt, daß

$$[L:K] \;>\; [L:K(\gamma_s)]\,.$$

Da $f(\gamma_s) = 0$, ist $\mu_{\gamma_s,K}(X)$ ein Teiler von $f(X)$, also

$$f(X) \;=\; \mu_{\gamma_s,K}(X)g(X)$$

für ein $g(X) \in K[X]$. Somit ist

$$f^\rho(X) \;=\; \mu^\rho_{\gamma_s,K}(X)g^\rho(X)\,.$$

Also gibt es ein $\tilde{s} \in [1,n]$ mit $\mu^\rho_{\gamma_s,K}(\tilde{\gamma}_{\tilde{s}}) = 0$. Satz 3 gibt nun einen Isomorphismus $\tau : K(\gamma_s) \xrightarrow{\sim} \tilde{K}(\tilde{\gamma}_{\tilde{s}})$ mit $\tau(\gamma_s) = \tilde{\gamma}_{\tilde{s}}$ und $\tau|^{\tilde{K}}_K = \rho$.

$$\begin{array}{ccc} L & & \tilde{L} \\ \uparrow & & \uparrow \\ K(\gamma_s) & \xrightarrow[\sim]{\tau} & \tilde{K}(\tilde{\gamma}_{\tilde{s}}) \\ \uparrow & & \uparrow \\ K & \xrightarrow[\sim]{\rho} & \tilde{K} \end{array}$$

Da L ein Zerfällungskörper von $f(X)$ über $K(\gamma_s)$ ist und $\tilde{L}$ ein Zerfällungskörper von $f^\rho(X)$ über $\tilde{K}(\tilde{\gamma}_{\tilde{s}})$ ist, und da ferner $[L:K(\gamma_s)] < [L:K]$, gibt die Induktionsvoraussetzung einen Isomorphismus $\sigma : L \xrightarrow{\sim} \tilde{L}$ mit $\sigma|^{\tilde{K}(\tilde{\gamma}_{\tilde{s}})}_{K(\gamma_s)} = \tau$, und also $\sigma|^{\tilde{K}}_K = \rho$.

$$\begin{array}{ccc} L & \xrightarrow[\sim]{\sigma} & \tilde{L} \\ \uparrow & & \uparrow \\ K(\gamma_s) & \xrightarrow[\sim]{\tau} & \tilde{K}(\tilde{\gamma}_{\tilde{s}}) \\ \uparrow & & \uparrow \\ K & \xrightarrow[\sim]{\rho} & \tilde{K} \end{array}$$

Dies zeigt die *Behauptung.* ▫

Der Beweis zu Satz 5 ist ein Beispiel dafür, daß es manchmal einfacher ist, eine allgemeinere Aussage zu zeigen, als nur einen Spezialfall.

Die Galoisgruppe von $f(X)$ wird aus den Automorphismen von L bestehen, die auf K identisch einschränken. Der Beweis von Satz 5 wird zu einer Methode zu ihrer Berechnung ausgebaut werden. Wesentlich wird hierbei sein, daß darin die Wahl von $\tilde{\gamma}_{\tilde{s}}$ zu bereits gewähltem γ_s nicht eindeutig getroffen werden kann. Cf. §3.4.1.

2.5.4 Endliche Zerfällungskörper

Wir wollen den Körper $\mathbf{F}_{p^k}$ mit $|\mathbf{F}_{p^k}| = p^k$ konstruieren, für eine beliebig vorgegebene Primzahl p und ein beliebig vorgegebenes $k \geqslant 1$. Die Namensgebung deutet auch schon an, daß es (bis auf Isomorphie) nur einen Körper mit dieser Kardinalität gibt.

Sei p eine Primzahl. Sei $k \geqslant 1$. Sei K der Zerfällungskörper von

$$z(X) \;:=\; X^{p^k} - X \in \mathbf{F}_p[X] \;.$$

Es ist $K|\mathbf{F}_p$.

Lemma.

(1) *Es ist* $|K| = p^k$.

(2) *Sei* L *ein Körper mit* $|L| = p^k$. *Dann ist* $L \simeq K$.

Wir schreiben auch $\mathbf{F}_{p^k} := K$. Es ist also $\mathbf{F}_{p^k}$ der Zerfällungskörper von $X^{p^k} - X$.

Beweis. Zu (1). Setze $\tilde{K} := \{x \in K \;:\; z(x) = 0\} \subseteq K$.

Wir *behaupten,* daß $\tilde{K}$ ein Teilkörper von K ist, der $\mathbf{F}_p$ enthält. In der Tat ist $z(x) = 0$ gleichbedeutend zu $\mathrm{Frob}_K^k(x) = x$; vgl. Aufgabe 24. Somit ist $\mathbf{F}_p \subseteq \tilde{K}$, da für Elemente in $\mathbf{F}_p$ sogar bereits $\mathrm{Frob}_K(x) = x$ ist; vgl. Aufgabe 12.(1) oder Aufgabe 24.(2). Insbesondere ist $1 \in \tilde{K}$. Sind $x,\, y \in \tilde{K}$, so ist

$$\mathrm{Frob}_K^k(xy) \;=\; \mathrm{Frob}_K^k(x)\,\mathrm{Frob}_K^k(y) \;=\; xy \;,$$

womit $xy \in \tilde{K}$; ferner ist

$$\mathrm{Frob}_K^k(x-y) \;=\; \mathrm{Frob}_K^k(x) - \mathrm{Frob}_K^k(y) \;=\; x-y \;,$$

woraus $x - y \in \tilde{K}$. Also ist $\tilde{K} \subseteq K$ ein Teilring. Ist $x \in \tilde{K} \smallsetminus \{0\}$, so ist

$$\mathrm{Frob}_K^k(x^{-1}) \;=\; \mathrm{Frob}_K^k(x)^{-1} \;=\; x^{-1} \;,$$

und also $x^{-1} \in \tilde{K}$. Somit ist $\tilde{K} \subseteq K$ ein Teilkörper. Die *Behauptung* ist gezeigt.

Man hätte für $\tilde{K} \subseteq K$ Teilkörper auch verwenden können, daß endliche Integritätsbereiche Körper sind.

Schreibe nun unter Verwendung der Zerfällungskörpereigenschaft von K

$$z(X) \;=\; \textstyle\prod_{i\in[1,p^k]}(X-\gamma_i) \;\in\; K[X]$$

mit $\gamma_i \in K$. Nach Definition ist aber $\gamma_i \in \tilde{K}$ für alle $i \in [1, p^k]$. Es folgt, abermals unter Verwendung der Zerfällungskörpereigenschaft von K,

$$\tilde{K} \;\subseteq\; K \;=\; \mathbf{F}_p(\gamma_1, \ldots, \gamma_{p^k}) \;\subseteq\; \tilde{K} \;,$$

und also $K = \tilde{K} = \{\gamma_1, \ldots, \gamma_{p^k}\}$.

Um nun zu zeigen, daß $|K| = p^k$, genügt es zu zeigen, daß $\gamma_i \neq \gamma_j$ für $1 \leqslant i < j \leqslant p^k$. Mit Aufgabe 25.(2) müssen wir zeigen, daß $\mathrm{ggT}(z(X), z'(X)) = 1$ in $K[X]$; vgl. auch Aufgabe 25.(3). In der Tat ist aber $z'(X) = -1$.

Zu (2). Es ist $\mathbf{F}_p \subseteq L$ der Primkörper. Mit Satz 5 und (1) genügt es zu zeigen, daß L ein Zerfällungskörper von $z(X) = X^{p^k} - X \in \mathbf{F}_p[X]$ ist. Da $(L \smallsetminus \{0\}, \cdot)$ eine Gruppe mit $p^k - 1$ Elementen ist, gilt für alle $y \in L \smallsetminus \{0\}$, daß $y^{p^k-1} = 1$; vgl. Aufgabe 11.(1.c). Also ist für alle $y \in L$ die Gleichung $z(y) = y^{p^k} - y = 0$ erfüllt. Abdividieren dieser p^k Nullstellen von $z(X)$ liefert

$$z(X) \;=\; X^{p^k} - X \;=\; \textstyle\prod_{y \in L}(X - y) \;\in\; L[X]\,,$$

da $z(X)$ ein normiertes Polynom von Grad p^k ist; vgl. auch Aufgabe 12.(2). Ferner ist $L = \mathbf{F}_p(y : y \in L)$. Somit ist L in der Tat ein Zerfällungskörper von $z(X) = X^{p^k} - X \in \mathbf{F}_p[X]$. ▫

Bemerkung. Die Abschätzung für den Grad des Zerfällungskörpers aus Satz 4 wird hier deutlich unterschritten, es ist $k = [\mathbf{F}_{p^k} : \mathbf{F}_p] \leqslant \deg(X^{p^k} - X) = p^k$.

Beispiel.

(1) Es ist $\mathbf{F}_4$ der Zerfällungskörper von $X^4 - X \in \mathbf{F}_2[X]$. In der Tat ist $X^4 - X = X(X-1)(X-\alpha)(X-(\alpha+1)) \in \mathbf{F}_4[X]$.

(2) Es ist $\mathbf{F}_8$ der Zerfällungskörper von $X^8 - X \in \mathbf{F}_2[X]$. Vgl. Aufgabe 29.$(5, 4)$. Vgl. auch das Beispiel in §2.5.1, Teil (3).

(3) Es ist $\mathbf{F}_9$ der Zerfällungskörper von $X^9 - X \in \mathbf{F}_3[X]$.

(4) Es ist $\mathbf{F}_p$ der Zerfällungskörper von $X^p - X \in \mathbf{F}_p[X]$. Vgl. auch Aufgaben 12.(2) und Aufgabe 24.(2).

Halten wir nochmals kurz fest:

Korollar. *Zu jeder Primpotenz gibt es bis auf Isomorphie genau einen Körper mit dieser Elementzahl.*

Beachte, daß umgekehrt die Kardinalität eines endlichen Körpers eine Primpotenz ist; vgl. Aufgabe 26.

Kapitel 3

Automorphismen

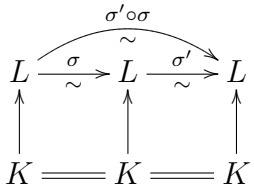
Wir werden die benötigten gruppentheoretischen Begriffe und Aussagen dann einführen, wenn sie gebraucht werden.

3.1 Die Automorphismengruppe einer Erweiterung

Definition. Sei $L|K$ eine Körpererweiterung. Sei

$$\mathrm{Aut}(L|K) \;:=\; \{\sigma : L \xrightarrow{\sim} L \;:\; \sigma|_K^K = \mathrm{id}_K\}$$

die *Automorphismengruppe von* $L|K$. Ihre Elemente heißen *Automorphismen von* $L|K$ (gesprochen: von L über K). Die Multiplikation zweier Elemente $\sigma, \sigma' \in \mathrm{Aut}(L|K)$ ist hierbei durch $\sigma \circ \sigma'$ gegeben.



In der Tat ist $\mathrm{Aut}(L|K)$ damit eine Gruppe. Denn Assoziativität folgt aus der Tatsache, daß Verketten von Abbildungen assoziativ ist. Das Element id_L fungiert als Einselement. Die zu einem $\sigma \in \mathrm{Aut}(L|K)$ inverse Abbildung σ^{-1} ist zum einen wieder in $\mathrm{Aut}(L|K)$, vgl. die erste Bemerkung in §1.4.1, und zum anderen auch das Inverse in dieser Gruppe, da $\sigma \circ \sigma^{-1} = \mathrm{id}_L$ und $\sigma^{-1} \circ \sigma = \mathrm{id}_L$.

3.2 Gruppenmorphismen, Untergruppen, Normalteiler

Seien G und H (multiplikativ geschriebene) Gruppen; vgl. §1.1, Erinnerung (1).

Definition. Ist G endlich, so spricht man von der *Ordnung* $|G|$ der Gruppe G.

Vgl. Aufgabe 11.

Definition. Eine Abbildung $G \xrightarrow{f} H$ heißt *Gruppenmorphismus,* falls $f(gg') = f(g)f(g')$ für alle $g,\, g' \in G$.

Dann ist $f(1_G) = f(1_G) \cdot f(1_G) \cdot f(1_G)^{-1} = f(1_G \cdot 1_G) \cdot f(1_G)^{-1} = f(1_G) \cdot f(1_G)^{-1} = 1_H$.

Für $g \in G$ ist $f(g^{-1}) = f(g^{-1}) \cdot f(g) \cdot f(g)^{-1} = f(g^{-1} \cdot g) \cdot f(g)^{-1} = f(1_G) \cdot f(g)^{-1} = 1_H \cdot f(g)^{-1} = f(g)^{-1}$.

Definition. Ein bijektiver Gruppenmorphismus heißt *Isomorphismus* von Gruppen, oder *Gruppenisomorphismus,* geschrieben $G \xrightarrow{\sim} H$. Zwei Gruppen G und H heißen *isomorph,* wenn es zwischen ihnen einen Isomorphismus gibt, geschrieben $G \simeq H$.

Bemerkung. *Ist* $G \xrightarrow[\sim]{f} H$ *ein Gruppenisomorphismus, so auch* $G \xleftarrow[\sim]{f^{-1}} H$.

Beweis. Es ist zu zeigen, daß f^{-1} ein Gruppenmorphismus ist. Seien $h,\, h' \in H$. Es wird $f^{-1}(h \cdot h') \;=\; f^{-1}(f(f^{-1}(h)) \cdot f(f^{-1}(h'))) \;=\; f^{-1}(f(f^{-1}(h) \cdot f^{-1}(h'))) \;=\; f^{-1}(h) \cdot f^{-1}(h')$. □

Definition. Eine Teilmenge $U \subseteq G$ heißt *Untergruppe,* wenn $1_G \in U$ ist, und wenn für alle $u,\, v \in U$ auch $uv^{-1} \in U$ ist. Wir schreiben diesenfalls $U \leqslant G$.

Bemerkung. Eine Untergruppe U von G ist mit der von G vererbten Multiplikation $(\cdot)|^{U}_{U \times U} : U \times U \longrightarrow U$ wieder eine Gruppe.

Beweis. Zu zeigen ist, daß die Einschränkung $(\cdot)|^{U}_{U \times U}$ existiert. Zunächst ist mit $v \in U$ auch $v^{-1} = 1 \cdot v^{-1} \in U$. Ferner folgt für G allgemein, daß $x^{-1}x = 1 = x^{-1}(x^{-1})^{-1}$, also $x = (x^{-1})^{-1}$. Somit wird für $u,\, v \in U$ auch $uv = u(v^{-1})^{-1} \in U$. □

Bemerkung. *Sei* $G \xrightarrow{f} H$ *ein Gruppenmorphismus. Sei*

$$\operatorname{Im} f \;:=\; f(G) \;=\; \{f(g) \;:\; g \in G\}$$

sein Bild. Es ist $\operatorname{Im} f \leqslant H$. *Ist dazuhin* f *injektiv, so ist* $f|^{\operatorname{Im} f} : G \longrightarrow \operatorname{Im} f$ *ein Isomorphismus.*

Siehe Aufgabe 37.(2, 3).

Bemerkung. *Sei* $g \in G$. *Die Abbildung* $G \xrightarrow{{}^{g}(-)} G,\, x \longmapsto {}^{g}x$ *ist ein Gruppenisomorphismus.*

Beweis. Wegen ${}^{g}(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = {}^{g}x\,{}^{g}y$ für $x,\, y \in G$ liegt ein Gruppenmorphismus vor. Da ${}^{g}(-)$ von ${}^{g^{-1}}(-)$ beidseitig invertiert wird, ist dieser Gruppenmorphismus auch bijektiv. □

Definition. Eine Untergruppe $U \leqslant G$ heißt *Normalteiler* in G, oder *normal* in G, falls

für alle $g \in G$ gilt, daß ${}^gU := gUg^{-1} := \{gug^{-1} \ : \ u \in U\}$ gleich U ist. Wir schreiben diesenfalls $U \trianglelefteq G$.

Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus.

Definition. Sei

$$\operatorname{Kern} f \ := \ \{g \in G \ : \ f(g) = 1_H\}$$

der *Kern* von f.

Bemerkung. *Es ist* $\operatorname{Kern} f \trianglelefteq G$.

Siehe Aufgabe 37.(5).

Bemerkung. *Es ist* $\operatorname{Kern} f = \{1_G\}$ *genau dann, wenn* f *injektiv ist.*

Beweis. Ist f injektiv, und ist $g \in \operatorname{Kern} f$, so folgt aus $f(g) = 1_H = f(1_G)$, daß $g = 1_G$. Also ist $\operatorname{Kern} f = \{1_G\}$.

Sei umgekehrt $\operatorname{Kern} f = \{1_G\}$ vorausgesetzt. Seien $g, g' \in G$ so, daß $f(g) = f(g')$. Dann ist $f(gg'^{-1}) = f(g)f(g')^{-1} = 1_H$, und also $gg'^{-1} = 1_G$, i.e. $g = g'$. ▫

Definition. Sei $U \leqslant G$. Für $g \in G$ sei $gU := \{\, gu \ : \ u \in U \,\} \subseteq U$ die *Linksnebenklasse* von g modulo U. Sei $G/U := \{\, gU \ : \ g \in G \,\}$ die *Linksfaktormenge* von G modulo U.

Für $x \in G$ ist $xU = U$ genau dann, wenn $x \in U$ liegt. Denn diesenfalls ist $xU \supseteq U$, da für $u \in U$ $u = xx^{-1}u \in xU$ liegt, sowie $xU \subseteq U$, da für $u \in U$ auch $xu \in U$ liegt. Vgl. auch Aufgabe 38.

Für $g, h \in G$ ist $gU = hU$ genau dann, wenn $h^{-1}gU = U$ ist, d.h. wenn $h^{-1}g \in U$ liegt.

Definition. Sei $N \trianglelefteq G$. Auf der Linksfaktormenge G/N können wir eine Multiplikation durch $gN \cdot hN := ghN$ definieren, wobei $g, h \in G$.

Denn für $g, \tilde{g}, h, \tilde{h} \in G$ mit $gN = \tilde{g}N$ und $hN = \tilde{h}N$ ist $\tilde{g}^{-1}g, \tilde{h}^{-1}h \in N$. Wir haben $ghN \overset{!}{=} \tilde{g}\tilde{h}N$ zu zeigen, i.e. $\tilde{h}^{-1}\tilde{g}^{-1}gh \overset{!}{\in} N$. Aber $\tilde{h}^{-1}\tilde{g}^{-1}gh = \tilde{h}^{-1}h(h^{-1}\tilde{g}^{-1}gh)$ liegt in N, da mit $\tilde{g}^{-1}g$ wegen $N \trianglelefteq G$ auch $h^{-1}\tilde{g}^{-1}gh$ in N liegt.

Es ist G/N eine Gruppe, da $gN \cdot 1N = gN = 1N \cdot gN$ ist, da $gN \cdot g^{-1}N = 1N = g^{-1}N \cdot gN$ ist und da $(gN \cdot hN) \cdot kN = ghN \cdot kN = ghkN = gN \cdot hkN = gN \cdot (hN \cdot kN)$ ist, wobei $g, h, k \in G$. Es heißt G/N die *Faktorgruppe* von G modulo N.

Wir haben den Gruppenmorphismus $\rho : G \longrightarrow G/N$, $g \longmapsto gN$. Denn es ist $\rho(g) \cdot \rho(h) = gN \cdot hN = ghN = \rho(gh)$ für $g, h \in G$.

Lemma. *Sei* $G \xrightarrow{f} H$ *ein Gruppenmorphismus. Sei* $N \trianglelefteq G$ *mit* $N \leqslant \operatorname{Kern} f$ *gegeben.*

Dann gibt es den Gruppenmorphismus $\bar{f} : G/N \longrightarrow H$, $gN \longmapsto f(g)$.

Es ist $\bar{f}$ *injektiv genau dann, wenn* $N = \operatorname{Kern} f$ *ist. Falls dem so ist, dann ist auch* $\bar{f}|^{\operatorname{Im} f} : G/\operatorname{Kern} f \longrightarrow \operatorname{Im} f$, $g \operatorname{Kern} f \longmapsto f(g)$ *ein Gruppenisomorphismus.*

Beweis. Es ist $\bar{f}$ wohldefiniert, da für $g, \tilde{g} \in G$ aus $gN = \tilde{g}N$ folgt, daß $g^{-1}\tilde{g} \in N \leqslant \operatorname{Kern} f$ liegt, und daraus, daß $f(g)^{-1}f(\tilde{g}) = f(g^{-1}\tilde{g}) = 1$ ist, d.h. $f(\tilde{g}) = f(g)$. Es ist $\bar{f}$ ein Gruppenmorphismus, da $\bar{f}(gN) \cdot \bar{f}(\tilde{g}N) = f(g)f(\tilde{g}) = f(g\tilde{g}) = \bar{f}(g\tilde{g}N) = \bar{f}(gN \cdot \tilde{g}N)$

ist für $g,\, \tilde{g} \in G$.

Es ist Kern $\bar{f} = \{\, gN \,:\, g \in G,\, f(g) = 1_H \,\} = (\text{Kern}\, f)/N$. Also ist $\bar{f}$ injektiv genau dann, wenn Kern $f = N$ ist. Diesenfalls ist $\bar{f}|^{\text{Im}\, f}$ bijektiv und also ein Gruppenisomorphismus.

3.3 Perfekte Körper

Definition. Ein Körper K heißt *perfekt,* falls (i) oder (ii) gilt.

(i) Es ist $\text{char}\, K = 0$.

(ii) Es ist $\text{char}\, K = p > 0$, und für jedes $x \in K$ gibt es ein $y \in K$ mit $y^p = x$.

Die Forderung in (ii) ist äquivalent dazu, zu verlangen, daß Frob_K ein Automorphismus ist; vgl. Aufgabe 24.(1).

Beispiel. Die Körper $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}(T)$ sind perfekt.

Beispiel. Ist K ein endlicher Körper, so ist K perfekt. In der Tat ist dann $\text{char}\, K =: p > 0$, und es ist Frob_K ein Automorphismus von K; vgl. Aufgabe 24.(1).

Beispiel. Sei p prim. Es ist $\mathbf{F}_p(T)$ nicht perfekt. In der Tat ist $\text{Frob}_{\mathbf{F}_p(X)}$ nicht surjektiv; vgl. Aufgabe 24.(1).

Lemma. *Sei K perfekt. Sei $f(X) \in K[X]$ ein normiertes irreduzibles Polynom von Grad $\deg f = n$. Sei $L|K$ so, daß $f(X)$ in $L[X]$ in Linearfaktoren zerfällt. Schreibe*

$$f(X) \;=\; (X - \gamma_1) \cdots (X - \gamma_n) \;\in\; L[X]\,.$$

Dann ist $\gamma_i \neq \gamma_j$ für $i,\, j \in [1, n]$ mit $i \neq j$.

Beweis. Nach Aufgabe 25.(2) genügt es zu zeigen, daß $\text{ggT}(f(X), f'(X)) = 1$, genommen in $L[X]$. Nach Aufgabe 25.(3) genügt es dazu wiederum zu zeigen, daß $\text{ggT}(f(X), f'(X)) = 1$, genommen in $K[X]$. Da $f(X) \in K[X]$ irreduzibel ist, genügt es dafür zu zeigen, daß $f(X)$ kein Teiler von $f'(X)$ ist. Da $\deg f' < \deg f$, genügt es also zu zeigen, daß $f'(X) \neq 0$.

Nehmen wir also *an,* es sei $f'(X) = \sum_{i \geqslant 1} i f_i X^{i-1} = 0$. Dann ist $i f_i = 0$ für alle $i \geqslant 0$. Ist $\text{char}\, K = 0$, so ist dies wegen $\deg f \geqslant 1$ nicht möglich. Ist $\text{char}\, K = p > 0$, so folgt $f_i = 0$ wann immer $i \not\equiv_p 0$, also $f(X) = \sum_{i \geqslant 0} f_{pi} X^{pi}$. Sei $g_i \in K$ mit $g_i^p = f_{pi}$ für $i \geqslant 0$. Anwendung von $\text{Frob}_{K(X)}$ wie in Aufgabe 24.(1) gibt

$$g(X)^p \;=\; (\textstyle\sum_{i \geqslant 0} g_i X^i)^p \;=\; \sum_{i \geqslant 0} g_i^p X^{pi} \;=\; \sum_{i \geqslant 0} f_{pi} X^{pi} \;=\; f(X)\,.$$

Somit ist $f(X)$ reduzibel, und wir haben einen *Widerspruch.* □

In Aufgabe 35 begegneten wir einem irreduziblen Polynom mit mehrfachen Nullstellen in seinem Zerfällungskörper. Um ein konkretes Beispiel zu haben, kann man dort etwa $K = \mathbf{F}_p(T)$ und $a = T$ setzen.

3.4 Die Automorphismengruppe eines Zerfällungskörpers

3.4.1 Theorie

Sei K ein perfekter Körper. Sei $f(X) \in K[X]$ ein Produkt verschiedener normierter irreduzibler Polynome. Sei $L|K$ der Zerfällungskörper von $f(X)$. Wir wollen ein Verfahren zur Berechnung von $\mathrm{Aut}(L|K)$, also der Automorphismengruppe der Zerfällungskörpererweiterung, angeben.

Schreibe

$$f(X) \;=\; (X-\gamma_1)(X-\gamma_2)\cdots(X-\gamma_n) \;\in\; L[X]$$

Bemerkung. *Sind $u(X)$, $v(X) \in K[X]$ normiert und irreduzibel, und gibt es ein $\delta \in L$ mit $u(\delta) = v(\delta) = 0$, so ist $u(X) = v(X)$. Umgekehrt gesprochen, verschiedene normierte irreduzible Polynome in $K[X]$ haben disjunkte Nullstellenmengen in L.*

Beweis. Es ist $u(X) = \mu_{\delta,K}(X) = v(X)$; vgl. erste Bemerkung in §2.3.2. ▫

Bemerkung. *Es ist $\gamma_i \neq \gamma_j$ für alle $i \neq j$ in $[1,n]$.*

Beweis. Sei $\gamma_i = \gamma_j$, aber $i \neq j$ *angenommen.* Schreibe $f(X) = g^{(1)}(X)\cdots g^{(b)}(X)$ mit $g^{(a)}(X) \in K[X]$ normiert und irreduzibel. Nach Voraussetzung ist $g^{(a)}(X) \neq g^{(a')}(X)$ für $a \neq a'$. Da nun $(X-\gamma_i)(X-\gamma_j) = (X-\gamma_i)^2$ ein Teiler von $f(X)$ in $L[X]$ ist, und da mit vorangegangener Bemerkung die Nullstellenmengen in L verschiedener irreduzibler Polynome aus $K[X]$ disjunkt sind, gibt es ein $a \in [1,b]$, für welches $g^{(a)}(X)$ in $L[X]$ von $(X-\gamma_i)^2$ geteilt wird. Dies ist aber mit dem Lemma in §3.3 wegen K perfekt nicht möglich, und wir haben einen *Widerspruch.* ▫

Um ein einigermaßen effizientes Verfahren zu bekommen, numerieren wir die Nullstellen von $f(X)$ in L wie folgt um.

Sei $\deg \mu_{\gamma_1,K}$ maximal unter den $\deg \mu_{\gamma_s,K}$ mit $s \in [1,n]$.

Sei $\deg \mu_{\gamma_2,K(\gamma_1)}$ maximal unter den $\deg \mu_{\gamma_s,K(\gamma_1)}$ mit $s \in [2,n]$.

Sei $\deg \mu_{\gamma_3,K(\gamma_1,\gamma_2)}$ maximal unter den $\deg \mu_{\gamma_s,K(\gamma_1,\gamma_2)}$ mit $s \in [3,n]$.

Usf. Dies wird etwa dadurch erreicht, daß bei der Bestimmung des Zerfällungskörper in jedem Schritt von den noch zu behandelnden irreduziblen Faktoren derjenige größten Grades als Minimalpolynom für die anstehende Körpererweiterung ausgewählt wird.

Sei ferner $m \in [1,n]$ minimal so, daß $K(\gamma_1,\ldots,\gamma_m) = K(\gamma_1,\ldots,\gamma_n)$.

Schreibe $\Gamma := \{\gamma_1,\ldots,\gamma_n\} \subseteq L$ für die Menge der Nullstellen von $f(X)$ in L.

Ist $\sigma \in \mathrm{Aut}(L|K)$, und ist $s \in [1,n]$, so ist

$$\begin{aligned} f(\sigma(\gamma_s)) &= \textstyle\sum_{i\geqslant 0} f_i \sigma(\gamma_s)^i \\ &= \sigma(\textstyle\sum_{i\geqslant 0} f_i \gamma_s^i) \\ &= \sigma(f(\gamma_s)) \\ &= \sigma(0) \\ &= 0\ ; \end{aligned}$$

vgl. auch die erste Bemerkung in §2.3.4. Folglich ist $\sigma|_\Gamma^\Gamma$ definiert, injektiv, und damit wegen Γ endlich auch surjektiv.

Setze $\sigma(\gamma_s) =: \gamma_{\bar\sigma(s)}$ für $s \in [1,n]$. Da $\sigma|_\Gamma^\Gamma$ bijektiv ist, und da $\gamma_i \neq \gamma_j$ für alle $i \neq j$ in $[1,n]$, definiert dies ein Element $\bar\sigma \in \mathcal{S}_n$, i.e. eine Bijektion von $[1,n]$ in sich.

Ist also z.B. $n=3$, $\sigma(\gamma_1)=\gamma_3$, $\sigma(\gamma_2)=\gamma_1$ und $\sigma(\gamma_3)=\gamma_2$, so ist $\bar\sigma = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)$.

> Man gewinnt $\bar\sigma$ also, indem man sich von der Operation von σ auf den $\gamma_s \in \Gamma$ "nur die Indizes notiert".

Bemerkung. *Sei $E(\delta_1,\dots,\delta_k)|E$ eine endliche polygene Körpererweiterung. Sei F ein weiterer Körper, und seien*

$$\rho,\ \tilde\rho\ :\ E(\delta_1,\dots,\delta_k) \longrightarrow F$$

Körpermorphismen. Ist $\rho|_{\{\delta_1,\dots,\delta_k\}} = \tilde\rho|_{\{\delta_1,\dots,\delta_n\}}$, so ist $\rho = \tilde\rho$.

Beweis. Jedes Element von $E(\delta_1,\dots,\delta_k)$ ist von der Form $\sum_{i_1,\dots,i_k\geqslant 0} e_{i_1,\dots,i_k}\delta_1^{i_1}\cdots\delta_k^{i_k}$ mit gewissen $e_{i_1,\dots,i_k} \in E$. Es wird

$$\begin{aligned} & \rho\big(\textstyle\sum_{i_1,\dots,i_k\geqslant 0} e_{i_1,\dots,i_k}\delta_1^{i_1}\cdots\delta_k^{i_k}\big) \\ = \ & \textstyle\sum_{i_1,\dots,i_k\geqslant 0} e_{i_1,\dots,i_k}\rho(\delta_1)^{i_1}\cdots\rho(\delta_k)^{i_k} \\ = \ & \textstyle\sum_{i_1,\dots,i_k\geqslant 0} e_{i_1,\dots,i_k}\tilde\rho(\delta_1)^{i_1}\cdots\tilde\rho(\delta_k)^{i_k} \\ = \ & \tilde\rho\big(\textstyle\sum_{i_1,\dots,i_k\geqslant 0} e_{i_1,\dots,i_k}\delta_1^{i_1}\cdots\delta_k^{i_k}\big)\ . \end{aligned}$$

□

Lemma. *Es ist*

$$\begin{aligned} \mathrm{Aut}(L|K) &\longrightarrow \mathcal{S}_n \\ \sigma &\longmapsto \bar\sigma \end{aligned}$$

ein injektiver Gruppenmorphismus, und damit ein Isomorphismus auf sein Bild.

Beweis. Zeigen wir, daß ein Gruppenmorphismus vorliegt. Seien $\sigma,\ \sigma' \in \mathrm{Aut}(L|K)$. Für $s \in [1,n]$ ist

$$\gamma_{\overline{\sigma\circ\sigma'}(s)} \ = \ (\sigma\circ\sigma')(\gamma_s) \ = \ \sigma(\gamma_{\bar\sigma'(s)}) \ = \ \gamma_{(\bar\sigma\circ\bar\sigma')(s)}\ .$$

Also ist $\overline{\sigma\circ\sigma'} = \bar\sigma\circ\bar\sigma'$.

Zeigen wir, daß dieser Gruppenmorphismus injektiv ist. Mit der Bemerkung aus §3.2 ist zu zeigen, daß aus $\bar\sigma = \mathrm{id}_{[1,n]}$ folgt, daß $\sigma = \mathrm{id}_L$. Ist aber $\bar\sigma = \mathrm{id}_{[1,n]}$, so ist $\sigma|_\Gamma^\Gamma = \mathrm{id}_\Gamma$, und

also $\sigma|_\Gamma = \mathrm{id}_L|_\Gamma$. Mit vorstehender Bemerkung folgt nun wegen $L = K(\gamma_1, \ldots, \gamma_n)$, daß $\sigma = \mathrm{id}_L$. ▫

Unter dem *Berechnen* der Gruppe $\mathrm{Aut}(L|K)$ werden wir das Berechnen ihres isomorphen Bildes in $\mathcal{S}_n$ bezüglich unserer gewählten Numerierung der Nullstellen von $f(X)$ in L verstehen.

Konstruktion. Die Existenz der nun folgenden Isomorphismen σ_i für $i \in [1, k]$ ist jeweils durch Satz 3 (Nullstelle induziert Morphismus) gesichert.

Sei $K \xrightarrow[\sim]{\sigma_0} K$ die Identität.

1. Schritt. Sei γ_1' eine Nullstelle von $\mu_{\gamma_1,K}^{\sigma_0}(X)$ $(= \mu_{\gamma_1,K}(X))$.

Sei $K(\gamma_1) \xrightarrow[\sim]{\sigma_1} K(\gamma_1')$, $\gamma_1 \longmapsto \gamma_1'$, allgemeiner $g(\gamma_1) \longmapsto g^{\sigma_0}(\gamma_1')$ $(= g(\gamma_1'))$ für $g(X) \in K[X]$.

2. Schritt. Sei γ_2' eine Nullstelle von $\mu_{\gamma_2,K(\gamma_1)}^{\sigma_1}(X)$.

Sei $K(\gamma_1, \gamma_2) \xrightarrow[\sim]{\sigma_2} K(\gamma_1', \gamma_2')$, $\gamma_2 \longmapsto \gamma_2'$, allgemeiner $g(\gamma_2) \longmapsto g^{\sigma_1}(\gamma_2')$ für $g(X) \in K(\gamma_1)[X]$.

3. Schritt. Sei γ_3' eine Nullstelle von $\mu_{\gamma_3,K(\gamma_1,\gamma_2)}^{\sigma_2}(X)$.

Sei $K(\gamma_1, \gamma_2, \gamma_3) \xrightarrow[\sim]{\sigma_2} K(\gamma_1', \gamma_2', \gamma_3')$, $\gamma_3 \longmapsto \gamma_3'$, allgemeiner $g(\gamma_3) \longmapsto g^{\sigma_2}(\gamma_3')$ für $g(X) \in K(\gamma_1, \gamma_2)[X]$.

Usf. bis zum m-ten Schritt. Es ist dann $L = K(\gamma_1, \ldots, \gamma_m) \xrightarrow[\sim]{\sigma_m} K(\gamma_1', \ldots, \gamma_m') = L$ in $\mathrm{Aut}(L|K)$ mit $\sigma_m(\gamma_s) = \gamma_s'$ für alle $s \in [1, m]$. In der Tat haben wir folgendes kommutatives Diagramm.

$$\begin{array}{ccc}
L = K(\gamma_1, \ldots, \gamma_m) & \xrightarrow[\sim]{\sigma_m} & K(\gamma_1', \ldots, \gamma_m') \\
\uparrow & & \uparrow \\
\vdots & & \vdots \\
\uparrow & & \uparrow \\
K(\gamma_1, \gamma_2, \gamma_3) & \xrightarrow[\sim]{\sigma_3} & K(\gamma_1', \gamma_2', \gamma_3') \\
\uparrow & & \uparrow \\
K(\gamma_1, \gamma_2) & \xrightarrow[\sim]{\sigma_2} & K(\gamma_1', \gamma_2') \\
\uparrow & & \uparrow \\
K(\gamma_1) & \xrightarrow[\sim]{\sigma_1} & K(\gamma_1') \\
\uparrow & & \uparrow \\
K & \xrightarrow[\sim]{\sigma_0 = \mathrm{id}_K} & K
\end{array}$$

Insbesondere ist σ_m ein K-linearer Isomorphismus, also $[K(\gamma_1, \ldots, \gamma_m) : K] = [K(\gamma_1', \ldots, \gamma_m') : K]$. Da $K(\gamma_1', \ldots, \gamma_m') \subseteq L = K(\gamma_1, \ldots, \gamma_m)$, folgt $L = K(\gamma_1', \ldots, \gamma_m')$.

Ende der Konstruktion.

Ein aus dieser Konstruktion gewinnbares Tupel $(\gamma_1', \gamma_2', \ldots, \gamma_m')$ heiße *zulässig.* Sei Z die Menge der zulässigen Tupel.

Da, wie oben allgemein angemerkt, $\sigma_m(\Gamma) = \Gamma$, folgt insbesondere, daß die Einträge eines zulässigen Tupels alle in Γ liegen, d.h. Nullstellen von $f(X)$ in L sind.

Satz 6 (Automorphismen durch zulässige Tupel)

Wir haben eine bijektive Abbildung

$$\begin{array}{rcl} \mathrm{Aut}(L|K) & \xrightarrow[\sim]{\Phi} & Z \\ \sigma & \longmapsto & (\sigma(\gamma_1), \ldots, \sigma(\gamma_m)) \; . \end{array}$$

Beweis. Zeigen wir zunächst, daß eine wohldefinierte Abbildung vorliegt, d.h. daß $(\sigma(\gamma_1), \ldots, \sigma(\gamma_m))$ in der Tat zulässig ist.

Wir *behaupten,* daß es eine Konstruktion gibt mit $\sigma_s(\gamma_i) = \gamma_i' = \sigma(\gamma_i)$ für alle $s \in [1, m]$ und alle $i \in [1, s]$.

Um eine solche Konstruktion durchzuführen, verwenden wir eine Induktion nach den Schritten $s \in [1, m]$. Es ist $\sigma_0 = \mathrm{id}_K$.

Seien nun die Schritte 1 bis $s-1$ bereits so durchgeführt, daß $\sigma_{s-1}(\gamma_i) = \gamma_i' = \sigma(\gamma_i)$ für alle $i \in [1, s-1]$. Mit obiger Bemerkung ist dann insbesondere $\sigma_{s-1} = \sigma|_{K(\gamma_1, \ldots, \gamma_{s-1})}^{K(\gamma_1', \ldots, \gamma_{s-1}')}$.

Schreibe $u(X) = \sum_{i \geqslant 0} u_j X^j := \mu_{\gamma_s, K(\gamma_1, \ldots, \gamma_{s-1})}(X) \in K(\gamma_1, \ldots, \gamma_{s-1})[X]$. Nun ist

$$\begin{array}{rcl} \mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1, \ldots, \gamma_{s-1})}(\sigma(\gamma_s)) & = & \sum_{j \geqslant 0} \sigma_{s-1}(u_j) \sigma(\gamma_s)^j \\ & = & \sum_{j \geqslant 0} \sigma(u_j) \sigma(\gamma_s)^j \\ & = & \sigma(\sum_{j \geqslant 0} u_j \gamma_s^j) \\ & = & \sigma(u(\gamma_s)) \\ & = & \sigma(\mu_{\gamma_s, K(\gamma_1, \ldots, \gamma_{s-1})}(\gamma_s)) \\ & = & \sigma(0) \\ & = & 0 \; . \end{array}$$

Somit dürfen wir $\sigma_s(\gamma_s) = \gamma_s' := \sigma(\gamma_s)$ wählen. Für $i \in [1, s-1]$ ist ferner $\sigma_s(\gamma_i) = \sigma_{s-1}(\gamma_i) = \gamma_i' = \sigma(\gamma_i)$. Dies zeigt die *Behauptung* und also, daß $(\sigma(\gamma_1), \ldots, \sigma(\gamma_s))$ in der Tat ein zulässiges Tupel ist.

Zeigen wir die Injektivität von Φ. Sind $\sigma, \tilde{\sigma} \in \mathrm{Aut}(L|K)$ mit $(\sigma(\gamma_1), \ldots, \sigma(\gamma_m)) = (\tilde{\sigma}(\gamma_1), \ldots, \tilde{\sigma}(\gamma_m))$ gegeben, so können wir wegen $L = K(\gamma_1, \ldots, \gamma_m)$ mit obiger Bemerkung folgern, daß $\sigma = \tilde{\sigma}$.

Zeigen wir die Surjektivität von Φ. Sei $(\gamma_1', \ldots, \gamma_m')$ ein zulässiges Tupel. Sei σ_m der aus der Konstruktion resultierende Automorphismus von $L|K$. Dann ist $(\gamma_1', \ldots, \gamma_s') = (\sigma_m(\gamma_1), \ldots, \sigma_m(\gamma_s))$. ▫

Bemerkung. Um $\mathrm{Aut}(L|K)$ also als Teilmenge von $\mathcal{S}_n$ zu berechnen, muß die Menge aller zulässigen Tupel ausgerechnet werden. Sodann muß für jedes zulässige Tupel die

Einschränkung des jeweilig via Φ^{-1} zugehörigen σ_m auf Γ berechnet werden, und aus dieser Einschränkung dann $\bar{\sigma}_m \in \mathcal{S}_n$ abgelesen werden.

Um die Permutation $\sigma_m|_\Gamma^\Gamma$ der Nullstellen zu bestimmen, ist es günstig, die Elemente γ_i' für alle $i \in [1,m]$ als Elemente von $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ zu kennen. Dazu muß im s-ten Schritt die Nullstellenmenge von $\mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})}(X)$ als Teilmenge von Γ bestimmt werden, was mit Faktorisieren dieses Polynoms in Magma erreicht werden kann. Somit kennt man $\sigma_m(\gamma_s) = \gamma_s'$ für alle $s \in [1,m]$. Um die noch fehlenden Elemente $\sigma_m(\gamma_t)$ für $t \in [m+1,n]$ zu bestimmen, ist es günstig, diese Elemente γ_t als polynomiale Ausdrücke in $\gamma_1, \ldots, \gamma_s$ zu kennen – dies resultiert aber bereits aus unserer Konstruktion des Zerfällungskörpers via Magma; cf. Aufgaben 30, 34.

Bemerkung. *Die Anzahl der zulässigen Tupel $|Z|$ ist gleich $[L:K]$.*

Beweis. Gehen wir in obige Konstruktion. Sei $s \in [1,m]$. Wir *behaupten,* daß $\mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})}(X)$ ein Teiler von $f(X)$ in $L[X]$ ist. Da $f(\gamma_s) = 0$, ist $f(X) = \mu_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})}(X)h(X)$ für ein $h(X) \in K(\gamma_1,\ldots,\gamma_{s-1})[X]$; vgl. Satz 2.(2), §2.3.2. Beachte, daß $f(X) \in K[X]$ und $\sigma_{s-1}|_K^K = \mathrm{id}_K$ impliziert, daß $f^{\sigma_{s-1}}(X) = f(X)$. Also erhalten wir in der Tat eine Faktorisierung

$$f(X) \;=\; f^{\sigma_{s-1}}(X) \;=\; \mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})}(X)\, h^{\sigma_{s-1}}(X)$$

in $L[X]$. Dies zeigt die *Behauptung.*

Da $f(X)$ in $L[X]$ in verschiedene Linearfaktoren zerfällt, zeigt die Behauptung nun, daß dies auch für $\mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})}(X)$ zutrifft. Somit haben wir im s-ten Schritt der Konstruktion

$$\deg \mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})} \;=\; \deg \mu_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})} \;=\; [K(\gamma_1,\ldots,\gamma_{s-1},\gamma_s) : K(\gamma_1,\ldots,\gamma_{s-1})]$$

Wahlmöglichkeiten für γ_s' als Nullstelle von $\mu^{\sigma_{s-1}}_{\gamma_s, K(\gamma_1,\ldots,\gamma_{s-1})}(X)$ in L. Es existieren mithin

$$[K(\gamma_1,\ldots,\gamma_m) : K(\gamma_1,\ldots,\gamma_{m-1})][K(\gamma_1,\ldots,\gamma_{m-1}) : K(\gamma_1,\ldots,\gamma_{m-2})] \cdots [K(\gamma_1) : K] \;=\; [L:K]$$

zulässige Tupel. □

Diese Bemerkung zeigt zusammen mit Satz 6 die

Folgerung. *Es ist* $|\mathrm{Aut}(L|K)| = [L:K]$.

Zusammen mit obigem Lemma betreffs $\mathrm{Aut}(L|K) \hookrightarrow \mathcal{S}_n$ zeigt dies wiederum die

Folgerung. *Es ist* $\mathrm{Aut}(L|K) \simeq \mathcal{S}_n$ *genau dann, wenn* $[L:K] = n!$.

Schließlich greifen wir der Terminologie insofern noch ein wenig vor, als daß der Begriff der *Galoiserweiterung* noch nicht fiel; cf. §3.5.1.4 unten. Nichtsdestoweniger:

Definition. Es heißt

$$\mathrm{Gal}(f(X)) \;=\; \mathrm{Gal}(L|K) \;:=\; \mathrm{Aut}(L|K)$$

die *Galoisgruppe* von $f(X) \in K[X]$, oder auch von L über K.

Verwendet man die Notation $\mathrm{Gal}(f(X))$, so darf man den Grundkörper K nicht vergessen, aus welchem $f(X) \in K[X]$ seine Koeffizienten hat.

In diesem Fall wird die Automorphismengruppe also alternativ auch nach ihrem Entdecker, Evariste Galois (1811-1832), benannt. Schon allein der Begriff der *Gruppe* stammt von Galois!

3.4.2 Praxis

3.4.2.1 Ein kleines Beispiel, $X^3 + X + 1 \in \mathbf{Q}[X]$

Sei $f(X) = X^3+X+1 \in \mathbf{Q}[X]$. In Aufgabe 34.(1) wurde der Zerfällungskörper $L = \mathbf{Q}(a, b)$ konstruiert, mit

$$\begin{array}{rcl} \mu_{a,\mathbf{Q}}(X) & = & X^3 + X + 1 \\ \mu_{b,\mathbf{Q}(a)}(X) & = & X^2 + aX + (a^2 + 1) \ . \end{array}$$

Es zerfiel

$$X^3 + X + 1 \ = \ (X - a)(X - b)(X + a + b) \ \in \ \mathbf{Q}(a, b)[X] \ .$$

Ferner war $[\mathbf{Q}(a, b) : \mathbf{Q}] = 6$. ([1]).

Sei

$$\begin{array}{rcl} \gamma_1 & := & a \\ \gamma_2 & := & b \\ \gamma_3 & := & -a - b \ \ ([2]) \ . \end{array}$$

Wir wollen ein isomorphes Bild $\mathrm{Gal}(X^3 + X + 1) = \mathrm{Gal}(\mathbf{Q}(a, b)|\mathbf{Q})$ als Untergruppe von $\mathcal{S}_3$ konstruieren.

Da $|\mathrm{Gal}(\mathbf{Q}(a, b)|\mathbf{Q})| = [\mathbf{Q}(a, b) : \mathbf{Q}] = 6$, und da auch $|\mathcal{S}_3| = 6$, ist das Ergebnis von vorneherein klar – es ist dieses gesuchte Bild gleich $\mathcal{S}_3$; vgl. die beiden Folgerungen in §3.4.1. Da wir das Verfahren illustrieren wollen, machen wir von dieser Überlegung keinen Gebrauch.

Es ist $m = 2$ und $n = 3$. Bestimmen wir die Menge Z der zulässigen Tupel, sowie das vom jeweils zugehörigen Automorphismus σ_2 gelieferte Element $\bar{\sigma}_2$ der $\mathcal{S}_3$, und somit insgesamt das Bild von $\mathrm{Gal}(X^3 + X + 1) = \mathrm{Gal}(\mathbf{Q}(a, b)|\mathbf{Q})$ in $\mathcal{S}_3$.

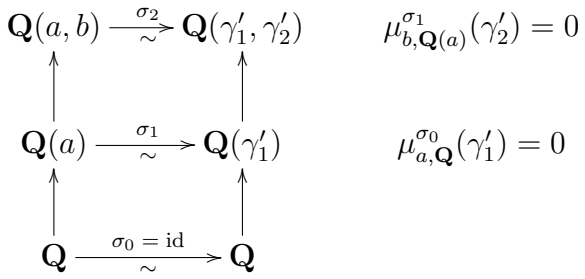
---

[1] Hierzu verwandten wir Magma wie folgt.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^3 + X + 1);
KK<a> := ext<Q | X^3 + X + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^3 + XX + 1);
KKK<b> := ext<KK | XX^2 + a*XX + a^2 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^3 + XXX + 1);
```

[2] In Magma entsprechend:

```
ga1 := a;
ga2 := b;
ga3 := -a-b;
```



Im folgenden Prozedere verstehen wir unter Nullstellen stets Nullstellen in $\mathbf{Q}(a,b)$.

Die Nullstellen von

$$\mu_{a,\mathbf{Q}}(X) \;=\; X^3+X+1$$

sind γ_1, γ_2 und γ_3 ([3]). Unter diesen haben wir ein γ_1' auszuwählen.

Fall $\gamma_1'=\gamma_1$. Es ist $\sigma_1(a)=\gamma_1$ (also $\sigma_1=\mathrm{id}_{\mathbf{Q}(a)}$). Insbesondere ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^2+\gamma_1 X+(\gamma_1^2+1)\;,$$

welches die Nullstellen γ_2 und γ_3 hat ([4]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2'=\gamma_2$. Es ist $\sigma_2(b)=\gamma_2$ (also $\sigma_2=\mathrm{id}_{\mathbf{Q}(a,b)}$). Somit ist (γ_1,γ_2) ein zulässiges Tupel. Ferner ist

$$\sigma_2(\gamma_3) \;=\; \sigma_2(-a-b) \;=\; -\sigma_2(a)-\sigma_2(b) \;=\; -\gamma_1-\gamma_2 \;=\; -a-b \;=\; \gamma_3 \;\;([5])\;.$$

Da also $\sigma_2(\gamma_1)=\gamma_1$, $\sigma_2(\gamma_2)=\gamma_2$ und $\sigma_2(\gamma_3)=\gamma_3$, folgt $\bar\sigma_2=\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right)$.

Subfall $\gamma_2'=\gamma_3$. Es ist $\sigma_2(b)=\gamma_3$. Somit ist (γ_1,γ_3) ein zulässiges Tupel. Ferner ist

$$\sigma_2(\gamma_3) \;=\; \sigma_2(-a-b) \;=\; -\sigma_2(a)-\sigma_2(b) \;=\; -\gamma_1-\gamma_3 \;=\; b \;=\; \gamma_2\;.$$

Da also $\sigma_2(\gamma_1)=\gamma_1$, $\sigma_2(\gamma_2)=\gamma_3$ und $\sigma_2(\gamma_3)=\gamma_2$, folgt $\bar\sigma_2=\left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)$.

Fall $\gamma_1'=\gamma_2$. Es ist $\sigma_1(a)=\gamma_2$. Insbesondere ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^2+\gamma_2 X+(\gamma_2^2+1)\;,$$

welches die Nullstellen γ_1 und γ_3 hat ([6]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2'=\gamma_1$. Es ist $\sigma_2(b)=\gamma_1$. Somit ist (γ_2,γ_1) ein zulässiges Tupel. Ferner ist

$$\sigma_2(\gamma_3) \;=\; \sigma_2(-a-b) \;=\; -\sigma_2(a)-\sigma_2(b) \;=\; -\gamma_2-\gamma_1 \;=\; -b-a \;=\; \gamma_3\;.$$

[3] `Factorisation(XXX^3 + XXX + 1);`

[4] `Factorisation(XXX^2 + ga1*XXX + (ga1^2 + 1));`

[5] Eine andere Möglichkeit besteht wegen $\sigma_2(\gamma_3)\in\Gamma$ nun auch nicht mehr. Dennoch ist diese Rechnung eine gute Probe.

[6] `Factorisation(XXX^2 + ga2*XXX + (ga2^2 + 1));`

Da also $\sigma_2(\gamma_1) = \gamma_2$, $\sigma_2(\gamma_2) = \gamma_1$ und $\sigma_2(\gamma_3) = \gamma_3$, folgt $\bar{\sigma}_2 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$.

Subfall $\gamma_2' = \gamma_3$. Es ist $\sigma_2(b) = \gamma_3 = -a - b$. Somit ist (γ_2, γ_3) ein zulässiges Tupel. Ferner ist

$$\sigma_2(\gamma_3) \;=\; \sigma_2(-a-b) \;=\; -\sigma_2(a) - \sigma_2(b) \;=\; -\gamma_2 - \gamma_3 \;=\; a \;=\; \gamma_1 \;.$$

Da also $\sigma_2(\gamma_1) = \gamma_2$, $\sigma_2(\gamma_2) = \gamma_3$ und $\sigma_2(\gamma_3) = \gamma_1$, folgt $\bar{\sigma}_2 = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$.

Fall $\gamma_1' = \gamma_3$. Es ist $\sigma_1(a) = \gamma_3$. Insbesondere ist

$$\mu_{b,\mathbf{Q}(a)}^{\sigma_1}(X) \;=\; X^2 + \gamma_3 X + (\gamma_3^2 + 1) \;,$$

welches die Nullstellen γ_1 und γ_2 hat ([7]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_1$. Es ist $\sigma_2(b) = \gamma_1$. Somit ist (γ_3, γ_1) ein zulässiges Tupel. Ferner ist

$$\sigma_2(\gamma_3) \;=\; \sigma_2(-a-b) \;=\; -\sigma_2(a) - \sigma_2(b) \;=\; -\gamma_3 - \gamma_1 \;=\; b \;=\; \gamma_2 \;.$$

Da also $\sigma_2(\gamma_1) = \gamma_3$, $\sigma_2(\gamma_2) = \gamma_1$ und $\sigma_2(\gamma_3) = \gamma_2$, folgt $\bar{\sigma}_2 = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)$.

Subfall $\gamma_2' = \gamma_2$. Es ist $\sigma_2(b) = \gamma_2$. Somit ist (γ_3, γ_2) ein zulässiges Tupel. Ferner ist

$$\sigma_2(\gamma_3) \;=\; \sigma_2(-a-b) \;=\; -\sigma_2(a) - \sigma_2(b) \;=\; -\gamma_3 - \gamma_2 \;=\; a \;=\; \gamma_1 \;.$$

Da also $\sigma_2(\gamma_1) = \gamma_3$, $\sigma_2(\gamma_2) = \gamma_2$ und $\sigma_2(\gamma_3) = \gamma_1$, folgt $\bar{\sigma}_2 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$.

Als Ergebnis erhalten wir

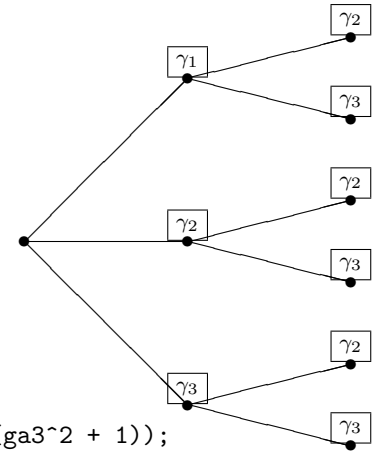
$$Z \;=\; \{(\gamma_1,\gamma_2),\, (\gamma_1,\gamma_3),\, (\gamma_2,\gamma_1),\, (\gamma_2,\gamma_3),\, (\gamma_3,\gamma_1),\, (\gamma_3,\gamma_2)\} \;,$$

und das isomorphe Bild von $\mathrm{Gal}(\mathbf{Q}(a,b)|\mathbf{Q})$ in $\mathcal{S}_3$ zu

$$\left\{\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right),\, \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)\right\} \;=\; \mathcal{S}_3 \;.$$

Kurz, es ist hier $\mathrm{Gal}(X^3 + X + 1) = \mathrm{Gal}(\mathbf{Q}(a,b)|\mathbf{Q}) = \mathrm{Aut}(\mathbf{Q}(a,b)|\mathbf{Q}) = \mathcal{S}_3$.

Man sieht also, es ist ein ganzer Baum von Fällen, Subfällen etc. abzuarbeiten.



[7] `Factorisation(XXX^2 + ga3*XXX + (ga3^2 + 1));`

In Magma gibt es:

```
G := GaloisGroup(X^3 + X + 1);
{u : u in G};
Order(G);
```

Vorsicht ist hier im allgemeinen aber deswegen geboten, weil die von Magma gewählte Numerierung mit der unsrigen nicht übereinstimmen muß.

Im Regelfall ist in der Tat $\mathrm{Gal}(L|K) = \mathcal{S}_n$. Aber nicht immer!

3.4.2.2 Zykelschreibweise in der symmetrischen Gruppe

Sei $n \geqslant 1$. Es bezeichne ein Zykel

$$(s_1, \ldots, s_k)$$

der *Länge* $k \geqslant 1$, mit $s_i \in [1,n]$ und $s_i \neq s_j$ für $i,\ j \in [1,k]$ mit $i \neq j$, das Element in $\mathcal{S}_n$, welches s_i auf s_{i+1} schickt für $i \in [1,k-1]$ und s_k auf s_1, und welches die Elemente aus $[1,n] \smallsetminus \{s_1, \ldots, s_k\}$ festläßt.

Bei Komposition *disjunkter* Zykeln, d.h. solchen, die keinen Eintrag gemeinsam haben, läßt man das Zeichen $(\circ)$ für Verkettung auch weg. Die Reihenfolge der Verkettung spielt bei Disjunktheit keine Rolle.

Unter der *Zykelschreibweise* eines Elements $\sigma \in \mathcal{S}_n$ verstehen wir eine Zerlegung von σ in ein disjunktes Produkt von Zyklen.

Für die Identität $\mathrm{id} = \mathrm{id}_{[1,n]}$ existiere hierbei keine Zykelschreibweise.

Z.B. ist

$$\left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&1&9&4&8&6&7&5&2 \end{smallmatrix}\right) \ = \ (1,3,9,2)(5,8) \ \in \ \mathcal{S}_9 \ .$$

Oder aber z.B.

$$\mathcal{S}_3 \ = \ \{\mathrm{id},\ (1,2),\ (1,3),\ (2,3),\ (1,2,3),\ (1,3,2)\} \ .$$

Schließlich ist z.B.

$$(1,3,4,5) \circ (2,4,3)(1,6) \ = \ (1,6,3,2,5) \ \in \ \mathcal{S}_7 \ .$$

3.4.2.3 Eine Abkürzung

3.4.2.3.1 Untergruppenerzeugnis

Sei G eine endliche Gruppe. Sei $n \geqslant 1$, und seien $g_1, \ldots, g_n \in G$. Sei $\langle g_1, \ldots, g_n \rangle$ der Schnitt aller Untergruppen, die alle Elemente $g_1, \ldots, g_n$ enthalten, also

$$\langle g_1, \ldots, g_n \rangle \ := \ \bigcap_{\substack{V \leqslant G \\ g_1, \ldots, g_n \in G}} V \ .$$

Dies ist wieder eine Untergruppe von G, genannt das *(Untergruppen-)Erzeugnis* der Elemente $g_1, \ldots, g_n$.

Es berechnet sich als Teilmenge U in G bestehend aus sämtlichen Produkten der Elemente $g_1, \ldots, g_n$ in beliebiger Reihenfolge. Es ist U unter Inversion abgeschlossen, da für $x \in U$ auch $x^{-1} = x^{\mathrm{o}(x)-1} \in U$ liegt; vgl. Aufgabe 11. Es enthält U das Element 1_G als leeres Produkt. Es enthält U mit zwei Elementen auch das Produkt des ersten mit dem Inversen des zweiten. Somit ist dies eine Untergruppe von G, die $g_1, \ldots, g_n$ enthält. Also ist

$$\langle g_1, \ldots, g_n \rangle \leqslant U \ .$$

Ferner ist U in allen Untergruppen enthalten, die $g_1, \ldots, g_n$ enthalten. Also ist

$$U \leqslant \langle g_1, \ldots, g_n \rangle \ .$$

Insgesamt ist folglich

$$U = \langle g_1, \ldots, g_n \rangle \ .$$

Den Fall $n = 1$ haben wir in Aufgabe 11.(1) besprochen. Dort haben wir auch festgestellt, daß $|\langle g_1 \rangle| = \mathrm{o}(g_1)$.

3.4.2.3.2 Untergruppenerzeugnis via Magma

Mittels Magma berechnet sich das Untergruppenerzeugnis wie folgt.

Berechnen wir z.B. $\langle (1,2,3),\, (1,2) \rangle \leqslant \mathcal{S}_3$.

```
U := sub< SymmetricGroup(3) | (1,2,3), (1,2) >;
Order(U);
{u : u in U};
```

Wir erhalten $|\langle (1,2,3),\, (1,2) \rangle| = 6$, also $\langle (1,2,3),\, (1,2) \rangle = \mathcal{S}_3$. Ferner wird eine Liste der Elemente ausgegeben.

Berechnen wir z.B. $\langle (1,2)(3,4),\, (1,3) \rangle \leqslant \mathcal{S}_4$.

```
U := sub< SymmetricGroup(4) | (1,2)(3,4), (1,3) >;
Order(U);
{u : u in U};
```

Wir erhalten $|\langle (1,2)(3,4),\, (1,3) \rangle| = 8$, genauer

$$\begin{aligned} &\langle (1,2)(3,4), (1,3) \rangle \ = \\ &\{\mathrm{id},\ (1,2)(3,4),\ (1,2,3,4),\ (2,4),\ (1,3),\ (1,4,3,2),\ (1,4)(2,3),\ (1,3)(2,4)\} \ . \end{aligned}$$

Es ist nun das Bild von $\mathrm{Aut}(L|K)$ in $\mathcal{S}_n$ eine Untergruppe. Unser Prozedere berechnete nun nacheinander Elemente dieses Bildes, bis alle Elemente gefunden waren. Berechnen wir in jedem Schritt das Erzeugnis der bereits gefundenen Elemente, so können wir bereits dann abbrechen, wenn die Ordnung dieses Erzeugnisses gleich der Ordnung $[L : K]$ des Bildes ist. Denn da das gesuchte Bild dieses Erzeugnis enthält, tritt dann Gleichheit ein.

3.4.2.3.3 Diskussion des kleinen Beispiels aus §3.4.2.1

Gehen wir das Prozedere in §3.4.2.1 diesbezüglich durch. Es soll eine Untergruppe von $\mathcal{S}_3$ der Ordnung $[\mathbf{Q}(a,b):\mathbf{Q}]=6$ erreicht werden.

Im ersten Subfall erhielten wir das Element $\left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right)=\mathrm{id}$ in unserer gesuchten Untergruppe von $\mathcal{S}_3$. Es ist $|\langle\mathrm{id}\rangle|=1<6$, wir haben also noch weitere Elemente zu suchen. Auch können wir id bei den weiters zu bildenden Erzeugnissen unterschlagen.

Im zweiten Subfall erhielten wir das Element $\left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)=(2,3)$. Es ist $|\langle(2,3)\rangle|=2<6$, wir haben also noch weitere Elemente zu suchen.

Im dritten Subfall erhielten wir das Element $\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)=(1,2)$. Es ist $|\langle(1,2),\,(2,3)\rangle|=6$ ([8]). Also ist das Bild von $\mathrm{Gal}(\mathbf{Q}(a,b)|\mathbf{Q})$ in $\mathcal{S}_3$ gleich $\langle(1,2),\,(2,3)\rangle$, da es letzteres enthält und dieselbe Ordnung hat, und wir sind fertig.

3.4.2.4 Ein großes Beispiel, $X^6-X^3+2\in\mathbf{Q}[X]$

Sei $f(X)=X^6-X^3+2\in\mathbf{Q}[X]$. In Aufgabe 34.(3) wurde der Zerfällungskörper $L=\mathbf{Q}(a,b,c)$ konstruiert, mit

$$\begin{array}{lcl}\mu_{a,\mathbf{Q}}(X) & = & X^6-X^3+2\\ \mu_{b,\mathbf{Q}(a)}(X) & = & X^3+(a^3-1)\\ \mu_{c,\mathbf{Q}(a,b)}(X) & = & X^2+aX+a^2\ .\end{array}$$

Es zerfiel

$$\begin{array}{cl} & X^6-X^3+2\\ = & (X-a)(X-b)(X-c)(X+c+a)\big(X-\frac{1}{2}(a^5-a^2)bc+b\big)\big(X+\frac{1}{2}(a^5-a^2)bc\big)\\ \in & \mathbf{Q}(a,b)[X]\ .\end{array}$$

Ferner war $[\mathbf{Q}(a,b,c):\mathbf{Q}]=36$. ([9]).

---

[8] `Order(sub< SymmetricGroup(3) | (1,2), (2,3) >);`

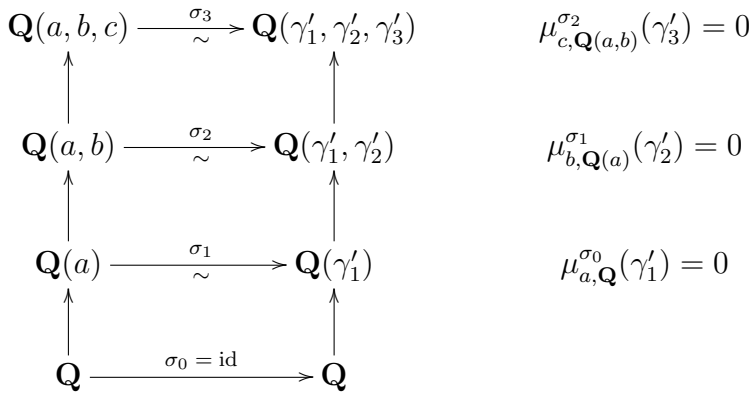
[9] Hierzu verwandten wir Magma wie folgt.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 - X^3 + 2);
KK<a> := ext<Q | X^6 - X^3 + 2>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 - XX^3 + 2);
KKK<b> := ext<KK | XX^3 + a^3 - 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^6 - XXX^3 + 2);
KKKK<c> := ext<KKK | XXX^2 + a*XXX + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 - XXXX^3 + 2);
```

Sei

$$\begin{aligned}\gamma_1 &:= a\\ \gamma_2 &:= b\\ \gamma_3 &:= c\\ \gamma_4 &:= -a-c\\ \gamma_5 &:= \tfrac{1}{2}(a^5-a^2)bc-b\\ \gamma_6 &:= -\tfrac{1}{2}(a^5-a^2)bc \ \ ([10])\ .\end{aligned}$$

Es ist $m=3$ und $n=6$. Bestimmen wir das Bild von $\mathrm{Gal}(X^6-X^3+2)=\mathrm{Gal}(\mathbf{Q}(a,b,c)|\mathbf{Q})$ in $\mathcal{S}_6$.



Im folgenden Prozedere verstehen wir unter Nullstellen stets Nullstellen in $\mathbf{Q}(a,b,c)$.

Die Nullstellen von

$$\mu_{a,\mathbf{Q}}(X) \ = \ X^6-X^3+2$$

sind γ_1, γ_2, γ_3, γ_4, γ_5 und γ_6 ([11]). Unter diesen haben wir ein γ_1' auszuwählen.

Fall $\gamma_1'=\gamma_1$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \ = \ X^3+(\gamma_1^3-1)\ ,$$

welches die Nullstellen γ_2, γ_5 und γ_6 hat ([12]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2'=\gamma_2$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \ = \ X^2+\gamma_1X+\gamma_1^2 \ \ ([13])\ ,$$

[10] In Magma entsprechend:

```
ga1 := a;
ga2 := b;
ga3 := c;
ga4 := -a-c;
ga5 := 1/2*(a^5 - a^2)*b*c - b;
ga6 := -1/2*(a^5 - a^2)*b*c;
```

[11] `Factorisation(XXXX^6 - XXXX^3 + 2);`

[12] `Factorisation(XXXX^3 + (ga1^3 - 1));`

welches die Nullstellen γ_3 und γ_4 hat ([14]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_2, \gamma_3)$. Es werden

$$\begin{array}{lllllll} \sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_1 - \gamma_3 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_2\gamma_3 - \gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_2\gamma_3 & = & \gamma_6 \, . \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&2&3&4&5&6 \end{smallmatrix}\right) = \mathrm{id}$.

Zwischenstand: $|\langle \mathrm{id} \rangle| = 1 < 36$.

Subsubfall $\gamma_3' = \gamma_4$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_2, \gamma_4)$. Es werden

$$\begin{array}{lllllll} \sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_1 - \gamma_4 & = & \gamma_3 \\ \sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_2\gamma_4 - \gamma_2 & = & \gamma_6 \\ \sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_2\gamma_4 & = & \gamma_5 \, , \end{array}$$

wobei Magma für den letzten Schritt hilft ([15]). Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&2&4&3&6&5 \end{smallmatrix}\right) = (3,4)(5,6)$.

Zwischenstand: $|\langle (3,4)(5,6) \rangle| = 2 < 36$.

Subfall $\gamma_2' = \gamma_5$. Es ist

$$\mu_{c,\mathbf{Q}(a,b)}^{\sigma_2}(X) \; = \; X^2 + \gamma_1 X + \gamma_1^2 \, ,$$

welches die Nullstellen γ_3 und γ_4 hat ([16]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_5, \gamma_3)$. Es werden

$$\begin{array}{lllllll} \sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_1 - \gamma_3 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_5\gamma_3 - \gamma_5 & = & \gamma_6 \\ \sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_5\gamma_3 & = & \gamma_2 \, . \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&3&4&6&2 \end{smallmatrix}\right) = (2,5,6)$.

[13] Es wurde also das in den Koeffizienten von $\mu_{c,\mathbf{Q}(a,b)}(X)$ auftretende a durch γ_1' substituiert. Tauchte in $\mu_{c,\mathbf{Q}(a,b)}(X)$ auch noch b in den Koeffizienten auf, so müßte man dafür nun γ_2' substitutieren. Dies ist aber zufälligerweise nicht der Fall.

[14] `Factorisation(XXXX^2 + ga1*XXXX + ga1^2);`

[15] E.g. `1/2*(ga1^5 - ga1^2)*ga2*ga4 - ga2;`. Oder aber, wenn man etwas besser automatisieren möchte, dann kann man wie folgt vorgehen.

```
R3<Ga1,Ga2,Ga3> := PolynomialRing(KKKK,3);
Ga4 := - Ga1 - Ga3;
Ga5 := 1/2*(Ga1^5 - Ga1^2)*Ga2*Ga3 - Ga2;
Ga6 := -1/2*(Ga1^5 - Ga1^2)*Ga2*Ga3;
Evaluate(Ga4,[ga1,ga2,ga4]);
Evaluate(Ga5,[ga1,ga2,ga4]);
Evaluate(Ga6,[ga1,ga2,ga4]);
Evaluate(Ga5,[ga1,ga2,ga4]) eq ga6;
Evaluate(Ga6,[ga1,ga2,ga4]) eq ga5;
```

[16] `Factorisation(XXXX^2 + ga1*XXXX + ga1^2);`

Zwischenstand: $|\langle (3,4)(5,6),\ (2,5,6)\rangle| = 6 < 36$ ([17]).

Subsubfall $\gamma_3' = \gamma_4$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_5, \gamma_4)$. Es werden

$$\begin{array}{lcllcll} \sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_1 - \gamma_4 & = & \gamma_3 \\ \sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_5\gamma_4 - \gamma_5 & = & \gamma_2 \\ \sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_5\gamma_4 & = & \gamma_6\ . \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&4&3&2&6 \end{smallmatrix}\right) = (2,5)(3,4)$.

Zwischenstand: $|\langle (3,4)(5,6),\ (2,5,6),\ (2,5)(3,4)\rangle| = 6 < 36$ ([18]). Damit ist $(2,5)(3,4)$ bereits in $\langle (3,4)(5,6),\ (2,5,6)\rangle$ enthalten, kann also bei weiters zu bildenden Erzeugnissen weggelassen werden.

Subfall $\gamma_2' = \gamma_6$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \ = \ X^2 + \gamma_1 X + \gamma_1^2\ ,$$

welches die Nullstellen γ_3 und γ_4 hat ([19]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_6, \gamma_3)$. Es werden

$$\begin{array}{lcllcll} \sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_1 - \gamma_3 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_6\gamma_3 - \gamma_6 & = & \gamma_2 \\ \sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_6\gamma_3 & = & \gamma_5\ . \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&6&3&4&2&5 \end{smallmatrix}\right) = (2,6,5)$.

Zwischenstand: $|\langle (3,4)(5,6),\ (2,5,6),\ (2,6,5)\rangle| = 6 < 36$ ([20]). Damit ist $(2,6,5)$ bereits in $\langle (3,4)(5,6),\ (2,5,6)\rangle$ enthalten (in der Tat ist $(2,5,6) = (2,6,5)^2$), kann also bei weiters zu bildenden Erzeugnissen weggelassen werden.

Subsubfall $\gamma_3' = \gamma_4$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_6, \gamma_4)$. Es werden

$$\begin{array}{lcllcll} \sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_1 - \gamma_4 & = & \gamma_3 \\ \sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_6\gamma_4 - \gamma_6 & = & \gamma_5 \\ \sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_1^5 - \gamma_1^2)\gamma_6\gamma_4 & = & \gamma_2\ . \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&6&4&3&5&2 \end{smallmatrix}\right) = (2,6)(3,4)$.

Zwischenstand: $|\langle (3,4)(5,6),\ (2,5,6),\ (2,6)(3,4)\rangle| = 6 < 36$ ([21]). Damit ist $(2,6)(3,4)$ bereits in $\langle (3,4)(5,6),\ (2,5,6)\rangle$ enthalten, kann also bei weiters zu bildenden Erzeugnissen weggelassen werden.

[17] `Order(sub<SymmetricGroup(6) | (3,4)(5,6), (2,5,6)>);`
[18] `Order(sub<SymmetricGroup(6) | (3,4)(5,6), (2,5,6), (2,5)(3,4)>);`
[19] `Factorisation(XXXX^2 + ga1*XXXX + ga1^2);`
[20] `Order(sub<SymmetricGroup(6) | (3,4)(5,6), (2,5,6), (2,6,5)>);`
[21] `Order(sub<SymmetricGroup(6) | (3,4)(5,6), (2,5,6), (2,6)(3,4)>);`

Fall $\gamma_1' = \gamma_2$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^3 + (\gamma_2^3 - 1)\;,$$

welches die Nullstellen γ_1, γ_3 und γ_4 hat ([22]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_1$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + \gamma_2 X + \gamma_2^2\;,$$

welches die Nullstellen γ_5 und γ_6 hat ([23]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_5$. Wir erhalten das zulässige Tupel $(\gamma_2, \gamma_1, \gamma_5)$. Es werden

$$\begin{array}{lcllcll}
\sigma_3(\gamma_4) & = & -\sigma_3(a) - \sigma_3(c) & = & -\gamma_2 - \gamma_5 & = & \gamma_6 \\
\sigma_3(\gamma_5) & = & \frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) - \sigma_3(b) & = & \frac{1}{2}(\gamma_2^5 - \gamma_2^2)\gamma_1\gamma_5 - \gamma_1 & = & \gamma_3 \\
\sigma_3(\gamma_6) & = & -\frac{1}{2}(\sigma_3(a)^5 - \sigma_3(a)^2)\sigma_3(b)\sigma_3(c) & = & -\frac{1}{2}(\gamma_2^5 - \gamma_2^2)\gamma_1\gamma_5 & = & \gamma_4\;.
\end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\2&1&5&6&3&4\end{smallmatrix}\right) = (1,2)(3,5)(4,6)$.

Zwischenstand : $|\langle(3,4)(5,6),\,(2,5,6),\,(1,2)(3,5)(4,6)\rangle| = 36 = 36$ ([24]).

Abbruch der Fallunterscheidungen, da fertig !

Als Ergebnis erhalten wir das isomorphe Bild von $\mathrm{Gal}(\mathbf{Q}(a,b,c)|\mathbf{Q})$ in $\mathcal{S}_6$ zu

$$\langle(3,4)(5,6),\,(2,5,6),\,(1,2)(3,5)(4,6)\rangle \;\;([25])\;.$$

In Magma gibt es, wie schon erwähnt :

```
G := GaloisGroup(X^6 - X^3 + 2);
{u : u in G};
Order(G);
```

Vorsicht ist hier aber deswegen geboten, weil die von Magma gewählte Numerierung mit der unsrigen nicht übereinstimmen muß.

3.5 Zwischenkörper

3.5.1 Dedekinds Lemma

3.5.1.1 Fixkörper unter Mengen von Morphismen

Sei L ein Körper. Sei E ein Körper. Sei $n \geqslant 1$. Seien

$$\sigma_1, \ldots, \sigma_n \;:\; L \longrightarrow E$$

paarweise verschiedene Körpermorphismen.

[22] `Factorisation(XXXX^3 + (ga2^3 - 1));`

[23] `Factorisation(XXXX^2 + ga2*XXXX + ga2^2);`

[24] `Order(sub<SymmetricGroup(6) | (3,4)(5,6), (2,5,6), (1,2)(3,5)(4,6)>);`

[25] Die Liste ihrer Elemente erhält man via

```
{u : u in sub<SymmetricGroup(6) | (3,4)(5,6), (2,5,6), (1,2)(3,5)(4,6)>};
```

Satz 7 (Dedekinds Lemma) *Sind* $\lambda_1, \ldots, \lambda_n \in E$ *gegeben mit*

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) \;=\; 0$$

für alle $x \in L$*, so ist* $\lambda_1 = \cdots = \lambda_n = 0$*.*

In diesem Sinne ist $(\sigma_1, \ldots, \sigma_n)$ also linear unabhängig über E.

Beweis. Nehmen wir das Gegenteil *an.* Sei $n \in \mathbf{Z}_{\geqslant 1}$ minimal so, daß es paarweise verschiedene Körpermorphismen $\sigma_1, \ldots, \sigma_n \;:\; L \longrightarrow E$ und $\lambda_1, \ldots, \lambda_n \in E$ so gibt, daß nicht $\lambda_1 = \cdots = \lambda_n = 0$ und daß

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) \;=\; 0$$

für alle $x \in L$. Aus dieser Minimalität folgt $\lambda_i \neq 0$ für alle $i \in [1, n]$, da ein i mit $\lambda_i = 0$ weggelassen werden könnte. Ferner ist $n \geqslant 2$, da aus $\lambda_1\sigma_1(1) = 0$ bereits $\lambda_1 = 0$ folgte.

Da $\sigma_1 \neq \sigma_n$, gibt es ein $y \in L$ mit $\sigma_1(y) \neq \sigma_n(y)$. Es ist

$$\begin{array}{rl} & \lambda_1\sigma_1(y)\sigma_1(x) + \lambda_2\sigma_2(y)\sigma_2(x) + \cdots + \lambda_n\sigma_n(y)\sigma_n(x) \\ = & \lambda_1\sigma_1(yx) + \lambda_2\sigma_2(yx) + \cdots + \lambda_n\sigma_n(yx) \\ = & 0 \end{array}$$

für alle $x \in L$. Da auch

$$\lambda_1\sigma_1(y)\sigma_1(x) + \lambda_2\sigma_1(y)\sigma_2(x) + \cdots + \lambda_n\sigma_1(y)\sigma_n(x) \;=\; 0$$

für alle $x \in L$, folgt durch Differenzbildung, daß auch

$$\lambda_2(\sigma_2(y) - \sigma_1(y))\sigma_2(x) + \cdots + \lambda_n(\sigma_n(y) - \sigma_1(y))\sigma_n(x) \;=\; 0$$

für alle $x \in L$. Da aber $\lambda_n(\sigma_n(y) - \sigma_1(y)) \neq 0$, *widerspricht* dies der Minimalität von n. ▫

Definition. Sei

$$\mathrm{Fix}_{\{\sigma_1,\ldots,\sigma_n\}} L \;:=\; \{x \in L \;:\; \sigma_i(x) = \sigma_j(x) \text{ für alle } i, j \in [1, n]\}$$

der *Fixkörper* von $\{\sigma_1, \ldots, \sigma_n\}$ in L; dies ist ein Teilkörper von L.

In der Tat ist $1 \in \mathrm{Fix}_{\{\sigma_1,\ldots,\sigma_n\}} L$, da $\sigma_i(1) = 1 = \sigma_j(1)$; es sind mit $x, x' \in L$ auch $x - x'$ und $x \cdot x'$ in $\mathrm{Fix}_{\{\sigma_1,\ldots,\sigma_n\}} L$, da

$$\begin{array}{rcccccl} \sigma_i(x - x') & = & \sigma_i(x) - \sigma_i(x') & = & \sigma_j(x) - \sigma_j(x') & = & \sigma_j(x - x') \\ \sigma_i(x \cdot x') & = & \sigma_i(x) \cdot \sigma_i(x') & = & \sigma_j(x) \cdot \sigma_j(x') & = & \sigma_j(x \cdot x')\,; \end{array}$$

es ist für $x \in L^\times$ auch $x^{-1} \in \mathrm{Fix}_{\{\sigma_1,\ldots,\sigma_n\}} L$, da

$$\sigma_i(x^{-1}) \;=\; \sigma_i(x)^{-1} \;=\; \sigma_j(x)^{-1} \;=\; \sigma_j(x^{-1})\,;$$

jeweils für $i, j \in [1, n]$.

Folgerung (zu Satz 7, Dedekinds Lemma). *Es ist* $[L : \mathrm{Fix}_{\{\sigma_1,\dots,\sigma_n\}} L] \geqslant n$.

Beweis. Schreibe $K := \mathrm{Fix}_{\{\sigma_1,\dots,\sigma_n\}} L$. Sei *angenommen,* es gebe ein über K erzeugendes Tupel $(x_1, \dots, x_{n-1})$ in L. Sei $S := (\sigma_j(x_i))_{i,j} \in E^{(n-1)\times n}$. Sei $v = (v_j)_j \in E^{n\times 1} \smallsetminus \{0\}$ mit $Sv = 0$.

Sei nun $y \in L$ gegeben. Schreibe $y = \sum_{i\in[1,n-1]} a_i x_i$ mit $a_i \in K$. Sei $w = (\sigma_1(a_i))_i \in E^{(n-1)\times 1}$. Es ist

$$\begin{aligned} 0 &= w^{\mathrm{t}} S v \\ &= \textstyle\sum_{i\in[1,n-1],\, j\in[1,n]} \sigma_1(a_i)\sigma_j(x_i)v_j \\ &= \textstyle\sum_{i\in[1,n-1],\, j\in[1,n]} \sigma_j(a_i)\sigma_j(x_i)v_j \\ &= \textstyle\sum_{i\in[1,n-1],\, j\in[1,n]} \sigma_j(a_i x_i)v_j \\ &= \textstyle\sum_{j\in[1,n]} \sigma_j\big(\sum_{i\in[1,n-1]} a_i x_i\big)v_j \\ &= \textstyle\sum_{j\in[1,n]} \sigma_j(y)v_j \ . \end{aligned}$$

Da dies für jedes $y \in L$ gilt, haben wir einen *Widerspruch* zu Satz 7 (Dedekinds Lemma). ▫

Bemerkung. *Sei $L|K$ eine endliche Erweiterung. Dann ist* $\mathrm{Aut}(L|K)$ *endlich und, genauer,* $|\mathrm{Aut}(L|K)| \leqslant [L : K]$.

Vgl. auch die erste Folgerung in §3.4.1. Dort erhielten wir $|\mathrm{Aut}(L|K)| = [L : K]$ für unseren Zerfällungskörper L.

Beweis. Sei M eine endliche Teilmenge von $\mathrm{Aut}(L|K)$. Dann ist $K \subseteq \mathrm{Fix}_M L \subseteq L$. Eine K-lineare Basis von L ist somit ein $\mathrm{Fix}_M L$-lineares Erzeugendensystem von L. Also ist $L|\mathrm{Fix}_M L$ eine endliche Erweiterung mit $[L : \mathrm{Fix}_M L] \leqslant [L : K]$. Mit vorstehender Folgerung wird $|M| \leqslant [L : \mathrm{Fix}_M L] \leqslant [L : K]$. Da dies für jede endliche Teilmenge M von $\mathrm{Aut}(L|K)$ gilt, folgt die Endlichkeit von $\mathrm{Aut}(L|K)$ sowie $|\mathrm{Aut}(L|K)| \leqslant [L : K]$. ▫

3.5.1.2 Die Spur

Sei L ein Körper. Sei P der Primkörper von L. Schreibe $\mathrm{Aut}(L) := \mathrm{Aut}(L|P) = \{L \xrightarrow[\sim]{\sigma} L\}$; vgl. Bemerkungen in §2.1. Insbesondere ist $\mathrm{Aut}(L)$ mit der Verkettung eine Gruppe.

Sei G eine endliche Untergruppe von $\mathrm{Aut}(L)$, also $G \leqslant \mathrm{Aut}(L)$. Wir erinnern an den Fixkörper

$$\mathrm{Fix}_G L \ = \ \{x \in L \ : \ \sigma(x) = x \text{ für alle } \sigma \in G\} \ .$$

Definition. Sei

$$\begin{array}{ccc} L & \xrightarrow{\mathrm{Tr}_G} & \mathrm{Fix}_G L \\ x & \longmapsto & \mathrm{Tr}_G(x) \ := \ \sum_{\sigma\in G} \sigma(x) \end{array}$$

die *Spur* auf L unter G (engl. trace). Für $x \in L$ ist in der Tat $\mathrm{Tr}_G(x) \in \mathrm{Fix}_G L$, da für $\rho \in G$

$$\rho(\mathrm{Tr}_G(x)) \ = \ \textstyle\sum_{\sigma\in G} \rho(\sigma(x)) \ \overset{\tilde\sigma \,=\, \rho\circ\sigma}{=} \ \sum_{\tilde\sigma\in G} \tilde\sigma(x) \ = \ \mathrm{Tr}_G(x) \ .$$

Ferner ist Tr_G eine $\mathrm{Fix}_G L$-lineare Abbildung, wie wir nun verifizieren. Die Verträglichkeit mit Summen ist ersichtlich. Sei also $y \in \mathrm{Fix}_G L$. Sei $x \in L$. Es wird

$$\mathrm{Tr}_G(yx) \;=\; \textstyle\sum_{\sigma\in G} \sigma(yx) \;=\; \sum_{\sigma\in G} y\sigma(x) \;=\; y\,\mathrm{Tr}_G(x)\;.$$

Bemerkung. *Es ist* $\mathrm{Tr}_G : L \longrightarrow \mathrm{Fix}_G L$ *surjektiv.*

Beweis. Schreibe $K = \mathrm{Fix}_G L$. Da Tr_G eine K-lineare Abbildung von L nach K ist, wäre ansonsten Tr_G die Nullabbildung. Dann aber wäre $\sum_{\sigma\in G} \sigma(x) = 0$ für alle $x \in L$, was wegen Satz 7 (Dedekinds Lemma) nicht zutrifft. ▫

3.5.1.3 Fixkörper unter Gruppen von Automorphismen

Satz 8 (Fixkörper unter Gruppe)

Sei L ein Körper. Sei G eine endliche Untergruppe von $\mathrm{Aut}(L)$, also $G \leqslant \mathrm{Aut}(L)$.

(1) *Es ist*
$$[L : \mathrm{Fix}_G L] \;=\; |G|\;.$$

(2) *Es ist*
$$G \;=\; \mathrm{Aut}(L|\,\mathrm{Fix}_G L)\;.$$

Beweis. Schreibe $n := |G|$ und $G = \{\sigma_1, \ldots, \sigma_n\}$. Schreibe $K := \mathrm{Fix}_G L$.

Zu (1). Mit der Folgerung zu Satz 7 aus §3.5.1.1 wissen wir, daß $[L : K] \geqslant n$. Sei $(x_1, \ldots, x_{n+1})$ ein Tupel von Elementen von L. Zu zeigen ist, daß dieses linear abhängig ist über K. Wir bilden die Matrix $T = (\sigma_i^{-1}(x_j))_{i,j} \in L^{n\times(n+1)}$. Es gibt ein $v = (v_j)_j \in L^{(n+1)\times 1} \smallsetminus \{0\}$ derart, daß $Tv = 0$. Sei etwa $v_{j_0} \neq 0$. Sei $w \in L$ derart, daß $\mathrm{Tr}_G(w) \neq 0$; vgl. Bemerkung in §3.5.1.2. Sei $v' = (v'_j)_j := wv_{j_0}^{-1}v \in L^{(n+1)\times 1}$. Es ist $Tv' = wv_{j_0}^{-1}Tv = 0$, aber $\mathrm{Tr}_G(v'_{j_0}) = \mathrm{Tr}_G(wv_{j_0}^{-1}v) = \mathrm{Tr}_G(w) \neq 0$. Somit ist auch

$$x_1\sigma_i(v'_1) + \cdots + x_{n+1}\sigma_i(v'_{n+1}) \;=\; \sigma_i\big(\sigma_i^{-1}(x_1)v'_1 + \cdots \sigma_i^{-1}(x_i)v'_{n+1}\big) \;=\; \sigma_i(0) \;=\; 0$$

für alle $i \in [1, n]$. Aufsummieren über $i \in [1, n]$ gibt

$$x_1\,\mathrm{Tr}_G(v'_1) + \cdots + x_{n+1}\,\mathrm{Tr}_G(v'_{n+1}) \;=\; 0\;,$$

was wegen $\mathrm{Tr}_G(v'_j) \in K$ stets und $\mathrm{Tr}_G(v'_{j_0}) \neq 0$ die lineare Abhängigkeit von $(x_1, \ldots, x_{n+1})$ über K zeigt.

Zu (2). Es ist $G \leqslant \mathrm{Aut}(L|K)$, da jedes $\sigma \in G$ zur Identität auf K einschränkt.

Mit der Bemerkung aus §3.5.1.1 ist aber $\mathrm{Aut}(L|K)$ endlich, und, genauer noch,

$$|G| \;\overset{(1)}{=}\; [L : K] \;\geqslant\; |\mathrm{Aut}(L|K)|\;.$$

Insgesamt ist also $G = \mathrm{Aut}(L|K)$. ▫

3.5.1.4 Galoiserweiterungen

Sei $L|K$ eine endliche Körpererweiterung.

Definition. Es heiße $L|K$ *galoisch* oder *Galoiserweiterung,* falls es eine endliche Untergruppe $G \leqslant \mathrm{Aut}(L)$ mit $K = \mathrm{Fix}_G L$ gibt.

Diesenfalls schreiben wir auch $\mathrm{Gal}(L|K) := \mathrm{Aut}(L|K)$ für die *Galoisgruppe* von $L|K$.

> Ist K perfekt und ist L der Zerfällungskörper eines normierten Polynoms $f(X) \in K[X]$, welches dort ein Produkt verschiedener normierter irreduzibler Faktoren ist, dann haben wir in §3.4.1 diese Bezeichnung schon verwendet. Dieser Vorgriff wird sich mit dem übernächsten Lemma als zulässig erweisen.

Sei $L|K$ eine endliche Erweiterung. Mit der Bemerkung aus §3.5.1.1 ist $\mathrm{Aut}(L|K)$ eine endliche Untergruppe von $\mathrm{Aut}(L)$.

Bemerkung. *Es ist $L|K$ galoisch genau dann, wenn $K = \mathrm{Fix}_{\mathrm{Aut}(L|K)} L$ gilt.*

Beweis. Es ist zu zeigen, daß aus $L|K$ galoisch folgt, daß $K = \mathrm{Fix}_{\mathrm{Aut}(L|K)} L$. Ist aber $G \leqslant \mathrm{Aut}(L)$ endlich und $K = \mathrm{Fix}_G L$, so ist mit Satz 8.(2) auch $G = \mathrm{Aut}(L|K)$. Somit ist in der Tat $K = \mathrm{Fix}_G L = \mathrm{Fix}_{\mathrm{Aut}(L|K)} L$. ▫

Bemerkung. *Es ist $L|K$ galoisch genau dann, wenn $|\mathrm{Aut}(L|K)| = [L : K]$ gilt.*

> Kurz, $L|K$ ist galoisch genau dann, wenn $\mathrm{Aut}(L|K)$ die "maximal vorstellbare" Ordnung hat.

Beweis. Mit Satz 8.(1) haben wir

$$\begin{array}{c} L \\ \Big| \\ {\scriptstyle |\mathrm{Aut}(L|K)|} \\ \mathrm{Fix}_{\mathrm{Aut}(L|K)} L \\ \Big| \\ K \end{array}$$

Mit voriger Bemerkung ist $L|K$ genau dann galoisch, wenn $K = \mathrm{Fix}_{\mathrm{Aut}(L|K)} L$. Dies ist wiederum äquivalent zu $[L : K] = [L : \mathrm{Fix}_{\mathrm{Aut}(L|K)} L]$, d.h. zu $[L : K] = |\mathrm{Aut}(L|K)|$. ▫

Lemma. *Sei $L|K$ galoisch. Sei $f(X) \in K[X]$ irreduzibel und normiert. Falls $f(X)$ in L eine Nullstelle besitzt, so zerfällt $f(X)$ in $L[X]$ in ein Produkt von Linearfaktoren.*

Beweis. Sei $y \in L$ mit $f(y) = 0$. Es genügt, ein normiertes irreduzibles Polynom in $K[X]$ mit Nullstelle y anzugeben, welches in $L[X]$ in Linearfaktoren zerfällt. Denn dieses ist ebenso wie $f(X)$ gleich dem Minimalpolynom von y über K; vgl. die erste Bemerkung in §2.3.2.

Sei $A := \{\sigma(y) \ : \ \sigma \in \mathrm{Aut}(L|K)\}$. Ist nun $\rho \in \mathrm{Aut}(L|K)$, so ist $\rho|_A^A$ definiert, injektiv und wegen A endlich also bijektiv. Sei

$$g(X) \ := \ \prod_{a\in A}(X-a) \ .$$

Dann ist

$$g^\rho(X) \ = \ \big(\prod_{a\in A}(X-a)\big)^\rho \ = \ \prod_{a\in A}(X-a)^\rho \ = \ \prod_{a\in A}(X-\rho(a)) \ \overset{\tilde a = \rho(a)}{=} \ \prod_{\tilde a\in A}(X-\tilde a) \ = \ g(X) \ .$$

Da dies für jedes $\rho \in \mathrm{Aut}(L|K)$ zutrifft, und da $K = \mathrm{Fix}_{\mathrm{Aut}(L|K)} L$, folgt $g(X) \in K[X]$.

Bleibt zu zeigen, daß $g(X)$ in $K[X]$ irreduzibel ist. Sei *angenommen,* wir hätten eine Zerlegung $g(X) = u(X)v(X)$ mit $u(X)$, $v(X) \in K[X]$ normiert und $\deg u$, $\deg v \ \geqslant \ 1$ gefunden. Dann gibt es eine Teilmenge $\emptyset \subsetneq B \subsetneq A$ mit

$$u(X) \ = \ \prod_{a\in B}(X-a)$$

Sei $b \in B$ und $c \in A \smallsetminus B$. Es gibt ein $\rho \in \mathrm{Aut}(L|K)$ so, daß $\rho(b) = c$, denn ist $b = \sigma(a)$ und $c = \tilde\sigma(a)$ mit σ, $\tilde\sigma \ \in \ \mathrm{Aut}(L|K)$, so kann man $\rho = \tilde\sigma \circ \sigma^{-1}$ nehmen. Nun ist $u(b) = 0$, also auch $0 = \rho(u(b)) = u(\rho(b)) = u(c)$, und somit $c \in B$, und wir haben einen *Widerspruch.* ▫

Lemma. *Sei K perfekt; vgl.* §3.3. *Sei $L|K$ eine endliche Erweiterung.*

Die folgenden Aussagen $(1, 2, 3)$ *sind äquivalent.*

(1) *Es ist $L|K$ galoisch.*

(2) *Es ist L Zerfällungskörper eines normierten Polynoms in $K[X]$, welches dort ein Produkt verschiedener normierter irreduzibler Faktoren ist.*

(3) *Es ist L Zerfällungskörper eines normierten Polynoms in $K[X]$.*

Beweis.

Ad (2) $\Rightarrow$ (1). Ist L ein solcher Zerfällungskörper, so ist $|\mathrm{Aut}(L|K)| = [L : K]$ nach der ersten Folgerung in §3.4.1. Nach voriger Bemerkung ist $L|K$ also galoisch.

Ad (1) $\Rightarrow$ (2). Sei umgekehrt $L|K$ galoisch. Sei $(\gamma_1, \ldots, \gamma_k)$ eine K-lineare Basis von L. Insbesondere ist also $L = K(\gamma_1, \ldots, \gamma_n)$. Sei $g(X)$ das Produkt über die Menge der Minimalpolynome von γ_i über K. In anderen Worten, wir bilden das Produkt dieser Minimalpolynome, unterbinden aber mehrfache irreduzible Faktoren. Zu zeigen bleibt, daß L der Zerfällungskörper von $g(X)$ ist. In der Tat wird L über K von den Nullstellen von $g(X)$ in L erzeugt, da die Menge dieser Nullstellen die Menge $\{\gamma_1, \ldots, \gamma_n\}$ umfaßt. Ferner zerfällt $g(X)$ in $L[X]$ in ein Produkt von Linearfaktoren, da dies nach vorangegangenem Lemma für alle seine irreduziblen Faktoren der Fall ist, deren jeder ja eine Nullstelle in L hat. ▫

Ad (2) $\Leftrightarrow$ (3). Zu zeigen ist nur $\Leftarrow$. Sei L also der Zerfällungskörper eines normierten Polynoms $f(X) \in K[X]$. Sei $\check f(X)$ das Produkt der Menge der irreduziblen normierten

Faktoren von $f(X)$. Wir haben zu zeigen, daß L auch der Zerfällungkörper von $\check{f}(X)$ ist. Zum einen zerfällt mit $f(X)$ auch sein Teiler $\check{f}(X)$ in $L[X]$ in ein Produkt von Linearfaktoren. Zum anderen ist die Menge der Nullstellen von $f(X)$ dieselbe wie die von $\check{f}(X)$, sodaß auch letztere L über K erzeugt. ▫

Beispiel.

(1) Es ist $\mathbf{Q}(\sqrt[3]{2})|\mathbf{Q}$ nicht galoisch, da X^3-2 in $\mathbf{Q}(\sqrt[3]{2})$ zwar eine Nullstelle hat, in $\mathbf{Q}(\sqrt[3]{2})[X]$ aber nicht in Linearfaktoren zerfällt; vgl. Beispiel in §2.5.1, Teil (2) und vorvoriges Lemma.

(2) Es ist $\mathbf{C}|\mathbf{R}$ galoisch. Denn es ist $\mathbf{R}$ perfekt und $\mathbf{C}$ Zerfällungskörper des irreduziblen Polynoms $X^2+1 \in \mathbf{R}[X]$; vgl. Beispiel in §2.5.1, Teil (1). In der Tat ist $\mathrm{Gal}(\mathbf{C}|\mathbf{R}) \simeq \mathcal{S}_2$; cf. Aufgabe 40.

(3) Es ist $\mathbf{F}_8|\mathbf{F}_2$ galoisch als Zerfällungskörper des irreduziblen Polynoms X^3+X+1 aus $\mathbf{F}_2[X]$; vgl. Beispiel in §2.5.1, Teil (3). Es ist $\mathrm{Gal}(\mathbf{F}_8|\mathbf{F}_2) = \langle \mathrm{Frob}_{\mathbf{F}_8} \rangle$, da $|\mathrm{Gal}(\mathbf{F}_8|\mathbf{F}_2)| = [\mathbf{F}_8 : \mathbf{F}_2] = 3$ und $\mathrm{o}(\mathrm{Frob}_{\mathbf{F}_8}) = 3$; vgl. auch §3.6 unten.

(4) Alle in den Aufgaben 30 und 34 berechneten Zerfällungskörper L sind galoisch über dem jeweiligen Grundkörper K. Jedoch ist keiner der bei der Konstruktion aufgetretenen echten Zwischenkörper galoisch über dem jeweiligen Grundkörper K, da das zu zerfällende irreduzible ([26]) Polynom in $K[X]$ zwar in diesem Zwischenkörper bereits eine Nullstelle hatte, über diesem aber noch nicht in Linearfaktoren zerfiel; vgl. vorvoriges Lemma.

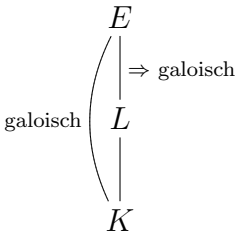
Es ist ein offenes Problem, ob es für jede endliche Gruppe G eine Galoiserweiterung $L|\mathbf{Q}$ so gibt, daß $\mathrm{Gal}(L|\mathbf{Q}) \simeq G$ (Stand 2009).

3.5.2 Korrespondenz von Untergruppen zu Zwischenkörpern

Lemma. *Seien $E|L|K$ endliche Körpererweiterungen. Sei $E|K$ galoisch. Schreibe*

$$T := \{L \xrightarrow{\tau} E : \tau \text{ Körpermorphismus mit } \tau|_K^K = \mathrm{id}_K\} .$$

(1) *Es ist $E|L$ galoisch.*



[26] Außer bei Aufgabe 30.(1), aber da gab es auch keine echten Zwischenkörper.

(2) *Die Abbildung*

$$\begin{array}{rcl} \mathrm{Gal}(E|K) & \xrightarrow{r} & T \\ \rho & \longmapsto & \rho|_L \ . \end{array}$$

ist surjektiv.

(3) *Es ist* $|T| = [L : K]$.

Zu (1) vgl. auch Aufgabe 47.(1).

Beweis. Schreibe $G := \mathrm{Gal}(E|K)$ und $U := \mathrm{Aut}(E|L) \leqslant G$.

Wir *behaupten,* daß für $\rho, \tilde{\rho} \in G$ gilt, daß genau dann $\rho|_L = \tilde{\rho}|_L$, wenn $\rho U = \tilde{\rho} U$. Denn ist $\rho U = \tilde{\rho} U$, so gibt es ein $\sigma \in U$ mit $\rho \circ \sigma = \tilde{\rho}$. Ist $x \in L$, so wird $\rho(x) = \rho(\sigma(x)) = \tilde{\rho}(x)$. Also ist $\rho|_L = \tilde{\rho}|_L$. Und ist umgekehrt $\rho|_L = \tilde{\rho}|_L$, so ist $(\tilde{\rho}^{-1} \circ \rho)(x) = x$ für alle $x \in L$, also $\tilde{\rho}^{-1} \circ \rho \in U$, woraus $\rho U = \tilde{\rho}(\tilde{\rho}^{-1} \circ \rho) U = \tilde{\rho} U$ folgt. Dies zeigt die *Behauptung.*

Mit der Behauptung ist für $\tau \in r(G)$, genauer, $\tau = \rho|_L$ für ein $\rho \in G$, auch

$$\begin{array}{rcl} r^{-1}(\{\tau\}) & = & \{\tilde{\rho} \in G \ : \ \tilde{\rho}|_L = \tau\} \\ & = & \{\tilde{\rho} \in G \ : \ \tilde{\rho}|_L = \rho|_L\} \\ & = & \{\tilde{\rho} \in G \ : \ \tilde{\rho} U = \rho U\} \\ & = & \rho U \ . \end{array}$$

Insbesondere ist $|r^{-1}(\{\tau\})| = |\rho U| = |U|$; vgl. Aufgabe 38.(1.b).

Da $G = \bigsqcup_{\tau \in r(G)} r^{-1}(\tau)$, ist $|G| = |U| \cdot |r(G)|$.

Mit der Folgerung zu Satz 7 aus §3.5.1.1 ist wegen $K \subseteq \mathrm{Fix}_T L$

$$[L : K] \ \geqslant \ [L : \mathrm{Fix}_T L] \ \geqslant \ |T| \ \geqslant \ |r(G)| \ .$$

Mit ebenjener Folgerung ist wegen $L \subseteq \mathrm{Fix}_U E$

$$[E : L] \ \geqslant \ [E : \mathrm{Fix}_U E] \ \geqslant \ |U| \qquad ([27]) \ .$$

Wir erhalten mit

$$|G| \ = \ [E : K] \ = \ [E : L][L : K] \ \geqslant \ [E : L]|T| \ \geqslant \ [E : L]|r(G)| \ \geqslant \ |U||r(G)| \ = \ |G| \ .$$

Also haben wir an allen Stellen in dieser Zeile Gleichheit.

Es folgt zum einen $[E : L] = |U|$. Mithin ist $E|L$ galoisch, wie in (1) behauptet; vgl. die zweite Bemerkung in §3.5.1.4.

Es folgt zum anderen $[L : K] = |T| = |r(G)|$. Mithin ist r surjektiv, wie in (2) behauptet, und $|T| = [L : K]$, wie in (3) behauptet. ▫

Einen alternativen Beweis zu Teil (1) im Fall K perfekt findet man in Aufgabe 47.(1).

[27] Letztere Ungleichung ist nach Satz 8.(1) eine Gleichheit, aber das brauchen wir nicht.

Ist G eine Gruppe und $N \trianglelefteq G$ ein Normalteiler darin, so erinnern wir daran, daß gemäß Aufgabe 42.(1) die Menge $G/N = \{gN \ : \ g \in G\}$ zuu einer Gruppe wird via $gN \cdot \tilde{g}N := (g \cdot \tilde{g})N$ für $g, \tilde{g} \in G$.

Satz 9 (Hauptsatz der Galoistheorie)

Sei $E|K$ eine endliche Galoiserweiterung mit Galoisgruppe $G := \mathrm{Gal}(E|K)$.

Sei $\mathcal{U} := \{U : U \leqslant G\}$ die Menge der Untergruppen von G.

Sei $\mathcal{Z} := \{L : E|L|K\}$ die Menge der Zwischenkörper zwischen K und E.

Wir haben folgende sich invertierende Bijektionen.

$$\begin{array}{rcl} \mathcal{U} & \tilde{\longrightarrow} & \mathcal{Z} \\ U & \longmapsto & \mathrm{Fix}_U E \\ \mathrm{Gal}(E|L) & \longmapsfrom & L \end{array}$$

Unter diesen werden Normalteiler von G auf Galoiserweiterungen von K abgebildet und umgekehrt. Ist $N \trianglelefteq G$, so haben wir einen Gruppenisomorphismus

$$\begin{array}{rcl} G/N & \tilde{\longrightarrow} & \mathrm{Gal}(\mathrm{Fix}_N E \,|\, K) \\ \rho N & \longmapsto & \rho|^{\mathrm{Fix}_N E}_{\mathrm{Fix}_N E} \, . \end{array}$$

Beweis. Wir zeigen die Bijektion zwischen $\mathcal{U}$ und $\mathcal{Z}$.

Ist $U \in \mathcal{U}$, also $U \leqslant G$ Untergruppe, so wird sie nach $\mathrm{Fix}_U E$ und wieder zurück nach $\mathrm{Aut}(E|\,\mathrm{Fix}_U E)$ abgebildet, was nach Satz 8.(2) wieder gleich U ist.

Ist $L \in \mathcal{Z}$, also $E|L|K$ Zwischenkörper, so wird dieser nach $\mathrm{Aut}(E|L)$ und wieder zurück nach $\mathrm{Fix}_{\mathrm{Aut}(E|L)} E$ abgebildet. Da $E|L$ nach vorigem Lemma galoisch ist, ist dieser Zwischenkörper wieder gleich E; vgl. erste Bemerkung in §3.5.1.4.

Also liegen sich invertierende Bijektionen vor.

Wir zeigen, daß Normalteiler unter dieser Bijektion zu Galoiserweiterungen von K korrespondieren. Sei $U \leqslant G$. Schreibe $L := \mathrm{Fix}_U E$.

Schreibe wieder, wie im vorstehenden Lemma,

$$T \ := \ \{L \xrightarrow{\tau} E : \tau \text{ Körpermorphismus mit } \tau|^K_K = \mathrm{id}_K\} \, .$$

Sei $L \overset{\kappa}{\hookrightarrow} E$ die Einbettungsabbildung. Wir haben eine injektive Abbildung

$$\begin{array}{rcl} \mathrm{Aut}(L|K) & \xrightarrow{s} & T \\ \sigma & \longrightarrow & \kappa \circ \sigma \end{array}$$

Wir gehen wie folgt vor.

$$\begin{aligned}
L|K \text{ galoisch} &\overset{1.}{\iff} |\mathrm{Aut}(L|K)| = [L:K] \\
&\overset{2.}{\iff} |\mathrm{Aut}(L|K)| = |T| \\
&\overset{3.}{\iff} \mathrm{Aut}(L|K) \overset{s}{\twoheadrightarrow} T \text{ surjektiv} \\
&\overset{4.}{\iff} \rho|_L \in s(\mathrm{Aut}(L|K)) \text{ für alle } \rho \in G \\
&\overset{5.}{\iff} \rho(L) = L \text{ für alle } \rho \in G \\
&\overset{6.}{\iff} \rho(\mathrm{Fix}_U E) = \mathrm{Fix}_U E \text{ für alle } \rho \in G \\
&\overset{7.}{\iff} \mathrm{Fix}_{{}^{\rho}U} E = \mathrm{Fix}_U E \text{ für alle } \rho \in G \\
&\overset{8.}{\iff} {}^{\rho}U = U \text{ für alle } \rho \in G \\
&\overset{9.}{\iff} U \trianglelefteq G
\end{aligned}$$

Zu 1. Siehe die zweite Bemerkung aus §3.5.1.4.

Zu 2. Es ist $|T| = [L:K]$; vgl. voriges Lemma, Teil (3).

Zu 3. Es ist s injektiv. Also ist s surjektiv genau dann, wenn $|\mathrm{Aut}(L|K)| = |T|$.

Zu 4. Es ist $T = \{\rho|_L \ : \ \rho \in G\}$; vgl. voriges Lemma, Teil (2).

Zu 5.

$\Longrightarrow$. Gibt es ein $\sigma \in \mathrm{Aut}(L|K)$ mit $\kappa \circ \sigma = \rho|_L$, so ist

$$\rho(L) \ = \ \rho|_L(L) \ = \ \kappa(\sigma(L)) \ = \ \kappa(L) \ = \ L \, .$$

$\Longleftarrow$. Ist $\rho(L) = L$, so ist $\rho|_L^L$ als eine injektive K-lineare Selbstabbildung des endlichdimensionalen K-Vektorraums L auch surjektiv. Also ist $\rho|_L^L \in \mathrm{Aut}(L|K)$, und sodann $\kappa \circ \rho|_L^L = \rho|_L$.

$$\begin{array}{ccc}
E & \xrightarrow[\sim]{\rho} & E \\
{\scriptstyle\kappa}\uparrow & \nearrow_{\rho|_L} & \uparrow{\scriptstyle\kappa} \\
L & \xrightarrow[\sim]{\rho|_L^L} & L
\end{array}$$

Zu 6. Einsetzen.

Zu 7. Sei $\rho \in G$. Sei $U \in \mathcal{U}$. Es wird

$$\begin{aligned}
\mathrm{Fix}_{{}^{\rho}U} E &= \{y \in E \ : \ ({}^{\rho}\sigma)(y) = y \text{ für alle } \sigma \in U\} \\
&= \{y \in E \ : \ \rho(\sigma(\rho^{-1}(y))) = y \text{ für alle } \sigma \in U\} \\
&= \{y \in E \ : \ \sigma(\rho^{-1}(y)) = \rho^{-1}(y) \text{ für alle } \sigma \in U\} \\
&= \{y \in E \ : \ \rho^{-1}(y) \in \mathrm{Fix}_U E\} \\
&= \{y \in E \ : \ y \in \rho(\mathrm{Fix}_U E)\} \\
&= \rho(\mathrm{Fix}_U E) \, .
\end{aligned}$$

Zu 8. Sei $\rho \in G$. Da $\mathcal{U} \longrightarrow \mathcal{Z}$, $V \longmapsto \mathrm{Fix}_V E$ bijektiv ist, ist $U = {}^{\rho}U$ genau dann, wenn $\mathrm{Fix}_{{}^{\rho}U} E = \mathrm{Fix}_U E$.

Zu 9. Definition Normalteiler.

Wir berechnen im Normalteilerfall die Galoisgruppe des korrespondierenden Körpers über K.

Sei $N \trianglelefteq G$. Schreibe $L := \mathrm{Fix}_N E$. Für alle $\rho \in G$ ist, wie eben gesehen, $\rho|_L^L \in \mathrm{Gal}(L|K)$. Somit haben wir einen Gruppenmorphismus

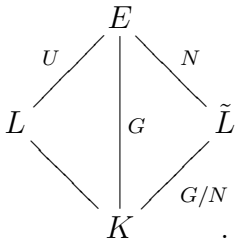
$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(L|K) \\ \rho & \longmapsto & \rho|_L^L \,. \end{array}$$

Dessen Kern ist gleich $\mathrm{Gal}(E|L) = N$. Mit Aufgabe 42.(2) erhalten wir einen injektiven Gruppenmorphismus

$$\begin{array}{ccc} G/N & \longrightarrow & \mathrm{Gal}(L|K) \\ \rho N & \longmapsto & \rho|_L^L \end{array}$$

Nun ist $|G/N| = [E : K]/[E : L] = [L : K] = |\mathrm{Gal}(L|K)|$. Also ist dieser Morphismus bijektiv ([28]). ▫

Eine Veranschaulichung. Sei $E|K$ eine endliche Galoiserweiterung mit Galoisgruppe $G := \mathrm{Gal}(E|K)$. Sei $U \leqslant G$; sei $L := \mathrm{Fix}_U E$, sei $N \trianglelefteq G$, sei $\tilde{L} := \mathrm{Fix}_N E$. Tragen wir Galoisgruppen bei Galoiserweiterungen ein, so erhalten wir



Bemerkung. In der Situation von Satz 9 können wir für einen gegebenen Zwischenkörper $E|L|K$ mit $L|K$ galoisch den letztaufgeführten Isomorphismus auch als "Kürzungsregel" schreiben,

$$\mathrm{Gal}(E|K)/\,\mathrm{Gal}(E|L) \;\simeq\; \mathrm{Gal}(L|K)\,.$$

3.6 Galoisgruppen von Erweiterungen endlicher Körper

Sei p prim. Seien $r,\, s \geqslant 1$. Betrachte die Erweiterung

$$\mathbf{F}_{p^{rs}} \,|\, \mathbf{F}_{p^r}$$

endlicher Körper; vgl. §2.5.4. Schreibe

$$F \;:=\; (\mathrm{Frob}_{\mathbf{F}_{p^{rs}}})^r \;:\; \mathbf{F}_{p^{rs}} \xrightarrow{\sim} \mathbf{F}_{p^{rs}} \;,\quad x \longmapsto x^{p^r} \;.$$

[28] Seine Surjektivität folgt auch aus den oben angeführten Surjektivitäten bzgl. T.

Für alle Elemente x von $\mathbf{F}_{p^r}$ ist $x^{p^r} = x$; vgl. Beweis zu Lemma in §2.5.4, Teil (2), oder Lösung zu Aufgabe 33.(2). Also ist $F \in \mathrm{Aut}(\mathbf{F}_{p^{rs}} \,|\, \mathbf{F}_{p^r})$.

Lemma. *Es ist* $\mathbf{F}_{p^{rs}}|\mathbf{F}_{p^r}$ *eine Galoiserweiterung mit Galoisgruppe* $\mathrm{Gal}(\mathbf{F}_{p^{rs}}|\mathbf{F}_{p^r}) = \langle F\rangle$ *von Ordnung* s*.*

Beweis. Sei $\mathbf{F}_{p^{rs}}^{\times} = \langle\xi\rangle$, wobei $\mathrm{o}(\xi) = p^{rs} - 1$; vgl. Aufgabe 27.(5).

Nun ist $F^i(\xi) = \xi^{p^{ri}} \neq \xi$ für $i \in [1, s-1]$, da dann $\xi^{p^{ri}-1} \neq 1$ wegen $p^{ri} - 1 \in [1, p^{rs} - 2] = [1, \mathrm{o}(\xi) - 1]$.

Auf der anderen Seite ist $F^s = \mathrm{id}_{\mathbf{F}_{p^{rs}}}$, da für $x \in \mathbf{F}_{p^{rs}}$ in der Tat $F^s(x) = x^{p^{rs}} = x$ ist.

Also ist $|\langle F\rangle| = \mathrm{o}(F) = s$.

Da mit der Bemerkung aus §3.5.1.1 aber

$$s \;=\; |\langle F\rangle| \;\leqslant\; |\mathrm{Aut}(\mathbf{F}_{p^{rs}} \,|\, \mathbf{F}_{p^r})| \;\leqslant\; [\mathbf{F}_{p^{rs}} : \mathbf{F}_{p^r}] \;=\; s$$

ist, gilt beidesmal Gleichheit ([29]). Also ist $\mathbf{F}_{p^{rs}} \,|\, \mathbf{F}_{p^r}$ galoisch; vgl. zweite Bemerkung in §3.5.1.4. Da $\langle F\rangle \leqslant \mathrm{Gal}(\mathbf{F}_{p^{rs}} \,|\, \mathbf{F}_{p^r})$ und da beide von Ordnung s sind, gilt auch hier Gleichheit. ▫

Zu $\mathbf{F}_{p^{rs}}|\mathbf{F}_{p^r}$ galoisch vgl. alternativ auch Aufgabe 47.(2).

[29] Vgl. auch Satz 8.(1).

Kapitel 4

Auflösbarkeit

Nun kehren wir zurück zum Ausgangsproblem. Sind die Nullstellen jedes Polynoms als iterierte Wurzelausdrücke schreibbar, wie dies in den Aufgaben 1 und 5 für die Polynome von Grad 3 und 4 durchgeführt wurde? Siehe dazu den Satz 11 von Abel in §4.4.3. Falls nein, kann man für ein gegebenes Polynom entscheiden, ob dies geht? Siehe dazu den Satz 10 von Galois in §4.4.2.

4.1 Auflösbare Gruppen

Alle Gruppen in diesem Abschnitt §4.1 seien endlich.

Vorsicht. Sei G eine Gruppe. Seien G_1 und G_2 Teilmengen von G.

Aus $G_1 \leqslant G_2 \leqslant G$ folgt $G_1 \leqslant G$.

Aber aus $G_1 \trianglelefteqslant G_2 \trianglelefteqslant G$ folgt im allgemeinen nicht $G_1 \trianglelefteqslant G$. So z.B. ist

$$\langle (1,2)(3,4) \rangle \trianglelefteqslant \langle (1,2)(3,4),\ (1,3)(2,4) \rangle \trianglelefteqslant \mathcal{S}_4 \,,$$

Berechne hierzu

$$\langle (1,2)(3,4),\ (1,3)(2,4) \rangle = \{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\} \,,$$

z.B. mit Magma. Alle Elemente dieser Gruppe haben Ordnung 1 oder 2. Sind x und y also daraus, so wird $yx = yx(xy)^2 = yxxyxy = xy$. Somit ist diese Untergruppe abelsch. Insbesondere ist $\langle (1,2)(3,4) \rangle$ darin ein Normalteiler.

Die mittlere Gruppe besteht aus id und allen Elementen der Form $(a,b)(c,d)$ in $\mathcal{S}_4$. Ist $\sigma \in \mathcal{S}_4$, so wird allgemein $\sigma \circ (a,b)(c,d) \circ \sigma^{-1} = \big(\sigma(a),\, \sigma(b)\big)\big(\sigma(c),\, \sigma(d)\big)$. Folglich ist die mittlere Gruppe normal in $\mathcal{S}_4$.

Wohingegen

$$\langle (1,2)(3,4) \rangle \not\trianglelefteqslant \mathcal{S}_4 \,,$$

da z.B. ${}^{(1,3)}(1,2)(3,4) = (3,2)(1,4) = (1,4)(2,3) \notin \langle (1,2)(3,4) \rangle$.

Definition. Sei G eine Gruppe. Sei $k \geqslant 0$. Ein Tupel $(G_i)_{i\in[0,k]} = (G_i)_i$ von Untergruppen von G heißt *Semisubnormalreihe* von G, falls

$$G_0 \trianglelefteqslant G_1 \trianglelefteqslant G_2 \trianglelefteqslant G_3 \trianglelefteqslant \cdots \trianglelefteqslant G_{k-1} \trianglelefteqslant G_k = G$$

Die Faktorgruppe G_i/G_{i-1} heißt i-ter *Subfaktor* dieser Semisubnormalreihe. Es heißt G_0 ihr *Anfangsterm.*

Falls dazuhin $G_0 = \{1\}$, so heißt $(G_i)_i$ *Subnormalreihe* von G.

Definition. Eine Gruppe G heiße *auflösbar,* wenn es eine Subnormalreihe $(G_i)_i$ von G gibt mit G_i/G_{i-1} abelsch für alle $i \in [1,k]$; kurz, mit allen Subfaktoren abelsch.

In diesem Sinne ist eine auflösbare Gruppe "stückweise abelsch".

Beispiel. Ist die Gruppe G abelsch, so ist sie auflösbar, wie man anhand der Subnormalreihe $\{1\} \trianglelefteqslant G$ erkennt.

Beispiel. Es ist $\mathcal{S}_3$ auflösbar wegen

$$\{\mathrm{id}\} \trianglelefteqslant \langle(1,2,3)\rangle \trianglelefteqslant \mathcal{S}_3 \,.$$

Schreibe $G_1 := \langle(1,2,3)\rangle$. Es ist $G_1/\{\mathrm{id}\} \simeq G_1$ abelsch. Ferner ist

$$\mathcal{S}_3/G_1 = \{\sigma G_1 : \sigma \in \mathcal{S}_3\} = \{\mathrm{id}\, G_1,\ (1,2)G_1\} = \langle(1,2)G_1\rangle \,,$$

mithin abelsch. Dagegen ist $\mathcal{S}_3$ nicht abelsch!

Beispiel. Es ist $\mathcal{S}_5$ nicht auflösbar. Siehe Aufgabe 49.(2).

Bemerkung. *Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus. Sei $(H_i)_{i\in[0,k]}$ eine Semisubnormalreihe von H. Dann ist $\big(f^{-1}(H_i)\big)_i$ eine Semisubnormalreihe von G.*

Ferner gibt es für $i \in [1,k]$ einen injektiven Gruppenmorphismus

$$\begin{array}{rcl} f^{-1}(H_i)/f^{-1}(H_{i-1}) & \xrightarrow{\bar{f}_i} & H_i/H_{i-1} \\ xf^{-1}(H_{i-1}) & \longmapsto & f(x)H_{i-1} \,. \end{array}$$

Ist f surjektiv, so ist dies ein Isomorphismus für alle $i \in [1,k]$.

Beweis. Sei $i \in [1,k]$. Es ist $f^{-1}(H_i) \leqslant G$; vgl. Lösung zu Aufgabe 37.(4). Betrachten wir den Gruppenmorphismus

$$\begin{array}{rcl} f^{-1}(H_i) & \xrightarrow{f_i} & H_i/H_{i-1} \\ x & \longmapsto & f(x)H_{i-1} \,. \end{array}$$

Es liegt x in dessen Kern genau dann, wenn $f(x) \in H_{i-1}$, also genau dann, wenn $x \in f^{-1}(H_{i-1})$. Insbesondere ist $f^{-1}(H_{i-1}) \trianglelefteqslant f^{-1}(H_i)$; vgl. auch Aufgabe 37.(4). Eine Anwendung von Aufgabe 42.(2) auf f_i gibt nun den injektiven Gruppenmorphismus $\bar{f}_i$ wie oben behauptet.

Sei dazuhin f surjektiv. Wir haben $\bar{f}_i$ als surjektiv nachzuweisen. Sei $yH_{i-1} \in H_i/H_{i-1}$. Sei $x \in G$ mit $f(x) = y$. Dann ist $x \in f^{-1}(H_i)$ und $\bar{f}_i(xf^{-1}(H_{i-1})) = f(x)H_{i-1} = yH_{i-1}$. ▫

Lemma. *Sei G eine auflösbare Gruppe. Sei $U \leqslant G$ eine Untergruppe. Dann ist U auflösbar.*

Beweis. Sei $U \overset{\iota}{\longrightarrow} G$ der Einbettungsmorphismus. Sei $(G_i)_i$ eine Subnormalreihe von G mit allen Subfaktoren abelsch. Mit vorstehender Bemerkung ist $(U \cap G_i)_i = \big(\iota^{-1}(G_i)\big)_i$ eine Semisubnormalreihe von H mit $(U \cap G_i)/(U \cap G_{i-1})$ isomorph zu einer Untergruppe von G_i/G_{i-1}, und somit insbesondere abelsch für $i \in [1,k]$. Schließlich ist $U \cap G_0 = U \cap \{1\} = \{1\}$, so daß $(U \cap G_i)_i$ eine Subnormalreihe ist. ▫

Eine Gruppe heiße *zyklisch,* falls sie von einem Element erzeugt ist. Zyklische Gruppen sind insbesondere abelsch.

Lemma. *Sei G eine auflösbare Gruppe. Dann hat G eine Subnormalreihe $(G_i)_i$ so, daß G_i/G_{i-1} zyklisch ist.*

Beweis. Betrachten wir zunächst den speziellen *Fall* einer abelschen Gruppe G. Wir führen eine Induktion über $|G|$, nehmen also an, daß die Aussage für alle abelschen Gruppen kleinerer Ordnung gezeigt ist. Für $\{1\} = G$ ist nichts zu zeigen. Sei also $\{1\} < G$, und sei $x \in G \smallsetminus \{1\}$. Nach Induktionsvoraussetzung existiert eine Subnormalreihe der abelschen Gruppe $G/\langle x\rangle$ mit allen Subfaktoren zyklisch. Ihr Urbild in G ist mit vorstehender Bemerkung eine Semisubnormalreihe in G mit Anfangsterm $\langle x\rangle$ und allen Subfaktoren zyklisch. Nehmen wir zu dieser noch den Term $\{1\}$ hinzu, so erhalten wir eine Subnormalreihe von G mit allen Subfaktoren zyklisch.

Betrachten wir nun den allgemeinen *Fall* einer auflösbaren Gruppe G. Wieder führen wir eine Induktion nach $|G|$. Sei $(G_i)_{i\in[0,k]}$ eine Subnormalreihe von G mit allen Subfaktoren abelsch. Ohne Einschränkung ist $k \geqslant 1$ und $G_{k-1} \neq G_k = G$.

Da auch G_{k-1} auflösbar ist, hat G_{k-1} nach Induktionsvoraussetzung eine Subnormalreihe mit allen Subfaktoren zyklisch.

Die abelsche Gruppe G/G_{k-1} hat mit dem abgehandelten speziellen Fall eine Subnormalreihe mit allen Subfaktoren zyklisch. Bilden wir deren Urbild unter $G \longrightarrow G/G_{k-1}$, $g \longmapsto gG_{k-1}$, so erhalten wir nach vorstehender Bemerkung eine Semisubnormalreihe von G mit allen Subfaktoren zyklisch und mit Anfangsterm G_{k-1}.

Aneinanderfügen jener Subnormalreihe von G_{k-1} mit dieser Semisubnormalreihe von G gibt eine Subnormalreihe von G mit allen Subfaktoren zyklisch. ▫

Bemerkung. *Sei $G \overset{f}{\longrightarrow} H$ ein Gruppenmorphismus. Sei $(G_i)_{i\in[1,k]}$ eine Subnormalreihe von G. Dann ist $\big(f(G_i)\big)_i$ eine Subnormalreihe von $f(G)$. Ferner gibt es einen surjektiven Gruppenmorphismus*

$$\begin{array}{rcl} G_i/G_{i-1} & \overset{\tilde{f}_i}{\longrightarrow} & f(G_i)/f(G_{i-1}) \\ xG_{i-1} & \longmapsto & f(x)f(G_{i-1}) \end{array}$$

für $i \in [1,k]$.

Beweis. Sei $i \in [1,k]$. Es ist $f(G_i) \leqslant H$; vgl. Aufgabe 37.(1). Zeigen wir, daß

$f(G_{i-1}) \trianglelefteq f(G_i)$. Sei $y \in G_{i-1}$. Sei $x \in G_i$. In der Tat ist ${}^{f(x)}f(y) = f({}^{x}y) \in f(G_{i-1})$.

Ferner ist der Anfangsterm von $\big(f(G_i)\big)_i$ gleich $f(G_0) = \{1\}$.

Wir haben den surjektiven Gruppenmorphismus

$$\begin{array}{rcl} G_i & \longrightarrow & f(G_i)/f(G_{i-1}) \\ x & \longmapsto & f(x)f(G_{i-1}) \ . \end{array}$$

Sind $x, \tilde{x} \in G_i$ gegeben mit $xG_{i-1} = \tilde{x}G_{i-1}$, d.h. $x^{-1}\tilde{x} \in G_{i-1}$, so ist $f(x)f(G_{i-1}) = f(\tilde{x})f(G_{i-1})$, da $f(x)^{-1}f(\tilde{x}) = f(x^{-1}\tilde{x}) \in f(G_{i-1})$. Also ist $\tilde{f}_i$ wohldefiniert. Ersichtlich ist auch $\tilde{f}_i$ ein surjektiver Gruppenmorphismus. □

Lemma. *Sei G eine auflösbare Gruppe. Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus. Dann ist auch $f(G)$ auflösbar.*

Beweis. Ist $(G_i)_i$ eine Subnormalreihe von G mit allen Subfaktoren abelsch, so ist mit vorstehender Bemerkung $\big(f(G_i)\big)_i$ eine Subnormalreihe von $f(G)$. Da G_i/G_{i-1} stets abelsch ist, und da es einen surjektiven Gruppenmorphismus von G_i/G_{i-1} nach $f(G_i)/f(G_{i-1})$ gibt, ist auch $f(G_i)/f(G_{i-1})$ stets abelsch; vgl. Aufgabe 42.(2). □

Zusammenfassung. *Sei G eine auflösbare Gruppe.*

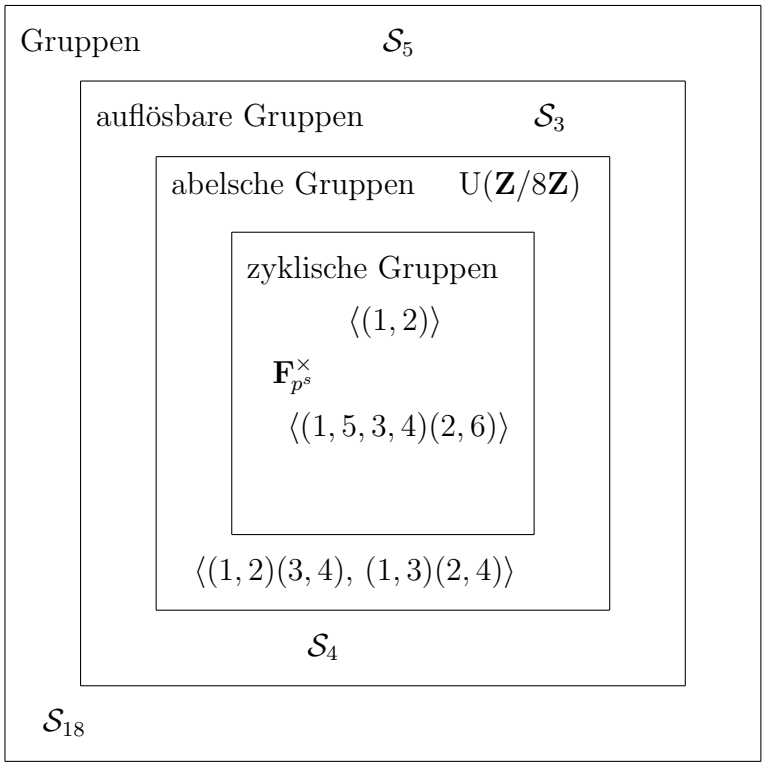
(1) *Untergruppen von G sind auflösbar.*

(2) *Bilder von G unter Gruppenmorphismen sind auflösbar.*

(3) *Es gibt eine Subnormalreihe von G mit allen Subfaktoren zyklisch, d.h. von einem Element erzeugt.*

4.2 Ein paar Gruppen

Stellen wir einmal ein paar typische Beispiele für endliche Gruppen in einem Bild zusammen. Ohne Anspruch auf Vollständigkeit!



Zu $\langle(1,2)(3,4),\ (1,3)(2,4)\rangle$, vgl. §4.1, Bemerkung zur Vorsicht.

Zu $\mathbf{F}_{p^s}^\times$ mit p prim, $s \geqslant 1$, vgl. Lemma aus §2.5.4 und Aufgabe 27.(5).

Zu $\mathrm{U}(\mathbf{Z}/8\mathbf{Z})$, vgl. Aufgabe 44.(2).

4.3 Auflösbare Erweiterungen, auflösbare Polynome

Sei K ein perfekter Körper.

4.3.1 Auflösbare Erweiterungen

Definition. Sei $L|K$ eine Körpererweiterung. Ein Element $x \in L$ heiße *radiziell* über K, falls es ein $m \geqslant 1$ gibt mit $x^m \in K$ (lat. radix, die Wurzel).

Beispiel. Es ist $\sqrt[3]{2} \in \mathbf{C}$ radiziell über $\mathbf{Q}$, da $(\sqrt[3]{2})^6 = 4 \in \mathbf{Q}$ (wobei der Exponent 3 natürlich auch gereicht hätte).

Beispiel. Es ist $\sqrt{2}+1 \in \mathbf{C}$ nicht radiziell über $\mathbf{Q}$. In der Tat ist $(\sqrt{2}+1)^k = a_k\sqrt{2}+b_k$ für $k \geqslant 1$, wobei $a_{k+1} = 2a_k + b_k$ und $b_{k+1} = a_k + b_k$. Mit Induktion erkennt man, daß $a_k > 0$ und $b_k > 0$ stets. Insbesondere ist $(\sqrt{2}+1)^k \notin \mathbf{Q}$ stets.

Definition. Eine endliche Körpererweiterung $L|K$ heiße *auflösbar,* wenn es ein $k \geqslant 0$ sowie Teilkörper $K_0, \ldots, K_k$ von L so gibt, daß

$$K \;=\; K_0 \;\subseteq\; K_1 \;\subseteq\; K_2 \;\subseteq\; K_3 \;\subseteq\; \cdots \;\subseteq\; K_{k-1} \;\subseteq\; K_k \;=\; L$$

und daß für alle $i \in [1,k]$ ein radizielles $a_i \in K_i$ über K_{i-1} existiert mit

$$K_i \;=\; K_{i-1}(a_i)\;.$$

Insgesamt ist dann also $L = K(a_1, \ldots, a_k)$, und a_i radiziell über $K(a_1, \ldots, a_{i-1})$ für $i \in [1,k]$.

Beispiel. Wegen der Kette

$$\mathbf{Q} \;\subseteq\; \mathbf{Q}(\sqrt[4]{2}) \;\subseteq\; \mathbf{Q}(\sqrt[4]{2},\; \sqrt[3]{\sqrt{2}-1})$$

ist $\mathbf{Q}(\sqrt[4]{2},\; \sqrt[3]{\sqrt{2}-1}) \,|\, \mathbf{Q}$ auflösbar.

> Ist $L|K$ auflösbar, so ist jedes Element von L ein "iterierter Wurzelausdruck" von Elementen von K.

Bemerkung. Seien $M|L|K$ endliche Erweiterungen. Ist $M|L$ auflösbar und $L|K$ auflösbar, so ist auch $M|K$ auflösbar.

Lemma. *Sei $L|K$ eine auflösbare endliche Erweiterung. Es gibt eine endliche Erweiterung $M|L$ mit $M|K$ auflösbar und galoisch.*

Beweis. Wir verwenden Induktion über $[L:K]$. Ist $L = K$, so kann man $M = L$ wählen.

Sei $L \neq K$. Sei $L|\tilde{L}|K$ mit $[L:\tilde{L}] > 1$, mit $L = \tilde{L}(b)$ und mit b radiziell über $\tilde{L}$. Sei $m \geqslant 1$ mit $b^m \in \tilde{L}$. Nach Induktionsvoraussetzung gibt es ein $\tilde{M}|\tilde{L}$ mit $\tilde{M}|K$ auflösbar und galoisch.

Sei

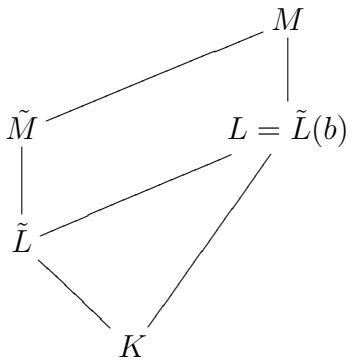
$$f(X) \;:=\; \textstyle\prod_{\sigma\in\mathrm{Gal}(\tilde{M}|K)}(X^m - \sigma(b^m)) \;\in\; \tilde{L}[X]\;.$$

Für $\rho \in \mathrm{Gal}(\tilde{M}|K)$ ist

$$\begin{array}{rcl} f^\rho(X) & = & \big(\prod_{\sigma\in\mathrm{Gal}(\tilde{M}|K)}(X^m - \sigma(b^m))\big)^\rho \\ & = & \prod_{\sigma\in\mathrm{Gal}(\tilde{M}|K)}(X^m - \sigma(b^m))^\rho \\ & = & \prod_{\sigma\in\mathrm{Gal}(\tilde{M}|K)}(X^m - \rho(\sigma(b^m))) \\ & \overset{\sigma' = \rho\circ\sigma}{=} & \prod_{\sigma'\in\mathrm{Gal}(M|K)}(X^m - \sigma'(b^m)) \\ & = & f(X)\;, \end{array}$$

und mithin $f(X) \in K[X]$; vgl. erste Bemerkung in §3.5.1.4. Sei $\hat{f}(X) \in K[X]$ das Produkt der Menge der normierten irreduziblen Faktoren von $f(X)$.

Sei M der Zerfällungskörper von $\hat{f}(X)$ über $\tilde{M}$. Da $\hat{f}(b) = 0$ in L, ist $\mu_{\tilde{L},b}(X)$ ein Teiler von $\hat{f}(X)$ in $\tilde{L}[x]$; vgl. Satz 2.(2). Also gibt es eine Nullstelle $\hat{b}$ von $\hat{f}(X)$ in M mit $\mu_{\tilde{L},b}(\hat{b}) = 0$. Somit gibt es einen Körpermorphismus von $L = \tilde{L}(b)$ nach M, der auf $\tilde{L}$ identisch einschränkt; vgl. Folgerung zu Satz 3. Wir fixieren einen solchen Morphismus und identifizieren ein Element in L mit seinem Bild in M. Also $M|L$.



Wegen $\hat{f}(X) \in K[X]$ ist $M|K$ galoisch; vgl. Aufgabe 45.(2).

Da $\tilde{M}|K$ auflösbar ist, bleibt zu zeigen, daß $M|\tilde{M}$ auflösbar ist. Seien $\gamma_1, \ldots, \gamma_k$ die Nullstellen von $f(X)$ in M. Es ist $M = \tilde{M}(\gamma_1, \ldots, \gamma_k)$. Für $i \in [1, k]$ ist $\gamma_i^m = \sigma(b^m)$ für ein $\sigma \in \mathrm{Gal}(\tilde{M}|K)$. Nun ist aber $\sigma(b^m) \in \sigma(\tilde{L}) \subseteq \tilde{M}$. Insgesamt ist γ_i radiziell über $\tilde{M}$, und so a fortiori radiziell über $\tilde{M}(\gamma_1, \ldots, \gamma_{i-1})$. Somit zeigt die Kette

$$\tilde{M} \subseteq \tilde{M}(\gamma_1) \subseteq \cdots \subseteq \tilde{M}(\gamma_1, \ldots, \gamma_{k-1}) \subseteq \tilde{M}(\gamma_1, \ldots, \gamma_{k-1}, \gamma_k) = M ,$$

daß $M|\tilde{M}$ auflösbar ist. □

4.3.2 Auflösbare Polynome

Definition. Sei $f(X) \in K[X]$ irreduzibel und normiert. Es heiße $f(X)$ *auflösbar,* wenn es eine auflösbare endliche Körpererweiterung $L|K$ gibt, für welche ein $b \in L$ mit $f(b) = 0$ existiert.

Beispiel. Sei $K = \mathbf{Q}$. Es ist das irreduzible Polynom

$$X^{12} + 4X^9 - 6X^8 - 48X^7 + 2X^6 + 96X^5 - 12X^4 - 164X^3 + 108X^2 + 24X - 23 \in \mathbf{Q}[X]$$

auflösbar, da, wie leicht zu verifizieren,

$$f\big(\sqrt[4]{2} + \sqrt[3]{\sqrt{2} - 1}\big) = 0 ,$$

und da, wie bereits festgestellt, $\mathbf{Q}(\sqrt[4]{2}, \sqrt[3]{\sqrt{2} - 1}) \,|\, \mathbf{Q}$ auflösbar ist; vgl. drittes Beispiel in §4.3.1.

Informell gesprochen heißt ein irreduzibles normiertes Polynom also auflösbar, wenn es eine Nullstelle hat, die sich als "iterierter Wurzelausdruck" von Elementen des Grundkörpers schreiben läßt.

4.4 Auflösbarkeitskriterien für Polynome

Sei K ein Körper mit $\operatorname{char} K = 0$. Insbesondere ist K perfekt.

Der Grund für diese einschränkende Bedingung ist in Aufgabe 44 zu suchen.

4.4.1 Erweitern um ein radizielles Element

Sei $n \geqslant 1$. Zerfalle $X^n - 1 \in K[X]$ in ein Produkt von Linearfaktoren.

Gemäß Aufgabe 44.(1) gibt es ein Element $\zeta_n \in K$ mit $\langle \zeta_n \rangle = \{z \in K \ : \ z^n = 1\}$ und $\mathrm{o}(\zeta_n) = n$.

Lemma. *Sei $K(b)|K$ eine endliche monogene Erweiterung mit $b^n \in K$. Dann ist $K(b)|K$ galoisch. Ferner gibt es einen injektiven Gruppenmorphismus von $\mathrm{Gal}(K(b)|K)$ nach $(\mathbf{Z}/n\mathbf{Z}, +)$. Insbesondere ist $\mathrm{Gal}(K(b)|K)$ abelsch.*

Beweis. Ohne Einschränkung ist $b \neq 0$. Schreibe $a := b^n \in K$. Da $\zeta_n^i b$ für $i \in [0, n-1]$ eine Nullstelle von $X^n - a \in K[X]$ ist, und da $\zeta_n^i b \neq \zeta_n^j b$ für $i, j \in [0, n-1]$ mit $i \neq j$, zerfällt

$$X^n - a \ = \ \textstyle\prod_{i \in [0,n-1]} (X - \zeta_n^i b) \ \in \ K(b)[X] \ .$$

Insbesondere ist $K(b)$ Zerfällungskörper von $X^n - a$, welches in $K[X]$ in verschiedene normierte irreduzible Faktoren zerlegt werden kann. Somit ist $K(b)|K$ galoisch; vgl. zweites Lemma in §3.5.1.4.

Sei $\sigma \in \mathrm{Gal}(K(b)|K)$. Beachte, daß $\sigma(b)^n - a = \sigma(b^n - a) = 0$. Wähle ein $j_\sigma \in \mathbf{Z}$ mit $\sigma(b) = \zeta_n^{j_\sigma} b$. Dies eine Abbildung

$$\begin{array}{rcl} \mathrm{Gal}(K(b)|K) & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ \sigma & \longmapsto & j_\sigma + n\mathbf{Z} \ . \end{array}$$

Das Bild hängt wegen $\mathrm{o}(\zeta_n) = n$ auch nicht von der getroffenen Wahl ab. In anderen Worten, ist $\sigma(b) = \zeta_n^j b$, so ist $j \equiv_n j_\sigma$.

Zeigen wir, daß ein Gruppenmorphismus vorliegt. Seien $\sigma, \tilde{\sigma} \in \mathrm{Gal}(K(b)|K)$. Dann wird

$$\zeta_n^{j_{\sigma\circ\tilde{\sigma}}} \ = \ (\sigma \circ \tilde{\sigma})(b) \ = \ \sigma(\zeta_n^{j_{\tilde{\sigma}}} b) \ = \ \zeta_n^{j_{\tilde{\sigma}}} \sigma(b) \ = \ \zeta_n^{j_{\tilde{\sigma}}} \zeta_n^{j_\sigma} b \ = \ \zeta_n^{j_\sigma + j_{\tilde{\sigma}}} b \ ,$$

und also $j_{\sigma\circ\tilde{\sigma}} \equiv_n j_\sigma + j_{\tilde{\sigma}}$.

Zeigen wir, daß dieser Gruppenmorphismus injektiv ist. Dazu zeigen wir, daß sein Kern gleich $\{\mathrm{id}_{K(b)}\}$ ist; vgl. letzte Bemerkung aus §3.2. Ist $\sigma \in \mathrm{Gal}(K(b)|K)$ mit $j_\sigma \equiv_n 0$ gegeben, so wird $\sigma(b) = \zeta_n^{j_\sigma} = \zeta_n^0 b = b$. Also ist $\sigma = \mathrm{id}_{K(b)}$; vgl. dritte Bemerkung aus §3.4.1. ▫

Lemma. *Sei $L|K$ eine endliche galoische Erweiterung mit $[L : K] = m$ so, daß m ein Teiler von n ist und daß $\mathrm{Gal}(L|K) = \langle \sigma \rangle$ für ein $\sigma \in \mathrm{Gal}(L|K)$. Dann gibt es ein $b \in L$ mit $b^m \in K$ und $L = K(b)$.*

Beweis. Es ist $\mathrm{o}(\sigma) = [L : K] = m$. Insbesondere ist $\sigma^i \neq \sigma^j$ für $i, j \in [0, m-1]$ mit $i \neq j$.

Schreibe $\zeta_m := \zeta_n^{n/m} \in K$. Es ist $\mathrm{o}(\zeta_m) = m$; vgl. Aufgabe 27.(2).

Mit Satz 7 (Dedekinds Lemma) aus §3.5.1 gibt es ein $x \in L$ mit

$$b \;:=\; \textstyle\sum_{i\in[0,m-1]} \zeta_m^{-i}\sigma^i(x) \;\neq\; 0\;.$$

Zeigen wir, daß $K(b) = L$. Es genügt wegen $[L : K] = m$ zu zeigen, daß $[K(b) : K] \overset{!}{\geqslant} m$. Dafür wiederum genügt es, m verschiedene Nullstellen von $\mu_{b,K}(X)$ in L anzugeben. Da aber $b \neq 0$, ist $\zeta_m^i b \neq \zeta_m^j b$ für $i, j \in [0, m-1]$ mit $i \neq j$. Für $j \in \mathbf{Z}$ ist ferner

$$\begin{array}{rcl}
\zeta_m^j b & = & \zeta_m^j \sum_{i\in[0,m-1]} \zeta_m^{-i}\sigma^i(x) \\
& = & \sum_{i\in[0,m-1]} \zeta_m^{-(i-j)}\sigma^i(x) \\
\overset{i' = i-j}{} & = & \sum_{i'\in[-j,m-1-j]} \zeta_m^{-i'}\sigma^{i'+j}(x) \\
& = & \sigma^j\big(\sum_{i'\in[-j,m-1-j]} \zeta_m^{-i'}\sigma^{i'}(x)\big) \\
\overset{\mathrm{o}(\zeta_m)=\mathrm{o}(\sigma)=m}{} & = & \sigma^j\big(\sum_{i'\in[0,m-1]} \zeta_m^{-i'}\sigma^{i'}(x)\big) \\
& = & \sigma^j(b)\;.
\end{array}$$

Also

$$\mu_{b,K}(\zeta_m^j b) \;=\; \mu_{b,K}(\sigma^j(b)) \;=\; \sigma^j\big(\mu_{b,K}(b)\big) \;=\; \sigma(0) \;=\; 0\;.$$

Zeigen wir, daß $b^m \in K$. Es ist, wie eben nachgerechnet,

$$\sigma^j(b^m) \;=\; \sigma^j(b)^m \;=\; (\zeta_m^j b)^m = \zeta_m^{mj} b^m \;=\; b^m$$

für alle $j \in \mathbf{Z}$. Also ist $b^m \in \mathrm{Fix}_{\langle\sigma\rangle} L = \mathrm{Fix}_{\mathrm{Gal}(K(b)|K)} L = K$; vgl. die erste Bemerkung in §3.5.1.4. ▫

4.4.2 Der Satz von Galois

Sei daran erinnert, daß $\mathrm{char}\, K = 0$.

Den Auflösbarkeitsbegriff für irreduzible und normierte Polynome und endliche Erweiterungen findet man in §4.3.2.

Den Auflösbarkeitsbegriff für endliche Gruppen findet man in §4.1.

Die Definition der Galoisgruppe eines Polynoms als Galoisgruppe der zugehörigen Zerfällungskörpererweiterung findet man in §3.4.1.

Satz 10 (Satz von Galois) *Sei $f(X) \in K[X]$ irreduzibel und normiert.*

Es ist $f(X)$ auflösbar genau dann, wenn $\mathrm{Gal}(f(X))$ *auflösbar ist.*

Beweis.

Sei zum einen $f(X)$ auflösbar. Sei $L|K$ eine auflösbare endliche Erweiterung, und sei $y \in L$ mit $f(y) = 0$. Ohne Einschränkung ist $L|K$ galoisch; cf. Lemma aus §4.3.1.

Sei nun $L = K(b_1, \ldots, b_\ell)$ mit $b_i^{n_i} \in K(b_1, \ldots, b_{i-1})$ für $i \in [1, \ell]$, wobei $n_i \geqslant 1$. Sei $n := \mathrm{kgV}(n_1, \ldots, n_\ell)$. Dann ist auch $b_i^n \in K(b_1, \ldots, b_{i-1})$ für $i \in [1, \ell]$.

Sei $L(\zeta_n)$ der Zerfällungskörper von $X^n - 1$ über L, wobei $\mathrm{o}(\zeta_n) = n$; vgl. Aufgabe 44.(1). Es ist $L(\zeta_n)|K$ galoisch; vgl. Aufgabe 45.(2). Wir haben die Kette

$$K \subseteq K(\zeta_n) \subseteq K(\zeta_n, b_1) \subseteq K(\zeta_n, b_1, b_2) \subseteq \cdots \subseteq K(\zeta_n, b_1, \ldots, b_k) = L(\zeta_n) ,$$

von Zwischenkörpern, die der Kette von Untergruppen

$$\mathrm{Gal}(L(\zeta_n)|K) \geqslant \mathrm{Gal}(L(\zeta_n)|K(\zeta_n)) \geqslant \mathrm{Gal}(L(\zeta_n)|K(\zeta_n, b_1)) \geqslant \mathrm{Gal}(L(\zeta_n)|K(\zeta_n, b_1, b_2)) \geqslant \cdots \geqslant \{\mathrm{id}_{L(\zeta_n)}\}$$

entspricht; vgl. Satz 9 (Hauptsatz der Galoistheorie), §3.5.2.

Es ist $K(\zeta_n)|K$ galoisch mit abelscher Galoisgruppe; vgl. Aufgabe 44.(3). Also ist

$$\mathrm{Gal}(L(\zeta_n)|K) \trianglerighteqslant \mathrm{Gal}(L(\zeta_n)|K(\zeta_n))$$

mit abelscher Faktorgruppe $\mathrm{Gal}(K(\zeta_n)|K)$; vgl. Satz 9.

Für $i \in [1, \ell]$ ist $K(\zeta_n, b_1, \ldots, b_i)|K(\zeta_n, b_1, \ldots, b_{i-1})$ galoisch mit abelscher Galoisgruppe; vgl. Lemma aus §4.4.1. Also ist

$$\mathrm{Gal}(L(\zeta_n)|K(\zeta_n, b_1, \ldots, b_i)) \trianglerighteqslant \mathrm{Gal}(L(\zeta_n)|K(\zeta_n, b_1, \ldots, b_{i-1}))$$

mit abelscher Faktorgruppe $\mathrm{Gal}(K(\zeta_n, b_1, \ldots, b_i)|K(\zeta_n, b_1, \ldots, b_{i-1}))$; vgl. Satz 9.

Somit ist $\mathrm{Gal}(L(\zeta_n)|K)$ auflösbar.

Da $f(X)$ eine Nullstelle y in L hat, zerfällt

$$f(X) = (X - \gamma_1)(X - \gamma_2) \cdots (X - \gamma_k) \in L[X]$$

in Linearfaktoren, wobei $y = \gamma_1$; vgl. erstes Lemma in §3.5.1.4. Somit ist der Teilkörper $L_0 := K(\gamma_1, \ldots, \gamma_k)$ in $L(\zeta_n)$ ein Zerfällungskörper von $f(X)$ über K, insbesondere also galoisch über K; vgl. zweites Lemma in §3.5.1.4.

Also ist $\mathrm{Gal}(f(X)) = \mathrm{Gal}(L_0|K) \simeq \mathrm{Gal}(L(\zeta_n)|K)/\mathrm{Gal}(L(\zeta_n)|L_0)$. Da $\mathrm{Gal}(L(\zeta_n)|K)$ auflösbar ist, folgt dies auch für $\mathrm{Gal}(f(X))$; vgl. Zusammenfassung in §4.1, Teil (2).

Sei zum anderen $\mathrm{Gal}(f(X))$ *auflösbar.* Sei L der Zerfällungskörper von $f(X)$ über K. Es ist $L|K$ galoisch; vgl. zweites Lemma in §3.5.1.4. Es ist $\mathrm{Gal}(f(X)) = \mathrm{Gal}(L|K)$.

Sei $n := [L : K]$. Sei $L(\zeta_n)$ der Zerfällungskörper von $X^n - 1$ über L, wobei $\mathrm{o}(\zeta_n) = n$; vgl. Aufgabe 44.(1). Es ist $L(\zeta_n)|K$ galoisch; vgl. Aufgabe 45.(2).

Da $f(X)$ eine Nullstelle in $L(\zeta_n)$ hat, genügt es zu zeigen, daß $L(\zeta_n)|K$ auflösbar ist.

Da ζ_n über K radiziell ist, ist $K(\zeta_n)|K$ auflösbar. Also genügt es zu zeigen, daß $L(\zeta_n)|K(\zeta_n)$ auflösbar ist.

Wir haben ein Kompositum von Gruppenmorphismen

$$\mathrm{Gal}(L(\zeta_n)|K(\zeta_n)) \hookrightarrow \mathrm{Gal}(L(\zeta_n)|K) \longrightarrow \mathrm{Gal}(L|K)\ ,$$

welches insgesamt $\sigma \in \mathrm{Gal}(L(\zeta_n)|K(\zeta_n))$ auf $\sigma|_L^L \in \mathrm{Gal}(L|K)$ abbildet. Der Kern ist gleich $\mathrm{Gal}(L(\zeta_n)|L) \cap \mathrm{Gal}(L(\zeta_n)|K(\zeta_n))$. Ein Automorphismus von $L(\zeta_n)$, der aber sowohl auf L identisch einschränkt als auch ζ_n auf ζ_n schickt, ist bereits die Identität; vgl. dritte Bemerkung in §3.4.1. Also ist der Kern gleich $\{\mathrm{id}_{L(\zeta_n)}\}$, und unser Kompositum somit injektiv. Da $\mathrm{Gal}(L|K)$ auflösbar ist, gilt dies auch für $G := \mathrm{Gal}(L(\zeta_n)|K(\zeta_n))$; vgl. Zusammenfassung in §4.1, Teil (1).

Sei

$$\{\mathrm{id}_{L(\zeta_n)}\} \;=\; G_0 \;\trianglelefteq\; G_1 \;\trianglelefteq\; \cdots \;\trianglelefteq\; G_k \;=\; G$$

eine Subnormalreihe mit allen Subfaktoren G_i/G_{i-1} zyklisch; vgl. Zusammenfassung in §4.1, Teil (3). Diese entspricht der Kette von Zwischenkörpern

$$L(\zeta_n) \;=\; \mathrm{Fix}_{G_0} L(\zeta_n) \;\supseteq\; \mathrm{Fix}_{G_1} L(\zeta_n) \;\supseteq\; \cdots \;\supseteq\; \mathrm{Fix}_{G_k} L(\zeta_n) \;=\; K(\zeta_n)\ ;$$

vgl. Satz 9, vgl. erste Bemerkung in §3.5.1.4. Da $G_{i-1} \trianglelefteq G_i$, ist $\mathrm{Fix}_{G_{i-1}} L(\zeta_n)|\,\mathrm{Fix}_{G_i} L(\zeta_n)$ galoisch mit zyklischer Galoisgruppe G_i/G_{i-1}; vgl. Satz 9.

Beachte, daß $|G_i/G_{i-1}| = |G_i|/|G_{i-1}|$ gemäß Aufgabe 38.(1.c) ein Teiler von $|G| = |\,\mathrm{Gal}(L(\zeta_n)|K(\zeta_n))|$ ist, was wiederum, via unseres injektiven Kompositums, ein Teiler von $|\,\mathrm{Gal}(L|K)| = [L : K] = n$ ist. Mit dem zweiten Lemma aus §4.4.1 folgt also, daß $\mathrm{Fix}_{G_{i-1}} L(\zeta_n) = \mathrm{Fix}_{G_i} L(\zeta_n)(b_i)$ für ein b_i radiziell über $\mathrm{Fix}_{G_i} L(\zeta_n)$. Also ist in der Tat $L(\zeta_n)|K(\zeta_n)$ auflösbar. ▫

4.4.3 Der Satz von Abel

Sei daran erinnert, daß $\mathrm{char}\, K = 0$.

Wir betrachten den Körper $\hat{K} := K(Y_0, \ldots, Y_{n-1}) = \mathrm{frac}\, K[Y_0, \ldots, Y_{n-1}]$.

Lemma. *Das Polynom $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0 \in \hat{K}[X]$ ist irreduzibel.*
Sein Zerfällungskörper hat Grad $n!$ über $\hat{K}$.

Beweis. Sei $\hat{E}$ der Zerfällungskörper von $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0$ über $\hat{K}$. Gemäß Aufgabe 50 genügt es auch für die behauptete Irreduzibilität zu zeigen, daß $[\hat{E} : \hat{K}] \stackrel{!}{=} n!$.

Sei $E := K(T_1, \ldots, T_n) \mid K(s_0, \ldots, s_{n-1}) =: L$ wie in Aufgabe 43, also

$$(*) \qquad \textstyle\sum_{i\in[0,n]} (-1)^{n-i} s_i X^i \;=\; (X - T_1) \cdots (X - T_n)\ .$$

Nach Aufgabe 43.(3, 4) ist $[E : L] = n!$. Mit der L-Basis aus Aufgabe 43.(4) sieht man, daß $E|L$ eine endliche und von den Nullstellen T_i erzeugte Erweiterung ist, so daß E auch der Zerfällungskörper von $\sum_{i\in[0,n]} (-1)^{n-i} s_i X^i$ über L ist.

Zerlege

$$X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0 \;=\; (X-\xi_1)\cdots(X-\xi_n) \;\in\; \hat{E}[X]\,.$$

Insbesondere ist

$$(**) \qquad (-1)^{n-i}s_i(\xi_1,\ldots,\xi_n) \;=\; Y_i$$

für $i \in [0,n-1]$, wie sich durch Einsetzen von ξ_i für T_i für $i \in [1,n]$ aus $(*)$ und nachfolgendem Koeffizientenvergleich ergibt.

Sei $K[s_0,\ldots,s_{n-1}] := \{f(s_0,\ldots,s_{n-1}) \;:\; f(X_0,\ldots,X_{n-1}) \in K[X_0,\ldots,X_{n-1}]\}$; dies ist ein Teilring von L.

Mit der Gebrauchsanweisung für Polynomringe aus §1.6.2 erhalten wir einen Ringmorphismus

$$\begin{array}{rcll} K[Y_1,\ldots,Y_n] & \xrightarrow{\varphi} & K[s_0,\ldots,s_{n-1}] & \\ Y_i & \longmapsto & (-1)^{n-i}s_i & \text{für } i \in [0,n-1]\,, \end{array}$$

welcher auf K identisch einschränkt, und welcher nach Konstruktion surjektiv ist.

Mit ebendieser Gebrauchsanweisung erhalten wir auch einen (Hilfs-)Ringmorphismus

$$\begin{array}{rcll} K[T_1,\ldots,T_n] & \xrightarrow{\psi} & \hat{E} & \\ Y_i & \longmapsto & \xi_i & \text{für } i \in [1,n]\,, \end{array}$$

welcher auf K identisch einschränkt. Es wird

$$\psi(\varphi(Y_i)) \;=\; \psi((-1)^{n-i}s_i) \;=\; (-1)^{n-i}s_i(\xi_1,\ldots,\xi_n) \;\overset{(**)}{=}\; Y_i$$

für $i \in [0,n-1]$. Also ist $\psi|_{K[s_0,\ldots,s_{n-1}]} \circ \varphi$ die Inklusionsabbildung

$$K[Y_1,\ldots,Y_n] \;\hookrightarrow\; \hat{K} \;\hookrightarrow\; \hat{E}\,.$$

Insbesondere ist φ injektiv, und insgesamt ein Ringisomorphismus.

Mit der Gebrauchsanweisung für Quotientenkörper aus §1.10.2 gibt es einen Körpermorphismus

$$\hat{K} \;=\; K(Y_0,\ldots,Y_{n-1}) \;\xrightarrow{\varphi'}\; K(s_0,\ldots,s_{n-1}) \;=\; L$$

mit $\varphi'|^{K[s_0,\ldots,s_{n-1}]}_{K[Y_0,\ldots,Y_{n-1}]} = \varphi$. Als Körpermorphismus ist φ' injektiv. Da $s_i \in \varphi(K[Y_0,\ldots,Y_{n-1}]) \subseteq \varphi'(K(Y_0,\ldots,Y_{n-1}))$ für $i \in [0,n-1]$, und da damit auch jeder Bruch von polynomialen Ausdrücken in den s_i mit Koeffizienten in K im Bild von φ' liegt, ist φ' auch surjektiv. Insgesamt ist φ' ein Körperisomorphismus.

Es ist $(X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0)^\varphi = \sum_{i\in[0,n]}(-1)^{n-i}s_iX^i$. Mit der Behauptung aus dem Beweis zu Satz 5 gibt es also einen Isomorphismus der jeweiligen Zerfällungskörper

$$\hat{E} \;\xrightarrow[\sim]{\varphi''}\; E$$

mit $\varphi''|^L_{\hat{K}} = \varphi'$.

$$\begin{array}{ccc} \hat{E} & \xrightarrow[\sim]{\varphi''} & K(T_1,\ldots,T_n) = E \\ \uparrow & & \uparrow \\ \hat{K} = K(Y_0,\ldots,Y_{n-1}) & \xrightarrow[\sim]{\varphi'} & K(s_0,\ldots,s_{n-1}) = L \\ \uparrow & & \uparrow \\ K[Y_0,\ldots,Y_{n-1}] & \xrightarrow[\sim]{\varphi} & K[s_0,\ldots,s_{n-1}] \end{array}$$

Nun ist $\dim_L E = n!$. Faßt man E via φ' als $\hat{K}$-Vektorraum auf, so wird auch $\dim_{\hat{K}} E = n!$, da φ' ein Isomorphismus ist. Das obere kommutative Viereck im Diagramm zeigt nun, daß $\hat{E} \xrightarrow{\varphi''} E$ ein Isomorphismus von $\hat{K}$-Vektorräumen ist. Also ist auch $[\hat{E} : \hat{K}] = \dim_{\hat{K}} \hat{E} = n!$. ▫

Beispiel (Mitternachtsformel). Sei einmal $n = 2$. Wir wollen direkt zeigen, daß das Polynom $X^2 + Y_1X + Y_0$ aus $\hat{K}[X]$ auflösbar ist. Sei M der Zerfällungskörper von $X^2 - (\frac{1}{4}Y_1^2 - Y_0)$ über $\hat{K}$. Sei $\omega \in M$ eine der Nullstellen dieses Polynoms in M. Es ist $\omega^2 = \frac{1}{4}Y_1^2 - Y_0$, insbesondere ist ω radiziell über $\hat{K}$. Schreibe alternativ

$$\omega \;=:\; \sqrt{\tfrac{1}{4}Y_1^2 - Y_0}\,.$$

Es ist $\hat{K}(\omega)|\hat{K}$ auflösbar ([30]). Ferner ist

$$-\tfrac{1}{2}Y_1 + \omega \;=\; -\tfrac{1}{2}Y_1 + \sqrt{\tfrac{1}{4}Y_1^2 - Y_0}$$

eine Nullstelle von $X^2 + Y_1X + Y_0$ in $\hat{K}(\omega)$, da

$$\begin{array}{rcl} (-\frac{1}{2}Y_1 + \omega)^2 + Y_1(-\frac{1}{2}Y_1 + \omega) + Y_0 & = & \frac{1}{4}Y_1^2 - Y_1\omega + \omega^2 - \frac{1}{2}Y_1^2 + \omega Y_1 + Y_0 \\ & = & \omega^2 - \frac{1}{4}Y_1^2 + Y_0 \\ & = & 0\,. \end{array}$$

Somit hat $X^2 + Y_1X + Y_0$ eine Nullstelle in einer auflösbaren Erweiterung von $\hat{K}$ und ist also auflösbar.

> Informell gesprochen ist $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0$ auflösbar genau dann, wenn es eine Lösungsformel für die polynomiale Gleichung n-ten Grades in "iterierten Wurzelausdrücken" in den Y_i gibt.

Satz 11 (Satz von Abel) *Sei $n \geqslant 1$.*

(1) *Es ist* $\mathrm{Gal}(X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0) \simeq \mathcal{S}_n$.

[30] Es ist auch $M = \hat{K}(\omega)$ nach Aufgabe 36.(2), aber das brauchen wir hier nicht.

(2) *Es ist* $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0$ *auflösbar, falls* $n \leqslant 4$.

(3) *Es ist* $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0$ nicht *auflösbar, falls* $n \geqslant 5$.

Beweis. Alle drei Aussagen haben einen Sinn, da $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0 \in \hat{K}[X]$ nach vorigem Lemma irreduzibel ist.

Der Zerfällungskörper $\hat{E}$ von $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0$ über $\hat{K}$ hat nach vorstehendem Lemma den Grad $[\hat{E} : \hat{K}] = n!$. Also ist

$$\mathrm{Gal}(X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0) \;\simeq\; \mathcal{S}_n \;,$$

wie in (1) behauptet; vgl. letzte Folgerung aus §3.4.1.

Mit dem Satz 10 von Galois aus §4.4.2 ist nun $X^n + Y_{n-1}X^{n-1} + \cdots + Y_0X^0$ auflösbar genau dann, wenn $\mathcal{S}_n$ auflösbar ist. Dies ist laut Aufgabe 49 genau dann der Fall, wenn $n \leqslant 4$. Dies zeigt (2) und (3). ▫

Nach Niels Henrik Abel (1802–1829) sind übrigens auch die *abelschen* Gruppen benannt.

Kapitel 5

Aufgaben und Lösungen

5.1 Aufgaben

Aufgabe 1 (Exkurs kubische Gleichung) Seien a, b, $c \in \mathbf{C}$ gegeben.

Wir wollen ein $x \in \mathbf{C}$ mit $x^3 + ax^2 + bx + c = 0$ bestimmen.

(1) Falls $a \neq 0$, so substituiere $y = x + \frac{a}{3}$, $x = y - \frac{a}{3}$. Zeige, daß eine Gleichung der Form $y^3 + py + q = 0$ resultiert, mit p, $q \in \mathbf{C}$. Gib p, q darin in Abhängigkeit von a, b, c an.

(2) Falls $p \neq 0$, so substituiere $y = z - \frac{p}{3z}$. Zeige, daß für eine Nullstelle $z \in \mathbf{C} \smallsetminus \{0\}$ der substituierten Gleichung das zugehörige y Nullstelle von $y^3 + py + q = 0$ ist.

(3) Löse die substituierte Gleichung aus (2).

(4) Bestimme mittels $(1, 2, 3)$ ein $x \in \mathbf{C}$ mit $x^3 + \frac{1}{2}x^2 + \frac{1}{2}x - \frac{1}{2} = 0$. (Taschenrechner!)

Aufgabe 2 (§1.5; Euklidscher Algorithmus) Seien $a, b \in \mathbf{Z}_{>0}$ mit $a < b$ gegeben.

Wir wollen $\mathrm{ggT}(a, b)$ bestimmen, sowie s, $t \in \mathbf{Z}$ mit $as + bt = \mathrm{ggT}(a, b)$.

(1) Division mit Rest liefert $b = aq + r$ mit $r \in [0, a-1]$. Zeige, daß $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, r)$.

(2) Sei $x_0 := b$ und $x_1 := a$. Sind x_k, $x_{k+1} \in \mathbf{Z}_{\geqslant 0}$ bekannt, mit $x_k > x_{k+1}$, so schreibe, falls $x_{k+1} \neq 0$,

$$x_k \;=\; x_{k+1} \cdot q_{k+1} + x_{k+2}$$

mit $x_{k+2} \in [0, x_{k+1} - 1]$.

Zeige, daß es ein $\ell \geqslant 0$ mit $x_\ell > 0$ und $x_{\ell+1} = 0$ gibt. Zeige, daß $\mathrm{ggT}(a, b) = x_\ell$.

(3) Seien $s_\ell := 1$ und $s_{\ell+1} := 0$. Sind s_k und s_{k+1} bekannt für ein $k \in [2, \ell]$, so setzen wir

$$s_{k-1} \;:=\; s_{k+1} - s_k q_{k-1}$$

Zeige, daß $as_1 + bs_2 = x_\ell$. (Hinweis: Zeige $x_k s_k + x_{k-1} s_{k+1} = x_\ell$ per Induktion.)

(4) Seien $a = 23$, $b = 87$. Finde mit $(1, 2, 3)$ Elemente s, $t \in \mathbf{Z}$ mit $as + bt = \mathrm{ggT}(a, b)$.

Aufgabe 3 (§1.3) Wir rechnen in $\mathbf{Z}/n\mathbf{Z}$, wobei $n \in \mathbf{Z}_{\geqslant 1}$. Die Ergebnisse sind durch Elemente $x \in \mathbf{Z}$ mit $-n/2 < x \leqslant n/2$ repräsentiert anzugeben.

(1) Wir rechnen in $\mathbf{Z}/7\mathbf{Z}$. Bestimme $4 \cdot 3 + 1$. Bestimme $6 \cdot 5 \cdot 4$.

(2) Wir rechnen in $\mathbf{Z}/32\mathbf{Z}$. Bestimme $3 \cdot 5 \cdot 7 \cdot 9$. Bestimme 31^{31}. Bestimme 4^3.

Aufgabe 4 (§1.3, Aufgabe 2)

(1) Sei $m \in \mathbf{Z}_{\geqslant 1}$. Sei $k \in [0, m-1]$. Zeige, daß $k + m\mathbf{Z}$ genau dann invertierbar ist in $\mathbf{Z}/m\mathbf{Z}$, wenn $\mathrm{ggT}(k, m) = 1$. Berechne $(23 + 87\mathbf{Z})^{-1}$ und $(17 + 1000\mathbf{Z})^{-1}$.

(2) Sei n teilerfremd zu 10. Schreibe $1/n$ als periodischen Dezimalbruch. Zeige, daß die Periodenlänge gleich $\min\{k \geqslant 1 \ : \ 10^k \equiv_n 1\}$ ist. Bestätige dies in den Fällen $n = 7$ und $n = 41$.

Aufgabe 5 (Exkurs biquadratische Gleichung) Seien a, b, c, $d \in \mathbf{C}$ gegeben.

Wir wollen ein $x \in \mathbf{C}$ mit $x^4 + ax^3 + bx^2 + cx + d = 0$ bestimmen.

(1) Falls $a \neq 0$, so substituiere $y = x + \frac{a}{4}$, $x = y - \frac{a}{4}$. Zeige, daß eine Gleichung der Form $y^4 + py^2 + qy + r = 0$ resultiert, mit p, q, $r \in \mathbf{C}$. Gib p, q, r darin in Abhängigkeit von a, b, c, d an.

(2) Sei $\alpha \in \mathbf{C}$ so gewählt, daß $\alpha^3 + \frac{1}{2}p\alpha^2 - r\alpha - \frac{1}{2}pr + \frac{1}{8}q^2 = 0$ (vgl. Aufgabe 1).

Falls $p + 2\alpha = 0$, so zeige, daß $y^4 + py^2 + qy + r = 0$ genau dann, wenn

$$(y^2 - \alpha)^2 \ = \ \alpha^2 - r \ .$$

Falls $p + 2\alpha \neq 0$, so zeige, daß $y^4 + py^2 + qy + r = 0$ genau dann, wenn

$$(y^2 - \alpha)^2 \ = \ -(2\alpha + p)(y + \tfrac{q}{2(2\alpha+p)})^2 \ .$$

(3) Schreibe $\gamma := \mathrm{i}\sqrt{6}$. Bestimme mittels $(1, 2)$ ein $x \in \mathbf{C}$ so, daß

$$x^4 + 4x^3 + 7x^2 + (6 + \gamma)x + \frac{3}{2} + \gamma \ = \ 0 \ .$$

Aufgabe 6 (§1.3, §1.4.3; Chinesischer Restsatz)

(1) Seien R und S kommutative Ringe. Seien auf dem kartesischen Produkt $R \times S$ Addition und Multiplikation definiert durch

$$\begin{array}{rcl} (r,s) & + & (r',s') := (r+r', s+s') \\ (r,s) & \cdot & (r',s') := (r\cdot r', s\cdot s') \end{array}$$

wobei $r,\, r' \in R$ und $s,\, s' \in S$. Zeige, daß hierdurch ein kommutativer Ring $R \times S$ definiert wird. Falls R und S Körper sind, trifft das dann auch auf $R \times S$ zu?

(2) Sei R ein kommutativer Ring. Seien $I,\, J \subseteq R$ Ideale derart, daß $I + J = R$. Zeige, daß

$$\begin{array}{rcccc} R/(I\cap J) & \longrightarrow & R/I & \times & R/J \\ r+(I\cap J) & \longmapsto & (r+I & , & r+J) \end{array}$$

ein Isomorphismus kommutativer Ringe ist. (Hinweis: Warum genügt es für die Surjektivität, $(1,0)$ und $(0,1)$ im Bild nachzuweisen?)

(3) Seien $m,\ n \in \mathbf{Z}$ gegeben mit $\mathrm{ggT}(m,n) = 1$. Seien mit dem Euklidschen Algorithmus auch bereits $s,\, t \in \mathbf{Z}$ ermittelt mit $ms + nt = 1$. Zeige, daß $\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ ist. Gib Isomorphismen in beide Richtungen an.

(4) Zeige, daß $\mathbf{Z}/12\mathbf{Z} \simeq \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ (als kommutative Ringe). Finde Isomorphismen in beide Richtungen.

Aufgabe 7 (§1.4.1 und §1.6.2)

(1) Sei K ein Körper. Sei R ein kommutativer Ring, und sei $R \neq \{0_R\}$. Sei $K \xrightarrow{f} R$ ein Morphismus von Ringen. Zeige, daß f injektiv ist.

(Insbesondere sind Körpermorphismen stets injektiv.)

(2) Sei R ein kommutativer Ring. Zeige, daß $R[X] \xrightarrow{\varphi} R\,,\ f(X) = \sum_{i\geqslant 0} f_i X^i \longmapsto f_0$ ein Ringmorphismus ist. Berechne $\mathrm{Kern}\,\varphi$. Zeige, daß $R[X]/XR[X] \simeq R$.

Aufgabe 8 (§1.6.4, §1.8.5; Euklidscher Algorithmus) Sei K ein Körper.

Seien $f(X),\, h(X) \in K[X]$ mit $\deg f \leqslant \deg h$ gegeben. Wir wollen ein $g(X) \in K[X]$ so bestimmen, daß $f(X)K[X] + h(X)K[X] = g(X)K[X]$.

(Ist $g(X)$ noch normiert, so ist dies nach Definition gleichbedeutend mit $\mathrm{ggT}(f(X), h(X)) = g(X)K[X]$, vgl. §1.7.4.)

Ferner wollen wir $s(X),\, t(X) \in K[X]$ so bestimmen, daß $f(X)s(X) + h(X)t(X) = g(X)$.

(1) Division mit Rest liefert $h(X) = f(X)q(X) + r(X)$ mit $q(X),\, r(X) \in K[X]$ und $\deg r < \deg q$. Zeige, daß $f(X)K[X] + h(X)K[X] = f(X)K[X] + r(X)K[X]$.

(2) Sei $u_0(X) := h(X)$ und $u_1(X) := f(X)$. Sind $u_k(X)$, $u_{k+1}(X) \in K[X]$ bekannt, so schreibe, falls $u_{k+1}(X) \neq 0$, $u_k(X) = u_{k+1}(X) \cdot q_{k+1}(X) + u_{k+2}(X)$ mit $q_{k+1}(X)$, $u_{k+2}(X) \in K[X]$ und $\deg u_{k+2}(X) < \deg u_{k+1}(X)$.

Zeige, daß es ein $\ell \geqslant 0$ mit $u_\ell(X) \neq 0$ und $u_{\ell+1}(X) = 0$ gibt. Setze $g(X) := u_\ell(X)$. Zeige, daß $f(X)K[X] + h(X)K[X] = g(X)K[X]$.

(3) Seien $s_\ell(X) := 1$ und $s_{\ell+1}(X) := 0$. Sind $s_k(X)$ und $s_{k+1}(X)$ bekannt für ein $k \in [2, \ell]$, so setzen wir $s_{k-1}(X) := s_{k+1}(X) - s_k(X)q_{k-1}(X)$.

Zeige, daß $f(X)s_1(X) + h(X)s_2(X) = g(X)$.

(4) Seien $f(X) = X^3 + 1 \in \mathbf{F}_2[X]$ und $h(X) = X^8 + X^3 + X + 1 \in \mathbf{F}_2[X]$.

Finde mit $(1, 2, 3)$ ein $g(X)$ mit $f(X)K[X] + h(X)K[X] = g(X)K[X]$ und Elemente $s(X)$, $t(X) \in \mathbf{F}_2[X]$ mit $f(X)s(X) + h(X)t(X) = g(X)$.

Aufgabe 9 (§1.6.1; Formales Ableiten) Sei R ein kommutativer Ring.

Für $f(X) = \sum_{i \geqslant 0} f_i X^i \in R[X]$ setzen wir

$$f'(X) \ := \ \sum_{i \geqslant 1} i f_i X^{i-1}$$

(wobei ein Element aus R mit einem Element $i \in \mathbf{Z}_{\geqslant 0}$ durch Bilden dessen i-facher Summe in R multipliziert werde).

Zeige, daß für $f(X)$, $g(X) \in R[X]$ und r, $s \in R$

$$\begin{aligned} (rf(X) + sg(X))' &= rf'(X) + sg'(X) \\ (f(X) \cdot g(X))' &= f'(X) \cdot g(X) + f(X) \cdot g'(X) \ . \end{aligned}$$

Aufgabe 10 (§1.7.5)

(1) Sei R ein Integritätsbereich. Sei $K \subseteq R$ ein Teilkörper von R, d.h. ein Teilring, der ein Körper ist. Sei R als K-Vektorraum endlichdimensional. Zeige, daß R ein Körper ist.

(2) Finde ein $n \geqslant 0$ und eine Basis $(z_1, \ldots, z_n)$ von $\mathbf{C}$ als $\mathbf{R}$-Vektorraum so, daß für alle $i \in [1, n]$ ein $j \in [1, n]$ mit $\bar{z}_i = z_j$ existiert.

Aufgabe 11 (§1.8.4) Die Ordnung eines Elements g in einer (multiplikativ geschriebenen) endlichen Gruppe G ist definiert als $\mathrm{o}(g) := \min\{n \in \mathbf{Z}_{\geqslant 1} \ : \ g^n = 1\}$. (Diese existiert, da wegen der Endlichkeit von G es $0 \leqslant k < \ell$ mit $g^k = g^\ell$ geben muß, woraus $g^{\ell-k} = 1$ folgt.)

Schreibe $b\langle a \rangle := \{ba^k \ : \ k \in \mathbf{Z}\}$ für a, $b \in G$.

Schreibe $\mathbf{F}_p^\times := \mathbf{F}_p \smallsetminus \{0\}$ für p prim.

(1) Sei $a \in G$ gegeben.

(a) Zeige, daß für b, $b' \in G$ entweder $b\langle a\rangle = b'\langle a\rangle$ oder $b\langle a\rangle \cap b'\langle a\rangle = \emptyset$.

(b) Zeige, daß $|b\langle a\rangle| = \mathrm{o}(a)$ für alle $b \in G$.

(c) Folgere, daß $\mathrm{o}(a)$ ein Teiler von $|G|$ ist.

(2) Bestimme alle Elementordnungen in $(\mathbf{F}_7^\times, \cdot)$. Verifiziere (1.c) in diesem Beispiel.

(3) Bestimme alle Elementordnungen in $(\mathbf{F}_{11}^\times, \cdot)$. Verifiziere (1.c) in diesem Beispiel.

Aufgabe 12 (§1.8.4, Aufgabe 11) Sei p prim.

(1) Sei $a \in \mathbf{F}_p$. Zeige, daß $a^p = a$ (Kleiner Fermatscher Satz; Hinweis: Aufgabe 11.(1.c)).

(2) Zeige, daß $X^p - X = \prod_{i\in\mathbf{F}_p}(X - i)$ in $\mathbf{F}_p[X]$. (Hinweis: (1).)
Berechne $\prod_{i\in[0,3-1]}(X - i)$ in $\mathbf{Z}[X]$ und vergleiche.

(3) Zeige, daß $(p-1)! \equiv_p -1$ (Satz von Wilson; Hinweis: Koeffizientenvergleich in (2)).
Ist $(n-1)! \equiv_n -1$ für alle $n \in \mathbf{Z}_{\geqslant 1}$?

(4) Sei $p \geqslant 3$. Sei $s(p) := \sum_{i\in[1,p-1]} \frac{1}{i}$. Zeige, daß der Zähler von $s(p)$ in gekürzter Bruchschreibweise durch p teilbar ist.
(Hinweis: Koeffizientenvergleich bei X^2 in (2)).

Aufgabe 13 (§1.7.2, §1.7.4)

(1) Seien a, $b \in \mathbf{Z}_{\geqslant 1}$. Zeige, daß $a\mathbf{Z} \cap b\mathbf{Z} = \mathrm{kgV}(a,b)\mathbf{Z}$.

(2) Finde das $x \in \mathbf{Z}_{\geqslant 1}$ mit $(12\mathbf{Z} + 30\mathbf{Z}) \cap 21\mathbf{Z} = x\mathbf{Z}$.

(3) Finde das $f(X) \in \mathbf{F}_2[X]$ mit

$$(X^4+1)\mathbf{F}_2[X] + (X^4+X^3+X+1)\mathbf{F}_2[X] + (X^3+1)\mathbf{F}_2[X] \;=\; f(X)\mathbf{F}_2[X]\,.$$

Aufgabe 14 (§1.6.2)

Gib einen Ringisomorphismus φ von $\mathbf{F}_2[X]$ nach $\mathbf{F}_2[X]$ an mit $\varphi \neq \mathrm{id}_{\mathbf{F}_2[X]}$, aber mit $\varphi^2 = \mathrm{id}_{\mathbf{F}_2[X]}$.

Aufgabe 15 (§1.7.3)

(1) Bestimme $\mathrm{char}(\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z})$.

(2) Sei $K \xrightarrow{f} L$ ein Morphismus von Körpern. Zeige, daß $\mathrm{char}\, K = \mathrm{char}\, L$.

Aufgabe 16 (§1.7, §1.5)

(1) Sei $n \in \mathbf{Z}_{\geqslant 1}$ nicht prim. Zeige, daß $\mathbf{Z}/n\mathbf{Z}$ kein Integritätsbereich ist.

(2) Berechne $\left(X^4 + 1 + (X^7 + 1)\mathbf{F}_3[X]\right)^{-1}$ in $\mathbf{F}_3[X]/(X^7 + 1)\mathbf{F}_3[X]$.

(3) Wieviele Elemente enthält $R := \mathbf{F}_2[X]/(X^3 + X^2 + X + 1)\mathbf{F}_2[X]$? Finde ein invertierbares Element in $R \smallsetminus \{1\}$. Ist R ein Integritätsbereich?

(4) Sei K ein Körper. Sei $f(X) \in K[X]$ mit $f(0) = f_0 \neq 0$.
Bestimme $(X + f(X)K[X])^{-1}$ in $K[X]/f(X)K[X]$ (in Abhängigkeit von $f(X)$).

Aufgabe 17 (§1.8.5) *Berechnen* eines Elementes in $\mathbf{F}_8$ bedeute, es als $\mathbf{F}_2$-Linearkombination in der Standardbasis $(\beta^0, \beta^1, \beta^2)$ zu schreiben. Entsprechend in $\mathbf{F}_4$ resp. $\mathbf{F}_9$.

(1) Bestimme die Verknüpfungstafeln von $\mathbf{F}_4$ bezüglich Addition und Multiplikation.

(2) Berechne $(\alpha^2 + 1)^3$, $(\beta^2 + 1)(\beta^6 + 1) + \beta^2$ und $(\iota + 1)^4 - \iota$.

(3) Berechne α^{-1}, $(\beta^2 + \beta + 1)^{-1}$ und $(\iota + 1)^{-1}$.

Aufgabe 18 (§1.8.5) Ist G eine Gruppe und $x \in G$, so schreibe $\langle x \rangle = \{x^k \ : \ k \in \mathbf{Z}\}$. Ist K ein Körper, so schreibe $K^\times := K \smallsetminus \{0\}$.

(1) Finde ein $x \in \mathbf{F}_4^\times$ mit $\langle x \rangle = \mathbf{F}_4^\times$.

(2) Finde ein $x \in \mathbf{F}_8^\times$ mit $\langle x \rangle = \mathbf{F}_8^\times$.

(3) Finde ein $x \in \mathbf{F}_9^\times$ mit $\langle x \rangle = \mathbf{F}_9^\times$.

Aufgabe 19 (§1.8.5)

Bestimme alle normierten irreduziblen Polynome in $\mathbf{F}_q[X]$ von Grad n.

(1) Sei $q = 4$ und $n = 2$.

(2) Sei $q = 3$ und $n = 3$.

(3) Sei $q = 2$ und $n = 4$.

Aufgabe 20 (§1.7, §1.8)

Zeige, daß die kommutativen Ringe $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ und $\mathbf{F}_9$ paarweise nichtisomorph sind.

Aufgabe 21 (§1.8.5)

Gibt es in $\mathbf{F}_8$ einen Teilkörper aus 4 Elementen? Warum?

Aufgabe 22 (§1.8.2)

(1) Sei $R \xrightarrow{f} S$ ein Morphismus kommutativer Ringe. Sei $J \subseteq S$ ein Ideal. Zeige, daß $f^{-1}(J) \subseteq R$ ein Ideal ist, das $\operatorname{Kern} f$ enthält.

(2) Sei R ein kommutativer Ring, und sei $I \subseteq R$ ein maximales Ideal. Zeige mittels (1) erneut, daß R/I ein Körper ist. (Hinweis: Wir haben zu zeigen, daß R/I genau zwei Ideale enthält. Wende (1) an auf $R \xrightarrow{\rho} R/I$. Sei J ein Ideal von R/I. In welchem Verhältnis stehen I und $\rho^{-1}(J)$? Verwende nun Maximalität von I.)

Aufgabe 23 (§1.10.1; Quotientenkörper)

Sei R ein Integritätsbereich. Zeige, daß $\operatorname{frac} R$ ein Körper ist.

Zeige also, daß Addition und Multiplikation die Axiome eines kommutativen Rings erfüllen und daß es zu jedem Element ungleich 0 in $\operatorname{frac} R$ ein multiplikativ inverses Element gibt; vgl. §1.10.1.

Aufgabe 24 (§1, §2.1; Frobenius)

(1) Sei K ein Körper mit $\operatorname{char} K =: p > 0$. Zeige, daß

$$\begin{array}{ccc} K & \xrightarrow{\mathrm{Frob}_K} & K \\ x & \longmapsto & \mathrm{Frob}_K(x) := x^p \end{array}$$

ein Körpermorphismus ist, der sogenannte *Frobenius.*
Ist Frob_K ein Automorphismus? (Hinweis: Betrachte $\mathbf{F}_p(X)$.)
Ist Frob_K ein Automorphismus, falls K endlich ist?

(2) Zeige unter Verwendung von $\mathrm{Frob}_{\mathbf{F}_p}$ und der ersten Bemerkung in §2.1 den Kleinen Fermatschen Satz erneut; vgl. Aufgabe 12.(1).

(3) Konstruiere einen Körper $\mathbf{F}_{27}$ aus 27 Elementen.
Bestimme $\{x \in \mathbf{F}_{27} \,:\, \mathrm{Frob}_{\mathbf{F}_{27}}(x) = x\}$.

(4) Konstruiere einen Körper $\mathbf{F}_{16}$ aus 16 Elementen.
Zeige, daß $\{x \in \mathbf{F}_{16} \,:\, \mathrm{Frob}^2_{\mathbf{F}_{16}}(x) = x\}$ ein Teilkörper von $\mathbf{F}_{16}$ isomorph zu $\mathbf{F}_4$ ist.

Aufgabe 25 (§1.7.4, §1.9)

(1) Sei K ein Körper mit $\operatorname{char} K = 0$. Seien $s, t \geqslant 1$. Sei $f(X) := X^s(X-1)^t$. Zeige, daß $\mathrm{ggT}(f(X), f'(X)) = X^{s-1}(X-1)^{t-1}$.

(2) Sei K ein Körper. Sei $f(X) \in K[X]$ vollständig in Linearfaktoren zerlegbar. Zeige, daß genau dann ein Linearfaktor in $f(X)$ mit Exponent $\geqslant 2$ auftritt (d.h. f eine doppelte Nullstelle in K hat), wenn $\mathrm{ggT}(f(X), f'(X)) \neq 1$.

(3) Sei L ein Körper, und sei K ein Teilkörper von L. Seien $f(X)$, $h(X) \in K[X]$. Zeige, daß der in $K[X]$ genommene ggT von $f(X)$ und $h(X)$ mit dem in $L[X]$ genommenen übereinstimmt.

Aufgabe 26 (§2.1) Sei L ein endlicher Körper.

(1) Zeige, daß $|L|$ eine Primpotenz ist. D.h. zeige, daß es eine Primzahl p gibt und ein $\ell \geqslant 1$ so, daß $|L| = p^\ell$.
(Hinweis: Kann $\operatorname{char} L = 0$ sein? Zeige, daß L ein endlichdimensionaler Vektorraum über seinem Primkörper ist.)

(2) Sei weiterhin $|L| = p^\ell$. Sei $K \subseteq L$ ein Teilkörper. Zeige, daß $|K| = p^k$ für einen Teiler k von ℓ. (Hinweis: Gradsatz 1).

(3) Bestimme alle Teilkörper von $\mathbf{F}_{27}$; vgl. Aufgabe 24.(3).

Aufgabe 27 (§1; Multiplikative Gruppe eines endlichen Körpers)

Sei $(G, \cdot)$ eine multiplikativ geschriebene endliche abelsche Gruppe. Seien a, $b \in G$.
Sei K ein Körper. Schreibe $K^\times := K \smallsetminus \{0\}$. Bezüglich $\mathrm{o}(a)$, vgl. Aufgabe 11.

(1) Sei $k \in \mathbf{Z}$. Zeige, daß genau dann $a^k = 1$ ist, wenn $\mathrm{o}(a)$ ein Teiler von k ist.
Ist $\mathrm{ggT}(\mathrm{o}(a), \mathrm{o}(b)) = 1$, so zeige $\mathrm{o}(ab) = \mathrm{o}(a)\mathrm{o}(b)$.

(2) Sei $d \in \mathbf{Z}_{\geqslant 1}$. Zeige $\mathrm{o}(a^d) = \frac{\mathrm{o}(a)}{\mathrm{ggT}(\mathrm{o}(a),d)}$.
Ist insbesondere d ein Teiler von $\mathrm{o}(a)$, dann ist $\mathrm{o}(a^d) = \frac{\mathrm{o}(a)}{d}$.

(3) Zeige, daß es in G ein Element von Ordnung $\mathrm{kgV}(\mathrm{o}(a), \mathrm{o}(b))$ gibt.
(Hinweis: Schreibe $\mathrm{o}(a) = p_1^{s_1} \cdots p_k^{s_k}$ und $\mathrm{o}(b) = p_1^{t_1} \cdots p_k^{t_k}$ mit p_i prim. Mit (2) haben wir ein Element $x_i \in G$ von Ordnung $p_i^{\max\{\, s_i\,,\, t_i\,\}}$ für alle i, nämlich je eine geeignete Potenz von a oder von b. Bestimme $\mathrm{o}(x_1 \cdots x_k)$ mit (1).)

(4) Sei x ein Element von G maximaler Ordnung. Zeige, daß $\mathrm{o}(g)$ ein Teiler von $\mathrm{o}(x)$ ist für alle $g \in G$. (Hinweis: Sonst wäre $\mathrm{o}(x) < \mathrm{kgV}(\mathrm{o}(x), \mathrm{o}(g))$. Verwende (3).)

(5) Sei nun $G \subseteq K^\times$ derart, daß die Multiplikation von Elementen von G durch die Multiplikation dieser Elemente in K gegeben ist; cf. auch §3.2 später.
Zeige, daß es ein $x \in G$ mit $\mathrm{o}(x) = |G|$ gibt.
Ist insbesondere K endlich und $G = K^\times$, so folgt, daß es ein $x \in K^\times$ mit $\mathrm{o}(x) = |K^\times| = |K| - 1$ gibt.
(Hinweis: Sei $x \in G$ von maximaler Ordnung. Es ist $\mathrm{o}(x)$ ein Teiler von $|G|$. Mit (4) folgt, daß alle Elemente von G Nullstellen von $X^{\mathrm{o}(x)} - 1$ sind. Ein Polynom mit $|G|$ Nullstellen hat Grad $\geqslant |G|$.)

(6) Gib in $\mathbf{F}_{16}^{\times}$ ein Element von Ordnung 15 an, samt seinen Potenzen; vgl. Aufgabe 24.(4).

(7) Finde eine Gruppe $G \subseteq \mathbf{C}^{\times}$ wie in (5) mit $|G| = 4$.

Aufgabe 28 (§2.3.1)

Sei $L|K$ eine endliche Körpererweiterung. Sei $x \in L$. Zeige, daß x algebraisch über K ist.

Aufgabe 29 (§1.9, §2.4)

Zerlege $f(X) \in K[X]$ in irreduzible Polynome unter Verwendung von Magma.

(Hinweis: $\mathbf{Q}$ via `Q := Rationals()`, $\mathbf{F}_2$ via `F := GF(2)` eingeben. Der Magma Calculator findet sich auf http://magma.maths.usyd.edu.au/calc .)

(1) $f(X) = X^4 + X + 1 \in \mathbf{Q}[X]$.

(2) $f(X) = X^5 + X + 1 \in \mathbf{Q}[X]$.

(3) $f(X) = X^5 + X + 1 \in \mathbf{Q}(\mathrm{i}\sqrt{3})[X]$.

(4) $f(X) = X^8 - X \in \mathbf{F}_2[X]$.

(5) $f(X) = X^8 - X \in \mathbf{F}_8[X]$.

(6) $f(X) = X^{15} - X + 1 \in \mathbf{F}_9[X]$.

Aufgabe 30 (§2.2, §2.3.3, implizit §2.5)

Sei $f(X) \in K[X]$ gegeben. Konstruiere in Magma eine endliche Körpererweiterung L von K so, daß $f(X) \in L[X]$ in Linearfaktoren zerfällt. Gib diese Faktorisierung an (unter Verwendung geeigneter Bezeichnungsweisen). Bestimme $[L : K]$.

(1) $f(X) = X^4 + X^2 + 1 \in \mathbf{Q}[X]$.

(2) $f(X) = X^6 + X^2 + 1 \in \mathbf{Q}[X]$.

(3) $f(X) = X^4 + X + 1 \in \mathbf{F}_4[X]$.

Aufgabe 31 (§2.3.2) Verwende Magma für Faktorisierungen, nicht aber, um Minimalpolynome direkt auszugeben.

(1) Bestimme $\mu_{\sqrt{2}+\sqrt{3},\mathbf{Q}}(X)$. Ist $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$? (Hinweis: Gradvergleich.)

(2) Bestimme die Minimalpolynome aller Elemente von $\mathbf{F}_8$. Gibt es einen Automorphismus von $\mathbf{F}_8$, der nicht gleich einer Potenz des Frobeniusautomorphismus ist?

Aufgabe 32 (§2.3.2) Sei $L|K$ eine Körpererweiterung.

Sei $y \in L$ algebraisch über K. Sei $\deg \mu_{y,K}$ ungerade.

Zeige, daß $\deg \mu_{y^2,K} = \deg \mu_{y,K}$ ist. Ist $\mu_{y,K}(X) = \mu_{y^2,K}(X)$?

Aufgabe 33 (§2.3.2) Sei p prim. Sei $k \geqslant 2$.

(1) Zeige, daß ein irreduzibles Polynom von Grad k in $\mathbf{F}_p[X]$ existiert.
(Hinweis: Nach Aufgabe 27.(5) ist $\mathbf{F}_{p^k}^\times = \langle y \rangle$ für ein $y \in \mathbf{F}_{p^k}^\times$; vgl. auch Kor. in §2.5.4. Insbesondere ist $\mathbf{F}_{p^k} = \mathbf{F}_p(y)$. Betrachte $\mu_{y,\mathbf{F}_p}(X)$.)

(2) Sei $f(X) \in \mathbf{F}_p[X]$ normiert und irreduzibel mit $\deg f = k$. Zeige, daß in $\mathbf{F}_p[X]$ das Polynom $X^{p^k} - X$ von $f(X)$ geteilt wird, nicht aber von $f(X)^2$.
(Hinweis: Sei $K := \mathbf{F}_p[T]/f(T)\mathbf{F}_p[T]$. Sei $y := T + f(T)\mathbf{F}_p[T] \in K$. Warum teilt $f(X) = \mu_{y,\mathbf{F}_p}(X)$ das Polynom $X^{p^k} - X$? Wie zerfällt $X^{p^k} - X$ in $K[X]$? Wie zerfällt also $f(X)$ in $K[X]$? Wie oft kann also $f(X)$ nur in $X^{p^k} - X$ aufgehen?)

Aufgabe 34 (§2.5)

Bestimme den Zerfällungskörper von $f(X) \in K[X]$ via Magma. Gib seinen Grad über K an. (Hinweis: Löse wie in Aufgabe 30. Damals fiel der Begriff des Zerfällungskörpers noch nicht.)

(1) $f(X) = X^3 + X + 1 \in \mathbf{Q}[X]$.

(2) $f(X) = X^4 + 4X^2 + 8X + 8 \in \mathbf{Q}[X]$.

(3) $f(X) = X^6 - X^3 + 2 \in \mathbf{Q}[X]$.

(4) $f(X) = X^2 + 1 \in \mathbf{Q}(\sqrt{2})[X]$.

Aufgabe 35 (§2.5)

Sei K ein Körper mit $\operatorname{char} K = p > 0$. Sei $a \in K^\times$ keine p-te Potenz eines Elements von $K^\times$. Sei L der Zerfällungskörper von $X^p - a \in K[X]$.

Zeige, daß $X^p - a \in K[X]$ irreduzibel ist. Zeige, daß $[L : K] = p$.

(Hinweis: Sei $b \in L$ eine Nullstelle. Dann ist $(X - b)^p = X^p - a$. Hätte $X^p - a$ einen nichttrivialen Faktor $f(X) \in K[X]$, so wäre dieser von der Form $(X - b)^s$ für ein $s \in [1, p-1]$. Dann aber wäre $f_0 = (-b)^s$ in K. Mit $su + pv = 1$ mit $u, v \in \mathbf{Z}$ wäre $(-b) = (-b)^{su+pv} = ((-b)^s)^u(-a)^v \in K$.)

Aufgabe 36 (§2.5, §2.3.2) Sei $K(y)|K$ eine endliche monogene Körpererweiterung.

Zeige oder widerlege.

(1) Es ist $K(y)$ ein Zerfällungskörper von $\mu_{y,K}(X)$.

(2) Ist $[K(y) : K] = 2$, so ist $K(y)$ ein Zerfällungskörper von $\mu_{y,K}(X)$.

Aufgabe 37 (§3.2) Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus.

(1) Sei $U \leqslant G$. Zeige, daß $f(U) \leqslant H$.

(2) Zeige, daß $\operatorname{Im} f \leqslant H$. (Hinweis: Spezialfall von (1).)

(3) Ist f injektiv, so zeige, daß $f|^{\operatorname{Im} f}$ ein Gruppenisomorphismus von G nach $\operatorname{Im} f$ ist.

(4) Sei $N \trianglelefteq H$. Zeige, daß $f^{-1}(N) \trianglelefteq G$.

(5) Zeige, daß $\operatorname{Kern} f \trianglelefteq G$. (Hinweis: Spezialfall von (4).)

Aufgabe 38 (§3.2; Satz von Lagrange) Sei G eine endliche Gruppe. Sei $U \leqslant G$. Schreibe $bU := \{bu : u \in U\}$ für $b \in G$.

(1) (Hinweis: Vgl. Aufgabe 11.(1).)

   (a) Zeige, daß für b, $b' \in G$ entweder $bU = b'U$ oder $bU \cap b'U = \emptyset$ ist.

   (b) Zeige, daß $|bU| = |U|$ für alle $b \in G$.

   (c) Folgere, daß $|U|$ ein Teiler von $|G|$ ist.

(2) Berechne $(1,3) \circ (1,3,4)$ und $(1,6,3) \circ (2,4,3,5) \circ (2,4)$ in $\mathcal{S}_6$.

(3) Gib alle Untergruppen von $\mathcal{S}_3$ an. Welche davon sind normal?

(4) Verifiziere (1.c) für $G = \mathcal{S}_{12}$ und $U = \langle (1,2,3,4,5,6,7,8,9,10,11,12), (1,3) \rangle$ via Magma.

Aufgabe 39 (§3.4) Sei K ein perfekter Körper. Sei $f(X) \in K[X]$ ein Produkt verschiedener irreduzibler Polynome.

Berechne $\operatorname{Gal}(f(X))$. Verwende hierzu Magma (ausgenommen `GaloisGroup`).

(1) $f(X) = X^4 + 4X^2 + 8X + 8 \in \mathbf{Q}[X]$ (vgl. Aufgabe 34.(2)).

(2) $f(X) = X^6 + X^2 + 1 \in \mathbf{Q}[X]$ (vgl. Aufgabe 30.(2)).

Aufgabe 40 (§3.4) Sei K ein perfekter Körper.

Sei $f(X) \in K[X]$ ein normiertes irreduzibles Polynom von Grad 2. Zeige, daß $\operatorname{Gal}(f(X)) \simeq \mathcal{S}_2$. Folgere, daß $\operatorname{Gal}(\mathbf{C}|\mathbf{R}) \simeq \mathcal{S}_2$.

Aufgabe 41 (§3.5.1.2) Sei L der Zerfällungskörper von $f(X) \in K[X]$, wobei K perfekt und $f(X)$ ein Produkt verschiedener irreduzibler normierter Polynome ist.

Sei $U \leqslant \operatorname{Gal}(L|K)$. Bestimme eine K-lineare Basis von $\operatorname{Fix}_U L$.

(Hinweis: Es ist $\operatorname{Tr}_U : L \longrightarrow \operatorname{Fix}_U L$, $x \longmapsto \sum_{\sigma \in U} \sigma(x)$ eine surjektive K-lineare Abbildung.)

(1) $f(X) = X^3 + X + 1 \in \mathbf{Q}[X]$, $U \xrightarrow{\sim} \langle (1,3) \rangle$ in der Notation von §3.4.2.1.

(2) $f(X) = X^3 + X + 1 \in \mathbf{Q}[X]$, $U \xrightarrow{\sim} \langle (1,2,3) \rangle$ in der Notation von §3.4.2.1.

(3) $f(X) = X^4 + 4X^2 + 8X + 8 \in \mathbf{Q}[X]$, $U \xrightarrow{\sim} \langle (1,2,3) \rangle$ in der Notation der Lösung zu Aufgabe 34.(2). (Hinweis: Magma !)

(4) $f(X) = X^{16} - X \in \mathbf{F}_2[X]$, $U = \langle \mathrm{Frob}_{\mathbf{F}_{16}}^2 \rangle$; vgl. Aufgabe 24.(4).

Aufgabe 42 (§3.2) Sei $G \xrightarrow{f} H$ ein Gruppenmorphismus. Sei $N \trianglelefteq G$ ein Normalteiler.

Zeige.

(1) Es ist $G/N := \{gN \ : \ g \in G\}$ eine Gruppe mit $1_{G/N} = 1_G \cdot N$ und $gN \cdot \tilde{g}N = (g \cdot \tilde{g})N$ für $g, \tilde{g} \in G$. Es heißt G/N *Faktorgruppe* von G nach (oder modulo) N.

(2) Es ist $G/\operatorname{Kern} f \longrightarrow \operatorname{Im} f$, $g \operatorname{Kern} f \longmapsto f(g)$ ein wohldefinierter Gruppenisomorphismus.

(3) Sind G und H endlich, so teilt $|\operatorname{Im} f|$ sowohl $|G|$ als auch $|H|$. (Hinweis: Lagrange.)

Aufgabe 43 (§3.5.1.1, vorbereitend zu §4.4.3) Sei K ein Körper. Sei $n \geqslant 1$.

Schreibe $E := K(T_1, \ldots, T_n)$.

(1) Gib einen injektiven Gruppenmorphismus $\mathcal{S}_n \longrightarrow \mathrm{Aut}(E|K)$ an. Wir identifizieren $\mathcal{S}_n$ mit ihrem Bild in $\mathrm{Aut}(E|K)$.

(2) Definiere

$$\textstyle\sum_{i\in[0,n]}(-1)^{n-i}s_iX^i \ = \ \sum_{i\in[0,n]}(-1)^{n-i}s_i(T_1,\ldots,T_n)X^i \ := \ (X-T_1)\cdots(X-T_n) \ \in \ E[X] \ .$$

Im Fall $n = 3$ berechne $s_i(T_1, T_2, T_3)$ für $i \in [0, 3]$.

(3) Definiere den Teilkörper

$$L \ := \ K(s_0\,,\ldots,s_{n-1}) \ := \ \left\{ \tfrac{f(s_0,\ldots,s_{n-1})}{g(s_0,\ldots,s_{n-1})} : f(X_0,\ldots,X_{n-1}),\, g(X_0,\ldots,X_{n-1}) \in K[X_0,\ldots,X_{n-1}],\ g(s_0,\ldots,s_{n-1}) \neq 0 \right\} \ \subseteq \ E \ .$$

Zeige $L \subseteq \mathrm{Fix}_{\mathcal{S}_n} E$. Folgere $[E : L] \geqslant n!$. (Hinweis: Dedekind.)

(4) Zeige, daß $[L(T_1\,,\ldots,T_{i-1}\,,T_i) : L(T_1\,,\ldots,T_{i-1})] \leqslant n + 1 - i$ für $i \in [1, n]$.
Folgere $[E : L] \leqslant n!$. Folgere $L = \mathrm{Fix}_{\mathcal{S}_n} E$.
Folgere $\mu_{T_i, L(T_1,\ldots,T_{i-1})}(X) \ = \ (X - T_i) \cdots (X - T_n)$.
Gib eine L-lineare Basis von E an.
(Hinweis: $(X - T_i) \cdots (X - T_n) = \frac{(X-T_1)\cdots(X-T_n)}{(X-T_1)\cdots(X-T_{i-1})} \in L(T_1, \ldots, T_{i-1})[X]$.)

Aufgabe 44 (vorbereitend zu §4.4.2) Sei K ein Körper mit $\operatorname{char} K = 0$. Sei $n \geqslant 1$.

Sei L der Zerfällungskörper von $X^n - 1 \in K[X]$ über K. Zeige.

(1) Es ist $\{z \in L \ : \ z^n = 1\}$ eine Untergruppe der Ordnung n von $L^\times$, die von einem Element ζ_n der Ordnung n erzeugt wird, welches wir fixieren. Es ist $L = K(\zeta_n)$. (Hinweis: Vgl. Aufgaben 27.(4, 5), 25.(2)).

(2) Sei $\mathrm{U}(\mathbf{Z}/n\mathbf{Z}) := \{k + n\mathbf{Z} \ : \ \mathrm{ggT}(k, n) = 1\}$. Zeige, daß $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ mit der Multiplikation aus $\mathbf{Z}/n\mathbf{Z}$ eine abelsche Gruppe bildet. Bestimme alle Elementordnungen in $\mathrm{U}(\mathbf{Z}/12\mathbf{Z})$. Ist $\mathrm{U}(\mathbf{Z}/12\mathbf{Z})$ von einem Element erzeugt?

(3) Sei für $\sigma \in \mathrm{Gal}(L|K)$ das Element $i_\sigma + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ definiert durch $\sigma(\zeta_n) = \zeta_n^{i_\sigma}$. Zeige, daß $\mathrm{Gal}(L|K) \longrightarrow \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, $\sigma \longmapsto i_\sigma + n\mathbf{Z}$ ein injektiver Gruppenmorphismus ist. Folgere, daß $\mathrm{Gal}(L|K)$ abelsch ist.

Aufgabe 45 (vorbereitend zu §4.4.2)

Sei K ein perfekter Körper. Sei $L|K$ eine endliche Erweiterung.

(1) Zeige, daß L perfekt ist. (Hinweis: L einmal wie üblich, und einmal via $x * y := x^p y$ für $x \in K$ und $y \in L$ als Vektorraum auffassen.)

(2) Sei $L|K$ galoisch. Sei $f(X) \in K[X]$ ein normiertes Polynom, welches in ein Produkt verschiedener normierter irreduzibler Polynome zerfällt. Sei M der Zerfällungskörper von $f(X)$ über L. Zeige, daß $M|K$ galoisch ist.

Aufgabe 46 (§3.4, §3.5.1.2)

(1) Bestimme die Galoisgruppe von $X^6 + 3X + 3 \in \mathbf{Q}[X]$ mit Magma (ausgenommen `GaloisGroup`).

(2) Bestimme alle Körper zwischen $\mathbf{Q}$ und dem Zerfällungskörper von $X^3 + X + 1 \in \mathbf{Q}[X]$. (Hinweis: Aufgabe 34.(1), §3.4.2.1, Aufgabe 41.)

Aufgabe 47 (§3.5.2, §3.6)

(1) Sei K perfekt, sei $E|L|K$ mit $E|K$ galoisch. Zeige mit einem Zerfällungskörperargument, daß $E|L$ galoisch ist; vgl. Lemma aus §3.5.2. (Hinweis: Aufgabe 45.(1).)

(2) Sei q eine Primpotenz, sei $s \geqslant 1$. Zeige mit einem Zerfällungskörperargument, daß $\mathbf{F}_{q^s}|\mathbf{F}_q$ galoisch ist; vgl. Lemma aus §3.6.

Aufgabe 48 (§3.5.2)

(1) Sei G eine endliche Gruppe. Sei $G = \langle g \rangle$ für ein $g \in G$ mit $\mathrm{o}(g) = n$, also G zyklisch. Zeige, daß jede Untergruppe von G von der Form $\langle g^d \rangle$ für einen Teiler d von n ist.

(2) Sei p prim. Sei $s \geqslant 1$. Ordne jedem Teiler d von s einen Körper K zwischen $\mathbf{F}_p$ und $\mathbf{F}_{p^s}$ mit $[K : \mathbf{F}_p] = d$ zu. Erhält man so alle Zwischenkörper?

(3) Konstruiere $\mathbf{F}_{64}$. Konstruiere alle Körper zwischen $\mathbf{F}_2$ und $\mathbf{F}_{64}$.
(Hinweis: `ElementToSequence` gibt Koeffizienten eines Element in $\mathbf{F}_{64}$ in Standardbasis.)

Aufgabe 49 (§4.1) Zeige.

(1) Es ist $\mathcal{S}_n$ auflösbar für $n \in [1, 4]$. (Verwende Magma, ausgenommen `IsSolvable`. Hinweis: Warum ist eine Untergruppe $U \leqslant G$ mit $2|U| = |G|$ normal?)

(2) Es ist $\mathcal{S}_n$ nicht auflösbar für $n \geqslant 5$.
(Hinweis: Sei $M \trianglelefteq N \leqslant \mathcal{S}_n$ mit N/M abelsch. Falls N alle Zykel der Länge 3 enthält, so auch M. Denn gegeben $(a, b, c) \in N$, so wird, da N/M abelsch, $(a, b, c) = (a, b, d) \circ (a, c, e) \circ (a, b, d)^{-1} \circ (a, c, e)^{-1} \in M$, wobei $|\{a, b, c, d, e\}| = 5$.)

Aufgabe 50 (§3.4.1) Sei K ein Körper. Sei $f(X) \in K[X]$ normiert von Grad $n \geqslant 1$.

Sei L der Zerfällungskörper von $f(X)$ über K. Zeige, daß $f(X) \in K[X]$ irreduzibel ist, falls $[L : K] = n!$.

Aufgabe 51 (§4.4.2) Ist $f(X) \in \mathbf{Q}[X]$ auflösbar?

(Verwende Magma, ausgenommen `GaloisGroup` und `IsSolvable`. Hinweis: Aufgabe 50.)

(1) $f(X) = X^5 + 5X^2 + 3 \in \mathbf{Q}[X]$.

(2) $f(X) = X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$.

Aufgabe 52 (§3.5.1.2, §3.5.1.4, §3.6)

Sei $L|K$ eine endliche Galoiserweiterung mit Galoisgruppe $G := \mathrm{Gal}(L|K)$. Sei die *Norm* erklärt durch

$$\begin{array}{ccc} L & \xrightarrow{\mathrm{N}_G} & K \\ x & \longmapsto & \mathrm{N}_G(x) := \prod_{\sigma \in G} \sigma(x) \end{array}$$

(1) Verifiziere, daß in der Tat $\mathrm{N}_G(x) \in K$ ist.

(2) Sei q eine Primpotenz. Sei $s \geqslant 1$. Sei $L = \mathbf{F}_{q^s}$ and $K = \mathbf{F}_q$. Weise die Norm als surjektiv nach.

Aufgabe 53 (Aufgabe 54) *Sei $m \geqslant 0$. Sei K ein Körper mit $|K| \geqslant m$.*

Sei V ein Vektorraum. Sei $U_i \subset V$ ein Teilraum für $i \in [1, m]$.

Zeige $\bigcup_{i\in[1,m]} U_i \subset V$.

Aufgabe 54 (§2.5, §3.5.1.4) Sei K ein perfekter Körper. Sei $L|K$ eine endliche Körpererweiterung. Zeige, daß es ein $t \in L$ mit $L = K(t)$ gibt.

Aufgabe 55 (§1.8.5, §1.9) Sei $f(X) = \sum_{k\geqslant 0} a_k X^k \in \mathbf{Z}[X]$ normiert und von Grad $n := \deg f$ gegeben.

(1) Sei $f(X) = g(X)h(X)$ mit $g(X)$, $h(X) \in \mathbf{Q}[X]$ normiert.
Zeige $g(X)$, $h(X) \in \mathbf{Z}[X]$.

(2) Sei p eine Primzahl. Sei $a_i \equiv_p 0$ für $i \in [0, n-1]$, aber $a_0 \not\equiv_{p^2} 0$.
Zeige, daß $f(X) \in \mathbf{Q}[X]$ irreduzibel ist.

5.2 Lösungen

Aufgabe 1

(1) Die Substitution liefert

$$\begin{aligned} x^3+ax^2+bx+c &= (y-\tfrac{a}{3})^3+a(y-\tfrac{a}{3})^2+b(y-\tfrac{a}{3})+c \\ &= y^3+(b-\tfrac{1}{3}a^2)y+(\tfrac{2}{27}a^3-\tfrac{1}{3}ab+c)\,. \end{aligned}$$

Also wird $p=b-\frac{1}{3}a^2$ und $q=\frac{2}{27}a^3-\frac{1}{3}ab+c$.

(2) Die Substitution liefert für $z\neq 0$

$$\begin{aligned} y^3+py+q &= (z-\tfrac{p}{3z})^3+p(z-\tfrac{p}{3z})+q \\ &= z^3+q-\tfrac{p^3}{27}z^{-3}\,. \end{aligned}$$

Mit $y=z-\frac{p}{3z}$ ist also $z^3+q-\frac{p^3}{27}\,z^{-3}=y^3+py+q$ für $z\neq 0$. Finden wir ein $z\in\mathbf{C}\setminus\{0\}$, das Nullstelle der linken Seite ist, so ist das zugehörige y Nullstelle der rechten Seite.

(3) Beachte, daß für $z\in\mathbf{C}$ mit $(z^3)^2+qz^3-\frac{p^3}{27}=0$ wegen $p\neq 0$ auch $z\neq 0$ ist. Also ist

$$\begin{aligned} \{z\in\mathbf{C}\setminus\{0\}\ :\ z^3+q-\tfrac{p^3}{27}z^{-3}=0\} &= \{z\in\mathbf{C}\ :\ (z^3)^2+qz^3-\tfrac{p^3}{27}=0\} \\ &= \left\{z\in\mathbf{C}\ :\ z^3=-\tfrac{q}{2}\pm\sqrt{\tfrac{q^2}{4}+\tfrac{p^3}{27}}\right\}\,. \end{aligned}$$

Beachte, daß die letzte Gleichung im Komplexen im Falle + und im Falle − im allgemeinen je 3 Lösungen hat. In der Tat, ist $w=|w|\exp(\mathrm{i}\arg w)\in\mathbf{C}\setminus\{0\}$, so ist $z=\sqrt[3]{|w|}\exp(\mathrm{i}\arg w/3+2\pi\mathrm{i}k/3)$ eine Lösung von $z^3=w$ für $k\in\{0,1,2\}$

(4) Die Substitution in (1) liefert $p=\frac{5}{12}$ und $q=-\frac{31}{54}$. Wir haben also gemäß (2)

$$z^6-\tfrac{31}{54}z^3+\tfrac{125}{46656}\ =\ 0$$

zu lösen. Nun ist $\sqrt{\frac{1}{4}(-\frac{31}{54})^2-\frac{125}{46656}}=\frac{7}{24}$. Also können wir etwa

$$z^3\ =\ -\tfrac{1}{2}\cdot(-\tfrac{31}{54})+\tfrac{7}{24}\ =\ \tfrac{125}{216}$$

ansetzen (Fall + in (3)) und $z=\sqrt[3]{\frac{125}{216}}=\frac{5}{6}$ verwenden.

Somit wird $y=z-\frac{1}{3}\cdot\frac{5}{12}\,z^{-1}=\frac{2}{3}$.

Schließlich wird $x=y-\frac{1}{3}\cdot\frac{1}{2}=\frac{1}{2}$ eine Lösung von $x^3+\frac{1}{2}x^2+\frac{1}{2}x-\frac{1}{2}=0$.

(Die komplette Faktorisierung ergibt sich zu

$$x^3+\tfrac{1}{2}x^2+\tfrac{1}{2}x-\tfrac{1}{2}\ =\ (x-\tfrac{1}{2})(x+\tfrac{1}{2}-\tfrac{\mathrm{i}}{2}\sqrt{3})(x+\tfrac{1}{2}+\tfrac{\mathrm{i}}{2}\sqrt{3})\ .\ )$$

Der Fall dreier verschiedener reeller Nullstellen (casus irreducibilis) eines Polynoms dritten Grades mit reellen Koeffizienten ist mit diesem Verfahren haarig, da man selbst bei ganzzahligen Nullstellen diese nicht immer aus den erhaltenen verschachtelten Wurzelausdrücken komplexer Zahlen erkennen kann. Aber immerhin finden wir eine Lösung, wenn auch manchmal nicht in optimaler Gestalt.

Aufgabe 2

(1) Eine positive ganze Zahl teilt a und b genau dann, wenn sie $\mathrm{ggT}(a,b)$ teilt. Diese Eigenschaft legt $\mathrm{ggT}(a,b)$ auch fest, da eine positive ganze Zahl durch die Menge ihrer Teiler bestimmt ist – als deren Maximum.

Wir haben also zu zeigen, daß $x \in \mathbf{Z}_{\geqslant 0}$ genau dann a und b teilt, wenn sie a und r teilt.

Teile x die beiden Zahlen a und b. Dann ist x auch ein Teiler von $b - aq = r$.

Teile umgekehrt x die beiden Zahlen a und r. Dann ist x auch ein Teiler von $aq + r = b$.

(2) Es ist $x_0 > x_1 > x_2 > \ldots$ eine strikt fallende Folge nichtnegativer ganzer Zahlen. Diese muß an einer Stelle Null werden, was die Existenz von ℓ mit $x_\ell > 0$ und $x_{\ell+1} = 0$ zeigt.

Desweiteren ist mit (1)

$$\mathrm{ggT}(a,b) \;=\; \mathrm{ggT}(x_0,x_1) \;=\; \mathrm{ggT}(x_1,x_2) \;=\; \cdots \;=\; \mathrm{ggT}(x_\ell,x_{\ell+1}) \;=\; \mathrm{ggT}(x_\ell,0) \;=\; x_\ell\ .$$

(3) Wir behaupten, daß $x_k s_k + x_{k-1}s_{k+1} = x_\ell$ für alle $k \in [1,\ell]$, insbesondere also für $k = 1$. Wir führen eine absteigende Induktion nach k. Der Induktionsanfang ist durch $x_\ell s_\ell + x_{\ell-1}s_{\ell+1} = x_\ell$ gesichert. Für den Induktionsschritt nehmen wir $x_k s_k + x_{k-1}s_{k+1} = x_\ell$ für ein $k \in [2,\ell]$ als bekannt an. Wir erhalten

$$\begin{array}{rcl} x_{k-1}s_{k-1} + x_{k-2}s_k & = & x_{k-1}(s_{k+1} - s_k q_{k-1}) + (x_{k-1}q_{k-1} + x_k)s_k \\ & = & x_k s_k + x_{k-1}s_{k+1} \\ & = & x_\ell\ . \end{array}$$

(4) Euklid liefert

$$\begin{array}{rcl} 87 & = & 23 \cdot 3 + 18 \\ 23 & = & 18 \cdot 1 + 5 \\ 18 & = & 5 \cdot 3 + 3 \\ 5 & = & 3 \cdot 1 + 2 \\ 3 & = & 2 \cdot 1 + 1 \\ 2 & = & 1 \cdot 2 + 0\ . \end{array}$$

Hier bricht der Algorithmus wegen des erhaltenen Restes 0 ab. Also ist $x_0 = 87$, $x_1 = 23$, $x_2 = 18$, $x_3 = 5$, $x_4 = 3$, $x_5 = 2$, $x_6 = 1$ und $x_7 = 0$. Insbesondere ist $\ell = 6$. Ferner werden $q_1 = 3$, $q_2 = 1$, $q_3 = 3$, $q_4 = 1$, $q_5 = 1$ und $q_6 = 2$.

Es folgt $\mathrm{ggT}(23,87) = 1$.

> Dies hätte man auch mit Primfaktorzerlegungen erkennen können. Bei großen Zahlen ist eine solche Zerlegung allerdings schwieriger durchzuführen als der Euklidsche Algorithmus.

Darüberhinaus erhalten wir als Folge der s_k mittels $s_{k-1} = s_{k+1} - s_k q_{k-1}$ folgendes, angefangen mit $s_7 = 0$, $s_6 = 1$.

$$\begin{array}{rcll} s_5 & = & 0 - 1 \cdot 1 & = \quad -1 \\ s_4 & = & 1 - (-1) \cdot 1 & = \quad 2 \\ s_3 & = & (-1) - 2 \cdot 3 & = \quad -7 \\ s_2 & = & 2 - (-7) \cdot 1 & = \quad 9 \\ s_1 & = & (-7) - 9 \cdot 3 & = \quad -34 \end{array}$$

Also wird $1 = x_\ell = x_1 s_1 + x_0 s_2 = 23 \cdot (-34) + 87 \cdot 9$, wie man leicht durch Nachrechnen nochmals bestätigt.

Aufgabe 3

(1) Es ist $4 \cdot 3 + 1 \equiv_7 13 \equiv_7 -1$.

Gemäß unserer Konvention wäre es auch zulässig gewesen, $4 \cdot 3 + 1 = -1$ zu schreiben, da aus dem Kontext hervorgeht, daß wir in $\mathbf{Z}/7\mathbf{Z}$ rechnen.

Es ist $6 \cdot 5 \cdot 4 = 30 \cdot 4 \equiv_7 2 \cdot 4 \equiv_7 1$.

(2) Es ist $3 \cdot 5 \cdot 7 \cdot 9 = 15 \cdot 63 \equiv_{32} 15 \cdot (-1) = -15$.
Es ist $31^{31} \equiv_3 2(-1)^{31} \equiv_{32} -1$.
Es ist $4^3 = 64 \equiv_{32} 0$.

Aufgabe 4

(1) Sei $g := \mathrm{ggT}(k, m) > 1$. *Nehmen wir an,* es ist $k + m\mathbf{Z}$ invertierbar. Dann gibt es ein $\ell \in \mathbf{Z}$ mit $k\ell \equiv_m 1$. Somit gibt es ein $u \in \mathbf{Z}$ mit $k\ell + um = 1$. Da aber g sowohl k als auch m teilt, teilt g auch $k\ell + um = 1$, *Widerspruch.*
Sei $\mathrm{ggT}(k, m) = 1$. Mit dem Euklidschen Algorithmus aus Aufgabe 2.(3) gibt es $s, t \in \mathbf{Z}$ mit $sk + tm = 1$. Also ist $sk \equiv_m 1$, d.h. $(s + m\mathbf{Z})(k + m\mathbf{Z}) = 1 + m\mathbf{Z}$.
Es ist $23 \cdot (-34) + 87 \cdot 9 = 1$, vgl. Aufgabe 2.(4). Also ist $23 \cdot (-34) \equiv_{87} 1$, d.h. $(23 + 87\mathbf{Z})^{-1} = -34 + 87\mathbf{Z}$.
Um $(17 + 1000\mathbf{Z})^{-1}$ zu berechnen, verwenden wir ebenfalls den Euklidschen Algorithmus. Wir erhalten

$$\begin{aligned} 1000 &= 17 \cdot 58 + 14 \\ 17 &= 14 \cdot 1 + 3 \\ 14 &= 3 \cdot 4 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0\,, \end{aligned}$$

wobei uns $\mathrm{ggT}(1000, 17) = 1$ gar nicht so sehr interessiert, sondern vielmehr

$$\begin{aligned} 0 - 1 \cdot 1 &= -1 \\ 1 - (-1) \cdot 4 &= 5 \\ (-1) - 5 \cdot 1 &= -6 \\ 5 - (-6) \cdot 58 &= 353\,, \end{aligned}$$

und also $353 \cdot 17 + (-6) \cdot 1000 = \mathrm{ggT}(1000, 17) = 1$.

(2) Ist $1/n = 0.\overline{a_1 a_2 \ldots a_k}$ mit Ziffern $a_i \in [0, 9]$, so bedeutet dies, daß $\frac{a_1 a_2 \ldots a_k}{99\ldots9} = 1/n$ (k-mal die Ziffer 9), und $k \geqslant 1$ ist minimal so gewählt, daß dies möglich ist. In anderen Worten, $k \geqslant 1$ ist minimal so gewählt, daß n ein Teiler von $10^k - 1$ ist. Abermals in anderen Worten, $k \geqslant 1$ ist minimal so gewählt, daß $10^k \equiv_n 1$.
Es ist $1/7 = 0.\overline{142857}$, die Periodenlänge ist also gleich 6. Und in der Tat ist

$$\begin{aligned} 10^1 &\equiv_7 3 \equiv_7 3 \\ 10^2 &\equiv_7 30 \equiv_7 2 \\ 10^3 &\equiv_7 20 \equiv_7 -1 \\ 10^4 &\equiv_7 -10 \equiv_7 -3 \\ 10^5 &\equiv_7 -30 \equiv_7 -2 \\ 10^6 &\equiv_7 -20 \equiv_7 1\,. \end{aligned}$$

Es ist $1/41 = 0.\overline{02439}$, die Periodenlänge ist also gleich 5. Und in der Tat ist

$$\begin{aligned} 10^1 &\equiv_{41} 10 \equiv_{41} 10 \\ 10^2 &\equiv_{41} 100 \equiv_{41} 18 \\ 10^3 &\equiv_{41} 180 \equiv_{41} 16 \\ 10^4 &\equiv_{41} 160 \equiv_{41} -4 \\ 10^5 &\equiv_{41} -40 \equiv_{41} 1\,. \end{aligned}$$

Aufgabe 5

(1) Die Substitution liefert

$$\begin{aligned} x^4 + ax^3 + bx^2 + cx &= (y - \tfrac{a}{4})^4 + a(y - \tfrac{a}{4})^3 + b(y - \tfrac{a}{4})^2 + c(y - \tfrac{a}{4}) + d \\ &= y^4 + (b - \tfrac{3}{8}a^2)y^2 + (\tfrac{1}{8}a^3 - \tfrac{1}{2}ab + c)y + (\tfrac{1}{16}a^2b - \tfrac{3}{256}a^4 - \tfrac{1}{4}ac + d) \end{aligned}$$

Also wird $p = b - \frac{3}{8}a^2$, $q = \frac{1}{8}a^3 - \frac{1}{2}ab + c$ und $r = \frac{1}{16}a^2b - \frac{3}{256}a^4 - \frac{1}{4}ac + d$.

(2) Zunächst können wir in beiden Fällen die Gleichung $y^4 + py^2 + qy + r = 0$ für noch beliebiges $\alpha \in \mathbf{C}$ äquivalent umformen zu

$$(*) \qquad (y^2 - \alpha)^2 \;=\; -(2\alpha + p)y^2 - qy + (\alpha^2 - r)\;.$$

Sei nun $\alpha \in \mathbf{C}$ so gewählt, daß $\alpha^3 + \frac{1}{2}p\alpha^2 - r\alpha - \frac{1}{2}pr + \frac{1}{8}q^2 = 0$.

Ist $p + 2\alpha = 0$, so kann nach Wahl von α nur $q = 0$ gewesen sein. Dann aber schreibt sich die Gleichung $(*)$

$$(y^2 - \alpha)^2 \;=\; \alpha^2 - r\;.$$

Ist $p + 2\alpha \neq 0$, dann wird

$$\begin{aligned} -(2\alpha + p)(y + \tfrac{q}{2(2\alpha+p)})^2 &= -(2\alpha + p)y^2 - qy - \tfrac{q^2}{4(2\alpha+p)} \\ &= -(2\alpha + p)y^2 - qy + \tfrac{2\alpha^3 + p\alpha^2 - 2r\alpha - pr}{2\alpha+p} \\ &= -(2\alpha + p)y^2 - qy + \tfrac{(2\alpha+p)(\alpha^2 - r)}{2\alpha+p} \\ &= -(2\alpha + p)y^2 - qy + (\alpha^2 - r)\;. \end{aligned}$$

Die Bedingung an α ergibt sich aus der Forderung, die Diskriminante der rechten Seite von $(*)$, gesehen als quadratisches Polynom in y, verschwinden zu lassen.

(3) Die Substitution in (1) liefert $p = 1$, $q = \gamma$ und $r = -\frac{1}{2}$.

Ein $\alpha \in \mathbf{C}$, welches die Gleichung $\alpha^3 + \frac{1}{2}\alpha^2 + \frac{1}{2}\alpha - \frac{1}{2} = 0$ erfüllt, ist nach Aufgabe 1.(4) z.B. mit $\alpha = \frac{1}{2}$ gegeben. Da $p + 2\alpha = 2 \neq 0$, haben wir ein $y \in \mathbf{C}$ mit

$$(y^2 - \tfrac{1}{2})^2 \;=\; -2(y + \tfrac{\gamma}{4})^2\;.$$

zu finden. Hierfür lösen wir etwa

$$y^2 - \tfrac{1}{2} \;=\; \mathrm{i}\sqrt{2}(y + \tfrac{\gamma}{4})$$

(wofür wir auch das Negative der rechten Seite hätten heranziehen können). Wir formen nach Einsetzen des Wertes von γ äquivalent um zu

$$y^2 - \mathrm{i}\sqrt{2} \cdot y + \tfrac{1}{2}(\sqrt{3} - 1) \;=\; 0$$

Wir erhalten etwa

$$y \;=\; \mathrm{i}\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt[4]{3}}{\sqrt{2}}\;,$$

und also

$$x \;=\; -1 + \mathrm{i}\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt[4]{3}}{\sqrt{2}}\;.$$

(Die vollständige Faktorisierung lautet

$$\begin{aligned} &x^4 + 4x^3 + 7x^2 + (6 + \gamma)x + \tfrac{3}{2} + \gamma \;= \\ &(x + 1 - \mathrm{i}\tfrac{\sqrt{2}}{2} - \mathrm{i}\tfrac{\sqrt[4]{3}}{\sqrt{2}})(x + 1 - \mathrm{i}\tfrac{\sqrt{2}}{2} + \mathrm{i}\tfrac{\sqrt[4]{3}}{\sqrt{2}})(x + 1 + \mathrm{i}\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt[4]{3}}{\sqrt{2}})(x + 1 + \mathrm{i}\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt[4]{3}}{\sqrt{2}})\;.) \end{aligned}$$

Aufgabe 6

(1) Setze an mit $0 = 0_{R\times S} := (0_R, 0_S)$ und $1 = 1_{R\times S} := (1_R, 1_S)$. Setze an mit $-(r,s) := (-r,-s)$ für $r \in R$ und $s \in S$..

Für (r,s), (r',s'), $(r'',s'') \in R \times S$ wird

$$\begin{array}{lcll}
(r,s)+(r',s') & = & (r+r', s+s') & = (r'+r, s'+s) \\
 & & & = (r',s')+(r,s) \\
(r,s)+(0,0) & = & (r+0, s+0) & = (r,s) \\
(r,s)+(-r,-s) & = & (r-r, s-s) & = (0,0) \\
((r,s)+(r',s'))+(r'',s'') & = & ((r+r')+r'', (s+s')+s'') & = (r+(r'+r''), s+(s'+s'')) \\
 & & & = (r,s)+((r',s')+(r''+s'')) \\
(r,s)\cdot(r',s') & = & (r\cdot r', s\cdot s') & = (r'\cdot r, s'\cdot s) \\
 & & & = (r',s')\cdot(r,s) \\
(r,s)\cdot(1,1) & = & (r\cdot 1, s\cdot 1) & = (r,s) \\
((r,s)\cdot(r',s'))\cdot(r'',s'') & = & ((r\cdot r')\cdot r'', (s\cdot s')\cdot s'') & = (r\cdot(r'\cdot r''), s\cdot(s'\cdot s'')) \\
 & & & = (r,s)\cdot((r',s')\cdot(r''\cdot s'')) \\
((r,s)+(r',s'))\cdot(r'',s'') & = & ((r+r')\cdot r'', (s+s')\cdot s'') & = (r\cdot r''+r'\cdot r'', s\cdot s''+s'\cdot s'') \\
 & & & = (r,s)\cdot(r'',s'')+(r',s')\cdot(r'',s'')\,.
\end{array}$$

Kurz, die Ringeigenschaften sind erfüllt, da sie eintragsweise erfüllt sind.

Sind R und S Körper, so sind zwar $(1,0)$ und $(0,1)$ ungleich $(0,0)$, aber $(1,0)(0,1) = (0,0)$. Also ist $R \times S$ diesenfalls kein Körper. (Es ist noch nicht einmal ein Integritätsbereich.)

(2) Die Abbildung

$$\begin{array}{ccccc}
R & \longrightarrow & R/I & \times & R/J \\
r & \longmapsto & (r+I & , & r+J)
\end{array}$$

ist ein Ringmorphismus, da 1 auf $1 = (1+I, 1+J)$ abgebildet wird, da die Summe $r+s$ auf $(r+s+I, r+s+J) = (r+I, r+J)+(s+I, s+J)$ abgebildet wird und da für r, $s \in R$ das Produkt $r\cdot s$ auf $(r\cdot s+I, r\cdot s+J) = (r+I, r+J)\cdot(s+I, s+J)$ abgebildet wird, wobei r, $s \in R$.

Dieser hat Kern $I \cap J$, da ein Element r genau dann auf 0 abgebildet wird, wenn $r+I = 0+I$ und $r+J = 0+J$, d.h. genau dann, wenn $r \in I \cap J$. Das Lemma aus §1.4.3 gibt den injektiven Ringmorphismus

$$\begin{array}{ccccc}
R/(I\cap J) & \longrightarrow & R/I & \times & R/J \\
r+(I\cap J) & \longmapsto & (r+I & , & r+J)\,.
\end{array}$$

Wir haben die Surjektivität dieses Ringmorphismus zu zeigen. Nun ist nach Voraussetzung $I+J = R$, wir können also $x \in I$ und $y \in J$ mit $x+y = 1$ finden. Es wird

$$x+I\cap J \longmapsto (x+I, x+J) = (0+I, x+y+J) = (0+I, 1+J)$$

abgebildet. Ferner wird

$$y+I\cap J \longmapsto (y+I, y+J) = (y+x+I, 0+J) = (1+I, 0+J)$$

abgebildet.

Sei nun $(u+I, v+J) \in R/I \times R/J$ vorgegeben. Da ein Ringmorphismus vorliegt, wird in der Tat

$$\begin{array}{rcl}
uy+vx+I\cap J & \longmapsto & (u+I,u+J)(y+I,y+J)+(v+I,v+J)(x+I,x+J) \\
 & = & (u+I,u+J)(1+I,0+J)+(v+I,v+J)(0+I,1+J) \\
 & = & (u+I,0+J)+(0+I,v+J) \\
 & = & (u+I,v+J)\,.
\end{array}$$

Kurz, da y auf $(1,0)$ und x auf $(0,1)$ geht, müssen nur y und x entsprechend zusammengesetzt werden, um im Bild $(r+I, s+J)$ zu erhalten.

Wir merken uns noch für Verwendung in (3), daß $uy+vx+I\cap J$ ein Urbild, und wegen Injektivität das Urbild von $(u+I, v+J)$ ist.

(3) Mit (2) bleibt zum einen zu zeigen, daß $m\mathbf{Z} + n\mathbf{Z} = \mathbf{Z}$, i.e. daß $m\mathbf{Z} + n\mathbf{Z} \supseteq \mathbf{Z}$. Da aber $1 = ms + nt \in m\mathbf{Z} + n\mathbf{Z}$ ist, ist auch $\mathbf{Z} = 1\mathbf{Z} \subseteq m\mathbf{Z} + n\mathbf{Z}$.

Zum anderen müssen wir $m\mathbf{Z} \cap n\mathbf{Z} = mn\mathbf{Z}$ nachweisen. Die Inklusion $\supseteq$ ist ersichtlich, auch ohne Verwendung der Voraussetzung $\mathrm{ggT}(m, n) = 1$.

Zeigen wir die Inklusion $\subseteq$. Sei $x \in m\mathbf{Z} \cap n\mathbf{Z}$. Schreibe $x = ma = nb$ für gewisse $a, b \in \mathbf{Z}$. Insbesondere teilt n das Produkt ma. Da n und m teilerfremd sind, teilt n daher a. Wir schreiben $a = nc$ für ein $c \in \mathbf{Z}$. Es wird $x = ma = mnc \in mn\mathbf{Z}$.

Der Isomorphismus in die eine Richtung ist wie in (2) gegeben durch

$$\begin{array}{rcl} \mathbf{Z}/mn\mathbf{Z} & \xrightarrow{\sim} & \mathbf{Z}/m\mathbf{Z} \quad \times \quad \mathbf{Z}/n\mathbf{Z} \\ z + mn\mathbf{Z} & \longmapsto & (z + m\mathbf{Z} \quad , \quad z + n\mathbf{Z}) \, . \end{array}$$

Da $ms + nt = 1$, folgt mit der Bemerkung am Ende von (2), daß für $u, v \in \mathbf{Z}$ das Urbild eines Elements $(u + m\mathbf{Z}, v + n\mathbf{Z})$ der rechten Seite durch $unt + vms + mn\mathbf{Z}$ gegeben ist. Dies liefert die Umkehrbijektion

$$\begin{array}{rcl} \mathbf{Z}/mn\mathbf{Z} & \xleftarrow{\sim} & \mathbf{Z}/m\mathbf{Z} \quad \times \quad \mathbf{Z}/n\mathbf{Z} \\ unt + vms + mn\mathbf{Z} & \longmapsfrom & (u + m\mathbf{Z} \quad , \quad v + n\mathbf{Z}) \, . \end{array}$$

Nach der ersten Bemerkung in §1.4.1 ist die Umkehrbijektion eines Ringisomorphismus ebenfalls ein Ringisomorphismus. (Dies hier direkt zu prüfen, wäre etwas lästig!)

(4) Die Aussage über den Isomorphismus folgt wegen $\mathrm{ggT}(3, 4) = 1$ aus (3).

Finden wir nun die Isomorphismen in beide Richtungen. Es ist $3 \cdot (-1) + 4 \cdot 1 = 1$, wie man auch ohne Euklid erkennt. Wir haben also $m = 3$, $s = -1$, $n = 4$ und $t = 1$ in die Lösung von (3) einzusetzen. Wir erhalten so

$$\begin{array}{rcl} \mathbf{Z}/12\mathbf{Z} & \xrightarrow{\sim} & \mathbf{Z}/3\mathbf{Z} \quad \times \quad \mathbf{Z}/4\mathbf{Z} \\ z + 12\mathbf{Z} & \longmapsto & (z + 3\mathbf{Z} \quad , \quad z + 4\mathbf{Z}) \, . \end{array}$$

in die eine und

$$\begin{array}{rcl} \mathbf{Z}/12\mathbf{Z} & \xleftarrow{\sim} & \mathbf{Z}/3\mathbf{Z} \quad \times \quad \mathbf{Z}/4\mathbf{Z} \\ 4u - 3v + 12\mathbf{Z} & \longmapsfrom & (u + 3\mathbf{Z} \quad , \quad v + 4\mathbf{Z}) \, . \end{array}$$

in die andere Richtung.

(Elementar ausgedrückt bedeutet dies nun, daß bei gegebenen $u, v \in \mathbf{Z}$ die Lösungen des Kongruenzsystems

$$\begin{array}{rcl} x & \equiv_3 & u \\ x & \equiv_4 & v \end{array}$$

gegeben sind durch $x \in \{4u - 3v + 12k \ : \ k \in \mathbf{Z}\}$.)

Aufgabe 7

(1) Um zu zeigen, daß $K \xrightarrow{f} R$ injektiv ist, müssen wir gemäß Lemma in §1.4.3 zeigen, daß $\mathrm{Kern}\, f = \{0_K\}$.

Mit demselben Lemma wissen wir, daß $\mathrm{Kern}\, f \subseteq K$ ein Ideal ist. Dank der letzten Bemerkung aus §1.2 wissen wir, daß dies $\mathrm{Kern}\, f = \{0_K\}$ oder $\mathrm{Kern}\, f = K$ zur Folge hat.

Sei *angenommen,* es ist $\mathrm{Kern}\, f = K$. Dann bildet f alle Elemente von K auf 0_R ab. Insbesondere wird $1_R = f(1_K) = 0_R$. Ist nun $x \in R$, so wird $x = x \cdot 1_R = x \cdot 0_R = 0_R$, und mithin $R = \{0_R\}$, *Widerspruch.*

Also ist $\mathrm{Kern}\, f = \{0_K\}$, wie zu zeigen war.

(2) Es ist $\varphi : K[X] \longrightarrow K$, $f(X) \longmapsto f(0) = f_0$ ein Ringmorphismus, wie man entweder direkt verifiziert, oder aber aus der Bemerkung aus §1.6.2 mit $n = 1$, $a = \mathrm{id}_K$ und $s = 0$ entnimmt – kurz, die Prozedur des Einsetzens der 0 ist ein Ringmorphismus.

Ist $f(X) = \sum_{i\geqslant 0} f_i X^i \in \operatorname{Kern}\varphi$, so ist $f_0 = 0$, und wir können $f(X) = X \cdot (\sum_{i\geqslant 1} f_{i+1} X^i)$ schreiben. Somit ist $\operatorname{Kern}\varphi \subseteq XR[X]$.

Ist umgekehrt $f(X) \in XR[X]$, so können wir $f(X) = Xg(X)$ für ein $g(X) \in R[X]$ schreiben und erhalten durch Koeffizientenvergleich $f_0 = 0$.

Insgesamt ist also $\operatorname{Kern}\varphi = XR[X]$.

Das Lemma aus §1.4.3 zeigt nun, da φ surjektiv ist, daß $R[X]/\operatorname{Kern}\varphi \simeq R$ ist.

Aufgabe 8

(1) Es ist $h(X) = f(X)q(X) + r(X)$. Wir haben zu zeigen, daß

$$f(X)K[X] + h(X)K[X] \stackrel{!}{=} f(X)K[X] + r(X)K[X] \,.$$

Da $h(X) = f(X)q(X)+r(X)$, ist $h(X)$ in der rechten Seite enthalten. Da auch $f(X)$ in der rechten Seite enthalten ist, ist jedes Element der linken Seite in der rechten Seite enthalten.

Da $r(X) = -f(X)q(X)+h(X)$, ist $r(X)$ in der linken Seite enthalten. Da auch $f(X)$ in der linken Seite enthalten ist, ist jedes Element der rechten Seite in der linken Seite enthalten.

(2) Es ist $\deg u_1 > \deg u_2 > \deg u_3 > \dots$ strikt fallend und kann daher nicht unendlich lang in $\mathbf{Z}_{\geqslant 0}$ fortgesetzt werden. Also muß es ein $\ell \geqslant 0$ geben, bei dem zwar noch $\deg u_\ell \geqslant 0$, aber $\deg u_{\ell+1} = -\infty$ ist, i.e. $u_{\ell+1}(X) = 0$.

Mit (1) ist nun

$$\begin{array}{rcl} h(X)K[X] + f(X)K[X] & = & u_0(X)K[X] + u_1(X)K[X] \\ & = & u_1(X)K[X] + u_2(X)K[X] \\ & = & \cdots \\ & = & u_\ell(X)K[X] + u_{\ell+1}(X)K[X] \\ & = & g(X)K[X] + 0 \cdot K[X] \\ & = & g(X)K[X] \,. \end{array}$$

(3) Wir behaupten, daß $u_k(X)s_k(X) + u_{k-1}(X)s_{k+1}(X) = g(X)$ für alle $k \in [1, \ell]$, insbesondere also für $k = 1$, was dann $f(X)s_1(X) + h(X)s_2(X) = g(X)$ gibt.

Wir führen eine absteigende Induktion nach k. Der Induktionsanfang ist durch $u_\ell(X)s_\ell(X) + u_{\ell-1}(X)s_{\ell+1}(X) = u_\ell(X) = g(X)$ gesichert. Für den Induktionsschritt nehmen wir $u_k(X)s_k(X) + u_{k-1}(X)s_{k+1}(X) = g(X)$ für ein $k \in [2, \ell]$ als bekannt an. Wir erhalten

$$\begin{array}{rl} & u_{k-1}(X)s_{k-1}(X) + u_{k-2}(X)s_k(X) \\ = & u_{k-1}(X)(s_{k+1}(X) - s_k(X)q_{k-1}(X)) + (u_{k-1}(X)q_{k-1}(X) + u_k(X))s_k(X) \\ = & u_{k-1}(X)s_{k+1}(X) + u_k(X)s_k(X) \\ = & g(X) \,. \end{array}$$

(4) Euklid liefert

$$\begin{array}{lcl} (X^8 + X^3 + X + 1) & = & (X^3 + 1)(X^5 + X^2 + 1) + (X^2 + X) \\ (X^3 + 1) & = & (X^2 + X)(X + 1) + (X + 1) \\ (X^2 + X) & = & (X + 1)X + 0 \,. \end{array}$$

Also ist $\ell = 3$ und $g(X) = X + 1$, und wir erhalten als Folge der $s_k(X)$ mit $s_4(X) = 0$ und $s_3(X) = 1$

$$\begin{array}{rcll} s_2(X) & = & 0 - 1 \cdot (X + 1) & = & X + 1 \\ s_1(X) & = & 1 - (X + 1) \cdot (X^5 + X^2 + 1) & = & X^6 + X^5 + X^3 + X^2 + X \end{array}$$

Es wird so $f(X)s_1(X) + h(X)s_2(X) = g(X)$, i.e.

$$(X^3+1)(X^6+X^5+X^3+X^2+X) + (X^8+X^3+X+1)(X+1) \;=\; (X+1)\,,$$

wie man auch leicht nachrechnet.

Aufgabe 9

Die Formel für die Addition folgt aus

$$\begin{aligned} rf(X) + sg(X) &= (\textstyle\sum_{i\geqslant 0}(rf_i + sg_i)X^i)' \\ &= \textstyle\sum_{i\geqslant 1} i(rf_i + sg_i)X^{i-1} \\ &= r\cdot(\textstyle\sum_{i\geqslant 1} if_iX^{i-1}) + s\cdot(\textstyle\sum_{i\geqslant 1} ig_iX^{i-1}) \\ &= rf'(X) + sg'(X)\,. \end{aligned}$$

Für die Formel für die Multiplikation zeigen wir zunächst, daß sie im Falle $f(X) = X^i$ und $g(X) = X^j$ gilt, wobei $i,\, j \in \mathbf{Z}_{\geqslant 0}$.

Es wird, falls $i \geqslant 1$ und $j \geqslant 1$,

$$\begin{aligned} (X^iX^j)' &= (X^{i+j})' \\ &= (i+j)(X^{i+j-1}) \\ &= i(X^{i-1})\cdot X^j + X^i\cdot j(X^{j-1}) \\ &= (X^i)'X^j + X^i(X^j)'\,. \end{aligned}$$

Falls $i = 0$, so wird $(X^0X^j)' = (X^j)' = (X^0)'X^j + X^0(X^j)'$. Analog im Fall $j = 0$.

Im allgemeinen Fall wird nun, unter Verwendung der Formel für die Addition

$$\begin{aligned} (f(X)g(X))' &= ((\textstyle\sum_{i\geqslant 0} f_iX^i)(\sum_{j\geqslant 0} g_jX^j))' \\ &= (\textstyle\sum_{i\geqslant 0}\sum_{j\geqslant 0} f_ig_jX^{i+j})' \\ &= \textstyle\sum_{i\geqslant 0}\sum_{j\geqslant 0} f_ig_j(X^{i+j})' \\ &= \textstyle\sum_{i\geqslant 0}\sum_{j\geqslant 0} f_ig_j((X^i)'X^j + X^i(X^j)') \\ &= \textstyle\sum_{i\geqslant 0}\sum_{j\geqslant 0} f_ig_j(X^i)'X^j + \sum_{i\geqslant 0}\sum_{j\geqslant 0} f_ig_jX^i(X^j)' \\ &= (\textstyle\sum_{i\geqslant 0} f_i(X^i)')(\sum_{j\geqslant 0} g_jX^j) + (\sum_{i\geqslant 0} f_iX^i)(\sum_{j\geqslant 0} g_j(X^j)') \\ &= (\textstyle\sum_{i\geqslant 0} f_iX^i)'(\sum_{j\geqslant 0} g_jX^j) + (\sum_{i\geqslant 0} f_iX^i)(\sum_{j\geqslant 0} g_jX^j)' \\ &= f'(X)g(X) + f(X)g'(X)\,. \end{aligned}$$

Aufgabe 10

(1) Sei $x \in R\setminus\{0\}$. Wir haben zu zeigen, daß x invertierbar ist. Die Abbildung $R \longrightarrow R$, $r \longmapsto xr$ ist injektiv. Da für $u,\, v \in K$ und $r,\, s \in R$ auch gilt, daß $x(ur+vs) = u(xr)+v(xs)$, ist diese Abbildung K-linear. Nun ist eine K-lineare Abbildung eines endlichdimensionalen Vektorraums in sich, auch als K-linearer Endomorphismus bezeichnet, genau dann injektiv, wenn die Determinante ihrer beschreibenden Matrix bezüglich einer gewählten Basis nicht verschwindet. Dann aber ist diese Matrix invertierbar, was zeigt, daß die fragliche Abbildung auch bijektiv ist.

Da nun insbesondere die Surjektivität der Abbildung $R \longrightarrow R$, $r \longmapsto xr$ nachgewiesen wurde, haben wir unter anderem das Element 1_R im Bild. Somit gibt es ein $r \in R$ so, daß $xr = 1_R$ ist. Mithin ist x invertierbar.

(2) Es ist $n = \dim_{\mathbf{R}} \mathbf{C} = 2$. Zum Beispiel kann man die Basis $(1+\mathrm{i}, 1-\mathrm{i})$ von $\mathbf{C}$ über $\mathbf{R}$ anführen.

Eine solche Basis heißt auch *Normalbasis*. Siehe auch [**1,** §II.N].

Aufgabe 11

(1) (a) Falls $b\langle a\rangle \cap b'\langle a\rangle \neq \emptyset$, dann gibt es ein Element $g \in G$ mit $g = ba^k = b'a^{k'}$ für gewisse $k, k' \in \mathbf{Z}$. Wir behaupten, daß $b\langle a\rangle = b'\langle a\rangle$. Aus Symmetriegründen genügt es zu zeigen, daß $b\langle a\rangle \subseteq b'\langle a\rangle$. Sei $\ell \in \mathbf{Z}$ gegeben. Wir haben zu zeigen, daß $ba^\ell \in b'\langle a\rangle$. In der Tat ist $b = b'a^{k'-k}$ und also $ba^\ell = ba^{k'-k+\ell} \in b'\langle a\rangle$.

(b) Zunächst einmal halten wir fest, daß Multiplikation mit b von links eine bijektive Abbildung $G \longrightarrow G$, $g \longmapsto bg$ liefert, invertiert von der Multiplikation mit b^{-1} von links. Also ist

$$|b\langle a\rangle| \;=\; |1\langle a\rangle| \;=\; |\{a^k \;:\; k \in \mathbf{Z}\}| \;.$$

Wenn wir für ein $k \in \mathbf{Z}$ mit Division mit Rest $k = \mathrm{o}(a)q + r$ mit $q \in \mathbf{Z}$ und $r \in [0, \mathrm{o}(a) - 1]$ schreiben, so erkennen wir, daß

$$a^k \;=\; a^{\mathrm{o}(a)q+r} \;=\; (a^{\mathrm{o}(a)})^q \cdot a^r \;=\; a^r \;.$$

Also ist $\{a^k \;:\; k \in \mathbf{Z}\} = \{a^k \;:\; k \in [0, \mathrm{o}(a) - 1]\}$.

Bleibt zu zeigen, daß $a^k \neq a^\ell$ für $0 \leqslant k < \ell \leqslant \mathrm{o}(a) - 1$. *Wäre* dem nicht so, dann wäre $a^{\ell-k} = 1$, obwohl $1 \leqslant \ell - k < \mathrm{o}(g)$, im *Widerspruch* zur Minimalität in der Definition von $\mathrm{o}(a)$.

(c) Mit (a) ist G eine disjunkte Vereinigung von Mengen der Form $b\langle a\rangle$ für gewisse $b \in G$. Diese Mengen haben mit (b) aber alle Kardinalität $\mathrm{o}(a)$. Somit ist $|G|$ ein Vielfaches von $\mathrm{o}(a)$.

(2) In $\mathbf{F}_7$ ist

$$\begin{array}{rcr} 3^1 &=& 3 \\ 3^2 &=& 2 \\ 3^3 &=& -1 \\ 3^4 &=& -3 \\ 3^5 &=& -2 \\ 3^6 &=& 1 \;. \end{array}$$

Wir entnehmen dieser Rechnung, daß

$$\begin{array}{rcrcr} \mathrm{o}(3^1) &=& \mathrm{o}(3) &=& 6 \\ \mathrm{o}(3^2) &=& \mathrm{o}(2) &=& 3 \\ \mathrm{o}(3^3) &=& \mathrm{o}(-1) &=& 2 \\ \mathrm{o}(3^4) &=& \mathrm{o}(-3) &=& 3 \\ \mathrm{o}(3^5) &=& \mathrm{o}(-2) &=& 6 \\ \mathrm{o}(3^6) &=& \mathrm{o}(1) &=& 1 \;. \end{array}$$

Alle diese Elementordnungen sind in der Tat Teiler von $7 - 1 = 6$.

(3) In $\mathbf{F}_{11}$ ist

$$\begin{array}{rcr} 2^1 &=& 2 \\ 2^2 &=& 4 \\ 2^3 &=& -3 \\ 2^4 &=& 5 \\ 2^5 &=& -1 \\ 2^6 &=& -2 \\ 2^7 &=& -4 \\ 2^8 &=& 3 \\ 2^9 &=& -5 \\ 2^{10} &=& 1 \;. \end{array}$$

Wir entnehmen dieser Rechnung, daß

$$\begin{array}{lcl} \mathrm{o}(2^1) &=& \mathrm{o}(2) \;=\; 10 \\ \mathrm{o}(2^2) &=& \mathrm{o}(4) \;=\; 5 \\ \mathrm{o}(2^3) &=& \mathrm{o}(-3) \;=\; 10 \\ \mathrm{o}(2^4) &=& \mathrm{o}(5) \;=\; 5 \\ \mathrm{o}(2^5) &=& \mathrm{o}(-1) \;=\; 2 \\ \mathrm{o}(2^6) &=& \mathrm{o}(-2) \;=\; 5 \\ \mathrm{o}(2^7) &=& \mathrm{o}(-4) \;=\; 10 \\ \mathrm{o}(2^8) &=& \mathrm{o}(3) \;=\; 5 \\ \mathrm{o}(2^9) &=& \mathrm{o}(-5) \;=\; 10 \\ \mathrm{o}(2^{10}) &=& \mathrm{o}(1) \;=\; 1\,. \end{array}$$

Alle diese Elementordnungen sind in der Tat Teiler von $11-1=10$.

Aufgabe 12

(1) Ist $a=0$, so ist $0^p=0$.

Ist $a\neq 0$, so ist mit Aufgabe 11.(1.c) ist $\mathrm{o}(a)$ ein Teiler von $|\mathbf{F}_p^\times|=p-1$, sagen wir $p-1=\mathrm{o}(a)\cdot m$ mit $m\in\mathbf{Z}_{\geqslant 1}$. Dann wird

$$a^{p-1} \;=\; a^{\mathrm{o}(a)\cdot m} \;=\; (a^{\mathrm{o}(a)})^m \;=\; 1\,,$$

und also $a^p=p$.

(2) Es hat mit (1) das Polynom X^p-X die Nullstellen $i\in\mathbf{F}_p$. Also zeigt sukzessives Abdividieren von Nullstellen, daß die linke Seite ein Vielfaches der rechten Seite ist. Da linke und rechte Seite normierte Polynome vom gleichen Grad p sind, ist die linke Seite gleich der rechten Seite.

Zum Beispiel wird $\prod_{i\in[0,3-1]}(X-i)=X^3-3X^2+2X$ in $\mathbf{Z}[X]$, und also in der Tat $\prod_{i\in\mathbf{F}_3}(X-i)=X^3-X$ in $\mathbf{F}_3[X]$.

(3) Für $p=2$ ist $(2-1)!=1\equiv_2 -1$.

Sei nun $p\geqslant 3$. Der Koeffizient von X auf der linken Seite von (2) ist gleich -1. Der Koeffizient von X auf der rechten Seite dagegen ist gleich $\prod_{i\in\mathbf{F}_p^\times} i$. Somit ist $-1=\prod_{i\in\mathbf{F}_p^\times} i$ in $\mathbf{F}_p$. In anderen Worten, es ist $-1\equiv_p (p-1)!$ in $\mathbf{Z}$.

Hingegen ist $(4-1)!=6\not\equiv_4 -1$. Also ist $(n-1)!\equiv_n -1$ für alle $n\in\mathbf{Z}_{\geqslant 1}$ nicht für alle $n\in\mathbf{Z}_{\geqslant 1}$ richtig.

> Man kann alternativ auch die Elemente von $\mathbf{F}_p^\times$ außer 1 und -1 zu sich invertierenden Paaren sortieren – beachte, daß das Polynom $X^2=1$ nur diese beiden Nullstellen aufweist, und daher in diesen Paaren jeweils zwei verschiedene Elemente stehen. Das Produkt über alle Elemente von $\mathbf{F}_p^\times$ ist also gleich
>
> $$1\cdot(-1)\cdot(\text{Produkt aller dieser Paareinträge}) \;=\; 1\cdot(-1)\cdot 1 \;=\; -1\,.$$

(4) Der Koeffizient von X^2 auf der linken Seite von (2) ist gleich 0, da $p\geqslant 3$. Der Koeffizient von X^2 auf der rechten Seite dagegen ist gleich

$$-\textstyle\sum_{j\in\mathbf{F}_p^\times}\prod_{i\in\mathbf{F}_p^\times\smallsetminus\{j\}} i\,.$$

Es folgt $0\equiv_p \sum_{j\in[1,p-1]}\frac{(p-1)!}{j}=:t(p)$ in $\mathbf{Z}$. Nun ist $s(p)=\frac{t(p)}{(p-1)!}$. Da $t(p)$ durch p teilbar ist, nicht aber $(p-1)!$, liefert auch vollständiges Kürzen einen durch p teilbaren Zähler von $s(p)$ in gekürzter Form.

> Der Zähler von $s(p)$ ist für $p\geqslant 5$ sogar durch p^2 teilbar (Hinweis von G. Nebe; Theorem von Wolstenholme).

Betrachte hierzu

$$\begin{aligned} 2\cdot s(p) &= (\tfrac{p}{1\cdot(p-1)}+\tfrac{1}{p-1})+(\tfrac{1}{2}+\tfrac{1}{p-2})+\cdots+(\tfrac{1}{p-1}+\tfrac{1}{1}) \\ &= \tfrac{p}{1\cdot(p-1)}+\tfrac{p}{2\cdot(p-2)}+\cdots+\tfrac{p}{(p-1)\cdot 1}\ . \end{aligned}$$

Wir haben also zu zeigen, daß $\frac{1}{1\cdot(p-1)}+\frac{1}{2\cdot(p-2)}+\cdots+\frac{1}{(p-1)\cdot 1}$ in gekürzter Form einen durch p teilbaren Nenner hat. Es genügt hierzu zu zeigen, daß die ganze Zahl

$$\tfrac{(p-1)!}{1}\cdot\tfrac{(p-1)!}{(p-1)}+\tfrac{(p-1)!}{2}\cdot\tfrac{(p-1)!}{(p-2)}+\cdots+\tfrac{(p-1)!}{(p-1)}\cdot\tfrac{(p-1)!}{1}$$

durch p teilbar ist. Nun ist $\frac{(p-1)!}{p-a}+\frac{(p-1)!}{a}=(p-1)!\frac{p}{(p-a)a}$ eine durch p teilbare ganze Zahl für $a\in[1,p-1]$, und mithin $\frac{(p-1)!}{p-a}\equiv_p -\frac{(p-1)!}{a}$. Also genügt es nach Ersetzung der jeweiligen zweiten Faktoren zu zeigen, daß

$$\tfrac{(p-1)!^2}{1^2}+\tfrac{(p-1)!^2}{2^2}+\cdots+\tfrac{(p-1)!^2}{(p-1)^2}$$

durch p teilbar ist.

Koeffizientenvergleich bei X^3 in (2) liefert, da $p\geqslant 5$, daß $0\equiv_p \sum_{0\leqslant i<j\leqslant p-1}\frac{(p-1)!}{ij}$. Also teilt p nach Multiplikation mit $2(p-1)!$ auch

$$\textstyle\sum_{i,\,j\,\in\,[0,p-1],\,i\neq j}\frac{(p-1)!^2}{ij}$$

Aus (3) wissen wir, daß p (und sogar p^2) ein Teiler von

$$\textstyle\sum_{i,\,j\,\in\,[0,p-1]}\frac{(p-1)!^2}{ij}\ =\ (\sum_{i\in[0,p-1]}\frac{(p-1)!}{i})^2$$

ist. Somit teilt p auch die Differenz dieser beiden Ausdrücke, und das ist gerade

$$\textstyle\sum_{i\in[0,p-1]}\frac{(p-1)!^2}{i^2}\ =\ \frac{(p-1)!^2}{1^2}+\frac{(p-1)!^2}{2^2}+\cdots+\frac{(p-1)!^2}{(p-1)^2}\ .$$

Aufgabe 13

(1) Da $\mathbf{Z}$ ein Hauptidealbereich ist, und da $a\mathbf{Z}\cap b\mathbf{Z}\neq\{0\}$ (da z.B. ab enthalten ist), gibt es genau ein $x\in\mathbf{Z}_{\geqslant 1}$ mit $a\mathbf{Z}\cap b\mathbf{Z}=x\mathbf{Z}$.

Wir behaupten, daß $x=\mathrm{kgV}(a,b)$ ist.

Zum einen ist $x\in a\mathbf{Z}$, also x Vielfaches von a, und $x\in b\mathbf{Z}$, also x Vielfaches von b.

Ist umgekehrt $y\in\mathbf{Z}_{\geqslant 1}$ gegeben mit y Vielfaches von a und y Vielfaches von b, dann ist $y\in a\mathbf{Z}\cap b\mathbf{Z}=x\mathbf{Z}$, und folglich y Vielfaches von x, insbesondere also $y\geqslant x$.

Also ist x das kleinste gemeinsame Vielfache von a und b, i.e. $x=\mathrm{kgV}(a,b)$.

Vgl. auch Aufgabe 6.(3); dort wurde der Spezialfall $\mathrm{ggT}(a,b)=1$ und also $\mathrm{kgV}(a,b)=ab$ gebraucht.

(2) Wir verwenden $a\mathbf{Z}\cap b\mathbf{Z}=\mathrm{kgV}(a,b)\mathbf{Z}$ nach (1) und $a\mathbf{Z}+b\mathbf{Z}=\mathrm{ggT}(a,b)\mathbf{Z}$ nach §1.7.2, wobei $a,\,b\in\mathbf{Z}$. Es wird

$$\begin{aligned} (12\mathbf{Z}+30\mathbf{Z})\cap 21\mathbf{Z} &= \mathrm{ggT}(12,30)\mathbf{Z}\cap 21\mathbf{Z} \\ &= 6\mathbf{Z}\cap 21\mathbf{Z} \\ &= \mathrm{kgV}(6,21)\mathbf{Z} \\ &= 42\mathbf{Z}\ . \end{aligned}$$

Also ist $x=42$.

(3) Wir verwenden Aufgabe 8. Zunächst wird mit Euklid

$$(X^4+1)\mathbf{F}_2[X]+(X^4+X^3+1)\mathbf{F}_2[X]\ =\ (X^2+1)\mathbf{F}_2[X]\ .$$

Dann gibt Euklid

$$(X^2+1)\mathbf{F}_2[X]+(X^3+1)\mathbf{F}_2[X]\ =\ (X+1)\mathbf{F}_2[X]$$

Insgesamt also

$$\begin{array}{rl} & \big((X^4+1)\mathbf{F}_2[X] + (X^4+X^3+X+1)\mathbf{F}_2[X]\big) + (X^3+1)\mathbf{F}_2[X] \\ = & (X^2+1)\mathbf{F}_2[X] + (X^3+1)\mathbf{F}_2[X] \\ = & (X+1)\mathbf{F}_2[X]\ . \end{array}$$

Also ist $f(X) = X + 1$.

Vgl. auch die Definition des ggT von Polynomen im Beispiel in §1.7.4.

Aufgabe 14

Wende die Bemerkung aus §1.6.2 (Gebrauchsanweisung für Polynomringe) an auf die Situation, in den dortigen Bezeichnungen, $n = 1$, $R = \mathbf{F}_2$, $S = \mathbf{F}_2[X]$, $a = c$ die Einbettung von $\mathbf{F}_2$ nach $\mathbf{F}_2[X]$, und $s_1 = u(X)$ für ein noch zu spezifizierendes Polynom $u(X) \in \mathbf{F}_2[X]$.

Dann wird $f(X) \in \mathbf{F}_2[X]$ abgebildet auf $f(u(X)) \in \mathbf{F}_2[X]$.

(Für $u(X) = X$ z.B. erhalten wir so die Identität auf $\mathbf{F}_2[X]$. Für $u(X) = X^2$ erhalten wir einen injektiven, aber nicht surjektiven Ringmorphismus – es liegt etwa das Polynom X nicht im Bild. Etc.)

Für $u(X) = X + 1$ erhalten wir einen Ringmorphismus φ von $\mathbf{F}_2[X]$ nach $\mathbf{F}_2[X]$, der nicht gleich der Identität ist. Es schickt φ das Polynom $f(X) \in \mathbf{F}_2[X]$ auf das Polynom $f(X+1) \in \mathbf{F}_2[X]$.

Wir *behaupten,* daß φ ein Isomorphismus ist, der $\varphi^2 = \mathrm{id}_{\mathbf{F}_2[X]}$ erfüllt. Dazu genügt es zu zeigen, daß letzteres gilt - eine Abbildung, die quadriert die Identität ist, ist insbesondere bijektiv.

Für $f(X) \in \mathbf{F}_2[X]$ wird in der Tat

$$\begin{array}{rcl} \varphi^2\big(f(X)\big) & = & \varphi\big(\varphi\big(f(X)\big)\big) \\ & = & \varphi\big(f(X+1)\big) \\ & = & f((X+1)+1) \\ & = & f(X)\ . \end{array}$$

Aufgabe 15

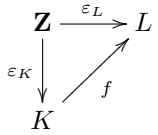
(1) Schreibe $R = \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}$. Es wird

$$\begin{array}{ccccc} \mathbf{Z} & \xrightarrow{\varepsilon_R} & \mathbf{Z}/8\mathbf{Z} & \times & \mathbf{Z}/12\mathbf{Z} \\ z & \longmapsto & (z+8\mathbf{Z} & \times & z+12\mathbf{Z})\ , \end{array}$$

da dies ein Ringmorphismus von $\mathbf{Z}$ nach R ist und es nur einen solchen gibt, namentlich ε_R; vgl. §1.7.3.

Der Kern von ε_R berechnet sich zu $8\mathbf{Z} \cap 12\mathbf{Z} = \mathrm{kgV}(8,12)\mathbf{Z} = 24\mathbf{Z}$; vgl. Aufgabe 13.(1). Also ist $\mathrm{char}(\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}) = 24$.

(2) Betrachte folgendes Dreieck von Ringmorphismen.



Dieses Dreieck kommutiert, i.e. $f \circ \varepsilon_K = \varepsilon_L$, da es nur einen Ringmorphismus von $\mathbf{Z}$ nach L gibt, namentlich ε_L; vgl. §1.7.3.

Um $\operatorname{char} K \stackrel{!}{=} \operatorname{char} L$ zu zeigen, haben wir zu zeigen, daß

$$(\operatorname{char} K)\mathbf{Z} \;=\; \operatorname{Kern}\varepsilon_K \stackrel{!}{=} \operatorname{Kern}\varepsilon_L \;=\; (\operatorname{char} L)\mathbf{Z}\,;$$

vgl. §1.7.3.

Beachte, daß f injektiv ist; vgl. Aufgabe 7. Also ist $f(x) = 0$ genau dann, wenn $x = 0$, wobei $x \in K$.

Also wird

$$\begin{array}{rcl} \operatorname{Kern}\varepsilon_L & = & \{z \in \mathbf{Z} \,:\, \varepsilon_L(z) = 0\} \\ & = & \{z \in \mathbf{Z} \,:\, f(\varepsilon_K(z)) = 0\} \\ & = & \{z \in \mathbf{Z} \,:\, \varepsilon_K(z) = 0\} \\ & = & \operatorname{Kern}\varepsilon_K\,. \end{array}$$

Aufgabe 16

(1) Sei etwa $n = ab$ mit $a, b \in [2, n-1]$. Dann sind $a \not\equiv_n 0$ und $b \not\equiv_n 0$, i.e. $a + n\mathbf{Z} \neq 0 + n\mathbf{Z}$ und $b + n\mathbf{Z} \neq 0 + n\mathbf{Z}$. Wohl aber ist

$$(a + n\mathbf{Z})(b + n\mathbf{Z}) \;=\; (ab + n\mathbf{Z}) \;=\; n + n\mathbf{Z} \;=\; 0 + n\mathbf{Z}\,.$$

Also ist $\mathbf{Z}/n\mathbf{Z}$ kein Integritätsbereich; vgl. §1.5.

(2) Euklid liefert

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

Also ist

$$(X^4+1)(X^6-X^5+X^4+X^3-X^2+X-1) \;\equiv_{X^7+1}\; 1\,,$$

mit anderen Worten,

$$\left(X^4+1+(X^7+1)\mathbf{F}_3[X]\right)^{-1} \;=\; X^6-X^5+X^4-X^3-X^2+X-1+(X^7+1)\mathbf{F}_3[X]\,.$$

Vgl. Aufgabe 8, Aufgabe 4.(1).

(3) Es ist $\dim_{\mathbf{F}_2} R = \deg(X^3+X^2+X+1) = 3$; vgl. Lemma aus §1.7.5. Also ist $|R| = 2^{\dim_{\mathbf{F}_2} R} = 2^3 = 8$.

Schreibe $\bar{X} := X + (X^3+X^2+X+1)\mathbf{F}_2[X]$.

Es ist z.B. $\bar{X}\cdot(\bar{X}^2+\bar{X}+1) = 1 + (\bar{X}^3+\bar{X}^2+\bar{X}+1) = 1$. Also ist $\bar{X}$ invertierbar. Ferner ist $\bar{X} \neq 1$, wie man etwa mit der in loc. cit. gegebenen Basis $(\bar{X}^0, \bar{X}^1, \bar{X}^2)$ erkennt, oder aber direkt dank $X \not\equiv_{X^4-1} 1$. Vgl. (4).

Da wir aber in $\mathbf{F}_2[X]$

$$X^3+X^2+X+1 \;=\; (X+1)(X^2+1) \;=\; (X+1)^3$$

haben, folgt nun, daß zwar $\bar{X}+1 \neq 0$ und $\bar{X}^2+1 \neq 0$ (wie man z.B. mit der eben genannten Basis erkennt), aber

$$(\bar{X}+1)(\bar{X}^2+1) \;=\; 0\,.$$

Also ist R kein Integritätsbereich.

(4) Schreibe $\bar{X} := X + f(X)K[X]$. Sei $n := \deg f$.

Es ist

$$0 \;=\; f(X) + f(X)K[X] \;=\; f(\bar{X}) \;=\; f_n\bar{X}^n + f_{n-1}\bar{X}^{n-1} + \cdots + f_1\bar{X} + f_0\,.$$

Also wird

$$1 \;=\; -f_0^{-1}(f_n\bar{X}^{n-1} + f_{n-1}\bar{X}^{n-2} + \cdots + f_1)\cdot\bar{X}.$$

Es folgt

$$(X + f(X)K[X])^{-1} \;=\; \bar{X}^{-1} \;=\; -f_0^{-1}(f_n\bar{X}^{n-1} + f_{n-1}\bar{X}^{n-2} + \cdots + f_1)\,.$$

Aufgabe 17

(1) Wir erhalten

$(+)$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

und

$(\cdot)$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

(2) Es wird

$$(\alpha^2+1)^3 \;=\; \alpha^3 \;=\; 1\;.$$

Es wird

$$(\beta^2+1)(\beta^6+1)+\beta^2 \;=\; (\beta^2+1)((\beta+1)^2+1)+\beta^2 \;=\; (\beta^2+1)\beta^2+\beta^2 \;=\; \beta^2+\beta+\beta^2+\beta^2 \;=\; \beta^2+\beta\;.$$

Es wird

$$(\iota+1)^4-\iota \;=\; ((\iota+1)^2)^2-\iota \;=\; (\iota^2+2\iota+1)^2-\iota \;=\; (-\iota)^2-\iota=-\iota-1\;.$$

(3) Es ist $X(X+1)+(X^2+X+1)\cdot 1=1$ in $\mathbf{F}_2[X]$, und somit $\alpha^{-1}=\alpha+1$. Man kann auch die Verknüpfungstafel aus (1) heranziehen.

Es ist $(X^2+X+1)X^2+(X^3+X+1)(X+1)=1$ in $\mathbf{F}_2[X]$, und somit $(\beta^2+\beta+1)^{-1}=\beta^2$.

Es ist $(X+1)(X-1)+(X^2+1)\cdot(-1)=1$ in $\mathbf{F}_3[X]$, und somit $(\iota+1)^{-1}=(\iota-1)$.

Man kann auch die Potenztabellen aus untenstehender Lösung zur Aufgabe 18 zur Inversion verwenden.

Aufgabe 18

(1) Es wird z.B.

$$\begin{aligned}\alpha^0 &= 1\\ \alpha^1 &= \alpha\\ \alpha^2 &= \alpha+1\;,\end{aligned}$$

und also $\langle\alpha\rangle=\mathbf{F}_4^\times$.

(2) Es wird z.B.

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

und also $\langle\beta\rangle=\mathbf{F}_8^\times$.

(3) Es wird z.B.

$$\begin{array}{rcl}(\iota+1)^0 & = & 1\\ (\iota+1)^1 & = & \iota+1\\ (\iota+1)^2 & = & -\iota\\ (\iota+1)^3 & = & -\iota+1\\ (\iota+1)^4 & = & -1\\ (\iota+1)^5 & = & -\iota-1\\ (\iota+1)^6 & = & \iota\\ (\iota+1)^7 & = & \iota-1\end{array}$$

und also $\langle \iota+1\rangle = \mathbf{F}_9^\times$.

Beachte, daß $\langle \iota\rangle \subsetneq \mathbf{F}_9^\times$.

Aufgabe 19

Bestimme alle normierten irreduziblen Polynome in $\mathbf{F}_q$ von Grad n.

(1) Da $n \leqslant 3$, suchen wir gerade die normierten Polynome in $\mathbf{F}_4[X]$ von Grad 2 ohne Nullstelle in $\mathbf{F}_4$. Wir listen alle normierten Polynome in $\mathbf{F}_4[X]$ von Grad 2 mit nichtverschwindendem konstanten Term auf, daneben ihre Nullstellen in $\mathbf{F}_4$.

Polynom	Nullstellenmenge
X^2+1	$\{1\}$
$X^2+\alpha$	$\{\alpha^2\}$
$X^2+\alpha^2$	$\{\alpha\}$
X^2+X+1	$\{\alpha,\, \alpha^2\}$
$X^2+X+\alpha$	$\emptyset$
$X^2+X+\alpha^2$	$\emptyset$
$X^2+\alpha X+1$	$\emptyset$
$X^2+\alpha X+\alpha$	$\emptyset$
$X^2+\alpha X+\alpha^2$	$\{1,\alpha^2\}$
$X^2+\alpha^2 X+1$	$\emptyset$
$X^2+\alpha^2 X+\alpha$	$\{1,\alpha\}$
$X^2+\alpha^2 X+\alpha^2$	$\emptyset$

Somit sind die normierten irreduziblen Polynome von Grad 2 in $\mathbf{F}_4[X]$ gegeben durch

$$X^2+X+\alpha,\ X^2+X+\alpha^2,\ X^2+\alpha X+1,\ X^2+\alpha X+\alpha,\ X^2+\alpha^2 X+1,\ X^2+\alpha^2 X+\alpha^2\ .$$

(2) Da $n \leqslant 3$, suchen wir gerade die normierten Polynome in $\mathbf{F}_3[X]$ von Grad 3 ohne Nullstelle in $\mathbf{F}_3$. Wir listen alle normierten Polynome in $\mathbf{F}_3[X]$ von Grad 3 mit nichtverschwindendem konstanten

Term auf, daneben ihre Nullstellen in $\mathbf{F}_3$.

Polynom	Nullstellenmenge
X^3+1	$\{-1\}$
X^3-1	$\{1\}$
X^3+X+1	$\{1\}$
X^3+X-1	$\{-1\}$
X^3-X+1	$\emptyset$
X^3-X-1	$\emptyset$
X^3+X^2+1	$\{1\}$
X^3+X^2-1	$\emptyset$
X^3+X^2+X+1	$\{-1\}$
X^3+X^2+X-1	$\emptyset$
X^3+X^2-X+1	$\emptyset$
X^3+X^2-X-1	$\{1,-1\}$
X^3-X^2+1	$\emptyset$
X^3-X^2-1	$\{-1\}$
X^3-X^2+X+1	$\emptyset$
X^3-X^2+X-1	$\{1\}$
X^3-X^2-X+1	$\{1,-1\}$
X^3-X^2-X-1	$\emptyset$

Somit sind die normierten irreduziblen Polynome von Grad 3 in $\mathbf{F}_3[X]$ gegeben durch

$$X^3-X+1,\ X^3-X-1,\ X^3+X^2-1,\ X^3+X^2+X-1,$$
$$X^3+X^2-X+1,\ X^3-X^2+1,\ X^3-X^2+X+1,\ X^3-X^2-X-1\ .$$

(3) Vorweg bemerken wir, daß X^2+X+1 das einzige (normierte) irreduzible Polynom von Grad 2 in $\mathbf{F}_2[X]$ ist.

Die (normierten) Polynome vierten Grades in $\mathbf{F}_2[X]$ ohne Nullstelle in $\mathbf{F}_2$ sind

$$X^4+X+1,\ X^4+X^2+1,\ X^4+X^3+1\ .$$

Wenn unter diesen eines nichttrivial in zwei Faktoren zerfllt, muß dieser Faktor von Grad 2 und irreduzibel sein – bei einem reduziblen Faktor von Grad 2 würde ja auch noch ein Faktor von Grad 1 abspalten, d.h. eine Nullstelle auftreten.

In der Tat ist $X^4+X^2+1=(X^2+X+1)^2$. Ferner sind weder X^4+X+1 noch X^4+X^3+1 durch X^2+X+1 teilbar (e.g. weil $\alpha^4+\alpha+1=1\neq 0$ und $\alpha^4+\alpha^3+1=\alpha\neq 0$). Also sind die irreduziblen Polynome von Grad 4 in $\mathbf{F}_2[X]$ gegeben durch

$$X^4+X+1,\ X^4+X^3+1\ .$$

Aufgabe 20

Es gibt keinen Isomorphismus $\mathbf{Z}/9\mathbf{Z}\xrightarrow{\sim}\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$, denn die Charakteristik von $\mathbf{Z}/9\mathbf{Z}$ ist 9, die Charakteristik von $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ aber 3.

Es gibt keinen Isomorphismus $\mathbf{Z}/9\mathbf{Z}\xrightarrow{\sim}\mathbf{F}_9$, denn die Charakteristik von $\mathbf{Z}/9\mathbf{Z}$ ist 9, die Charakteristik von $\mathbf{F}_9$ aber 3.

Es gibt keinen Isomorphismus $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}\xrightarrow{f}_{\sim}\mathbf{F}_9$, denn es wäre sonst $f((1,0))f((0,1))=f((0,0))=0$, aber $f((1,0))\neq 0$ und $f((0,1))\neq 0$, was wegen $\mathbf{F}_9$ Körper nicht geht. Kurz, da $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ kein Integritätsbereich ist, $\mathbf{F}_9$ als Körper aber schon, geht das nicht. (Alternativ kann man anführen, daß es in $\mathbf{F}_9$ ein invertierbares Element der Ordnung 8 gibt, in $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ aber nicht.)

Aufgabe 21

Wir behaupten, daß es in $\mathbf{F}_8$ keinen Teilring aus 4 Elementen gibt.

Angenommen, doch. Sei $R \subseteq \mathbf{F}_8$ ein Teilring mit $|R| = 4$. Da R ein endlicher Integritätsbereich ist, ist R ein Teilkörper von $\mathbf{F}_8$. Es ist $R^\times := R \setminus \{0\}$ eine Gruppe aus 3 Elementen. Nach Aufgabe 11.(1.c) teilt die Ordnung jedes Elements in $R^\times$ die 3. Nun haben nach loc. cit. aber alle Elemente von $\mathbf{F}_8^\times$ eine Ordnung, die 7 teilt, insbesondere auch die von $R^\times$. Da aber $\mathrm{ggT}(3,7) = 1$, müssen alle Elementordnungen von $R^\times$ die 1 teilen, i.e. gleich 1 sein. Nun hat aber nur die Eins einer Gruppe die Ordnung 1. Also $R^\times = \{1\}$. Aber $|R^\times| = 3$. Dies ist ein *Widerspruch.*

Aufgabe 22

Sei $R \xrightarrow{f} S$ ein Morphismus kommutativer Ringe. Sei $I \subseteq S$ ein Ideal.

(1) Da $f(0) = 0 \in J$, ist $0 \in f^{-1}(J)$.

Sind $x,\, y \in f^{-1}(J)$, so ist $f(x-y) = f(x) - f(y) \in J$, also $x - y \in f^{-1}(J)$.

Ist $x \in f^{-1}(J)$ und ist $r \in R$, so ist $f(rx) = f(r)f(x) \in J$, und also $rx \in f^{-1}(J)$.

Also ist $f^{-1}(J) \subseteq R$ ein Ideal.

Ist $r \in \operatorname{Kern} f$, so ist $f(r) = 0 \in J$, und also $r \in f^{-1}(J)$. Also ist $\operatorname{Kern} f \subseteq J$. (Alternativ, da $\{0\} \subseteq J$, ist auch $f^{-1}(\{0\}) \subseteq f^{-1}(J)$.)

(2) Wir haben zu zeigen, daß R/I genau 2 Ideale enthält. Wir wenden (1) an auf $R \xrightarrow{\rho} R/I$. Sei $J \subseteq R/I$ ein Ideal. Dann ist

$$I \;=\; \operatorname{Kern}\rho \;\subseteq\; \rho^{-1}(J) \;\subseteq\; R\,.$$

Da $I \subseteq R$ ein maximales Ideal ist, folgt $\rho^{-1}(J) = I$ oder $\rho^{-1}(J) = R$.

Ersterenfalls ist, wegen ρ surjektiv, $J = \rho(\rho^{-1}(J)) = \rho(I) = \{0_{R/I}\}$.

Zweiterenfalls ist, wegen ρ surjektiv, $J = \rho(\rho^{-1}(J)) = \rho(R) = R/I$.

Die Menge der Ideale von R/I ist somit gleich $\{\{0_{R/I}\},\ R/I\}$. Es bleibt uns anzumerken, daß $R/I \neq \{0_{R/I}\}$, da $I \subsetneq R$, daß also in der Tat auch zwei verschiedene Ideale aufgelistet sind.

Aufgabe 23

Addition und Multiplikation sind ersichtlich kommutativ. Die Multiplikation ist ersichtlich assoziativ. Das Element $\frac{1}{1}$ ist ersichtlich neutral bezüglich der Multiplikation.

Die nun noch fehlenden Eigenschaften wollen wir nachweisen. Seien $\frac{r}{s},\ \frac{r'}{s'},\ \frac{r''}{s''} \in \operatorname{frac} R$.

Es wird $\frac{r}{s} + \frac{0}{1} = \frac{r\cdot 1 + s\cdot 0}{s\cdot 1} = \frac{r}{s}$.

Es wird $\frac{r}{s} + \frac{(-r)}{s} = \frac{rs+(-r)s}{s^2} = \frac{0}{s^2} = \frac{0}{1}$.

Es wird

$$\begin{aligned}
(\tfrac{r}{s} + \tfrac{r'}{s'}) + \tfrac{r''}{s''} &= \tfrac{rs'+r's}{ss'} + \tfrac{r''}{s''} \\
&= \tfrac{(rs'+r's)s''+r''ss'}{ss's''} \\
&= \tfrac{rs's''+r'ss''+r''ss'}{ss's''} \\
&= \tfrac{rs's''+s(r's''+r''s')}{ss's''} \\
&= \tfrac{r}{s} + \tfrac{r's''+r''s'}{s's''} \\
&= \tfrac{r}{s} + (\tfrac{r'}{s'} + \tfrac{r''}{s''})\,.
\end{aligned}$$

Es wird

$$\begin{aligned}(\tfrac{r}{s}+\tfrac{r'}{s'})\tfrac{r''}{s''} &= \tfrac{rs'+r's}{ss'}\tfrac{r''}{s''}\\ &= \tfrac{(rs'+r's)r''}{ss's''}\\ &= \tfrac{(rs'+r's)r''s''}{ss's''^2}\\ &= \tfrac{rr''s's''+r'r''ss''}{ss''s's''}\\ &= \tfrac{rr''}{ss''}+\tfrac{r'r''}{s's''}\ .\end{aligned}$$

Es ist $\frac{r}{s}=\frac{0}{1}$ genau dann, wenn $r\cdot 1 = s\cdot 0$; i.e. genau dann, wenn $r=0$. Sei also $r\neq 0$. Es wird $\frac{r}{s}\frac{s}{r}=\frac{rs}{sr}=\frac{1}{1}$.

Aufgabe 24

(1) Es ist $\mathrm{Frob}_K(1)=1^p=1$. Es ist $\mathrm{Frob}_K(xy)=(xy)^p=x^py^p$ für $x,\,y\in K$. Für die Verträglichkeit mit der Addition merken wir an, daß der Binomialkoeffizient $\binom{p}{i}=\frac{p!}{i!(p-i)!}$ für $i\in[1,p-1]$ im Zähler einen Faktor p enthält, nicht aber im Nenner. Also ist diesenfalls $\binom{p}{i}$ ein Vielfaches von p. Es folgt

$$\mathrm{Frob}_K(x+y)\ =\ (x+y)^p\ =\ x^p+\tbinom{p}{1}x^{p-1}y^1+\cdots+\tbinom{p}{p-1}x^1y^{p-1}+y^p\ =\ x^p+y^p\ =\ \mathrm{Frob}_K(x)+\mathrm{Frob}_K(y)\ ,$$

da in K gilt, daß $p=0$.

Als Morphismus von Körpern ist Frob_K injektiv; vgl. Aufgabe 7.(1).

Ist K ein endlicher Körper, so ist Frob_K als injektive Selbstabbildung einer endlichen Menge auch bijektiv, und mithin ein Automorphismus.

Allgemein ist das aber nicht der Fall. So z.B. ist $\mathrm{Frob}_{\mathbf{F}_p(X)}$ nicht surjektiv, da $X\in\mathbf{F}_p(X)$ nicht in $\mathrm{Frob}_K(\mathbf{F}_p(X))$ liegt. Denn *wäre* $X=\left(\frac{f(X)}{g(X)}\right)^p$ für gewisse $f(X)\in\mathbf{F}_p[X]$ und $g(X)\in\mathbf{F}_p[X]\smallsetminus\{0\}$, dann wäre $Xg(X)^p=f(X)^p$, und also

$$1\ \equiv_p\ 1+p\deg g\ =\ \deg(Xg(X)^p)\ =\ \deg(f(X)^p)\ =\ p\deg f\ \equiv_p\ 0\ ,$$

Widerspruch.

(2) Es ist $\mathrm{Frob}_{\mathbf{F}_p}$ ein Automorphismus von $\mathbf{F}_p$.

Nach der ersten Bemerkung in §2.1 operiert aber jeder Automorphismus eines Körpers K von Charakteristik p identisch auf dem Primkörper, d.h. auf den Elementen im Bild von ε_K.

Im Falle $K=\mathbf{F}_p$ ist nun $\varepsilon_{\mathbf{F}_p}$ surjektiv, i.e. es ist $\mathbf{F}_p$ sein eigener Primkörper. Es folgt $\mathrm{Frob}_{\mathbf{F}_p}=\mathrm{id}_{\mathbf{F}_p}$. Elementweise geschrieben heißt dies, daß $x^p=\mathrm{Frob}_{\mathbf{F}_p}(x)=x$ für alle $x\in\mathbf{F}_p$. In anderen Worten, es ist $z^p\equiv_p z$ für alle $z\in\mathbf{Z}$, und dies ist die Aussage des Kleinen Fermatschen Satzes.

(3) Z.B. ist $X^3-X+1\in\mathbf{F}_3[X]$ mangels Nullstelle irreduzibel. Sei

$$\mathbf{F}_{27}\ :=\ \mathbf{F}_3[X]/(X^3-X+1)\mathbf{F}_3[X]\ .$$

Schreibe $\gamma:=X+(X^3-X+1)\mathbf{F}_3[X]$. Dann ist $\gamma^3=\gamma-1$ und $3=0$ in $\mathbf{F}_{27}$. Eine Basis von $\mathbf{F}_{27}$ über $\mathbf{F}_3$ ist gegeben durch $(\gamma^0,\gamma^1,\gamma^2)$, und insbesondere ist $|\mathbf{F}_{27}|=3^3=27$ wie gewünscht.

Sei $x=\lambda_2\gamma^2+\lambda_1\gamma^1+\lambda_0\gamma^0\in\mathbf{F}_{27}$, wobei $\lambda_i\in\mathbf{F}_3$ für $i\in[0,2]$. Es wird

$$\begin{aligned}\mathrm{Frob}_{\mathbf{F}_{27}}(x)-x &= (\lambda_2\gamma^2+\lambda_1\gamma^1+\lambda_0\gamma^0)^3-(\lambda_2\gamma^2+\lambda_1\gamma^1+\lambda_0\gamma^0)\\ &= (\lambda_2^3\gamma^6+\lambda_1^3\gamma^3+\lambda_0^3\gamma^0)-(\lambda_2\gamma^2+\lambda_1\gamma^1+\lambda_0\gamma^0)\\ &= (\lambda_2\gamma^6+\lambda_1\gamma^3+\lambda_0\gamma^0)-(\lambda_2\gamma^2+\lambda_1\gamma^1+\lambda_0\gamma^0)\\ &= \lambda_2\gamma^6+\lambda_1\gamma^3-\lambda_2\gamma^2-\lambda_1\gamma^1\\ &= \lambda_2(\gamma-1)^2+\lambda_1(\gamma-1)-\lambda_2\gamma^2-\lambda_1\gamma^1\\ &= \lambda_2\gamma^1+(\lambda_1+\lambda_2)\gamma^0\ .\end{aligned}$$

Dies ist wegen der linearen Unabhängigkeit von $(\gamma^0, \gamma^1, \gamma^2)$ über $\mathbf{F}_3$ genau dann gleich 0, wenn $\lambda_2 = 0$ und $\lambda_1 = 0$. Also ist

$$\{x \in \mathbf{F}_{27} \ : \ \mathrm{Frob}_{\mathbf{F}_{27}}(x) = x\} \ = \ \{\lambda_2\gamma^2 + \lambda_1\gamma^1 + \lambda_0\gamma^0 \ : \ \lambda_i \in \mathbf{F}_3, \ \lambda_1 = \lambda_2 = 0\} \ = \ \mathbf{F}_3 \ .$$

Alternativ kann man hierfür anführen, daß $\mathrm{Frob}_{\mathbf{F}_{27}}(x) = x$ gilt für alle Elemente des Primkörpers $\mathbf{F}_3$, daß das Polynom $X^3 - X$ höchstens 3 Nullstellen in $\mathbf{F}_{27}$ haben kann und daß somit genau diese drei Elemente von $\mathbf{F}_3$ Nullstellen davon sind.

(4) Z.B. ist $X^4 + X + 1 \in \mathbf{F}_2[X]$ irreduzibel; vgl. Aufgabe 19.(3). Sei

$$\mathbf{F}_{16} \ := \ \mathbf{F}_2[X]/(X^4 + X + 1)\mathbf{F}_2[X] \ .$$

Schreibe $\delta := X + (X^4 + X + 1)\mathbf{F}_2[X]$. Dann ist $\delta^4 = \delta + 1$ und $2 = 0$ in $\mathbf{F}_{16}$. Eine Basis von $\mathbf{F}_{16}$ über $\mathbf{F}_2$ ist gegeben durch $(\delta^0, \delta^1, \delta^2, \delta^3)$, und insbesondere ist $|\mathbf{F}_{16}| = 2^4 = 16$ wie gewünscht.
Sei $x = \lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0 \in \mathbf{F}_{16}$, wobei $\lambda_i \in \mathbf{F}_2$ für $i \in [0, 3]$. Es wird

$$\begin{array}{rcl} \mathrm{Frob}^2_{\mathbf{F}_{16}}(x) - x & = & (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0)^4 - (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0) \\ & = & (\lambda_3\delta^{12} + \lambda_2\delta^8 + \lambda_1\delta^4 + \lambda_0\delta^0) + (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1 + \lambda_0\delta^0) \\ & = & (\lambda_3(\delta+1)^3 + \lambda_2(\delta+1)^2 + \lambda_1(\delta+1)) + (\lambda_3\delta^3 + \lambda_2\delta^2 + \lambda_1\delta^1) \\ & = & \lambda_3(\delta^2 + \delta + 1) + \lambda_2 + \lambda_1 \ . \end{array}$$

Wegen der linearen Unabhängigkeit von $(\delta^0, \delta^1, \delta^2, \delta^3)$ über $\mathbf{F}_2$ ist dies genau dann gleich 0, wenn $\lambda_3 = 0$ und $\lambda_1 = \lambda_2$. Also ist

$$K := \{x \in \mathbf{F}_{16} \ : \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x) = x\} \ = \ \{\lambda_1(\delta^2 + \delta) + \lambda_0 \ : \ \lambda_0, \ \lambda_1 \ \in \mathbf{F}_2\} \ .$$

Es ist K ein Teilkörper, da $\mathrm{Frob}^2_{\mathbf{F}_{16}}(1) = 1$, und da aus $x, y \in \mathbf{F}_{16}$ mit $\mathrm{Frob}^2_{\mathbf{F}_{16}}(x) = x$ und $\mathrm{Frob}^2_{\mathbf{F}_{16}}(y) = y$ folgt, daß

$$\mathrm{Frob}^2_{\mathbf{F}_{16}}(x - y) \ = \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x) - \mathrm{Frob}^2_{\mathbf{F}_{16}}(y) \ = \ x - y \ ,$$

daß

$$\mathrm{Frob}^2_{\mathbf{F}_{16}}(xy) \ = \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x)\,\mathrm{Frob}^2_{\mathbf{F}_{16}}(y) \ = \ xy$$

und daß, falls $x \neq 0$,

$$\mathrm{Frob}^2_{\mathbf{F}_{16}}(x^{-1}) \ = \ \mathrm{Frob}^2_{\mathbf{F}_{16}}(x)^{-1} \ = \ x^{-1} \ .$$

Also ist K ein Teilring abgeschlossen unter Inversion von nichtverschwindenden Elementen, und somit ein Teilkörper. (Festgestellt zu haben, daß ein Teilring eines endlichen Körpers vorliegt, hätte auch gereicht, da ein endlicher Integritätsbereich notwendig ein Körper ist.)
Nun ist

$$(\delta^2 + \delta)^2 + (\delta^2 + \delta) + 1 \ = \ \delta^4 + \delta^2 + \delta^2 + \delta + 1 \ = \ 0 \ .$$

Also faktorisiert der Ringmorphismus

$$\begin{array}{rcl} \mathbf{F}_2[X] & \longrightarrow & \mathbf{F}_{16} \\ X & \longmapsto & \delta^2 + \delta \end{array}$$

über den Ringmorphismus

$$\begin{array}{rcl} \mathbf{F}_2[X]/(X^2 + X + 1)\mathbf{F}_2[X] & \longrightarrow & \mathbf{F}_{16} \\ X + (X^2 + X + 1)\mathbf{F}_2[X] & \longmapsto & \delta^2 + \delta \ . \end{array}$$

In der Tat schickt ersterer das Polynom $X^2 + X + 1$ auf $(\delta^2 + \delta)^2 + (\delta^2 + \delta) + 1 = 0_{\mathbf{F}_{16}}$, und also das Ideal $(X^2 + X + 1)\mathbf{F}_2[X]$ auf $\{0_{\mathbf{F}_{16}}\}$.

In Standardnotation umgeschrieben liest sich letzterer nun

$$\begin{array}{ccc} \mathbf{F}_4 & \longrightarrow & \mathbf{F}_{16} \\ \alpha & \longmapsto & \delta^2+\delta\ . \end{array}$$

Als Körpermorphismus ist dieser nun injektiv; vgl. Aufgabe 7. Da $\mathbf{F}_4 = \langle 1, \alpha\rangle_{\mathbf{F}_2}$ (Vektorraumerzeugnis über $\mathbf{F}_2$), und da dieser Morphismus $\mathbf{F}_2$-linear ist, ist das Bild gegeben durch $\langle 1, \delta^2+\delta\rangle_{\mathbf{F}_2}$. Dies ist aber gerade gleich K. Somit liefert unser injektiver Körpermorphismus durch Einschränkung des Bildbereichs einen Körperisomorphismus

$$\begin{array}{ccc} \mathbf{F}_4 & \longrightarrow & K \\ \alpha & \longmapsto & \delta^2+\delta\ . \end{array}$$

Man hätte zur Konstruktion von $\mathbf{F}_{16}$ alternativ auch ein irreduzibles Polynom von Grad 2 in $\mathbf{F}_4[X]$ verwenden können; vgl. Aufgabe 19.(3).

Aufgabe 25

(1) Es ist $f'(X) = X^{s-1}(X-1)^{t-1}(tX+s(X-1))$. Um also zu zeigen, daß $\mathrm{ggT}(f(X), f'(X)) = X^{s-1}(X-1)^{t-1}$, genügt es, zu zeigen, daß $X(X-1)$ und $tX+s(X-1)$ teilerfremd sind. Und in der Tat, X teilt letzteres Polynom nicht, da X wegen $s \neq 0$ den Summanden $s(X-1)$ nicht teilt. Genauso teilt $(X-1)$ letzteres Polynom nicht, da es wegen $t \neq 0$ den Summanden tX nicht teilt.

So zu argumentieren können wir uns leisten, da wir in $K[X]$ die eindeutige Zerlegung in irreduzible Polynome kennen; vgl. §1.9.

(2) Nach Voraussetzung können wir $f(X) = \prod_{i\in[1,r]}(X-\gamma_i)^{s_i}$ für gewisse $r \geqslant 0$, $\gamma_i \in K$ und $s_i \geqslant 1$ schreiben, wobei $\gamma_i \neq \gamma_j$ falls $i \neq j$.

Beachte, daß

$$f'(X) \;=\; \sum_{k\in[1,r]} s_i(X-\gamma_i)^{s_i-1} \prod_{i\in[1,r]\smallsetminus\{k\}} (X-\gamma_i)^{s_i}\ .$$

Ist $s_i = 1$ für alle $i \in [1,r]$, so wird $f'(\gamma_j) = \prod_{i\in[1,r]\smallsetminus\{j\}}(\gamma_j-\gamma_i) \neq 0$ und somit $f'(X)$ kein Vielfaches von $(X-\gamma_j)$ für alle $j \in [1,r]$. Folglich ist $\mathrm{ggT}(f(X), f'(X)) = 1$.

Ist umgekehrt $s_j \geqslant 2$ für ein $j \in [1,r]$, so wird $f'(\gamma_j) = s_j(\gamma_i-\gamma_i)^{s_j-1}\prod_{i\in[1,r]\smallsetminus\{j\}}(\gamma_j-\gamma_i) = 0$. Also ist $(X-\gamma_j)$ ein Teiler von $f'(X)$, und also insgesamt ein Teiler von $\mathrm{ggT}(f(X), f'(X))$. Folglich ist $\mathrm{ggT}(f(X), f'(X)) \neq 1$.

(3) Sei $g_K(X)$ der in $K[X]$ genommene ggT von $f(X)$ und $h(X)$.

Sei $g_L(X)$ der in $L[X]$ genommene ggT von $f(X)$ und $h(X)$.

Mit dem Euklidschen Algorithmus gibt es $s_K(X), t_K(X) \in K[X]$ mit

$$(*) \qquad f(X)s_K(X) + h(X)t_K(X) \;=\; g_K(X)$$

und $s_L(X), t_L(X) \in L[X]$ mit

$$(**) \qquad f(X)s_L(X) + h(X)t_L(X) \;=\; g_L(X)\ ;$$

vgl. Aufgabe 8.

Da $g_L(X)$ ein Teiler von $f(X)$ und von $h(X)$ in $L[X]$ ist, zeigt $(*)$, daß $g_L(X)$ auch ein Teiler von $g_K(X)$ in $L[X]$ ist.

Da $g_K(X)$ ein Teiler von $f(X)$ und von $h(X)$ in $K[X]$ ist, zeigt $(**)$, daß $g_K(X)$ auch ein Teiler von $g_L(X)$ in $L[X]$ ist.

Insgesamt folgt $g_K(X) = g_L(X)$.

Aufgabe 26

(1) Es ist $\operatorname{char} L > 0$, da $\operatorname{char} L = 0$ zur Folge hätte, daß $\mathbf{Z} \xrightarrow{\varepsilon_L} L$ den Kern $(\operatorname{char} L)\mathbf{Z} = \{0\}$ hätte, und somit injektiv wäre, was wegen L endlich nicht geht.

Schreibe also $\operatorname{char} L =: p > 0$. Wir haben den Primkörper $\mathbf{F}_p \subseteq L$; vgl. §2.1.

Es ist L ein $\mathbf{F}_p$-Vektorraum; vgl. die erste Bemerkung in §1.7.5. Da L endlich ist, ist L ein endlichdimensionaler $\mathbf{F}_p$-Vektorraum. Sei $\ell := \dim_{\mathbf{F}_p} L = [L : \mathbf{F}_p]$. Es folgt $|L| = p^\ell$.

(2) Erste Lösung. Es ist $\ell = [L : \mathbf{F}_p] = [L : K][K : \mathbf{F}_p]$. Folglich ist $[K : \mathbf{F}_p] =: k$ ein Teiler von ℓ. Ferner ist $|K| = p^k$.

Zweite Lösung, alternativ. Es ist L ein endlichdimensionaler K-Vektorraum. Schreibe $m := [L : K]$. Mit (1) gibt es ein $k \geqslant 1$ mit $K = p^k$; beachte $\operatorname{char} K = \operatorname{char} L = p$. Also ist $(p^k)^m = p^\ell$. Mithin ist $km = \ell$.

(3) Nach (2) haben alle Teilkörper von $\mathbf{F}_{27}$ eine Kardinalität 3^k mit k einem Teiler von 3. Es folgt, daß diese Kardinalität $3^1 = 3$ oder $3^3 = 27$ haben. Also sind der Primkörper $\mathbf{F}_3$ und der gesamte Körper $\mathbf{F}_{27}$ die einzigen Teilkörper von $\mathbf{F}_{27}$.

Vgl. auch Aufgabe 21.

Aufgabe 27

(1) Zur *ersten* Behauptung.

Ist $\mathrm{o}(a)$ ein Teiler von k, ist also $k = \mathrm{o}(a)\ell$ für ein $\ell \in \mathbf{Z}$, dann ist $a^k = a^{\mathrm{o}(a)\ell} = (a^{\mathrm{o}(a)})^\ell = 1^\ell = 1$.

Sei umgekehrt $a^k = 1$. Schreibe $k = \mathrm{o}(a)\ell + r$ mit $\ell \in \mathbf{Z}$ und $r \in [0, \mathrm{o}(a) - 1]$. Dann ist

$$1 \;=\; a^k \;=\; a^{\mathrm{o}(a)\ell + r} \;=\; (a^{\mathrm{o}(a)})^\ell \cdot a^r \;=\; a^r \;.$$

Wäre $r \geqslant 1$, so wäre dies im Widerspruch zur Minimalität von $\mathrm{o}(a)$. Also ist $r = 0$, i.e. $\mathrm{o}(a)$ ein Teiler von k.

Zur *zweiten* Behauptung.

Zum einen ist $(ab)^{\mathrm{o}(a)\mathrm{o}(b)} = (a^{\mathrm{o}(a)})^{\mathrm{o}(b)}(b^{\mathrm{o}(b)})^{\mathrm{o}(a)} = 1^{\mathrm{o}(b)}1^{\mathrm{o}(a)} = 1$.

Sei zum anderen $(ab)^k = 1$ für ein $k \in \mathbf{Z}_{\geqslant 1}$.

Dann ist $a^k = b^{-k}$. Es ist $a^k \in \langle a \rangle$, und $\langle a \rangle$ ist eine Gruppe mit $|\langle a \rangle| = \mathrm{o}(a)$ nach Aufgabe 11.(1.b). Nach Aufgabe 11.(1.c), angewandt auf diese Gruppe $\langle a \rangle$, ist $\mathrm{o}(a^k)$ ein Teiler von $\mathrm{o}(a)$.

(Hierfür kann alternativ auch folgendes vorgebracht werden. Es ist $(a^k)^{\mathrm{o}(a)} = a^{k\mathrm{o}(a)} = (a^{\mathrm{o}(a)})^k = 1^k = 1$. Mit der ersten Behauptung folgt, daß $\mathrm{o}(a^k)$ ein Teiler von $\mathrm{o}(a)$ ist.)

Analog ist $\mathrm{o}(b^{-k})$ ein Teiler von $\mathrm{o}(b)$.

Somit ist $\mathrm{o}(a^k) = \mathrm{o}(b^{-k})$ ein gemeinsamer Teiler von $\mathrm{o}(a)$ und von $\mathrm{o}(b)$, und also gleich 1, da $\mathrm{ggT}(\mathrm{o}(a), \mathrm{o}(b)) = 1$. Dies aber hat $a^k = b^{-k} = 1$ zur Folge.

Dank der ersten Behauptung folgt, daß $\mathrm{o}(a)$ und $\mathrm{o}(b)$ beide Teiler von k sind. Wegen $\mathrm{ggT}(\mathrm{o}(a), \mathrm{o}(b)) = 1$ folgt, daß $\mathrm{o}(a)\mathrm{o}(b)$ ein Teiler von k ist, insbesondere, daß $\mathrm{o}(a)\mathrm{o}(b) \leqslant k$ ist.

Somit ist $\mathrm{o}(a)\mathrm{o}(b)$ der minimale positive Exponent, dessen Potenz von ab gleich 1 ist. In anderen Worten, es ist in der Tat $\mathrm{o}(ab) = \mathrm{o}(a)\mathrm{o}(b)$.

(2) Schreibe $g := \mathrm{ggT}(\mathrm{o}(a), d)$.

Da g ein Teiler von d ist, folgt zum einen $(a^d)^{\frac{\mathrm{o}(a)}{g}} = a^{\frac{\mathrm{o}(a)d}{g}} = (a^{\mathrm{o}(a)})^{\frac{d}{g}} = 1$.

Sei zum anderen $k \in \mathbf{Z}_{\geqslant 1}$ mit $(a^d)^k = 1$ gegeben. Dank (1) ist $\mathrm{o}(a)$ ein Teiler von dk und somit $\frac{\mathrm{o}(a)}{g}$ ein Teiler von $\frac{d}{g} \cdot k$. Da $\frac{\mathrm{o}(a)}{g}$ und $\frac{d}{g}$ aber teilerfremd sind, folgt, daß $\frac{\mathrm{o}(a)}{g}$ bereits ein Teiler von k ist. Insbesondere gilt $\frac{\mathrm{o}(a)}{g} \leqslant k$.

Somit ist $\frac{\mathrm{o}(a)}{g}$ der minimale positive Exponent, dessen Potenz von a^d gleich 1 ist. In anderen Worten, es ist in der Tat $\mathrm{o}(a^d) = \frac{\mathrm{o}(a)}{g}$.

(3) Schreibe $\mathrm{o}(a) = p_1^{s_1} \cdots p_k^{s_k}$ und $\mathrm{o}(b) = p_1^{t_1} \cdots p_k^{t_k}$ mit $k \geqslant 0$, $p_i > 0$ prim und $s_i, t_i \in \mathbf{Z}_{\geqslant 0}$ für $i \in [1,k]$, wobei $p_i \neq p_j$ für $i, j \in [1,k]$ mit $i \neq j$.

Sei $i \in [1,k]$ gegeben. Mit (2) gibt es ein Element von Ordnung $p_i^{s_i}$ in G, nämlich eine geeignete Potenz von a. Mit (2) gibt es auch ein Element von Ordnung $p_i^{t_i}$ in G, nämlich eine geeignete Potenz von b. Somit gibt es auch ein Element $x_i \in G$ von Ordnung $p_i^{\max\{s_i,t_i\}}$ in G.

Mit (1) folgt aus der Teilerfremdheit der Primpotenzen, daß

$$\mathrm{o}(x_1 \cdots x_k) \;=\; \mathrm{o}(x_1) \cdots \mathrm{o}(x_k) \;=\; p_1^{\max\{s_1,t_1\}} \cdots p_k^{\max\{s_k,t_k\}} \;=\; \mathrm{kgV}(\mathrm{o}(a), \mathrm{o}(b)) \,.$$

(4) *Wäre* $\mathrm{o}(g)$ kein Teiler von $\mathrm{o}(x)$ ist für ein $g \in G$, so wäre $\mathrm{o}(x) < \mathrm{kgV}(\mathrm{o}(x), \mathrm{o}(g))$. Sei $\tilde{g}$ ein mit (3) existentes Element von G von Ordnung $\mathrm{kgV}(\mathrm{o}(x), \mathrm{o}(g))$. Dann ist $\mathrm{o}(x) < \mathrm{o}(\tilde{g})$. Wir haben einen *Widerspruch* zur Maximalität von $\mathrm{o}(x)$.

(5) Sei $x \in G$ von maximaler Ordnung.

Zunächst ist $\mathrm{o}(x)$ ein Teiler von $|G|$; vgl. Aufgabe 11.(1.c).

Mit (4) folgt andererseits, daß für alle $g \in G$ gilt, daß $\mathrm{o}(g)$ ein Teiler von $\mathrm{o}(x)$ ist, und insbesondere, daß $g^{\mathrm{o}(x)} = 1$ ist. Folglich sind alle Elemente von G Nullstellen von $X^{\mathrm{o}(x)} - 1$. Ein Polynom mit $|G|$ Nullstellen hat aber Grad $\geqslant |G|$, da zu diesen Nullstellen gehörige Linearfaktoren abdividiert werden können; cf. §1.6.4. Also ist $\mathrm{o}(x) \geqslant |G|$.

Insgesamt folgt $\mathrm{o}(x) = |G|$.

(6) Wir verwenden die Schreibweise der Lösung von Aufgabe 24.(4). Sei also $\delta \in \mathbf{F}_4$ mit $\delta^4 + \delta + 1 = 0$. Wir erhalten folgende Potenzen, ausgedrückt in der Standardbasis $(1, \delta, \delta^2, \delta^3)$ über $\mathbf{F}_2$.

$$\begin{array}{lcll}
\delta^0 & = & 1 & \\
\delta^1 & = & \delta & \\
\delta^2 & = & \delta^2 & \\
\delta^3 & = & \delta^3 & \\
\delta^4 & = & \delta + 1 & \\
\delta^5 & = & \delta^2 + \delta & \\
\delta^6 & = & \delta^3 + \delta^2 & \\
\delta^7 & = & \delta^3 + \delta + 1 & \\
\delta^8 & = & \delta^2 + 1 & \\
\delta^9 & = & \delta^3 + \delta & \\
\delta^{10} & = & \delta^2 + \delta + 1 & \\
\delta^{11} & = & \delta^3 + \delta^2 + \delta & \\
\delta^{12} & = & \delta^3 + \delta^2 + \delta + 1 & \\
\delta^{13} & = & \delta^3 + \delta^2 + 1 & \\
\delta^{14} & = & \delta^3 + 1 & \\
\delta^{15} & = & 1 & \text{(zur Probe)}
\end{array}$$

Vgl. auch Aufgabe 11.(2, 3) und Aufgabe 18.

(7) Es ist $G = \{1, \mathrm{i}, -1, -\mathrm{i}\} \subseteq \mathbf{C}^\times$ eine Gruppe mit $|G| = 4$, deren Multiplikation von der Multiplikation in $\mathbf{C}$ stammt.

Aufgabe 28

Schreibe $n := [L : K]$. Das Tupel $(x^0, x^1, \ldots, x^n)$ hat Länge $n+1$, ist also linear abhängig. Somit gibt es $\lambda_i \in K$ für $i \in [0,n]$ so, daß

$$\lambda_0 x^0 + \cdots + \lambda_n x^n \;=\; 0 \,,$$

aber so, daß $\lambda_j \neq 0$ für wenigstens ein $j \in [0,n]$. Setzen wir $f(X) = \sum_{i \in [0,n]} \lambda_i X^i \in K[X]$, so haben wir also ein Polynom ungleich 0 gefunden, welches $f(x) = 0$ erfüllt. Folglich ist x algebraisch über K.

Aufgabe 29

(1) Es ist $X^4 + X + 1$ irreduzibel in $\mathbf{Q}[X]$.
Magma:

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + X + 1);
```

(2) Es ist

$$X^5 + X + 1 \;=\; (X^2 + X + 1)(X^3 - X^2 + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{Q}[X]$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^5 + X + 1);
```

(3) Schreibe $\gamma := \mathrm{i}\sqrt{3}$. Es ist

$$X^5 + X + 1 \;=\; (X + \frac{1-\gamma}{2})(X + \frac{1+\gamma}{2})(X^3 - X^2 + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{Q}(\gamma)[X]$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
KK<ga> := ext<Q | X^2 + 3>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^5 + XX + 1);
```

(4) Es ist

$$X^8 - X \;=\; X(X+1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{F}_2[X]$.

```
F := GF(2);
R<X> := PolynomialRing(F);
Factorisation(X^8 - X);
```

(5) Es ist

$$X^8 - X \;=\; X(X+1)(X+\beta)(X+\beta^2)(X+\beta^3)(X+\beta^4)(X+\beta^5)(X+\beta^6)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{F}_8[X]$ (was man auch ohne Magma erkennt, da jedes Element von $\mathbf{F}_8$ eine Nullstelle von $X^8 - X$ ist).

```
F := GF(2);
R<X> := PolynomialRing(F);
FF<b> := ext<F | X^3 + X + 1>;
RR<XX> := PolynomialRing(FF);
Factorisation(XX^8 - XX);
```

(6) Es ist

$$X^{15} - X + 1 = \\ (X + \iota + 1)(X - \iota + 1)(X^2 + X + \iota - 1)(X^2 + X - \iota - 1)(X^9 - X^8 - X^7 - X^4 - X^3 + X^2 - X + 1)$$

die Zerlegung in irreduzible Faktoren in $\mathbf{F}_9[X]$.

```
F := GF(3);
R<X> := PolynomialRing(F);
FF<i> := ext<F | X^2 + 1>;
RR<XX> := PolynomialRing(FF);
Factorisation(XX^15 - XX + 1);
```

Aufgabe 30

(1) Es ist $X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1)$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}[X]$. Sei $\mathbf{Q}(a)|\mathbf{Q}$ mit $a^2 + a + 1 = 0$.
Es ist $X^4 + X^2 + 1 = (X + a)(X - a)(X + a + 1)(X - a - 1)$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a)[X]$.
Mit $L = \mathbf{Q}(a)$ und $K = \mathbf{Q}$ ist $[L : K] = 2$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + X^2 + 1);
KK<a> := ext<Q | X^2 + X + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^4 + XX^2 + 1);
```

(2) Es ist $X^6 + X^2 + 1$ irreduzibel in $\mathbf{Q}[X]$. Sei $\mathbf{Q}(a)|\mathbf{Q}$ mit $a^6 + a^2 + 1 = 0$.
Es ist $X^6 + X^2 + 1 = (X + a)(X - a)(X^4 + a^2X^2 + (a^4 + 1))$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a)[X]$. Sei $\mathbf{Q}(a, b)|\mathbf{Q}(a)$ mit $b^4 + a^2b^2 + (a^4 + 1) = 0$.
Es ist $X^6 + X^2 + 1 = (X + a)(X - a)(X + b)(X - b)(X^2 + (a^2 + b^2))$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a, b)[X]$. Sei $\mathbf{Q}(a, b, c)|\mathbf{Q}(a, b)$ mit $c^2 + (a^2 + b^2) = 0$.
Es ist $X^6 + X^2 + 1 = (X + a)(X - a)(X + b)(X - b)(X + c)(X - c)$ die Zerlegung in irreduzible Polynome in $\mathbf{Q}(a, b, c)[X]$.
Mit $L = \mathbf{Q}(a)$ und $K = \mathbf{Q}$ ist

$$[L : K] \;=\; [\mathbf{Q}(a, b, c) : \mathbf{Q}(a, b)][\mathbf{Q}(a, b) : \mathbf{Q}(a)][\mathbf{Q}(a) : \mathbf{Q}] \;=\; 6 \cdot 4 \cdot 2 \;=\; 48\,,$$

wie man den Graden der jeweiligen Minimalpolynome entnimmt.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 + X^2 + 1);
KK<a> := ext<Q | X^6 + X^2 + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 + XX^2 + 1);
KKK<b> := ext<KK | XX^4 + a^2*XX^2 + a^4 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^6 + XXX^2 + 1);
KKKK<c> := ext<KKK | XXX^2 + b^2 + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 + XXXX^2 + 1);
```

(3) Es ist $X^4+X+1=(X^2+X+\alpha)(X^2+X+\alpha^2)$ die Zerlegung in irreduzible Polynome in $\mathbf{F}_4[X]$. Sei $\mathbf{F}_4(b)|\mathbf{F}_4$ mit $b^2+b+\alpha=0$.
Es ist $X^4+X+1=(X+b)(X+b+\alpha)(X+b+1)(X+b+\alpha+1)$ die Zerlegung in irreduzible Polynome in $\mathbf{F}_4(b)[X]$.
Mit $L=\mathbf{F}_4(b)$ und $K=\mathbf{F}_4$ ist $[L:K]=2$ (und insbesondere $|\mathbf{F}_4(b)|=16$.).

```
F := GF(2);
R<X> := PolynomialRing(F);
FF<a> := ext<F | X^2 + X + 1>;
RR<XX> := PolynomialRing(FF);
Factorisation(XX^4 + XX + 1);
FFF<b> := ext<FF | XX^2 + XX + a>;
RRR<XXX> := PolynomialRing(FFF);
Factorisation(XXX^4 + XXX + 1);
```

... plus eine Umformung der entstandenen Koeffizienten von Hand.

Aufgabe 31

(1) Zunächst stellen wir mittels Magma fest, daß $X^2-2\in\mathbf{Q}[X]$ und $X^2-3\in\mathbf{Q}(\sqrt{2})[X]$ irreduzibel sind. Folglich ist

$$[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}] \;=\; [\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}):\mathbf{Q}] \;=\; 2\cdot 2 \;=\; 4\,.$$

Eine Basis von $\mathbf{Q}(\sqrt{2},\sqrt{3})$ über $\mathbf{Q}$ ist gegeben durch

$$(1,\,\sqrt{2},\,\sqrt{3},\,\sqrt{6})\,,$$

wofür wir $\sqrt{2}\sqrt{3}=\sqrt{6}$ vereinfacht haben.
Wir verwenden die Charakterisierung von $\mu_{\sqrt{2}+\sqrt{3},\mathbf{Q}}(X)$ als normiertes Polynom minimalen Grades in $\mathbf{Q}[X]$ mit Nullstelle $\sqrt{2}+\sqrt{3}$.
Wir berechnen also einmal die Potenzen von $\sqrt{2}+\sqrt{3}$, ausgedrückt in der vorstehenden Basis.

$$\begin{array}{lcrcrcrcr}
(\sqrt{2}+\sqrt{3})^0 &=& 1\cdot 1 &+& 0\cdot\sqrt{2} &+& 0\cdot\sqrt{3} &+& 0\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^1 &=& 0\cdot 1 &+& 1\cdot\sqrt{2} &+& 1\cdot\sqrt{3} &+& 0\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^2 &=& 5\cdot 1 &+& 0\cdot\sqrt{2} &+& 0\cdot\sqrt{3} &+& 2\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^3 &=& 0\cdot 1 &+& 11\cdot\sqrt{2} &+& 9\cdot\sqrt{3} &+& 0\cdot\sqrt{6}\\
(\sqrt{2}+\sqrt{3})^4 &=& 49\cdot 1 &+& 0\cdot\sqrt{2} &+& 0\cdot\sqrt{3} &+& 20\cdot\sqrt{6}
\end{array}$$

Es stellt sich mittels Linearer Algebra heraus, daß

$$\Big((\sqrt{2}+\sqrt{3})^0,\,(\sqrt{2}+\sqrt{3})^1,\,(\sqrt{2}+\sqrt{3})^2,\,(\sqrt{2}+\sqrt{3})^3\Big)$$

linear unabhängig ist.
Ferner stellt sich mittels Linearer Algebra heraus, daß

$$(\sqrt{2}+\sqrt{3})^4-10(\sqrt{2}+\sqrt{3})^2+(\sqrt{2}+\sqrt{3})^0 \;=\; 0\,.$$

Dies, zusammen mit der vorher festgestellen linearen Unabhängigkeit, zeigt, daß X^4-10X^2+1 das normierte Polynom kleinsten Grades mit Nullstelle $\sqrt{2}+\sqrt{3}$ ist. In anderen Worten, wir haben

$$\mu_{\sqrt{2}+\sqrt{3},\mathbf{Q}}(X) \;=\; X^4-10X^2+1\,.$$

Insbesondere ist $[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]=4$. Aus Dimensionsgründen folgt, daß $\mathbf{Q}(\sqrt{2}+\sqrt{3})=\mathbf{Q}(\sqrt{2},\sqrt{3})$.

(2) Zunächst ist natürlich

$$\begin{aligned}\mu_{0,\mathbf{F}_2}(X) &= X\\ \mu_{1,\mathbf{F}_2}(X) &= X+1\,.\end{aligned}$$

Es hat das irreduzible Polynom $X^3+X+1\in\mathbf{F}_2[X]$ die Nullstelle β, und also auch die Nullstellen β^2 und β^4, wie eine Anwendung des Frobenius liefert; vgl. Bemerkung in §2.3.4. Also

$$\begin{aligned}\mu_{\beta,\mathbf{F}_2}(X) &= X^3+X+1\\ \mu_{\beta^2,\mathbf{F}_2}(X) &= X^3+X+1\\ \mu_{\beta^4,\mathbf{F}_2}(X) &= X^3+X+1\,.\end{aligned}$$

Berechnen wir das Minimalpolynom von β^3. Die Potenzen von β^3, ausgedrückt in der Standardbasis $(\beta^0,\beta^1,\beta^2)$, sind gegeben durch

$$\begin{aligned}(\beta^3)^0 &= 1\cdot\beta^0 + 0\cdot\beta^1 + 0\cdot\beta^2\\ (\beta^3)^1 &= 1\cdot\beta^0 + 1\cdot\beta^1 + 0\cdot\beta^2\\ (\beta^3)^2 &= 1\cdot\beta^0 + 0\cdot\beta^1 + 1\cdot\beta^2\\ (\beta^3)^3 &= 0\cdot\beta^0 + 0\cdot\beta^1 + 1\cdot\beta^2\,.\end{aligned}$$

Wir sehen, daß

$$\big((\beta^3)^0,\,(\beta^3)^1,\,(\beta^3)^2\big)$$

linear unabhängig über $\mathbf{F}_2$ ist. Ferner ist

$$(\beta^3)^3+(\beta^3)^2+(\beta^3)^0 \;=\; 0\,.$$

Beides zusammen gibt X^3+X^2+1 als normiertes Polynom minimalen Grades mit Nullstelle β^3, in anderen Worten, $\mu_{\beta^3,\mathbf{F}_2}(X)=X^3+X^2+1\in\mathbf{F}_2[X]$. Anwendung des Frobenius liefert die weiteren Nullstellen β^6 und $\beta^{12}=\beta^5$; vgl. Bemerkung in §2.3.4. Also

$$\begin{aligned}\mu_{\beta^3,\mathbf{F}_2}(X) &= X^3+X^2+1\\ \mu_{\beta^5,\mathbf{F}_2}(X) &= X^3+X^2+1\\ \mu_{\beta^6,\mathbf{F}_2}(X) &= X^3+X^2+1\,.\end{aligned}$$

Ein Automorphismus von $\mathbf{F}_8=\mathbf{F}_2(\beta)$ schränkt nach der ersten Bemerkung in §2.1 identisch auf $\mathbf{F}_2$ ein und muß mit der Bemerkung in §2.3.4 folglich das Element β auf eine Nullstelle seines Minimalpolynoms X^3+X+1 über $\mathbf{F}_2$ schicken, als da wären β, β^2 und β^4.

Nun schickt aber $\mathrm{Frob}^0_{\mathbf{F}_8}$ bereits β nach β, $\mathrm{Frob}^1_{\mathbf{F}_8}$ schickt β nach β^2 und $\mathrm{Frob}^2_{\mathbf{F}_8}$ schickt β nach β^4.

Da ein Körpermorphismus von $\mathbf{F}_8=\mathbf{F}_2(\beta)$ in einen anderen Körper bereits durch das Bild von β festliegt, gibt es also außer den Potenzen des Frobenius keine weiteren Automorphismen von $\mathbf{F}_8$.

Aufgabe 32

Es ist $K(y)|K(y^2)|K$. Um zu zeigen, daß $\deg\mu_{y^2,K}=\deg\mu_{y,K}$ ist, genügt es zu zeigen, daß $K(y^2)=K(y)$; vgl. Satz 2.(2) (Minimalpolynom).

Nun ist $K(y)=K(y^2)(y)$ ebenfalls eine endliche monogene Erweiterung. Es ist y eine Nullstelle von $X^2-y^2\in K(y^2)[X]$. Also ist $\mu_{y,K(y^2)}(X)$ ein Teiler von X^2-y^2, und insbesondere von Grad 1 oder von Grad 2. Dies zieht $[K(y):K(y^2)]\in\{1,2\}$ nach sich.

Mit Satz 1 (Gradsatz) ist nun $[K(y):K]=[K(y):K(y^2)][K(y^2):K]$. Da $[K(y):K]$ ungerade ist, folgt $[K(y):K(y^2)]=1$, und mithin $K(y)=K(y^2)$.

Zur Frage, ob $\mu_{y,K}(X)=\mu_{y^2,K}(X)$ ist. Dies ist im allgemeinen nicht der Fall. Sei z.B. $K=\mathbf{Q}$ und $y=\sqrt[3]{2}$. Es ist

$$\mu_{\sqrt[3]{2},\mathbf{Q}}(X) \;=\; X^3-2\,,$$

wohingegen sich

$$\mu_{(\sqrt[3]{2})^2,\mathbf{Q}}(X) \;=\; X^3 - 4$$

ergibt. Denn beide Polynome sind laut Magma irreduzibel und haben das jeweilig angegebene Element als Nullstelle.

Ferner liefert der Grad des ersten Minimalpolynoms, daß in der Tat $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ ungerade ist.

Aufgabe 33

(1) Nach dem Korollar in §2.5.4 existiert (bis auf Isomorphie genau) ein Körper mit p^k Elementen, genannt $\mathbf{F}_{p^k}$.

Nach Aufgabe 27.(5) gibt es in $\mathbf{F}_{p^k}^\times$ ein Element y mit $\mathrm{o}(y) = p^k - 1$. Mit Aufgabe 11.(1.b) ist $|\langle y\rangle| = \mathrm{o}(y)$, und folglich

$$\mathbf{F}_{p^k}^\times \;=\; \langle y\rangle\ .$$

In der Lösung zu Aufgabe 11.(1.b) haben wir gesehen, daß

$$\langle y\rangle \;=\; \{y^i \;:\; i \in \mathbf{Z}\} \;=\; \{y^i \;:\; i \in [0, \mathrm{o}(y) - 1]\} \;=\; \{y^i \;:\; i \in [0, p^k - 2]\}\ .$$

Insgesamt ist also

$$\mathbf{F}_{p^k}^\times \;=\; \{y^i \;:\; i \in [0, p^k - 2]\}$$

Insbesondere ist

$$\mathbf{F}_{p^k} \;=\; \mathbf{F}_p(y) \;=\; \{f(y) \;:\; f(X) \in \mathbf{F}_p[X]\}\ ,$$

da in letzterer Menge das Element y^i für alle $i \geqslant 0$ und das Element 0 auftreten.

Mit Satz 2.(2) (Minimalpolynom) ist

$$\deg \mu_{y,\mathbf{F}_p} \;=\; [\mathbf{F}_p(y) : \mathbf{F}_p] \;=\; [\mathbf{F}_{p^k} : \mathbf{F}_p] \;=\; k\ .$$

Mit Satz 2.(3) ist $\mu_{y,\mathbf{F}_p}(X)$ irreduzibel.

(2) Sei $K := \mathbf{F}_p[T]/f(T)\mathbf{F}_p[T]$. Sei $y := T + f(T)\mathbf{F}_p[T] \in K^\times$. Es ist $\mathrm{o}(y)$ ein Teiler von $|K^\times| = p^k - 1$. Also ist $y^{p^k} = y \cdot y^{p^k - 1} = y$.

Da y somit eine Nullstelle von $X^{p^k} - X$ ist ist mit Satz 2.(2) das Minimalpolynom $\mu_{y,\mathbf{F}_p}(X)$ ein Teiler von $X^{p^k} - X$ in $\mathbf{F}_p[X]$. Nun ist aber $\mu_{y,\mathbf{F}_p}(X) = f(X)$, e.g. da dies ein normiertes irreduzibles Polynom mit Nullstelle y ist.

Sei $z \in K^\times$. Genauso wie für y folgt auch, daß z eine Nullstelle von $X^{p^k} - X$ ist. Ferner ist 0 eine Nullstelle dieses Polynoms. Also hat dieses Polynom sämtliche Elemente von K als Nullstelle. Sukzessives Abdividieren und Gradvergleich liefert

$$X^{p^k} - X \;=\; \prod_{z \in K} (X - z) \;\in\; K[X]\ .$$

Da nun $f(X)$ auch in $K[X]$ ein Teiler von $X^{p^k} - X$ ist, folgt, daß $f(X)$ in $K[X]$ in Linearfaktoren zerfällt (von denen keiner mit Exponent $\geqslant 2$ auftritt).

Da in der Zerlegung von $X^{p^k} - X$ in $K[X]$ kein Linearfaktor mit Exponent $\geqslant 2$ auftritt, kann $f(X)^2$ das Polynom $X^{p^k} - X$ in $K[X]$ und daher auch in $\mathbf{F}_p[X]$ nicht teilen. (Es folgt auch noch, daß in der Zerlegung von $f(X)$ in $K[X]$ kein Linearfaktor mit Exponent $\geqslant 2$ auftritt.)

Aufgabe 34

(1) Sei $\mathbf{Q}(a,b)|\mathbf{Q}$ mit $a^3+a+1=0$ und $b^2+ab+(a^2+1)=0$. Dann wird

$$X^3+X+1 \;=\; (X-a)(X-b)(X+a+b) \;\in\; \mathbf{Q}(a,b)[X]$$

Da auch $\mathbf{Q}(a,b,-a-b)=\mathbf{Q}(a,b)$, ist $\mathbf{Q}(a,b)$ der Zerfällungskörper von $X^3+X+1\in\mathbf{Q}[X]$.
Es ist $[\mathbf{Q}(a,b):\mathbf{Q}]=[\mathbf{Q}(a,b):\mathbf{Q}(a)][\mathbf{Q}(a):\mathbf{Q}]=2\cdot 3=6$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^3 + X + 1);
KK<a> := ext<Q | X^3 + X + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^3 + XX + 1);
KKK<b> := ext<KK | XX^2 + a*XX + a^2 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^3 + XXX + 1);
```

(2) Sei $\mathbf{Q}(a,b)|\mathbf{Q}$ mit $a^4+4a^2+4a+8=0$ und $b^3+ab^2+(a^2+4)b+(a^3+4a+8)=0$. In $\mathbf{Q}(a,b)[X]$ wird

$$\begin{aligned} & X^4+4X^2+8X+8 \\ = \;& (X-a)\cdot(X-b)\cdot \\ & \cdot\big(X+\tfrac{1}{28}(-2a^3+3a^2-2a-6)b^2+\tfrac{1}{14}(3a^3-a^2+10a+16)b+\tfrac{1}{14}(-2a^3+3a^2-2a-20)\big)\cdot \\ & \cdot\big(X+\tfrac{1}{28}(2a^3-3a^2+2a+6)b^2+\tfrac{1}{14}(-3a^3+a^2-10a-2)b+\tfrac{1}{14}(2a^3-3a^2+16a+20)\big)\;. \end{aligned}$$

Da $\mathbf{Q}(a,b)$ von den Nullstellen dieses Polynoms erzeugt wird, ist $\mathbf{Q}(a,b)$ der Zerfällungskörper von $X^4+4X^2+8X+8\in\mathbf{Q}[X]$.
Es ist $[\mathbf{Q}(a,b):\mathbf{Q}]=[\mathbf{Q}(a,b):\mathbf{Q}(a)][\mathbf{Q}(a):\mathbf{Q}]=3\cdot 4=12$.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + 4*X^2 + 8*X + 8);
KK<a> := ext<Q | X^4 + 4*X^2 + 8*X + 8>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^4 + 4*XX^2 + 8*XX + 8);
KKK<b> := ext<KK | XX^3 + a*XX^2 + (a^2 + 4)*XX + a^3 + 4*a + 8>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^4 + 4*XXX^2 + 8*XXX + 8);
```

(3) Sei $\mathbf{Q}(a,b,c)|\mathbf{Q}$ mit $a^6-a^3+2=0$, $b^3+(a^3-1)=0$ und $c^2+ac+a^2=0$. In $\mathbf{Q}(a,b,c)[X]$ wird

$$X^6-X^3+2 \;=\; (X-a)(X-b)(X-c)(X+c+a)\big(X-\tfrac{1}{2}(a^5-a^2)bc+b\big)\big(X+\tfrac{1}{2}(a^5-a^2)bc\big)\;.$$

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 - X^3 + 2);
KK<a> := ext<Q | X^6 - X^3 + 2>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 - XX^3 + 2);
KKK<b> := ext<KK | XX^3 + a^3 - 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^6 - XXX^3 + 2);
KKKK<c> := ext<KKK | XXX^2 + a*XXX + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 - XXXX^3 + 2);
```

Da $\mathbf{Q}(a,b,c)$ von den Nullstellen dieses Polynoms erzeugt wird, ist $\mathbf{Q}(a,b,c)$ der Zerfällungskörper von $X^6 - X^3 + 2 \in \mathbf{Q}[X]$.

Es ist $[\mathbf{Q}(a,b,c) : \mathbf{Q}] = [\mathbf{Q}(a,b,c) : \mathbf{Q}(a,b)][\mathbf{Q}(a,b) : \mathbf{Q}(a)][\mathbf{Q}(a) : \mathbf{Q}] = 2 \cdot 3 \cdot 6 = 36$.

(4) In $\mathbf{Q}(\sqrt{2}, \mathrm{i})$ wird

$$X^2 + 1 \;=\; (X + \mathrm{i})(X - \mathrm{i}) \; .$$

Somit ist $\mathbf{Q}(\sqrt{2}, \mathrm{i})$ der Zerfällungskörper von $X^2 + 1$ über $\mathbf{Q}(\sqrt{2})$.

Es wird $[\mathbf{Q}(\sqrt{2}, \mathrm{i}) : \mathbf{Q}(\sqrt{2})] = 2$, da $X^2 + 1$ in $\mathbf{Q}(\sqrt{2})[X]$ irreduzibel ist, da es ja sogar in $\mathbf{R}[X]$ irreduzibel ist.

Magma ist nicht unbedingt erforderlich. Will man es anwenden, sieht das z.B. wie folgt aus.

```
Q := Rationals();
S<T> := PolynomialRing(Q);
K<a> := ext<Q | T^2 - 2>;
R<X> := PolynomialRing(K);
Factorisation(X^2 + 1);
KK<b> := ext<K | X^2 + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^2 + 1);
```

Teilaufgabe (4) diene nur der Illustration, daß der Grundkörper auch eine Erweiterung von $\mathbf{Q}$ sein kann.

Aufgabe 35

Sei L ein Zerfällungskörper von $X^p - a$. Sei $b \in L$ eine Nullstelle von $X^p - a$, i.e. sei $b^p = a$. Dann ist $(X - b)^p = X^p - b^p = X^p - a$ in $L[X]$.

Sei *angenommen,* es hat $X^p - a$ einen nichttrivialen normierten Faktor $f(X) \in K[X]$. Dann ist $f(X)$ in $L[X]$ von der Form $(X - b)^s$ für ein $s \in [1, p-1]$. Insbesondere ist $f_0 = (-b)^s \in K$. Seien u, $v \in \mathbf{Z}$ so, daß $su + pv = 1$. Es folgt

$$-b \;=\; (-b)^{su+pv} \;=\; \underbrace{((-b)^s)^u}_{\in K}\underbrace{(-1)^{pv}a^v}_{\in K} \;\in\; K \; ,$$

und mithin $b \in K$. Also ist a die p-te Potenz des Elements b von K, im *Widerspruch* zur Voraussetzung an a.

Somit ist $X^p - a$ als in $K[X]$ irreduzibel nachgewiesen.

Nun ist $\mu_{b,K}(X) = X^p - a$, da dies ein normiertes irreduzibles Polynom in $K[X]$ mit Nullstelle b ist. Mit Satz 2.(2) (Minimalpolynom) folgt nun, daß $[K(b) : K] = p$. Da andererseits, wie oben schon festgestellt,

$$X^p - a \;=\; (X - b)^p \;\in\; K(b)[X]$$

ist, ist $K(b)$ ein Zerfällungskörper von $X^p - a$.

Da zwei Zerfällungskörper isomorph sind, folgt $[L : K] = [K(b) : K] = p$. (Da desweiteren $K(b) \subseteq L$, folgt $K(b) = L$.)

Da der Frobenius für endliche Körper bijektiv ist, kann ein Element $a \in K$ wie in der Aufgabenstellung vorausgesetzt nur für einen unendlichen Körper K der Charakteristik p (wie z.B. $\mathbf{F}_p(T)$) existieren.

Aufgabe 36

(1) Die Aussage ist falsch. So z.B. ist in Aufgabe 34.(1) (in den Bezeichnungen der dortigen Lösung) zwar $\mu_{a,\mathbf{Q}}(X) = X^3 + X + 1$, aber $\mathbf{Q}(a)$ kein Zerfällungskörper von $X^3 + X + 1$, da die Zerlegung dieses Polynom in irreduzible Faktoren in $\mathbf{Q}(a)[X]$ die Gestalt

$$X^3 + X + 1 \;=\; (X - a)(X^2 + aX + a^2 + 1)$$

hat, und darin also ein Faktor von Grad $\geqslant 2$ aufgetreten ist.

(2) Die Aussage ist richtig. Denn es ist $X - y$ ein Teiler von $\mu_{y,K}(X)$ in $K(y)[X]$, da $\mu_{y,K}(y) = 0$. Es ist aber mit Satz 2.(2) (Minimalpolynom) $\deg \mu_{y,K} = [K(y) : K] = 2$. Somit liefert Division die Zerlegung

$$\mu_{y,K}(X) \;=\; (X - y)(X - z)$$

in $K(y)[X]$. Da insbesondere $z \in K(y)$ ist, ist $K(y, z) = K(y)$ der Zerfällungskörper von $\mu_{y,K}(X)$.

Aufgabe 37

(1) Zum einen ist $1_H = f(1_G) \in f(U)$. Seien zum anderen $x,\, y \,\in\, f(U)$ gegeben. Schreibe $x = f(u)$ und $y = f(v)$ mit $u,\, v \,\in\, U$. Es wird

$$xy^{-1} \;=\; f(u)f(v)^{-1} \;=\; f(uv^{-1}) \;\in\; f(U)\,.$$

(2) Da $G \leqslant G$, können wir (1) anwenden und erhalten $\operatorname{Im} f = f(G) \leqslant H$.

(3) Mit (2) ist $\operatorname{Im} f \leqslant G$, und insbesondere $\operatorname{Im} f$ eine Gruppe, mit von H vererbter Multiplikation. Da f ein Gruppenmorphismus ist, gilt dies auch für $f|^{\operatorname{Im} f}$. Da nun nach Voraussetzung f injektiv ist, ist $f|^{\operatorname{Im} f}$ bijektiv. Insgesamt ist $f|^{\operatorname{Im} f}$ also ein Gruppenisomorphismus.

(4) Zeigen wir zunächst, daß aus $N \leqslant H$ folgt, daß $f^{-1}(N) \leqslant G$. Zum einen ist $f(1_G) = 1_H \in N$, also $1_G \in f^{-1}(N)$. Seien zum anderen $x,\, y \,\in\, f^{-1}(N)$, d.h. $f(x),\, f(y) \,\in\, N$. Dann ist

$$f(xy^{-1}) \;=\; f(x)f(y)^{-1} \;\in\; N\,,$$

also $xy^{-1} \in f^{-1}(N)$.

Zeigen wir nun, daß aus $N \trianglelefteq H$ noch folgt, daß $f^{-1}(N) \trianglelefteq G$.

Sei $g \in G$. Wir *behaupten,* daß ${}^g f^{-1}(N) \subseteq f^{-1}(N)$. Sei hierzu $x \in f^{-1}(N)$, d.h. $f(x) \in N$. Dann wird

$$f({}^g x) \;=\; f(gxg^{-1}) \;=\; f(g)f(x)f(g)^{-1} \;=\; {}^{f(g)}f(x) \;\in\; N\,,$$

da $N \trianglelefteq H$, also ${}^g x \in f^{-1}(N)$. Dies zeigt die *Behaupptung.*

Diese Behauptung auf g^{-1} statt g angewandt liefert ${}^{g^{-1}}f^{-1}(N) \subseteq f^{-1}(N)$. Diese Inklusionsbeziehung auf beiden Seiten von links mit g konjugiert gibt

$$f^{-1}(N) \;=\; {}^g({}^{g^{-1}}f^{-1}(N)) \;\subseteq\; {}^g f^{-1}(N)\,.$$

Insgesamt also ${}^g f^{-1}(N) = f^{-1}(N)$.

(5) Da $\{1_H\} \trianglelefteq H$, können wir (4) anwenden und erhalten $\operatorname{Kern} f = \{g \in G \;:\; f(g) = 1_H\} = f^{-1}(\{1_H\}) \trianglelefteq G$.

Aufgabe 38

(1) Sei $U \leqslant G$. Die Voraussetzung $|G|$ endlich werden wir erst im Teil (c) brauchen.

(a) Seien $b, b' \in G$. Sei $bU \cap b'U \neq \emptyset$. Zu zeigen ist, daß $bU = b'U$. Durch Rollenvertauschung von b und b' genügt es zu zeigen, daß $bU \subseteq b'U$. Sei also $x \in bU \cap b'U$. Schreibe $x = bu = b'v$ mit $u, v \in U$. Sei $y \in bU$. Wir haben zu zeigen, daß $y \in b'U$. Schreibe $y = bw$ mit $w \in U$. In der Tat wird

$$y \;=\; bw \;=\; b' \underbrace{vu^{-1}w}_{\in U} \;\in\; b'U\ .$$

(b) Die Abbildungen $U \longrightarrow bU$, $u \longmapsto bu$ und $bU \longrightarrow U$, $x \longmapsto b^{-1}x$ invertieren sich wechselseitig, da

$$u \;\longmapsto\; bu \;\longmapsto b^{-1}bu \;=\; u$$

und

$$x \;\longmapsto\; b^{-1}x \;\longmapsto\; bb^{-1}x \;=\; x\ .$$

Insbesondere ist $U \longrightarrow bU$, $u \longmapsto bu$ eine Bijektion.

(c) Sei nun $|G|$ endlich. Mit (a) ist G eine disjunkte Vereinigung von Teilmengen der Form bU für gewisse $b \in G$. Mit (b) haben alle Teilnehmer dieser disjunkten Vereinigung die Kardinalität $|U|$. Also ist $|U|$ ein Teiler von $|G|$.

(2) Es ist $(1,3) \circ (1,3,4) = (3,4)$. Es ist $(1,6,3) \circ (2,4,3,5) \circ (2,4) = (1,6,3,5,2)$.

(3) Nichtnormale Untergruppen:

$$\langle(1,2)\rangle,\ \langle(1,3)\rangle,\ \langle(2,3)\rangle \;\leqslant\; \mathcal{S}_3\ .$$

Normale Untergruppen:

$$\{\mathrm{id}\},\ \langle(1,2,3)\rangle,\ \mathcal{S}_3 \;\trianglelefteqslant\; \mathcal{S}_3\ .$$

Man erhält die komplette Liste durch sukzessives Hinzufügen von Erzeugenden. Auf diese Weise kann man die Untergruppen erhalten, die minimal über einer gegebenen Untergruppe liegen, d.h. so, daß echt dazwischen keine weitere liegt.

So z.B. erkennt man (von Hand oder via Magma), daß für jedes Element $x \in \mathcal{S}_3 \smallsetminus \{(1,2)\}$ gilt, daß bereits $\langle(1,2),\, x\rangle = \mathcal{S}_3$. Also kann es echt zwischen $\langle(1,2)\rangle$ und $\mathcal{S}_3$ keine weiteren Untergruppen mehr geben.

Schließlich prüft man die erhaltene Liste von Untergruppen auf Normalität durch.

(4) Mittels `Order(sub<SymmetricGroup(12) | (1,2,3,4,5,6,7,8,9,10,11,12), (1,3)>);` erhalten wir die Ordnung der angegebenen Untergruppe

$$|\langle(1,2,3,4,5,6,7,8,9,10,11,12),\ (1,3)\rangle| \;=\; 1036800\ .$$

Ferner ist

$$|\mathcal{S}_{12}| \;=\; 12! \;=\; 479001600$$

Und in der Tat ist $479001600/1036800 = 462$.

Aufgabe 39

(1) In Aufgabe 34.(2) wurde der Zerfällungskörper $\mathbf{Q}(a,b)$ konstruiert, mit

$$\begin{array}{lcl} \mu_{a,\mathbf{Q}}(X) & = & X^4 + 4X^2 + 4X + 8 \\ \mu_{b,\mathbf{Q}(a)}(X) & = & X^3 + aX^2 + (a^2+4)X + (a^3+4a+8)\ . \end{array}$$

Insbesondere war $[\mathbf{Q}(a,b) : \mathbf{Q}] = 12$ festgestellt worden. Es zerfiel

$$\begin{array}{ll} & X^4 + 4X^2 + 8X + 8 \\ = & (X-a)\cdot(X-b)\cdot \\ & \cdot\big(X + \frac{1}{28}(-2a^3+3a^2-2a-6)b^2 + \frac{1}{14}(3a^3-a^2+10a+16)b + \frac{1}{14}(-2a^3+3a^2-2a-20)\big)\cdot \\ & \cdot\big(X + \frac{1}{28}(2a^3-3a^2+2a+6)b^2 + \frac{1}{14}(-3a^3+a^2-10a-2)b + \frac{1}{14}(2a^3-3a^2+16a+20)\big)\ . \end{array}$$

An den für all dies notwendig gewesenen Magma-Quelltext hängen wir noch die Definitionen

$$\begin{array}{lcl}\gamma_1 & := & a\\ \gamma_2 & := & b\\ \gamma_3 & := & \frac{1}{28}(2a^3-3a^2+2a+6)b^2+\frac{1}{14}(-3a^3+a^2-10a-16)b+\frac{1}{14}(2a^3-3a^2+2a+20)\\ \gamma_4 & := & \frac{1}{28}(-2a^3+3a^2-2a-6)b^2+\frac{1}{14}(3a^3-a^2+10a+2)b+\frac{1}{14}(-2a^3+3a^2-16a-20)\end{array}$$

an.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^4 + 4*X^2 + 8*X + 8);
KK<a> := ext<Q | X^4 + 4*X^2 + 8*X + 8>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^4 + 4*XX^2 + 8*XX + 8);
KKK<b> := ext<KK | XX^3 + a*XX^2 + (a^2 + 4)*XX + a^3 + 4*a + 8>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^4 + 4*XXX^2 + 8*XXX + 8);
ga1 := a;
ga2 := b;
ga3 := 1/28*(2*a^3 - 3*a^2 + 2*a + 6)*b^2 + 1/14*(-3*a^3 + a^2 - 10*a - 16)*b
       + 1/14*(2*a^3 - 3*a^2 + 2*a + 20);
ga4 := 1/28*(-2*a^3 + 3*a^2 - 2*a - 6)*b^2 + 1/14*(3*a^3 - a^2 + 10*a + 2)*b
       + 1/14*(-2*a^3 + 3*a^2 - 16*a - 20);
```

Es ist $m = 2$ und $n = 4$. Bestimmen wir das Bild von $\mathrm{Gal}(X^4 + 4X^2 + 8X + 8)$ in $\mathcal{S}_4$.

$$\begin{array}{ccc}\mathbf{Q}(a,b) & \xrightarrow[\sim]{\sigma_2} & \mathbf{Q}(\gamma_1',\gamma_2')\\ \uparrow & & \uparrow\\ \mathbf{Q}(a) & \xrightarrow[\sim]{\sigma_1} & \mathbf{Q}(\gamma_1')\\ \uparrow & & \uparrow\\ \mathbf{Q} & = & \mathbf{Q}\end{array}$$

Nullstellen bedeute im folgenden stets Nullstellen in $\mathbf{Q}(a,b)$.

Die Nullstellen von

$$\mu_{a,\mathbf{Q}}(X) \;=\; X^4+4X^2+8X+8$$

sind γ_1, γ_2, γ_3 und γ_4 ([31]). Unter diesen haben wir ein γ_1' auszuwählen.

Fall $\gamma_1' = \gamma_1$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^3+\gamma_1X^2+(\gamma_1^2+4)X+(\gamma_1^3+4\gamma_1+8)\;,$$

welches die Nullstellen γ_2, γ_3 und γ_4 hat ([32]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_2$. Wir erhalten das zulässige Tupel (γ_1, γ_2). Es werden

$$\begin{array}{lcl}\sigma_2(\gamma_3) & = & \frac{1}{28}(2\gamma_1^3-3\gamma_1^2+2\gamma_1+6)\gamma_2^2+\frac{1}{14}(-3\gamma_1^3+\gamma_1^2-10\gamma_1-16)\gamma_2+\frac{1}{14}(2\gamma_1^3-3\gamma_1^2+2\gamma_1+20)\\ & = & \gamma_3\\ \sigma_2(\gamma_4) & = & \frac{1}{28}(-2\gamma_1^3+3\gamma_1^2-2\gamma_1-6)\gamma_2^2+\frac{1}{14}(3\gamma_1^3-\gamma_1^2+10\gamma_1+2)\gamma_2+\frac{1}{14}(-2\gamma_1^3+3\gamma_1^2-16\gamma_1-20)\\ & = & \gamma_4\end{array}$$

[31] `Factorisation(XXX^4 + 4*XXX^2 + 8*XXX + 8);`

[32] `Factorisation(XXX^3 + ga1*XXX^2 + (ga1^2 + 4)*XXX + (ga1^3 + 4*ga1 + 8));`

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\1&2&3&4\end{smallmatrix}\right) = \mathrm{id}$. Das war klar, denn schickt man γ_1 auf γ_1 und γ_2 auf γ_2, so erhält man die Identität. Der Systematik halber haben wir es vollständig angeführt.

Zwischenstand: $|\langle \mathrm{id}\rangle| = 1 < 12$.

Subfall $\gamma_2' = \gamma_3$. Wir erhalten das zulässige Tupel (γ_1, γ_3). Es werden

$$\begin{aligned}\sigma_2(\gamma_3) &= \tfrac{1}{28}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 6)\gamma_3^2 + \tfrac{1}{14}(-3\gamma_1^3 + \gamma_1^2 - 10\gamma_1 - 16)\gamma_3 + \tfrac{1}{14}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 20)\\ &= \gamma_4\\ \sigma_2(\gamma_4) &= \tfrac{1}{28}(-2\gamma_1^3 + 3\gamma_1^2 - 2\gamma_1 - 6)\gamma_3^2 + \tfrac{1}{14}(3\gamma_1^3 - \gamma_1^2 + 10\gamma_1 + 2)\gamma_3 + \tfrac{1}{14}(-2\gamma_1^3 + 3\gamma_1^2 - 16\gamma_1 - 20)\\ &= \gamma_2\ ,\end{aligned}$$

wobei Magma für den letzten Schritt hilft ([33]).

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right) = (2,3,4)$.

Zwischenstand: $|\langle (2,3,4)\rangle| = 3 < 12$.

Subfall $\gamma_2' = \gamma_4$. Wir erhalten das zulässige Tupel (γ_1, γ_4). Es werden

$$\begin{aligned}\sigma_2(\gamma_3) &= \tfrac{1}{28}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 6)\gamma_4^2 + \tfrac{1}{14}(-3\gamma_1^3 + \gamma_1^2 - 10\gamma_1 - 16)\gamma_4 + \tfrac{1}{14}(2\gamma_1^3 - 3\gamma_1^2 + 2\gamma_1 + 20)\\ &= \gamma_2\\ \sigma_2(\gamma_4) &= \tfrac{1}{28}(-2\gamma_1^3 + 3\gamma_1^2 - 2\gamma_1 - 6)\gamma_4^2 + \tfrac{1}{14}(3\gamma_1^3 - \gamma_1^2 + 10\gamma_1 + 2)\gamma_4 + \tfrac{1}{14}(-2\gamma_1^3 + 3\gamma_1^2 - 16\gamma_1 - 20)\\ &= \gamma_3\end{aligned}$$

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right) = (2,4,3)$.

Zwischenstand: $|\langle (2,3,4),\ (2,4,3)\rangle| = 3 < 12$. Es kann $(2,4,3)$ weiters wieder entfallen.

Fall $\gamma_1' = \gamma_2$. Es ist

$$\mu_{b,\mathbf{Q}(a)}^{\sigma_2}(X) \ = \ X^3 + \gamma_2 X^2 + (\gamma_2^2 + 4)X + (\gamma_2^3 + 4\gamma_2 + 8)\ ,$$

welches die Nullstellen γ_1, γ_3 und γ_4 hat ([34]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_1$. Wir erhalten das zulässige Tupel (γ_2, γ_1). Es werden

$$\begin{aligned}\sigma_2(\gamma_3) &= \tfrac{1}{28}(2\gamma_2^3 - 3\gamma_2^2 + 2\gamma_2 + 6)\gamma_1^2 + \tfrac{1}{14}(-3\gamma_2^3 + \gamma_2^2 - 10\gamma_2 - 16)\gamma_1 + \tfrac{1}{14}(2\gamma_2^3 - 3\gamma_2^2 + 2\gamma_2 + 20)\\ &= \gamma_4\\ \sigma_2(\gamma_4) &= \tfrac{1}{28}(-2\gamma_2^3 + 3\gamma_2^2 - 2\gamma_2 - 6)\gamma_1^2 + \tfrac{1}{14}(3\gamma_2^3 - \gamma_2^2 + 10\gamma_2 + 2)\gamma_1 + \tfrac{1}{14}(-2\gamma_2^3 + 3\gamma_2^2 - 16\gamma_2 - 20)\\ &= \gamma_3\end{aligned}$$

Insgesamt $\bar\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right) = (1,2)(3,4)$.

[33] Man kann wie folgt vorgehen.

```
R2<Ga1,Ga2> := PolynomialRing(KKK,2);
Ga3 := 1/28*(2*Ga1^3 - 3*Ga1^2 + 2*Ga1 + 6)*Ga2^2 + 1/14*(-3*Ga1^3 + Ga1^2 - 10*Ga1 - 16)*Ga2
       + 1/14*(2*Ga1^3 - 3*Ga1^2 + 2*Ga1 + 20);
Ga4 := 1/28*(-2*Ga1^3 + 3*Ga1^2 - 2*Ga1 - 6)*Ga2^2 + 1/14*(3*Ga1^3 - Ga1^2 + 10*Ga1 + 2)*Ga2
       + 1/14*(-2*Ga1^3 + 3*Ga1^2 - 16*Ga1 - 20);
Evaluate(Ga3,[ga1,ga3]);
Evaluate(Ga4,[ga1,ga3]);
Evaluate(Ga3,[ga1,ga3]) eq ga4;
```

[34] `Factorisation(XXX^3 + ga2*XXX^2 + (ga2^2 + 4)*XXX + (ga2^3 + 4*ga2 + 8));`

Zwischenstand: $|\langle(2,3,4),\,(1,2)(3,4)\rangle| = 12$ ([35]).

Abbruch der Fallunterscheidungen, da fertig!

Als Ergebnis erhalten wir das isomorphe Bild von $\mathrm{Gal}(X^4+4X^2+8X+8)$ in $\mathcal{S}_4$

$$\langle(2,3,4),\,(1,2)(3,4)\rangle\ .$$

Die Liste ihrer Elemente erhält man via `{u : u in sub<SymmetricGroup(4) | (2,3,4), (1,2)(3,4)>};`, sie war nicht verlang, sieht hier aber noch ganz hübsch aus:

$\langle(2,3,4),\,(1,2)(3,4)\rangle\ =$
$\{\mathrm{id},\,(1,2,3),\,(1,2,4),\,(1,3,2),\,(1,3,4),\,(1,4,2),\,(1,4,3),\,(2,3,4),\,(2,4,3),\,(1,2)(3,4),\,(1,3)(2,4),\,(1,4)(2,3)\}\ .$

(2) In Aufgabe 30.(2) wurde der Zerfällungskörper $\mathbf{Q}(a,b,c)$ konstruiert, mit

$$\begin{array}{lcl}\mu_{a,\mathbf{Q}}(X) & = & X^6+X^2+1\\ \mu_{b,\mathbf{Q}(a)}(X) & = & X^4+a^2X^2+(a^4+1)\\ \mu_{c,\mathbf{Q}(a,b,c)}(X) & = & X^2+(a^2+b^2)\ .\end{array}$$

Insbesondere war $[\mathbf{Q}(a,b,c):\mathbf{Q}]=48$ festgestellt worden. Es zerfiel

$$X^6+X^2+1\ =\ (X-a)(X-b)(X-c)(X+a)(X+b)(X+c)\ .$$

An den damaligen Magma-Quelltext hängen wir noch die Definitionen

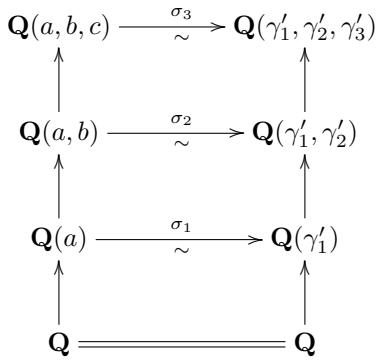
$$\begin{array}{lcl}\gamma_1 & = & a\\ \gamma_2 & = & b\\ \gamma_3 & = & c\\ \gamma_4 & = & -a\\ \gamma_5 & = & -b\\ \gamma_6 & = & -c\end{array}$$

an.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 + X^2 + 1);
KK<a> := ext<Q | X^6 + X^2 + 1>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 + XX^2 + 1);
KKK<b> := ext<KK | XX^4 + a^2*XX^2 + a^4 + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^6 + XXX^2 + 1);
KKKK<c> := ext<KKK | XXX^2 + b^2 + a^2>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 + XXXX^2 + 1);
ga1 := a;
ga2 := b;
ga3 := c;
ga4 := -a;
ga5 := -b;
ga6 := -c;
```

[35] `Order(sub<SymmetricGroup(4) | (2,3,4), (1,2)(3,4)>);`

Es ist $m = 3$ und $n = 6$. Bestimmen wir das Bild von $\mathrm{Gal}(X^6 + X^2 + 1)$ in $\mathcal{S}_6$.



Nullstellen bedeute im folgenden stets Nullstellen in $\mathbf{Q}(a,b,c)$.

Die Nullstellen von

$$\mu_{a,\mathbf{Q}}(X) \;=\; X^6 + X^2 + 1$$

sind γ_1, γ_2, γ_3, γ_4, γ_5 und γ_6 ([36]). Unter diesen haben wir ein γ_1' auszuwählen.

Fall $\gamma_1' = \gamma_1$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^4 + \gamma_1^2 X^2 + (\gamma_1^4 + 1)\;,$$

welches die Nullstellen γ_2, γ_3, γ_5 und γ_6 hat ([37]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_2$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_2^2)\;,$$

welches die Nullstellen γ_3 und γ_6 hat ([38]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_2, \gamma_3)$. Es werden

$$\begin{array}{lcllcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_6) & = & -\gamma_3 & = & \gamma_6\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{smallmatrix}\right) = \mathrm{id}$.

Zwischenstand: $|\langle \mathrm{id}\rangle| = 1 < 48$.

Subsubfall $\gamma_3' = \gamma_6$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_2, \gamma_6)$. Es werden

$$\begin{array}{lcllcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_6) & = & -\gamma_6 & = & \gamma_3\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\1&2&6&4&5&3\end{smallmatrix}\right) = (3,6)$.

Zwischenstand: $|\langle(3,6)\rangle| = 2$.

[36] `Factorisation(XXXX^6 + XXXX^2 + 1);`
[37] `Factorisation(XXXX^4 + ga1^2 * XXXX^2 + (ga1^4 + 1));`
[38] `Factorisation(XXXX^2 + (ga1^2 + ga2^2));`

Subfall $\gamma_2' = \gamma_3$. Es ist

$$\mu_{c,\mathbf{Q}(a,b)}^{\sigma_2}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_3^2)\;,$$

welches die Nullstellen γ_2 und γ_5 hat ([39]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_2$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_3, \gamma_2)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_3 & = & \gamma_6 \\ \sigma_3(\gamma_6) & = & -\gamma_2 & = & \gamma_5\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&3&2&4&6&5 \end{smallmatrix}\right) = (2,3)(5,6)$.

Zwischenstand: $|\langle (3,6),\, (2,3)(5,6)\rangle| = 8 < 48$ ([40]).

Subsubfall $\gamma_3' = \gamma_5$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_3, \gamma_5)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_3 & = & \gamma_6 \\ \sigma_3(\gamma_6) & = & -\gamma_5 & = & \gamma_2\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&3&5&4&6&2 \end{smallmatrix}\right) = (2,3,5,6)$.

Zwischenstand: $|\langle (3,6),\, (2,3)(5,6),\, (2,3,5,6)\rangle| = 8 < 48$ ([41]). Es kann $(2,3,5,6)$ weiters wieder entfallen.

Subfall $\gamma_2' = \gamma_5$. Es ist

$$\mu_{c,\mathbf{Q}(a,b)}^{\sigma_2}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_5^2)\;,$$

welches die Nullstellen γ_3 und γ_6 hat ([42]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_5, \gamma_3)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_5 & = & \gamma_2 \\ \sigma_3(\gamma_6) & = & -\gamma_3 & = & \gamma_6\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&3&4&2&6 \end{smallmatrix}\right) = (2,5)$.

Zwischenstand: $|\langle (3,6),\, (2,3)(5,6),\, (2,5)\rangle| = 8 < 48$ ([43]). Es kann $(2,5)$ weiters wieder entfallen.

Subsubfall $\gamma_3' = \gamma_6$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_5, \gamma_6)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_5 & = & \gamma_2 \\ \sigma_3(\gamma_6) & = & -\gamma_6 & = & \gamma_3\;. \end{array}$$

Insgesamt $\bar{\sigma}_3 = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&6&4&2&3 \end{smallmatrix}\right) = (2,5)(3,6)$.

[39] `Factorisation(XXXX^2 + (ga1^2 + ga3^2));`
[40] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6)>);`
[41] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,3,5,6)>);`
[42] `Factorisation(XXXX^2 + (ga1^2 + ga5^2));`
[43] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,5)>);`

Zwischenstand: $|\langle(3,6),\,(2,3)(5,6),\,(2,5)(3,6)\rangle| = 8 < 48$ ([44]). Es kann $(2,5)(3,6)$ weiters wieder entfallen.

Subfall $\gamma_2' = \gamma_6$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_1^2 + \gamma_6^2)\;,$$

welches die Nullstellen γ_2 und γ_5 hat ([45]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_2$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_6, \gamma_2)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_6 & = & \gamma_3 \\ \sigma_3(\gamma_6) & = & -\gamma_2 & = & \gamma_5\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\1&6&2&4&3&5\end{smallmatrix}\right) = (2,6,5,3)$.

Zwischenstand: $|\langle(3,6),\,(2,3)(5,6),\,(2,6,5,3)\rangle| = 8 < 48$ ([46]). Es kann $(2,6,5,3)$ weiters wieder entfallen.

Subsubfall $\gamma_3' = \gamma_5$. Wir erhalten das zulässige Tupel $(\gamma_1, \gamma_6, \gamma_5)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_5) & = & -\gamma_6 & = & \gamma_3 \\ \sigma_3(\gamma_6) & = & -\gamma_5 & = & \gamma_2\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\1&6&5&4&3&2\end{smallmatrix}\right) = (2,6)(3,5)$.

Zwischenstand: $|\langle(3,6),\,(2,3)(5,6),\,(2,6)(3,5)\rangle| = 8 < 48$ ([47]). Es kann $(2,6)(3,5)$ weiters wieder entfallen.

Fall $\gamma_1' = \gamma_2$. Es ist

$$\mu^{\sigma_1}_{b,\mathbf{Q}(a)}(X) \;=\; X^4 + \gamma_2^2 X^2 + (\gamma_2^4 + 1)\;,$$

welches die Nullstellen γ_1, γ_3, γ_4 und γ_6 hat ([48]). Unter diesen haben wir ein γ_2' auszuwählen.

Subfall $\gamma_2' = \gamma_1$. Es ist

$$\mu^{\sigma_2}_{c,\mathbf{Q}(a,b)}(X) \;=\; X^2 + (\gamma_2^2 + \gamma_1^2)\;,$$

welches die Nullstellen γ_3 und γ_6 hat ([49]). Unter diesen haben wir ein γ_3' auszuwählen.

Subsubfall $\gamma_3' = \gamma_3$. Wir erhalten das zulässige Tupel $(\gamma_2, \gamma_1, \gamma_3)$. Es werden

$$\begin{array}{rcrcl} \sigma_3(\gamma_4) & = & -\gamma_2 & = & \gamma_5 \\ \sigma_3(\gamma_5) & = & -\gamma_1 & = & \gamma_4 \\ \sigma_3(\gamma_6) & = & -\gamma_3 & = & \gamma_6\;. \end{array}$$

Insgesamt $\bar\sigma_3 = \left(\begin{smallmatrix}1&2&3&4&5&6\\2&1&3&5&4&6\end{smallmatrix}\right) = (1,2)(4,5)$.

---

[44] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,5)(3,6)>);`
[45] `Factorisation(XXXX^2 + (ga1^2 + ga6^2));`
[46] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,6,5,3)>);`
[47] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (2,6)(3,5)>);`
[48] `Factorisation(XXXX^4 + ga2^2 * XXXX^2 + (ga2^4 + 1));`
[49] `Factorisation(XXXX^2 + (ga2^2 + ga1^2));`

Zwischenstand: $|\langle(3,6),\,(2,3)(5,6),\,(1,2)(4,5)\rangle| = 48$ ([50]).

Abbruch der Fallunterscheidungen, da fertig!

Als Ergebnis erhalten wir das isomorphe Bild von $\mathrm{Gal}(X^6+X^2+1)$ in $\mathcal{S}_6$

$$\langle(3,6),\,(2,3)(5,6),\,(1,2)(4,5)\rangle\ .$$

Die Liste ihrer Elemente erhält man mit

```
{u : u in sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (1,2)(4,5)>};
```

Mit etwas mehr Erfahrung kann man sich auch "verdächtige Fälle" auswählen, um so ein langes Stagnieren des Erzeugnisses, wie hier geschehen, zu verhindern zu versuchen.

Aufgabe 40

Sei $K(a)|K$ mit $\mu_{a,K}(X) = f(X)$. Es ist $K(a)$ Zerfällungskörper von $f(X)$; vgl. Aufgabe 36.(2). Folglich ist $|\mathrm{Gal}(f(X))| = [K(a):K] = 2$. Auf der anderen Seite ist $\deg f = 2$, und mithin $\mathrm{Gal}(f(X))$ isomorph zu einer Untergruppe von $\mathcal{S}_2$. Folglich ist $\mathrm{Gal}(f(X)) \simeq \mathcal{S}_2$.

Ist speziell $K = \mathbf{R}$ und $f(X) = X^2+1 \in \mathbf{R}[X]$, so folgt $\mathcal{S}_2 \simeq \mathrm{Gal}(X^2+1) = \mathrm{Gal}(\mathbf{R}(i)|\mathbf{R}) = \mathrm{Gal}(\mathbf{C}|\mathbf{R})$.

Aufgabe 41

(1) In der Notation von §3.4.2.1 ist der Zerfällungskörper von $X^3+X+1 \in \mathbf{Q}[X]$ gegeben durch $\mathbf{Q}(a,b)$ mit $a^3+a+1=0$ und $b^2+ab+(a^2+1)=0$. Insbesondere ist

$$(1, a, a^2, b, ba, ba^2)$$

eine $\mathbf{Q}$-lineare Basis von $\mathbf{Q}(a,b)$.

Es waren $\gamma_1 = a$, $\gamma_2 = b$ und $\gamma_3 = -a-b$ die Nullstellen von $f(X)$ in $\mathbf{Q}(a,b)$.

Das Bild von $\mathrm{Gal}(\mathbf{Q}(a,b)|\mathbf{Q})$ in $\mathcal{S}_3$ bezüglich dieser Nullstellennumerierung ist gleich $\mathcal{S}_3$.

Es ist $\langle(1,3)\rangle = \{\mathrm{id},\,(1,3)\}$. Die zugehörigen Automorphismen schicken

$$\begin{array}{ccccccc} a & \overset{\mathrm{id}}{\longmapsto} & a & \qquad & a & \overset{(1,3)}{\longmapsto} & -a-b \\ b & \longmapsto & b & & b & \longmapsto & b\ . \end{array}$$

Da $\mathrm{Tr}_{\langle(1,3)\rangle} : \mathbf{Q}(a,b) \longrightarrow \mathrm{Fix}_{\langle(1,3)\rangle}\,\mathbf{Q}(a,b)$ eine surjektive $\mathbf{Q}$-lineare Abbildung ist, ist das Bildtupel der $\mathbf{Q}$-Basis $(1,a,a^2,b,ba,ba^2)$ von $\mathbf{Q}(a,b)$ ein $\mathbf{Q}$-Erzeugendensystem von $\mathrm{Fix}_{\langle(1,3)\rangle}\,\mathbf{Q}(a,b)$. Berechnen wir dieses eintragsweise, so erhalten wir

$$\begin{array}{rl} & \big(\mathrm{Tr}_{\langle(1,3)\rangle}(1),\ \mathrm{Tr}_{\langle(1,3)\rangle}(a),\ \mathrm{Tr}_{\langle(1,3)\rangle}(a^2),\ \mathrm{Tr}_{\langle(1,3)\rangle}(b),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba^2)\big) \\ = & \big(1+1,\ a+(-a-b),\ a^2+(-a-b)^2,\ b+b,\ ba+b(-a-b),\ b(a^2+(-a-b)^2a^2)\big) \\ = & \big(2,\ -b,\ 2a^2+2ab+b^2,\ 2b,\ -b^2,\ b(2a^2+2ab+b^2)\big) \\ = & \big(2,\ -b,\ 2a^2+2ab-ab-(a^2+1),\ 2b,\ ab+(a^2+1),\ b(2a^2+2ab-ab-(a^2+1))\big) \\ = & \big(2,\ -b,\ a^2+ba-1,\ 2b,\ a^2+ba+1,\ b(a^2+ab-1)\big) \\ = & \big(2,\ -b,\ a^2+ba-1,\ 2b,\ a^2+ba+1,\ ba^2-a(ab+(a^2+1))-1\big) \\ = & \big(2,\ -b,\ a^2+ba-1,\ 2b,\ a^2+ba+1,\ ba^2-ba^2-a^3-a-1\big) \\ = & \big(2,\ -b,\ a^2+ba-1,\ 2b,\ a^2+ba+1,\ 0\big)\ . \end{array}$$

Dieses $\mathbf{Q}$-Erzeugendensystem kann etwa zur $\mathbf{Q}$-Basis

$$\big(1,\ b,\ a^2+ba+1\big)$$

von $\mathrm{Fix}_{\langle(1,3)\rangle}\,\mathbf{Q}(a,b)$ umgeformt und ausgedünnt werden. Man erkennt auch, daß

$$\mathrm{Fix}_{\langle(1,3)\rangle}\,\mathbf{Q}(a,b) \;=\; \mathbf{Q}(b)\ ,$$

da $-b^2 = ba+a^2+1$.

[50] `Order(sub<SymmetricGroup(6) | (3,6), (2,3)(5,6), (1,2)(4,5)>);`

(2) Die allgemeine Situation ist wie in (1).

Es ist $\langle(1,2,3)\rangle = \{\mathrm{id}, (1,2,3), (1,3,2)\}$. Die zugehörigen Automorphismen schicken

$$\begin{array}{cccccccccc} a & \overset{\mathrm{id}}{\longmapsto} & a & a & \overset{(1,2,3)}{\longmapsto} & b & a & \overset{(1,3,2)}{\longmapsto} & -a-b \\ b & \longmapsto & b & b & \longmapsto & -a-b & b & \longmapsto & a\,. \end{array}$$

Da $\mathrm{Tr}_{\langle(1,2,3)\rangle} : \mathbf{Q}(a,b) \longrightarrow \mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b)$ eine surjektive $\mathbf{Q}$-lineare Abbildung ist, ist das Bildtupel der $\mathbf{Q}$-Basis $(1, a, a^2, b, ba, ba^2)$ von $\mathbf{Q}(a,b)$ ein $\mathbf{Q}$-Erzeugendensystem von $\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b)$. Berechnen wir dieses eintragsweise, so erhalten wir.

$$\begin{array}{ll} & \big(\mathrm{Tr}_{\langle(1,3)\rangle}(1),\ \mathrm{Tr}_{\langle(1,3)\rangle}(a),\ \mathrm{Tr}_{\langle(1,3)\rangle}(a^2),\ \mathrm{Tr}_{\langle(1,3)\rangle}(b),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba^2)\big) \\ = & \big(1+1+1,\ a+b+(-a-b),\ a^2+b^2+(-a-b)^2, \\ & b+(-a-b)+a,\ ba+(-a-b)b+a(-a-b),\ ba^2+(-a-b)b^2+a(-a-b)^2\big) \\ = & \big(3,\ 0,\ 2a^2+2b^2+2ab,\ 0,\ -a^2-b^2-ab,\ -b^3+a^3+3a^2b\big) \\ = & \big(3,\ 0,\ -2,\ 0,\ 1,\ -a+b+3a^2b\big) \end{array}$$

Dieses $\mathbf{Q}$-Erzeugendensystem kann etwa zur $\mathbf{Q}$-Basis

$$\big(1,\ -a+b+3a^2b\big)$$

von $\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b)$ umgeformt und ausgedünnt werden. Man erkennt auch, daß

$$\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b) \;=\; \mathbf{Q}(-a+b+3a^2b) \qquad ([51])\,.$$

(3) In der Notation der Lösung zu Aufgabe 34.(2) ist der Zerfällungskörper von $X^4+4X^2+8X+8 \in \mathbf{Q}[X]$ gegeben durch $\mathbf{Q}(a,b)$ mit $a^4+4a^2+8a+8=0$ und $b^3+ab^2+(a^2+4)b+a^3+4a+8=0$. Insbesondere ist

$$(1,\ a,\ a^2,\ a^3,\ b,\ ba,\ ba^2,\ ba^3,\ b^2,\ b^2a,\ b^2a^2,\ b^2a^3)$$

eine $\mathbf{Q}$-lineare Basis von $\mathbf{Q}(a,b)$. Wir verwenden Magma; vgl. auch Lösung zu Aufgabe 39.(1).

Seien

$$\begin{array}{lcl} \gamma_1 & := & a \\ \gamma_2 & := & b \\ \gamma_3 & := & \frac{1}{28}(2a^3-3a^2+2a+6)b^2+\frac{1}{14}(-3a^3+a^2-10a-16)b+\frac{1}{14}(2a^3-3a^2+2a+20) \\ \gamma_4 & := & \frac{1}{28}(-2a^3+3a^2-2a-6)b^2+\frac{1}{14}(3a^3-a^2+10a+2)b+\frac{1}{14}(-2a^3+3a^2-16a-20) \end{array}$$

die Nullstellen von X^4+4X^2+8X+8 in $\mathbf{Q}(a,b)$.

In Magma kann man $\mathrm{Tr}_{\langle(1,2,3)\rangle}$ (nach Eingabe der benötigten Daten wir in Lösung zu Aufgabe 39.(1)) z.B. wie folgt eingeben.

```
RBIG<A,B> := PolynomialRing(KKK,2);
Tr := func< u | Evaluate(u,[ga1,ga2]) + Evaluate(u,[ga2,ga3]) + Evaluate(u,[ga3,ga1])>;
```

Will man damit die Spur von, sagen wir, a^2b wissen, muß `Tr(A^2*B);` eingegeben werden.

[51] Cf. `MinimalPolynomial(b*a^2 + (-a-b)*b^2 + a*(-a-b)^2,Q);` , vorausgesetzt, $\mathbf{Q}(a,b)$ ist in Magma wie in §3.4.2.1 eingegeben.

Das Resultat notieren wir als Matrix. In den Zeilen stehen die Koeffizienten der Bilder der obigen Basiselemente von $\mathbf{Q}(a,b)$, ausgedrückt in ebendieser Basis.

		a^0b^0	a^1b^0	a^2b^0	a^3b^0	a^0b^1	a^1b^1	a^2b^1	a^3b^1	a^0b^2	a^1b^2	a^2b^2	a^3b^2
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^0b^0)$		84	0	0	0	0	0	0	0	0	0	0	0
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^1b^0)$		40	32	−6	4	−4	−20	2	−6	6	2	−3	2
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^2b^0)$		−48	40	−4	12	−40	−32	−8	−4	32	20	−2	6
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^3b^0)$		−560	−112	0	0	0	56	−28	28	0	0	14	0
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^0b^1)$		40	32	−6	4	−4	−20	2	−6	6	2	−3	2
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^1b^1)$		−64	−40	4	−12	40	32	8	4	−32	−20	2	−6
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^2b^1)$	$\frac{1}{28}$	−48	−16	−32	−16	128	24	20	−4	−80	−64	−2	−8
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^3b^1)$		96	−192	−48	32	−32	64	−96	64	48	16	32	16
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^0b^2)$		−48	40	−4	12	−40	−32	−8	−4	32	20	−2	6
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^1b^2)$		176	−16	80	−16	−96	24	20	−4	32	48	−2	−8
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^2b^2)$		288	96	−32	−16	128	−32	48	−32	−80	−64	−16	−8
$\mathrm{Tr}_{\langle(1,2,3)\rangle}(a^3b^2)$		512	320	−368	96	352	−256	−64	−32	−80	−176	−16	48

In Magma kann man Matrizen mit Einträgen in $\mathbf{Q}$ wie folgt eingeben. Der Quelltext

```
Q := Rationals();
M := RMatrixSpace(Q,2,3)!Matrix([[1,2,3],[4,5,6]]);
```

z.B. liefert die 2×3-Matrix $M = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{smallmatrix}\right) \in \mathbf{Q}^{2\times 3}$.
Unsere 12×12-Matrix kann unter Zuhilfenahme von Magma via `EchelonForm(M);` zeilenweise umgeformt werden zu

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & -4 & 2 & -2 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 4 & -4 & 2 & 0 & -4 & -2 & 0 & 2 & 0 & 0 & 1 \end{pmatrix}$$

Wir erhalten als $\mathbf{Q}$-Basis von $\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b)$

$$\left(1,\ 8a - 4ab + 2a^2b - 2a^3b - a^2b^2,\ a^2 - 2b + b^2 + ab^2,\ 4a - 4a^2 + 2a^3 - 4ab - 2a^2b + 2b^2 + a^3b^2\right).$$

Da `MinimalPolynomial(a^2 - 2b + b^2 + a b^2,Q);` das Minimalpolynom des dritten Basiselements über $\mathbf{Q}$ zu $X^4 + 8X^3 + 80X^2 - 192 * X + 128 \ni \mathbf{Q}[X]$ liefert, ist in der Tat

$$\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b) \;=\; \mathbf{Q}(a^2 - 2b + b^2 + ab^2)\,.$$

(4) Sei $\mathbf{F}_{16} = \mathbf{F}_4(\delta)$ mit $\delta^4 + \delta + 1 = 0$; vgl. Lösung zu Aufgabe 24.(4). Es ist $\mathbf{F}_{16}$ der Zerfällungskörper von $X^{16} - X$; vgl. §2.5.4. Es ist $\mathrm{o}(\mathrm{Frob}_{\mathbf{F}_{16}}) = 4$, also $\langle \mathrm{Frob}^2_{\mathbf{F}_{16}}\rangle = \{\mathrm{Frob}^0_{\mathbf{F}_{16}},\ \mathrm{Frob}^2_{\mathbf{F}_{16}}\}$.
Die $\mathbf{F}_2$-Basis $(1, \delta, \delta^2, \delta^3)$ von $\mathbf{F}_{16}$ wird also abgebildet auf

$$\begin{array}{rl} & \left(\mathrm{Tr}_{\langle \mathrm{Frob}^2_{\mathbf{F}_{16}}\rangle}(1),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2_{\mathbf{F}_{16}}\rangle}(\delta),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2_{\mathbf{F}_{16}}\rangle}(\delta^2),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2_{\mathbf{F}_{16}}\rangle}(\delta^3)\right) \\ = & \left(1+1,\ \delta+\delta^4,\ \delta^2+\delta^8,\ \delta^3+\delta^1 2\right) \\ = & \left(0,\ 1,\ 1,\ \delta^2+\delta+1\right). \end{array}$$

Vgl. Lösung zu Aufgabe 27.(6). Dies kann zur Basis

$$\left(1,\ \delta^2 + \delta\right)$$

von $\mathrm{Fix}_{\langle \mathrm{Frob}^2_{\mathbf{F}_{16}}\rangle}\,\mathbf{F}_4$ umgeformt werden. Vgl. auch das Ergebnis von Aufgabe 24.(4).

Es fällt auf, daß in allen betrachteten Beispielen $[L : \mathrm{Fix}_U L] = |U|$ ist. Wir werden dies noch allgemein bestätigen; cf. Satz 8.(1).

Aufgabe 42

(1) Für die Wohldefiniertheit der Multiplikation ist zu zeigen, daß im Falle $gN = g'N$ und $\tilde{g}N = \tilde{g}'N$ auch $(g \cdot \tilde{g})N = (g' \cdot \tilde{g}')N$ ist, wobei g, g', $\tilde{g}$, $\tilde{g}' \in G$.
In der Tat ist dann $g' = gn$ und $\tilde{g}' = \tilde{g}\tilde{n}$ für gewisse n, $\tilde{n} \in N$, und es wird

$$g'\tilde{g}' \;=\; gn\tilde{g}\tilde{n} \;=\; g\tilde{g}\underbrace{\underbrace{\tilde{g}^{-1}n\tilde{g}}_{\in N}\tilde{n}}_{\in N}\,,$$

mithin $g'\tilde{g}'N = g\tilde{g}N$.
Die Gruppeneigenschaften wie Assoziativität, Einselement $1_G N$ und Inverses $g^{-1}N$ zu $gN \in G/N$ vererben sich nun alle aus denen für G.

(2) Für die Wohldefiniertheit ist zu zeigen, daß aus $g \operatorname{Kern} f = g' \operatorname{Kern} f$ auch $f(g) = f(g')$ folgt, wobei g, $g' \in G$. In der Tat haben wir diesenfalls $g' = gn$ für ein $n \in \operatorname{Kern} f$. Es wird $f(g') = f(gn) = f(g)f(n) = f(g) \cdot 1_H = f(g)$.
Nach Konstruktion liegt nun ein surjektiver Gruppenmorphismus $G/N \longrightarrow \operatorname{Im} f$, $g \operatorname{Kern} f \longmapsto f(g)$ vor.
Für die Injektivität ist zu zeigen, daß sein Kern gleich $\{1_G\}$ ist. Sei $g \in G$ so, daß $g \operatorname{Kern} f \longmapsto f(g) = 1_H$. Dann ist $g \in \operatorname{Kern} f$, i.e. $g \operatorname{Kern} f = 1_G \operatorname{Kern} f$.

(3) Nach Aufgaben 38.(1.c), 37.(2) ist $|\operatorname{Im} f|$ ein Teiler von $|H|$. Nach Aufgabe 37.(5) ist insbesondere $N \leqslant G$. Die Lösung zur Aufgabe 38.(1.c) zeigt nun, daß $|G| = |N||G/N|$ – in der Tat kann G in $|G/N|$ Teilmengen der Kardinalität $|N|$ disjunkt zerlegt werden. Mit (2) ist also $|\operatorname{Im} f| = |G/N|$ ein Teiler von $|G|$.

Aufgabe 43

(1) Sei $\sigma \in \mathcal{S}_n$. Wir *behaupten,* daß es genau einen Automorphismus $\hat{\sigma}$ von $K(T_1, \ldots, T_n)$ mit $\hat{\sigma}(T_i) = T_{\sigma(i)}$ für $i \in [1, n]$ und $\tilde{\sigma}|_K^K = \mathrm{id}_K$ gibt, sowie, daß für σ, $\rho \in \mathcal{S}_n$ gilt, daß $\widehat{\rho \circ \sigma} = \hat{\rho} \circ \hat{\sigma}$.
Nach der Gebrauchsanweisung für Polynomringe gibt es genau einen Ringmorphismus

$$\tilde{\sigma} \;:\; K[T_1, \ldots, T_n] \;\longrightarrow\; K[T_1, \ldots, T_n]$$

mit $\sigma(T_i) = T_{\sigma(i)}$ für $i \in [1, n]$ und $\tilde{\sigma}|_K$ gleich der Einbettung $K \xrightarrow{c} K[T_1, \ldots, T_n]$, i.e. $\tilde{\sigma}|_K^K = \mathrm{id}_K$; vgl. §1.6.2.
Nach der Gebrauchsanweisung für Quotientenkörper, angewandt auf das Kompositum

$$K[T_1, \ldots, T_n] \xrightarrow{\tilde{\sigma}} K[T_1, \ldots, T_n] \xrightarrow{\lambda} K(T_1, \ldots, T_n)\,,$$

gibt es genau einen Ringmorphismus – dann auch Körpermorphismus –

$$\hat{\sigma} \;:\; K(T_1, \ldots, T_n) \xrightarrow{\hat{\sigma}} K(T_1, \ldots, T_n)$$

mit $\hat{\sigma} \circ \lambda = \lambda \circ \tilde{\sigma}$.

$$\begin{array}{ccc} K[T_1, \ldots, T_n] & \xrightarrow{\tilde{\sigma}} & K[T_1, \ldots, T_n] \\ \lambda \downarrow & & \downarrow \lambda \\ K(T_1, \ldots, T_n) & \xrightarrow{\hat{\sigma}} & K(T_1, \ldots, T_n)\,. \end{array}$$

Insgesamt gibt es genau einen Körpermorphismus $K(T_1,\dots,T_n) \xrightarrow{\hat\sigma} K(T_1,\dots,T_n)$ mit mit $\hat\sigma(T_i) = T_{\sigma(i)}$ für $i \in [1,n]$.

Seien nun $\sigma, \rho \in \mathcal{S}_n$ gegeben. Es ist $\widehat{\rho\circ\sigma}$ der einzige Körpermorphismus von $K(T_1,\dots,T_n)$ in sich mit

$$\widehat{\rho\circ\sigma}(T_i) \;=\; T_{\widehat{\rho\circ\sigma}(i)} \;=\; T_{(\rho(\sigma(i))}$$

für $i \in [1,n]$. Nun ist aber auch für den Körpermorphismus $\hat\rho\circ\hat\sigma$ von $K(T_1,\dots,T_n)$ in sich

$$(\hat\rho\circ\hat\sigma)(T_i) \;=\; \hat\rho(\hat\sigma(T_i)) \;=\; \hat\rho(T_{\sigma(i)}) \;=\; T_{\rho(\sigma(i))}$$

für $i \in [1,n]$. Also ist $\widehat{\rho\circ\sigma} = \hat\rho\circ\hat\sigma$.

Beachte noch, daß $\widehat{\mathrm{id}} = \mathrm{id}$, da die Identität die verlangte Eigenschaft $\mathrm{id}(T_i) = T_i = T_{\mathrm{id}(i)}$ hat.

Insbesondere zeigt $\widehat{\sigma^{-1}}\circ\hat\sigma = \widehat{\sigma^{-1}\circ\sigma} = \widehat{\mathrm{id}} = \mathrm{id}$, daß $\hat\sigma$ auch surjektiv und damit ein Automorphismus von $K(T_1,\dots,T_n)$ ist.

Dies zeigt die *Behauptung.*

Damit haben wir einen Gruppenmorphismus $\mathcal{S}_n \longrightarrow \mathrm{Aut}\big(K(T_1,\dots,T_n)|K\big)$, $\sigma \longmapsto \hat\sigma$, definiert. Dieser ist injektiv, da $\hat\sigma = \mathrm{id}$ insbesondere zu $T_{\sigma(i)} = \hat\sigma(T_i) = T_i$ für $i \in [1,n]$ führt, und somit zu $\sigma = \mathrm{id}$.

Die angesprochene Identifikation bedeutet in der Praxis, daß wir fürderhin einfach wieder σ statt $\hat\sigma$ schreiben.

(2) Wir setzen

$$u(X) \;:=\; +s_nX^n - s_{n-1}X^{n-1} + \cdots \pm s_1X \mp s_0 \;:=\; (X-T_1)(X-T_2)\cdots(X-T_n) \;\in\; E[X]\,.$$

In anderen Worten, es ist s_i die Summe aus allen Produkten aus $n-i$ verschiedenen Faktoren aus $\{T_1,\dots,T_n\}$, wobei $i \in [0,n]$.

Z.B. wird für $n = 3$

$$\begin{aligned} s_0 &= T_1T_2T_3 \\ s_1 &= T_1T_2 + T_1T_3 + T_2T_3 \\ s_2 &= T_1 + T_2 + T_3 \\ s_3 &= 1\,. \end{aligned}$$

(3) Ist $\sigma \in \mathcal{S}_n$, so wird, in der Notation der Lösung zu (2),

$$\begin{aligned} u^\sigma(X) &\overset{1.}{=} ((X-T_1)(X-T_2)\cdots(X-T_n))^\sigma \\ &= (X-T_1)^\sigma(X-T_2)^\sigma\cdots(X-T_n)^\sigma \\ &= (X-\sigma(T_1))(X-\sigma(T_2))\cdots(X-\sigma(T_n)) \\ &= (X-T_{\sigma(1)})(X-T_{\sigma(2)})\cdots(X-T_{\sigma(n)}) \\ &= (X-T_1)(X-T_2)\cdots(X-T_n) \\ &= u(X) \\ &= +s_nX^n - s_{n-1}X^{n-1} + \cdots \pm s_1X \mp s_0 \\ &\overset{2.}{=} (+s_nX^n - s_{n-1}X^{n-1} + \cdots \pm s_1X \mp s_0)^\sigma \\ &= +\sigma(s_n)X^n - \sigma(s_{n-1})X^{n-1} + \cdots \pm \sigma(s_1)X \mp \sigma(s_0)\,. \end{aligned}$$

Koeffizientenvergleich gibt $\sigma(s_i) = s_i$ für $i \in [0,n]$. Ist

Beachte, daß L ein Teilkörper von E ist, da L das Element 1_E enthält, und da Differenz und Quotient zweier Elemente von L wieder in L liegen, wobei bei der Quotientenbildung der Nenner ungleich 0 sei.

Ist $\frac{f(s_0,\dots,s_{n-1})}{g(s_0,\dots,s_{n-1})}$ wie in der Aufgabenstellung ein beliebig gewähltes Element aus L, und ist $\sigma \in \mathcal{S}_n$, so wird

$$\sigma\big(\tfrac{f(s_0,\dots,s_{n-1})}{g(s_0,\dots,s_{n-1})}\big) \;=\; \tfrac{\sigma(f(s_0,\dots,s_{n-1}))}{\sigma(g(s_0,\dots,s_{n-1}))} \;=\; \tfrac{f(\sigma(s_0),\dots,\sigma(s_{n-1})))}{g(\sigma(s_0),\dots,\sigma(s_{n-1})))} \;=\; \tfrac{f(s_0,\dots,s_{n-1})}{g(s_0,\dots,s_{n-1})}\,.$$

Also ist $\sigma|_L^L = \mathrm{id}_L$.

Da dies für alle $\sigma \in \mathcal{S}_n$ gilt, ist $L \subseteq \mathrm{Fix}_{\mathcal{S}_n} E$.

Mit der Folgerung zu Satz 7 (Dedekinds Lemma) ist also $[E : L] \geqslant [E : \mathrm{Fix}_{\mathcal{S}_n} E] \geqslant |\mathcal{S}_n| = n!$.

(4) Sei $i \in [1, n]$. Betrachte

$$g_i(X) \;:=\; (X - T_i) \cdots (X - T_n) \;=\; \frac{u(X)}{(X - T_1) \cdots (X - T_{i-1})} \;\in\; E(X) \,.$$

Ersterer Ausdruck zeigt, daß $g_i(X) \in E[X]$ liegt. Insbesondere geht die Polynomdivision von $u(X)$ durch $(X - T_1) \cdots (X - T_{i-1})$ auf. Nun liegen aber $u(X) \in L[X] \subseteq L(T_1, \ldots, T_{i-1})[X]$ und $(X - T_1) \cdots (X - T_{i-1}) \in L(T_1, \ldots, T_{i-1})[X]$. Der Polynomdivisionsalgorithmus zeigt nun, daß auch der Quotient $g_i(X)$ in $L(T_1, \ldots, T_{i-1})[X]$ liegt.

Es ist also $g_i(X)$ ein normiertes Polynom mit Nullstelle T_i. Insbesondere ist T_i algebraisch über $L(T_1, \ldots, T_{i-1})$. Ferner ist $\mu_{T_i,\, L(T_1,\ldots,T_{i-1})}(X)$ ein Teiler von $g_i(X)$; vgl. Satz 2.(2), §2.3.2. Mit loc. cit. ist auch

$$[L(T_1, \ldots, T_{i-1}, T_i) : L(T_1, \ldots, T_{i-1})] \;=\; \deg \mu_{T_i,\, L(T_1,\ldots,T_{i-1})} \;\leqslant\; \deg g_i \;=\; n - i + 1 \,.$$

Beachte schließlich, daß $L(T_1, \ldots, T_n) = E$. In der Tat ist jedes Polynom in T_1, …, T_n mit Koeffizienten in K in der linken Seite enthalten. Ist ein solches Polynom ungleich null, so ist, da $L(T_1, \ldots, T_n)$ ein Teilkörper von E ist, also auch sein Inverses in $L(T_1, \ldots, T_n)$. Damit ist auch jedes beliebige Element von E, das sich ja als Bruch zweier solcher Polynome mit Nenner ungleich null schreiben läßt, in $L(T_1, \ldots, T_n)$.

In der Produktzerlegung

$$[E : L] \;=\; [L(T_1) : L] \cdots [L(T_1, T_2) : L(T_1)] \cdots [L(T_1, \ldots, T_n) : L(T_1, \ldots, T_{n-1})]$$

ist der i-te Faktor $\leqslant n - i + 1$, wohingegen das Produkt $\geqslant n! = \prod_{i \in [1,n]} (n - i + 1)$ ist. Mithin ist der i-te Faktor

$$[L(T_1, \ldots, T_{i-1}, T_i) : L(T_1, \ldots, T_{i-1})] \;=\; n - i + 1$$

für $i \in [1, n]$. Somit ist $\mu_{T_i,\, L(T_1,\ldots,T_{i-1})}(X) = g_i(X) = (X - T_i) \cdots (X - T_n)$ für $i \in [1, n]$; vgl. Satz 2.(2).

Eine L-lineare Basis von E ist also etwa gegeben durch

$$\left(T_1^{\alpha_1} \cdots T_n^{\alpha_n} \;:\; \alpha_i \in [0, n - i] \text{ für } i \in [1, n]\right) .$$

In der Tat folgt aus Gradgründen auch $L(T_1, \ldots, T_{n-1}) = E$. Dies sieht man auch direkt ein, denn $T_n = s_{n-1} - (T_1 + \cdots + T_{n-1})$.

Aufgabe 44

(1) Schreibe $Z := \{z \in L \;:\; z^n = 1\}$. Es ist $1 \in Z$. Sind $z, \tilde{z} \in Z$, so ist auch $(z\tilde{z}^{-1})^n = z^n (\tilde{z}^n)^{-1} = 1$, also $z\tilde{z}^{-1} \in Z$. Also ist $Z \leqslant L^\times$.

Es zerfällt $X^n - 1$ in $L[X]$ in Linearfaktoren. Da nun

$$\mathrm{ggT}(X^n - 1, (X^n - 1)') \;=\; \mathrm{ggT}(X^n - 1,\, nX^{n-1}) \;=\; 1 \qquad ({}^{52}) \,,$$

enthält diese Produktzerlegung von $X^n - 1$ auch n verschiedene Linearfaktoren; vgl. Aufgabe 25.(2). Da aber Z gerade die Nullstellenmenge von $X^n - 1$ in L ist, folgt $|Z| = n$.

Wir verwenden die Argumente für Aufgabe 27.(5). Sei ζ_n ein Element von Z maximaler Ordnung. Es ist $\mathrm{o}(\zeta_n)$ ein Teiler von $|Z| = n$.

[52] Wofür man $\mathrm{char}\, K = 0$ benötigt.

Mit Aufgabe 27.(4) ist $\mathrm{o}(z)$ ein Teiler von $\mathrm{o}(\zeta_n)$ für alle $z \in Z$. Also ist z eine Nullstelle von $X^{\mathrm{o}(\zeta_n)} - 1$ in L. Da letzteres Polynom mithin n verschiedene Nullstellen in L hat, folgt $n \leqslant \deg(X^{\mathrm{o}(\zeta_n)} - 1) = \mathrm{o}(\zeta_n)$.

Zusammen ist $\mathrm{o}(\zeta_n) = n$. Aber dies impliziert $|\langle\zeta_n\rangle| = \mathrm{o}(\zeta_n) = n = |Z|$, und somit $\langle\zeta_n\rangle = Z$; vgl. Aufgabe 11.(1.b).

Da $L = K(z : z \in Z)$ als Zerfällungskörper von $X^n - 1 \in K[X]$, und da $Z = \{\zeta_n^i \ : \ i \in [0, n-1]\}$, ist $L = K(\zeta_n)$.

(2) Zunächst einmal halten wir fest, daß $\mathrm{ggT}(k, n) = \mathrm{ggT}(k + zn, n)$ für $z \in \mathbf{Z}$, und also das Auswahlkriterium für $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, es sei $\mathrm{ggT}(k, n) = 1$, unabhängig vom betrachteten Repräsentanten k ist.

Wir haben zu zeigen, daß das Produkt zweier Elemente von $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ wieder in dieser Menge liegt, daß eine Eins in $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ liegt, und daß zu jedem Element von $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ ein multiplikativ Inverses in $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ vorhanden ist. Dann ist $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ mit der Multiplikation eine Gruppe; abelsch, da $\mathbf{Z}/n\mathbf{Z}$ ein kommutativer Ring ist.

Seien $k + n\mathbf{Z}$, $\tilde{k} + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$. Dann ist $\mathrm{ggT}(k, n) = 1$ und $\mathrm{ggT}(\tilde{k}, n) = 1$, und somit auch $\mathrm{ggT}(k\tilde{k}, n) = 1$, i.e. $(k + n\mathbf{Z})(\tilde{k} + n\mathbf{Z}) \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$.

Es ist $1 + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ ein Einselement.

Sei $k + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$. Da $\mathrm{ggT}(k, n) = 1$, gibt es s, $t \in \mathbf{Z}$ mit $sk + tn = 1$; vgl. Aufgabe 2. Es ist $\mathrm{ggT}(s, n) = 1$, da ein gemeinsamer Faktor von s und n auch in $sk + tn = 1$ auftreten würde. Also ist $s + n\mathbf{Z} \in \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$. Ferner ist

$$(s + n\mathbf{Z})(k + n\mathbf{Z}) \ = \ sk + n\mathbf{Z} \ = \ (sk + tn) + n\mathbf{Z} \ = \ 1 + n\mathbf{Z} \, .$$

Die Elementordnungen in $\mathrm{U}(\mathbf{Z}/12\mathbf{Z})$ ergeben sich wie folgt. Wir verwenden die Konvention, z für $z + 12\mathbf{Z}$ zu schreiben.

$$\begin{array}{lcl} \mathrm{o}(1) & = & 1 \\ \mathrm{o}(5) & = & 2 \\ \mathrm{o}(-5) & = & 2 \\ \mathrm{o}(-1) & = & 2 \end{array}$$

Folglich ist $\mathrm{U}(\mathbf{Z}/12\mathbf{Z})$ nicht von einem Element erzeugt, denn dieses müßte Ordnung 4 haben; vgl. Aufgabe 11.(1.b).

> Ist jedoch p prim, so ist $\mathrm{U}(\mathbf{Z}/p\mathbf{Z}) = \mathbf{F}_p^\times$ von einem Element erzeugt, vgl. Aufgabe 27.(5).

(3) Zeigen wir, daß eine wohldefinierte Abbildung $\mathrm{Gal}(L|K) \longrightarrow \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, $\sigma \longmapsto i_\sigma$ vorliegt.

Zum einen ist zu zeigen, daß aus $\zeta_n^i = \zeta_n^j$ folgt, daß $i + n\mathbf{Z} = j + n\mathbf{Z}$; daß also das Element ζ_n^i die Restklasse des Exponenten i modulo n bestimmt. Nun ist aber $\mathrm{o}(\zeta_n) = n$ in $L^\times$ nach (1). Aus $\zeta_n^i = \zeta_n^j$, d.h. aus $\zeta_n^{j-i} = 1$ folgt also, daß $n = \mathrm{o}(\zeta_n)$ den Exponenten $j - i$ teilt, d.h. daß $j \equiv_n i$.

Zum anderen ist zu zeigen, daß $\mathrm{ggT}(i_\sigma, n) = 1$ für $\sigma \in \mathrm{Gal}(L|K)$. Nun ist aber

$$\zeta_n \ = \ \sigma^{-1}(\sigma(\zeta_n)) \ = \ \sigma^{-1}(\zeta_n^{i_\sigma}) \ = \ \sigma^{-1}(\zeta_n)^{i_\sigma} \ = \ \zeta_n^{i_{\sigma^{-1}} \cdot i_\sigma}$$

Folglich ist $i_{\sigma^{-1}} \cdot i_\sigma \equiv_n 1$, i.e. es gibt ein $t \in \mathbf{Z}$ mit $i_{\sigma^{-1}} \cdot i_\sigma + nt = 1$. Somit können i_σ und n keinen nichttrivialen gemeinsamen Faktor haben, da dieser auch in 1 aufgehen würde.

Zeigen wir, daß ein Gruppenmorphismus vorliegt. Seien σ, $\rho \in \mathrm{Gal}(L|K)$. Es wird

$$\zeta_n^{i_{\rho\circ\sigma}} \ = \ (\rho \circ \sigma)(\zeta_n) = \rho(\zeta_n^{i_\sigma}) \ = \ \rho(\zeta_n)^{i_\sigma} \ = \ (\zeta_n^{i_\rho})^{i_\sigma} \ = \ \zeta_n^{i_\rho \cdot i_\sigma} \ ,$$

also $i_{\rho\circ\sigma} + n\mathbf{Z} = (i_\rho + n\mathbf{Z}) \cdot (i_\sigma + n\mathbf{Z})$.

Zeigen wir, daß dieser Gruppenmorphismus $\mathrm{Gal}(L|K) \longrightarrow \mathrm{U}(\mathbf{Z}/n\mathbf{Z})$, $\sigma \longmapsto i_\sigma + n\mathbf{Z}$ injektiv ist. Ist $i_\sigma \equiv_n 1$, so ist

$$\sigma(\zeta_n) \ = \ \zeta_n^{i_\sigma} \ = \ \zeta_n \ = \ \mathrm{id}(\zeta_n) \, ,$$

da $\mathrm{o}(\zeta_n) = n$. Da $L = K(\zeta_n)$, folgt $\sigma = \mathrm{id}_L$; vgl. dritte Bemerkung aus §3.4.1.

Da also $\mathrm{Gal}(L|K)$ isomorph zu einer Untergruppe der abelschen Gruppe $\mathrm{U}(\mathbf{Z}/n\mathbf{Z})$ ist, ist $\mathrm{Gal}(L|K)$ insbesondere abelsch.

Aufgabe 45

(1) Ist $\mathrm{char}\, K = 0$, so ist $\mathrm{char}\, L = 0$ und somit L perfekt.

Ist $\mathrm{char}\, K = p > 0$, so ist $\mathrm{Frob}_K : K \xrightarrow{\sim} K$. Wir haben zu zeigen, daß $\mathrm{Frob}_L : L \longrightarrow L$ surjektiv ist.

Es ist L ein K-Vektorraum wie üblich.

Ferner wird L zu einem K-Vektorraum vermöge der Addition auf L und der skalaren Multiplikation $x * y := x^p y$ für $x \in K$ und $y \in L$. Schreibe diesen $L^{(p)}$. In der Tat ist für $y,\ y' \in L$ und $x,\ x' \in K$

$$\begin{array}{lcllcll} 1 * y & = & 1^p \cdot y & = & 1 \cdot y & = & y \\ x * (y + y') & = & x^p(y + y') & = & x^p y + x^p y' & = & x * y + x * y' \\ (x + x') * y & = & (x + x')^p y & = & x^p y + x'^p y & = & x * y + x' * y \\ (xx') * y & = & (xx')^p y & = & x^p x'^p y & = & x * (x' * y)\ . \end{array}$$

Sei $(y_1, \ldots, y_n)$ eine K-Basis von L. Dann ist $(y_1, \ldots, y_n)$ auch eine K-Basis von $L^{(p)}$, wie man wie folgt einsieht.

Lineare Unabhängigkeit. Aus

$$x_1 * y_1 + \cdots + x_n * y_n \ = \ 0$$

für $x_i \in K$ folgt, daß $x_1^p y_1 + \cdots + x_n^p y_n = 0$, woraus $x_i^p = 0$ stets, woraus, wegen Injektivität von Frob_K, $x_i = 0$ stets.

Erzeugendensystem. Es gibt für ein gegebenes y Elemente $x_i \in K$ mit

$$y = x_1 y_1 + \cdots + x_n y_n\ .$$

Sei $\tilde{x}_i^p = x_i$ stets, was wegen Frob_K surjektiv möglich ist. Also wird

$$y = \tilde{x}_1^p y_1 + \cdots + \tilde{x}_n^p y_n \ = \ \tilde{x}_1 * y_1 + \cdots + \tilde{x}_n * y_n\ .$$

Da nun $(y_1, \ldots, y_n)$ als K-Basis von $L^{(p)}$ nachgewiesen ist, folgt $\dim_K L^{(p)} = n = \dim_K L$.

Nun ist Frob_L sicher injektiv. Aufgefaßt als Abbildung von L nach $L^{(p)}$ ist nun Frob_L auch K-linear, da

$$\mathrm{Frob}_L(xy) \ = \ x^p y^p \ = \ x * \mathrm{Frob}_L(y)$$

für $x \in K$ und $y \in L$. Als injektive Abbildung zwischen gleichdimensionalen Vektorräumen L und $L^{(p)}$ ist Frob_L also auch surjektiv.

Somit ist L perfekt.

(2) Es genügt zu zeigen, daß M Zerfällungskörper eines Polynoms in $K[X]$ ist, welches in ein Produkt verschiedener irreduzibler Polynome zerfällt.

Da $L|K$ galoisch ist, ist L Zerfällungskörper eines Polynoms $g(X) \in K[X]$, welches in ein Produkt verschiedener irreduzibler Polynome zerfällt; vgl. zweites Lemma in §3.5.1.4.

Sei $h(X) := \mathrm{kgV}(f(X), g(X)) \in K[X]$. Mit loc. cit. genügt es zu zeigen, daß M der Zerfällungskörper von $h(X)$ ist.

Sei $\{\gamma_1, \ldots, \gamma_k\}$ die Nullstellenmenge von $g(X)$ in M. Da $g(X)$ bereits in $L[X]$ in Linearfaktoren zerfällt, ist $\{\gamma_1, \ldots, \gamma_k\} \subseteq L$.

Sei $\{\varphi_1, \ldots, \varphi_\ell\}$ die Nullstellenmenge von $f(X)$ in M. Die Situation stellt sich so dar.

$$\begin{array}{rcl} M & = & L(\varphi_1, \ldots, \varphi_\ell) \\ | & & \\ L & = & K(\gamma_1, \ldots, \gamma_k) \\ | & & \\ K & & \end{array}$$

Es ist $\{\gamma_1, \ldots, \gamma_k\} \cup \{\varphi_1, \ldots, \varphi_\ell\}$ die Nullstellenmenge von $h(X)$ in M. Es ist $M = L(\varphi_1, \ldots, \varphi_\ell) = K(\gamma_1, \ldots, \gamma_k, \varphi_1, \ldots, \varphi_\ell)$. Da sich dieses Erzeugnis durch Weglassen von doppelt aufgeführten Erzeugern nicht ändert, erzeugt die Nullstellenmenge von $h(X)$ in M den Körper M über K.

Um zu zeigen, daß $h(X) \in M[X]$ in ein Produkt von Linearfaktoren zerfällt, genügt es zu zeigen, daß jeder normierte irreduzible Faktor $u(X)$ von $h(X)$ in $K[X]$ im größeren Polynomring $M[X]$ in ein Produkt von Linearfaktoren zerfällt.

Wir betrachten also solch ein $u(X)$. Es ist $u(X)$ ein Teiler von $f(X)$ oder von $g(X)$ in $K[X]$ (möglicherweise von beiden).

Teilt $u(X)$ das Polynom $f(X)$, dann zerfällt daher $u(X)$ bereits in $L[X]$ in Linearfaktoren, also auch in $M[X]$.

Teilt $u(X)$ das Polynom $g(X)$, dann zerfällt daher $u(X)$ in $M[X]$ in Linearfaktoren.

Aufgabe 46

(1) Es ergibt sich der Zerfällungskörper von $X^6 + 3X + 3 \in \mathbf{Q}[X]$ zu $\mathbf{Q}(a, b, c, d)$ mit

$$\begin{array}{rcl} 0 & = & a^6 + 3a + 3 \\ 0 & = & b^3 + \frac{1}{17}(-6a^5 + 14a^4 - 10a^3 + 12a^2 + 6a - 15)b^2 \\ & & + \frac{1}{17}(-3a^5 + 7a^4 - 5a^3 + 6a^2 + 3a - 33)b + \frac{1}{17}(3a^5 - 7a^4 + 5a^3 - 6a^2 - 3a - 18) \\ 0 & = & c^2 + \frac{1}{17}(6a^5 - 14a^4 + 10a^3 - 12a^2 + 11a + 15)c + \frac{1}{17}(-11a^5 + 3a^4 - 7a^3 + 5a^2 - 6a - 36) \\ 0 & = & d^2 + \big(b + \frac{1}{17}(-6a^5 + 14a^4 - 10a^3 + 12a^2 + 6a - 15)\big)d \\ & & + \big(b^2 + \frac{1}{17}(-6a^5 + 14a^4 - 10a^3 + 12a^2 + 6a - 15)b + \frac{1}{17}(-3a^5 + 7a^4 - 5a^3 + 6a^2 + 3a - 33)\big) \; . \end{array}$$

Insbesondere ist $|\operatorname{Gal}(X^6 + 3X + 3)| = [\mathbf{Q}(a, b, c, d) : \mathbf{Q}] = 2 \cdot 2 \cdot 3 \cdot 6 = 72$.

Wir erhalten die Nullstellen

$$\begin{array}{rcl} \gamma_1 & := & a \\ \gamma_2 & := & b \\ \gamma_3 & := & c \\ \gamma_4 & := & d \\ \gamma_5 & := & -c - \frac{1}{17}(6a^5 - 14a^4 + 10a^3 - 12a^2 + 11a + 15) \\ \gamma_6 & := & -d - b + \frac{1}{17}(6a^5 - 14a^4 + 10a^3 - 12a^2 - 6a + 15) \end{array}$$

von $X^6 + 3X + 3 \in \mathbf{Q}(a, b, c, d)[X]$.

Wir gehen diesesmal nun nicht systematisch durch die Fälle, Subfälle etc., sondern suchen per Zufallsprinzip Erzeuger der Galoisgruppe, in der Hoffnung, daß das schneller geht.

Folgender Magma-Quelltext liefert das Resultat.

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^6 + 3*X + 3);
KK<a> := ext<Q | X^6 + 3*X + 3>;
```

```
RR<XX> := PolynomialRing(KK);
Factorisation(XX^6 + 3*XX + 3);
KKK<b> := ext<KK | XX^3 + 1/17*(-6*a^5 + 14*a^4 - 10*a^3 + 12*a^2 + 6*a - 15)*XX^2
          + 1/17*(-3*a^5 + 7*a^4 - 5*a^3 + 6*a^2 + 3*a - 33)*XX
          + 1/17*(3*a^5 - 7*a^4 + 5*a^3 - 6*a^2 - 3*a - 18)>;
RRR<XXX> := PolynomialRing(KKK);
KKKK<c> := ext<KKK | XXX^2 + 1/17*(6*a^5 - 14*a^4 + 10*a^3 - 12*a^2 + 11*a + 15)*XXX
           + 1/17*(-11*a^5 + 3*a^4 - 7*a^3 + 5*a^2 - 6*a - 36)>;
RRRR<XXXX> := PolynomialRing(KKKK);
Factorisation(XXXX^6 + 3*XXXX + 3);
KKKKK<d> := ext<KKKK | XXXX^2 + (b
            + 1/17*(-6*a^5 + 14*a^4 - 10*a^3 + 12*a^2 + 6*a - 15))*XXXX
            + b^2 + 1/17*(-6*a^5 + 14*a^4 - 10*a^3 + 12*a^2 + 6*a - 15)*b
            + 1/17*(-3*a^5 + 7*a^4 - 5*a^3 + 6*a^2 + 3*a - 33)>;
RRRRR<XXXXX> := PolynomialRing(KKKKK);
Factorisation(XXXXX^6 + 3*XXXXX + 3);
RBIG<Ga1,Ga2,Ga3,Ga4,Y> := PolynomialRing(Q,5);
Ga5 := -Ga3 - 1/17*(6*Ga1^5 - 14*Ga1^4 + 10*Ga1^3 - 12*Ga1^2 + 11*Ga1 + 15);
Ga6 := -Ga4 - Ga2 + 1/17*(6*Ga1^5 - 14*Ga1^4 + 10*Ga1^3 - 12*Ga1^2 - 6*Ga1 + 15);
ga1 := a;
ga2 := b;
ga3 := c;
ga4 := d;
ga5 := Evaluate(Ga5,[ga1,ga2,ga3,ga4,0]);
ga6 := Evaluate(Ga6,[ga1,ga2,ga3,ga4,0]);
(XXXXX-ga1)*(XXXXX-ga2)*(XXXXX-ga3)*(XXXXX-ga4)*(XXXXX-ga5)*(XXXXX-ga6); // zur Probe
muga1 := Y^6 + 3*Y + 3;
muga2 := Y^3 + 1/17*(-6*Ga1^5 + 14*Ga1^4 - 10*Ga1^3 + 12*Ga1^2 + 6*Ga1 - 15)*Y^2
         + 1/17*(-3*Ga1^5 + 7*Ga1^4 - 5*Ga1^3 + 6*Ga1^2 + 3*Ga1 - 33)*Y
         + 1/17*(3*Ga1^5 - 7*Ga1^4 + 5*Ga1^3 - 6*Ga1^2 - 3*Ga1 - 18);
muga3 := Y^2 + 1/17*(6*Ga1^5 - 14*Ga1^4 + 10*Ga1^3 - 12*Ga1^2 + 11*Ga1 + 15)*Y
         + 1/17*(-11*Ga1^5 + 3*Ga1^4 - 7*Ga1^3 + 5*Ga1^2 - 6*Ga1 - 36);
muga4 := Y^2 + (Ga2 + 1/17*(-6*Ga1^5 + 14*Ga1^4 - 10*Ga1^3 + 12*Ga1^2 + 6*Ga1 - 15))*Y
         + Ga2^2 + 1/17*(-6*Ga1^5 + 14*Ga1^4 - 10*Ga1^3 + 12*Ga1^2 + 6*Ga1 - 15)*Ga2
         + 1/17*(-3*Ga1^5 + 7*Ga1^4 - 5*Ga1^3 + 6*Ga1^2 + 3*Ga1 - 33);

muga1s:= Evaluate(muga1,[0,0,0,0,XXXXX]);
Factorisation(muga1s); // 123456 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga1,0,0,0,XXXXX]);
Factorisation(muga2s); // 246 (resultierende Nullstellennummern)
muga3s:= Evaluate(muga3,[ga1,ga2,0,0,XXXXX]);
Factorisation(muga3s); // 35
muga4s:= Evaluate(muga4,[ga1,ga2,ga5,0,XXXXX]);
Factorisation(muga4s); // 46
Evaluate(Ga5,[ga1,ga2,ga5,ga4,0]); // 3
Evaluate(Ga6,[ga1,ga2,ga5,ga4,0]); // 6 // (3,5)
Order(sub<SymmetricGroup(6) | (3,5)>);
// *** Zwischenstand: Ordnung = 2 ***
Evaluate(Ga5,[ga1,ga2,ga5,ga6,0]); // 3
Evaluate(Ga6,[ga1,ga2,ga5,ga6,0]); // 4 // (3,5)(4,6)
Order(sub<SymmetricGroup(6) | (3,5), (3,5)(4,6)>);
// Erzeugnis auch = <(3,5), (4,6)>
// *** Zwischenstand: Ordnung = 4 ***
```

```
muga1s:= Evaluate(muga1,[0,0,0,0,XXXXX]);
Factorisation(muga1s); // 123456
muga2s:= Evaluate(muga2,[ga1,0,0,0,XXXXX]);
Factorisation(muga2s); // 246
muga3s:= Evaluate(muga3,[ga1,ga4,0,0,XXXXX]);
Factorisation(muga3s); // 35
muga4s:= Evaluate(muga4,[ga1,ga4,ga5,0,XXXXX]);
Factorisation(muga4s); // 26
Evaluate(Ga5,[ga1,ga4,ga5,ga2,0]); // 3
Evaluate(Ga6,[ga1,ga4,ga5,ga2,0]); // 6 // (2,4)(3,5)
Order(sub<SymmetricGroup(6) | (3,5), (4,6), (2,4)(3,5)>);
// Erzeugnis auch = <(3,5),(4,6),(2,4)>
// *** Zwischenstand: Ordnung = 12 ***
muga1s:= Evaluate(muga1,[0,0,0,0,XXXXX]);
Factorisation(muga1s); // 123456 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga2,0,0,0,XXXXX]);
Factorisation(muga2s); // 135
muga3s:= Evaluate(muga3,[ga2,ga1,0,0,XXXXX]);
Factorisation(muga3s); // 46
muga4s:= Evaluate(muga4,[ga2,ga1,ga4,0,XXXXX]);
Factorisation(muga4s); // 35
Evaluate(Ga5,[ga2,ga1,ga4,ga3,0]); // 6
Evaluate(Ga6,[ga2,ga1,ga4,ga3,0]); // 5 // (1,2)(3,4)(5,6)
Order(sub<SymmetricGroup(6) | (3,5), (4,6), (2,4), (1,2)(3,4)(5,6)>);
// Erzeugnis auch = <(4,6), (2,4), (1,2)(3,4)(5,6)>
// *** Zwischenstand: Ordnung = 72 ***
```

Es ergibt sich $\mathrm{Gal}(X^6+3X+3) \xrightarrow{\sim} \langle (4,6),(2,4),(1,2)(3,4)(5,6)\rangle$;

(2) Was bislang geschah.

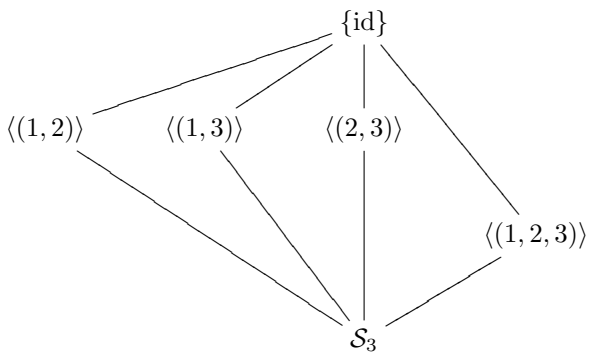
Gemäß Aufgabe 34.(1) ist der Zerfällungskörper von $X^3+X+1 \in \mathbf{Q}[X]$ gegeben durch $\mathbf{Q}(a,b)$ mit $a^3+a+1=0$ und $b^2+ab+a^2+1=0$. Insbesondere ist $[\mathbf{Q}(a,b):\mathbf{Q}]=6$, und $\mathbf{Q}(a,b)|\mathbf{Q}$ galoisch; cf. zweites Lemma in §3.5.1.4.

Seien $\gamma_1 := a$, $\gamma_2 = b$ und $\gamma_3 := -a-b$ die Nullstellen von X^3+X+1 in $\mathbf{Q}(a,b)$.

Nach §3.4.2.1 (resp. letzter Folgerung in §3.4.1) ist $\mathrm{Gal}(X^3+X+1) \xrightarrow{\sim} \mathcal{S}_3$. Wir identifizieren entlang diesem Isomorphismus.

Nach Satz 9 (Hauptsatz) entsprechen die gesuchten Zwischenkörper zwischen $\mathbf{Q}$ und $\mathbf{Q}(a,b)$ den Untergruppen von $\mathrm{Gal}(X^3+X+1) = \mathrm{Gal}(\mathbf{Q}(a,b)|\mathbf{Q}) = \mathcal{S}_3$.

In Aufgabe 38.(3) wurden die Untergruppen von $\mathcal{S}_3$ ermittelt wie im folgenden Diagramm angegeben. Hierbei sind Linien von oben nach unten als Inklusion zu lesen.



Die Korrespondenz weist nun einer Untergruppe U den Zwischenkörper $\mathrm{Fix}_U\, \mathbf{Q}(a,b)$ zu.

Es sind $\mathrm{Fix}_{\{\mathrm{id}\}}\,\mathbf{Q}(a,b) = \mathbf{Q}(a,b)$ und $\mathrm{Fix}_{\mathcal{S}_3}\,\mathbf{Q}(a,b) = \mathbf{Q}$; vgl. erste Bemerkung in §3.5.1.4.

In Aufgabe 41.(1) wurde eine $\mathbf{Q}$-Basis von $\mathrm{Fix}_{\langle(1,3)\rangle}\,\mathbf{Q}(a,b)$ zu $(1,\ b,\ a^2+ba+1)$ bestimmt. Da $-b^2 = ba + a^2 + 1$, folgt $\mathrm{Fix}_{\langle(1,3)\rangle}\,\mathbf{Q}(a,b) = \mathbf{Q}(b)$.

In Aufgabe 41.(2) wurde eine $\mathbf{Q}$-Basis von $\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b)$ zu $(1,\ -a+b+3a^2b)$ bestimmt. Es folgt $\mathrm{Fix}_{\langle(1,2,3)\rangle}\,\mathbf{Q}(a,b) = \mathbf{Q}(-a+b+3a^2b)$.

Wir setzen diese Berechnung nun fort.

Für $\langle(1,2)\rangle = \{\mathrm{id},\ (1,2)\}$ schicken die zugehörigen Automorphismen

$$\begin{array}{cccccc} a & \overset{\mathrm{id}}{\longmapsto} & a & a & \overset{(1,2)}{\longmapsto} & b \\ b & \longmapsto & b & b & \longmapsto & a\,. \end{array}$$

Wir erhalten folgendes $\mathbf{Q}$-Erzeugendensystem von $\mathrm{Fix}_{\langle(1,2)\rangle}\,\mathbf{Q}(a,b)$.

$$\begin{array}{ll} & \big(\mathrm{Tr}_{\langle(1,2)\rangle}(1),\ \mathrm{Tr}_{\langle(1,2)\rangle}(a),\ \mathrm{Tr}_{\langle(1,2)\rangle}(a^2),\ \mathrm{Tr}_{\langle(1,2)\rangle}(b),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba),\ \mathrm{Tr}_{\langle(1,3)\rangle}(ba^2)\big) \\ = & \big(1+1,\ a+b,\ a^2+b^2,\ b+a,\ ba+ab,\ ba^2+ab^2\big) \\ = & \big(2,\ a+b,\ -ba-1,\ a+b,\ 2ba,\ 1\big)\,. \end{array}$$

Dies reduziert sich z.B. zur $\mathbf{Q}$-Basis

$$\big(1,\ a+b,\ -ba-1\big)\,.$$

Da nun $(a+b)^2 = -ba-1$, wird $\mathrm{Fix}_{\langle(1,2)\rangle}\,\mathbf{Q}(a,b) = \mathbf{Q}(a+b)$.

Für $\langle(2,3)\rangle = \{\mathrm{id},\ (2,3)\}$ schicken die zugehörigen Automorphismen

$$\begin{array}{cccccc} a & \overset{\mathrm{id}}{\longmapsto} & a & a & \overset{(2,3)}{\longmapsto} & a \\ b & \longmapsto & b & b & \longmapsto & -a-b\,. \end{array}$$

Wir erhalten folgendes $\mathbf{Q}$-Erzeugendensystem von $\mathrm{Fix}_{\langle(2,3)\rangle}\,\mathbf{Q}(a,b)$.

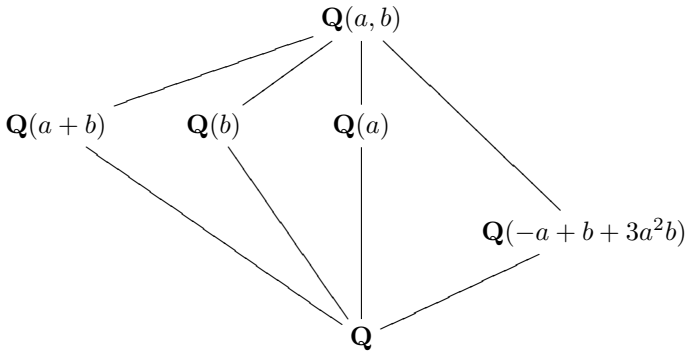
$$\begin{array}{ll} & \big(\mathrm{Tr}_{\langle(2,3)\rangle}(1),\ \mathrm{Tr}_{\langle(2,3)\rangle}(a),\ \mathrm{Tr}_{\langle(2,3)\rangle}(a^2),\ \mathrm{Tr}_{\langle(2,3)\rangle}(b),\ \mathrm{Tr}_{\langle(2,3)\rangle}(ba),\ \mathrm{Tr}_{\langle(2,3)\rangle}(ba^2)\big) \\ = & \big(1+1,\ a+a,\ a^2+a^2,\ b+(-a-b),\ ba+(-a-b)a,\ ba^2+(-a-b)a^2\big) \\ = & \big(2,\ 2a,\ 2a^2,\ -a,\ -a^2,\ a+1\big) \end{array}$$

Dies reduziert sich z.B. zur $\mathbf{Q}$-Basis

$$\big(1,\ a,\ a^2\big)\,.$$

Also wird $\mathrm{Fix}_{\langle(2,3)\rangle}\,\mathbf{Q}(a,b) = \mathbf{Q}(a)$.

Wir tragen in das den Untergruppen entsprechende Körperdiagramm die Fixkörper ein. Hierbei sind Linien von unten nach oben als Inklusion zu lesen.



Aufgabe 47

(1) Mit dem zweiten Lemma aus §3.5.1.4 ist E der Zerfällungskörper eines normierten Polynoms $g(X) \in K[X]$, das dort in verschiedene normierte irreduzible Faktoren zerfällt. In $E[X]$ zerfällt $g(X)$ in verschiedene Linearfaktoren; vgl. die zweite Bemerkung in §3.4.1. Also zerfällt $g(X)$ auch in $L[X]$ in verschiedene normierte irreduzible Faktoren. Nun ist E auch Zerfällungskörper von $g(X)$ über L; vgl. zweite Bemerkung aus §2.5.1. Also ist $E|L$ galoisch; vgl. Aufgabe 45.(1) und zweites Lemma aus §3.5.1.4.

(2) Sei $q = p^r$ für p prim und $r \geqslant 1$. Nach dem Lemma aus §2.5.4 ist $\mathbf{F}_{q^s}$ Zerfällungskörper von $X^{q^s} - X$ über $\mathbf{F}_p$. Im Beweis zu loc. cit., Teil (1), wurde auch gezeigt, daß $X^{q^s} - X$ in $\mathbf{F}_{q^s}[X]$ in verschiedene Linearfaktoren zerfällt. Also zerfällt $X^{q^s} - X$ in $\mathbf{F}_q[X]$ in verschiedene irreduzible Faktoren. Nun ist $\mathbf{F}_{q^s}$ auch Zerfällungskörper von $X^{q^s} - X$ über $\mathbf{F}_q$; vgl. zweite Bemerkung aus §2.5.1. Also ist $\mathbf{F}_{q^s}|\mathbf{F}_q$ galoisch.

Aufgabe 48

(1) Zunächst zeigen wir, daß für $a \in \mathbf{Z}$ genau dann $g^a = 1$ ist, wenn $\mathrm{o}(g) = n$ ein Teiler von a ist. Ist $a \equiv_n 0$, so ist $g^a = 1$. Ist umgekehrt $g^a = 1$, so schreibe $a = nq + r$ mit $q \in \mathbf{Z}$ und $r \in [0, n-1]$. Dann folgt $g^r = g^{nq} g^r = g^a = 1$, und also, wegen der Minimalität von $\mathrm{o}(g)$, $r = 0$; vgl. Aufgabe 11.

Sei $U \leqslant G$. Sei $e := |G|/|U| = n/|U|$; vgl. Aufgabe 38.(1.c). Wir wollen zeigen, daß $U = \langle g^e \rangle$.

Ist $g^i \in U$, so ist $(g^i)^{|U|} = 1$ mit Aufgabe 11.(1.c), und also $i|U|$ ein Vielfaches von $n = e|U|$. Somit ist i Vielfaches von e, und also $g^i \in \langle g^e \rangle$. Insgesamt ist $U \leqslant \langle g^e \rangle$.

Ferner ist $\mathrm{o}(g^e) = |U|$; vgl. Aufgabe 27.(2). Also ist $|U| = |\langle g^e \rangle|$; vgl. Aufgabe 11.(1.b). Es folgt $U = \langle g^e \rangle$.

(2) Schreibe $\mathrm{Frob} := \mathrm{Frob}_{\mathbf{F}_{p^s}}$. Es ist $\mathrm{Gal}(\mathbf{F}_{p^s}|\mathbf{F}_p) = \langle \mathrm{Frob} \rangle$ von Ordnung s; vgl. §3.6.

Sei d ein Teiler von s. Sei $K := \mathrm{Fix}_{\langle \mathrm{Frob}^d \rangle} \mathbf{F}_{p^s}$. Es ist $\mathrm{Gal}(\mathbf{F}_{p^s}|K) = \langle \mathrm{Frob}^d \rangle$ von Ordnung s/d; vgl. Satz 8.(2) aus §3.5.1.3 und Aufgabe 27.(2). Also ist $[K : \mathbf{F}_p] = d$, insbesondere also $K \simeq \mathbf{F}_{p^d}$.

Auf diese Weise erhält man alle Zwischenkörper, da jede Untergruppe von $\langle \mathrm{Frob} \rangle$ nach (1) von der Form $\langle \mathrm{Frob}^d \rangle$ ist für einen Teiler d von s, und da nach Satz 9 (Hauptsatz der Galoistheorie) aus §3.5.2 jeder Körper zwischen $\mathbf{F}_{p^s}$ und $\mathbf{F}_p$ Fixkörper einer Untergruppe von $\langle \mathrm{Frob} \rangle$ in $\mathbf{F}_{p^s}$ ist.

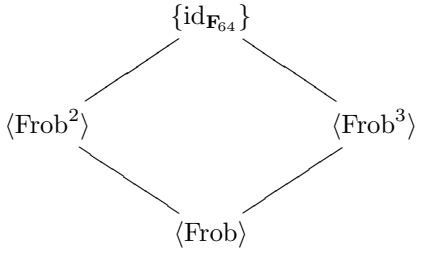
(3) Es ist $X^6 + X + 1 \in \mathbf{F}_2[X]$ irreduzibel. Also können wir $\mathbf{F}_{64} = \mathbf{F}_2(\varepsilon)$ mit $\varepsilon^6 = \varepsilon + 1$ konstruieren. Dies kann z.B. mittels

```
F := GF(2);
R<X> := PolynomialRing(F);
Factorisation(X^6 + X + 1);
FF<e> := ext<F | X^6 + X + 1>;
```

in Magma geschehen.

Es ist $\mathrm{Gal}(\mathbf{F}_{64}|\mathbf{F}_2) = \langle \mathrm{Frob}_{\mathbf{F}_{64}} \rangle$ von Ordnung 6. Schreibe kurz $\mathrm{Frob} := \mathrm{Frob}_{\mathbf{F}_{64}}$.

Gemäß (1) sind die Untergruppen von $\langle \mathrm{Frob} \rangle$ gegeben durch



wobei $|\langle \mathrm{Frob}^2 \rangle| = 3$ und $\langle \mathrm{Frob}^3 \rangle| = 2$.

Sicher ist $\mathrm{Fix}_{\{\mathrm{id}_{\mathbf{F}_{64}}\}} \mathbf{F}_{64} = \mathbf{F}_{64} = \mathbf{F}_2(\varepsilon)$ und $\mathrm{Fix}_{\langle \mathrm{Frob} \rangle} \mathbf{F}_{64} = \mathbf{F}_2$; vgl. erste Bemerkung in §3.5.1.4.

Wir berechnen $\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64}$. Eine $\mathbf{F}_2$-Basis von $\mathbf{F}_{64}$ ist gegeben durch $(1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5)$. Da $\mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}$ eine surjektive $\mathbf{F}_2$-lineare Abbildung von $\mathbf{F}_{64}$ nach $\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64}$ ist, wird unter dieser Abbildung diese Basis auf ein $\mathbf{F}_2$-Erzeugendensystem abgebildet; vgl. §3.5.1.2.

Allgemein ist $\mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(x) = x + x^4 + x^{16}$ für $x \in \mathbf{F}_{64}$.

Somit wird

$$\begin{array}{ll} & \big(\mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(1),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^2),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^3),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^4)),\ \mathrm{Tr}_{\langle \mathrm{Frob}^2 \rangle}(\varepsilon^5)\big) \\ = & \big(1+1+1,\ \varepsilon+\varepsilon^4+\varepsilon^{16},\ \varepsilon^2+\varepsilon^8+\varepsilon^{32},\ \varepsilon^3+\varepsilon^{12}+\varepsilon^{48},\ \varepsilon^4+\varepsilon^{16}+\varepsilon,\ \varepsilon^5+\varepsilon^{20}+\varepsilon^{17}\big) \\ = & \big(1,\ 1,\ 1,\ 0,\ 1,\ \varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^5\big) \end{array}$$

Also ist eine $\mathbf{F}_2$-Basis von $\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64}$ gegeben durch $(1,\ \varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^5)$. Somit ist

$$\mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64} \ = \ \mathbf{F}_2(\varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^5)\ .$$

In der Tat ist $\mu_{\varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^5, \mathbf{F}_2}(X) = X^2 + X + 1$, womit wir mit Satz 3 (Morphismen induziert von Nullstellen) einen Isomorphismus

$$\begin{array}{ccc} \mathbf{F}_4 & \xrightarrow{\sim} & \mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64} \\ \alpha & \longmapsto & \varepsilon+\varepsilon^3+\varepsilon^4+\varepsilon^5 \end{array}$$

bekommen, unter Verwendung unserer Standardnotation.

Wir berechnen $\mathrm{Fix}_{\langle \mathrm{Frob}^3 \rangle} \mathbf{F}_{64}$. Eine $\mathbf{F}_2$-Basis von $\mathbf{F}_{64}$ ist gegeben durch $(1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5)$.

Allgemein ist $\mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(x) = x + x^8$ für $x \in \mathbf{F}_{64}$.

Somit wird

$$\begin{array}{ll} & \big(\mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(1),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^2),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^3),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^4)),\ \mathrm{Tr}_{\langle \mathrm{Frob}^3 \rangle}(\varepsilon^5)\big) \\ = & \big(1+1,\ \varepsilon+\varepsilon^8,\ \varepsilon^2+\varepsilon^{16},\ \varepsilon^3+\varepsilon^{24},\ \varepsilon^4+\varepsilon^{32},\ \varepsilon^5+\varepsilon^{40}\big) \\ = & \big(0,\ \varepsilon+\varepsilon^2+\varepsilon^3,\ 1+\varepsilon+\varepsilon^2+\varepsilon^4,\ 1+\varepsilon^3+\varepsilon^4,\ 1+\varepsilon^3+\varepsilon^4,\ 1+\varepsilon+\varepsilon^2+\varepsilon^3\big) \end{array}$$

Also ist eine $\mathbf{F}_2$-Basis von $\mathrm{Fix}_{\langle \mathrm{Frob}^3 \rangle} \mathbf{F}_{64}$ gegeben durch $(1,\ \varepsilon+\varepsilon^2+\varepsilon^3,\ \varepsilon^3+\varepsilon^4,\ )$. Beachte, daß

$$(\varepsilon+\varepsilon^2+\varepsilon^3)^2 \ = \ 1 + (\varepsilon+\varepsilon^2+\varepsilon^3) + (\varepsilon^3+\varepsilon^4)\ .$$

Somit ist

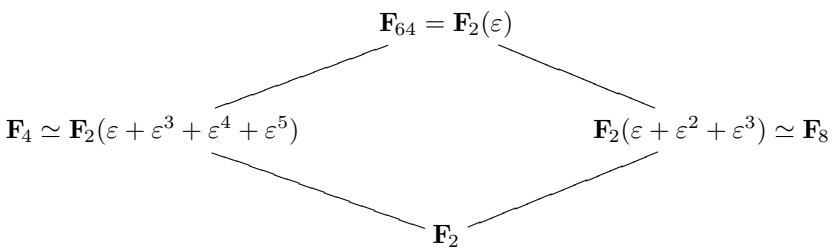
$$\mathrm{Fix}_{\langle \mathrm{Frob}^3 \rangle} \mathbf{F}_{64} \ = \ \mathbf{F}_2(\varepsilon+\varepsilon^2+\varepsilon^3)\ .$$

In der Tat ist $\mu_{\varepsilon+\varepsilon^2+\varepsilon^3, \mathbf{F}_2}(X) = X^3 + X + 1$, womit wir mit Satz 3 (Morphismen induziert von Nullstellen) einen Isomorphismus

$$\begin{array}{ccc} \mathbf{F}_8 & \xrightarrow{\sim} & \mathrm{Fix}_{\langle \mathrm{Frob}^2 \rangle} \mathbf{F}_{64} \\ \beta & \longmapsto & \varepsilon+\varepsilon^2+\varepsilon^3 \end{array}$$

bekommen, unter Verwendung unserer Standardnotation.

Alle Zwischenkörper in ein dem obigen Untergruppendiagramm entsprechendes Diagramm eingetragen, erhalten wir also folgendes.



Aufgabe 49

(1) Es sind $\mathcal{S}_1 = \{\mathrm{id}\}$ und $\mathcal{S}_2 = \langle(1,2)\rangle$ abelsch und somit auflösbar.

Die Auflösbarkeit von $\mathcal{S}_3$ wurde im ersten Beispiel in §4.1 eingesehen.

Wir zeigen die Auflösbarkeit von $\mathcal{S}_4$. Es ist $N := \langle(1,2)(3,4),\ (1,3)(2,4)\rangle$ ein abelscher Normalteiler von $\mathcal{S}_4$, vgl. Bemerkung zur Vorsicht in §4.1.

Sei $A := \langle(1,2)(3,4),\ (1,3)(2,4),\ (1,2,3)\rangle$ ([53]). Laut Magma ist $|A| = 12$.

Sei allgemein G eine endliche Gruppe, und sei $H \leqslant G$ mit $2|H| = |G|$. Wir *behaupten,* daß $H \trianglelefteq G$.

Sei $g \in G$. Zu zeigen ist, daß ${}^gH = gHg^{-1} \stackrel{!}{=} H$, i.e. daß $gH \stackrel{!}{=} Hg$.

Wir bemerken, daß $G = H \sqcup xH = H \sqcup Hx$ für jedes $x \in G \smallsetminus H$; vgl. Aufgabe 38.(1). Insbesondere ist $xH = G \smallsetminus H = Hx$.

Ist nun $g \in H$, so ist $gH = H = Hg$. Ist $g \notin H$, so ist $gH = G \smallsetminus H = Hg$ mit der eben gemachten Bemerkung. Dies zeigt die *Behauptung.*

Insbesondere ist $A \trianglelefteq \mathcal{S}_4$. Da $N \trianglelefteq \mathcal{S}_4$, ist auch $N \trianglelefteq A$. Insgesamt also

$$\{\mathrm{id}\} \ \trianglelefteq\ N \ \trianglelefteq\ A \ \trianglelefteq\ \mathcal{S}_4\ .$$

Wie schon festgestellt, ist $N/\{\mathrm{id}\} \simeq N$ abelsch.

Eine Gruppe von Primzahlordnung p ist zyklisch, und also auch abelsch. Denn ein Element darin hat Ordnung 1 oder p; vgl. Aufgabe 11.(1.c). Also hat jedes Element $\neq 1$ darin Ordnung p, und erzeugt daher die Gruppe; vgl. Aufgabe 11.(1.b).

Somit ist A/N zyklisch wegen $|A/N| = |A|/|N| = 3$ prim; vgl. Lösung zu Aufgabe 38.(1).

Ferner ist $\mathcal{S}_4/A$ zyklisch wegen $|\mathcal{S}_4/A| = |\mathcal{S}_4|/|A| = 2$ prim; vgl. Lösung zu Aufgabe 38.(1).

Insgesamt ist $\mathcal{S}_4$ als auflösbar nachgewiesen.

(2) Sei, dem Hinweis folgend, $M \trianglelefteq N \leqslant \mathcal{S}_n$ mit N/M abelsch gegeben. Wir *behaupten,* daß wenn N alle Zykel der Länge 3 enthält, so auch M.

Seien $x,\ y \in N$. Da N/M abelsch ist, wird

$$\begin{aligned}(xyx^{-1}y^{-1})M &= (xM)(yM)(xM)^{-1}(yM)^{-1}\\ &= (xM)(xM)^{-1}(yM)(yM)^{-1}\\ &= ((xx^{-1})M)((yy^{-1})M)\\ &= 1\cdot M\ ,\end{aligned}$$

und also $xyx^{-1}y^{-1} \in M$.

Sei (a,b,c) ein beliebiger Zykel von Länge 3 aus $\mathcal{S}_n$. Sei $\{a,b,c,d,e\} \subseteq [1,n]$ mit $|\{a,b,c,d,e\}| = 5$. Dies ist möglich, da $n \geqslant 5$.

Nach Voraussetzung sind (a,b,d) und (a,c,e) in N. Mit der eben gemachten Bemerkung wird

$$M\ \ni\ (a,b,d)\circ(a,c,e)\circ(a,b,d)^{-1}\circ(a,c,e)^{-1}\ =\ (a,b,c)\ .$$

Somit enthält auch M jeden Zykel von Länge 3 aus $\mathcal{S}_n$.

Sei nun *angenommen,* es ist $\mathcal{S}_n$ auflösbar. Sei

$$\{\mathrm{id}\}\ =\ G_0\ \trianglelefteq\ G_1\ \trianglelefteq\ \cdots\ \trianglelefteq\ G_k\ =\ \mathcal{S}_n$$

eine Subnormalreihe mit allen Subfaktoren abelsch. Es enthält G_k alle Zykel der Länge 3 aus $\mathcal{S}_n$. Da nun mit G_i auch G_{i-1} jeweils alle Zykel der Länge 3 aus $\mathcal{S}_n$ enthält, folgt mit absteigender Induktion, daß dies auch für $G_0 = \{\mathrm{id}\}$ zutrifft. Dies ist ein *Widerspruch.*

Also existiert in $\mathcal{S}_n$ keine Subnormalreihe mit allen Subfaktoren abelsch. D.h. $\mathcal{S}_n$ ist nicht auflösbar.

[53] Es ist $A = \mathcal{A}_4$ der Kern der Signumsabbildung $\mathcal{S}_4 \longrightarrow \{\pm 1\}$.

Aufgabe 50

Sei $\hat{f}(X) \in K[X]$ das Produkt über die Menge der irreduziblen normierten Faktoren von $f(X) \in K[X]$. Es ist L auch ein Zerfällungskörper von $\hat{f}(X)$ über K, da mit $f(X)$ auch sein Teiler $\hat{f}(X)$ in $L[X]$ in Linearfaktoren zerfällt, und da jede Nullstelle von $f(X)$ in L auch eine Nullstelle von $\hat{f}(X)$ ist, und somit die Nullstellen des letzteren ebenfalls L über K erzeugen.

Es folgt $(\deg f)! = n! = [L : K] \leqslant (\deg \hat{f})! \leqslant (\deg f)!$, also $(\deg \hat{f})! = (\deg f)!$, also $\deg \hat{f} = \deg f$ und also $\hat{f}(X) = f(X)$; vgl. Satz 4 aus §2.5.2.

In anderen Worten, $f(X) \in K[X]$ zerfällt in ein Produkt verschiedener normierter irreduzibler Faktoren.

Somit können wir die letzte Folgerung aus §3.4.1 anwenden, und stellen fest, daß $\mathrm{Gal}(f(X)) \xrightarrow{\sim} \mathcal{S}_n$. In anderen Worten, für jede Permutation der Nullstellen von $f(X)$ in L gibt es einen Automorphismus von $L|K$, der zu dieser Permutation einschränkt.

Sei nun *angenommen,* es ist $f(X) = u(X)v(X)$ mit $u(X), v(X) \in K[X]$ normiert und mit $\deg u, \deg v \geqslant 1$. Dann gibt es ein $y \in L$ mit $u(y) = 0$ und ein $z \in L$ mit $v(z) = 0$. Da y und z insbesondere beides Nullstellen von $f(X)$ in L sind, gibt es nach dem eben Gesagten ein $\sigma \in \mathrm{Aut}(L|K)$ mit $\sigma(y) = z$. Also ist $u(z) = u(\sigma(y)) = \sigma(u(y)) = \sigma(0) = 0$ und $v(z) = 0$. Somit ist $\mu_{z,K}(X)$ ein Teiler von $u(X)$ und von $v(X)$; vgl. Satz 2 aus §2.3.2. Also ist $\mu_{z,K}(X)^2$ ein Teiler von $f(X)$, und wir haben einen *Widerspruch.*

Ein alternatives Argument. Die Konstruktion des Zerfällungskörpers liefert nur dann eine Erweiterung von Grad $n!$, wenn im i-ten Schritt eine Erweiterung von Grad $n - i + 1$ vorgenommen wird, wobei $i \in [1, n]$, denn ansonsten resultiert ein echt kleinerer Grad. Zerfällt nun $f(X)$ in zwei Faktoren von Grad $\geqslant 1$, so ist schon im ersten Schritt keine Erweiterung um Grad n mehr möglich.

Aufgabe 51

(1) Der Zerfällungskörper von $X^5 + 5X^2 + 3 \in \mathbf{Q}[X]$ ergibt sich mittels Magma zu $\mathbf{Q}(a, b)$ mit

$$\begin{aligned} 0 &= a^5 + 5a^2 + 3 \\ 0 &= b^2 - \tfrac{1}{3}(a^4 + a^3 + a^2 + 3a + 3)b - (a - 1)\ . \end{aligned}$$

Insbesondere ist $[\mathbf{Q}(a, b) : \mathbf{Q}] = 10$, und somit auch $|\mathrm{Gal}(X^5 + 5X^2 + 3)| = 10$.
Wir berechnen $\mathrm{Gal}(X^5 + 5X^2 + 3) = \langle (2, 3)(4, 5), (1, 2, 4, 5, 3) \rangle$. Der zugehörige Magma-Quelltext:

```
Q := Rationals();
R<X> := PolynomialRing(Q);
Factorisation(X^5 + 5*X^2 + 3);
KK<a> := ext<Q | X^5 + 5*X^2 + 3>;
RR<XX> := PolynomialRing(KK);
Factorisation(XX^5 + 5*XX^2 + 3);
KKK<b> := ext<KK | XX^2 + 1/3*(-a^4 - a^3 - a^2 - 3*a - 3)*XX - a + 1>;
RRR<XXX> := PolynomialRing(KKK);
Factorisation(XXX^5 + 5*XXX^2 + 3);
RBIG<Ga1,Ga2,Y> := PolynomialRing(Q,3);
Ga3 := -Ga2 + 1/3*(Ga1^4 + Ga1^3 + Ga1^2 + 3*Ga1 + 3);
Ga4 := 1/3*(Ga1^4 + 5*Ga1)*Ga2 - 1/3*(Ga1^4 + 5*Ga1);
Ga5 := -1/3*(Ga1^4 + 5*Ga1)*Ga2 - 1/3*(Ga1^3 + Ga1^2 + Ga1 + 3);
ga1 := a;
ga2 := b;
ga3 := Evaluate(Ga3,[ga1,ga2,0]);;
ga4 := Evaluate(Ga4,[ga1,ga2,0]);;
ga5 := Evaluate(Ga5,[ga1,ga2,0]);;
```

```
(XXX-ga1)*(XXX-ga2)*(XXX-ga3)*(XXX-ga4)*(XXX-ga5); // zur Probe
muga1 := Y^5 + 5*Y^2 + 3;
muga2 := Y^2 - 1/3*(Ga1^4 + Ga1^3 + Ga1^2 + 3*Ga1 + 3)*Y - (Ga1 - 1);

muga1s:= Evaluate(muga1,[0,0,XXX]);
Factorisation(muga1s); // 12345 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga1,0,XXX]);
Factorisation(muga2s); // 23 (resultierende Nullstellennummern)
Evaluate(Ga3,[ga1,ga3,0]); // 2
Evaluate(Ga4,[ga1,ga3,0]); // 5
Evaluate(Ga5,[ga1,ga3,0]); // 4 // (2,3)(4,5)
Order(sub<SymmetricGroup(5) | (2,3)(4,5)>);
// *** Zwischenstand: Ordnung = 2 ***
muga1s:= Evaluate(muga1,[0,0,XXX]);
Factorisation(muga1s); // 12345 (resultierende Nullstellennummern)
muga2s:= Evaluate(muga2,[ga2,0,XXX]);
Factorisation(muga2s); // 14 (resultierende Nullstellennummern)
Evaluate(Ga3,[ga2,ga4,0]); // 1
Evaluate(Ga4,[ga2,ga4,0]); // 5
Evaluate(Ga5,[ga2,ga4,0]); // 3 // (1,2,4,5,3)
Order(sub<SymmetricGroup(5) | (2,3)(4,5), (1,2,4,5,3)>);
// *** Zwischenstand: Ordnung = 10 ***
```

Sei $G := \mathrm{Gal}(X^5 + 5X^2 + 3) = \langle (2,3)(4,5), (1,2,4,5,3) \rangle$. Sei $N := \langle (1,2,4,5,3) \rangle \leqslant G$.

Da $|G| = 2|N|$, ist $N \trianglelefteqslant G$; vgl. Argument in der Lösung zu Aufgabe 49.(1). Betrachte die Subnormalreihe

$$\{\mathrm{id}\} \trianglelefteqslant N \trianglelefteqslant G\,.$$

Da die Subfaktoren beide von primer Ordnung sind, namentlich 5 und 2, sind beide Subfaktoren zyklisch, insbesondere abelsch; vgl. Argument in der Lösung zu Aufgabe 49.(1)

Somit ist G auflösbar. Mit dem Satz 10 von Galois aus §4.4.2 ist mithin $X^5 + 5X^2 + 3 \in \mathbf{Q}[X]$ auflösbar.

(2) Der Zerfällungskörper von $X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$ ergibt sich mittels Magma in der üblichen Weise zu $\mathbf{Q}(a,b,c,d)$ mit

$$\begin{aligned} 0 &= a^5 + 5a^2 + 2 \\ 0 &= b^4 + ab^3 + a^2b^2 + (a^3+5)b + (a^4+5a) \\ 0 &= c^3 + (b+a)c^2 + (b^2+ab+a^2)c + (b^3+ab^2+a^2b+(a^3+5)) \\ 0 &= d^2 + (c+(b+a))d + (c^2+(b+a)c+(b^2+ab+a^2))\,. \end{aligned}$$

Insbesondere ist $[\mathbf{Q}(a,b,c,d) : \mathbf{Q}] = 5 \cdot 4 \cdot 3 \cdot 2 = 5!$, und somit $\mathrm{Gal}(X^5 + 5X^2 + 2) = \mathcal{S}_5$; vgl. letzte Folgerung in §3.4.1.

Ferner hat sich im Verlauf dieser Rechnung $X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$ als irreduzibel herausgestellt, was auch mit Aufgabe 50 im nachhinein nochmals bestätigt wird.

Dank Aufgabe 49.(2) ist $\mathcal{S}_5$ nicht auflösbar. Mit dem Satz 10 von Galois aus §4.4.2 ist mithin $X^5 + 5X^2 + 2 \in \mathbf{Q}[X]$ nicht auflösbar.

Aufgabe 52

(1) Sei $\rho \in G$. Sei $x \in L$. Es ist $\rho(\mathrm{N}_G(x)) = \rho(\prod_{\sigma\in G}\sigma(x)) = \prod_{\sigma\in G}(\rho\circ\sigma)(x) = \prod_{\tau\in G}\tau(x) = \mathrm{N}_G(x)$, wobei $\tau := \rho\circ\sigma$ substituiert wurde. Also ist $\mathrm{N}_G(x) \in \mathrm{Fix}_G(L) = K$; vgl. erste Bemerkung in §3.5.1.4.

(2) Hier ist $G = \langle F \rangle = \{ F^i : i \in [0, s-1] \}$, wobei $F(x) = x^q$ für $x \in \mathbf{F}_{q^s}$; vgl. §3.6.
Für $x \in \mathbf{F}_{q^s}$ ist also

$$\mathrm{N}_G(x) \;=\; \prod_{i \in [0,s-1]} F^i(x) \;=\; x^{q^0+q^1+\cdots+q^{s-1}} \;=\; x^{(q^s-1)/(q-1)} \,.$$

Da $\mathrm{N}_G(0) = 0$ und $\mathrm{N}_G(\mathbf{F}_{q^s}^\times) \subseteq \mathbf{F}_q^\times$, genügt es zu zeigen, daß $N := \mathrm{N}_G|_{\mathbf{F}_{q^s}^\times}^{\mathbf{F}_q^\times}$ surjektiv ist.

Sei $y \in \mathbf{F}_{q^s}^\times$ ein Erzeuger dieser zyklischen Gruppe, d.h. $\mathbf{F}_{q^s}^\times = \langle y \rangle$; vgl. Aufgabe 27.(5). Mithin ist $\mathrm{o}(y) = |\mathbf{F}_{q^s}^\times| = q^s - 1$. Es ist

$$|\langle \mathrm{N}_G(y) \rangle| \;=\; \mathrm{o}(\mathrm{N}_G(y)) \;=\; \mathrm{o}(y^{(q^s-1)/(q-1)}) \;=\; \mathrm{o}(y^{\mathrm{o}(y)/(q-1)}) \;=\; q-1 \,;$$

vgl. Aufgabe 27.(2). Da $|\mathbf{F}_q^\times| = q-1$ ist, folgt $\langle \mathrm{N}_G(y) \rangle = \mathbf{F}_q^\times$. Also ist jedes Element von $\mathbf{F}_q^\times$ von der Form $\mathrm{N}_G(y)^k = \mathrm{N}_G(y^k)$ für ein $k \in \mathbf{Z}$, weswegen N_G surjektiv ist.

Aufgabe 53 ([54])

O.E. ist $U_i \not\subseteq \bigcup_{j \in [1,m] \smallsetminus \{i\}} U_j$ für $i \in [1,m]$, da ansonsten U_i weggelassen werden kann, ohne die Vereinigungsmenge zu ändern.

O.E. ist $m \geqslant 2$.

Es genügt zu zeigen, daß $\bigcup_{i \in [1,m]} U_i$ kein Vektorraum ist. *Annahme,* doch.

Wähle $\alpha_k \in K \smallsetminus \{0\}$ für $k \in [1, m-1]$ mit $|\{ \alpha_k : k \in [1, m-1] \}| = m-1$. Dies ist möglich, da $|K| \geqslant m$.

Wähle $u_1 \in U_1 \smallsetminus \bigcup_{j \in [1,m] \smallsetminus \{1\}} U_j$. Wähle $u_2 \in U_2 \smallsetminus \bigcup_{j \in [1,m] \smallsetminus \{2\}} U_j$.

Sei $k \in [1, m-1]$. Es ist $u_1 + \alpha_k u_2 \in \bigcup_{i \in [1,m]} U_i$. Es ist $u_1 + \alpha_k u_2 \notin U_1$, denn sonst wäre auch $u_2 \in U_1$. Es ist $u_1 + \alpha_k u_2 \notin U_2$, denn sonst wäre auch $u_1 \in U_2$. Also ist $u_1 + \alpha_k u_2 \in \bigcup_{i \in [3,m]} U_i$.

Da $u_2 \neq 0$, ist $|\{ u_1 + \alpha_k u_2 : k \in [1, m-1] \}| = m-1$. Folglich gibt es $j \in [3,m]$ und $s, t \in [1, m-1]$ mit $s \neq t$, aber $u_1 + \alpha_s u_2 \in U_j$ und $u_1 + \alpha_t u_2 \in U_j$. Die Differenz liefert $u_2 \in U_j$, im *Widerspruch* zur Wahl von u_2 .

Aufgabe 54

Schreibe $n := [L : K]$.

Fall K endlich. Dann ist $|L| = |K|^n$. Also gibt es ein $t \in L^\times$ mit $\mathrm{o}(t) = |L|$; cf. Aufgabe 27.(5). Da zudem $0 \in K$ liegt, ist folglich $L = K(t)$.

Fall K unendlich. Sei $(y_1, \ldots, y_n)$ eine K-lineare Basis von L. Dann ist $L = K(y_1, \ldots, y_n)$; cf. §2.3.3. Sei $f(X) := \prod_{i \in [1,n]} \mu_{y_i,K}(X) \in K[X] \subseteq L[X]$. Sei M ein Zerfällungskörper von $f(X) \in L[X]$; cf. Satz 4.

Sei $k := \deg f$. Sei $f(X) = \prod_{i \in [1,k]} (X - \gamma_i) \in M$ mit $\gamma_i \in M$, wobei $\gamma_i = y_i$ für $i \in [1,n]$. Es wird

$$M \;=\; L(\gamma_1, \ldots, \gamma_k) \;=\; K(y_1, \ldots, y_n, \gamma_1, \ldots, \gamma_n) \;=\; K(\gamma_1, \ldots, , \gamma_n) \,.$$

Also ist M auch ein Zerfällungskörper von $f(X) \in K[X]$; cf. §2.5.1. Folglich liegen Körpererweiterungen $M|L|K$ vor mit $M|K$ galoisch; cf. §3.5.1.4. Schreibe $G := \mathrm{Gal}(M|K)$. Es ist $|G| = [M : K]$ endlich; cf. Sätze 4, 5, §3.5.1.4.

Da G endlich viele Untergruppen hat, ist die Menge der Zwischenkörper zwischen K und M nach Hauptsatz endlich; cf. Satz 9. Insbesondere ist

$$\mathcal{E} \;:=\; \{ E : L|E|K \text{ und } E \subset L \}$$

[54] Diese Lösung kenne ich von Fabian Dyga.

endlich. Wähle $t \in L \smallsetminus \bigcup_{E\in\mathcal{E}} E$; cf. Aufgabe 53. Dann ist $L|K(t)|K$, aber $K(t) \notin \mathcal{E}$, da *ansonsten* $t \in K(t) \in \bigcup_{E\in\mathcal{E}} E$ läge, was es nach Wahl von t *nicht* tut. Folglich ist $K(t) = L$.

Aufgabe 55

Vorbemerkung. Jedes $x \in \mathbf{Q}^\times$ können wir bis auf Vorzeichen in Primfaktoren zerlegen,

$$x \;=\; \varepsilon \prod_{p>0 \text{ prim}} p^{\alpha_p} \;,$$

wobei $\varepsilon \in \{-1,+1\}$ und wobei $\alpha_p \in \mathbf{Z}$ stets, mit $\alpha_p \neq 0$ nur für endlich viele Primzahlen p. Dies kann e.g. durch Primfaktorzerlegung des Nenners und des Zählers von x erreicht werden. Schreibe

$$\mathrm{v}_p(x) \;:=\; \alpha_p \;.$$

Wir setzen noch $\mathrm{v}_p(0) := +\infty$.

Für $x, y \in \mathbf{Q}$ mit $\mathrm{v}_p(x) < \mathrm{v}_p(y)$ ist $\mathrm{v}_p(x+y) = \mathrm{v}_p(x)$. Denn da $xp^{-\mathrm{v}_p(x)} = \frac{a}{z}$ mit $a, z \in \mathbf{Z} \smallsetminus p\mathbf{Z}$ geschrieben werden kann und $yp^{-\mathrm{v}_p(x)} = \frac{pb}{w}$ mit $b \in \mathbf{Z}$ und $w \in \mathbf{Z} \smallsetminus p\mathbf{Z}$, ist $(x+y)p^{-\mathrm{v}_p(x)} = \frac{aw+pbz}{zw}$ mit $aw + pbz,\, zw \in \mathbf{Z} \smallsetminus p\mathbf{Z}$.

(1) Schreibe $g(X) = \sum_{i\geqslant 0} b_i X^i$ und $h(X) = \sum_{i\geqslant 0} \tilde{b}_i X^i$. Seien $k := \deg g$ und $\tilde{k} := \deg h$.
Annahme, es ist $g(X) \in \mathbf{Q}[X] \smallsetminus \mathbf{Z}[X]$. Dann können wir eine Primzahl $p > 0$ mit

$$v \;:=\; \min\{\, \mathrm{v}_p(b_i) \,:\, i \in [0,k] \,\} \;<\; 0$$

wählen. Sei $j := \min\{\, i \in [0,k-1] \,:\, \mathrm{v}_p(b_i) = v \,\}$. Sei

$$\tilde{v} \;:=\; \min\{\, \mathrm{v}_p(\tilde{b}_i) \,:\, i \in [0,\tilde{k}] \,\} \;\leqslant\; 0 \;.$$

Sei $\tilde{j} := \min\{\, i \in [0,\tilde{k}-1] \,:\, \mathrm{v}_p(\tilde{b}_i) = \tilde{v} \,\}$.
Es ist $a_{j+\tilde{j}} = \sum_{i\in[0,j+\tilde{j}]} b_i \tilde{b}_{j+\tilde{j}-i}$. Da $\mathrm{v}_p(b_j\tilde{b}_{\tilde{j}}) < \mathrm{v}_p(b_i\tilde{b}_{j+\tilde{j}-i})$ für $i \in [0, j+\tilde{j}] \smallsetminus \{j\}$, folgt

$$0 \;\leqslant\; \mathrm{v}_p(a_{j+\tilde{j}}) \;=\; \mathrm{v}_p(\textstyle\sum_{i\in[0,j+\tilde{j}]} b_i\tilde{b}_{j+\tilde{j}-i}) \;=\; \mathrm{v}_p(b_j\tilde{b}_{\tilde{j}}) \;=\; v+\tilde{v} \;<\; 0 \;,$$

was einen *Widerspruch* darstellt. Also ist $g(X) \in \mathbf{Z}[X]$. Genauso folgt $f(X) \in \mathbf{Z}[X]$.

(2) *Annahme,* es gebe eine Zerlegung $f(X) = g(X)h(X)$ mit $g(X), h(X) \in \mathbf{Q}[X]$ o.E. normiert, $\deg g > 1$ und $\deg h > 1$. Nach (1) sind $g(X), h(X) \in \mathbf{Z}[X]$. Schreibe $k := \deg g$ und $\tilde{k} := \deg h$.
Sei $\mathbf{Z} \xrightarrow{\rho} \mathbf{F}_p$, $z \longmapsto z + p\mathbf{Z}$ die Restklassenabbildung; cf. §1.4.1. Es ist

$$X^n \;=\; f^\rho(X) \;=\; g^\rho(X)h^\rho(X) \;;$$

cf. §1.4.3. Also ist $g^\rho(X) = X^k$ und $h^\rho(X) = X^{\tilde{k}}$; cf. §1.9. Folglich sind die konstanten Koeffizienten von $g(X)$ und von $h(X)$ beide durch p teilbar. Daher ist der konstante Koeffizient von $g(X)h(X) = f(X)$ durch p^2 teilbar. Dies ist aber nicht der Fall gemäß unserer Voraussetzung. Wir haben einen *Widerspruch.* Somit ist $f(X)$ irreduzibel.

Literatur

[1] Artin, E., mit Milgram, N.A., *Galoissche Theorie,* Harri Deutsch, 1968
(vgl. auch projecteuclid.org/euclid.ndml/1175197041, MathSciNet MR0006974).

[2] Bosma, W.; Cannon, J.J.; Fieker, C.; Steel, A. (eds.), *Handbook of Magma functions,* Edition 2.16, 2010; cf. magma.maths.usyd.edu.au, magma.maths.usyd.edu.au/calc.

[3] Edwards, H. M., *Galois Theory,* Springer GTM 101, 1984.

[4] Jantzen, J.C.; Schwermer, J., *Algebra,* Springer, 2006.

[5] Lang, S., *Algebra,* Springer GTM 211, 2002.