

# Computeralgebra

Matthias Künzer

Universität Stuttgart

19. April 2012

# Inhalt

<b>1</b>	<b>Elementarteiler</b>	<b>6</b>
1.1	Teilbarkeit . . . . .	6
1.2	Elementarteilerform . . . . .	6
<b>2</b>	<b>Polynomfaktorisierung</b>	<b>12</b>
2.1	Quadratfreie Zerlegung . . . . .	12
2.2	Gleichgradige Zerlegung . . . . .	13
2.3	Zerlegung in irreduzible Faktoren . . . . .	15
<b>3</b>	<b>Charaktertafeln</b>	<b>18</b>
3.1	Wedderburn-Zerlegung . . . . .	18
3.1.1	Peirce-Zerlegung . . . . .	18
3.1.2	Halbeinfache Algebren . . . . .	20
3.2	Gruppenalgebren . . . . .	25
3.2.1	Gruppenringe . . . . .	25
3.2.2	Maschke . . . . .	26
3.3	Charaktere . . . . .	26
3.3.1	Definition . . . . .	26
3.3.2	Der triviale Charakter . . . . .	27
3.3.3	Unabhängigkeit von der Wahl des Wedderburnisomorphismus $\omega$ . . . . .	28
3.3.4	Orthogonalitätsrelationen . . . . .	29
3.4	Der Dixon-Algorithmus . . . . .	32
3.4.1	Ein Isomorphismus von Zentren . . . . .	32
3.4.2	Eine Betrachtung modulo $p$ . . . . .	34
3.4.3	Charakterwerte rekonstruieren von Betrachtung modulo $p$ . . . . .	36
3.4.4	Der resultierende Algorithmus . . . . .	37
<b>4</b>	<b>Ringe ganzer Zahlen</b>	<b>39</b>
4.1	Begriff . . . . .	39
4.2	Spurbilinearform und $\mathbf{Z}$ -Gitter . . . . .	42
4.3	$\mathbf{Z}$ -Maximalordnung . . . . .	45
4.4	Diskriminante . . . . .	46
4.5	$p$ -Radikal-Stabilisatoren . . . . .	46
4.5.1	$p$ -Radikal . . . . .	46
4.5.2	Stabilisator . . . . .	48
4.5.3	Pohst-Zassenhaus-Bernardi . . . . .	50
4.5.4	Bestimmung der $\mathbf{Z}$ -Maximalordnung $\mathcal{O}_K$ . . . . .	51
4.6	Kreisteilungskörper . . . . .	52
4.6.1	Einheitswurzeln mit Primpotenzordnung . . . . .	52
4.6.1.1	Spur und Diskriminante im Primpotenzfall . . . . .	52
4.6.1.2	Der Ring der ganzen Zahlen in $\mathbf{Q}(\zeta)$ im Primpotenzfall . . . . .	53
4.6.2	Der Ring der ganzen Zahlen in $\mathbf{Q}(\zeta)$ . . . . .	54
<b>A</b>	<b>Aufgaben und Lösungen</b>	<b>58</b>
A.1	Aufgaben . . . . .	58
A.2	Lösungen . . . . .	70

## Verzeichnis der Sätze, der Algorithmen und einiger Lemmata

Satz 4	§1.2	S. 8	Elementarteilersatz
Algorithmus 9	§2.1	S. 13	Quadratfreie Zerlegung
Lemma 11	§2.2	S. 14	Gleichgradige Zerlegung
Algorithmus 13	§2.3	S. 16	Cantor-Zassenhaus-Split
Lemma 16	§3.1.1	S. 19	Peirce-Zerlegung
Lemma 24	§3.1.2	S. 22	Schur
Satz 25	§3.1.2	S. 23	Wedderburn
Lemma 27	§3.2.2	S. 26	Maschke
Satz 38	§3.3.4	S. 30	Orthogonalitätsrelationen
Algorithmus 51	§3.4.4	S. 37	Dixon
Lemma 68, 69	§4.3	S. 45	$\mathbf{Z}$ -Maximalordnung
Algorithmus 73	§4.5.1	S. 47	$p$ -Jacobson-Radikal
Algorithmus 76	§4.5.2	S. 49	Stabilisator
Satz 79	§4.5.3	S. 50	Pohst-Zassenhaus
Algorithmus 82	§4.5.4	S. 51	$\mathbf{Z}$ -Maximalordnung bestimmen
Satz 89	§4.6.2	S. 56	$\mathbf{Z}$ -Maximalordnung von Kreisteilungskörpern

## Vorwort

Folgende Themen werden behandelt.

Elementarteiler. Matrizen über Hauptidealbereichen, wie etwa  $\mathbf{Z}$  oder  $\mathbf{C}[X]$ , können durch Multiplikation von links und rechts mit invertierbaren Matrizen auf Diagonalform gebracht werden, mit sich konsekutiv teilenden Diagonaleinträgen, welche im wesentlichen eindeutig festliegen.

Polynomfaktorisierung. Ein normiertes Polynom in  $\mathbf{F}_p[X]$  läßt sich (bis auf Reihenfolge) eindeutig in in normierte irreduzible Faktoren zerlegen. Diese aufzufinden ist ein a priori endliches Problem. Nichtsdestoweniger stellt sich die Frage nach einem guten Verfahren.

Charaktertafeln. Der Charakter einer irreduziblen gewöhnlichen Darstellung einer endlichen Gruppe ist die Abbildung, die einem Gruppenelement die Spur seiner darstellenden Matrix zuordnet. Diese Charaktere helfen dann umgekehrt wieder, um die Gruppe besser zu verstehen. Wir wollen uns mit der Berechnung der Charaktere befassen.

Ringe ganzer Zahlen. Ein Zahlkörper ist eine endliche Körpererweiterung von  $\mathbf{Q}$ , wie e.g.  $\mathbf{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbf{Q}\}$ . Der Ring der ganzen Zahlen  $\mathcal{O}_K \subseteq K$  eines Zahlkörpers  $K$  besteht aus den Elementen von  $K$ , die Nullstellen normierter Polynome in  $\mathbf{Z}[X]$  sind. Wir wollen  $\mathcal{O}_K$  berechnen.

Vorausgesetzt werden Kenntnisse aus der Algebra.

Dank geht an JANA FRANZ und JULIA VINOGRADSKA für Korrekturen und Verbesserungen, sowie an GABRIELE NEBE für Hilfe mit dem Satz von Pohst-Zassenhaus.

Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Stuttgart, den 24.03.2011

Matthias Künzer

### Konventionen.

- Sei  $f : X \rightarrow Y$  eine Abbildung. Seien  $U \subseteq X$  und  $V \subseteq Y$  so, daß  $f(U) \subseteq V$ . Schreibe  $f|_U^V : U \rightarrow V$ ,  $x \mapsto f(x)$ . Schreibe auch  $f|_U := f|_U^Y$  und  $f|_V := f|_X^V$ , sofern anwendbar.
- Ist  $M$  eine endliche Menge, so schreiben wir  $|M|$  für die Anzahl ihrer Elemente.
- Sprechen wir von *zwei Elementen*  $x$  und  $y$  einer Menge, so kann auch  $x = y$  sein.
- Für Elemente  $x$  und  $y$  sei  $\partial_{x,y} := 1$ , falls  $x = y$ , und  $\partial_{x,y} := 0$ , falls  $x \neq y$ .
- Gegeben  $a, b \in \mathbf{Z}$ , schreiben wir  $[a, b] := \{c \in \mathbf{Z} : a \leq c \leq b\}$  für das ganzzahlige Intervall. Ferner schreiben wir  $\mathbf{Z}_{\geq a} := \{z \in \mathbf{Z} : z \geq a\}$  etc.
- Sei  $R$  ein kommutativer Ring. Seien  $m, n \geq 0$ . Sei  $R^{m \times n}$  die Menge der  $m \times n$ -Matrizen mit Einträgen in  $R$ . Wir identifizieren  $R^{1 \times 1}$  und  $R$ .
- Leere Einträge in Matrizen seien null.
- Sei  $R$  ein kommutativer Ring. Seien  $m, n \geq 0$ . Sei  $i \in [1, m]$  und  $j \in [1, n]$ . Es bezeichnet  $e_{i,j} \in R^{m \times n}$  die Matrix, die an Position  $(i, j)$  den Eintrag 1 hat, und 0 sonst.  
Es bezeichnet  $E = E_m \in R^{m \times m}$  die Einheitsmatrix.  
Es bezeichnet  $0 = 0_{m \times n} \in R^{m \times n}$  die Nullmatrix.  
Sei  $t \geq 0$  und  $n_s \geq 1$  für  $s \in [1, t]$  gegeben. Wir schreiben  $e_{i,j}^s \in R^{n_1 \times n_1} \times \dots \times R^{n_t \times n_t}$  für das Tupel, das an Position  $s$  die Matrix mit Eintrag 1 an Position  $(i, j)$  und Nullen sonst stehen hat, und ansonsten Nullmatrizen.
- Die Spurabbildung auf Matrizen wird mit  $\text{tr}$  bezeichnet.
- Ist  $R$  ein kommutativer Ring, und sind  $a, b, c \in R$ , so schreiben wir  $a \equiv_c b$ , falls  $a - b = cx$  für ein  $x \in R$ .
- Ist  $R$  ein kommutativer Ring, ist  $x \in R$  und sind  $k, \ell \in \mathbf{Z}_{\geq 0}$ , so schreiben wir  $x^{k^\ell} := x^{(k^\ell)}$ .
- Sei  $K$  ein Körper. Der ggT von Polynomen in  $K[X]$  sei stets normiert oder 0.
- Sei  $L|K$  eine Körpererweiterung. Sei  $t \in L$ . Es bezeichnet  $\mu_{t,K}(X) \in K[X]$  das Minimalpolynom von  $t$  über  $K$ .
- Sei  $A$  ein Ring. Unter einem  $A$ -Modul verstehen wir einen  $A$ -Linksmodul.
- Sei  $A$  ein Ring. Sei  $M$  ein  $A$ -Modul. Sei  $X \subseteq M$ . Schreibe

$${}_R X := \left\{ \sum_{i \in [1, k]} a_i x_i : k \geq 0, a_i \in A \text{ und } x_i \in X \text{ für } i \in [1, k] \right\}.$$

Ist  $X = \{x_1, \dots, x_n\}$ , so schreiben wir auch  ${}_R \langle x_1, \dots, x_n \rangle := {}_R \langle \{x_1, \dots, x_n\} \rangle$ .

- Sei  $A$  ein Ring. Sei  $M$  ein  $A$ -Modul. Sei  $k \geq 0$ . Schreibe  $M^{\oplus k} := \bigoplus_{i \in [1, k]} M$ .
- Sei  $A$  ein Ring. Es bezeichne  $U(A) := \{u \in A : \text{es gibt ein } v \in A \text{ mit } uv = vu = 1\}$  die Einheitengruppe von  $A$ .
- Sei  $A$  ein Ring. Es bezeichne  $Z(A) := \{x \in A : \text{es ist } xy = yx \text{ für alle } y \in A\}$  das Zentrum von  $A$ . Es ist  $Z(A) \subseteq A$  ein Teilring.
- Sei  $K$  ein Körper. Sei  $V$  ein endlichdimensionaler Vektorraum. Sei  $f \in \text{End}_K V$ . Es bezeichnet  $\text{tr } f \in K$  die Spur von  $f$ .
- Sei  $G$  eine Gruppe. Sei  $g \in G$ . Es bezeichnet  $g^G := \{x^{-1}gx : x \in G\}$  die Konjugationsklasse von  $g$  in  $G$ .
- Sei  $m \geq 1$ . Wir schreiben  $\zeta_m := \exp(2\pi i/m) \in \mathbf{C}$ .

# Kapitel 1

## Elementarteiler

### 1.1 Teilbarkeit

Sei  $R$  ein Integritätsbereich, i.e. ein kommutativer nullteilerfreier Ring ungleich  $\{0\}$ .

Für  $x_1, \dots, x_k \in R$  schreiben wir

$$\langle x_1, \dots, x_k \rangle = {}_R\langle x_1, \dots, x_k \rangle := \left\{ \sum_{i \in [1, k]} s_i x_i : s_i \in R \text{ für } i \in [1, k] \right\} \subseteq R.$$

für das von  $x_1, \dots, x_k$  erzeugte Ideal. E.g. ist  $\langle 0 \rangle = \{0\}$ .

Für  $x \in R$  schreiben wir auch  $Rx = xR = \langle x \rangle$ .

Ein Element  $a \in R$  *teilt* ein Element  $b \in R$ , falls  $\langle a \rangle \supseteq \langle b \rangle$ .

Für  $a, b \in R$  ist  $\langle a \rangle = \langle b \rangle$  genau dann, wenn es eine Einheit  $u$  in  $R$  mit  $au = b$  gibt.

### 1.2 Elementarteilerform

Sei nun  $R$  ein Hauptidealbereich, i.e. ein Integritätsbereich, in welchem jedes Ideal von einem Element erzeugt ist.

E.g.  $R = \mathbf{Z}$  oder  $R = K[X]$  für einen Körper  $K$ ; cf. Aufgabe 1.(1). Nicht aber e.g.  $\mathbf{Z}[X]$ ; cf. Aufgabe 1.(2).

Insbesondere gibt es für  $x, y \in R$  ein  $z \in R$  mit

$$\langle z \rangle = \langle x, y \rangle$$

In anderen Worten, zum einen sind  $x$  und  $y$  Vielfache von  $z$ , zum anderen ist  $z = sx + ty$  für gewisse  $s, t \in R$ . Man nennt  $z$  auch *größten gemeinsamen Teiler* von  $x$  und  $y$ , geschrieben  $z =: \text{ggT}(x, y)$ , wobei dieser nur bis auf eine Einheit in  $R$  festliegt.

E.g. in  $\mathbf{Z}$  und in  $K[X]$  kann der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers verwandt werden.



Wir erinnern daran, daß  $R$  ein Hauptidealbereich und  $A \in R^{m \times n}$  ist.

**Satz 4 (Elementarteilersatz)**

*Es gibt  $S \in \text{SL}_m^{\mathbb{Q}}(R)$  und  $T \in \text{SL}_n^{\mathbb{Q}}(R)$  mit  $SAT$  in Elementarteilerform.*

Cf. Aufgabe 5.

*Beweis.* Wir führen eine Induktion über  $\min\{m, n\}$ . Wir haben  $A$  so mit Quasielementarmatrizen von links und von rechts zu multiplizieren, daß eine Matrix in Elementarteilerform entsteht.

Beim Induktionsanfang  $\min\{m, n\} = 0$  ist nichts zu tun.

Sei  $\min\{m, n\} \geq 1$ . Sei die Aussage gezeigt für Matrizen in  $R^{(m-1) \times (n-1)}$ . Wir multiplizieren unsere Matrix  $A = (a_{i,j})_{i,j} \in R^{m \times n}$  beidseitig mit Quasielementarmatrizen, ändern dabei aber mißbräuchlicherweise die Bezeichnung für diese Matrix nicht.

**Äußere Schleife.** Sei  $j = 1$ . Solange  $j \leq n$ , führe aus:

*Innere Schleife.*

*Säubern der ersten Spalte.* Sei  $i = 2$ . Solange  $i \leq m$ , führe aus:

Seien  $s, t \in R$  so, daß  $sa_{1,1} + ta_{i,1} = z$  mit  $\langle a_{1,1}, a_{i,1} \rangle = \langle z \rangle$ . Sei hierbei  $s = 1$  und  $t = 0$ , falls  $a_{1,1}$  ein Teiler von  $a_{i,1}$  ist.

Falls  $z = 0$ , führen wir keine Matrixoperation durch.

Falls  $z \neq 0$ , schreiben wir  $a'_{1,1} := a_{1,1}/z$  und  $a'_{i,1} := a_{i,1}/z$ . Multiplikation von  $A$  von links mit  $\begin{pmatrix} s & t \\ -a'_{i,1} & a'_{1,1} \end{pmatrix}_{1,i}$  liefert eine Matrix, die an Position  $(i, 1)$  einen Nulleintrag aufweist, in den Positionen  $(\tilde{i}, 1)$  für  $\tilde{i} \in [2, m] \setminus \{i\}$  aber unverändert bleibt.

Der neue Eintrag  $z$  an Position  $(1,1)$  teilt den alten, sowie den ehemaligen Eintrag an Position  $(i, 1)$ .

Zähle  $i$  eins hoch. Ende der *Ausführung*.

*Säubern der ersten Zeile.* Genauso können wir durch Multiplikation mit Quasielementarmatrizen von rechts erreichen, daß an den Positionen  $(1, 2), \dots, (1, n)$  die Matrix  $A$  nur Nulleinträge aufweist, wobei der Eintrag an Position  $(1, 1)$  durch einen seiner Teiler ersetzt wird. Wird hierbei die erste Spalte geändert, so wird der Betrag des Eintrags an Position  $(1, 1)$  echt verkleinert.

Nun erfolge wieder ein *Säubern der ersten Spalte*. Wird hierbei die erste Zeile geändert, so wird der Betrag des Eintrags an Position  $(1, 1)$  echt verkleinert.

Nun erfolge wieder ein *Säubern der ersten Zeile*. Wird hierbei die erste Spalte geändert, so wird der Betrag des Eintrags an Position  $(1, 1)$  echt verkleinert.

Usf.

Dies setzen wir fort, bis  $A$  von der Form

$$A = \begin{pmatrix} a_{1,1} & & & \\ \vdots & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,2} & \cdots & \cdots & a_{m,n} \end{pmatrix}$$

ist, wobei  $a_{1,1}$  jeden Eintrag teilt, den unsere Matrix zu Beginn der inneren Schleife in der ersten Spalte und der ersten Zeile hatte.

Dies tritt in der Tat ein, da der Betrag des Eintrags an Position  $(1, 1)$  nur endlich oft echt verkleinert werden kann, und da bei nach Säubern der ersten Spalte und der ersten Zeile gleichgebliebenem Eintrag an Position  $(1, 1)$  die erste Spalte und die erste Zeile danach an den Positionen ungleich  $(1, 1)$  nur Nullen aufweisen.

Ende der *inneren Schleife*.

Zähle  $j$  eins hoch.

*Frage.* Ist  $\langle a_{1,1} \rangle \supseteq \langle a_{i,j} \rangle$  für alle  $i \in [2, m]$ ?

Falls nein, so multipliziere  $A$  mit  $\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}_{1,j}$  von rechts und beginne die innere Schleife.

Nach ihrer Durchführung teilt  $a_{1,1}$  alle Einträge, die  $A$  vor ihrer Durchführung in der ersten (wie in der  $j$ -ten) Spalte hatte, und also auch alle Einträge, die  $A$  nun in der  $j$ -ten Spalte hat, da letztere  $R$ -Linearkombinationen ersterer sind.

Ende der *Ausführung*.

Es ist  $A$  nun von der Form

$$A = \begin{pmatrix} a_{1,1} & & & \\ \vdots & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,2} & \cdots & \cdots & a_{m,n} \end{pmatrix}$$

mit  $\langle a_{1,1} \rangle \supseteq \langle a_{i,j} \rangle$  für alle  $i \in [2, m]$  und alle  $j \in [2, n]$ .

Ende der *äußeren Schleife*.

Schreibe

$$A' := \begin{pmatrix} a_{2,2} & \cdots & a_{2,n} \\ \vdots & & \vdots \\ a_{m,2} & \cdots & a_{m,n} \end{pmatrix},$$

so daß sich in Blockmatrixschreibweise  $A = \begin{pmatrix} a_{1,1} & \\ & A' \end{pmatrix}$  ergibt.

Nach Induktionsvoraussetzung gibt es  $S' \in \mathrm{SL}_{m-1}^{\mathbb{Q}}(R)$  und  $T' \in \mathrm{SL}_{n-1}^{\mathbb{Q}}(R)$  mit  $S'A'T' = D'$  in Elementarteilerform. Da  $a_{1,1}$  jeden Eintrag von  $A'$  teilt, teilt  $a_{1,1}$  auch jeden Eintrag von  $D'$ . In Blockmatrixschreibweise wird nun

$$\begin{pmatrix} 1 & \\ & S' \end{pmatrix} \begin{pmatrix} a_{1,1} & \\ & A' \end{pmatrix} \begin{pmatrix} 1 & \\ & T' \end{pmatrix} = \begin{pmatrix} a_{1,1} & \\ & D' \end{pmatrix},$$

und letztere Matrix ist in der Tat in Elementarteilerform. □

**Korollar 5** *Es ist  $\mathrm{SL}_m^{\mathbb{Q}}(R) = \mathrm{SL}_m(R)$ .*

*Beweis.* Sei  $A \in \mathrm{SL}_m(R)$  gegeben. Nach Satz 4 gibt es  $S, T \in \mathrm{SL}_m^{\mathbb{Q}}(R)$  mit  $SAT = D$  in Elementarteilerform. Es wird

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_m \end{pmatrix} = \begin{pmatrix} d_2^{-1} & & \\ & d_2 & \\ & & \ddots \end{pmatrix}_{1,2} \cdots \begin{pmatrix} d_m^{-1} & & \\ & d_m & \\ & & \ddots \end{pmatrix}_{1,m} \in \mathrm{SL}_m^{\mathbb{Q}}(R)$$

da ja  $d_1 = d_2^{-1} \cdots d_m^{-1}$ . Also ist auch  $A = S^{-1}DT^{-1} \in \mathrm{SL}_m^{\mathbb{Q}}(R)$ .  $\square$

Sei  $\ell \in [1, \min\{m, n\}]$ . Ein  $\ell \times \ell$ -Minor von  $A$  ist die Determinante einer Teilmatrix  $(a_{i_s, j_t})_{s,t} \in R^{\ell \times \ell}$ , wobei  $1 \leq i_1 < i_2 < \cdots < i_\ell \leq m$  und  $1 \leq j_1 < j_2 < \cdots < j_\ell \leq n$ . Sei  $M_\ell(A) \subseteq R$  das von allen  $\ell \times \ell$ -Minoren von  $A$  erzeugte Ideal in  $R$ .

**Lemma 6** *Seien  $d_1, \dots, d_k$  Elementarteiler von  $A$ , wobei  $k = \mathrm{rk} A$ .*

*Sei  $\ell \in [1, \min\{m, n\}]$ . Dann ist*

$$M_\ell(A) = \begin{cases} \langle \prod_{i \in [1, \ell]} d_i \rangle & \text{falls } \ell \leq k \\ \langle 0 \rangle & \text{falls } \ell > k \end{cases}$$

*Insbesondere sind die Elementarteiler von  $A$  bis auf Einheiten in  $R$  eindeutig bestimmt.*

*Beweis.* Seien  $S \in \mathrm{GL}_m(R)$  und  $T \in \mathrm{GL}_n(R)$  so, daß

$$SAT = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \end{pmatrix} =: D$$

in Elementarteilerform ist; cf. Satz 4.

Die rechte Seite der behaupteten Gleichung ist gleich  $M_\ell(D)$  Denn ein  $\ell \times \ell$ -Minor von  $D$  ist gleich null oder von der Form  $\prod_{i \in J} d_i$  mit  $J \subseteq [1, k]$  und  $|J| = \ell$ . Letzteres tritt nur ein, falls  $\ell \leq k$ , und dann teilt wird dieser Minor vom Minor  $\prod_{i \in [1, \ell]} d_i$  geteilt.

Es bleibt also ganz allgemein zu zeigen, daß  $M_\ell(B) \stackrel{!}{=} M_\ell(BQ) \stackrel{!}{=} M_\ell(PBQ)$  für  $B \in R^{m \times n}$ ,  $P \in \mathrm{GL}_m(R)$  und  $Q \in \mathrm{GL}_n(R)$ .

Aus Symmetriegründen genügt es,  $M_\ell(B) \stackrel{!}{=} M_\ell(BQ)$  für  $B \in R^{m \times n}$  und  $Q \in \mathrm{GL}_n(R)$  zu zeigen.

Da  $B = (BQ)Q^{-1}$ , genügt es,  $M_\ell(B) \stackrel{!}{\supseteq} M_\ell(BQ)$  für  $B \in R^{m \times n}$  und  $Q \in \mathrm{GL}_n(R)$  zu zeigen. Zeigen wir dies allgemeiner für  $B \in R^{m \times n}$  und  $Q \in R^{n \times n}$ . Hierbei betrachten wir  $B$  als fest gewählt.

Sei  $1 \leq i_1 < i_2 < \cdots < i_\ell \leq m$  und  $1 \leq j_1 < j_2 < \cdots < j_\ell \leq n$ . Schreibe  $BQ = (c_{i_s, j_t}(Q))_{s,t} \in R^{m \times n}$ . Wir haben zu zeigen, daß  $\det(c_{i_s, j_t}(Q))_{s,t} \stackrel{!}{\in} M_\ell(B)$ .

Wir dürfen annehmen, daß die Spalten  $j_1, \dots, j_\ell$  von  $Q$  Standardbasisvektoren sind, da  $\det(c_{i_s, j_t}(Q))_{s,t}$  linear in diesen Spalten von  $Q$  ist.

Somit ist  $\det(c_{i_s, j_t}(Q))_{s,t}$  bis auf Vorzeichen ein  $\ell \times \ell$ -Minor von  $B$ , oder gleich null. Jedenfalls ist es in  $M_\ell(B)$  enthalten.  $\square$

**Bemerkung 7** Es wird  $SL_m(\mathbf{Z})$  von Elementarmatrizen erzeugt.

*Beweis.* Nach Korollar 5 genügt es zu zeigen, daß  $SL_2(\mathbf{Z}) \stackrel{!}{=} \langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle =: E$ .

Für  $z \in \mathbf{Z}$  ist  $\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^z \in E$  und  $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^z \in E$ .

Ferner ist  $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in E$ . Also sind auch  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in E$ .

Sei  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ . Wir haben zu zeigen, daß  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \stackrel{!}{\in} E$ . Dank  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in E$  sind o.E.  $a, c \geq 0$ .

Wir führen eine Induktion nach  $\min\{a, c\}$ .

Induktionsanfang  $\min\{a, c\} = 0$ .

Den Fall  $a = 0$  können wir durch Linksmultiplikation mit  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  auf den nächsten Fall zurückführen.

Falls  $c = 0$ , dann ist wegen  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in SL_2(\mathbf{Z})$  und  $a \geq 0$  auch  $a = 1$ , und damit auch  $c = 1$ . Und  $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in E$ .

Induktionsschritt. Sei  $\min\{a, c\} > 0$ .

Falls  $0 < a \leq c$ , dann finde  $k \in \mathbf{Z}$  mit  $c - ka \in [0, a - 1]$ . Nach Induktionsvoraussetzung ist  $\begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c-ka & d-kb \end{pmatrix} \in E$ , also ist auch  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in E$ .

Falls  $0 < c \leq a$ , dann finde  $k \in \mathbf{Z}$  mit  $a - kc \in [0, c - 1]$ . Nach Induktionsvoraussetzung ist  $\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-kc & b-kd \\ c & d \end{pmatrix} \in E$ , also ist auch  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in E$ .  $\square$

# Kapitel 2

## Polynomfaktorisierung

Sei  $p \geq 2$  prim. Sei  $f(X) \in \mathbf{F}_p[X]$  normiert. Sei  $n := \deg f \geq 1$ . Wir wollen  $f(X)$  in normierte irreduzible Faktoren zerlegen; cf. Aufgabe 6.

Das ist wegen der Endlichkeit der Menge  $\{a(X) \in \mathbf{F}_p[X] \setminus \{0\} : 1 \leq \deg a \leq n\}$  der potentiellen Teiler von  $f(X)$  a priori ein endliches Problem. Cf. Aufgabe 8. Auch der hier zu behandelnde Algorithmus wird letzten Endes auf eine endliche Suche angewiesen sein.

### 2.1 Quadratfreie Zerlegung

Ein Polynom in  $\mathbf{F}_p[X] \setminus \{0\}$  heie *quadratfrei*, falls es in  $\mathbf{F}_p[X]$  nicht vom Quadrat eines normierten irreduziblen Polynoms geteilt wird.

Wir wollen eine Zerlegung

$$f(X) = u_1(X) u_2(X) \cdots u_n(X)$$

in quadratfreie normierte Polynome  $u_i(X) \in \mathbf{F}_p[X]$  finden.

Sei  $u(X) = \sum_{i \geq 0} a_i X^i \in \mathbf{F}_p[X] \setminus \{0\}$  mit  $\deg u \geq 1$  gegeben, wobei  $a_i \in \mathbf{F}_p$ . Sei  $k \geq 0$  maximal so, da  $u(X) = \check{u}(X^{p^k})$  fr ein  $\check{u}(X) \in \mathbf{F}_p[X]$ . Dieses  $\check{u}(X)$  liegt eindeutig fest und heie *Frobeniusreduktion* von  $u(X)$ . Es ergibt sich

$$\begin{aligned} k &= \max\{\ell \geq 0 : p^\ell \mid i \text{ fr alle } i \geq 0 \text{ mit } a_i \neq 0\} \\ \check{u}(X) &= \sum_{i \geq 0} u_{p^k i} X^i. \end{aligned}$$

Beachte, da dann auch  $u(X) = \check{u}(X^{p^k}) = \check{u}(X)^{p^k}$ , da  $a^p = a$  fr  $a \in \mathbf{F}_p$ .

Beachte ferner, da  $\check{u}'(X) \neq 0$ , sowie, da  $\deg \check{u} \geq 1$ .

Ist insbesondere  $u(X)$  irreduzibel, dann ist  $u(X) = \check{u}(X)$ , und somit  $u'(X) = \check{u}'(X) \neq 0$ .

Ist e.g.  $p = 2$  und  $u(X) = X^{32} + X^{24} + 1$ , so ist  $\check{u}(X) = X^4 + X^3 + 1$ .

**Lemma 8** *Es ist  $u(X) \in \mathbf{F}_p[X] \setminus \{0\}$  genau dann quadratfrei, wenn*

$$\text{ggT}(u(X), u'(X)) = 1.$$

*Beweis.* Sei  $u(X)$  nicht quadratfrei. Dann gibt es ein  $v(X) \in \mathbf{F}_p[X]$  von Grad  $\geq 1$  und ein  $w(X) \in \mathbf{F}_p[X]$  so, daß  $u(X) = v(X)^2 w(X)$ . Es folgt

$$u'(X) = v(X)^2 w'(X) + 2v(X)v'(X)w(X)$$

und also, daß  $v(X)$  auch  $\text{ggT}(u(X), u'(X))$  teilt. Also ist  $\text{ggT}(u(X), u'(X)) \neq 1$ .

Sei umgekehrt  $u(X)$  quadratfrei. *Annahme*,  $\text{ggT}(u(X), u'(X)) \neq 1$ . Sei  $g(X)$  ein irreduzibler Faktor von  $\text{ggT}(u(X), u'(X))$ . Schreibe  $u(X) = g(X)h(X)$  für ein  $h(X) \in \mathbf{F}_p[X]$ . Da auch

$$u'(X) = g'(X)h(X) + g(X)h'(X)$$

ein Vielfaches von  $g(X)$  ist, teilt  $g(X)$  das Produkt  $g'(X)h(X)$ . Da  $g(X)$  irreduzibel ist, ist  $g'(X) \neq 0$ ; da nun  $\deg g' < \deg g$ , folgt, daß  $g(X)$  kein Teiler von  $g'(X)$  ist. Folglich ist  $g(X)$  ein Teiler von  $h(X)$ . Dies aber *widerspricht* der Quadratfreiheit von  $u(X)$ . Also ist  $\text{ggT}(u(X), u'(X)) = 1$ .  $\square$

### Algorithmus 9 (Quadratfreie Zerlegung)

Wir wollen  $f(X)$  in quadratfreie Faktoren zerlegen. Per Induktion genügt es, einen quadratfreien Teiler von  $f(X)$  von Grad  $\geq 1$  zu finden.

Sei  $h_1(X) := f(X)$ .

Sei  $h_2(X) := \text{ggT}(\check{h}_1(X), \check{h}'_1(X))$ . Ist  $h_2(X) = 1$ , so ist  $\check{h}_1(X)$  nach Lemma 8 ein quadratfreier Teiler von  $f(X)$  von Grad  $\geq 1$ , und wir sind fertig. Ansonsten ist  $\deg h_2 \geq 1$ .

Sei  $h_3(X) := \text{ggT}(\check{h}_2(X), \check{h}'_2(X))$ . Ist  $h_3(X) = 1$ , so ist  $\check{h}_2(X)$  nach Lemma 8 ein quadratfreier Teiler von  $f(X)$  von Grad  $\geq 1$ , und wir sind fertig. Ansonsten ist  $\deg h_3 \geq 1$ .

Usf.

Es ist hierbei  $\check{h}'_i \neq 0$  und  $\deg h_{i+1} \leq \deg \check{h}'_i < \deg \check{h}_i \leq \deg h_i$  stets. Also bricht das Verfahren nach höchstens  $n$  Schritten ab.

Cf. Aufgabe 8.(2).

## 2.2 Gleichgradige Zerlegung

Sei  $f(X)$  zudem quadratfrei. Wir wollen eine Zerlegung

$$f(X) = f_1(X)f_2(X) \cdots f_n(X)$$

in normierte Polynome  $f_i(X) \in \mathbf{F}_p[X]$  so finden, daß die normierten irreduziblen Faktoren von  $f_i(X)$  alle den Grad  $i$  haben für  $i \in [1, n]$ . Eine solche Zerlegung heiße *gleichgradig*.

**Lemma 10** *Sei  $d \geq 1$ . Es ist*

$$X^{p^d} - X = \prod_{\substack{g(X) \in \mathbf{F}_p[X] \text{ norm. u. irr.}, \\ \deg g \mid d}} g(X).$$

*Beweis.* Es ist  $\text{ggT}(X^{p^d} - X, (X^{p^d} - X)') = \text{ggT}(X^{p^d} - X, -1) = 1$ . Also ist  $X^{p^d} - X$  quadratfrei; cf. Lemma 8.

Sei  $e \mid d$ . Sei  $g(X) \in \mathbf{F}_p[X]$  ein normiertes irreduzibles Polynom von Grad  $e$ . Es ist  $K := \mathbf{F}_p[T]/\langle g(T) \rangle$  ein Körper mit einer Einheitengruppe von Ordnung  $p^e - 1$ . Schreibe  $t := T + \langle g(T) \rangle \in K$ . Schreibe  $\text{Frob} : K \xrightarrow{\sim} K, s \mapsto s^p$  für den Frobeniusautomorphismus von  $K$ .

Es ist  $t = 0$  oder aber  $t^{p^e-1} = 1$ . Jedenfalls ist  $t^{p^e} = t$ , i.e.  $\text{Frob}^e(t) = t$ . Also ist auch  $t^{p^d} = \text{Frob}^d(t) = (\text{Frob}^e)^{d/e}(t) = t$ . Also teilt das Minimalpolynom  $\mu_{t, \mathbf{F}_p}(X) = g(X)$  von  $t$  das Polynom  $X^{p^d} - X$ .

Sei umgekehrt  $h(X)$  ein normierter irreduzibler Faktor von  $X^{p^d} - X$ . Wir haben zu zeigen, daß  $\deg h \mid d$ . Hierzu ziehen wir den Körper  $\mathbf{F}_{p^d}$  heran. Da seine multiplikative Gruppe die Ordnung  $p^d - 1$  hat, sind alle seine Elemente Nullstellen von  $X^{p^d} - X$ . Mit einem Gradvergleich folgt  $X^{p^d} - X = \prod_{\xi \in \mathbf{F}_{p^d}} (X - \xi)$ ; cf. Lemma 8. Somit gibt es ein  $\eta \in \mathbf{F}_{p^d}$  mit  $h(\eta) = 0$ . Es folgt  $\mu_{\eta, \mathbf{F}_p}(X) = h(X)$ , und also  $\deg h = [\mathbf{F}_p(\eta) : \mathbf{F}_p]$ . Die Behauptung folgt nun aus

$$d = [\mathbf{F}_{p^d} : \mathbf{F}_p] = [\mathbf{F}_{p^d} : \mathbf{F}_p(\eta)][\mathbf{F}_p(\eta) : \mathbf{F}_p].$$

□

**Lemma 11 (Gleichgradige Zerlegung)**

*Definiere rekursiv  $h_1(X) := f(X)$  und*

$$h_i(X) := \frac{h_{i-1}(X)}{\text{ggT}(h_{i-1}(X), X^{p^{i-1}} - X)}$$

*für  $i \in [2, n]$ . Setze*

$$f_i(X) := \text{ggT}(h_i(X), X^{p^i} - X)$$

*für  $i \in [1, n]$ . Dann haben wir eine gleichgradige Zerlegung*

$$f(X) = f_1(X)f_2(X) \cdots f_n(X).$$

Man kann die Berechnung natürlich abbrechen, sobald  $h_i(X) = 1$ .

*Beweis.*

Es ist  $h_1(X)$  der Teiler von  $f(X)$ , der alle seine irreduziblen normierten Faktoren von Grad  $\geq 1$  enthält – i.e. alle.

Es ist  $h_2(X)$  der Teiler von  $f(X)$ , der alle seine irreduziblen normierten Faktoren von Grad  $\geq 2$  enthält, da dank  $h_1(X)$  quadratfrei diejenigen von Grad 1 wegdividiert wurden; cf. Lemma 10.

Es ist  $h_3(X)$  der Teiler von  $f(X)$ , der alle seine irreduziblen normierten Faktoren von Grad  $\geq 3$  enthält, da dank  $h_2(X)$  quadratfrei dazuhin diejenigen von Grad 2 wegdividiert wurden; cf. Lemma 10.

Usf.

Für  $i \in [1, n]$  ist, wegen  $h_i(X)$  quadratfrei,  $f_i(X)$  der Teiler von  $f(X)$ , der alle seine irreduziblen normierten Faktoren von Grad  $i$  enthält; cf. Lemma 10.(1).  $\square$

Cf. Aufgabe 8.(2).

## 2.3 Zerlegung in irreduzible Faktoren

Sei  $d \geq 1$ . Sei  $f(X)$  zudem quadratfrei und zerfalle in ein Produkt normierter irreduzibler Polynome von Grad  $d$ . Wir wollen diese bestimmen.

**Bemerkung 12** Sei  $h(X) \in \mathbf{F}_p[X]$  mit  $\deg h \geq 1$ .

- (1) Es ist  $f(X)$  ein Teiler von  $h(X)^{p^d} - h(X)$ .
- (2) Ist  $p \geq 3$ , so sind die Polynome  $h(X)$ ,  $h(X)^{\frac{p^d-1}{2}} - 1$  und  $h(X)^{\frac{p^d-1}{2}} + 1$  paarweise teilerfremd und geben im Produkt gleich  $h(X)^{p^d} - h(X)$ .
- (3) Ist  $p = 2$ , so sind die Polynome  $h(X)$ ,  $h(X)^{2^0-1} + h(X)^{2^1-1} + h(X)^{2^2-1} + \dots + h(X)^{2^{d-1}-1}$  und  $1 + h(X)^{2^0} + h(X)^{2^1} + h(X)^{2^2} + \dots + h(X)^{2^{d-1}}$  paarweise teilerfremd und geben im Produkt gleich  $h(X)^{2^d} - h(X)$ .

*Beweis.*

Zu (1). Da  $f(X)$  in normierte irreduzible Faktoren von Grad  $d$  zerfällt und quadratfrei ist, ist  $f(X)$  ein Teiler von  $X^{p^d} - X$ ; cf. Lemma 10.

Also genügt es zu zeigen, daß  $X^{p^d} - X$  ein Teiler von  $h(X)^{p^d} - h(X)$  ist.

Schreibe  $h(X) = \sum_{i \geq 0} a_i X^i$  mit  $a_i \in \mathbf{F}_p$ . Es ist

$$\begin{aligned} h(X)^{p^d} - h(X) &= \left( \sum_{i \geq 0} a_i X^i \right)^{p^d} - \left( \sum_{i \geq 0} a_i X^i \right) \\ &= \left( \sum_{i \geq 0} a_i (X^i)^{p^d} \right) - \left( \sum_{i \geq 0} a_i X^i \right) \\ &= \sum_{i \geq 1} a_i (X^{i \cdot p^d} - X^i), \end{aligned}$$

und es ist

$$X^{i \cdot p^d} - X^i = (X^{p^d} - X)(X^{p^d \cdot (i-1) + 0} + X^{p^d \cdot (i-2) + 1} + \dots + X^{p^d \cdot 0 + (i-1)})$$

für  $i \geq 1$ .

Zu (2). Ein gemeinsamer Teiler von  $h(X)$  und  $h(X)^{\frac{p^d-1}{2}} - 1$  teilt auch  $-1$ , ist also trivial. Ein gemeinsamer Teiler von  $h(X)$  und  $h(X)^{\frac{p^d-1}{2}} + 1$  teilt auch  $1$ , ist also trivial. Ein gemeinsamer Teiler von  $h(X)^{\frac{p^d-1}{2}} - 1$  und  $h(X)^{\frac{p^d-1}{2}} + 1$  teilt auch ihre Differenz  $-2$ , ist also trivial.

Zu (3). Ein gemeinsamer Teiler von  $h(X)$  und  $h(X)^{2^0-1} + h(X)^{2^1-1} + \dots + h(X)^{2^{d-1}-1}$  teilt auch  $h(X)^{2^0-1}$ , ist also trivial. Ein gemeinsamer Teiler von  $h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}}$  und  $1 + h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}}$  teilt auch  $1$ , ist also trivial.

Schließlich wird noch

$$\begin{aligned}
& (h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}})(1 + h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}}) \\
&= (h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}}) + (h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}})^2 \\
&= (h(X)^{2^0} + h(X)^{2^1} + \dots + h(X)^{2^{d-1}}) + (h(X)^{2^1} + h(X)^{2^2} + \dots + h(X)^{2^d}) \\
&= h(X) + h(X)^{2^d}.
\end{aligned}$$

□

### Algorithmus 13 (Cantor-Zassenhaus-Split)

Wir wollen  $f(X)$  in irreduzible normierte Faktoren zerlegen. Per Induktion genügt es,  $f(X)$  nichttrivial in Faktoren zu zerlegen, falls  $\deg f \geq 2d$ .

Durchlaufe  $h(X) \in \mathbf{F}_p[X]$  die normierten Polynome mit  $\deg h \in [1, d]$ .

Falls  $p \geq 3$ , so ist

$$h(X)^{p^d} - h(X) \stackrel{\text{Bem. 12.(2)}}{=} h(X)(h(X)^{\frac{p^d-1}{2}} - 1)(h(X)^{\frac{p^d-1}{2}} + 1),$$

und also

$$\begin{aligned}
f(X) & \stackrel{\text{Bem. 12.(1)}}{=} \text{ggT}(f(X), h(X)^{p^d} - h(X)) \\
& \stackrel{\text{Bem. 12.(2)}}{=} \text{ggT}(f(X), h(X)) \cdot \text{ggT}(f(X), h(X)^{\frac{p^d-1}{2}} - 1) \cdot \text{ggT}(f(X), h(X)^{\frac{p^d-1}{2}} + 1).
\end{aligned}$$

Falls  $p = 2$ , so ist

$$\begin{aligned}
& h(X)^{2^d} - h(X) \stackrel{\text{Bem. 12.(3)}}{=} \\
& h(X)(h(X)^{1-1} + h(X)^{2-1} + \dots + h(X)^{2^{d-1}-1})(h(X)^0 + h(X)^1 + h(X)^2 + \dots + h(X)^{2^{d-1}}),
\end{aligned}$$

und also

$$\begin{aligned}
f(X) & \stackrel{\text{Bem. 12.(1)}}{=} \text{ggT}(f(X), h(X)^{2^d} - h(X)) \\
& \stackrel{\text{Bem. 12.(3)}}{=} \text{ggT}(f(X), h(X)) \cdot \text{ggT}(f(X), h(X)^{1-1} + h(X)^{2-1} + \dots + h(X)^{2^{d-1}-1}) \\
& \quad \cdot \text{ggT}(f(X), h(X)^0 + h(X)^1 + h(X)^2 + \dots + h(X)^{2^{d-1}}).
\end{aligned}$$

Bei diesem Durchlauf tritt auch ein irreduzibler normierter Faktor von  $f(X)$  als  $h(X)$  auf, so daß dann der erste Faktor gleich  $h(X)$  wird und so spätestens dann die Zerlegung nichttrivial.

Nun wiederhole man das Verfahren für die gefundenen Faktoren einer solchen nichttrivialen Zerlegung; usf.

- Die Art des Durchlaufs der  $h(X)$ , ob systematisch oder zufällig, bleibt dabei dem Anwender überlassen. Vgl. Aufgabe 8.(2).
- Falls  $p \geq 3$ , so kann zur Berechnung von  $\text{ggT}(f(X), h(X)^{\frac{p^d-1}{2}} \pm 1)$  zunächst  $h(X)^{\frac{p^d-1}{2}} \pm 1$  in  $\mathbf{F}_p[X]/\langle f(X) \rangle$  berechnet und dann ein Repräsentant des Resultats herangezogen werden, da allgemein für  $u(X), v(X) \in \mathbf{F}_p[X]$  sich

$$\text{ggT}(f(X), u(X)) = \text{ggT}(f(X), u(X) + v(X)f(X))$$

ergibt, dafür die Wahl des Repräsentanten modulo  $\langle f(X) \rangle$  also keine Rolle spielt.

Für  $p = 2$  entsprechend.

Cf. Aufgabe 8.(2).

- Stellen wir noch einen groben Vergleich unseres Algorithmus mit dem naiven Algorithmus an.

Der naive Algorithmus testet alle normierten Polynome von Grad  $d$  auf die Eigenschaft hin,  $f(X)$  zu teilen. Die Wahrscheinlichkeit, unter den  $p^d$  derartigen Polynomen durch blinde Wahl einen Teiler von  $f(X)$  zu finden, ist gering. Man sucht also lange.

Die Zerlegung

$$f(X) = \text{ggT}(\dots) \cdot \text{ggT}(\dots) \cdot \text{ggT}(\dots)$$

aus unserem Algorithmus ist dagegen bereits dann brauchbar, wenn zwei der Faktoren ungleich 1 sind. Die Wahrscheinlichkeit,  $f(X)$  so erfolgreich aufgespalten zu haben, ist eher hoch. Bereits nach wenigen getesteten Polynomen  $h(X)$  wird man meistens die Suche beenden können, um den Algorithmus auf die entstandenen nichttrivialen Faktoren anzuwenden, usf. (Sicher ist dieses "wenigen" aber nicht. Sicher ist nur, daß man die Suche beenden kann, wenn man alle normierten Polynome  $h(X)$  von Grad  $d$  getestet hat. Das dauert dann ebenfalls lange, tritt aber in der Praxis kaum jemals auf.)

# Kapitel 3

## Charaktertafeln

### 3.1 Wedderburn-Zerlegung

#### 3.1.1 Peirce-Zerlegung

Sei  $A$  ein Ring.

**Definition 14** Ein Element  $e \in A$  heißt *idempotent*, falls  $e^2 = e$ .

Ein Idempotent  $e \in A \setminus \{0\}$  heißt *primitiv*, falls aus  $e = e' + e''$  mit  $e', e''$  Idempotenten mit  $e'e'' = 0$  und  $e''e' = 0$  bereits  $e' = 0$  oder  $e'' = 0$  folgt.

Sei  $n \geq 1$ . Ein Tupel  $\underline{e} = (e_1, \dots, e_n)$  von Idempotenten von  $A$  heißt *orthogonale Zerlegung in Idempotente* (in  $A$ ), falls  $1 = e_1 + \dots + e_n$  und falls  $e_i e_j = 0$  ist für  $i, j \in [1, n]$  mit  $i \neq j$ .

Eine orthogonale Zerlegung in Idempotente  $\underline{e} = (e_1, \dots, e_n)$  heie *orthogonale Zerlegung in primitive Idempotente* (in  $A$ ), falls  $e_i$  primitiv ist für  $i \in [1, n]$ .

**Bemerkung 15** Sei  $M$  ein  $A$ -Modul. Sei  $\underline{e} = (e_1, \dots, e_n)$  eine orthogonale Zerlegung in Idempotente in  $A$ . Dann ist

$$M = \bigoplus_{i \in [1, n]} e_i M$$

als abelsche Gruppe.

*Beweis.* Wegen  $1 = e_1 + \dots + e_n$  ist  $m = e_1 m + \dots + e_n m$ , und also  $M$  gleich der Summe der Untergruppen  $e_i M$ . Wir haben die Direktheit dieser Summe zu zeigen.

Sei also  $m_1 + \dots + m_n = 0$  mit  $m_i \in e_i M$  für  $i \in [1, n]$ . Beachte, daß  $m_j = e_j m'_j$  für ein  $m'_j \in M$ , und also  $e_j m_j = e_j^2 m'_j = e_j m'_j = m_j$  für  $j \in [1, n]$ .

Sei  $i \in [1, m]$  gegeben. Wir haben zu zeigen, daß  $m_i \stackrel{!}{=} 0$ . In der Tat wird

$$0 = e_i(m_1 + \cdots + m_n) = e_i(e_1 m_1 + \cdots + e_n m_n) = e_i m_i .$$

□

**Lemma 16 (Peirce-Zerlegung)** Sei  $\underline{e} = (e_1, \dots, e_n)$  eine orthogonale Zerlegung in Idempotente in  $A$ . Es wird

$$A = \bigoplus_{i,j \in [1,n]} e_i A e_j$$

als abelsche Gruppe.

*Beweis.* Mit Bemerkung 15 und der dazu analogen Aussage für  $A$ -Rechtsmoduln wird

$$A = \bigoplus_{i \in [1,n]} e_i A = \bigoplus_{i \in [1,n]} \left( \bigoplus_{j \in [1,n]} e_i A e_j \right) = \bigoplus_{i,j \in [1,n]} e_i A e_j .$$

**Beispiel 17** Sei  $K$  ein Körper. Sei  $A = K^{3 \times 3}$ . Wir haben die orthogonale Zerlegung in Idempotente  $\underline{e} = \left( \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$  in  $A$ . Dementsprechend wird

$$A = e_1 A e_1 \oplus e_2 A e_1 \oplus e_1 A e_2 \oplus e_2 A e_2 = \begin{pmatrix} K & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 0 \\ K & 0 & 0 \\ K & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & K & K \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 & 0 \\ 0 & K & K \\ 0 & K & K \end{pmatrix} .$$

Es ist  $e_1$  primitiv. Denn es ist  $e_1 A e_1$  ein Teilring von  $A$  (mit einer anderen 1), welcher isomorph zu  $K$  ist. Aus  $e_1 = e' + e''$  wie in Definition 14 folgt  $e_1 e' = (e' + e'')e' = e'$  etc., also  $e', e'' \in e_1 A e_1$ . Da  $e_1 A e_1$  ein Körper ist, folgt aber aus  $e' e'' = 0$ , daß  $e' = 0$  oder  $e'' = 0$ .

Es ist  $e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$  nicht primitiv.

**Bemerkung 18** Sei  $e \in A$  ein Idempotent. Es ist  $e$  primitiv genau dann, wenn  $Ae$  ein unzerlegbarer  $A$ -Modul ist, i.e. wenn  $Ae \neq 0$  und wenn aus einer Zerlegung  $Ae = X \oplus Y$  in  $A$ -Moduln bereits  $X = 0$  oder  $Y = 0$  folgt.

*Beweis.* Siehe Aufgabe 10. □

**Bemerkung 19** Sei  $A$  ein Ring. Seien  $e, f \in A$  Idempotente.

Es ist

$$\begin{aligned} \text{Hom}_A(Ae, Af) &\longrightarrow eAf \\ \varphi &\longmapsto \varphi(e) \\ (be \mapsto beaf) &\longleftarrow eaf \end{aligned}$$

ein Isomorphismus abelscher Gruppen, mit Inverser wie angegeben, wobei  $a, b \in A$ .

*Beweis.* Siehe Aufgabe 11. □

### 3.1.2 Halbeinfache Algebren

Sei  $K$  ein Körper.

#### Definition 20

- (1) Eine  $(K-)$ Algebra ist ein Paar  $(A, \varphi)$  aus einem Ring  $A$  und einem Ringmorphismus  $K \xrightarrow{\varphi} A$  mit  $\varphi(A) \subseteq Z(A)$ . Oft schreibt man kurz  $A = (A, \varphi)$ .  
Via  $\lambda \cdot a := \varphi(\lambda)a$  für  $\lambda \in K$  und  $a \in A$  wird  $A$  zu einem Vektorraum über  $K$ .  
Es ist e.g.  $K = (K, \text{id})$  eine  $K$ -Algebra.
- (2) Seien  $A = (A, \varphi)$  und  $B = (B, \psi)$   $K$ -Algebren. Ein  $(K-)$ Algebrenmorphismus  $A \xrightarrow{f} B$  ist ein Ringmorphismus von  $A$  nach  $B$ , für welchen  $f \circ \varphi = \psi$  ist.

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 \swarrow \varphi & & \nearrow \psi \\
 & K &
 \end{array}$$

Ein Ringmorphismus  $f : A \rightarrow B$  ist genau dann ein  $K$ -Algebrenmorphismus, wenn er zudem eine  $K$ -lineare Abbildung ist, da die Aussage  $f(\lambda \cdot a) = \lambda \cdot f(a)$  für  $\lambda \in K$  und  $a \in A$  äquivalent ist zur Aussage  $(f \circ \varphi)(\lambda)f(a) = \psi(\lambda)f(a)$  für  $\lambda \in K$  und  $a \in A$ , was wegen  $1 \in A$  wiederum äquivalent ist zu  $f \circ \varphi = \psi$ .

Es ist e.g.  $\varphi : K \rightarrow A$  ein  $K$ -Algebrenmorphismus.

Ein  $(K-)$ Algebrenisomorphismus, geschrieben  $A \xrightarrow{f} B$ , ist ein bijektiver  $K$ -Algebrenmorphismus.

Diesfalls ist auch seine Umkehrabbildung ein  $K$ -Algebrenisomorphismus.

Existiert ein  $K$ -Algebrenisomorphismus  $A \xrightarrow{f} B$ , so heißen  $A$  und  $B$  *isomorph*, geschrieben  $A \simeq B$ .

- (3) Es heißt  $A$  *endlichdimensional*, wenn  $A$  als  $K$ -Vektorraum endlichdimensional ist.  
Ein  $A$ -Modul  $M$  ist via  $\lambda \cdot m := \varphi(\lambda)m$  auch ein  $K$ -Vektorraum, wobei  $\lambda \in K$  und  $m \in M$ .  
Es heißt  $M$  *endlichdimensional*, falls  $M$  als  $K$ -Vektorraum endlichdimensional ist.
- (4) Eine endlichdimensionale  $K$ -Algebra  $A$  heißt *halbeinfach*, falls für jeden endlichdimensionalen  $A$ -Modul  $M$  und jeden Teilmodul  $N \subseteq M$  ein Teilmodul  $X \subseteq M$  mit  $M = N \oplus X$  existiert.

**Beispiel 21** Sei  $n \geq 0$ . Es ist  $K^{n \times n}$ , zusammen mit  $K \rightarrow Z(K^{n \times n})$ ,  $\lambda \mapsto \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix}$ , eine  $K$ -Algebra. Diese ist auch halbeinfach, wie wir in Aufgabe 14 sehen werden.

**Bemerkung 22** Sei  $A$  eine endlichdimensionale  $K$ -Algebra. Es gibt eine orthogonale Zerlegung in primitive Idempotente in  $A$ .

*Beweis.* Siehe Aufgabe 12. □

**Lemma 23** Sei  $A$  eine endlichdimensionale  $K$ -Algebra.

Die folgenden Aussagen (1), (2), (3) und (4) sind äquivalent.

- (1) Es ist  $A$  halbeinfach.
- (2) Es ist  $Ae$  einfach für jedes primitive Idempotent  $e \in A$ .
- (3) Es gibt eine orthogonale Zerlegung in primitive Idempotente  $\underline{e} = (e_1, \dots, e_n)$  in  $A$  so, daß  $A = \bigoplus_{i \in [1, n]} Ae_i$  und  $Ae_i$  ein einfacher  $A$ -Modul ist für  $i \in [1, n]$ .
- (4) Es gibt eine Zerlegung  $A = \bigoplus_{i \in [1, n]} S_i$  mit  $n \geq 0$  und einfachen  $A$ -Linksteilmoduln  $S_i$  für  $i \in [1, n]$ .

*Beweis.*

Zu (1)  $\Rightarrow$  (2). Sei  $0 \neq N \subseteq Ae$  ein Teilmodul. Wir haben  $N \stackrel{!}{=} Ae$  zu zeigen. Nach (1) gibt es einen Teilmodul  $X \subseteq Ae$  mit  $Ae = N \oplus X$ ; cf. Definition 20.(3). Da  $Ae$  unzerlegbar ist und da  $N \neq 0$ , folgt  $X = 0$ ; cf. Bemerkung 18. Also ist  $N$  als Kern der Projektion auf  $X$  gleich  $Ae$ .

Zu (2)  $\Rightarrow$  (3). Es gibt eine orthogonale Zerlegung in primitive Idempotente  $\underline{e} = (e_1, \dots, e_n)$  in  $A$ ; cf. Bemerkung 22. Es ist  $A = \bigoplus_{i \in [1, n]} Ae_i$ ; cf. Bemerkung 15. Nach (2) ist  $Ae_i$  einfach für  $i \in [1, n]$ .

Zu (3)  $\Rightarrow$  (4). Setze  $S_i := Ae_i$  für  $i \in [1, n]$ .

Zu (4)  $\Rightarrow$  (1). Sei  $M$  ein endlichdimensionaler  $A$ -Modul. Sei  $(m_1, \dots, m_\ell)$  eine  $K$ -lineare Basis von  $M$ . Es ist

$$\begin{array}{ccc} A^{\oplus \ell} & \xrightarrow{f} & M \\ (a_1, \dots, a_\ell) & \mapsto & \sum_{i \in [1, \ell]} a_i m_i \end{array}$$

eine surjektive  $A$ -lineare Abbildung.

Ist  $T \subseteq A^{\oplus \ell}$  ein einfacher Teilmodul, so ist  $f(T)$  isomorph zu  $T$  oder zu 0, da der Kern von  $f|_T$  gleich 0 oder gleich  $T$  ist; und somit ist  $f(T)$  einfach oder gleich 0.

Nun verwenden wir  $A = \bigoplus_{i \in [1, n]} S_i$ , wobei  $S_i$  ein einfacher  $A$ -Modul ist für  $i \in [1, n]$ . Also ist  $A^{\oplus \ell} = \bigoplus_{j \in [1, \ell n]} T_j$  für gewisse einfache Teilmoduln  $T_j$ . Wir erhalten

$$M = f(A^{\oplus \ell}) = f({}_A \langle T_j : j \in [1, \ell n] \rangle) = {}_A \langle f(T_j) : j \in [1, \ell n] \rangle.$$

Folglich ist  $M$  das  $A$ -lineare Erzeugnis seiner einfachen Teilmoduln.

Wegen  $M$  endlichdimensional hat jede nichtleere Teilmenge von

$$\{Y \subseteq M : Y \text{ ist Teilmodul}\}$$

ein maximales Element.

Sei nun  $N \subseteq M$  ein Teilmodul. Sei  $X \subseteq M$  maximal unter den Teilmoduln von  $M$ , die Schnitt 0 mit  $N$  haben. Wir wollen  $N \oplus X \stackrel{!}{=} M$  zeigen. *Annahme*,  $N \oplus X \subset M$ . Dann gibt es einen einfachen Teilmodul  $T \subseteq M$  mit  $T \not\subseteq N \oplus X$ , da  $M$  von seinen einfachen Teilmoduln erzeugt wird. Es ist  $(N \oplus X) \cap T \subset T$ . Wegen  $T$  einfach folgt hieraus, daß  $(N \oplus X) \cap T = 0$ . Dies liefert  $N \oplus X \oplus T \subseteq M$ , und also  $N \cap (X \oplus T) = 0$ , im *Widerspruch* zur Maximalität von  $X$ .  $\square$

**Lemma 24 (Schur)** *Sei  $A$  eine endlichdimensionale  $K$ -Algebra.*

*Seien  $S$  und  $T$  einfache  $A$ -Moduln.*

- (1) *Eine  $A$ -lineare Abbildung  $\varphi : S \rightarrow T$  ist ein Isomorphismus oder gleich 0.*
- (2) *Es ist  $\text{End}_A S$  ein Schiefkörper.*
- (3) *Es ist  $\text{Hom}_A(S, T) = 0$ , falls  $S \not\cong T$ .*
- (4) *Ist  $K$  algebraisch abgeschlossen, so ist  $\psi : K \rightarrow \text{End}_A S$ ,  $\lambda \mapsto \lambda \text{id}_S$  ein Isomorphismus von  $K$ -Algebren.*

*Beweis.*

Zu (1). Sei  $\varphi \in \text{Hom}_A(S, T) \setminus \{0\}$ . Wir wollen zeigen, daß  $\varphi$  ein Isomorphismus ist.

Da Kern  $\varphi \subseteq S$  ein Teilmodul ist, folgt aus  $S$  einfach, daß Kern  $\varphi \in \{0, S\}$ . Da  $\varphi \neq 0$ , folgt Kern  $\varphi = 0$ . Somit ist  $\varphi$  injektiv.

Da Im  $\varphi \subseteq T$  ein Teilmodul ist, folgt aus  $T$  einfach, daß Im  $\varphi \in \{0, T\}$ . Da  $\varphi \neq 0$ , folgt Im  $\varphi = T$ . Somit ist  $\varphi$  surjektiv.

Zu (2). Dank (1) ist jedes Element in  $(\text{End}_A S) \setminus \{0\}$  ein Isomorphismus, und damit invertierbar.

Zu (3). Gibt es in  $\text{Hom}_A(S, T)$  keine Isomorphismen, so gibt es darin dank (1) nur den Nullmorphimus.

Zu (4). Es ist  $\psi$  ein Morphismus von  $K$ -Algebren; cf. Aufgabe 15. Wir haben zu zeigen, daß  $\psi$  bijektiv ist.

Es ist Kern  $\psi$  ein Ideal im Körper  $K$ , mithin gleich 0 oder gleich  $K$ . Letzteres ist nicht möglich, da  $1 \in K$  auf die Identität auf  $S$  abgebildet wird und wegen  $S \neq 0$  auch  $\text{id}_S \neq 0$  ist. Somit ist  $\psi$  injektiv.

Es ist  $K' := \psi(K) \simeq K$  ein Teilkörper von  $D := \text{End}_A S$ . Sei  $\xi \in D$ . Wir haben  $\xi \stackrel{!}{\in} K'$  zu zeigen.

Wir *behaupten*, daß  $D$  endlichdimensional ist. Da  $\text{End}_A S \subseteq \text{End}_K S$  ein Teilraum ist, genügt es zu zeigen, daß  $S$  endlichdimensional ist. Sei  $s \in S \setminus \{0\}$ . Es ist die  $A$ -lineare Abbildung  $A \rightarrow S$ ,  $a \mapsto as$  ungleich 0. Wegen  $S$  einfach ist ihr Bild gleich  $S$ . Da  $A$  endlichdimensional und diese Abbildung auch  $K$ -linear ist, folgt die *Behauptung*.

Der Kern des Ringmorphismus  $K'[X] \rightarrow D$ ,  $f(X) \mapsto f(\xi)$  ist wegen  $D$  endlichdimensional ungleich 0 und hat somit einen normierten Idealerzeuger  $\mu_{\xi, K'}(X) \in K'[X]$ .

Es ist  $\mu_{\xi, K'}(X) \in K'[X]$  irreduzibel, da aus  $\mu_{\xi, K'}(X) = f(X)g(X)$  mit  $f(X), g(X) \in K'[X]$  normiert folgt, daß  $0 = \mu_{\xi, K'}(\xi) = f(\xi)g(\xi)$ , also, wegen  $D$  Schiefkörper,  $f(\xi) = 0$  oder  $g(\xi) = 0$ , und hieraus wiederum, daß  $\mu_{\xi, K'}(X)$  ein Teiler von  $f(X)$  oder von  $g(X)$  ist.

Da  $K$  algebraisch abgeschlossen ist, trifft dies auch für  $K'$  zu. Also ist  $\deg \mu_{\xi, K'} = 1$ , also  $\mu_{\xi, K'}(X) = X - \xi \in K'[X]$  und somit  $\xi \in K'$ .  $\square$

**Satz 25 (Wedderburn)** *Sei  $K$  algebraisch abgeschlossen.*

*Sei  $A$  eine endlichdimensionale  $K$ -Algebra.*

*Die folgenden Aussagen (1) und (2) sind äquivalent.*

- (1) *Es ist  $A$  halbeinfach.*
- (2) *Es gibt  $t \geq 0$  und  $m_s \geq 1$  für  $s \in [1, t]$  so, daß als  $K$ -Algebren*

$$A \simeq K^{m_1 \times m_1} \times \dots \times K^{m_t \times m_t} .$$

*Ein zugehöriger Isomorphismus heißt auch Wedderburnisomorphismus.*

*Beweis.*

Zu (2)  $\Rightarrow$  (1). Es ist  $K^{m_s \times m_s}$  halbeinfach für  $s \in [1, t]$ ; cf. Aufgabe 14.(1).

Also ist  $K^{m_1 \times m_1} \times \dots \times K^{m_t \times m_t}$  halbeinfach; cf. Aufgabe 14.(2).

Somit ist auch  $A$  halbeinfach; cf. Aufgabe 14.(3).

Zu (1)  $\Rightarrow$  (2). Sei  $(e_1, \dots, e_n)$  eine orthogonale Zerlegung in primitive Idempotente in  $A$ ; cf. Bemerkung 22. Es ist  $Ae_i$  ein einfacher  $A$ -Modul für  $i \in [1, n]$ ; cf. Lemma 23. Heißen  $i, j \in [1, n]$  äquivalent, geschrieben  $i \sim j$ , wenn  $Ae_i \simeq Ae_j$  als  $A$ -Moduln. Seien die  $e_i$  o.E. so angeordnet, daß die Äquivalenzklassen Intervalle sind. Seien die Äquivalenzklassen  $[n_0 + 1, n_1], [n_1 + 1, n_2], \dots, [n_{t-1} + 1, n_t]$  mit  $0 = n_0 < n_1 < \dots < n_{t-1} < n_t = n$ .

Wähle einen Isomorphismus  $\alpha_{i, n_s} : Ae_{n_s} \xrightarrow{\sim} Ae_i$  von  $A$ -Moduln für alle  $s \in [1, t]$  und alle  $i \in [n_{s-1} + 1, n_s]$ . Wähle dabei  $\alpha_{n_s, n_s} := \text{id}_{Ae_{n_s}}$ .

Für  $i \sim j \sim n_s$  setzen wir  $\alpha_{j, i} := \alpha_{j, n_s} \circ \alpha_{i, n_s}^{-1} : Ae_i \xrightarrow{\sim} Ae_j$ . Ist  $i = n_s$  für ein  $s \in [1, t]$ , so stimmt dies mit der bisherigen Definition überein. Für  $i \sim j \sim k \sim n_s$  ist dann

$$\alpha_{k, j} \circ \alpha_{j, i} = \alpha_{k, n_s} \circ \alpha_{j, n_s}^{-1} \circ \alpha_{j, n_s} \circ \alpha_{i, n_s}^{-1} = \alpha_{k, n_s} \circ \alpha_{i, n_s}^{-1} = \alpha_{k, i} .$$

Sei  $B := K^{(n_1-n_0) \times (n_1-n_0)} \times K^{(n_2-n_1) \times (n_2-n_1)} \times \dots \times K^{(n_t-n_{t-1}) \times (n_t-n_{t-1})}$ .

Ist  $s \in [1, t]$  und sind  $i, j \in [n_{s-1} + 1, n_s]$ , so sei  $\eta_{i,j}$  das Element von  $B$ , dessen  $s$ -ter Tupeleintrag an Matrixposition  $(i - n_{s-1}, j - n_{s-1})$  eine 1 aufweist, und Nullen sonst, und dessen übrige Tupeleinträge alle Nullmatrizen sind. Es ist

$$(\eta_{i,j} : i, j \in [1, n], i \sim j)$$

eine  $K$ -lineare Basis von  $B$ .

Wir erhalten eine  $K$ -lineare Abbildung durch die Setzung

$$\begin{array}{ccc} B & \xrightarrow{\omega} & A \\ \eta_{i,j} & \mapsto & \alpha_{j,i}(e_i) \end{array}$$

für  $i \sim j$ .

Beachte, daß dabei stets  $\alpha_{j,i}(e_i)$  in  $e_i A e_j$  liegt, da es ohnehin in  $A e_j$  liegt und zudem  $e_i \alpha_{j,i}(e_i) = \alpha_{j,i}(e_i e_i) = \alpha_{j,i}(e_i)$  ist.

*Wir wollen zeigen, daß  $\omega$  ein  $K$ -Algebrenisomorphismus ist.*

*Injektivität.* Es ist  $A = \bigoplus_{i,j \in [1, n]} e_i A e_j$  und  $\alpha_{j,i}(e_i) \in e_i A e_j \setminus \{0\}$  für  $i \sim j$ . Also ist das Bild unserer Basis linear unabhängig und  $\omega$  somit injektiv; cf. Lemma 16.

*Surjektivität.* Es genügt zu zeigen, daß

$$\dim_K A \stackrel{!}{=} \dim_K B = \sum_{s \in [1, t]} (n_s - n_{s-1})^2.$$

Wegen  $A = \bigoplus_{i,j \in [1, n]} e_i A e_j$  und  $|\{(i, j) \in [1, n] \times [1, n] : i \sim j\}| = \sum_{s \in [1, t]} (n_s - n_{s-1})^2$  genügt es zu zeigen, daß  $\dim_K e_i A e_j \stackrel{!}{=} 0$  für  $i \not\sim j$  und  $\dim_K e_i A e_j \stackrel{!}{=} 1$  für  $i \sim j$ .

Für  $i \not\sim j$  ist  $e_i A e_j \simeq \text{Hom}_A(A e_i, A e_j) = 0$ ; cf. Bemerkung 19, Lemma 24.(3). Also ist  $\dim_K e_i A e_j = 0$ .

Für  $i \sim j$  schränkt der  $A$ -lineare Isomorphismus  $\alpha_{j,i} : A e_i \xrightarrow{\sim} A e_j$  zu einem  $K$ -linearen Isomorphismus  $e_i A e_i \xrightarrow{\sim} e_i A e_j$  ein. Ferner ist  $e_i A e_i \simeq \text{Hom}_A(A e_i, A e_i) \simeq K$ ; cf. Bemerkung 19, Lemma 24.(4); wobei die Isomorphie insgesamt  $\lambda e_i \longleftarrow (a e_i \mapsto \lambda a e_i) \longleftarrow 1$  abbildet und somit  $K$ -linear ist. Also ist  $\dim_K e_i A e_j = 1$ .

*$K$ -Algebrenmorphismus.* Um zu zeigen, daß  $\omega$  ein  $K$ -Algebrenmorphismus ist, genügt es zu zeigen, daß  $\omega(\eta_{i,j} \eta_{k,\ell}) \stackrel{!}{=} \omega(\eta_{i,j}) \omega(\eta_{k,\ell})$  für  $i \sim j$  und  $k \sim \ell$ , und daß  $\omega(1_B) \stackrel{!}{=} 1_A$ .

Ist  $j \neq k$ , so wird zum einen  $\omega(\eta_{i,j} \eta_{k,\ell}) = \omega(0) = 0$ , und zum anderen  $\omega(\eta_{i,j}) \omega(\eta_{k,\ell}) \in e_i A e_j \cdot e_k A e_\ell = 0$ .

Ist  $j = k$ , so wird zum einen

$$\omega(\eta_{i,j} \eta_{j,\ell}) = \omega(\eta_{i,\ell}) = \alpha_{\ell,i}(e_i),$$

und zum anderen

$$\omega(\eta_{i,j}) \omega(\eta_{j,\ell}) = \alpha_{j,i}(e_i) \alpha_{\ell,j}(e_j) = \alpha_{\ell,j}(\alpha_{j,i}(e_i) e_j) = \alpha_{\ell,j}(\alpha_{j,i}(e_i)) = \alpha_{\ell,i}(e_i).$$

Schließlich ist  $\alpha_{i,i} = \alpha_{i,n_s} \circ \alpha_{i,n_s}^{-1} = \text{id}_{Ae_i}$  für  $i \in [1, n]$ , wobei  $i \sim n_s$ , und also

$$\omega(1_B) = \omega\left(\sum_{i \in [1, n]} \eta_{i,i}\right) = \sum_{i \in [1, n]} \omega(\eta_{i,i}) = \sum_{i \in [1, n]} \alpha_{i,i}(e_i) = \sum_{i \in [1, n]} e_i = 1_A.$$

□

Insbesondere folgt aus Satz 25 für  $K$  algebraisch abgeschlossen, daß man bei der Definition einer halbeinfachen endlichdimensionalen  $K$ -Algebra von der linken Seite auf die rechte Seite wechseln kann, was die Operation von  $A$  auf Moduln angeht, ohne den Begriff der Halbeinfachheit zu ändern; cf. Definition 20.(4), cf. auch Lemma 23.

Aus einem Wedderburnisomorphismus für  $\mathbf{C}G$  kann man problemlos die Charaktertafel ablesen; cf. §3.3.1 unten, Aufgabe 24. Dies setzt allerdings die Kenntnis der  $e_i$  und der  $\alpha_{j,i}$  voraus, in der Notation des Beweises zu Satz 25. Und da diese schwierig zu beschaffen sind, wollen wir das Problem der algorithmischen Konstruktion eines Wedderburnisomorphismus umgehen und auf anderem Wege zur Charaktertafel kommen.

## 3.2 Gruppenalgebren

Sei  $G$  eine endliche Gruppe, mit neutralem Element  $1 = 1_G$ .

### 3.2.1 Gruppenringe

Sei  $R \neq 0$  ein kommutativer Ring.

**Definition 26** Es bestehe  $RG$  als Menge aus den formalen  $R$ -Linearkombinationen der Elemente von  $G$ , i.e.

$$RG := \left\{ \sum_{g \in G} r_g g : r_g \in R \text{ für } g \in G \right\}^{(1)}.$$

Wir haben eine injektive Abbildung  $G \rightarrow RG$ ,  $h \mapsto \sum_g \partial_{g,h} h$ , welche wir zur Identifikation verwenden und so  $G$  als Teilmenge von  $RG$  betrachten.

Addition und Multiplikation auf  $RG$  sind für  $\sum_{g \in G} r_g g$ ,  $\sum_{g \in G} s_g g \in RG$  erklärt durch

$$\begin{aligned} \left( \sum_{g \in G} r_g g \right) + \left( \sum_{g \in G} s_g g \right) &= \sum_{g \in G} (r_g + s_g) g \\ \left( \sum_{g \in G} r_g g \right) \cdot \left( \sum_{h \in G} s_h h \right) &= \sum_{x \in G} \left( \sum_{g, h \in G, gh=x} r_g s_h \right) x \end{aligned}$$

Insbesondere ist  $g \cdot_G h = g \cdot_{RG} h$  für  $g, h \in G$ .

Es ist  $RG = (RG, +, \cdot)$  ein Ring; cf. Aufgabe 16.(1).

Das neutrale Element der Addition ist  $0_{RG} = \sum_g 0g \in RG$ .

Das neutrale Element der Multiplikation ist  $1_{RG} = 1_G \in RG$ .

<sup>1</sup>Formal kann  $RG$  als Menge der Abbildungen  $G \rightarrow R$ ,  $g \mapsto r_g$  aufgefaßt werden.

### 3.2.2 Maschke

Sei  $K$  ein Körper.

Es wird  $KG$  vermöge  $\varphi : K \rightarrow KG, \lambda \mapsto \lambda \cdot 1_G$  zu einer  $K$ -Algebra.

#### Lemma 27 (Maschke)

Es ist  $KG$  halbeinfach genau dann, wenn  $|G|$  kein Vielfaches von  $\text{char } K$  ist.

*Beweis.* Siehe Aufgabe 19. □

## 3.3 Charaktere

Sei  $G$  eine endliche Gruppe.

### 3.3.1 Definition

Wir wählen einen Wedderburnisomorphismus

$$\begin{aligned} \mathbf{C}G &\xrightarrow{\omega} \mathbf{C}^{n_1 \times n_1} \times \dots \times \mathbf{C}^{n_t \times n_t} =: B \\ \xi &\mapsto (\omega^1(\xi), \dots, \omega^t(\xi)); \end{aligned}$$

cf. Lemma 27, Satz 25. (Die oberen Indizes an  $\omega$  seien hierbei keine Exponenten.)

Schreibe dabei noch  $\omega^s(\xi) = (\omega_{i,j}^s(\xi))_{i,j} \in \mathbf{C}^{n_s \times n_s}$  für  $\xi \in \mathbf{C}G$  und  $s \in [1, t]$ .

Für  $s \in [1, t]$  und  $i, j \in [1, n_s]$  schreiben wir  $e_{i,j}^s \in \mathbf{C}^{n_1 \times n_1} \times \dots \times \mathbf{C}^{n_t \times n_t} = B$  für das Tupel, das an Position  $s$  die Matrix mit Eintrag 1 an Position  $(i, j)$  und Nullen sonst stehen hat, und ansonsten Nullmatrizen. Es ist  $(e_{i,i}^s : s \in [1, t], i \in [1, n_s])$  eine orthogonale Zerlegung in primitive Idempotente in  $B$ , da  $Be_{i,i}^s$  als einfacher  $B$ -Modul insbesondere unzerlegbar ist; cf. Aufgabe 10, Lösung zu Aufgabe 14.(1, 2).

Vermittels  $\omega$  betrachten wir kommentarlos einen  $B$ -Modul  $X$  auch als  $\mathbf{C}G$ -Modul. Dieselbenfalls ist dann  $\xi \cdot x := \omega(\xi) \cdot x$  für  $\xi \in \mathbf{C}G$  und  $x \in X$ . Umgekehrt betrachten wir einen  $\mathbf{C}G$ -Modul kommentarlos auch als  $B$ -Modul.

**Definition 28** Sei  $s \in [1, t]$ . Sei

$$\begin{aligned} \chi_s &: G \rightarrow \mathbf{C} \\ g &\mapsto \chi_s(g) := \text{tr } \omega^s(g) = \sum_{i \in [1, n_s]} \omega_{i,i}^s(g) \end{aligned}$$

Die Abbildungen  $\chi_1, \chi_2, \dots, \chi_t$  heißen *irreduzible (gewöhnliche) Charaktere* von  $G$ .

Ein (*gewöhnlicher*) *Charakter* von  $G$  ist eine Linearkombination irreduzibler Charaktere von  $G$  mit Koeffizienten in  $\mathbf{Z}_{\geq 0}$ .

Ein *virtueller Charakter* von  $G$  ist eine Linearkombination irreduzibler Charaktere von  $G$  mit Koeffizienten in  $\mathbf{Z}$ .

**Bemerkung 29** Es ist  $\chi_s(1) = n_s$  für  $s \in [1, t]$ .

**Bemerkung 30**

(1) Sei  $s \in [1, t]$ . Sind  $g$  und  $h$  in  $G$  konjugiert, so ist  $\chi_s(g) = \chi_s(h)$ .

(2) Die Anzahl der Konjugationsklassen in  $G$  beträgt  $t$ .

*Beweis.* Zu (1). Sei etwa  $h = x^{-1}gx$  mit  $x \in G$ . Dann wird

$$\omega^s(h) = \omega^s(x^{-1}gx) = \omega^s(x)^{-1}\omega^s(g)\omega^s(x),$$

und also

$$\chi_s(h) = \text{tr } \omega^s(h) = \text{tr}(\omega^s(x)^{-1}\omega^s(g)\omega^s(x)) = \text{tr } \omega^s(g) = \chi_s(g).$$

Zu (2). Siehe Aufgabe 22.(3). □

**Definition 31** Sei  $G = \bigsqcup_{s \in [1, t]} g_s^G$ , i.e. seien  $g_1, \dots, g_t$  Repräsentanten der Konjugationsklassen von  $G$ . Wähle insbesondere  $g_1 := 1$ .

Die (*gewöhnliche*) *Charaktertafel* von  $G$  ist definiert als

$$X = X(G) := (\chi_r(g_s))_{r, s \in [1, t]} \in \mathbf{C}^{t \times t}.$$

### 3.3.2 Der triviale Charakter

**Bemerkung 32** Es ist  $\{Be_{1,1}^1, \dots, Be_{1,1}^t\}$  ein Repräsentantensystem für die Isoklassen einfacher  $\mathbf{C}G$ -Moduln.

*Beweis.* Es ist  $B = \bigoplus_{s \in [1, t]} \bigoplus_{i \in [1, n_s]} Be_{i,i}^s$  eine Zerlegung in einfache  $B$ -Moduln; cf. Lösung zu Aufgabe 14.(1, 2).

Sei  $M$  ein einfacher  $\mathbf{C}G$ -Modul. Wir *behaupten*, daß es ein  $s \in [1, t]$  so gibt, daß  $M \stackrel{!}{\simeq} Be_{1,1}^s$ . Sei dazu  $m \in M \setminus \{0\}$  gewählt. Wir haben die  $B$ -lineare Abbildung  $f : B \rightarrow M, b \mapsto bm$ . Da diese nicht verschwindet, gibt es ein  $s \in [1, t]$  und ein  $i \in [1, n_s]$  mit  $f|_{Be_{i,i}^s} \neq 0$ , und also mit  $f|_{Be_{i,i}^s} : Be_{i,i}^s \rightarrow M$  einem Isomorphismus; cf. Lemma 24.(1). Schließlich ist  $Be_{i,i}^s \rightarrow Be_{1,1}^s, b \mapsto be_{i,1}^s$  ein Isomorphismus, mit Inversem  $Be_{1,1}^s \rightarrow Be_{i,i}^s, b \mapsto be_{1,i}^s$ . Die *Behauptung* ist gezeigt.

Seien  $s, s' \in [1, t]$  mit  $s \neq s'$ . Es operiert  $\sum_{i \in [1, n_s]} e_{i,i}^s$  identisch auf  $Be_{1,1}^s$ , aber annulliert  $Be_{1,1}^{s'}$ . Also sind diese beiden  $\mathbf{C}G$ -Moduln nicht isomorph. □

**Bemerkung 33** Wir können und werden die Numerierung der  $\omega^s$  so wählen, daß  $n_1 = 1$  und  $\omega^1(g) = 1 \in \mathbf{C} = \mathbf{C}^{1 \times 1}$  für  $g \in G$ . Insbesondere ist  $\chi_1(g) = 1$  für  $g \in G$ .

*Beweis.* Der triviale Gruppenmorphismus  $G \rightarrow \mathbf{U}(\mathbf{C}) = \mathbf{C} \setminus \{0\}$ ,  $g \mapsto 1$  läßt sich eindeutig zu einem  $\mathbf{C}$ -Algebrenmorphismus  $\alpha : \mathbf{CG} \rightarrow \mathbf{C}$ ,  $\sum_g z_g g \mapsto \sum_g z_g$  fortsetzen; cf. Aufgabe 16.(2). Dies liefert den einfachen (da eindimensionalen)  $\mathbf{CG}$ -Modul  $M := \mathbf{C}$ , mit der Multiplikation  $\xi \cdot m := \alpha(\xi)m$  für  $\xi \in \mathbf{CG}$  und  $m \in M$ . Insbesondere ist  $g \cdot m = m$  für  $g \in G$  und  $m \in M$ .

Nach Bemerkung 32 gibt es o.E.  $\varphi : Be_{1,1}^1 \xrightarrow{\sim} M$ . Ein Dimensionsvergleich gibt  $n_1 = 1$ . Es ist  $\omega^1(g) = 1$  für  $g \in G$ , denn  $\varphi(\omega^1(g) \cdot e_{1,1}^1) = \varphi(g \cdot e_{1,1}^1) = g \cdot \varphi(e_{1,1}^1) = \alpha(g) \cdot \varphi(e_{1,1}^1) = \varphi(e_{1,1}^1)$ .  $\square$

Somit hat die Charaktertafel von  $G$  die Form

$$X = X(G) = \begin{array}{c} \chi_1 \\ \chi_2 \\ \vdots \\ \chi_t \end{array} \begin{array}{cccc} g_1 = 1 & g_2 & \cdots & g_t \\ \left[ \begin{array}{cccc} 1 & 1 & \cdots & 1 \\ n_2 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ n_t & * & \cdots & * \end{array} \right] \end{array}$$

### 3.3.3 Unabhängigkeit von der Wahl des Wedderburnisomorphismus $\omega$

Für einen Ring  $A$ , für  $a \in A$  und für einen  $A$ -Modul  $M$  schreiben wir

$$\ell_M(a) : M \rightarrow M, \quad m \mapsto am.$$

**Bemerkung 34** Sei  $s \in [1, t]$ . Sei  $i \in [1, n_s]$ . Sei  $\xi \in \mathbf{CG}$ . Es ist  $\omega^s(\xi)$  die beschreibende Matrix von  $\ell_{Be_{i,i}^s}(\xi)$  bezüglich der  $\mathbf{C}$ -linearen Basis  $(e_{1,i}^s, \dots, e_{n_s,i}^s)$  von  $Be_{i,i}^s$ .

Insbesondere ist  $\text{tr}(\ell_{Be_{i,i}^s}(g)) = \chi_s(g)$  für  $g \in G$ .

*Beweis.* Für  $j \in [1, n_s]$  ist  $(\ell_{Be_{i,i}^s}(\xi))(e_{j,i}^s) = \xi \cdot e_{j,i}^s = \omega^s(\xi)e_{j,i}^s = \sum_{k \in [1, n_s]} \omega_{k,j}^s(\xi)e_{k,i}^s$ .  $\square$

**Bemerkung 35** Sei  $N_1, \dots, N_t$  ein Repräsentantensystem für die Isoklassen der einfachen  $\mathbf{CG}$ -Moduln. Setze  $\tilde{\chi}_s(g) := \text{tr}(\ell_{N_s}(g))$  für  $s \in [1, t]$  und  $g \in G$ . Es gibt eine Bijektion  $\sigma : [1, t] \rightarrow [1, t]$  mit

$$\tilde{\chi}_s = \chi_{\sigma(s)}$$

für  $s \in [1, t]$ .

Es folgt, daß  $\chi_1, \dots, \chi_t$  bis auf Numerierung nicht von der Wahl des Wedderburnisomorphismus  $\omega$  abhängen; cf. Bemerkung 32.

Ferner können wir festhalten, daß die irreduziblen Charaktere von  $G$  gerade die Abbildungen von der Form  $G \rightarrow \mathbf{C}$ ,  $g \mapsto \text{tr}(\ell_M(g))$ , wobei  $M$  ein irreduzibler  $\mathbf{CG}$ -Modul ist, sind.

*Beweis.* Mit Bemerkungen 32 und 34 bleibt zu zeigen, daß für endlichdimensionale  $\mathbf{C}G$ -Moduln  $N, N'$  und einen Isomorphismus  $f : N \xrightarrow{\sim} N'$  auch

$$\mathrm{tr}(\ell_N(g)) = \mathrm{tr}(\ell_{N'}(g))$$

ist für  $g \in G$ . Dies aber folgt aus  $f \circ \ell_N(g) = \ell_{N'}(g) \circ f$ .  $\square$

### 3.3.4 Orthogonalitätsrelationen

**Lemma 36** *Sei  $g \in G$ . Es ist*

$$\sum_{s \in [1, t]} n_s \chi_s(g) = \partial_{g,1} |G|.$$

*Beweis.* Wir schreiben weiterhin  $B := \prod_{s \in [1, t]} \mathbf{C}^{n_s \times n_s}$ . Via  $\omega$  ist  $B$  auch ein  $\mathbf{C}G$ -Modul.

Sei  $g \in G$ . Wir haben folgendes kommutative Viereck von  $\mathbf{C}$ -linearen Abbildungen; cf. §3.3.3.

$$\begin{array}{ccc} \mathbf{C}G & \xrightarrow{\omega} & B \\ \ell_{\mathbf{C}G}(g) \downarrow & & \downarrow \ell_B(g) \\ \mathbf{C}G & \xrightarrow{\omega} & B \end{array}$$

Denn für  $\xi \in \mathbf{C}G$  ist  $\omega((\ell_{\mathbf{C}G}(g))(\xi)) = \omega(g \cdot \xi) = \omega(g) \cdot \omega(\xi) \stackrel{\text{Def.}}{=} g \cdot \omega(\xi) = (\ell_B(g))\omega(\xi)$ .

Folglich ist  $\mathrm{tr} \ell_{\mathbf{C}G}(g) = \mathrm{tr}(\omega^{-1} \circ \ell_B(g) \circ \omega) = \mathrm{tr} \ell_B(g)$ .

*Berechnung von  $\mathrm{tr} \ell_{\mathbf{C}G}(g)$ ,* in der  $\mathbf{C}$ -linearen Basis  $G$  von  $\mathbf{C}G$ . Wir erhalten

$$\mathrm{tr} \ell_{\mathbf{C}G}(g) = \partial_{g,1} |G|,$$

da für  $g \neq 1$  kein Gruppenelement auf sich, sondern auf ein anderes Gruppenelement abgebildet wird; cf. auch Lösung zu Aufgabe 20.(2).

*Berechnung von  $\mathrm{tr} \ell_B(g)$ .* Wir haben die Zerlegung

$$B = \bigoplus_{s \in [1, t]} \bigoplus_{i \in [1, n_s]} B e_{i,i}^s$$

in  $\mathbf{C}G$ -Teilmoduln. In  $B e_{i,i}^s$  wählen wir die  $\mathbf{C}$ -lineare Basis  $(e_{1,i}^s, \dots, e_{n_s,i}^s)$ . Diese Basen setzen wir zu einer Basis von  $B$  zusammen.

Da eine Zerlegung in  $\mathbf{C}G$ -Teilmoduln vorliegt, ergibt sich in dieser Basis die beschreibende Matrix von  $\ell_B(g)$  als Blockdiagonalmatrix mit den beschreibenden Matrizen von  $\ell_B(g)|_{B e_{i,i}^s} = \ell_{B e_{i,i}^s}(g)$  als Diagonalblöcken, wobei  $s \in [1, t]$  und  $i \in [1, n_s]$ . Eine solche Matrix ist aber eben durch  $\omega^s(g)$  gegeben, abhängig von  $s \in [1, t]$ , aber unabhängig von  $i \in [1, n_s]$ ; cf. Bemerkung 34. Wir summieren über alle diese Diagonalblöcke und erhalten

$$\mathrm{tr} \ell_B(g) = \sum_{s \in [1, t]} \sum_{i \in [1, n_s]} \mathrm{tr} \omega^s(g) = \sum_{s \in [1, t]} \sum_{i \in [1, n_s]} \chi_s(g) = \sum_{s \in [1, t]} n_s \chi_s(g).$$

$\square$

Für  $s \in [1, t]$  schreiben wir

$$\varepsilon_s := \omega^{-1} \left( \sum_{i \in [1, n_s]} e_{i,i}^s \right) \in \mathbf{CG}.$$

Da  $(\sum_{i \in [1, n_1]} e_{i,i}^1, \dots, \sum_{i \in [1, n_t]} e_{i,i}^t)$  die orthogonale Zerlegung in primitive Idempotente in  $Z(B)$  ist und da  $\omega$  ein Ringisomorphismus ist, ist auch  $(\varepsilon_1, \dots, \varepsilon_t)$  die orthogonale Zerlegung in primitive Idempotente in  $Z(\mathbf{CG})$ ; cf. Aufgaben 22.(1) und 21.

**Lemma 37** Für  $s \in [1, t]$  ist

$$\varepsilon_s = \frac{n_s}{|G|} \sum_{g \in G} \chi_s(g^{-1}) g.$$

*Beweis.* Schreibe  $\varepsilon_s =: \sum_g z_g^s g$  für  $s \in [1, t]$ , wobei  $z_g^s \in \mathbf{C}$ . Für  $h \in G$  und  $r \in [1, t]$  wird zum einen

$$\omega^r(\varepsilon_s \cdot h) = \omega^r(\varepsilon_s) \cdot \omega^r(h) = \partial_{s,r} \omega^r(h)$$

und zum anderen

$$\omega^r(\varepsilon_s \cdot h) = \omega^r(\sum_g z_g^s gh) = \sum_g z_g^s \omega^r(gh).$$

Anwenden von  $\text{tr}$  auf beide resultierende Terme und Summation über  $r$  mit einem Faktor  $n_r$  gewichtet gibt

$$\begin{aligned} n_s \chi_s(h) &= \sum_r n_r \partial_{s,r} \chi_r(h) \\ &= \sum_r n_r \text{tr}(\partial_{s,r} \omega^r(h)) \\ &= \sum_r n_r \text{tr}(\sum_g z_g^s \omega^r(gh)) \\ &= \sum_g z_g^s \sum_r n_r \chi_r(gh) \\ &\stackrel{\text{L. 36}}{=} \sum_g z_g^s \partial_{gh,1} |G| \\ &= z_{h^{-1}}^s |G|. \end{aligned}$$

Es folgt  $z_{h^{-1}}^s = \frac{n_s}{|G|} \chi_s(h)$ , also auch  $z_g^s = \frac{n_s}{|G|} \chi_s(g^{-1})$  für  $g \in G$ , wie zu zeigen war.  $\square$

Wir schreiben  $\overline{a + bi} := a - bi$  für  $a, b \in \mathbf{R}$ .

**Satz 38 (Orthogonalitätsrelationen)**

(1) Seien  $r, s \in [1, t]$ . Es ist

$$\sum_{g \in G} \chi_r(g) \overline{\chi_s(g)} = |G| \partial_{r,s}.$$

(2) Seien  $g, h \in G$ . Es ist

$$\sum_{s \in [1, t]} \chi_s(g) \overline{\chi_s(h)} = \partial_{g^c, h^c} |G| |g^G|^{-1}.$$

*Beweis.* Zu (1). Es ist

$$\partial_{r,s} \frac{n_s}{|G|} \sum_x \chi_s(x^{-1})x \stackrel{\text{L.37}}{=} \partial_{r,s} \varepsilon_s = \varepsilon_s \varepsilon_r \stackrel{\text{L.37}}{=} \frac{n_s n_r}{|G|^2} \sum_x \left( \sum_{gh=x} \chi_s(g^{-1}) \chi_r(h^{-1}) \right) x .$$

Koeffizientenvergleich bei  $x = 1$  liefert

$$\partial_{r,s} \frac{n_s^2}{|G|} = \frac{n_s n_r}{|G|^2} \sum_g \chi_s(g^{-1}) \chi_r(g) ,$$

$$\text{d.h. } |G| \partial_{r,s} = \sum_g \chi_r(g) \chi_s(g^{-1}) .$$

Die Aussage folgt nun wegen  $\chi_s(g^{-1}) = \overline{\chi_s(g)}$ ; cf. Aufgabe 23.(2).

Zu (2). Wir erinnern an die Charaktertafel  $X = X(G) = (\chi_r(g_s))_{r,s}$ ; cf. Definition 31. Sei

$$Y := |G|^{-1/2} X \begin{pmatrix} |g_1^G|^{1/2} & & \\ & \ddots & \\ & & |g_t^G|^{1/2} \end{pmatrix} .$$

Die Aussage (1) bedeutet

$$E_t = |G|^{-1} X \begin{pmatrix} |g_1^G| & & \\ & \ddots & \\ & & |g_t^G| \end{pmatrix} \bar{X}^t = Y \bar{Y}^t ,$$

i.e.  $Y$  unitär. Vertauschung der Faktoren gibt

$$E_t = \bar{Y}^t Y = |G|^{-1} \begin{pmatrix} |g_1^G|^{1/2} & & \\ & \ddots & \\ & & |g_t^G|^{1/2} \end{pmatrix} \bar{X}^t X \begin{pmatrix} |g_1^G|^{1/2} & & \\ & \ddots & \\ & & |g_t^G|^{1/2} \end{pmatrix} ,$$

i.e.

$$\bar{X}^t X = |G| \begin{pmatrix} |g_1^G|^{-1} & & \\ & \ddots & \\ & & |g_t^G|^{-1} \end{pmatrix} ,$$

i.e.

$$\sum_q \overline{\chi_q(g_r)} \chi_q(g_s) = \partial_{r,s} |G| |g_r^G|^{-1}$$

für  $r, s \in [1, t]$ , i.e.

$$\sum_q \chi_q(g) \overline{\chi_q(h)} = \partial_{g^G, h^G} |G| |g^G|^{-1}$$

für  $g, h \in G$ . □

Es ist Lemma 36 ein Spezialfall von (2).

### 3.4 Der Dixon-Algorithmus

Sei  $G$  eine endliche Gruppe. Sei  $G = \bigsqcup_{s \in [1, t]} g_s^G$ , mit  $g_1 = 1$ .

Schreibe  $e := \text{kgV}(|\langle g_1 \rangle|, \dots, |\langle g_t \rangle|)$  für den *Exponenten* von  $G$ .

Sei ferner  $p$  die kleinste Primzahl mit  $p > |G|$  und mit  $p \equiv_e 1$ ; cf. Aufgabe 32.

Sei

$$\begin{aligned} \mathbf{C}G &\xrightarrow[\sim]{\omega} \mathbf{C}^{n_1 \times n_1} \times \dots \times \mathbf{C}^{n_t \times n_t} =: B \\ \xi &\longmapsto (\omega^1(\xi), \dots, \omega^t(\xi)); \end{aligned}$$

ein Wedderburnisomorphismus, mit  $\omega^1(g) = 1$  für  $g \in G$ .

Es ist  $\chi_s(g) = \text{tr } \omega^s(g) \in \mathbf{Z}[\zeta_e]$  für  $g \in G$  und  $s \in [1, t]$ ; cf. Aufgabe 23.(1).

Für  $s \in [1, t]$  schreiben wir

$$K_s := \sum_{x \in g_s^G} x.$$

Es ist  $(K_s)_{s \in [1, t]}$  eine  $\mathbf{C}$ -lineare Basis von  $Z(\mathbf{C}G)$ , linear unabhängig nach Konstruktion und erzeugend nach Aufgabe 22.(2).

#### 3.4.1 Ein Isomorphismus von Zentren

Wir wollen Aufgabe 22.(1) etwas präzisieren.

Für  $\xi \in Z(\mathbf{C}G)$  und  $s \in [1, t]$  ist  $\omega^s(\xi) = \omega_Z^s(\xi) \cdot E_{n_s}$  für ein eindeutig bestimmtes  $\omega_Z^s(\xi) \in \mathbf{C}$ .

Dies gibt folgendes kommutative Viereck

$$\begin{array}{ccc} \mathbf{C}G & \xrightarrow[\sim]{\omega} & \mathbf{C}^{n_1 \times n_1} \times \dots \times \mathbf{C}^{n_t \times n_t} = B & & (z_s E_{n_s})_s \\ \uparrow & & \uparrow \varphi & & \uparrow \\ Z(\mathbf{C}G) & \xrightarrow{\omega_Z} & \mathbf{C} \times \dots \times \mathbf{C} = \mathbf{C}^{\times t} & & (z_s)_s \end{array}$$

$$\xi \longmapsto \omega_Z(\xi) := (\omega_Z^s(\xi))_s$$

Hierbei ist auch  $\omega_Z$  ein  $\mathbf{C}$ -Algebrenmorphismus, da  $\varphi$  ein injektiver  $\mathbf{C}$ -Algebrenmorphismus ist und wir für  $\xi, \tilde{\xi} \in Z(\mathbf{C}G)$  und  $\lambda, \tilde{\lambda} \in \mathbf{C}$

$$\begin{aligned} \varphi(\omega_Z(1)) &= \omega(1) = 1 & & = \varphi(1) \\ \varphi(\omega_Z(\xi \tilde{\xi})) &= \omega(\xi \tilde{\xi}) = \omega(\xi) \omega(\tilde{\xi}) &= \varphi(\omega_Z(\xi)) \varphi(\omega_Z(\tilde{\xi})) &= \varphi(\omega_Z(\xi) \omega_Z(\tilde{\xi})) \\ \varphi(\omega_Z(\lambda \xi + \tilde{\lambda} \tilde{\xi})) &= \omega(\lambda \xi + \tilde{\lambda} \tilde{\xi}) = \lambda \omega(\xi) + \tilde{\lambda} \omega(\tilde{\xi}) &= \lambda \varphi(\omega_Z(\xi)) + \tilde{\lambda} \varphi(\omega_Z(\tilde{\xi})) &= \varphi(\lambda \omega_Z(\xi) + \tilde{\lambda} \omega_Z(\tilde{\xi})) \end{aligned}$$

haben.

Es ist  $\omega_Z$  injektiv, aus Dimensionsgründen also bijektiv.

**Bemerkung 39** *Es ist*

$$\beta_{r,s} := \omega_Z^r(K_s) = \chi_r(g_s) \cdot \frac{|g_s^G|}{n_r} \in \mathbf{Q}(\zeta_e)$$

für  $r, s \in [1, t]$ . Insbesondere ist  $\beta_{r,1} = 1$  für  $r \in [1, t]$ , sowie  $\beta_{1,s} = |g_s^G|$  für  $s \in [1, t]$ .

*Beweis.* Es ist

$$\begin{aligned} \chi_r(g_s) \cdot |g_s^G| &= \sum_{x \in g_s^G} \chi_r(x) \\ &= \sum_{x \in g_s^G} \operatorname{tr} \omega^r(x) \\ &= \operatorname{tr} \omega^r(K_s) \\ &= \operatorname{tr}(\omega_Z^r(K_s) \mathbf{E}_{n_r}) \\ &= n_r \omega_Z^r(K_s). \end{aligned}$$

□

**Bemerkung 40** *Es ist  $(\beta_{r,s})_{r,s} \in \operatorname{GL}_t(\mathbf{C})$ .*

*Beweis.* Es ist  $(\beta_{r,s})_{r,s}$  eine beschreibende Matrix der bijektiven  $\mathbf{C}$ -linearen Abbildung  $\omega_Z$ . □

**Bemerkung 41** *Für  $s \in [1, t]$  sei  $s' \in [1, t]$  durch  $g_{s'}^G = (g_s^{-1})^G$  definiert. Es ist*

$$\sum_{s \in [1, t]} \beta_{r,s} \beta_{r,s'} |g_s^G|^{-1} = \frac{|G|}{n_r^2}.$$

*Beweis.* Es ist  $|g_s^G| = |g_{s'}^G|$  für  $s \in [1, t]$ , da die Bijektion  $G \rightarrow G$ ,  $x \mapsto x^{-1}$  zu einer Bijektion  $g_s^G \rightarrow g_{s'}^G$  einschränkt.

Es ist  $\chi_r(g_{s'}) = \overline{\chi_r(g_s)}$ ; cf. Aufgabe 23.(2), Bemerkung 30.(1).

Es wird

$$\begin{aligned} \sum_{s \in [1, t]} \beta_{r,s} \beta_{r,s'} |g_s^G|^{-1} &\stackrel{\text{B. 39}}{=} \sum_{s \in [1, t]} \chi_r(g_s) \cdot \frac{|g_s^G|}{n_r} \cdot \chi_r(g_{s'}) \cdot \frac{|g_{s'}^G|}{n_r} |g_s^G|^{-1} \\ &= \sum_{s \in [1, t]} \chi_r(g_s) \cdot \overline{\chi_r(g_s)} \cdot |g_s^G| \cdot \frac{1}{n_r^2} \\ &\stackrel{\text{S. 38.(1)}}{=} |G| \cdot \frac{1}{n_r^2}. \end{aligned}$$

□

Seien  $r, s \in [1, t]$ . Es ist  $K_r \cdot K_s \in Z(\mathbf{CG})$ . Also können wir

$$K_r \cdot K_s =: \sum_{a \in [1, t]} \gamma_{r,s,a} K_a$$

setzen, mit eindeutig bestimmten  $\gamma_{r,s,a} \in \mathbf{C}$ .

**Bemerkung 42** Seien  $q, r \in [1, t]$ .

Es ist

$$\beta_{q,r} \beta_{q,s} = \sum_{a \in [1, t]} \gamma_{r,s,a} \beta_{q,a}$$

für  $s \in [1, t]$ .

Als Matrixgleichung geschrieben, besagt dies, daß

$$\beta_{q,r} (\beta_{q,s})_s = (\gamma_{r,s,a})_{s,a} (\beta_{q,a})_a .$$

Es ist also  $(\beta_{q,a})_a$  ein Eigenvektor von  $(\gamma_{r,s,a})_{s,a}$  zum Eigenwert  $\beta_{q,r}$ .

*Beweis.* Mit der definierenden Gleichung für  $\gamma_{r,s,a}$  erhalten wir

$$\begin{aligned} \beta_{q,r} \beta_{q,s} &= \omega_{\mathbf{Z}}^q(K_r) \omega_{\mathbf{Z}}^q(K_s) \\ &= \omega_{\mathbf{Z}}^q(K_r K_s) \\ &= \omega_{\mathbf{Z}}^q\left(\sum_{a \in [1, t]} \gamma_{r,s,a} K_a\right) \\ &= \sum_{a \in [1, t]} \gamma_{r,s,a} \omega_{\mathbf{Z}}^q(K_a) \\ &= \sum_{a \in [1, t]} \gamma_{r,s,a} \beta_{q,a} . \end{aligned}$$

□

**Bemerkung 43** Seien  $r, s, a \in [1, t]$ . Es ist

$$\gamma_{r,s,a} = |\{(x, y) \in g_r^G \times g_s^G : xy = g_a\}| \in \mathbf{Z}_{\geq 0} .$$

*Beweis.* Dies folgt aus der definierenden Gleichung für  $\gamma_{r,s,a}$  und der Berechnung von  $K_r K_s$  in CG. □

### 3.4.2 Eine Betrachtung modulo $p$

Folgende Bemerkung werden wir erst in §4.6.2 zeigen können (ohne dort auf die nun folgenden Entwicklungen Bezug zu nehmen).

**Bemerkung 44** Sei  $m \geq 1$ . Ist  $\lambda \in \mathbf{Q}(\zeta_m)$  eine Nullstelle eines normierten Polynoms in  $\mathbf{Z}[X]$ , so ist  $\lambda \in \mathbf{Z}[\zeta_m]$ .

*Verweis.* Siehe Definition 52 und Satz 89 unten. □

**Bemerkung 45** Es ist  $\beta_{q,r} \in \mathbf{Z}[\zeta_m]$  für  $q, r \in [1, t]$ .

*Beweis.* Mit den Bemerkungen 39 und 44 genügt es anzumerken, daß  $\beta_{q,r}$  dank Bemerkungen 42 und 43 ein Eigenwert der Matrix  $(\gamma_{r,s,a})_{s,a} \in \mathbf{Z}^{t \times t}$  ist.

**Bemerkung 46** Wir können und werden einen surjektiven Ringmorphismus

$$\theta : \mathbf{Z}[\zeta_e] \longrightarrow \mathbf{F}_p$$

wählen mit  $\theta(\zeta_e)$  von Ordnung  $e$  in  $U(\mathbf{F}_p) = \mathbf{F}_p \setminus \{0\}$ . Wir schreiben dann  $\bar{\zeta}_e := \theta(\zeta_e)$ .

Es ist  $\theta|_{\mathbf{Z}} : \mathbf{Z} \longrightarrow \mathbf{F}_p$  die Restklassenabbildung.

*Beweis.* Sei  $\Phi_e(X) \in \mathbf{Z}[X]$  das  $e$ -te Kreisteilungspolynom. Es ist  $\Phi_e(X) = \mu_{\zeta_e, \mathbf{Q}}(X)$ . Wir haben einen Ringisomorphismus  $\mathbf{Z}[X]/\langle \Phi_e(X) \rangle \xrightarrow{\sim} \mathbf{Z}[\zeta_e]$ ,  $X + \langle \Phi_e(X) \rangle \mapsto \zeta_e$ . Also genügt es, in  $\mathbf{F}_p$  eine Nullstelle von  $\Phi_e(X)$  zu finden, die in  $U(\mathbf{F}_p)$  die Ordnung  $e$  hat, und die also als Bild von  $X + \langle \Phi_e(X) \rangle$ , und damit via Komposition auch als Bild von  $\zeta_e$ , Verwendung finden kann. Nun ist  $U(\mathbf{F}_p)$  eine zyklische Gruppe von Ordnung  $p - 1$ . Da  $e$  ein Teiler von  $p - 1$  ist, gibt es in  $U(\mathbf{F}_p)$  genau eine zyklische Untergruppe von Ordnung  $e$ . Sei  $\bar{\zeta}_e$  ein Erzeuger dieser Untergruppe, so daß  $\bar{\zeta}_e$  in  $U(\mathbf{F}_p)$  die Ordnung  $e$  hat. Bleibt zu zeigen, daß  $\Phi_e(\bar{\zeta}_e) \stackrel{!}{=} 0$  in  $\mathbf{F}_p$ . Es ist

$$X^e - 1 = \prod_{d|e} \Phi_d(X).$$

Da  $\mathbf{F}_p$  ein Körper und  $\bar{\zeta}_e$  dort eine Nullstelle von  $X^e - 1$  ist, ist  $\bar{\zeta}_e$  dort eine Nullstelle von  $\Phi_d(X)$  für ein  $d|e$ . Wäre  $\bar{\zeta}_e$  eine Nullstelle von  $\Phi_d(X)$  für ein  $d|e$  mit  $d \neq e$ , dann wäre  $\bar{\zeta}_e$  auch eine Nullstelle von  $X^d - 1$ , was aber der Ordnung von  $\bar{\zeta}_e$  widerspricht. Also ist  $\bar{\zeta}_e$  eine Nullstelle von  $\Phi_e(X)$ .

Schließlich ist  $\theta|_{\mathbf{Z}} : \mathbf{Z} \longrightarrow \mathbf{F}_p$  die Restklassenabbildung, da es genau einen Ringmorphismus von  $\mathbf{Z}$  nach  $\mathbf{F}_p$  gibt.  $\square$

**Lemma 47** Es ist  $(\theta(\beta_{r,s}))_{r,s} \in \mathrm{GL}_t(\mathbf{F}_p)$ .

Das liefert erneut, daß  $(\beta_{r,s})_{r,s} \in \mathrm{GL}_t(\mathbf{C})$ ; cf. Bemerkung 40.

*Beweis.* Es ist

$$\sum_r \beta_{q,r} \cdot n_s \chi_s(g_r^{-1}) \stackrel{\text{B.39}}{=} \sum_r \chi_q(g_r) \frac{|g_r^G|}{n_q} \cdot n_s \chi_s(g_r^{-1}) \stackrel{\text{S.38.(1)}}{=} |G| \partial_{q,s} \frac{n_s}{n_q} = |G| \partial_{q,s}$$

für  $q, r \in [1, t]$ . Also ist  $(\beta_{r,s})_{r,s} \cdot (n_s \chi_s(g_r^{-1}))_{r,s} = |G| \mathbf{E}_t$ , und somit

$$(\theta(\beta_{r,s}))_{r,s} \cdot (\theta(n_s \chi_s(g_r^{-1})))_{r,s} = \theta(|G|) \mathbf{E}_t;$$

cf. Aufgabe 23.(1). Da  $p > |G|$ , ist  $\theta(|G|)$  invertierbar.  $\square$

**Lemma 48** Es sind  $(\theta(\beta_{q,a}))_a$  für  $q \in [1, r]$  die einzigen gemeinsamen Eigenvektoren von  $(\theta(\gamma_{r,s,a}))_{s,a}$  für  $r \in [1, t]$  mit erstem Eintrag gleich 1.

*Beweis.* Für  $q, r \in [1, t]$  ist  $(\beta_{q,a})_a$  ein Eigenvektor von  $(\gamma_{r,s,a})_{s,a}$  zum Eigenwert  $\beta_{q,r}$  mit erstem Eintrag  $\beta_{q,1} = 1$ ; cf. Bemerkungen 39 und 42.

Für  $q, r \in [1, t]$  ist also  $(\theta(\beta_{q,a}))_a$  ein Eigenvektor von  $(\theta(\gamma_{r,s,a}))_{s,a}$  zum Eigenwert  $\theta(\beta_{q,r})$  mit erstem Eintrag gleich  $\theta(\beta_{q,1}) = 1$ .

*Annahme,* es ist  $x \in \mathbf{F}_p^{t \times 1} \setminus \left( \bigcup_{q \in [1, t]} \mathbf{F}_p \langle (\theta(\beta_{q,a}))_a \rangle \right)$  ein Eigenvektor von  $(\theta(\gamma_{r,s,a}))_{s,a}$  für  $r \in [1, t]$ .

Schreibe  $x = \sum_{q \in [1, t]} \lambda_q (\theta(\beta_{q,a}))_a$  mit  $\lambda_q \in \mathbf{F}_p$ ; cf. Lemma 47. Nach Annahme enthält der Träger  $T := \{q \in [1, t] : \lambda_q \neq 0\}$  mindestens zwei Elemente.

Dank Lemma 47 ist das Tupel  $\left( (\theta(\beta_{q,a}))_a \right)_{q \in T}$  linear unabhängig.

Mit Aufgabe 29 folgt, unter Verwendung von Lemma 47 für die verlangte lineare Unabhängigkeit, daß  $\theta(\beta_{q,r}) = \theta(\beta_{\tilde{q},r})$  für alle  $q, \tilde{q} \in T$  und alle  $r \in [1, t]$ . In anderen Worten, die Zeilen mit Index in  $T$  der Matrix  $(\theta(\beta_{r,s}))_{r,s}$  stimmen überein. Da  $|T| \geq 2$ , ist dies ein *Widerspruch* zur Regularität dieser Matrix; cf. Lemma 47.  $\square$

### 3.4.3 Charakterwerte rekonstruieren von Betrachtung modulo $p$

**Bemerkung 49** Seien  $k, \ell \in \mathbf{Z}$ . Es ist  $\sum_{i \in [0, e-1]} \bar{\zeta}_e^{-i\ell} \bar{\zeta}_e^{ik} = \theta(\partial_{k+e\mathbf{Z}, \ell+e\mathbf{Z}} \cdot e)$ .

*Beweis.* Schreibe  $\bar{\zeta} := \bar{\zeta}_e = \theta(\zeta_e) \in \mathbf{F}_p$ , dies ist ein Element von Ordnung  $e$  in  $U(\mathbf{F}_p)$ .

Ist  $k \equiv_e \ell$ , so ist  $\sum_{i \in [0, e-1]} \bar{\zeta}^{-i\ell} \bar{\zeta}^{ik} = \theta(e)$ .

Ist  $k \not\equiv_e \ell$ , so ist  $\bar{\zeta}^{k-\ell} - 1 \neq 0$ . Es wird

$$\begin{aligned} & (\bar{\zeta}^{k-\ell} - 1) \left( \sum_{i \in [0, e-1]} \bar{\zeta}^{-i\ell} \bar{\zeta}^{ik} \right) \\ &= \left( \sum_{i \in [0, e-1]} \bar{\zeta}^{(i+1)(k-\ell)} \right) - \left( \sum_{i \in [0, e-1]} \bar{\zeta}^{i(k-\ell)} \right) \\ &= \bar{\zeta}^{e(k-\ell)} - \bar{\zeta}^{0(k-\ell)} \\ &= 0, \end{aligned}$$

und also  $\sum_{i \in [0, e-1]} \bar{\zeta}^{-i\ell} \bar{\zeta}^{ik} = 0$ .  $\square$

**Lemma 50** Seien  $r, s \in [1, t]$ . Für  $\ell \in [0, e-1]$  sei  $x_{r,s;\ell}$  der Repräsentant in  $[0, p-1]$  von

$$\theta(e)^{-1} \sum_{i \in [0, e-1]} \bar{\zeta}_e^{-i\ell} \cdot \theta(\chi_r(g_s^i)) \in \mathbf{F}_p.$$

Dann ist

$$\chi_r(g_s) = \sum_{\ell \in [0, e-1]} x_{r,s;\ell} \zeta_e^\ell \in \mathbf{Z}[\zeta_e].$$

*Beweis.* Schreibe  $\zeta := \zeta_e$  und  $\bar{\zeta} := \bar{\zeta}_e$ .

Habe  $\omega^r(g_s)$  diagonalisiert die Gestalt  $\begin{pmatrix} \zeta^{m_{r,s;1}} & & \\ & \ddots & \\ & & \zeta^{m_{r,s;n_r}} \end{pmatrix}$ , wobei  $m_{r,s;j} \in [0, e-1]$  für  $j \in [1, n_r]$ ; cf. Lösung zu Aufgabe 23.

Es ist

$$\theta(\chi_r(g_s^i)) = \sum_{j \in [1, n_r]} \bar{\zeta}^{i \cdot m_{r,s;j}},$$

für  $i \in [0, e-1]$ , und also

$$\theta(e)^{-1} \sum_{i \in [0, e-1]} \bar{\zeta}^{-i\ell} \cdot \theta(\chi_r(g_s^i)) = \theta(e)^{-1} \sum_{j \in [1, n_r]} \sum_{i \in [0, e-1]} \bar{\zeta}^{-i\ell} \cdot \bar{\zeta}^{i \cdot m_{r,s;j}} \stackrel{\text{B. 49}}{=} \theta\left(\sum_{j \in [1, n_r]} \partial_{\ell, m_{r,s;j}}\right) \in \mathbf{F}_p.$$

für  $\ell \in [0, e-1]$ . Da  $n_r \leq |G| < p$ , ist  $x_{r,s;\ell} = \sum_{j \in [1, n_r]} \partial_{\ell, m_{r,s;j}}$  davon der Repräsentant in  $[0, p-1]$ .

Sodann ist

$$\sum_{\ell \in [0, e-1]} x_{r,s;\ell} \zeta^\ell = \sum_{j \in [1, n_r]} \sum_{\ell \in [0, e-1]} \partial_{\ell, m_{r,s;j}} \zeta^\ell = \sum_{j \in [1, n_r]} \zeta^{m_{r,s;j}} = \chi_r(g_s).$$

□

### 3.4.4 Der resultierende Algorithmus

Sei an die Bezeichnungen eingangs §3.4 erinnert.

#### Algorithmus 51 (Dixon)

- (1) Wähle  $\bar{\zeta}_e \in \mathbf{F}_p$  von Ordnung  $e$  in  $U(\mathbf{F}_p)$ . Setze entsprechend den Ringmorphismus  $\theta : \mathbf{Z}[\zeta_e] \rightarrow \mathbf{F}_p$ ,  $\zeta_e \mapsto \bar{\zeta}_e$ ; cf. Bemerkung 46.
- (2) Berechne die Matrizen  $(\theta(\gamma_{r,s,a}))_{s,a}$  für  $r \in [1, t]$  gemäß Bemerkung 43.
- (3) Bestimme die  $t$  gemeinsamen Eigenvektoren der Matrizen  $(\theta(\gamma_{r,s,a}))_{s,a} \in \mathbf{F}_p^{t \times t}$  für  $r \in [1, t]$  mit jeweils erstem Eintrag 1. Gemäß Lemma 48 haben wir damit die Matrix  $(\theta(\beta_{q,a}))_{q,a}$  bis auf die Reihenfolge der Zeilen ermittelt. Wir wählen eine solche Reihenfolge, was auf ein Neusortieren der Wedderburn-Faktoren hinausläuft. Hierzu verwenden wir implizit, daß es uns über  $\mathbf{F}_p$  möglich ist, die charakteristischen Polynome dieser Matrizen in Linearfaktoren zu zerlegen.
- (4) Unter Verwendung von (3) und der Tatsache, daß  $n_r \stackrel{\text{cf. } \omega}{\leq} |G| < p$ , können wir  $n_r$  für  $r \in [1, t]$  der Gleichung

$$\sum_{s \in [1, t]} \theta(\beta_{r,s}) \theta(\beta_{r,s'}) \theta(|g_s^G|)^{-1} = \theta(|G|) \theta(n_r^2)^{-1}$$

aus Bemerkung 41 entnehmen.

(5) Mit (3) und (4) entnehmen wir  $\theta(\chi_r(g_s))$  für  $r, s \in [1, t]$  der Gleichung

$$\theta(\beta_{r,s}) = \theta(\chi_r(g_s)) \theta(|g_s^G|) \theta(n_r)^{-1}$$

aus Bemerkung 39, beachte, daß  $n_r \leq |G| < p$ .

(6) Bestimme für  $s \in [1, t]$  und  $i \in [0, e-1]$  den Index  $\sigma(s, i) \in [1, t]$  mit  $(g_s^i)^G = g_{\sigma(s,i)}^G$ .  
Beachte, daß  $\chi_r(g_s^i) = \chi_r(g_{\sigma(s,i)})$  für  $r \in [1, t]$ .

(7) Mit (5) und (6) können wir  $\chi_r(g_s)$  für  $r, s \in [1, t]$  unter Verwendung von Lemma 50 berechnen.

Somit ist die Charaktertafel von  $G$  berechnet, ohne auf einen Wedderburnisomorphismus zurückgegriffen zu haben. Cf. Aufgabe 34.

# Kapitel 4

## Ringe ganzer Zahlen

Sei  $K|\mathbf{Q}$  eine endliche Körpererweiterung. Schreibe  $n := [K : \mathbf{Q}] = \dim_{\mathbf{Q}} K$ .

### 4.1 Begriff

**Definition 52** Sei

$$\mathcal{O}_K := \{ \alpha \in K : \text{es gibt ein normiertes Polynom } f(X) \in \mathbf{Z}[X] \text{ mit } f(\alpha) = 0 \}$$

die Teilmenge der ganzen Zahlen von  $K$ .

Das Ziel ist die Berechnung von  $\mathcal{O}_K$  bei gegebenem  $K$ .

**Bemerkung 53** Sind  $L|K|\mathbf{Q}$  endliche Körpererweiterungen, dann ist  $K \cap \mathcal{O}_L = \mathcal{O}_K$ .

**Bemerkung 54** Sei  $\alpha \in K$ . Es gibt ein  $z \in \mathbf{Z} \setminus \{0\}$  mit  $z\alpha \in \mathcal{O}_K$ .

Insbesondere ist  $K = \text{frac } \mathcal{O}_K$ ; genauer, wir identifizieren entlang  $\text{frac } \mathcal{O}_K \xrightarrow{\sim} K$ ,  $\alpha/\beta \mapsto \alpha/\beta$ , wobei  $\alpha \in \mathcal{O}_K$  und  $\beta \in \mathcal{O}_K \setminus \{0\}$ , dessen Surjektivität eben festgestellt wurde.

*Beweis.* Da  $K|\mathbf{Q}$  endlich ist, ist  $\alpha$  algebraisch über  $K$ . Sei  $\alpha^n + \sum_{i \in [0, n-1]} x_i \alpha^i = 0$ , wobei  $n \geq 1$  und  $x_i \in \mathbf{Q}$  für  $i \in [0, n-1]$ . Sei  $z \in \mathbf{Z} \setminus \{0\}$  so, daß  $zx_i \in \mathbf{Z}$  für alle  $i \in [0, n-1]$ . Dann ist  $(z\alpha)^n + \sum_{i \in [0, n-1]} z^{n-i} x_i (z\alpha)^i = 0$ , und somit  $z\alpha \in \mathcal{O}_K$ .  $\square$

**Definition 55** Ein  $\mathbf{Z}$ -Modul  $M$  heißt *endlich erzeugt*, wenn es eine endliche Teilmenge  $X \subseteq M$  mit  $M = \mathbf{z}\langle X \rangle$  gibt.

**Lemma 56** *Es ist*

- $$\begin{aligned} \mathcal{O}_K &\stackrel{1.}{=} \{ \alpha \in K : \mathbf{Z}[\alpha] = \mathbf{z}\langle \alpha^0, \dots, \alpha^m \rangle \text{ für ein } m \geq 0 \} \\ &\stackrel{2.}{=} \{ \alpha \in K : \mathbf{Z}[\alpha] \text{ ist ein endlich erzeugter } \mathbf{Z}\text{-Modul} \} \\ &\stackrel{3.}{=} \{ \alpha \in K : \mathbf{Z}[\alpha] \text{ ist in einem endlich erzeugten } \mathbf{Z}\text{-Teilmodul von } K \text{ enthalten} \}. \end{aligned}$$

*Beweis.* Sei  $\alpha \in K$ .

Zu  $\stackrel{1.}{\subseteq}$ . Ist  $f(X) = X^{m+1} + \sum_{i \in [0, m]} z_i X^i \in \mathbf{Z}[X]$  mit  $f(\alpha) = 0$  gegeben, wobei  $m \geq 0$ , dann ist  $\mathbf{Z}[\alpha] = \mathbf{z}\langle \alpha^0, \dots, \alpha^m \rangle$ , da auch für  $k \geq m + 1$  per Induktion über  $k$

$$\alpha^k = \alpha^{k-m-1} \alpha^{m+1} = \alpha^{k-m-1} (-\sum_{i \in [0, m]} z_i \alpha^i) = -\sum_{i \in [0, m]} z_i \alpha^{k-m-1+i} \in \mathbf{z}\langle \alpha^0, \dots, \alpha^m \rangle$$

ist.

Zu  $\stackrel{2.}{\subseteq}, \stackrel{3.}{\subseteq}$ .

Zu  $\stackrel{1.}{\supseteq}$ . Ist  $\mathbf{Z}[\alpha] = \mathbf{z}\langle \alpha^0, \dots, \alpha^m \rangle$ , dann ist  $\alpha^{m+1} \in \mathbf{z}\langle \alpha^0, \dots, \alpha^m \rangle$ , i.e. es gibt es ein normiertes Polynom von Grad  $m + 1$  mit Nullstelle  $\alpha$ .

Zu  $\stackrel{2.}{\supseteq}$ . Sei  $\mathbf{Z}[\alpha]$  ein endlich erzeugter  $\mathbf{Z}$ -Modul, sagen wir,  $\mathbf{Z}[\alpha] = \mathbf{z}\langle \xi_1, \dots, \xi_k \rangle$  für ein  $k \geq 0$  und  $\xi_i \in \mathbf{Z}[\alpha]$  für  $i \in [1, k]$ .

Schreibe  $A_k := \mathbf{z}\langle \alpha^0, \dots, \alpha^k \rangle \subseteq \mathbf{Z}[\alpha]$  für  $k \geq 0$ . Es ist  $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$  eine aufsteigende Kette von  $\mathbf{Z}$ -Teilmoduln von  $\mathbf{Z}[\alpha]$ .

Für  $i \in [1, k]$  gibt es ein  $m_i \geq 0$  so, daß  $\xi_i \in A_{m_i}$ . Sei  $m := \max\{m_i : i \in [1, k]\}$ . Dann ist  $\xi_i \in A_m$  für  $i \in [1, k]$ , und also auch

$$\mathbf{Z}[\alpha] = \mathbf{z}\langle \xi_1, \dots, \xi_k \rangle \subseteq A_m \subseteq \mathbf{Z}[\alpha],$$

mithin  $A_m = \mathbf{Z}[\alpha]$ .

Zu  $\stackrel{3.}{\supseteq}$ . Teilmoduln endlich erzeugter  $\mathbf{Z}$ -Moduln sind endlich erzeugt; cf. Aufgabe 35.(2).  $\square$

**Bemerkung 57** *Sei  $\mathbf{Z} \subseteq R \subseteq K$  mit  $R$  einem Teilring von  $K$  und mit  $R$  einem endlich erzeugten  $\mathbf{Z}$ -Modul. Sei  $\alpha \in \mathcal{O}_K$ .*

*Dann ist auch der Teilring  $R[\alpha] \subseteq K$  ein endlich erzeugter  $\mathbf{Z}$ -Modul.*

Natürlich enthält jeder Teilring von  $K$  auch  $\mathbf{Z}$ .

*Beweis.* Sei  $R = \mathbf{z}\langle \rho_1, \dots, \rho_k \rangle$ , wobei  $k \geq 1$  und  $\rho_i \in R$  für  $i \in [1, k]$ . Sei  $\mathbf{Z}[\alpha] = \mathbf{z}\langle \alpha^0, \dots, \alpha^m \rangle$ , wobei  $m \geq 0$ ; cf. Lemma 56. Wir behaupten, daß

$$R[\alpha] \stackrel{!}{=} \mathbf{z}\langle \rho_i \alpha^j : i \in [1, k], j \in [0, m] \rangle =: S.$$

Zu zeigen ist  $\stackrel{!}{\subseteq}$ .

Es ist  $R \subseteq S$ , da  $\rho_i \alpha^0 \in S$  für  $i \in [1, k]$ .

Falls  $m = 0$ , dann ist  $\alpha \in \mathbf{Z}[\alpha] = \mathbf{Z} \subseteq R$ .

Falls  $m \geq 1$ , dann schreiben wir  $1 = \sum_{i \in [1, k]} z_i \rho_i$  mit  $z_i \in \mathbf{Z}$  für  $i \in [1, k]$  und erhalten  $\alpha = 1 \cdot \alpha = \sum_{i \in [1, k]} z_i \rho_i \alpha^1 \in S$ .

Jedenfalls ist also  $\alpha \in S$ .

Bleibt zu zeigen, daß der  $\mathbf{Z}$ -Teilmodul  $S$  ein Teilring von  $K$  ist. Es ist  $1 \in R \subseteq S$ . Dank Distributivität genügt es, noch zu zeigen, daß  $(\rho_i \alpha^j)(\rho_{i'} \alpha^{j'}) \stackrel{!}{\in} S$  für  $i, i' \in [1, k]$  und  $j, j' \in [0, m]$ . Da  $\rho_i \rho_{i'} \in R$ , können wir  $\rho_i \rho_{i'} = \sum_{a \in [1, k]} u_a \rho_a$  schreiben mit  $u_a \in \mathbf{Z}$  für  $a \in [1, k]$ . Da  $\alpha^{j+j'} \in \mathbf{Z}[\alpha]$ , können wir  $\alpha^{j+j'} = \sum_{b \in [1, k]} v_b \alpha^b$  schreiben mit  $v_b \in \mathbf{Z}$  für  $b \in [0, m]$ . Es wird

$$(\rho_i \alpha^j)(\rho_{i'} \alpha^{j'}) = \sum_{a \in [1, k]} \sum_{b \in [1, k]} \underbrace{u_a v_b}_{\in \mathbf{Z}} \rho_a \alpha^b \in S.$$

□

**Lemma 58** *Es ist  $\mathcal{O}_K$  ein Teilring von  $K$ .*

*Beweis.* Es sind  $0, 1 \in \mathcal{O}_K$ . Seien  $\alpha, \beta \in \mathcal{O}_K$ . Wir haben zu zeigen, daß  $\alpha - \beta$  und  $\alpha \cdot \beta$  in  $\mathcal{O}_K$  liegen. Da  $\mathbf{Z}[\alpha - \beta], \mathbf{Z}[\alpha \cdot \beta] \subseteq \mathbf{Z}[\alpha, \beta]$ , genügt es zu zeigen, daß  $\mathbf{Z}[\alpha, \beta] = (\mathbf{Z}[\beta])[\alpha]$  ein endlich erzeugter  $\mathbf{Z}$ -Modul ist; cf. Lemma 56. Dies aber folgt aus  $\mathbf{Z}[\beta]$  endlich erzeugter  $\mathbf{Z}$ -Modul und  $\alpha \in \mathcal{O}_K$ ; cf. Lemma 56, Bemerkung 57. □

**Bemerkung 59** *Sei  $\mathbf{Z} \subseteq R \subseteq K$  mit  $R$  einem Teilring von  $K$  und mit  $R$  einem endlich erzeugten  $\mathbf{Z}$ -Modul. Sei  $K = \left\{ \frac{\rho}{\sigma} : \rho \in R, \sigma \in R \setminus \{0\} \right\}$ . Sei  $R$  ein Hauptidealbereich.*

*Dann ist  $R = \mathcal{O}_K$ .*

*Beweis.* Ist  $\xi \in R$ , so ist  $\mathbf{Z}[\xi] \subseteq R$ . Da  $R$  ein endlich erzeugter  $\mathbf{Z}$ -Modul ist, folgt  $\xi \in \mathcal{O}_K$ ; cf. Lemma 56. Folglich ist  $R \subseteq \mathcal{O}_K$ .

Sei umgekehrt  $\alpha \in \mathcal{O}_K$ . Wir wollen  $\alpha \stackrel{!}{\in} R$  zeigen.

Sei  $\alpha^m + \sum_{i \in [0, m-1]} z_i \alpha^i = 0$ , wobei  $m \geq 1$  und  $z_i \in \mathbf{Z}$  für  $i \in [0, m-1]$ . Schreibe

$$A := {}_R \langle \alpha^0, \dots, \alpha^{m-1} \rangle \neq 0.$$

Es ist  $\alpha^m = -\sum_{i \in [0, m-1]} z_i \alpha^i \in A$ , und also  $\alpha A \subseteq A$ .

Schreibe  $\alpha = \frac{\rho}{\sigma}$  mit  $\rho \in R$  und  $\sigma \in R \setminus \{0\}$ . Es ist  $\sigma^{m-1} \alpha^i \in R$  für  $i \in [0, m-1]$ , und also  $\sigma^{m-1} A \subseteq R$ . Es ist  $\sigma^{m-1} A$  ein Ideal in  $R$ . Da  $R$  ein Hauptidealbereich ist, können wir  $\sigma^{m-1} A = {}_R \langle \tau \rangle$  mit einem  $\tau \in R \setminus \{0\}$  schreiben. Es ist

$$\alpha \cdot {}_R \langle \tau \rangle = \alpha \cdot \sigma^{m-1} A \subseteq \sigma^{m-1} A = {}_R \langle \tau \rangle,$$

also  $\alpha \tau = \xi \tau$  für ein  $\xi \in R$ , und somit  $\alpha = \xi \in R$ . □

**Beispiel 60**

Sei  $\alpha \in \mathbf{C}$  algebraisch über  $\mathbf{Q}$ , i.e. Nullstelle eines Polynoms  $f(X) \in \mathbf{Q}[X] \setminus \{0\}$ . Beachte, daß sich jedes Element von  $\mathbf{Q}(\alpha) = \mathbf{Q}\langle \alpha^i : i \geq 0 \rangle$  sogar in der Form  $\frac{\beta}{z}$  mit  $\beta \in \mathbf{Z}[\alpha] = \mathbf{Z}\langle \alpha^i : i \geq 0 \rangle$  und  $z \in \mathbf{Z} \setminus \{0\}$  schreiben läßt.

- (1) Es ist  $\mathcal{O}_{\mathbf{Q}} = \mathbf{Z}$ , da  $\mathbf{Z}$  ein Hauptidealbereich ist; cf. Bemerkung 59.
- (2) Es ist  $\mathcal{O}_{\mathbf{Q}(\zeta_3)} = \mathbf{Z}[\zeta_3]$ , da  $\mathbf{Z}[\zeta_3] = \mathbf{Z}\langle \zeta_3^0, \zeta_3^1 \rangle$  ein Hauptidealbereich ist; cf. Aufgabe 36.(3), Bemerkung 59. Oder cf. Aufgabe 39.
- (3) Es ist  $\mathcal{O}_{\mathbf{Q}(i)} = \mathbf{Z}[i]$ , da  $\mathbf{Z}[i] = \mathbf{Z}\langle i^0, i^1 \rangle$  ein Hauptidealbereich ist; cf. Aufgabe 36.(1), Bemerkung 59. Oder cf. Aufgabe 39.
- (4) Es ist  $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[(1 + \sqrt{5})/2]$ ; cf. Aufgabe 39. Insbesondere ist  $\mathbf{Z}[\sqrt{5}]$  kein Hauptidealbereich.
- (5) Es ist  $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$ ; cf. Aufgabe 39. Dennoch ist  $\mathbf{Z}[\sqrt{-5}]$  kein Hauptidealbereich; cf. Aufgabe 36.(2).

## 4.2 Spurbilinearform und $\mathbf{Z}$ -Gitter

Um zu zeigen, daß  $\mathcal{O}_K$  als  $\mathbf{Z}$ -Modul endlich erzeugt ist, wollen wir die Spurabbildung  $\text{Tr}_{K|\mathbf{Q}} : K \rightarrow \mathbf{Q}$  verwenden, wobei  $\text{Tr}_{K|\mathbf{Q}}(\alpha)$  die Spur des  $\mathbf{Q}$ -linearen Endomorphismus  $K \rightarrow K$ ,  $\beta \mapsto \alpha\beta$  bezeichnet.

**Bemerkung 61** Die  $\mathbf{Q}$ -Bilinearform

$$\begin{aligned} K \times K &\longrightarrow \mathbf{Q} \\ (\alpha, \beta) &\longmapsto \text{Tr}_{K|\mathbf{Q}}(\alpha \cdot \beta), \end{aligned}$$

Spurbilinearform auf  $K$  genannt, ist nichtausgeartet.

*Beweis.* Sei  $\alpha \in K \setminus \{0\}$ . Es ist  $\text{Tr}_{K|\mathbf{Q}}(\alpha \cdot \alpha^{-1}) = \text{Tr}_{K|\mathbf{Q}}(1) = n \neq 0$ . ◻

**Definition 62** Für eine Teilmenge  $X \subseteq K$  setzen wir

$$X^\# := \{ \eta \in K : \text{Tr}_{K|\mathbf{Q}}(\eta \cdot X) \subseteq \mathbf{Z} \},$$

genannt das *Dual* von  $X$ .

Sind  $X \subseteq Y \subseteq K$  gegeben, so ist  $X^\# \supseteq Y^\#$ .

**Definition 63**

Ein  $\mathbf{Z}$ -Gitter in  $K$  ist ein endlich erzeugter  $\mathbf{Z}$ -Teilmodul  $G \subseteq K$  mit  $\mathbf{Q}\langle G \rangle = K$  <sup>(2)</sup>.

Eine  $\mathbf{Z}$ -lineare Basis des  $\mathbf{Z}$ -Gitters  $G$  ist ein Tupel  $(\alpha_1, \dots, \alpha_n)$  mit  $\alpha_i \in G$  für  $i \in [1, n]$  und  $G = \mathbf{z}\langle \alpha_1, \dots, \alpha_n \rangle$ .

Beachte, daß aus  $\mathbf{Q}\langle G \rangle = K$  und  $\dim_{\mathbf{Q}} K = n$  folgt, daß diesenfalls  $(\alpha_1, \dots, \alpha_n)$  ein  $\mathbf{Q}$ -linear unabhängiges Tupel ist, und also eine  $\mathbf{Q}$ -lineare Basis von  $K$ .

**Bemerkung 64** *Es gibt ein  $\mathbf{Z}$ -Gitter in  $K$ , das in  $\mathcal{O}_K$  liegt.*

*Beweis.* Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Q}$ -lineare Basis von  $K$ . Sei  $z_i \in \mathbf{Z} \setminus \{0\}$  so, daß  $z_i \alpha_i \in \mathcal{O}_K$  für  $i \in [1, n]$ ; cf. Bemerkung 54. Dann ist auch  $G := \mathbf{z}\langle z_1 \alpha_1, \dots, z_n \alpha_n \rangle \subseteq \mathcal{O}_K$ ; cf. Lemma 58. Ferner ist  $\alpha_i \in \mathbf{Q}\langle G \rangle$  für  $i \in [1, n]$  und also  $K = \mathbf{Q}\langle G \rangle$ .  $\square$

**Bemerkung 65**

Sei  $G = \mathbf{z}\langle \beta_1, \dots, \beta_m \rangle$  ein  $\mathbf{Z}$ -Gitter in  $K$ , wobei  $m \geq 0$  und  $\beta_i \in K$  für  $i \in [1, m]$ .

Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Q}$ -lineare Basis von  $K$ .

Sei  $\beta_j = \sum_{i \in [1, n]} \alpha_i x_{i,j}$  für  $j \in [1, m]$ , wobei  $X := (x_{i,j})_{i,j} \in \mathbf{Q}^{n \times m}$ .

Sei  $y \in \mathbf{Z} \setminus \{0\}$  so, daß  $yX \in \mathbf{Z}^{n \times m}$ .

Da  $\mathbf{Q}\langle G \rangle = K$ , ist  $m \geq n$  und der Rang von  $X$  gleich  $n$ .

Seien  $S \in \mathrm{GL}_n(\mathbf{Z})$  und  $T = (t_{j,\ell})_{j,\ell} \in \mathrm{GL}_m(\mathbf{Z})$  so, daß

$$S(yX)T = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \in \mathbf{Z}^{n \times m}$$

mit  $d_1, \dots, d_n \in \mathbf{Z} \setminus \{0\}$ ; cf. Satz 4.

Sei  $\gamma_\ell := \sum_{j \in [1, m]} \beta_j t_{j,\ell}$  für  $\ell \in [1, n]$ . Dann ist  $(\gamma_1, \dots, \gamma_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $G$ .

Insbesondere hat jedes  $\mathbf{Z}$ -Gitter in  $K$  eine  $\mathbf{Z}$ -lineare Basis.

*Beweis.* Es ist zu zeigen, daß  $G \stackrel{!}{=} \mathbf{z}\langle \gamma_1, \dots, \gamma_n \rangle$ .

Zu  $\stackrel{!}{\supseteq}$ . Es ist  $\gamma_\ell \in G$  für  $\ell \in [1, n]$ .

Zu  $\stackrel{!}{\subseteq}$ . Es genügt zu zeigen, daß  $\beta_j \stackrel{!}{\in} \mathbf{z}\langle \gamma_1, \dots, \gamma_n \rangle$  für  $j \in [1, m]$ ,

Schreibe  $T^{-1} =: (t'_{\ell,j})_{\ell,j} \in \mathrm{GL}_m(\mathbf{Z})$ .

<sup>2</sup>In der Literatur auch als *volles  $\mathbf{Z}$ -Gitter* in  $K$  bezeichnet.

Für  $i \in [1, n]$  und  $\ell \in [n + 1, m]$  ist  $\sum_{s \in [1, m]} x_{i,s} t_{s,\ell} = 0$ . Für  $j \in [1, m]$  wird also

$$\begin{aligned}
\beta_j &= \sum_{s \in [1, m]} \beta_s \partial_{s,j} \\
&= \sum_{s \in [1, m]} \sum_{\ell \in [1, m]} \beta_s t_{s,\ell} t'_{\ell,j} \\
&= \sum_{i \in [1, n]} \sum_{\ell \in [1, m]} \sum_{s \in [1, m]} \alpha_i x_{i,s} t_{s,\ell} t'_{\ell,j} \\
&= \sum_{i \in [1, n]} \sum_{\ell \in [1, n]} \sum_{s \in [1, m]} \alpha_i x_{i,s} t_{s,\ell} t'_{\ell,j} \\
&= \sum_{\ell \in [1, n]} \sum_{s \in [1, m]} \beta_s t_{s,\ell} t'_{\ell,j} \\
&= \sum_{\ell \in [1, n]} \gamma_\ell t'_{\ell,j} \\
&\in \mathbf{z} \langle \gamma_1, \dots, \gamma_n \rangle.
\end{aligned}$$

□

### Bemerkung 66

- (1) Sei  $G$  ein  $\mathbf{Z}$ -Gitter in  $K$ . Sei  $(\xi_1, \dots, \xi_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $G$ ; cf. Bemerkung 65. Dies ist auch eine  $\mathbf{Q}$ -lineare Basis von  $K$ .

Sei  $(\xi_1^*, \dots, \xi_n^*)$  die bezüglich Spurbilinearform dazu duale  $\mathbf{Q}$ -lineare Basis von  $K$ , i.e. sei  $\text{Tr}_{K|\mathbf{Q}}(\xi_i \xi_j^*) = \partial_{i,j}$  für  $i, j \in [1, n]$ .

Es ist  $G^\#$  ein  $\mathbf{Z}$ -Gitter in  $K$ , mit  $\mathbf{Z}$ -linearer Basis  $(\xi_1^*, \dots, \xi_n^*)$ .

Es ist  $G^{\#\#} = G$ .

- (2) Seien  $G$  und  $H$  zwei  $\mathbf{Z}$ -Gitter in  $K$  mit  $G \subseteq H$ .

Ist  $A \subseteq K$  ein  $\mathbf{Z}$ -Teilmodul mit  $G \subseteq A \subseteq H$ , dann ist  $A$  ein  $\mathbf{Z}$ -Gitter in  $K$ .

*Beweis.*

- (1) Es wird

$$G^\# = \{ \eta \in K : \text{Tr}_{K|\mathbf{Q}}(\eta \cdot G) \subseteq \mathbf{Z} \} = \{ \eta \in K : \text{Tr}_{K|\mathbf{Q}}(\eta \cdot \xi_i) \in \mathbf{Z} \text{ für } i \in [1, n] \}.$$

Wir behaupten, daß

$$G^\# \stackrel{!}{=} \mathbf{z} \langle \xi_1^*, \dots, \xi_n^* \rangle.$$

Dann ist insbesondere  $G^\#$  ein  $\mathbf{Z}$ -Gitter in  $K$ .

Davon folgt  $\stackrel{!}{\supseteq}$  nach Wahl der  $\xi_i^*$ .

Zeigen wir  $\stackrel{!}{\subseteq}$ . Sei  $\eta \in K$  mit  $\text{Tr}_{K|\mathbf{Q}}(\eta \cdot \xi_i) \in \mathbf{Z}$  für  $i \in [1, n]$  gegeben. Schreibe  $\eta = \sum_{i \in [1, n]} x_i \cdot \xi_i^*$  mit  $x_i \in \mathbf{Q}$ . Für  $j \in [1, n]$  wird

$$\begin{aligned}
\mathbf{Z} &\ni \text{Tr}_{K|\mathbf{Q}}(\eta \cdot \xi_j) \\
&= \text{Tr}_{K|\mathbf{Q}}(\sum_{i \in [1, n]} x_i \cdot \xi_i^* \cdot \xi_j) \\
&= \sum_{i \in [1, n]} x_i \cdot \text{Tr}_{K|\mathbf{Q}}(\xi_i^* \cdot \xi_j) \\
&= \sum_{i \in [1, n]} x_i \cdot \partial_{i,j} = x_j.
\end{aligned}$$

Das Argument von oben, angewandt auf  $G^\#$  statt auf  $G$ , gibt  $G^{\#\#} = \mathbf{z}\langle \xi_1, \dots, \xi_n \rangle$  und somit  $G^{\#\#} = G$ .

- (2) Es ist  $K = \mathbf{Q}\langle G \rangle \subseteq \mathbf{Q}\langle A \rangle \subseteq K$ , also  $\mathbf{Q}\langle A \rangle = K$ . Es ist  $A \subseteq H$  ein  $\mathbf{Z}$ -Teilmodul. Da  $H$  endlich erzeugt ist, ist auch  $A$  endlich erzeugt; cf. Aufgabe 35.(2).

□

### 4.3 $\mathbf{Z}$ -Maximalordnung

#### Definition 67

Ein Teilring  $R \subseteq K$ , der zugleich ein  $\mathbf{Z}$ -Gitter in  $K$  ist, heißt  $\mathbf{Z}$ -Ordnung in  $K$ .

**Lemma 68** *Es ist  $\mathcal{O}_K$  eine  $\mathbf{Z}$ -Ordnung in  $K$ . Es ist  $\mathcal{O}_K \subseteq \mathcal{O}_K^\#$ .*

*Beweis.* Dank Lemma 58 ist  $\mathcal{O}_K$  ein Teilring von  $K$ . Bleibt also zu zeigen, daß  $\mathcal{O}_K$  ein  $\mathbf{Z}$ -Gitter in  $K$  ist.

Sei  $G$  ein  $\mathbf{Z}$ -Gitter in  $K$ , das in  $\mathcal{O}_K$  liegt; cf. Bemerkung 64.

Da  $\text{Tr}_{K|\mathbf{Q}}(\mathcal{O}_K \cdot \mathcal{O}_K) \subseteq \text{Tr}_{K|\mathbf{Q}}(\mathcal{O}_K) \subseteq \mathbf{Z}$ , ist  $\mathcal{O}_K \subseteq \mathcal{O}_K^\#$ ; cf. Aufgabe 40.(2). Also ist  $G \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^\# \subseteq G^\#$ , und somit  $\mathcal{O}_K$  ein  $\mathbf{Z}$ -Gitter in  $K$ ; cf. Bemerkung 66.(1, 2). □

#### Lemma 69 ( $\mathbf{Z}$ -Maximalordnung)

*Jede  $\mathbf{Z}$ -Ordnung  $R$  in  $K$  ist in der  $\mathbf{Z}$ -Ordnung  $\mathcal{O}_K$  enthalten.*

Wir sagen auch,  $\mathcal{O}_K$  ist die  $\mathbf{Z}$ -Maximalordnung in  $K$ .

*Beweis.* Sei  $\beta \in R$ . Wir haben zu zeigen, daß  $\beta \in \mathcal{O}_K$ . Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $R$ . Für  $i \in [1, n]$  sei

$$\beta \cdot \alpha_i = \sum_{j \in [1, n]} x_{i,j} \alpha_j$$

mit  $(x_{i,j})_{i,j} \in \mathbf{Z}^{n \times n}$ . Folglich ist  $(\beta \cdot \mathbf{E}_n - (x_{i,j})_{i,j}) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ , wobei  $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ .

Also ist  $\det(\beta \cdot \mathbf{E}_n - (x_{i,j})_{i,j}) = 0$ . Mit  $\chi(X) := \det(X \cdot \mathbf{E}_n - (x_{i,j})_{i,j})$  ist mithin  $\chi(\beta) = 0$ . Die Leibnizformel für die Determinante zeigt, daß  $\chi(X)$  ein normiertes Polynom mit Koeffizienten in  $\mathbf{Z}$  ist. Somit ist  $\beta \in \mathcal{O}_K$ . □

## 4.4 Diskriminante

**Definition 70 (und Bemerkung)** Sei  $G$  ein  $\mathbf{Z}$ -Gitter in  $K$ . Sei  $G = \mathbf{z}\langle \xi_1, \dots, \xi_n \rangle$ . Schreibe

$$\Delta(G) := \det\left(\left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi_i \cdot \xi_j)\right)_{i,j \in [1,n]}\right) \in \mathbf{Q}$$

für die *Diskriminante* von  $G$ .

Diese ist unabhängig von der Wahl der  $\mathbf{Z}$ -linearen Basis  $(\xi_1, \dots, \xi_n)$  von  $G$ .

Es ist  $\Delta(G) \in \mathbf{Z}$ , falls  $G \subseteq G^\#$ .

*Beweis.* Seien  $(\xi_1, \dots, \xi_n)$  und  $(\xi'_1, \dots, \xi'_n)$  zwei  $\mathbf{Z}$ -lineare Basen von  $G$ . Für  $j \in [1, n]$  ist dann  $\xi'_j = \sum_i \xi_i x_{i,j}$  und  $\xi_j = \sum_i \xi'_i y_{i,j}$  mit  $(x_{i,j})_{i,j}, (y_{i,j})_{i,j} \in \mathbf{Z}^{n \times n}$ . Es folgt  $(x_{i,j})_{i,j} \cdot (y_{i,j})_{i,j} = E_n$ . Also sind  $(x_{i,j})_{i,j}, (y_{i,j})_{i,j} \in \mathrm{GL}_n(\mathbf{Z})$ . Insbesondere ist  $\det((x_{i,j})_{i,j}) \in \{-1, +1\}$ .

Es wird

$$\begin{aligned} \left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi'_i \cdot \xi'_j)\right)_{i,j} &= \left(\mathrm{Tr}_{K|\mathbf{Q}}\left(\sum_{k,\ell} x_{k,i} \xi_k \cdot \xi_\ell x_{\ell,j}\right)\right)_{i,j} \\ &= \left(\sum_{k,\ell} x_{k,i} \cdot \mathrm{Tr}_{K|\mathbf{Q}}(\xi_k \cdot \xi_\ell) \cdot x_{\ell,j}\right)_{i,j} \\ &= (x_{k,i})_{i,k} \cdot \left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi_k \cdot \xi_\ell)\right)_{k,\ell} \cdot (x_{\ell,j})_{\ell,j}, \end{aligned}$$

und somit

$$\begin{aligned} \det\left(\left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi'_i \cdot \xi'_j)\right)_{i,j}\right) &= \det((x_{k,i})_{i,k}) \cdot \det\left(\left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi_k \cdot \xi_\ell)\right)_{k,\ell}\right) \cdot \det((x_{\ell,j})_{\ell,j}) \\ &= \left(\det((x_{k,i})_{i,k})\right)^2 \cdot \det\left(\left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi_k \cdot \xi_\ell)\right)_{k,\ell}\right) \\ &= \det\left(\left(\mathrm{Tr}_{K|\mathbf{Q}}(\xi_k \cdot \xi_\ell)\right)_{k,\ell}\right). \end{aligned}$$

Ist schließlich  $G \subseteq G^\#$ , so ist  $\mathrm{Tr}_{K|\mathbf{Q}}(\xi_i \cdot \xi_j) \in \mathbf{Z}$  für  $i, j \in [1, n]$ . □

### Definition 71

Sei  $\Delta_K := \Delta(\mathcal{O}_K) \in \mathbf{Z}$  die *Diskriminante von  $K$* ; cf. Lemma 68, Definition 70.

## 4.5 $p$ -Radikal-Stabilisatoren

Sei  $R$  eine  $\mathbf{Z}$ -Ordnung in  $K$ . Sei  $p \in \mathbf{Z}_{>0}$  eine Primzahl.

### 4.5.1 $p$ -Radikal

**Definition 72** Sei

$$\mathrm{Jac}_p(R) := \{\alpha \in R : \text{es ist } \alpha^m \in pR \text{ für ein } m \geq 0\} \subseteq R$$

das  $p$ -(*Jacobson*-)Radikal von  $R$ .

**Algorithmus 73 ( $p$ -Jacobson-Radikal)**

Wir wollen  $\text{Jac}_p(R)$  berechnen.

Schreibe  $\varphi : R \rightarrow R/pR$ ,  $\alpha \mapsto \alpha + pR$  für den Restklassenmorphimus.

Da  $\text{char}(R/pR) = p$ , verfügen wir über den *Frobenius* genannten Ringmorphimus

$$\begin{aligned} \text{Frob} : R/pR &\longrightarrow R/pR \\ \alpha + pR &\longmapsto \alpha^p + pR. \end{aligned}$$

Insbesondere ist der Frobenius  $\mathbf{Z}$ -linear, und damit  $\mathbf{F}_p$ -linear.

Es ist

$$\text{Jac}_p(R) = \varphi^{-1}\left(\bigcup_{m \geq 0} \{\alpha + pR : (\alpha + pR)^m = 0\}\right) = \varphi^{-1}\left(\bigcup_{i \geq 0} \text{Kern}(\text{Frob}^i)\right)$$

Die Dimension des Kerns einer Matrix  $A \in \mathbf{F}_p^{n \times n}$  ändert sich nicht, wenn man  $A \in \bar{\mathbf{F}}_p^{n \times n}$  betrachtet, da die Zeilenstufenform von  $A$  über  $\mathbf{F}_p$  auch eine Zeilenstufenform von  $A$  über  $\bar{\mathbf{F}}_p$  ist. Über  $\bar{\mathbf{F}}_p$  ist dann  $\bigcup_{i \geq 0} \text{Kern} A^i = \text{Kern}(A^n)$ , da wir  $A$  als in Jordanform gegeben voraussetzen dürfen und in  $n$ -ter Potenz alle nilpotenten Jordanblöcke von  $A$  verschwunden sind. Aus Dimensionsgründen gilt nun  $\bigcup_{i \geq 0} \text{Kern} A^i = \text{Kern}(A^n)$  auch über  $\mathbf{F}_p$ .

Also ist

$$\text{Jac}_p(R) = \varphi^{-1}\left(\text{Kern}(\text{Frob}^n)\right).$$

Cf. Aufgabe 44.

**Bemerkung 74**

- (1) *Es ist  $\text{Jac}_p(R)$  ein Ideal in  $R$ , das  $pR$  enthält. Es ist  $\text{Jac}_p(R) \subset R$ . Insbesondere ist  $\text{Jac}_p(R)$  ein  $\mathbf{Z}$ -Gitter in  $K$ ; cf. Bemerkung 66.(2).*
- (2) *Es gibt ein  $m \geq 0$  mit  $\text{Jac}_p(R)^m \subseteq pR$ .*

*Beweis.*

Zu (1). Nach Konstruktion ist  $pR \subseteq \text{Jac}_p(R) \subseteq R$ .

Zeigen wir, daß  $\text{Jac}_p(R) \subseteq R$  ein Ideal ist.

Seien  $\alpha, \tilde{\alpha} \in \text{Jac}_p(R)$ . Sei  $k \geq 0$  mit  $\alpha^k \in pR$ . Sei  $\tilde{k} \geq 0$  mit  $\tilde{\alpha}^{\tilde{k}} \in pR$ . Sei  $\beta \in R$ .

Es wird  $(\beta\alpha)^k = \beta^k \alpha^k \in pR$ , also  $\beta\alpha \in \text{Jac}_p(R)$ .

Es wird

$$(\alpha + \tilde{\alpha})^{k+\tilde{k}} = \left(\sum_{i \in [0, k]} \binom{k+\tilde{k}}{i} \underbrace{\alpha^i \tilde{\alpha}^{k+\tilde{k}-i}}_{\in pR}\right) + \left(\sum_{i \in [k+1, k+\tilde{k}]} \binom{k+\tilde{k}}{i} \underbrace{\alpha^i \tilde{\alpha}^{k+\tilde{k}-i}}_{\in pR}\right) \in pR,$$

also  $\alpha + \tilde{\alpha} \in \text{Jac}_p(R)$ .

Für  $\text{Jac}_p(R) \stackrel{!}{\subset} R$  genügt es zu zeigen, daß  $1 \stackrel{!}{\notin} \text{Jac}_p(R)$ , i.e.  $1 \stackrel{!}{\notin} pR$ , i.e.  $p^{-1} \stackrel{!}{\notin} R$ . Dafür genügt es zu zeigen, daß  $p^{-1} \notin \mathcal{O}_K$ ; cf. Lemma 69. Wäre  $p^{-1} \in \mathcal{O}_K$ , dann wäre  $p^{-1} \in \mathbf{Q} \cap \mathcal{O}_K \stackrel{\text{B.53}}{=} \mathcal{O}_{\mathbf{Q}} \stackrel{\text{B.59}}{=} \mathbf{Z}$ , dem ist aber *nicht* so.

Zu (2). Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $\text{Jac}_p(R)$ ; cf. Bemerkung 65.

Wähle  $m_i \geq 0$  mit  $\alpha_i^{m_i} \in pR$ . Schreibe  $m := m_1 + \dots + m_n$ . Wir wollen zeigen, daß  $\text{Jac}_p(R)^m \stackrel{!}{\subseteq} pR$ . Seien dazu  $b_{i,j} \in \mathbf{Z}$  für  $i \in [1, n]$  und  $j \in [1, m]$  gegeben. Es wird

$$\prod_{j \in [1, m]} \left( \sum_{i \in [1, n]} \alpha_i b_{i,j} \right) = \sum_{\ell_i \geq 0, \ell_1 + \dots + \ell_n = m} c_{\ell_1, \dots, \ell_n} \alpha_1^{\ell_1} \cdots \alpha_n^{\ell_n}$$

für gewisse  $c_{\ell_1, \dots, \ell_n} \in \mathbf{Z}$ . Da  $\ell_1 + \dots + \ell_n = m$ , gibt es jeweils ein  $i \in [1, n]$  mit  $\ell_i \geq m_i$ , und also mit  $\alpha_i^{\ell_i} \in pR$ . Somit liegt die genannte Summe in  $pR$ .  $\square$

## 4.5.2 Stabilisator

Sei  $G \subseteq K$  ein  $\mathbf{Z}$ -Gitter. Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $G$ .

**Bemerkung 75** *Der Stabilisator*

$$\text{Stab}(G) := \{ \beta \in K : \beta G \subseteq G \}$$

*ist eine  $\mathbf{Z}$ -Ordnung in  $K$ .*

*Beweis.* Zeigen wir, daß  $\text{Stab}(G)$  ein Teilring ist. Es sind  $0, 1 \in \text{Stab}(G)$ .

Sind  $\beta, \tilde{\beta} \in \text{Stab}(G)$ , dann ist auch  $(\beta - \tilde{\beta})G \subseteq \beta G + \tilde{\beta}G \subseteq G$  und  $\beta\tilde{\beta}G \subseteq \beta G \subseteq G$ , also sind  $\beta - \tilde{\beta}, \beta\tilde{\beta} \in \text{Stab}(G)$ .

Es bleibt zu zeigen, daß  $\text{Stab}(G)$  ein  $\mathbf{Z}$ -Gitter in  $K$  ist. Dazu genügt es zu zeigen, daß  $\text{Stab}(G)$  ein  $\mathbf{Z}$ -Gitter enthält und in einem  $\mathbf{Z}$ -Gitter enthalten ist; cf. Bemerkung 66.(2).

Da  $\text{Tr}_{K|\mathbf{Q}}(G) = \mathbf{z} \langle \text{Tr}_{K|\mathbf{Q}}(\alpha_1), \dots, \text{Tr}_{K|\mathbf{Q}}(\alpha_n) \rangle \subseteq \mathbf{Q}$ , gibt es ein  $z \in \mathbf{Z} \setminus \{0\}$  mit  $\text{Tr}_{K|\mathbf{Q}}(zG) \subseteq \mathbf{Z}$ .

Sei  $\beta \in \text{Stab}(G)$ . Für  $\alpha \in G$  ist  $\beta\alpha \in G$  und also  $\text{Tr}_{K|\mathbf{Q}}(z\beta\alpha) \in \text{Tr}_{K|\mathbf{Q}}(zG) \subseteq \mathbf{Z}$ . Folglich ist  $\text{Tr}_{K|\mathbf{Q}}(z\beta G) \subseteq \mathbf{Z}$ . Es folgt  $z\text{Stab}(G) \subseteq G^\#$ , also  $\text{Stab}(G) \subseteq z^{-1}G^\#$ .

Seien  $i, j \in [1, n]$ . Wir können ein  $w_{i,j} \in \mathbf{Z} \setminus \{0\}$  mit  $w_{i,j} \alpha_i \alpha_j \in G$  wählen. Denn wir können hierfür etwa den Hauptnenner der Koeffizienten von  $\alpha_i \alpha_j$ , ausgedrückt als Linearkombination der  $\mathbf{Q}$ -linearen Basis  $(\alpha_1, \dots, \alpha_n)$  von  $K$ , nehmen.

Sei  $w := \text{kgV}(w_{i,j} : i, j \in [1, n])$ . Dann ist  $w\alpha_i \alpha_j \in G$  für  $i, j \in [1, n]$ , also  $w\alpha_i G \subseteq G$  für  $i \in [1, n]$ , also  $wG \subseteq \text{Stab}(G)$ .

Insgesamt ist also

$$wG \subseteq \text{Stab}(G) \subseteq z^{-1}G^\#.$$

Sowohl  $zG$  als auch  $z^{-1}G^\#$  sind  $\mathbf{Z}$ -Gitter in  $K$ ; cf. Bemerkung 66.(1).  $\square$

**Algorithmus 76 (Stabilisator)**

Wir wollen eine  $\mathbf{Z}$ -lineare Basis von  $\text{Stab}(G)$  bestimmen.

Seien  $i, j \in [1, n]$ . Schreibe  $\alpha_i \cdot \alpha_j = \sum_{k \in [1, n]} u_{i,j,k} \alpha_k$  mit  $u_{i,j,k} \in \mathbf{Q}$ .

Sei  $U_k := (u_{i,j,k})_{i,j}$  für  $k \in [1, n]$ . Sei  $U := (U_1 | U_2 | \dots | U_n) \in \mathbf{Q}^{n \times n^2}$  die durch Nebeneinanderstellen der  $U_k$  entstehende Matrix.

Sei  $w \in \mathbf{Z} \setminus \{0\}$  mit  $wU \in \mathbf{Z}^{n \times n^2}$ .

Seien  $S = (s_{i,j})_{i,j} \in \text{GL}_n(\mathbf{Z})$  und  $T \in \text{GL}_{n^2}(\mathbf{Z})$  so, daß  $S(wU)T = (D | 0_{n \times n} | \dots | 0_{n \times n})$ , wobei  $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \in \mathbf{Z}^{n \times n}$ ; cf. Satz 4.

Betrachte ein Element  $\xi = \sum_{i \in [1, n]} v_i \alpha_i \in K$ , wobei  $v := (v_1 \dots v_n) \in \mathbf{Q}^{1 \times n}$ .

Es ist  $\xi \in \text{Stab}(G)$  genau dann, wenn  $G \ni \xi \cdot \alpha_j = \sum_i v_i \alpha_i \alpha_j = \sum_{i,k} v_i u_{i,j,k} \alpha_k$  für  $j \in [1, n]$ , i.e. wenn  $\sum_i v_i u_{i,j,k} \in \mathbf{Z}$  für  $j, k \in [1, n]$ , i.e. wenn  $vU \in \mathbf{Z}^{1 \times n^2}$ , i.e. wenn  $vS^{-1}w^{-1}(S(wU)T) \in \mathbf{Z}^{1 \times n^2}$ , i.e. wenn  $vS^{-1}w^{-1}D \in \mathbf{Z}^{1 \times n}$ .

Es hat  $U$  den Rang  $n$ , denn aus  $vU = 0$  kann man  $\xi \cdot \alpha_j = 0$  für alle  $j \in [1, n]$  folgern, damit  $\xi = 0$ , mithin  $v = 0$ . Also ist  $d_i \neq 0$  für  $i \in [1, n]$ .

Es wird

$$\text{Stab}(G) = \left\{ \sum_i v_i \alpha_i : (v_1 \dots v_n) = xD^{-1}wS \text{ für ein } x \in \mathbf{Z}^{1 \times n} \right\}.$$

Da  $D^{-1}wS \in \text{GL}_n(\mathbf{Q})$ , folgt, daß eine  $\mathbf{Z}$ -lineare Basis von  $\text{Stab}(G)$  gegeben ist durch

$$\left( \sum_{i \in [1, n]} d_1^{-1} w s_{1,i} \alpha_i, \dots, \sum_{i \in [1, n]} d_n^{-1} w s_{n,i} \alpha_i \right).$$

Cf. Aufgabe 47.(2).

**Bemerkung 77** Ist  $\{0\} \subset J \subseteq R$  ein Ideal, dann ist  $J$  ein  $\mathbf{Z}$ -Gitter in  $K$ .

Insbesondere ist  $\text{Stab}(J)$  eine  $\mathbf{Z}$ -Ordnung in  $K$ , die  $R$  enthält.

*Beweis.* Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $R$ .

Sei  $\beta \in J \setminus \{0\}$ . Es ist  $(\beta\alpha_1, \dots, \beta\alpha_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $\beta R$ . Also ist  $\beta R$  ein  $\mathbf{Z}$ -Gitter in  $K$ . Da  $J \subseteq R$  ein Ideal ist, ist  $\beta R \subseteq J \subseteq R$ . Folglich ist auch  $J$  ein  $\mathbf{Z}$ -Gitter in  $K$ ; cf. Bemerkung 66.(2).

Nach Bemerkung 75 ist  $\text{Stab}(J)$  eine  $\mathbf{Z}$ -Ordnung in  $K$ . Da  $J$  ein Ideal in  $R$  ist, ist  $R \subseteq \text{Stab}(J)$ .  $\square$

**Beispiel 78** Sei  $\beta \in K \setminus \{0\}$ . Dann ist  $\text{Stab}(\beta R) = \text{Stab}(R) = R$ .

*Beweis.* Zum einen ist für  $\alpha \in K$  genau dann  $\alpha\beta R \subseteq \beta R$ , wenn  $\alpha R \subseteq R$ .

Zum anderen ist  $\text{Stab}(R) \supseteq R$ , da  $R$  ein Teilring von  $K$  ist, und  $\text{Stab}(R) \subseteq R$ , da für  $\alpha \in \text{Stab}(R)$  insbesondere  $\alpha = \alpha \cdot 1 \in \alpha R \subseteq R$  wird.  $\square$

### 4.5.3 Pohst-Zassenhaus-Bernardi

Wir erinnern daran, daß  $K|\mathbf{Q}$  eine endliche Körpererweiterung mit  $\dim_{\mathbf{Q}} K = n$  und daß  $R$  eine  $\mathbf{Z}$ -Ordnung in  $K$  ist.

#### Satz 79 (Pohst-Zassenhaus)

- (1) *Es ist  $R \subseteq \text{Stab}(\text{Jac}_p(R))$  und  $|\text{Stab}(\text{Jac}_p(R))/R| \mid p^{n-1}$ .*
- (2) *Es ist  $p$  kein Teiler von  $|\mathcal{O}_K/R|$  genau dann, wenn  $R = \text{Stab}(\text{Jac}_p(R))$ .*

*Beweis (D. Bernardi).* Schreibe  $R' := \text{Stab}(\text{Jac}_p(R))$ .

Zu (1). Es ist  $R \subseteq R'$ ; cf. Bemerkungen 74.(1) und 77.

Es ist  $R \simeq \mathbf{Z}^n$  als  $\mathbf{Z}$ -Moduln, und somit auch  $R/pR \simeq \mathbf{Z}^n/p\mathbf{Z}^n \simeq \mathbf{F}_p^n$ .

Sei  $\alpha' \in R'$ . Wegen  $p \in \text{Jac}_p(R)$  ist  $p\alpha' \in \text{Jac}_p(R)$ ; cf. Bemerkung 74.(1).

Also ist  $pR \subseteq pR' \subseteq \text{Jac}_p(R) \stackrel{\text{B. 74.(1)}}{\subset} R$ .

Folglich ist  $p^n = |R/pR|$  ein echtes Vielfaches von  $|pR'/pR| = |R'/R|$ .

Zu (2).

Zu  $\Rightarrow$ . Sei  $R \subset R'$ . Dann ist  $R \subset R' \subseteq \mathcal{O}_K$ ; cf. Lemma 69. Dank (1) ist  $|R'/R|$  eine Potenz von  $p$ . Also folgt  $p \mid |R'/R| \mid |\mathcal{O}_K/R|$ .

Zu  $\Leftarrow$ . Sei  $R = R'$ . Setze

$$S := \{\alpha \in \mathcal{O}_K : \text{es ist } p^k \alpha \in R \text{ für ein } k \geq 0\}.$$

Es ist  $R \subseteq S \subseteq \mathcal{O}_K$ . Es ist  $S$  ein Teilring von  $\mathcal{O}_K$ , denn mit  $\alpha, \beta \in S$ , wobei  $p^k \alpha \in R$  und  $p^\ell \beta \in R$  für gewisse  $k, \ell \geq 0$ , wird  $p^{\max\{k, \ell\}}(\alpha - \beta) \in R$  und  $p^{k+\ell} \alpha \cdot \beta \in R$ , mithin  $\alpha - \beta, \alpha \cdot \beta \in S$ . Somit ist  $S$  eine  $\mathbf{Z}$ -Ordnung in  $K$ ; cf. Lemma 68, Bemerkung 66.(2). Sei  $(\sigma_1, \dots, \sigma_n)$  eine  $\mathbf{Z}$ -lineare Basis von  $S$ . Sei  $t \geq 0$  so gewählt, daß  $p^t \sigma_i \in R$  für alle  $i \in [1, n]$ . Somit ist  $p^t S \subseteq R$ .

Es ist  $p$  kein Teiler von  $|\mathcal{O}_K/S|$ . Denn wäre  $p$  ein Teiler von  $|\mathcal{O}_K/S|$ , dann gäbe es ein  $\alpha \in \mathcal{O}_K \setminus S$  mit  $p\alpha \in S$ , also  $p^t \cdot p\alpha \in R$  und somit  $\alpha \in S$ , was *nicht der Fall* ist.

Es genügt also zu zeigen, daß  $R \stackrel{!}{=} S$ .

*Annahme*, es ist  $R \subset S$ . Sei  $m \geq 0$  so, daß  $\text{Jac}_p(R)^m \subseteq pR$ ; cf. Bemerkung 74.(2). Es ist  $\text{Jac}_p(R)^{mt} \cdot S \subseteq p^t S \subseteq R$ .

Sei  $u \geq 0$  maximal mit  $\text{Jac}_p(R)^u \cdot S \not\subseteq R$ . Es ist  $\text{Jac}_p(R)^{u+1} \cdot S \subseteq R$ .

Wähle ein  $\sigma \in \text{Jac}_p(R)^u \cdot S \setminus R \subseteq S$ . Wir wollen zeigen, daß  $\text{Jac}_p(R) \cdot \sigma \stackrel{!}{\subseteq} \text{Jac}_p(R)$ .

Sei  $\alpha \in \text{Jac}_p(R)$  gegeben. Es ist

$$\alpha \cdot \sigma \in \text{Jac}_p(R) \cdot \text{Jac}_p(R)^u \cdot S = \text{Jac}_p(R)^{u+1} \cdot S \subseteq R.$$

Es ist

$$(\alpha \cdot \sigma)^{m+u+1} = \alpha^m \cdot \alpha^{u+1} \cdot \sigma^{m+u+1} \in \text{Jac}_p(R)^m \cdot \text{Jac}_p(R)^{u+1} \cdot S \subseteq \text{Jac}_p(R)^m \subseteq pR.$$

Also ist  $\alpha \cdot \sigma \in \text{Jac}_p(R)$ .

Es folgt  $\text{Jac}_p(R) \cdot \sigma \subseteq \text{Jac}_p(R)$ , i.e.  $\sigma \in \text{Stab}(\text{Jac}_p(R)) = R'$ . Da aber  $R' = R$  vorausgesetzt wurde, folgt  $\sigma \in R$ , im *Widerspruch* zur Wahl von  $\sigma$ .  $\square$

**Bemerkung 80** *Es ist  $|\Delta(R)|$  ein Vielfaches von  $|\mathcal{O}_K/R|$ .*

*Beweis.* Es ist  $R \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^\# \subseteq R^\#$ ; cf. Lemma 68, Definition 62. Also ist  $|\Delta(R)| = |R^\#/R|$  ein Vielfaches von  $|\mathcal{O}_K/R|$ ; cf. Aufgabe 41.(2).  $\square$

**Korollar 81 (zu Satz 79)**

*Ist  $\text{Jac}_p(R) \subseteq R$  ein Hauptideal für alle Primzahlen  $p$ , die  $\Delta(R)$  teilen, dann ist  $R = \mathcal{O}_K$ .*

*Insbesondere, ist  $R$  ein Hauptidealbereich, so ist  $R = \mathcal{O}_K$ .*

Cf. Bemerkung 59.

*Beweis.* Sei  $p$  eine Primzahl, die  $\Delta(R)$  teilt. Nach Voraussetzung ist  $\text{Jac}_p(R) = \beta R$  für ein  $\beta \in R$ . Da  $0 \neq pR \subseteq \text{Jac}_p(R)$ , ist  $\beta \neq 0$ . Es folgt

$$\text{Stab}(\text{Jac}_p(R)) = \text{Stab}(\beta R) \stackrel{\text{Bsp. 78}}{=} R.$$

Also  $p$  kein Teiler von  $|\mathcal{O}_K/R|$ ; cf. Satz 79.

Da aber  $|\Delta(R)|$  ein Vielfaches von  $|\mathcal{O}_K/R|$  ist, folgt  $|\mathcal{O}_K/R| = 1$ , i.e.  $R = \mathcal{O}_K$ .  $\square$

#### 4.5.4 Bestimmung der $\mathbf{Z}$ -Maximalordnung $\mathcal{O}_K$

**Algorithmus 82 ( $\mathbf{Z}$ -Maximalordnung bestimmen)**

Wir wollen ausgehend von einer endlichen Erweiterung  $K|\mathbf{Q}$  mit  $\dim_{\mathbf{Q}} K = n$  die  $\mathbf{Z}$ -Maximalordnung  $\mathcal{O}_K$  bestimmen.

- (1) Wähle ein  $\mathbf{Z}$ -Gitter  $G$  in  $K$ .
- (2) Sei  $R := \text{Stab}(G)$ . Es ist  $R$  eine  $\mathbf{Z}$ -Ordnung in  $K$ ; cf. Bemerkung 75.
- (3) Berechne die Diskriminante  $\Delta(R)$ ; cf. Aufgabe 47.(1). Sei  $P$  die Menge der Primteiler von  $\Delta(R)$ .

Es ist  $|\Delta(R)| = |R^\#/R|$  ein Vielfaches von  $|\mathcal{O}_K/R|$ ; cf. Bemerkung 80. Somit tauchen alle Primteiler von  $|\mathcal{O}_K/R|$  in  $P$  auf.

- (4) Durchlaufe  $p \in P$ .
- (5) Berechne  $R \subseteq R' := \text{Stab}(\text{Jac}_p(R))$ ; cf. Aufgaben 44 und 47.(2).
- (6) Ist  $R \subset R'$ , dann verfare wie folgt. Es ist  $|\mathcal{O}_K/R'|$  ein Teiler von  $|\mathcal{O}_K/R|$  mit  $|\mathcal{O}_K/R'| \neq |\mathcal{O}_K/R|$ . Es tauchen alle Primfaktoren von  $|\mathcal{O}_K/R'|$  in  $P$  auf. Die Elemente von  $P$ , die  $|\mathcal{O}_K/R|$  nicht teilen, teilen auch  $|\mathcal{O}_K/R'|$  nicht. Ersetze  $R$  durch  $R'$  (aber belasse  $P$ ). Gehe nach (5).
- (7) Es ist  $R = R'$ , und also  $p$  kein Teiler von  $|\mathcal{O}_K/R|$ ; cf. Satz 79.(2). Gehe nach (4).
- (8) Es ist nun kein Element von  $P$  mehr ein Teiler von  $|\mathcal{O}_K/R|$ . Da alle Primteiler von  $|\mathcal{O}_K/R|$  in  $P$  auftauchen, bedeutet dies, daß  $|\mathcal{O}_K/R| = 1$ , i.e. daß  $R = \mathcal{O}_K$ .

Der Algorithmus endet nach höchstens  $|P| + |\mathcal{O}_K/R|$  Durchläufen von (5), wenn  $R$  die anfängliche  $\mathbf{Z}$ -Ordnung aus (2) bezeichnet.

Cf. Aufgabe 48.

## 4.6 Kreisteilungskörper

### 4.6.1 Einheitswurzeln mit Primpotenzordnung

Sei  $p \in \mathbf{Z}_{>0}$  prim. Sei  $m \geq 1$ . Wir schreiben auch

$$q := p^{m-1} \quad \text{und} \quad \zeta := \zeta_{p^m} = \zeta_{pq}.$$

Sei  $K := \mathbf{Q}(\zeta) = \mathbf{Q}(\zeta_{pq})$ . Es ist  $n := \dim_{\mathbf{Q}} K = (p-1)q$ .

#### 4.6.1.1 Spur und Diskriminante im Primpotenzfall

**Bemerkung 83** Sei  $k \in \mathbf{Z}$ . Es ist

$$\text{Tr}_{K|\mathbf{Q}}(\zeta_{pq}^k) = \left\{ \begin{array}{ll} (p-1)q & \text{falls } k \equiv_{pq} 0 \\ -q & \text{falls } k \not\equiv_{pq} 0, \text{ aber } k \equiv_q 0 \\ 0 & \text{falls } k \not\equiv_q 0 \end{array} \right\} = pq \partial_{k+pq\mathbf{Z},0} - q \partial_{k+q\mathbf{Z},0}.$$

*Beweis.* Sei allgemein  $\alpha \in K$ . Schreibe  $\mu_{\alpha, \mathbf{Q}}(X) =: X^\ell + \sum_{i \in [0, \ell-1]} a_i X^i$ . Es ist

$$\text{Tr}_{K|\mathbf{Q}}(\alpha) = -\frac{n}{\ell} a_{\ell-1};$$

cf. Aufgabe 40.(1).

Sei  $s \in [0, m]$  so, daß  $k \not\equiv_{p^{s+1}} 0$ , aber  $k \equiv_{p^s} 0$ .

Fall  $s = m$ . Es ist  $\mathrm{Tr}_{K|\mathbf{Q}}(\zeta^k) = \mathrm{Tr}_{K|\mathbf{Q}}(1) = n = (p-1)q$ .

Fall  $s = m-1$ . Es hat  $\zeta^k$  die multiplikative Ordnung  $p$ . Also ist

$$\mu_{\zeta^k, \mathbf{Q}}(X) = \Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X^0.$$

Es folgt  $\mathrm{Tr}_{K|\mathbf{Q}}(\zeta^k) = -\frac{n}{p-1} = -q$ .

Fall  $s \in [0, m-2]$ . Es hat  $\zeta^k$  die multiplikative Ordnung  $p^{m-s}$ . Also ist

$$\mu_{\zeta^k, \mathbf{Q}}(X) = \Phi_{p^{m-s}}(X) = X^{(p-1) \cdot p^{m-s-1}} + X^{(p-2) \cdot p^{m-s-1}} + \dots + X^{0 \cdot p^{m-s-1}}.$$

Es folgt  $\mathrm{Tr}_{K|\mathbf{Q}}(\zeta^k) = -\frac{n}{(p-1)p^{m-s-1}} \cdot 0 = 0$ . □

**Lemma 84** Es ist  $|\Delta(\mathbf{Z}[\zeta_{pq}])| = p^{q(mp-m-1)} = p^{nm-q}$ .

*Beweis.* Siehe Aufgabe 49. □

#### 4.6.1.2 Der Ring der ganzen Zahlen in $\mathbf{Q}(\zeta)$ im Primpotenzfall

**Bemerkung 85** Es ist  $\mathrm{Jac}_p(\mathbf{Z}[\zeta_{pq}]) = \mathbf{z}_{[\zeta_{pq}]} \langle \zeta_{pq} - 1 \rangle$ .

*Beweis.* Da der Frobenius  $\mathbf{F}_p[X] \rightarrow \mathbf{F}_p[X]$ ,  $f(X) \mapsto f(X)^p$ , ein Ringendomorphismus ist, ist  $(X+1)^{p^k} \equiv_p X^{p^k} + 1$  für alle  $k \geq 0$ , wobei die Kongruenz in  $\mathbf{Z}[X]$  zu lesen ist.

Es ist  $\Phi_{pq}(X) \cdot (X^q - 1) = (X^{pq} - 1)$ . Also ist

$$\Phi_{pq}(X+1) \cdot X^q \equiv_p \Phi_{pq}(X+1) \cdot ((X+1)^q - 1) = (X+1)^{pq} - 1 \equiv_p X^{pq}.$$

Da  $\mathbf{F}_p[X]$  nullteilerfrei ist, folgt  $\Phi_{pq}(X+1) \equiv_p X^{q(p-1)}$ .

Es ist  $\Phi_{pq}(X+1) = \mu_{\zeta-1, \mathbf{Q}}(X)$ , und also

$$\begin{aligned} \mathbf{Z}[\zeta] &= \mathbf{Z}[\zeta-1] \xleftarrow{\sim} \mathbf{Z}[X] / \langle \Phi_{pq}(X+1) \rangle \\ \zeta-1 &\longleftarrow X + \langle \Phi_{pq}(X+1) \rangle. \end{aligned}$$

Folglich haben wir Ringisomorphismen

$$\begin{aligned} \mathbf{Z}[\zeta] / p\mathbf{Z}[\zeta] &\xleftarrow{\sim} \mathbf{Z}[X] / \langle p, \Phi_{pq}(X+1) \rangle \xrightarrow{\sim} \mathbf{F}_p[X] / \langle \Phi_{pq}(X+1) \rangle = \mathbf{F}_p[X] / \langle X^{q(p-1)} \rangle \\ (\zeta-1) + p\mathbf{Z}[\zeta] &\longleftarrow X + \langle p, \Phi_{pq}(X+1) \rangle \longmapsto X + \langle \Phi_{pq}(X+1) \rangle. \end{aligned}$$

Schreiben wir die Restklassenabbildung  $\varphi : \mathbf{Z}[\zeta] \rightarrow \mathbf{Z}[\zeta] / p\mathbf{Z}[\zeta]$ ,  $\alpha \mapsto \alpha + p\mathbf{Z}[\zeta]$ , so ist

$$\mathrm{Jac}_p(\mathbf{Z}[\zeta]) = \varphi^{-1}(\{ \alpha + \mathbf{Z}[\zeta] \in \mathbf{Z}[\zeta] / p\mathbf{Z}[\zeta] : \text{es gibt ein } m \geq 0 \text{ mit } (\alpha + p\mathbf{Z}[\zeta])^m = 0 \}).$$

Es ist

$$\begin{aligned} \{ f(X) + \langle X^{q(p-1)} \rangle \in \mathbf{F}_p[X] / \langle X^{q(p-1)} \rangle : \text{es gibt ein } m \geq 0 \text{ mit } (f(X) + \langle X^{q(p-1)} \rangle)^m = 0 \} \\ = \langle X \rangle / \langle X^{q(p-1)} \rangle, \end{aligned}$$

wie man erkennt, wenn man  $f(X) = a + Xb(X)$  mit  $a \in \mathbf{F}_p$  und  $b(X) \in \mathbf{F}_p[X]$  ansetzt. Isomorph übertragen, liefert dies

$$\text{Jac}_p(\mathbf{Z}[\zeta]) = \varphi^{-1}(\langle (\zeta - 1) + p\mathbf{Z}[\zeta] \rangle) = \langle \zeta - 1, p \rangle \subseteq \mathbf{Z}[\zeta].$$

Bleibt zu zeigen, daß  $p \stackrel{!}{\in} \langle \zeta - 1 \rangle$ . In der Tat wird

$$\begin{aligned} (\zeta - 1)\left(-\sum_{s \in [0, p-1]} \sum_{i \in [0, sq-1]} \zeta^i\right) &= \left(\sum_{s \in [0, p-1]} \sum_{i \in [0, sq-1]} \zeta^i\right) - \left(\sum_{s \in [0, p-1]} \sum_{i \in [0, sq-1]} \zeta^{i+1}\right) \\ &= \left(\sum_{s \in [0, p-1]} \sum_{i \in [0, sq-1]} \zeta^i\right) - \left(\sum_{s \in [0, p-1]} \sum_{i \in [1, sq]} \zeta^i\right) \\ &= \sum_{s \in [0, p-1]} (1 - \zeta^{sq}) \\ &= p - \sum_{s \in [0, p-1]} \zeta^{sq} \\ &= p - \Phi_{pq}(\zeta) \\ &= p. \end{aligned}$$

□

**Lemma 86** *Es ist  $\mathcal{O}_{\mathbf{Q}(\zeta_{pq})} = \mathbf{Z}[\zeta_{pq}]$ .*

*Beweis.* Es ist  $|\mathcal{O}_{\mathbf{Q}(\zeta)}/\mathbf{Z}[\zeta]|$  ein Teiler von  $\Delta(\mathbf{Z}[\zeta])$ ; cf. Bemerkung 80. Somit ist  $|\mathcal{O}_{\mathbf{Q}(\zeta)}/\mathbf{Z}[\zeta]|$  eine Potenz von  $p$ ; cf. Aufgabe 41.(2), Lemma 84. Also genügt es zu zeigen, daß  $\text{Jac}_p(\mathbf{Z}[\zeta])$  ein Hauptideal in  $\mathbf{Z}[\zeta]$  ist; cf. Korollar 81. In der Tat ist  $\text{Jac}_p(\mathbf{Z}[\zeta]) = \mathbf{z}_{[\zeta]} \langle \zeta - 1 \rangle$ , und somit ein Hauptideal; cf. Bemerkung 85. □

Cf. auch Aufgabe 51.(4).

## 4.6.2 Der Ring der ganzen Zahlen in $\mathbf{Q}(\zeta)$

**Lemma 87** *Seien  $K|\mathbf{Q}$  und  $L|\mathbf{Q}$  endliche Erweiterungen. Sei  $KL$  ihr Kompositum.*

*Setze  $\mathcal{O}_K \mathcal{O}_L := \mathbf{z} \langle \alpha \beta : \alpha \in \mathcal{O}_K, \beta \in \mathcal{O}_L \rangle \subseteq KL$ .*

*Sei  $[K : \mathbf{Q}] \cdot [L : \mathbf{Q}] = [KL : \mathbf{Q}]$ , i.e. seien  $K$  und  $L$  linear disjunkt über  $\mathbf{Q}$ .*

*Seien  $\Delta_K$  und  $\Delta_L$  teilerfremd.*

$$(1) \text{ Es ist } \mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L.$$

$$(2) \text{ Es ist } \Delta_{KL} = \Delta_K^\ell \cdot \Delta_L^k.$$

*Beweis.*

Zu (1). Es sind  $\mathcal{O}_K \subseteq \mathcal{O}_{KL}$  und  $\mathcal{O}_L \subseteq \mathcal{O}_{KL}$ , und also ist  $\mathcal{O}_K \mathcal{O}_L \subseteq \mathcal{O}_{KL}$ .

Wir haben  $\mathcal{O}_K \mathcal{O}_L \stackrel{!}{\supseteq} \mathcal{O}_{KL}$  zu zeigen.

Sei  $(\kappa_1, \dots, \kappa_k)$  eine  $\mathbf{Z}$ -lineare Basis von  $\mathcal{O}_K$ ; dies ist auch eine  $\mathbf{Q}$ -lineare Basis von  $K$ ; cf. Lemma 68.

Sei  $(\lambda_1, \dots, \lambda_\ell)$  eine  $\mathbf{Z}$ -lineare Basis von  $\mathcal{O}_L$ ; dies ist auch eine  $\mathbf{Q}$ -lineare Basis von  $L$ ; cf. Lemma 68.

Es ist  $(\kappa_i \lambda_j : i \in [1, k], j \in [1, \ell])$  ein  $\mathbf{Z}$ -linear erzeugendes Tupel von  $\mathcal{O}_K \mathcal{O}_L$ . Es ist auch eine  $\mathbf{Q}$ -lineare Basis von  $KL$ , da es  $KL$  erzeugt und  $[KL : \mathbf{Q}]$  Elemente enthält, da  $K$  und  $L$  linear disjunkt sind über  $\mathbf{Q}$ .

Beachte, daß  $\text{Tr}_{K|\mathbf{Q}}(\eta) = \text{Tr}_{KL|L}(\eta)$  für  $\eta \in K$ , da  $(\kappa_1, \dots, \kappa_k)$  sowohl eine  $\mathbf{Q}$ -lineare Basis von  $K$  als auch, wegen  $K$  und  $L$  linear disjunkt über  $\mathbf{Q}$ , eine  $L$ -lineare Basis von  $KL$  ist, und daher die  $\mathbf{Q}$ -linear beschreibende Matrix der Multiplikation mit  $\eta$  auf  $K$  auch eine  $L$ -linear beschreibende Matrix der Multiplikation mit  $\eta$  auf  $KL$  ist.

Sei  $\xi \in \mathcal{O}_{KL}$ . Schreibe  $\xi = \sum_{i,j} x_{i,j} \kappa_i \lambda_j$  mit  $x_{i,j} \in \mathbf{Q}$  für  $i \in [1, k]$  und  $j \in [1, \ell]$ . Wir haben zu zeigen, daß  $x_{i,j} \in \mathbf{Z}$  für  $i \in [1, k]$  und  $j \in [1, \ell]$ .

Für  $i \in [1, k]$  setzen wir  $\alpha_i := \sum_j x_{i,j} \lambda_j \in L$ . Für  $s \in [1, k]$  wird

$$\begin{aligned} \sum_i \text{Tr}_{K|\mathbf{Q}}(\kappa_s \kappa_i) \alpha_i &= \sum_{i,j} \text{Tr}_{K|\mathbf{Q}}(\kappa_s \kappa_i) x_{i,j} \lambda_j \\ &= \sum_{i,j} \text{Tr}_{KL|L}(\kappa_s \kappa_i) x_{i,j} \lambda_j \\ &= \sum_{i,j} \text{Tr}_{KL|L}(\kappa_s \kappa_i x_{i,j} \lambda_j) \\ &= \text{Tr}_{KL|L}(\kappa_s \xi) \\ &\in \mathcal{O}_L, \end{aligned}$$

da mit  $\kappa_s$  und  $\xi$  auch  $\kappa_s \xi$  in  $\mathcal{O}_{KL}$  liegt und da  $\text{Tr}_{KL|L}(\mathcal{O}_{KL}) \subseteq \mathcal{O}_L$ ; cf. Aufgabe 50.

Multiplikation mit der Adjunkten von  $(\text{Tr}_{K|\mathbf{Q}}(\kappa_i \kappa_s))_{i,s} \in \mathbf{Q}^{k \times k}$  zeigt nun, daß  $\Delta_K \alpha_s \in \mathcal{O}_L$  für  $s \in [1, k]$ , i.e. daß

$$\Delta_K x_{i,j} \in \mathbf{Z}$$

für  $i \in [1, k]$  und  $j \in [1, \ell]$ , da  $(\lambda_1, \dots, \lambda_\ell)$  eine  $\mathbf{Z}$ -lineare Basis von  $\mathcal{O}_L$  ist.

Genauso folgt, daß

$$\Delta_L x_{i,j} \in \mathbf{Z}$$

für  $i \in [1, k]$  und  $j \in [1, \ell]$ .

Da  $\Delta_K$  und  $\Delta_L$  teilerfremd sind, gibt es  $u, v \in \mathbf{Z}$  mit  $u \Delta_K + v \Delta_L = 1$ . Für  $i \in [1, k]$  und  $j \in [1, \ell]$  wird

$$x_{i,j} = u \Delta_K x_{i,j} + v \Delta_L x_{i,j} \in \mathbf{Z}.$$

Zu (2). Beachte zunächst, daß  $\text{Tr}_{KL|\mathbf{Q}} = \text{Tr}_{L|\mathbf{Q}} \circ \text{Tr}_{KL|L}$ , und sich für  $\xi \in K$  und  $\eta \in L$  also

$$\text{Tr}_{KL|\mathbf{Q}}(xy) = \text{Tr}_{L|\mathbf{Q}}(\text{Tr}_{KL|L}(xy)) = \text{Tr}_{L|\mathbf{Q}}(\text{Tr}_{KL|L}(x)y) = \text{Tr}_{L|\mathbf{Q}}(\text{Tr}_{K|\mathbf{Q}}(x)y) = \text{Tr}_{K|\mathbf{Q}}(x) \cdot \text{Tr}_{L|\mathbf{Q}}(y)$$

ergibt.

Wir wählen eine lineare Ordnung auf  $[1, k] \times [1, \ell]$ , bezüglich der wir im folgenden unsere Matrixeinträge schreiben. Sind  $(a_{i,s})_{i,s} \in \mathbf{Q}^{k \times k}$  und  $(b_{j,t})_{j,t} \in \mathbf{Q}^{\ell \times \ell}$  gegeben, dann ist

$$(a_{i,s} \cdot b_{j,t})_{(i,j),(s,t)} = (a_{i,s} \cdot b_{j,t})_{(i,j) \in [1,k] \times [1,\ell], (s,t) \in [1,k] \times [1,\ell]} \in \mathbf{Q}^{k\ell \times k\ell},$$

und wir erhalten

$$(a_{i,s'} \cdot b_{j,t'})_{(i,j),(s',t')} = (a_{i,s} \cdot \partial_{j,t})_{(i,j),(s,t)} \cdot (\partial_{i',s'} \cdot b_{j',t'})_{(i',j'),(s',t')},$$

da der Eintrag in Zeile  $(i, s)$  und Spalte  $(j', t')$  des letzteren Matrixprodukts gleich

$$\sum_{(s,t) \in [1,k] \times [1,\ell]} a_{i,s} \cdot \partial_{j,t} \cdot \partial_{s,s'} \cdot b_{t,t'} = a_{i,s'} \cdot b_{j,t'}.$$

Folglich ist

$$\begin{aligned} \det((a_{i,s'} \cdot b_{j,t'})_{(i,j),(s',t')}) &= \det((a_{i,s} \cdot \partial_{j,t})_{(i,j),(s,t)}) \cdot \det((\partial_{i',s'} \cdot b_{j',t'})_{(i',j'),(s',t')}) \\ &= \det((a_{i,s})_{i,s})^\ell \cdot \det((b_{j,t})_{j,t})^k, \end{aligned}$$

denn ein Umsortieren unserer gewählten Reihenfolge bei Zeilen und Spalten simultan ändert am Wert der Determinante nichts und liefert im ersten Faktor eine Blockdiagonalmatrix mit  $\ell$  Blöcken jeweils gleich  $(a_{i,s})_{i,s}$ , im zweiten Faktor eine Blockdiagonalmatrix mit  $k$  Blöcken jeweils gleich  $(b_{j,t})_{j,t}$ .

Wir erhalten so

$$\begin{aligned} \Delta_{KL} &= \det((\text{Tr}_{KL|\mathbf{Q}}(\kappa_i \lambda_j \kappa_s \lambda_t))_{(i,j),(s,t)}) \\ &= \det((\text{Tr}_{K|\mathbf{Q}}(\kappa_i \kappa_s) \text{Tr}_{L|\mathbf{Q}}(\lambda_j \lambda_t))_{(i,j),(s,t)}) \\ &= \det((\text{Tr}_{K|\mathbf{Q}}(\kappa_i \kappa_s)_{i,s})^\ell \cdot \det((\text{Tr}_{L|\mathbf{Q}}(\lambda_j \lambda_t)_{j,t})^k) \\ &= \Delta_K^\ell \cdot \Delta_L^k. \end{aligned}$$

□

Gerne wüßte ich auch noch einen Beweis von  $\text{Tr}_{LK|L}(\mathcal{O}_{KL}) \subseteq \mathcal{O}_L$ , ohne, wie in der Lösung zu Aufgabe 50, Galoistheorie bemühen zu müssen.

**Bemerkung 88** Seien  $s, t \geq 1$  teilerfremd.

Es ist  $\mathbf{Z}[\zeta_{st}] = \mathbf{Z}[\zeta_s] \mathbf{Z}[\zeta_t]$ . Es ist  $\mathbf{Q}(\zeta_{st}) = \mathbf{Q}(\zeta_s) \mathbf{Q}(\zeta_t)$ .

*Beweis.* Seien  $u, v \in \mathbf{Z}$  so, daß  $us + vt = 1$ . Dann ist  $\zeta_{st} = \zeta_{st}^{us+vt} = \zeta_t^u \cdot \zeta_s^v$  und somit auch  $\mathbf{Z}[\zeta_{st}] = \mathbf{Z}[\zeta_s] \mathbf{Z}[\zeta_t]$  und  $\mathbf{Q}(\zeta_{st}) = \mathbf{Q}(\zeta_s) \mathbf{Q}(\zeta_t)$ , da die Inklusion  $\supseteq$  jeweils von vorneherein feststeht. □

**Satz 89 (Z-Maximalordnung von Kreisteilungskörpern)**

Sei  $k \geq 1$ . Es ist  $\mathcal{O}_{\mathbf{Q}(\zeta_k)} = \mathbf{Z}[\zeta_k]$ . Jeder Primteiler von  $\Delta_{\mathbf{Q}(\zeta_k)}$  teilt auch  $k$ .

*Beweis.* Wir führen eine Induktion über  $k \geq 1$ .

Ist  $k$  eine Primpotenz, so sind wir fertig mit dank der Lemmata 86 und 84.

Ist  $k$  keine Primpotenz, so schreibe  $k = st$  mit  $s, t > 1$  teilerfremd.

Unter Verwendung der Eulerschen  $\varphi$ -Funktion ergibt sich

$$[\mathbf{Q}(\zeta_{st}) : \mathbf{Q}] = \varphi(st) = \varphi(s) \cdot \varphi(t) = [\mathbf{Q}(\zeta_s) : \mathbf{Q}] \cdot [\mathbf{Q}(\zeta_t) : \mathbf{Q}].$$

Nach Induktionsvoraussetzung ist jeder Primteiler von  $\Delta_{\mathbf{Q}(\zeta_s)}$  ein Teiler von  $s$  und jeder Primteiler von  $\Delta_{\mathbf{Q}(\zeta_t)}$  ein Teiler von  $t$ . Da  $s$  und  $t$  teilerfremd sind, folgt, daß  $\Delta_{\mathbf{Q}(\zeta_s)}$  und  $\Delta_{\mathbf{Q}(\zeta_t)}$  teilerfremd sind.

Es wird

$$\mathcal{O}_{\mathbf{Q}(\zeta_k)} \stackrel{\text{B. 88}}{=} \mathcal{O}_{\mathbf{Q}(\zeta_s)\mathbf{Q}(\zeta_t)} \stackrel{\text{L. 87.(1)}}{=} \mathcal{O}_{\mathbf{Q}(\zeta_s)} \mathcal{O}_{\mathbf{Q}(\zeta_t)} \stackrel{\text{I.V.}}{=} \mathbf{Z}[\zeta_s] \mathbf{Z}[\zeta_t] \stackrel{\text{B. 88}}{=} \mathbf{Z}[\zeta_k].$$

Ferner wird

$$\Delta_{\mathbf{Q}(\zeta_k)} \stackrel{\text{B. 88}}{=} \Delta_{\mathbf{Q}(\zeta_s)\mathbf{Q}(\zeta_t)} \stackrel{\text{L. 87.(2)}}{=} \Delta_{\mathbf{Q}(\zeta_s)}^{\varphi(t)} \Delta_{\mathbf{Q}(\zeta_t)}^{\varphi(s)},$$

so daß jeder Primteiler von  $\Delta_{\mathbf{Q}(\zeta_k)}$  ein Teiler von  $\Delta_{\mathbf{Q}(\zeta_s)}^{\varphi(t)} \Delta_{\mathbf{Q}(\zeta_t)}^{\varphi(s)}$  und damit nach Induktionsvoraussetzung auch ein Teiler von  $st = k$  ist.  $\square$

Auch eine genaue Formel für  $\Delta_{\mathbf{Q}(\zeta_k)}$  läßt sich mit dieser Argumentation herleiten.

# Anhang A

## Aufgaben und Lösungen

### A.1 Aufgaben

Zum Lösen der Übungsaufgaben kann resp. soll Magma verwandt werden.

Siehe e.g. `magma.maths.usyd.edu.au/calc/`.

**Aufgabe 1 (§1.1)** Zeige oder widerlege.

Sei  $R$  ein Ring.

- (1) Ist  $R$  ein Körper, so ist  $R[X]$  ein Hauptidealbereich.
- (2) Ist  $R$  ein Hauptidealbereich, so auch  $R[X]$ .
- (3) Ist  $R$  ein Hauptidealbereich und ist  $a \in R$ , so ist  $R/\langle a \rangle$  ein Hauptidealbereich.
- (4) Ist  $R$  ein Hauptidealbereich, und ist  $x \in R$  eine Nichteinheit, die nicht in ein Produkt von Nichteinheiten zerlegbar ist, so ist  $R/\langle x \rangle$  ein Körper.

**Aufgabe 2 (§1.2)** Sei  $R$  ein Hauptidealbereich.

- (1) Sei  $n \geq 2$ . Sei  $x = (x_i)_i \in R^{n \times 1}$  mit  $\langle x_1, \dots, x_n \rangle = R$  gegeben.  
Zeige, daß es ein  $A = (a_{i,j})_{i,j} \in \mathrm{SL}_n(R)$  gibt mit  $(a_{i,1})_i = x$ .
- (2) Sei  $R = \mathbf{Z}$ . Sei  $x = \begin{pmatrix} 2 \\ 3 \\ 4 \\ 5 \end{pmatrix}$ . Gib ein  $A \in \mathrm{SL}_4(\mathbf{Z})$  an, welches  $x$  als erste Spalte enthält.

**Aufgabe 3 (§1.2)** Sei  $m \geq 0$ . Sei  $A \in \mathbf{Z}^{m \times m}$ .

Bestimme  $S \in \mathrm{GL}_m(\mathbf{Z})$  und  $T \in \mathrm{GL}_n(\mathbf{Z})$  so, daß  $SAT$  in Elementarteilerform ist. Dokumentiere dabei die Schritte gemäß Beweis zu Satz 4. Vergleiche das Resultat mit dem von `SmithForm` gelieferten.

$$(1) A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

$$(2) A = \begin{pmatrix} 2 & 2 & 3 & 5 \\ 4 & 8 & 5 & 5 \\ 4 & 4 & 1 & 1 \\ -2 & 6 & 6 & 4 \end{pmatrix}.$$

**Aufgabe 4 (§1.2)** Erstelle ein Magma-Programm, welches für  $m, n \geq 0$  die Elementarteiler einer Matrix in  $\mathbf{Z}^{m \times n}$  über Minoren ausrechnet. Verwende `Determinant`.

Vergleiche seine Laufzeit mit der von `SmithForm`.

**Aufgabe 5 (§1.2)** Erstelle ein Magma-Programm, welches für  $m, n \geq 0$  und eine Matrix  $A \in \mathbf{Z}^{m \times n}$  Matrizen  $S \in \mathrm{SL}_m(\mathbf{Z})$  und  $T \in \mathrm{SL}_n(\mathbf{Z})$  so berechnet, daß  $SAT$  in Elementarteilerform ist, wie im Beweis zu Satz 4 beschrieben. Verwende `Matrix(SparseMatrix(...))` und `ExtendedGreatestCommonDivisor`.

Vergleiche seine Laufzeit mit der von `SmithForm`.

**Aufgabe 6 (§1.1)** Sei  $R$  ein Hauptidealbereich. Sei  $x \in R \setminus \{0\}$  gegeben.

Ein Element  $y \in R$  heie *prim*, falls  $R/\langle y \rangle$  ein Integritätsbereich ist.

Eine Nichteinheit  $y \in R$  heie *irreduzibel*, falls sie nicht in ein Produkt zweier Nichteinheiten zerlegt werden kann; cf. Aufgabe 1.(4).

- (1) Zeige, daß ein Element in  $R \setminus \{0\}$  genau dann irreduzibel ist, wenn es prim ist.
- (2) Zeige, daß es eine Zerlegung  $x = ex_1x_2 \cdots x_n$  gibt mit  $x_i \in R$  prim für  $i \in [1, n]$  und einer Einheit  $e \in R$ .
- (3) Sei  $x = ex_1x_2 \cdots x_n = \tilde{e}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_{\tilde{n}}$  mit  $x_i \in R$  prim für  $i \in [1, n]$  und  $\tilde{x}_i$  prim für  $i \in [1, \tilde{n}]$ , sowie Einheiten  $e, \tilde{e} \in R$ . Zeige, daß  $n = \tilde{n}$  und daß es eine Bijektion  $\sigma : [1, n] \xrightarrow{\sim} [1, \tilde{n}]$  so gibt, daß für alle  $i \in [1, n]$  eine Einheit  $f_i \in R$  mit  $x_i = \tilde{x}_{\sigma(i)}f_i$  existiert.

**Aufgabe 7 (§2.2)**

- (1) Weise unter Verwendung von Magma durch direkte Rechnung nach, daß die Einheitengruppe des Körpers  $\mathbf{F}_{2^k}$  mit  $[\mathbf{F}_{2^k} : \mathbf{F}_2] = k$  zyklisch ist für  $k \in [2, 13]$ . Entscheide jeweils, ob es ein  $x \in \mathbf{F}_{2^k}$  mit  $\mathbf{F}_{2^k} = \mathbf{F}_2(x)$ , aber  $\langle x \rangle < \mathbf{F}_{2^k} \setminus \{0\}$  gibt.
- (2) Berechne mittels Magma das Produkt aller normierten irreduziblen Polynome in  $\mathbf{F}_3[X]$ , deren Grad ein Teiler von 12 ist.
- (3) Berechne mittels Magma das Produkt  $\prod_{\xi \in \mathbf{F}_{5^4}} (X - \xi)$ .

**Aufgabe 8 (§2)** Sei  $p$  prim. Sei  $f(X) \in \mathbf{F}_p[X]$  normiert.

- (1) Schreibe ein Magma-Programm, welches  $f(X)$  naiv in Faktoren zerlegt, d.h. durch Absuchen aller normierten Polynome von Grad  $\leq \deg f$ .
- (2) Setze das Cantor-Zassenhaus-Verfahren aus §2.3 in ein Magma-Programm um, samt vorbereitenden Schritten aus §2.1 und §2.2.
- (3) Vergleiche die Laufzeiten der Programme aus (1) und (2) mit dem Magma-Befehl `Factorisation`.

**Aufgabe 9 (§2)** Gemäß Kronecker ist die Faktorisierung eines Polynoms in  $\mathbf{Z}[X]$  in irreduzible Faktoren eine in endlich vielen Schritten durchführbare Aufgabe.

Sei  $f(X) \in \mathbf{Z}[X]$  gegeben. Schreibe  $n := \deg f$ . Wähle  $z_i \in \mathbf{Z}$  für  $i \in [1, n+1]$  mit  $f(z_i) \neq 0$  und  $|\{z_i : i \in [1, n+1]\}| = n+1$ . Ist  $g(X) \in \mathbf{Z}[X]$  ein Teiler von  $f(X)$ , so ist auch  $g(z_i)$  ein Teiler von  $f(z_i)$  für  $i \in [1, n+1]$ . Betrachte die endliche Menge  $T := \{\underline{t} = (t_i)_{i \in [1, n]} : t_i \in \mathbf{Z}, t_i \mid f(z_i) \text{ für } i \in [1, n]\}$ . Zu  $\underline{t} \in T$  gibt es genau ein Polynom  $g_{\underline{t}}(X) \in \mathbf{Q}[X]$  mit  $g_{\underline{t}}(z_i) = t_i$  für  $i \in [1, n]$ . Teste, ob  $g_{\underline{t}}(X)$  ein Teiler von  $f(X)$  ist. Falls ja, teile und setze mit dem Quotienten fort.

Implementiere diesen (nicht optimalen) Algorithmus in Magma. Dies unter Verwendung der dort eingebauten Faktorisierung in  $\mathbf{Z}$  (e.g. `Divisors`), aber nicht der in  $\mathbf{Z}[X]$ .

**Aufgabe 10 (§3.1.1)** Sei  $A$  ein Ring. Sei  $e \in A$  ein Idempotent.

Zeige, daß der  $A$ -Modul  $Ae$  genau dann unzerlegbar ist, wenn  $e$  primitiv ist.

**Aufgabe 11 (§3.1.1)** Sei  $A$  ein Ring. Seien  $e, f \in A$  Idempotente.

Zeige, daß

$$\begin{array}{ccc} \text{Hom}_A(Ae, Af) & \longrightarrow & eAf \\ \varphi & \longmapsto & \varphi(e) \\ (be \mapsto beaf) & \longleftarrow & eaf \end{array}$$

ein Isomorphismus abelscher Gruppen ist, mit Inverser wie angegeben, wobei  $a, b \in A$ .

**Aufgabe 12 (§3.1.2)** Sei  $K$  ein Körper. Sei  $A$  eine endlichdimensionale  $K$ -Algebra.

Zeige, daß in  $A$  eine orthogonale Zerlegung in primitive Idempotente existiert.

Ist diese eindeutig bestimmt?

**Aufgabe 13 (§3.1.2)** Sei  $A$  eine endlichdimensionale  $\mathbf{C}$ -Algebra.

Entscheide, ob  $A$  halbeinfach ist.

- (1)  $A = \mathbf{C}[X]/\langle X^2 \rangle$ .

$$(2) A = \mathbf{C}[X]/\langle X^2 + 1 \rangle.$$

$$(3) A = \begin{pmatrix} \mathbf{C} & \mathbf{C} \\ 0 & \mathbf{C} \end{pmatrix}.$$

**Aufgabe 14 (§3.1.2)** Sei  $K$  ein Körper.

Seien  $A$  und  $B$  endlichdimensionale  $K$ -Algebren. Zeige.

- (1) Sei  $n \geq 0$ . Es ist  $K^{n \times n}$  halbeinfach.
- (2) Sind  $A$  und  $B$  halbeinfach, dann auch  $A \times B$ .
- (3) Ist  $A$  halbeinfach und ist  $f : A \rightarrow B$  ein surjektiver  $K$ -Algebrenmorphismus, dann ist auch  $B$  halbeinfach.

**Aufgabe 15 (§3.1.2)** Sei  $K$  ein Körper. Sei  $A$  eine  $K$ -Algebra. Sei  $M$  ein  $A$ -Modul.

Definiere auf  $\text{End}_A M$  die Struktur einer  $K$ -Algebra, mit Komposition als Multiplikation und mit zugehörigem Ringmorphismus  $\psi : K \rightarrow \text{End}_A M$ ,  $\lambda \mapsto \lambda \text{id}_M$ .

**Aufgabe 16 (§3.2.1)** Sei  $G$  eine endliche Gruppe. Sei  $R \neq 0$  ein kommutativer Ring.

- (1) Zeige, daß  $RG$  ein Ring ist.
- (2) Sei  $K$  ein Körper. Sei  $A$  eine  $K$ -Algebra. Zeige, daß für jeden Gruppenmorphismus  $\varphi : G \rightarrow \text{U}(A)$  genau ein  $K$ -Algebrenmorphismus  $\psi : KG \rightarrow A$  mit  $\psi|_G^{\text{U}(A)} = \varphi$  existiert.

**Aufgabe 17 (§3.2, §3.1.2)** Zeige folgende  $\mathbf{C}$ -Algebrenisomorphismen mittels Magma.

- (1) Sei  $\mathcal{C}_3 := \langle c : c^3 = 1 \rangle$ . Schreibe  $\zeta = \zeta_3 := \exp(2\pi i/3)$ .

$$\begin{aligned} \mathbf{C}\mathcal{C}_3 &\longrightarrow \mathbf{C} \times \mathbf{C} \times \mathbf{C} \\ c &\longmapsto (1, \zeta, \zeta^2) \end{aligned}$$

- (2) Sei  $\mathcal{S}_3$  die symmetrische Gruppe auf 3 Elementen.

$$\begin{aligned} \mathbf{C}\mathcal{S}_3 &\longrightarrow \mathbf{C} \times \mathbf{C}^{2 \times 2} \times \mathbf{C} \\ (1, 2) &\longmapsto (1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1) \\ (1, 2, 3) &\longmapsto (1, \begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}, 1) \end{aligned}$$

- (3) Sei  $\mathcal{S}_4$  die symmetrische Gruppe auf 4 Elementen.

$$\begin{aligned} \mathbf{C}\mathcal{S}_4 &\longrightarrow \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{3 \times 3} \times \mathbf{C}^{3 \times 3} \times \mathbf{C}^{2 \times 2} \\ (1, 2) &\longmapsto (1, -1, \begin{pmatrix} -11 & -24 & 2 \\ 5 & 11 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -5 & 24 \\ -1 & 5 \end{pmatrix}) \\ (1, 2, 3, 4) &\longmapsto (1, -1, \begin{pmatrix} 26 & 57 & 2 \\ -11 & -24 & -1 \\ -4 & -8 & -1 \end{pmatrix}, \begin{pmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ -4 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & -15 \\ 1 & -4 \end{pmatrix}) \end{aligned}$$

(4) Sei  $\mathcal{D}_{10} := \langle a, b : a^5 = 1, b^2 = 1, (ba)^2 = 1 \rangle$ . Sei  $\vartheta \in \mathbf{C}$  mit  $\vartheta^2 + 5\vartheta + 5 = 0$ .

$$\begin{aligned} \mathbf{C}\mathcal{D}_{10} &\longrightarrow \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{2 \times 2} \times \mathbf{C}^{2 \times 2} \\ a &\longmapsto (1, 1, \begin{pmatrix} 1 & 1 \\ \vartheta & \vartheta+1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -\vartheta-5 & -\vartheta-4 \end{pmatrix}) \\ b &\longmapsto (1, -1, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}) \end{aligned}$$

**Aufgabe 18 (§3.2.1)** Zeige, daß  $\mathbf{Z}\mathcal{S}_3$  zum Teilring

$$\{(a, \begin{pmatrix} b & c \\ 3d & e \end{pmatrix}, f) : a, b, c, d, e, f \in \mathbf{Z}, a \equiv_2 f, a \equiv_3 b, e \equiv_3 f\} \subseteq \mathbf{Z} \times \mathbf{Z}^{2 \times 2} \times \mathbf{Z}$$

isomorph ist. (Hinweis: In Aufgabe 17.(2) Bild betrachten.)

**Aufgabe 19 (§3.2.2)** Sei  $K$  ein Körper. Sei  $G$  eine endliche Gruppe.

Zeige, daß  $KG$  genau dann halbeinfach ist, wenn  $|G|$  kein Vielfaches von  $\text{char } K$  ist.

**Aufgabe 20 (§3.2.1)** Zeige oder widerlege.

Sei  $G$  eine endliche Gruppe.

- (1) Es ist  $\mathbf{Z}G$  nullteilerfrei.
- (2) Es enthält  $\mathbf{Z}G$  nur die Idempotente 0 und 1. (Hinweis: Spur von Multiplikation mit  $e$  in Basis  $G$  und bezüglich  $\mathbf{Z}Ge \oplus \mathbf{Z}G(1-e)$  vergleichen).
- (3) Es enthält  $\mathbf{C}G$  keine nilpotenten Elemente ungleich 0.
- (4) Ist  $G$  abelsch, so enthält  $\mathbf{C}G$  keine nilpotenten Elemente ungleich 0.
- (5) Sei  $p$  prim. Ist  $G$  eine  $p$ -Gruppe, so sind alle einfachen  $\mathbf{F}_p G$ -Linksmoduln isomorph.

**Aufgabe 21 (§3.3.4, Aufgabe 12)** Sei  $K$  ein Körper.

Sei  $A$  eine kommutative endlichdimensionale  $K$ -Algebra.

Zeige, daß es (bis auf Reihenfolge) genau eine orthogonale Zerlegung in primitive Idempotente in  $A$  gibt. (Hinweis: Verwende Aufgabe 12.)

**Aufgabe 22 (§3.3)** Sei  $G$  eine endliche Gruppe.

Sei  $t \geq 0$  und  $n_s \geq 1$  für  $s \in [1, t]$  mit  $\mathbf{C}G \simeq \prod_{i \in [1, t]} \mathbf{C}^{n_s \times n_s}$ .

Wir schreiben  $g^G := \{x^{-1}gx : x \in G\}$  für die Konjugationsklasse von  $g \in G$ .

- (1) Zeige, daß  $Z(\mathbf{C}G) \simeq \mathbf{C}^{\times t}$  als  $\mathbf{C}$ -Algebren.
- (2) Zeige, daß  $Z(\mathbf{C}G) = \mathbf{C} \langle \sum_{x \in g^G} x : g \in G \rangle$ .

(3) Folgere, daß  $|\{g^G : g \in G\}| = \dim_{\mathbf{C}} \mathbf{Z}(\mathbf{C}G) = t$ .

**Aufgabe 23 (§3.3.4)** Sei  $G$  eine endliche Gruppe.

Sei  $\chi$  ein irreduzibler Charakter von  $G$ . Sei  $g \in G$  ein Element von Ordnung  $k := |\langle g \rangle|$ .

- (1) Schreibe  $\zeta = \zeta_k := \exp(2\pi i/k)$ . Zeige, daß  $\chi(g) = \sum_{j \in [0, k-1]} x_j \zeta^j$  für gewisse  $x_j \in \mathbf{Z}_{\geq 0}$  mit  $\sum_{j \in [0, k-1]} x_j = \chi(1)$ .
- (2) Zeige, daß  $\chi(g^{-1}) = \overline{\chi(g)}$  (komplexe Konjugation).
- (3) Zeige, daß auch  $G \rightarrow \mathbf{C}$ ,  $h \mapsto \overline{\chi(h)}$  ein irreduzibler Charakter von  $G$  ist. (Hinweis: Dualraum.)

**Aufgabe 24 (§3.3.1)**

- (1) Bestimme die Charaktertafel von  $\mathcal{C}_3$ .
- (2) Bestimme die Charaktertafel von  $\mathcal{S}_3$ .
- (3) Bestimme die Charaktertafel von  $\mathcal{S}_4$ .
- (4) Bestimme die Charaktertafel von  $\mathcal{D}_{10}$ .

Vergleiche jeweils mit der von Magma gelieferten Charaktertafel.  
(Hinweis: Aufgabe 17.)

**Aufgabe 25 (§3.3.1)** Sei  $H$  und  $G$  endliche Gruppen.

Sei  $\varphi : H \rightarrow G$  ein Gruppenmorphismus.

- (1) Sei  $\chi$  ein Charakter von  $G$ . Zeige, daß  $\chi \circ \varphi$  ein Charakter von  $H$  ist.
- (2) Sei  $\varphi$  surjektiv. Sei  $\chi$  ein irreduzibler Charakter von  $G$ . Zeige, daß  $\chi \circ \varphi$  ein irreduzibler Charakter von  $H$  ist.
- (3) Betrachte den injektiven Gruppenmorphismus  $\varphi : \mathcal{S}_3 \hookrightarrow \mathcal{S}_4$ . Zerlege  $\chi|_{\mathcal{S}_3} := \chi \circ \varphi$  in irreduzible Charaktere für alle irreduziblen Charaktere  $\chi$  der  $\mathcal{S}_4$ .
- (4) Zeige, daß  $\varphi : \mathcal{S}_4 \rightarrow \mathcal{S}_3$ ,  $(1, 2) \mapsto (1, 2)$ ,  $(2, 3) \mapsto (2, 3)$ ,  $(3, 4) \mapsto (1, 2)$  ein surjektiver Gruppenmorphismus ist. Finde den irreduziblen Charakter  $\chi \circ \varphi$  in der Charaktertafel von  $\mathcal{S}_4$  für alle irreduziblen Charaktere  $\chi$  von  $\mathcal{S}_3$ .

**Aufgabe 26 (§3.3.1)** Sei  $G$  eine endliche Gruppe.

Gegeben seien  $\mathbf{C}G$ -Moduln  $V$  und  $W$ . Dies sind insbesondere  $\mathbf{C}$ -Vektorräume.

- (1) Definiere auf  $V \otimes_{\mathbf{C}} W$  eine  $\mathbf{C}G$ -Modulstruktur mit  $g(v \otimes w) = gv \otimes gw$  für  $g \in G$ ,  $v \in V$  und  $w \in W$ .
- (2) Seien  $\chi$  und  $\psi$  Charaktere von  $G$ . Zeige, daß auch  $\chi \cdot \psi : G \rightarrow \mathbf{C}$ ,  $g \mapsto \chi(g) \cdot \psi(g)$  ein Charakter von  $G$  ist. (Hinweis: Tensoriere Moduln zu  $\chi$  und  $\psi$ .)

**Aufgabe 27 (§3.3.1)** Wir betrachten die Charaktertafel der  $\mathcal{S}_4$  in den Bezeichnungen der Lösung zu Aufgabe 24.(3).

- (1) Verifiziere Satz 38.(1) für  $\chi_r$  und  $\chi_s$  mit  $(r, s) \in \{(4, 4), (4, 5), (5, 5)\}$ .
- (2) Schreibe den Charakter  $\chi_4 \cdot \chi_5$  als Linearkombination irreduzibler Charaktere mit Koeffizienten in  $\mathbf{Z}_{\geq 0}$ .
- (3) Bestimme das zu  $\chi_4$  gehörige primitive zentrale Idempotent  $\varepsilon_4 \in \mathbf{C}\mathcal{S}_4$ . (Hinweis: Lemma 37.)

**Aufgabe 28 (§3.3.1, §3.1.2)** Sei  $G$  eine endliche Gruppe.

Sei  $\omega : \mathbf{C}G \xrightarrow{\sim} \mathbf{C}^{n_1 \times n_1} \times \dots \times \mathbf{C}^{n_t \times n_t}$  ein Wedderburnisomorphismus, mit Bezeichnungen wie in §3.3.1.

Zeige, daß

$$\omega^{-1}(z^1, \dots, z^t) = \sum_{g \in G} \left( \frac{1}{|G|} \sum_{s \in [1, t]} n_s \operatorname{tr}(\omega^s(g^{-1}) z^s) \right) g$$

wobei  $z^s \in \mathbf{C}^{n_s \times n_s}$ .

**Aufgabe 29 (§3.4.2)** Sei  $K$  ein Körper. Sei  $n \geq 1$ . Sei  $A \in K^{n \times n}$ .

Sei  $k \geq 1$ . Sei  $x_i \in K^{n \times 1}$  ein Eigenvektor von  $A$  zum Eigenwert  $\lambda_i \in K$  gegeben für  $i \in [1, k]$ . Sei hierbei  $(x_1, \dots, x_k)$  linear unabhängig.

Seien  $\mu_i \in K \setminus \{0\}$  für  $i \in [1, k]$  so, daß  $y := \sum_{i \in [1, k]} \mu_i x_i$  ein Eigenvektor von  $A$  ist.

Zeige, daß  $\lambda_i = \lambda_j$  für alle  $i, j \in [1, k]$ .

**Aufgabe 30 (§3.4.2)** Sei  $p$  prim. Sei  $n \geq 1$ . Sei  $k \geq 1$ . Seien  $A_1, \dots, A_k \in \mathbf{F}_p^{n \times n}$ .

Schreibe eine Magma-Funktion, die eine Matrix mit linear unabhängigem Spaltentupel maximaler Größe ausgibt, deren Spalten aus gemeinsamen Eigenvektoren von  $A_i$  für  $i \in [1, k]$  bestehen. (Hinweis: Verwende  $\mathbf{Eigenvalues}(A)$ . Vorsicht,  $\mathbf{Kernel}(A)$  und  $\mathbf{VectorSpace}(\mathbf{GF}(p), n)$  arbeiten mit Zeilen, es muß mit  $\mathbf{Transpose}(A)$  geeignet transponiert werden.)

**Aufgabe 31 (§3.4.1)** Sei  $G$  eine endliche Gruppe. Sei  $G = \bigsqcup_{s \in [1, t]} g_s^G$ .

Sei  $K_s := \sum_{x \in g_s^G} x$  für  $s \in [1, t]$ . Sei  $K_r \cdot K_s := \sum_{a \in [1, t]} \gamma_{r, s, a} K_a$  für  $r, s \in [1, t]$ , wobei  $\gamma_{r, s, a} \in \mathbf{Z}_{\geq 0}$ ; cf. Aufgabe 22.(2), Bemerkung 43. Sei  $p$  eine Primzahl. Sei  $\theta : \mathbf{Z} \rightarrow \mathbf{F}_p$  die Restklassenabbildung. (In der Notation von Bemerkung 46 wäre dies  $\theta|_{\mathbf{Z}}$ .)

Schreibe eine Magma-Funktion, die in Abhängigkeit von  $G$  (als Untergruppe einer symmetrischen Gruppe vorliegend) und  $p$  das Tupel

$$\left( (\theta(\gamma_{r, s, a}))_{s, a} \right)_r$$

von Matrizen in  $\mathbf{F}_p^{t \times t}$  berechnet, und dieses zusammen mit  $t$ , Repräsentanten der Konjugationsklassen und den Konjugationsklassen zurückgibt.

(Hinweis: Bemerkung 45, `ConjugacyClasses(S)` [i].)

**Aufgabe 32 (§3.4)** Sei  $n \in \mathbf{Z}_{\geq 1}$ .

- (1) Sei  $b \in n\mathbf{Z}$ . Sei  $q$  ein Primteiler von  $\Phi_n(b)$ . Zeige, daß  $q \equiv_n 1$ . (Hinweis: Ist  $r$  maximal mit  $b^n \equiv_{q^r} 1$ , dann ist  $n$  die Ordnung von  $b$  in  $\mathbf{Z}/q^r$ , aber  $n$  und  $q$  sind teilerfremd.)
- (2) Zeige, daß  $\{p \in \mathbf{Z}_{>0} : p \text{ prim, } p \equiv_n 1\}$  unendlich ist.  
(Hinweis: Annahme, nicht. Sei  $P$  das Produkt der endlich vielen. Sei  $x \in \mathbf{Z}$  so, daß  $\Phi_n(xPn) > 1$ . Sei  $q$  ein Primteiler von  $\Phi_n(xPn)$ . Verwende (1).)

**Aufgabe 33 (§3.4)** Sei  $G$  eine endliche Gruppe.

Sei  $G = \bigsqcup_{s \in [1, t]} g_s^G$ . Sei  $e := \text{kgV}(|\langle g_1 \rangle|, \dots, |\langle g_t \rangle|)$ .

Schreibe eine Magma-Funktion, die in Abhängigkeit von  $G$  die kleinste Primzahl  $p$  mit  $p > |G|$  und  $p \equiv_e 1$  findet, einen Ringmorphismus  $\theta : \mathbf{Z}[\zeta_e] \rightarrow \mathbf{F}_p$  konstruiert, welcher  $\zeta_e$  auf ein Element der Ordnung  $e$  in  $U(\mathbf{F}_p)$  schickt, und welche  $\mathbf{Z}[\zeta_e]$ ,  $\theta$ ,  $p$ ,  $e$  und  $\zeta_e$  zurückgibt. (Hinweis: `IsPrime(n)`, `Exponent(G)`.)

**Aufgabe 34 (§3.4.4)**

- (1) Setze den Dixon-Algorithmus aus §3.4.4 in ein Magma-Programm um, welches zu einer endlichen Gruppe  $G$  die Charakertafel berechnet, sofern eine Primzahl  $p$  wie zu Beginn von §3.4 gefunden werden kann. Gib den Exponenten  $e$  von  $G$  und die Konjugationsklassenrepräsentanten  $g_i$  mit aus. (Hinweis: Aufgaben 30, 31, 33.)
- (2) Vergleiche die Resultate aus Aufgabe 24 mit dem jeweiligen aus (1).
- (3) Vergleiche das Resultat von `CharacterTable` bei  $\mathcal{S}_6$  und  $\mathcal{A}_6$  mit dem jeweiligen aus (1).

**Aufgabe 35 (§4.1)** Sei  $R$  ein Ring. Ein  $R$ -Modul  $M$  heißt *endlich erzeugt*, wenn es eine endliche Teilmenge  $X \subseteq M$  mit  $M = {}_R\langle X \rangle$  gibt.

- (1) Sei  $M \xrightarrow{p} M''$  eine surjektive  $R$ -lineare Abbildung zwischen  $R$ -Moduln. Seien  $M''$  und  $\text{Kern } p$  endlich erzeugt. Zeige, daß  $M$  endlich erzeugt ist.
- (2) Sei  $R$  ein Hauptidealbereich. Sei  $N$  ein endlich erzeugter  $R$ -Modul. Sei  $M \subseteq N$  ein Teilmodul. Zeige, daß  $M$  ein endlich erzeugter  $R$ -Modul ist.

**Aufgabe 36 (§4.1)** Ist  $R$  ein Hauptidealbereich? (Hinweise:  $f : R \setminus \{0\} \rightarrow \mathbf{Z}_{\geq 0}$  so, daß  $r = sq + p$  mit  $f(p) \in [0, f(s) - 1]$ . Indizes von Idealen betrachten.)

- (1)  $R = \mathbf{Z}[i]$ .
- (2)  $R = \mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[i\sqrt{5}]$ .
- (3)  $R = \mathbf{Z}[\zeta_3]$ .

**Aufgabe 37 (§3.3.1, §4.1)** Sei  $G$  eine endliche Gruppe.

Sei  $\omega : \mathbf{C}G \xrightarrow{\sim} \mathbf{C}^{n_1 \times n_1} \times \dots \times \mathbf{C}^{n_t \times n_t}$  ein Wedderburnisomorphismus; cf. §3.3.1.

Wir verwenden die Bezeichnungen von §3.4.

Zeige, daß  $n_s$  ein Teiler von  $|G|$  ist für  $s \in [1, t]$ .

(Hinweis: Bemerkung 45, Aufgabe 23.(1), Satz 38.(1).)

**Aufgabe 38 (§4.1)**

- (1) Sei  $R$  ein Hauptidealbereich. Sei  $Q = \text{frac } R$  sein Quotientenkörper.  
Sei  $f(X) \in R[X] \setminus \{0\}$ . Sei  $f(X) = u(X) \cdot v(X)$  mit  $u(X), v(X) \in Q[X]$ . Zeige, daß es ein  $q \in Q \setminus \{0\}$  gibt mit  $q \cdot u(X) \in R[X]$  und  $q^{-1} \cdot v(X) \in R[X]$ .
- (2) Sei  $K|\mathbf{Q}$  eine endliche Erweiterung. Sei  $\alpha \in K$ . Zeige, daß genau dann  $\alpha \in \mathcal{O}_K$  ist, wenn  $\mu_{\alpha, \mathbf{Q}}(X) \in \mathbf{Z}[X]$ . (Hinweis:  $R = \mathbf{Z}$ .)

**Aufgabe 39 (§4.1, Aufgabe 38)**

Sei  $d \in \mathbf{Z} \setminus \{0, 1\}$  quadratfrei, i.e. nicht durch das Quadrat einer Primzahl teilbar.

Bestimme  $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ . (Hinweis: Aufgabe 38.(2).)

Gib ein solches  $d$  an mit  $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$  kein Hauptidealbereich.

Gib ein solches  $d$  an mit  $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} \neq \mathbf{Z}[\sqrt{d}]$ .

**Aufgabe 40 (§4.3, Aufgabe 38)** Sei  $K|\mathbf{Q}$  eine endliche Erweiterung. Sei  $\alpha \in K$ .

Sei  $\mu_{\alpha, \mathbf{Q}}(X) = X^m + \sum_{i \in [0, m-1]} a_i X^i$  mit  $m \geq 1$  und  $a_i \in \mathbf{Q}$  für  $i \in [1, m-1]$ .

- (1) Zeige, daß  $\text{Tr}_{K|\mathbf{Q}}(\alpha) = -[K : \mathbf{Q}(\alpha)] \cdot a_{m-1}$ .
- (2) Folgere, daß  $\text{Tr}_{K|\mathbf{Q}}(\mathcal{O}_K) \subseteq \mathbf{Z}$ . (Hinweis: Aufgabe 38.(2).)

**Aufgabe 41 (§4.2)** Sei  $G$  ein  $\mathbf{Z}$ -Gitter in  $K$ . Zeige.

- (1) Es ist  $\Delta(G^\#) = \Delta(G)^{-1}$ .
- (2) Ist  $G$  ein  $\mathbf{Z}$ -Gitter in  $K$  mit  $G \subseteq G^\#$ , dann ist  $|\Delta(G)| = |G^\# / G|$  und  $\Delta(G) \cdot G^\# \subseteq G$ .

**Aufgabe 42 (§4.2, Aufgabe 39)**

Sei  $d \in \mathbf{Z} \setminus \{0, 1\}$  quadratfrei, i.e. nicht durch das Quadrat einer Primzahl teilbar.

Schreibe  $K := \mathbf{Q}(\sqrt{d})$ . Gib eine  $\mathbf{Z}$ -lineare Basis von  $\mathcal{O}_K$  und eine dazu bezüglich der Spurbilinearform duale Basis an. Bestimme die Diskriminante  $\Delta_K$ .

(Hinweis: Aufgabe 39.)

**Aufgabe 43 (Aufgabe 44)** Sei  $K|\mathbf{Q}$  eine endliche Körpererweiterung. Sei  $n := [K : \mathbf{Q}]$ .

Sei  $G \subseteq K$  ein  $\mathbf{Z}$ -Gitter. Sei  $G = \mathbf{z}\langle \beta_1, \dots, \beta_m \rangle$  für ein  $m \geq n$  und  $\beta_i \in G$  für  $i \in [1, m]$ .

Schreibe ein Magma-Programm `zbasis`, das eine  $\mathbf{Z}$ -lineare Basis von  $G$  berechnet; cf. Beweis zu Bemerkung 65.

Verwende dazu `ElementToSequence`.

**Aufgabe 44 (§4.5.1)** Sei  $K|\mathbf{Q}$  eine endliche Körpererweiterung. Sei  $n := [K : \mathbf{Q}]$ .

Sei  $R \subseteq K$  eine  $\mathbf{Z}$ -Ordnung. Sei eine  $\mathbf{Z}$ -lineare Basis  $(\beta_1, \dots, \beta_n)$  von  $R$  bekannt.

Schreibe ein Magma-Programm, das eine  $\mathbf{Z}$ -lineare Basis von  $\text{Jac}_p(R)$  berechnet. Cf. Algorithmus 73.

Verwende dazu `BasisMatrix` und `Kernel`, sowie `zbasis` aus Aufgabe 43.

**Aufgabe 45 (§4.2, §4.3)** Sei  $K|\mathbf{Q}$  eine endliche Körpererweiterung.

- (1) Seien  $G$  und  $H$  zwei  $\mathbf{Z}$ -Gitter in  $K$  mit  $G \subseteq H$ . Zeige, daß  $|H/G| = |G^\# / H^\#|$ .
- (2) Sei  $R$  eine  $\mathbf{Z}$ -Ordnung in  $K$ . Sei  $\Delta(R)$  quadratfrei, i.e. nicht durch das Quadrat einer Primzahl teilbar.  
Zeige, daß  $R = \mathcal{O}_K$ .

- (3) Sei  $\alpha \in \mathbf{C}$  eine Nullstelle des irreduziblen Polynoms  $X^3 + X + 1 \in \mathbf{Q}[X]$ . Sei  $K := \mathbf{Q}(\alpha)$ . Zeige, daß  $\mathcal{O}_K = \mathbf{Z}[\alpha]$ .

**Aufgabe 46 (§4.2)** Sei  $K|\mathbf{Q}$  eine endliche Erweiterung.

Seien  $G$  und  $H$  zwei  $\mathbf{Z}$ -Gitter in  $K$ . Zeige.

- (1) Es ist  $G \cap H$  ein  $\mathbf{Z}$ -Gitter in  $K$ .
- (2) Es ist  $G + H = \{g + h : g \in G, h \in H\}$  ein  $\mathbf{Z}$ -Gitter in  $K$ .
- (3) Es ist  $(G + H)^\# = G^\# \cap H^\#$  und  $(G \cap H)^\# = G^\# + H^\#$ .

**Aufgabe 47 (§4.4, §4.5.2)** Sei  $K|\mathbf{Q}$  eine endliche Körpererweiterung. Sei  $n := [K : \mathbf{Q}]$ .

Sei  $G \subseteq K$  ein  $\mathbf{Z}$ -Gitter. Sei eine  $\mathbf{Z}$ -lineare Basis  $(\alpha_1, \dots, \alpha_n)$  von  $G$  bekannt.

- (1) Schreibe ein Magma-Programm, das die Diskriminante  $\Delta(G)$  berechnet. Verwende dazu `NumberField` (für Testdaten), `Trace`, `Determinant`.
- (2) Schreibe ein Magma-Programm, das von der  $\mathbf{Z}$ -Ordnung  $\text{Stab}(G)$  in  $K$  eine  $\mathbf{Z}$ -lineare Basis berechnet; cf. Algorithmus 76. Verwende dazu `SmithForm`.

**Aufgabe 48 (§4.5.4)**

- (1) Schreibe ein Magma-Programm, das ausgehend von einer endlichen Erweiterung  $K|\mathbf{Q}$  die  $\mathbf{Z}$ -Maximalordnung  $\mathcal{O}_K$  berechnet; cf. Algorithmus 82. (Hinweis: Aufgaben 44, 47.)
- (2) Finde experimentell ein normiertes Polynom  $f(X) \in \mathbf{Z}[X]$  von Grad 3 mit Koeffizienten von Betrag  $\leq 30$  so, daß für  $\alpha \in \mathbf{C}$  mit  $f(\alpha) = 0$  der Algorithmus aus (1) angewandt auf  $\mathbf{Q}(\alpha)$  im Verlauf seiner Ausführung möglichst oft die Ordnung vergrößert. Selbe Frage für möglichst viele verschiedene Primfaktoren in  $|\mathcal{O}_{\mathbf{Q}(\alpha)}/\mathbf{Z}[\alpha]|$ .

**Aufgabe 49 (§4.6.1.1)** Sei  $p \in \mathbf{Z}_{>0}$  prim. Sei  $m \geq 1$ .

Schreibe  $\zeta := \zeta_{p^m}$ . Schreibe  $q := p^{m-1}$ .

- (1) Zeige, daß  $|\mathbf{Z}[\zeta]/\mathbf{z}[\zeta]\langle \zeta^q - 1 \rangle| = p^m$ .
- (2) Zeige, daß  $|\Delta(\mathbf{Z}[\zeta])| = p^{q(mp-m-1)}$ .  
(Hinweis: Berechne  $|\mathbf{Z}[\zeta]^\#/\mathbf{z}[\zeta]\langle \zeta^q - 1 \rangle|$  und verwende (1) und Bemerkung 83.)

**Aufgabe 50 (§4.6.2)** Seien  $E|K|\mathbf{Q}$  endliche Erweiterungen.

Zeige, daß  $\text{Tr}_{E|K}(\mathcal{O}_E) \subseteq \mathcal{O}_K$ .

(Hinweis: Verwende Galoistheorie, nicht die Methoden von Aufgaben 38 und 40.)

**Aufgabe 51 (§4.5.3, §4.6.1.2)** Sei  $\alpha \in \mathbf{C}$  algebraisch über  $\mathbf{Q}$ . Sei  $p \in \mathbf{Z}_{>0}$  prim.

Für ein Polynom  $f(X) \in \mathbf{Z}[X]$  schreiben wir  $\bar{f}(X) \in \mathbf{F}_p[X]$  für seine Restklasse.

Sei  $k \geq 1$ ,  $e_i \geq 1$  und  $f_i(X) \in \mathbf{Z}[X]$  normiert für  $i \in [1, k]$  so, daß

$$\bar{\mu}_{\alpha, \mathbf{Q}}(X) = \bar{f}_1(X)^{e_1} \cdots \bar{f}_k(X)^{e_k}$$

ist mit  $\bar{f}_i(X)$  irreduzibel für  $i \in [1, k]$ .

Schreibe  $g(X) := f_1(X) \cdots f_k(X)$  und  $h(X) := f_1(X)^{e_1-1} \cdots f_k(X)^{e_k-1}$ .

Es ist  $g(X)h(X) = \mu_{\alpha, \mathbf{Q}}(X) + pa(X)$  für ein  $a(X) \in \mathbf{Z}[X]$ .

Sei vorausgesetzt, daß  $\bar{f}_i(X)$  kein Teiler von  $\bar{a}(X)$  ist für  $i \in [1, k]$  mit  $e_i \geq 2$ .

- (1) Zeige, daß  $\text{Jac}_p(\mathbf{Z}[\alpha]) = \mathbf{z}[\alpha] \langle p, g(\alpha) \rangle \subseteq \mathbf{Z}[\alpha]$ .  
(Hinweis: Urbilder nilpotenter Elemente.)
- (2) Zeige, daß  $p$  kein Teiler von  $|\mathcal{O}_{\mathbf{Q}(\alpha)}/\mathbf{Z}[\alpha]|$  ist. (Hinweis: Satz 79.(2).)
- (3) Verwende (2), um in Magma ein hinreichendes Kriterium dafür zu implementieren, daß  $\mathbf{Z}[\alpha]$  bereits eine  $\mathbf{Z}$ -Maximalordnung ist. Verwende **Factorisation**.  
(Hinweis: Aufgabe 47.(1) für benötigte Primzahlen.)
- (4) Zeige durch eine Anwendung von (2) auf  $\alpha := \zeta_p^m - 1$  für  $p$  prim und  $m \geq 1$  erneut, daß  $\mathbf{Z}[\zeta_p^m] = \mathcal{O}_{\mathbf{Q}(\zeta_p^m)}$ . Verwende hierzu die Diskriminante aus Lemma 84. Verwende ferner, daß  $\mu_{\alpha, \mathbf{Q}}(X) \equiv_p X^{p^{m-1}(p-1)}$  gemäß Beweis zu Bemerkung 85.

## A.2 Lösungen

### Aufgabe 1

- (1) Die Aussage ist richtig. Sei  $\langle 0 \rangle \neq I \subseteq R[X]$  ein Ideal. Wir wollen zeigen, daß  $I$  von einem Element erzeugt wird. Sei  $f(X)$  ein Element minimalen Grades von  $I \setminus \{0\}$ . Wir wollen zeigen, daß  $I \stackrel{!}{=} \langle f(X) \rangle$ . Zu zeigen ist hiervon nur  $I \stackrel{!}{\subseteq} \langle f(X) \rangle$ . Sei  $g(X) \in I$ . Dank Polynomdivision können wir  $a(X), b(X) \in R[X]$  so finden, daß  $g(X) = f(X)a(X) + b(X)$  und daß  $b(X) = 0$  oder  $(b(X) \neq 0$  und  $\deg b < \deg f$ ).

*Angenommen*, es ist  $b(X) \neq 0$ . Dann ist  $b(X) = g(X) - f(X)a(X) \in I \setminus \{0\}$ . Da  $\deg b < \deg f$  ist, ist das aber ein *Widerspruch* zur Wahl von  $f(X)$ .

Also ist  $b(X) = 0$ . Es folgt  $g(X) = f(X)a(X) \in I$ .

- (2) Die Aussage ist falsch. Wir wollen dazu zeigen, daß  $\mathbf{Z}[X]$  kein Hauptidealbereich ist. Hierzu wiederum wollen wir zeigen, daß  $\langle 2, X \rangle$  nicht von einem Element erzeugt ist.

Sei *angenommen*, es ist  $\langle 2, X \rangle = \langle f(X) \rangle$  für ein  $f(X) \in \mathbf{Z}[X]$ . Dann ist 2 ein Vielfaches von  $f(X)$ . Somit ist  $\deg f = 0$ . Ferner ist  $X$  ein Vielfaches von  $f$ . Somit ist der Leitkoeffizient von  $f(X)$  in  $\{-1, +1\}$ . Zusammengenommen ist  $f(X)$  in  $\{-1, +1\}$ , und also  $\langle 2, X \rangle = \langle f(X) \rangle = \mathbf{Z}[X]$ . Insbesondere gibt es  $u(X), v(X) \in \mathbf{Z}[X]$  mit  $u(X) \cdot 2 + v(X) \cdot X = 1$ . Einsetzen von 0 liefert  $u(0) \cdot 2 + v(0) \cdot 0 = 1$  in  $\mathbf{Z}$ . Somit ist 1 in  $\mathbf{Z}$  ein Vielfaches von 2, und wir haben einen *Widerspruch*.

- (3) Die Aussage ist falsch. Wir wollen dazu zeigen, daß  $\mathbf{Z}/\langle 4 \rangle$  kein Hauptidealbereich ist. In der Tat ist dieser Ring wegen  $2 + \langle 4 \rangle \neq 0$ , aber  $(2 + \langle 4 \rangle)^2 = 0$  nicht nullteilerfrei.

- (4) Die Aussage ist richtig. Sei  $x \in R$  eine nicht in ein Produkt von Nichteinheiten zerlegbare Nichteinheit. Man nennt ein solches  $x$  auch *irreduzibel*.

Wir wollen zeigen, daß  $R/\langle x \rangle$  ein Körper ist, i.e. daß  $\langle x \rangle \subset R$  ein maximales Ideal ist. *Annahme*, nicht. Dann gibt es ein Ideal  $I$  in  $R$  mit  $\langle x \rangle \subset I \subset R$ . Da  $R$  ein Hauptidealbereich ist, gibt es ein  $y \in R$  mit  $I = \langle y \rangle$ . Da  $\langle y \rangle \subset R$ , ist  $y$  eine Nichteinheit. Da  $\langle x \rangle \subseteq \langle y \rangle$ , gibt es ein  $z \in R$  mit  $x = yz$ . Da  $\langle x \rangle \neq \langle y \rangle$ , ist  $z$  eine Nichteinheit. Wir haben einen *Widerspruch*.

Insbesondere ist  $R/\langle x \rangle$  für irreduzibles  $x \in R$  ein Integritätsbereich, i.e.  $x$  ist *prim*.

### Aufgabe 2

- (1) Nach Satz 4 gibt es ein  $S \in \mathrm{SL}_n(R)$  und ein  $T \in \mathrm{SL}_1(R) = \{(1)\}$  mit  $Sx = SxT =: y$  in Elementarteilerform. Also ist  $y = \begin{pmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$  für ein  $d_1 \in R$ . Da  $x = S^{-1}y$ , ist  $x$  das  $d_1$ -fache der ersten Zeile von  $S^{-1}$ . Da  $\langle x_1, \dots, x_n \rangle = R$ , ist  $d_1$  eine Einheit. Es ist

$$A := S^{-1} \mathrm{diag}(d_1, d_1^{-1}, 1, \dots, 1) \in \mathrm{SL}_n(R)$$

und hat  $x$  als erste Spalte.

- (2) Magma gibt via

```
Z := Integers();
M := RMatrixSpace(Z,4,1);
x := M!Matrix([[2],[3],[4],[5]]);
y,S,T := SmithForm(x);
print S^(-1)*DiagonalMatrix([y[1,1],y[1,1]^(-1),1,1]); // y[1,1] ist zufaellig gleich 1
```

die Matrix

$$A := \begin{pmatrix} 2 & -1 & 1 & -1 \\ 3 & -1 & 2 & -1 \\ 4 & -2 & 3 & -1 \\ 5 & -2 & 3 & -1 \end{pmatrix} \in \mathrm{SL}_4(\mathbf{Z}).$$

Frei Auge kann man die Matrix

$$A := \begin{pmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 5 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_4(\mathbf{Z})$$

erkennen.

### Aufgabe 3

- (1) Das Verfahren gibt folgende Umformungsschritte. Wir lassen hierbei wirkungslose Umformungsschritte weg und fassen ab und an mehrere Schritte zusammen.

$$\begin{aligned} & \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 3 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -3 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \end{pmatrix} \\ \rightsquigarrow & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 0 & 12 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 12 \end{pmatrix} \end{aligned}$$

Dies gibt auch

$$S := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 2 \\ 0 & -2 & 3 \end{pmatrix} \begin{pmatrix} 2 & -1 & 0 \\ -3 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 0 \\ 3 & -2 & 2 \\ 6 & -4 & 3 \end{pmatrix}$$

und

$$T := \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & -12 \\ 1 & 4 & -16 \\ 0 & 1 & -3 \end{pmatrix}.$$

Magma hingegen liefert mit

```
Z := Integers();
M := RMatrixSpace(Z,3,3);
A := M!Matrix([[2,0,0],[0,3,0],[0,0,4]]);
D,S,T := SmithForm(A);
print D,S,T;
```

die Elementarteilerform  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 12 \end{pmatrix}$ , aber mittels  $S = \begin{pmatrix} -1 & 1 & 0 \\ -3 & 2 & -1 \\ 6 & -4 & 3 \end{pmatrix}$  und  $T = \begin{pmatrix} 1 & -3 & -6 \\ 1 & -2 & -4 \\ 0 & 1 & 3 \end{pmatrix}$ .

- (2) Das Verfahren gibt folgende Umformungsschritte. Wir lassen hierbei wirkungslose Umformungsschritte weg und fassen ab und an mehrere Schritte zusammen.

$$\begin{aligned} & \begin{pmatrix} 2 & 2 & 3 & 5 \\ 4 & 8 & 5 & 5 \\ 4 & 4 & 1 & 1 \\ -2 & 6 & 6 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 2 & 3 & 5 \\ 0 & 4 & -1 & -5 \\ 0 & 0 & -5 & -9 \\ 0 & 8 & 9 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 3 & 5 \\ 0 & 4 & -1 & -5 \\ 0 & 0 & -5 & -9 \\ 0 & 8 & 9 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 5 \\ -1 & 4 & -2 & -5 \\ -5 & 0 & -10 & -9 \\ 9 & 8 & 18 & 9 \end{pmatrix} \\ \rightsquigarrow & \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 4 & -2 & 0 \\ -5 & 0 & -10 & 16 \\ 9 & 8 & 18 & -36 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & -2 & 0 \\ 0 & 0 & -10 & 16 \\ 0 & 8 & 18 & -36 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & -2 & 0 \\ 0 & 0 & -10 & 16 \\ 0 & 0 & 22 & -36 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 10 & 0 & 16 \\ 0 & -22 & 0 & -36 \end{pmatrix} \\ \rightsquigarrow & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & -20 & 16 \\ 0 & 0 & 44 & -36 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -20 & 16 \\ 0 & 0 & 44 & -36 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}. \end{aligned}$$

Dies gibt auch

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -4 & 9 & -9 & -4 \\ -3 & 10 & -11 & -5 \end{pmatrix}, \quad T = \begin{pmatrix} -1 & 3 & -7 & 5 \\ 0 & 0 & 1 & 0 \\ 1 & -2 & 4 & -5 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Magma liefert ebenfalls die Elementarteilerform  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$ , aber mittels

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 2 & 8 & 3 \\ -1 & -2 & -9 & -4 \\ 2 & 5 & 19 & 9 \\ -1 & -3 & -11 & -5 \end{pmatrix}.$$

**Aufgabe 4**

Wir rechnen.

```
// test data

A := RMatrixSpace(Integers(),3,4)!Matrix([[3,2,3,3],[2,4,4,4],[3,4,4,5]]);
A2 := RMatrixSpace(Integers(),5,5)!DiagonalMatrix([3,4,6,8,12]);

// function

ElementaryDivisorsViaMinors := function(A)
  m := NumberOfRows(A);
  n := NumberOfColumns(A);
  k := Rank(A);
  d := [0 : i in [0..k]];
  for l in [0..k] do
    MM := RMatrixSpace(Integers(),1,1);
    for I in Subsets({1..m},1) do
      for J in Subsets({1..n},1) do
        AA := MM![A[i,j] : j in J, i in I];
        d[l+1] := Gcd(d[l+1],Determinant(AA));
      end for;
    end for;
  end for;
  return [d[i+2]/d[i+1] : i in [0..k-1]];
end function;

// shorter, equivalent solution

ElementaryDivisorsViaMinors := function(A)
  m := NumberOfRows(A);
  n := NumberOfColumns(A);
  k := Rank(A);
  d := [Gcd([Determinant(RMatrixSpace(Integers(),1,1)!A[i,j] : j in J, i in I])
    : I in Subsets({1..m},1), J in Subsets({1..n},1))] : l in [0..k]];
  return [d[i+2]/d[i+1] : i in [0..k-1]];
end function;

// test

ElementaryDivisorsViaMinors(A);
ElementaryDivisorsViaMinors(A2);

// test for time consumption

A3 := RMatrixSpace(Integers(),13,11)!Random({-5..5}) : i in [1..11*13]];
time ElementaryDivisorsViaMinors(A3);
time SmithForm(A3);
```

Im vorliegenden Fall brauchte das Minorenverfahren auf meinem Rechner ca. 100 Sekunden.

Die von `SmithForm` benötigte Zeit lag immer noch unter der Meßbarkeitsschwelle.

Was passiert in der Funktion für  $\ell = 0$ ?

### Aufgabe 5

Wir können etwa wie folgt vorgehen.

```
// test data

DD := DiagonalMatrix([1,2,4,8,16]);
U := Matrix([[0,1,1,1,0],[0,1,0,0,1],[1,1,0,0,1],[1,0,1,0,1],[0,0,1,1,0]]);
A := U * DD * U;
A2 := U * DD * U^-1;
A3 := U^2 * DD * U^3;
A4 := U^2 * DD * U^-3;

// help functions

CleanColumn := function(A,k) // clean first column of region [k,m] x [k,n] as far as possible
m := NumberOfRows(A);
S := MatrixRing(Integers(),m)!1;
for i in [k+1..m] do
  if not ((A[k][k] eq 0) and (A[i][k] eq 0)) then
    if A[k][k] eq 0 then
      g := A[i][k];
      s := 0;
      t := 1;
    elif (A[i][k] mod A[k][k] eq 0) then
      g := A[k][k];
      s := 1;
      t := 0;
    else
      g,s,t := ExtendedGreatestCommonDivisor(A[k][k],A[i][k]);
    end if;
    apkk := Integers()!(A[k][k]/g);
    apik := Integers()!(A[i][k]/g);
    M := Matrix(SparseMatrix(m,m,[<k,k,s-1>,<k,i,t>,<i,k,-apik>,<i,i,apkk-1>]))
      + MatrixRing(Integers(),m)!1;
    S := M * S;
    A := M * A;
  end if;
end for;
return A,S;
end function;

CleanRow := function(A,k) // clean first row of region [k,m] x [k,n] as far as possible
B,T := CleanColumn(Transpose(A),k);
return Transpose(B), Transpose(T);
end function;

// function

Smith := function(A)
m := NumberOfRows(A);
```

```

n := NumberOfColumns(A);
min := Minimum(m,n);
S := MatrixRing(Integers(),m)!1;
T := MatrixRing(Integers(),n)!1;
for k in [1..min] do
  divides := false;
  for j in [k+1..n+1] do
    clean := false;
    if not divides then
      while not clean do
        A,M := CleanColumn(A,k);
        S := M * S;
        A,M := CleanRow(A,k);
        T := T * M;
        clean := ((k eq m) or IsZero(SubmatrixRange(A,k+1,k,m,k))) and
          ((k eq n) or IsZero(SubmatrixRange(A,k,k+1,k,n)));
      end while;
    end if;
    if j le n then
      divides := true;
      for l in [k+1..m] do
        if A[k][k] eq 0 then
          if A[l][j] ne 0 then
            divides := false;
            break l;
          end if;
        else
          if not A[l][j] mod A[k][k] eq 0 then
            divides := false;
            break l;
          end if;
        end if;
      end for;
      if not divides then
        M := Matrix(SparseMatrix(n,n,[<j,k,1>])) + MatrixRing(Integers(),n)!1;
        A := A * M;
        T := T * M;
      end if;
    end if;
  end for;
end for;
return A,S,T;
end function;

// test

time D,S,T := Smith(A);
print S*A*T;
print Determinant(S), Determinant(T);

time D,S,T := Smith(A2);
print S*A2*T;
print Determinant(S), Determinant(T);

```

```

time D,S,T := Smith(A3);
print S*A3*T;
print Determinant(S), Determinant(T);

time D,S,T := Smith(A4);
print S*A4*T;
print Determinant(S), Determinant(T);

for i in [1..10] do
  m := 4; n := 6; b := 5; A5 := RMatrixSpace(Integers(),m,n)! [Random([-b..b]) : i in [1..m*n]];
  time D,S,T := Smith(A5);
  print D;
  if not IsZero(D - S*A5*T) or not Determinant(S) eq 1 or not Determinant(T) eq 1 then
    print "Alarm!";
    break i;
  end if;
end for;

for i in [1..1000] do
  m := 24; n := 22; b := 5; A5 := (RMatrixSpace(Integers(),m,n)! [Random([-b..b]) : i in [1..m*n]])
    * DiagonalMatrix([Random([-b..b]) : i in [1..n]]);

  print "eigenes:";
  time D,S,T := Smith(A5);
  //print D;
  if not IsZero(D - S*A5*T) then
  //if not IsZero(D - S*A5*T) or not Determinant(S) eq 1 or not Determinant(T) eq 1 then
    print "Alarm!";
    break i;
  end if;
  print "Magma:";
  time D,S,T := SmithForm(A5);
end for;

```

Der letztgenannte Test lieferte Beispiele, die mit dem eigenen Programm `Smith` zwischen 0,03 und 3282 Sekunden benötigen.

Magmas Programm `SmithForm` benötigte für dieselben Matrizen zwischen 0,00 und 0,25 Sekunden.

Die Maxima in diesem Versuch wurden an verschiedenen Beispielen angenommen.

## Aufgabe 6

- (1) Sei  $y \in R \setminus \{0\}$  prim. Wir wollen zeigen, daß  $y$  irreduzibel ist. *Annahme*, nicht. Zunächst ist  $y$  eine Nichteinheit, da  $R/\langle y \rangle$  als Integritätsbereich ungleich  $\{0\}$  ist. Sei  $y = uv$  mit Nichteinheiten  $u, v \in R$ . Da  $y \neq 0$ , sind auch  $u, v \neq 0$ . Dann ist  $uv \equiv_y 0$ , und also o.E.  $u \equiv_y 0$ , da  $R/\langle y \rangle$  ein Integritätsbereich ist. Somit ist  $u = yw$  für ein  $w \in R$ . Aus  $u = yw = uv$  folgt  $1 = vw$ , im *Widerspruch* zu  $v$  Nichteinheit.

Sei umgekehrt  $y \in R \setminus \{0\}$  irreduzibel. Nach Aufgabe 1.(4) ist  $R/\langle y \rangle$  ein Körper, insbesondere also ein Integritätsbereich.

- (2) Wir bemerken zunächst, daß jede nichtleere Menge  $M$  von Idealen von  $R$  ein maximales Element enthält (i.e. daß  $R$  noethersch ist). *Annahme*, nicht. Dann gibt es  $I_i \in M$  für  $i \in \mathbf{Z}_{\geq 1}$  mit  $I_i \subset I_{i+1}$

stets; angefangen mit  $I_1 \in M$  beliebig, und unter Verwendung dessen, daß  $\{I_i : i \in [1, j]\}$  kein maximales Element von  $M$  enthält für  $j \geq 1$ . Sei  $I := \bigcup_{i \geq 1} I_i$ . Schreibe  $I = \langle y \rangle$  für ein  $y \in R$ . Es gibt ein  $j \geq 1$  mit  $y \in I_j$ . Also ist  $I = \langle y \rangle \subseteq I_j \subset I_{j+1} \subseteq I$ , was ein *Widerspruch* ist.

Zurück zur Aufgabe. Nach (1) genügt es, eine Zerlegung  $x = ex_1x_2 \cdots x_n$  zu finden mit  $x_i \in R$  irreduzibel für  $i \in [1, n]$  und mit einer Einheit  $e$ ; kurz, eine *Zerlegung in irreduzible Elemente*.

Sei  $M$  die Menge der Ideale  $\neq \{0\}$  von  $R$ , für welche der Erzeuger keine Zerlegung in irreduzible Elemente zuläßt. Wir müssen zeigen, daß  $M = \emptyset$ . *Annahme*, nicht. Dann hat  $M$  ein maximales Element  $\langle y \rangle$ , wobei  $y \in R$ . Insbesondere kann  $y$  weder irreduzibel noch eine Einheit sein. Also gibt es Nichteinheiten  $u, v \in R$  mit  $y = uv$ . Nun ist  $\langle y \rangle \subset \langle u \rangle$ , da  $v$  keine Einheit ist, und also hat  $u$  eine Zerlegung in irreduzible Elemente. Genauso hat  $v$  eine Zerlegung in irreduzible Elemente. Folglich hat auch  $y = uv$  eine Zerlegung in irreduzible Elemente. Dies *widerspricht* aber der Wahl von  $y$ .

(3) O.E. ist  $n \leq \tilde{n}$ .

Wir führen eine Induktion über  $n$ .

*Induktionsanfang.* Ist  $n = 0$ , so ist  $x$  eine Einheit. Wäre  $\tilde{n} \geq 1$ , so wäre  $\tilde{x}_i$  eine Einheit und prim, was *nicht geht*, da der Nullring kein Integritätsbereich ist. Also ist  $\tilde{n} = 0$ . Die fragte Bijektion ist  $\sigma : \emptyset \xrightarrow{\sim} \emptyset$ .

*Induktionsschritt.* Sei  $n \geq 1$ . Es ist

$$x = ex_1x_2 \cdots x_n = \tilde{e}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_{\tilde{n}}$$

wie angegeben. Nach (1) ist  $x_1$  prim. Da  $0 \equiv_{x_1} \tilde{e}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_{\tilde{n}}$  und da  $\tilde{e}$  auch modulo  $x_1$  noch eine Einheit ist, gibt es ein  $j \in [1, \tilde{n}]$  mit  $\tilde{x}_j \equiv_{x_1} 0$ . O.E. ist  $j = 1$ . Also ist  $\tilde{x}_1 = x_1f_1$  für ein  $f_1 \in R$ . Da  $\tilde{x}_1$  nach (1) irreduzibel und  $x_1$  eine Nichteinheit ist, folgt, daß  $f_1$  eine Einheit ist. Kürzen von  $x_1$  gibt

$$x = ex_2 \cdots x_n = (\tilde{e}f_1)\tilde{x}_2 \cdots \tilde{x}_{\tilde{n}}.$$

Nach Induktionsvoraussetzung ist  $n = \tilde{n}$ , und es gibt eine Bijektion  $\rho : [2, n] \xrightarrow{\sim} [2, \tilde{n}]$  so, daß für alle  $i \in [2, n]$  eine Einheit  $f_i \in R$  mit  $x_i = \tilde{x}_{\rho(i)}f_i$  existiert. Setzen wir  $\sigma(1) := 1$  und  $\sigma(i) := \rho(i)$  für  $i \in [2, n]$ , so ergibt sich die gewünschte Aussage.

## Aufgabe 7

(1) Wir rechnen.

```
P<X> := PolynomialRing(GF(2));
for k in [13..13] do
  F<a> := GF(2^k);
  for t in F do
    mu := MinimalPolynomial(t);
    if Degree(mu) eq k then
      print t, "generates the field extension GF(2^",k,")|GF(2)";
      if #{t^i : i in [0..2^k-2]} eq 2^k - 1 then
        print t, "generates the group GF(2^",k,")-{0}";
      else
        print t, "does not generate the group GF(2^",k,")-{0}";
        break t;
      end if;
    end if;
  end for;
end for;
```

Es gibt also für alle  $k \in [2, 8]$  je ein Element in  $\mathbf{F}_{2^k} \setminus \{0\}$ , welches sowohl die Körpererweiterung als auch die multiplikative Gruppe erzeugt.

Ferner gibt es für  $k \in \{4, 6, 8, 9, 10, 11, 12\}$  je ein Element in  $\mathbf{F}_{2^k} \setminus \{0\}$ , welches zwar die Körpererweiterung, nicht aber die multiplikative Gruppe erzeugt. Für  $k \in \{2, 3, 5, 7, 13\}$  gibt es das nicht.

(2) Wir rechnen.

```
p := 3;
P<X> := PolynomialRing(GF(p));
prod := P!1;
for i in [1..12] do
  if 12 mod i eq 0 then
    l := [];
    for j in [0..i-1] do
      Append(~l, GF(p));
    end for;
    M := CartesianProduct(l);
    for tup in M do
      g := P!([tup[j] : j in [1..i]] cat [1]);
      if IsIrreducible(g) then
        prod *:= g;
      end if;
    end for;
  end if;
end for;
print "product =", prod;
```

Wir erhalten nach einiger Rechenzeit als Produkt  $X^{531441} - X = X^{3^{12}} - X$ . Cf. Lemma 10.

(3) Wir rechnen.

```
p := 5;
m := 4;
F<a> := GF(p^m);
P<X> := PolynomialRing(GF(p));
print "minimal polynomial = ", MinimalPolynomial(a); // out of interest
PP<X> := PolynomialRing(GF(p^m));
print "product =", &*[ X - xi : xi in F];
```

Wir erhalten als Produkt  $X^{625} - X = X^{5^4} - X$ . Cf. Beweis zu Lemma 10.

## Aufgabe 8

(1) Wir rechnen.

```
// test data

p := 2;
F := GF(p);
P<X> := PolynomialRing(F);
if p eq 3 then f := (X^3-X-1)^9*(X^2 + 1)^16*(X+1)^12*X^7*(X^2+X-1)^15*
(X^2 - X - 1)^13*(X^5-X^3+X^2+X-1)^6; end if; // example for p = 3
if p eq 2 then f := (X^3+X+1)^9*(X^2+X+1)^16*(X+1)^12*X^7*(X^4+X+1)^15*
```

```
(X^4+X^3+1)^13*(X^4+X^3+X^2+X+1)^6; end if; // example for p = 2
if p eq 5 then f := P!([Random(F) : i in [0..10]] cat [1]);
end if; // random example for p = 5
```

```
// function
```

```
DecomposeNaively := function(f,p)
  F := GF(p);
  P<X> := PolynomialRing(F);
  irreduciblefactors := [];
  while Degree(f) gt 1 do
    for i in [1..Degree(f)] do
      l := [];
      for j in [0..i-1] do
        Append(~l,GF(p));
      end for;
      M := CartesianProduct(l);
      for tup in M do
        g := P!([tup[j] : j in [1..i]] cat [1]);
        if f mod g eq 0 then
          break i;
        end if;
      end for;
    end for;
    Append(~irreduciblefactors,g);
    f div:= g;
  end while;
  return irreduciblefactors;
end function;
```

```
// test
```

```
time irreduciblefactors := DecomposeNaively(f,p);
[Factorisation(g) : g in irreduciblefactors];
prod := 1; for g in irreduciblefactors do prod *= g; end for;
print f - prod;
```

(2) Wir rechnen.

```
// test data
```

```
p := 2;
F := GF(p);
P<X> := PolynomialRing(F);
if p eq 3 then f := ((X^3-X-1)^9*(X^2 + 1)^16*(X+1)^12*X^7*(X^2+X-1)^15*
(X^2 - X - 1)^13*(X^5-X^3+X^2+X-1)^6)^m; end if; // example for p = 3
if p eq 2 then f := ((X^3+X+1)^9*(X^2+X+1)^16*(X+1)^12*X^7*(X^4+X+1)^15*
(X^4+X^3+1)^13*(X^4+X^3+X^2+X+1)^6)^m; end if; // example for p = 2
if p eq 5 then f := P!([Random(F) : i in [0..100]] cat [1]);
end if; // random example for p = 5
```

```
// function: Frobenius reduction
```

```

FrobeniusReduction := function(g,p) // g : nonzero element of P
  F := GF(p);
  P<X> := PolynomialRing(F);
  coeffs := Coefficients(g);
  minval := Valuation(Degree(g),p);
  for i in [0..Degree(g)] do
    if coeffs[i+1] ne 0 then
      minval := Minimum(minval,Valuation(i,p));
    end if;
  end for;
  return &+[coeffs[i*p^minval + 1] * X^i : i in [0..Degree(g)/p^minval]];
end function;

// function: factorisation into squarefree polynomials

SquarefreeFactors := function(f,p)
  F := GF(p);
  P<X> := PolynomialRing(F);
  squarefreefactors := [];
  while Degree(f) gt 0 do
    h := f;
    while Degree(h) gt 0 do
      hred := FrobeniusReduction(h,p);
      h := Gcd(hred,Derivative(hred));
      if Degree(h) eq 0 then
        Append(~squarefreefactors,hred);
        f := P!(f/hred);
      end if;
    end while;
  end while;
  return squarefreefactors;
end function;

// test of SquarefreeFactors

squarefreefactors := SquarefreeFactors(f,p);
[Factorisation(g) : g in squarefreefactors];
print f - &*[g : g in squarefreefactors];

// function: equal degree factorisation

EqualDegreeFactors := function(f,p)
  F := GF(p);
  P<X> := PolynomialRing(F);
  equaldegreefactors := [];
  for u in SquarefreeFactors(f,p) do
    i := 0;
    g := u;
    while Degree(g) gt 0 do
      i += 1;
      PF := quo<P | g>; // for faster performance: calculate in PF instead of P
      h := Gcd(g,P!((PF!X)^(p^i)-(PF!X)));
      if Degree(h) ne 0 then Append(~equaldegreefactors,<h,i>); end if;
    end while;
  end for;
end function;

```

```

    g := P!(g/Gcd(g,P!((PF!X)^(p^i)-(PF!X))));
  end while;
end for;
return equaldegreefactors;
end function;

// test of EqualDegreeFactors

equaldegreefactors := EqualDegreeFactors(f,p);
[Factorisation(g[1]) : g in equaldegreefactors];
prod := 1; for g in equaldegreefactors do prod := g[1]; end for;
print f - prod;

// function: factorisation into irreducibles

Decompose := function(f,p)
  F := GF(p);
  P<X> := PolynomialRing(F);
  irreduciblefactors := [];
  if p ne 2 then
    for v in EqualDegreeFactors(f,p) do
      g := [v[1]];
      alreadydone := [];
      while Maximum([Degree(u) : u in g]) gt v[2] do
        gnew := [];
        hdeg := Random([1..v[2]]);
        h := P!([Random(F) : i in [0..hdeg-1]] cat [1]);
        if not h in alreadydone then
          for u in g do
            PF := quo<P | u>; // for faster performance: calculate in PF instead of P
            hf := PF!h;
            f1 := Gcd(u,P!hf);
            f2 := Gcd(u,P!(hf^(Integers()!((p^v[2]-1)/2)) - 1));
            f3 := Gcd(u,P!(hf^(Integers()!((p^v[2]-1)/2)) + 1));
            if f1 ne 1 then
              Append(~gnew,f1);
            end if;
            if f2 ne 1 then
              Append(~gnew,f2);
            end if;
            if f3 ne 1 then
              Append(~gnew,f3);
            end if;
          end for;
          if #gnew eq #g then
            Append(~alreadydone,h);
          else
            g := gnew;
            alreadydone := [];
          end if;
        end if;
      end while;
      irreduciblefactors cat:= g;
    end for;
  end if;
end function;

```

```

end for;
else
for v in EqualDegreeFactors(f,p) do
g := [v[1]];
alreadydone := [];
while Maximum([Degree(u) : u in g]) gt v[2] do
gnew := [];
hdeg := Random([1..v[2]]);
h := P!([Random(F) : i in [0..hdeg-1]] cat [1]);
if not h in alreadydone then
for u in g do
PF := quo<P | u>; // for faster performance: calculate in PF instead of P
hf := PF!h;
hff := &+[hf^(2^i-1) : i in [0..v[2]-1]];
f1 := Gcd(u,P!hf);
f2 := Gcd(u,P!hff);
f3 := Gcd(u,P!(hf*hff + 1));
if f1 ne 1 then
Append(~gnew,f1);
end if;
if f2 ne 1 then
Append(~gnew,f2);
end if;
if f3 ne 1 then
Append(~gnew,f3);
end if;
end for;
if #gnew eq #g then
Append(~alreadydone,h);
else
g := gnew;
alreadydone := [];
end if;
end if;
end while;
irreduciblefactors cat:= g;
end for;
end if;
return irreduciblefactors;
end function;

// test

time irreduciblefactors := Decompose(f,p);
[Factorisation(g) : g in irreduciblefactors];
prod := 1; for g in irreduciblefactors do prod := g; end for;
f - prod;

```

Weitere Verbesserungen können dadurch erzielt werden, die weitere Zerlegung eines wiederholt auftretenden und daher bereits zerlegten Faktors nicht wiederholt durchzuführen.

- (3) Wir vergleichen (1) und (2) e.g. folgendermaßen noch mit `Factorisation`.

```
p := 5;
```

```

F := GF(p);
P<X> := PolynomialRing(F);
f := P!([Random(F) : i in [0..100]] cat [1]); // random example for p = 5
time Factorisation(f,p);

```

Folgende grobe Messungen fanden auf meinem Rechner statt.

Betrachten wir ein zufällig gewähltes normiertes Polynom von Grad 11 in  $\mathbf{F}_5[X]$ . Der Algorithmus aus (1) braucht bis zu 450s, der Algorithmus aus (2) bis zu 0,03s, und `Factorisation` bis zu 0,01s.

Betrachten wir ein zufällig gewähltes normiertes Polynom von Grad 101 in  $\mathbf{F}_5[X]$ . Der Algorithmus aus (1) braucht sehr lange, der Algorithmus aus (2) bis zu 2s, und `Factorisation` bis zu 0,02s.

Betrachten wir ein zufällig gewähltes normiertes Polynom von Grad 1001 in  $\mathbf{F}_5[X]$ . Der Algorithmus aus (2) braucht bis zu 850s, und `Factorisation` bis zu 0,68s.

### Aufgabe 9

```

// function

Decompose := function(f);
Z := Integers();
Q := Rationals();
P<X> := PolynomialRing(Z);
PP<X> := PolynomialRing(Q);
z := Gcd(Coefficients(P!f));
f := P!(PP!f/z);
factors := [];
while Degree(f) ge 1 do
n := Degree(f);
k := -(n div 2);
support := [];
while #support lt n+1 do
if Evaluate(f,k) ne 0 then
Append(~support,k);
end if;
k += 1;
end while;
// the following set T is big
T := CartesianProduct([Divisors(Z!Abs(Evaluate(f,i)))
cat [-j : j in Divisors(Z!Abs(Evaluate(f,i)))] : i in support]);
prod := &*[ X-i : i in support];
for t in T do
pol := [P!(prod div (X - support[i])) : i in [1..n+1]];
g := &+[PP!(t[i]*pol[i])/Evaluate(pol[i],support[i]) : i in [1..n+1]];
g_is_integral := true;
for x in Coefficients(g) do
if not x in Z then
g_is_integral := false;
break x;
end if;
end for;
if g_is_integral and Degree(g) ge 1 then
if f mod (P!g) eq 0 then

```

```

f_help := f div (P!g);
if &and[ x in Z : x in Coefficients(g)] then
  f := P!f_help;
  Append(~factors,P!g);
  break t;
end if;
end if;
end if;
end for;
end while;
Append(~factors,P!f);
if factors[#factors] eq 1 then
  Prune(~factors);
end if;
integer_factors := [];
for x in Factorisation(z) do
  for i in [1..x[2]] do
    Append(~integer_factors,x[1]);
  end for;
end for;
factors cat:= integer_factors;
return factors;
end function;

```

```
// test
```

```

Z := Integers();
P<X> := PolynomialRing(Z);

```

```

Decompose(210*X);
Decompose(130*(X^2 - 1));
Decompose(2*X^2 + 1);
Decompose(-45*(X^4 + X^3 - 1));
Decompose((2*X^2 + 1)*(3*X - 2));
Decompose(24*((2*X^2 + 1)*(2*X^3+X+1)));
Decompose((2*X^2 + 1)*(X^4+X^3+X^2+X+1));
Decompose(-345*(X^7 + X^3 - 1));
Decompose((2*X^2 + 1)^2*(X^4+X^3+X^2+X+1));

```

### Aufgabe 10

Sei  $Ae$  unzerlegbar. Es ist  $Ae \neq 0$ , also  $e \neq 0$ .

Sei  $e = e' + e''$  mit  $e'^2 = e'$ ,  $e''^2 = e''$ ,  $e'e'' = 0$  und  $e''e' = 0$ .

Es genügt zu zeigen, daß  $Ae \stackrel{!}{=} Ae' \oplus Ae''$ , da dann wegen  $Ae$  unzerlegbar folgt, daß  $Ae' = 0$  oder  $Ae'' = 0$ , also auch  $e' = 0$  oder  $e'' = 0$ , womit  $e$  als primitiv nachgewiesen ist.

Es ist  $Ae' \subseteq Ae$ , da  $ae' = ae'(e' + e'') = ae'e$  für  $a \in A$ . Analog ist  $Ae'' \subseteq Ae$ .

Es ist  $Ae = Ae' + Ae''$ , da  $ae = ae' + ae''$  für  $a \in A$ .

Bleibt die Direktheit zu zeigen. Seien  $a' \in Ae'$  und  $a'' \in Ae''$  mit  $a' + a'' = 0$  gegeben. Dann ist  $0 = (a' + a'')e' = (a'e' + a''e'')e' = a'e' = a'$  und also auch  $a'' = -a' = 0$ .

Sei  $e$  primitiv. Es ist  $e \neq 0$ , also  $Ae \neq 0$ . Sei  $Ae = X \oplus Y$  für Teilmoduln  $X, Y \subseteq Ae$ . Sei  $\pi : Ae = X \oplus Y \longrightarrow Ae, x + y \longmapsto x$ , wobei  $x \in X$  und  $y \in Y$ . Es ist  $\pi$  eine  $A$ -lineare Abbildung. Es ist  $\pi^2 = \pi$ .

Setze  $e' := \pi(e)$  und  $e'' := e - \pi(e)$ .

Es ist  $ee' = e\pi(e) = \pi(ee) = \pi(e) = e'$ . Es ist  $e'e = \pi(e)e = \pi(e)$ , da  $\pi(e) \in Ae$ .

Es ist  $e'^2 = e'\pi(e) = \pi(e'e) = \pi(e') = \pi(\pi(e)) = \pi(e) = e'$ .

Es ist  $e''^2 = (e - e')^2 = e^2 - ee' - e'e + e'^2 = e - e' - e' + e' = e''$ .

Es ist  $e'e'' = e'(e - e') = e' - e' = 0$ . Es ist  $e''e' = (e - e')e' = e' - e' = 0$ .

Da  $e$  primitiv ist, folgt  $e' = 0$  oder  $e'' = 0$ .

Ist  $e' = 0$ , dann ist  $\pi(ae) = a\pi(e) = ae' = 0$  für  $a \in A$ . Somit ist  $X = \pi(Ae) = 0$ ,

Ist  $e'' = 0$ , dann ist  $e = e'$  und also  $\pi(ae) = a\pi(e) = ae' = ae$  für  $a \in A$ . Also ist  $\pi = \text{id}_{Ae}$ , und somit  $Y = \text{Kern } \pi = 0$ .

Also ist  $Ae$  unzerlegbar.

### Aufgabe 11

Beachte, daß für  $\varphi \in \text{Hom}_A(Ae, Af)$  in der Tat  $\varphi(e) \in Af$  mit  $e\varphi(e) = \varphi(e)$  ist, insgesamt also  $\varphi(e) \in eAf$ .

Die somit wohldefinierte Abbildung  $\text{Hom}_A(Ae, Af) \longrightarrow eAf, \varphi \longmapsto \varphi(e)$ , ist zudem ein Morphismus abelscher Gruppen.

Beachte, daß für  $a \in A$  die Abbildung  $Ae \longrightarrow Af, be \longmapsto (be)(eaf) = beaf$  für  $b \in A$ , in der Tat  $A$ -linear ist.

Die somit wohldefinierte Abbildung  $eAf \longrightarrow \text{Hom}_A(Ae, Af), eaf \longmapsto (be \longmapsto (be)(eaf) = beaf)$ , ist zudem ein Morphismus abelscher Gruppen.

Wir wollen zeigen, daß die beiden Abbildungen sich gegenseitig invertieren.

Für  $\varphi \in \text{Hom}_A(Ae, Af)$  ist

$$\varphi \longmapsto \varphi(e) \longmapsto (be \longmapsto be\varphi(e) = \varphi(bee) = \varphi(be)) = \varphi.$$

Für  $a \in A$  ist

$$eaf \longmapsto (be \longmapsto beaf) \longmapsto (be \longmapsto beaf)(e) = eaf.$$

### Aufgabe 12

Annahme, es gibt keine orthogonale Zerlegung in primitive Idempotente in  $A$ .

*Behauptung.* Für alle  $n \in \mathbf{Z}_{\geq 1}$  gibt es eine orthogonale Zerlegung in Idempotente  $\underline{e} = (e_1, \dots, e_n)$  in  $A$  mit  $e_i \neq 0$  für  $i \in [1, n]$ .

Induktion über  $n \geq 1$ .

*Induktionsanfang.* Es ist (1) eine orthogonale Zerlegung in Idempotente in  $A$ .

*Induktionsschritt.* Sei  $\underline{e} = (e_1, \dots, e_n)$  eine orthogonale Zerlegung in Idempotente in  $A$  mit  $e_i \neq 0$  für  $i \in [1, n]$ .

Es gibt ein  $k \in [1, n]$  mit  $e_k$  nicht primitiv. Also gibt es Idempotente  $e' \neq 0$  und  $e'' \neq 0$  in  $A$  mit  $e_k = e' + e''$  und  $e'e'' = e''e' = 0$ .

Da  $e_i \neq 0$  für  $i \in [1, n] \setminus \{k\}$  und da  $e' \neq 0$  und  $e'' \neq 0$ , genügt es zu zeigen, daß

$$(e_1, \dots, e_{k-1}, e', e'', e_{k+1}, \dots, e_n)$$

eine orthogonale Zerlegung in Idempotente ist.

Dieses Tupel besteht aus Idempotenten.

Seine Summe ist 1.

Es ist  $e'e'' = e''e' = 0$ .

Es ist  $e_ie_j = 0$  für  $i, j \in [1, n] \setminus \{k\}$ .

Es ist  $e'e_i = e'(e' + e'')e_i = e'e_k e_i = 0$  für  $i \in [1, n] \setminus \{k\}$ .

Genauso ist auch  $e_i e' = 0$ ,  $e''e_i = 0$  und  $e_i e'' = 0$  für  $i \in [1, n] \setminus \{k\}$ .

Dies zeigt die *Behauptung*.

Setze  $n := 1 + \dim_K A$  und wähle eine orthogonale Zerlegung  $(e_1, \dots, e_n)$  in Idempotente in  $A$ . Nach Bemerkung 15 ist  $A = \bigoplus_{i \in [1, n]} Ae_i$ . Es ist  $0 \neq e_i \in Ae_i$  und somit  $\dim_K Ae_i \geq 1$  für  $i \in [1, n]$ . Zusammen ist also

$$\dim_K A = \sum_{i \in [1, n]} \dim_K Ae_i \geq n,$$

und wir haben einen Widerspruch.

Ist  $K$  nicht endlich, so stellt das Auffinden einer orthogonalen Zerlegung in primitive Idempotente ein ernsthaftes algorithmisches Problem dar. Das Problem hierbei ist, ein Idempotent  $e$  auf Primitivität zu testen und ggf. zu zerlegen. Durch Übergang zu  $eAe$  ist hierbei o.E.  $e = 1$ . Somit lautet die Aufgabe, in einer endlichdimensionalen  $K$ -Algebra  $A$  ein Idempotent  $\notin \{0, 1\}$  zu finden oder als nichtexistent nachzuweisen.

Desweiteren, nein, im allgemeinen gibt es in  $A$  mehrere orthogonale Zerlegungen in primitive Idempotente.

Sei etwa  $A = \mathbf{C}^{2 \times 2}$ .

Es ist  $(e_1, e_2) := \left( \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$  eine orthogonale Zerlegung in primitive Idempotente in  $A$ . Denn es ist  $\dim_{\mathbf{C}} e_1 A e_1 = 1$  und  $\dim_{\mathbf{C}} e_2 A e_2 = 1$ . Wäre  $e_1 = e' + e''$  mit Idempotenten  $e' \neq 0$  und  $e'' \neq 0$  so, daß  $e'e'' = e''e' = 0$ , dann wäre

$$e_1 A e_1 = e' A e' \oplus e' A e'' \oplus e'' A e' \oplus e'' A e'',$$

worin der erste und der letzte Summand nicht verschwände, was aus Dimensionsgründen nicht ginge. Also ist  $e_1$  primitiv. Genauso ist auch  $e_2$  primitiv.

Der Ringautomorphismus  $A \xrightarrow{\sim} A$ ,  $x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} x \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$  gibt, daß auch

$$f_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} e_1 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$$

und

$$f_2 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} e_2 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

eine von orthogonale Zerlegung in primitive Idempotente  $(f_1, f_2)$  bilden. Diese ist von  $(e_1, e_2)$  verschieden.

### Aufgabe 13

(1) Es ist  $A = \mathbf{C}[X]/\langle X^2 \rangle$  nicht halbeinfach. Denn im  $A$ -Modul  $A$  gibt es für den Teilmodul

$$N := {}_A \langle X + \langle X^2 \rangle \rangle \subseteq A$$

keinen weiteren Teilmodul  $X \subseteq A$  mit  $N \oplus X = A$ , wie wir nun zeigen wollen.

*Annahme*, es gibt einen Teilmodul  $X \subseteq A$  mit  $A = N \oplus X$ . Sei  $\pi : A \rightarrow A$  die Projektion auf  $N$ . Es ist  $\pi$  eine  $A$ -lineare Abbildung, welche  $1 + \langle X^2 \rangle$  auf  $Xf(X) + \langle X^2 \rangle$  schickt für ein  $f(X) \in \mathbf{C}[X]$ . Es ist  $Xf(X) + \langle X^2 \rangle = \lambda X + \langle X^2 \rangle$ , wobei  $\lambda := f(0) \in \mathbf{C}$ . Es ist  $\pi|_N = \text{id}_N$ . Also ist

$$\begin{aligned} 0 &\neq X + \langle X^2 \rangle \\ &= \pi(X + \langle X^2 \rangle) \\ &= \pi((X + \langle X^2 \rangle) \cdot (1 + \langle X^2 \rangle)) \\ &= (X + \langle X^2 \rangle) \cdot \pi(1 + \langle X^2 \rangle) \\ &= (X + \langle X^2 \rangle)(\lambda X + \langle X^2 \rangle) \\ &= \lambda X^2 + \langle X^2 \rangle \\ &= 0, \end{aligned}$$

und wir haben einen *Widerspruch*.

(2) Nach dem Chinesischen Restsatz ist

$$A = \mathbf{C}[X]/\langle X^2 + 1 \rangle \simeq \mathbf{C}[X]/\langle X + i \rangle \times \mathbf{C}[X]/\langle X - i \rangle \simeq \mathbf{C} \times \mathbf{C},$$

und also ist  $A$  dank der untenstehenden Aufgabe 14 halbeinfach.

Ein direkterer Weg geht wie folgt. Wir haben eine orthogonale Zerlegung in Idempotente

$$(e_1, e_2) := ((iX + 1)/2 + \langle X^2 + 1 \rangle, (-iX + 1)/2 + \langle X^2 + 1 \rangle),$$

die man e.g. mit obigem Chinesischen-Restsatz-Isomorphismus als Urbilder von  $(1, 0)$  und  $(0, 1)$  aus  $\mathbf{C} \times \mathbf{C}$  erhält, da dieser  $f(X) + \langle X^2 + 1 \rangle \in A$  nach  $(f(-i), f(i)) \in \mathbf{C} \times \mathbf{C}$  abbildet, so daß man Lagrange-Interpolation verwenden kann.

Nun sind  $e_1, e_2 \neq 0$ , und somit  $\dim_{\mathbf{C}} Ae_1 \geq 1$  und  $\dim_{\mathbf{C}} Ae_2 \geq 1$ . Da  $\dim_{\mathbf{C}} A = 2$ , bleibt nur die Möglichkeit  $\dim_{\mathbf{C}} Ae_1 = 1$  und  $\dim_{\mathbf{C}} Ae_2 = 1$ . Also sind  $Ae_1$  und  $Ae_2$  einfache  $A$ -Moduln. Es folgt, daß  $A$  halbeinfach ist; cf. Bemerkung 15, Lemma 23.

(3) Es ist  $A = \begin{pmatrix} \mathbf{C} & \mathbf{C} \\ 0 & \mathbf{C} \end{pmatrix}$  nicht halbeinfach. Denn der  $A$ -Modul  $M := \begin{pmatrix} \mathbf{C} \\ \mathbf{C} \end{pmatrix}$  hat den Teilmodul  $N := \begin{pmatrix} \mathbf{C} \\ 0 \end{pmatrix}$ , und wir wollen zeigen, daß es keinen Teilmodul  $X \subseteq \begin{pmatrix} \mathbf{C} \\ \mathbf{C} \end{pmatrix}$  mit  $N \oplus X = M$  geben kann. *Annahme*, es gibt ein ebensolches  $X$ . Dann ist  $\dim_{\mathbf{C}} X = \dim_{\mathbf{C}} M - \dim_{\mathbf{C}} N = 2 - 1 = 1$ . Also ist  $X = \mathbf{C} \langle \begin{pmatrix} x \\ y \end{pmatrix} \rangle$  für gewisse  $x, y \in \mathbf{C}$ , nicht beide null. Die Bedingung  $N \cap X = 0$  liefert, daß  $y \neq 0$  ist. Nun ist  $X \subseteq M$  ein Teilmodul, also folgt aus  $\begin{pmatrix} x \\ y \end{pmatrix} \in X$ , daß  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix} \in X$ . Insgesamt ist  $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} y \\ 0 \end{pmatrix} \in N \cap X$ , und wir haben einen *Widerspruch*.

## Aufgabe 14

(1) Für  $j, k \in [1, n]$  schreiben wir  $e_{j,k} \in K^{n \times n}$  für die Matrix, die an Position  $(j, k)$  den Eintrag 1 hat, und ansonsten Nullen.

Es ist  $(e_{1,1}, \dots, e_{n,n})$  eine orthogonale Zerlegung in Idempotente. Mithin ist

$$K^{n \times n} = \bigoplus_{i \in [1, n]} K^{n \times n} e_{i,i}.$$

Sei  $i \in [1, n]$ . Wir *behaupten*, daß  $K^{n \times n} e_{i,i}$  ein einfacher  $K^{n \times n}$ -Modul ist.

Sei  $0 \neq X \subseteq K^{n \times n} e_{i,i}$  ein Teilmodul. Wir haben  $X \stackrel{!}{=} K^{n \times n} e_{i,i}$  nachzuweisen. Sei

$$x = \sum_{j \in [1, n]} x_j e_{j,i} \in X \setminus \{0\},$$

wobei  $x_j \in K$  für  $j \in [1, n]$ . Sei  $\ell \in [1, n]$  mit  $x_\ell \neq 0$ .

Für  $k \in [1, n]$  wird

$$X \ni x_\ell^{-1} e_{k,\ell} \sum_{j \in [1, n]} x_j e_{j,i} = e_{k,i}.$$

Also liegt von der  $K$ -linearen Basis  $(e_{1,i}, \dots, e_{n,i})$  von  $K^{n \times n} e_{i,i}$  jeder Eintrag im Teilraum  $X$ . Dies zeigt  $X = K^{n \times n} e_{i,i}$  und damit die *Behauptung*.

Nach Lemma 23 ist also  $K^{n \times n}$  halbeinfach.

- (2) Ist  $S \subseteq A$  ein einfacher  $A$ -Teilmodul, so ist  $S \times 0 \subseteq A \times B$  ein einfacher  $A \times B$ -Teilmodul von  $A \times B$ , da in der ersten Komponente nur  $A$  operiert.

Analog in zweiter Komponente.

Schreibe  $A = \bigoplus_{i \in [1, m]} S_i$ , wobei  $S_i \subseteq A$  ein einfacher  $A$ -Teilmodul ist für  $i \in [1, m]$ ; cf. Lemma 23.

Schreibe  $B = \bigoplus_{j \in [1, n]} T_j$ , wobei  $T_j \subseteq B$  ein einfacher  $B$ -Teilmodul ist für  $j \in [1, n]$ ; cf. Lemma 23.

Es ist

$$A \times B = \left( \bigoplus_{i \in [1, m]} S_i \times 0 \right) \oplus \left( \bigoplus_{j \in [1, n]} 0 \times T_j \right).$$

Nach Lemma 23 ist also  $A \times B$  halbeinfach.

- (3) Sei  $M$  ein endlichdimensionaler  $B$ -Modul. Sei  $N \subseteq M$  ein  $B$ -Teilmodul. Wir haben einen  $B$ -Teilmodul  $X \subseteq M$  so zu finden, daß  $M = N \oplus X$ .

Es ist  $M$  ein  $A$ -Modul via  $a \cdot m := f(a)m$  für  $a \in A$  und  $m \in M$ . Es ist  $N \subseteq M$  auch ein  $A$ -Teilmodul. Da  $A$  halbeinfach ist, gibt es einen  $A$ -Teilmodul  $X \subseteq M$  mit  $M = N \oplus X$ . Da  $f : A \rightarrow B$  surjektiv ist, ist  $X$  auch ein  $B$ -Teilmodul.

### Aufgabe 15

Seien  $f, g \in \text{End}_A M$ . Definiere  $f + g \in \text{End}_A M$  durch  $(f + g)(m) := f(m) + g(m)$  für  $m \in M$ . Ausgestattet mit dieser Addition ist  $\text{End}_A M$  eine abelsche Gruppe, wobei die Nullabbildung, die jedes Element von  $M$  auf 0 schickt, das (additiv) neutrale Element darstellt.

Für  $f, g, h \in \text{End}_A M$  ist  $(f + g) \circ h = f \circ h + g \circ h$ , da  $((f + g) \circ h)(m) = (f + g)(h(m)) = f(h(m)) + g(h(m)) = (f \circ h + g \circ h)(m)$  für  $m \in M$ , und  $h \circ (f + g) = h \circ f + h \circ g$ , da  $(h \circ (f + g))(m) = h(f(m) + g(m)) = h(f(m)) + h(g(m)) = (h \circ f + h \circ g)(m)$  für  $m \in M$ .

Ferner ist die Komposition auf  $\text{End}_A M$  assoziativ, und es ist  $\text{id} \circ f = f \circ \text{id} = f$  für  $f \in \text{End}_A M$ .

Ausgestattet mit der Komposition ( $\circ$ ) als Multiplikation wird die abelsche Gruppe  $\text{End}_A M$  also zu einem Ring.

Sei  $\psi : K \rightarrow \text{End}_A M$ ,  $\lambda \mapsto \lambda \text{id}_M$ , wobei  $\lambda \text{id}_M : m \mapsto \lambda m$ .

Seien  $\lambda, \mu \in K$ .

Es ist  $\psi(\lambda + \mu) = (\lambda + \mu) \text{id}_M = \lambda \text{id}_M + \mu \text{id}_M = \psi(\lambda) + \psi(\mu)$ , vorletzteres, da  $((\lambda + \mu) \text{id}_M)(m) = (\lambda + \mu)m = \lambda m + \mu m = (\lambda \text{id}_M)(m) + (\mu \text{id}_M)(m) = (\lambda \text{id}_M + \mu \text{id}_M)(m)$  für  $m \in M$ .

Es ist  $\psi(1) = 1 \text{id}_M = \text{id}_M = 1_{\text{End}_A M}$ .

Es ist  $\psi(\lambda \cdot \mu) = (\lambda \cdot \mu) \text{id}_M = (\lambda \text{id}_M) \circ (\mu \text{id}_M) = \psi(\lambda) \circ \psi(\mu)$ , vorletzteres, da  $((\lambda \cdot \mu) \text{id}_M)(m) = (\lambda \cdot \mu)m = \lambda(\mu m) = (\lambda \text{id}_M)((\mu \text{id}_M)(m)) = ((\lambda \text{id}_M) \circ (\mu \text{id}_M))(m)$  für  $m \in M$ .

Also ist  $\psi$  ein Ringmorphismus.

Bleibt zu zeigen, daß das Bild von  $\psi$  im Zentrum von  $\text{End}_A M$  liegt. Sei  $f \in \text{End}_A M$ . Sei  $\lambda \in K$ . Es wird  $\psi(\lambda) \circ f = (\lambda \text{id}_M) \circ f = f \circ (\lambda \text{id}_M) = f \circ \psi(\lambda)$ , vorletzteres, da  $((\lambda \text{id}_M) \circ f)(m) = \lambda f(m) = f(\lambda m) = (f \circ (\lambda \text{id}_M))(m)$  für  $m \in M$ .

Also ist  $\text{End}_A M = (\text{End}_A M, \psi)$  eine  $K$ -Algebra.

### Aufgabe 16

- (1) Nach Konstruktion ist  $(RG, +)$  eine abelsche Gruppe, mit  $0_{RG} = 0_R \cdot 1_G$ .

Seien  $\sum_g r_g g, \sum_g s_g g, \sum_g t_g g \in RG$ .

*Neutrales Element der Multiplikation.* Sei  $1_{RG} := 1_R \cdot 1_G$ . Es ist

$$\begin{aligned} 1_{RG} \cdot \sum_h r_h h &= (\sum_g \partial_{g,1} g)(\sum_h r_h h) \\ &= \sum_x (\sum_{gh=x} \partial_{g,1} r_h) x \\ &= \sum_x r_x x. \end{aligned}$$

Analog auf der anderen Seite.

*Assoziativität der Multiplikation.* Es ist

$$\begin{aligned} ((\sum_g r_g g)(\sum_h s_h h))(\sum_k t_k k) &= (\sum_x (\sum_{gh=x} r_g s_h) x)(\sum_k t_k k) \\ &= \sum_y (\sum_{xk=y} (\sum_{gh=x} r_g s_h t_k)) y \\ &= \sum_y (\sum_{ghk=y} r_g s_h t_k) y, \end{aligned}$$

genauso mit der anderen Klammerung.

*Distributivität der Multiplikation und der Addition.* Es ist

$$\begin{aligned} ((\sum_g r_g g) + (\sum_g s_g g))(\sum_h t_h h) &= (\sum_g (r_g + s_g) g)(\sum_h t_h h) \\ &= \sum_x (\sum_{gh=x} (r_g + s_g) t_h) x \\ &= \sum_x ((\sum_{gh=x} r_g t_h) + (\sum_{gh=x} s_g t_h)) x \\ &= \sum_x (\sum_{gh=x} r_g t_h) x + \sum_x (\sum_{gh=x} s_g t_h) x \\ &= (\sum_g r_g g)(\sum_h t_h h) + (\sum_g s_g g)(\sum_h t_h h). \end{aligned}$$

Genauso mit der Multiplikation von der anderen Seite.

- (2) *Eindeutigkeit.* Es ist  $G$  eine  $K$ -lineare Basis von  $KG$ . Also gibt es genau eine  $K$ -lineare Abbildung  $\psi : KG \rightarrow A$  mit  $\psi|_G^{\text{U}(A)} = \varphi$ . Somit gibt es höchstens einen  $K$ -Algebrenmorphismus  $\psi : KG \rightarrow A$  mit  $\psi|_G^{\text{U}(A)} = \varphi$ , nämlich genau dann, wenn besagte  $K$ -lineare Abbildung ein  $K$ -Algebrenmorphismus ist.

*Existenz.* Sei  $\psi : KG \rightarrow A, \sum_g r_g g \mapsto \sum_g r_g \varphi(g)$ . Dies ist die  $K$ -lineare Abbildung von  $KG$  nach  $A$  mit  $\psi|_G^{\text{U}(A)} = \varphi$ . Wir haben zu zeigen, daß sie ein  $K$ -Algebrenmorphismus ist.

Es ist  $\psi(1_{RG}) = \psi(1_R \cdot 1_G) = 1_R \cdot \varphi(1_G) = 1_R \cdot 1_{\text{U}(A)} = 1_A$ .

Für  $\sum_g r_g g, \sum_g s_g g \in RG$  wird ferner

$$\begin{aligned} \psi((\sum_g r_g g) \cdot (\sum_h s_h h)) &= \psi(\sum_x (\sum_{gh=x} r_g s_h) x) \\ &= \sum_x (\sum_{gh=x} r_g s_h) \varphi(x) \\ &= \sum_g \sum_h r_g s_h \varphi(gh) \\ &= \sum_g \sum_h r_g s_h \varphi(g) \varphi(h) \\ &= (\sum_g r_g \varphi(g)) \cdot (\sum_h s_h \varphi(h)) \\ &= \psi(\sum_g r_g g) \cdot \psi(\sum_h s_h h). \end{aligned}$$

Umgekehrt liefert jeder  $K$ -Algebrenmorphismus  $\psi : KG \rightarrow A$  durch Einschränkung einen Gruppenmorphismus  $\psi|_G^{\text{U}(A)} : G \rightarrow \text{U}(A)$ ; beachte, daß  $\psi(G) \subseteq \psi(\text{U}(KG)) \subseteq \text{U}(A)$ .

**Aufgabe 17**

Wir werden folgende Tatsache zu verwenden haben. Seien  $n, m \geq 1$ . Sei

$$G = \langle g_1, \dots, g_n : r_1(g_1, \dots, g_n), \dots, r_m(g_1, \dots, g_n) \rangle,$$

wobei  $r_i(g_1, \dots, g_n)$  ein Wort in den  $g_j$  ist für  $i \in [1, m]$ .

Wir haben eine Abbildung  $\{g_1, \dots, g_n\} \xrightarrow{e} CG, g_i \mapsto g_i$ .

Sei  $A$  eine  $\mathbf{C}$ -Algebra.

Ist  $\{g_1, \dots, g_n\} \xrightarrow{f} U(A)$  eine Abbildung in die Einheitengruppe  $U(A)$  von  $A$  so, daß

$$r_i(f(g_1), \dots, f(g_n)) = 1$$

für  $i \in [1, m]$ , dann gibt es genau einen  $\mathbf{C}$ -Algebrenmorphismus  $CG \xrightarrow{\hat{f}} A$ , der das Viereck

$$\begin{array}{ccc} \{g_1, \dots, g_n\} & \xrightarrow{f} & U(A) \\ e \downarrow & & \downarrow \\ CG & \xrightarrow{\hat{f}} & A \end{array}$$

kommutativ macht.

- (1) Die Abbildung  $C_3 \rightarrow U(\mathbf{C} \times \mathbf{C} \times \mathbf{C}), c \mapsto (1, \zeta, \zeta^2)$  ist als Gruppenmorphismus wohldefiniert, da das Bild von  $c$  die Relation für  $c$  erfüllt, i.e. da  $(1, \zeta, \zeta^2)^3 = 1$  ist. Durch lineare Ausdehnung definiert dies dann den angegebenen  $\mathbf{C}$ -Algebrenmorphismus.

Dessen Matrix bezüglich der Basis  $(1, c, c^2)$  im Urbildbereich und der Standardbasis im Bildbereich ist

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix},$$

und diese hat Determinante  $-3 - 6\zeta$ .

```
Q := Rational();
P<X> := PolynomialRing(Q);
K<z> := ext<Q|X^2+X+1>;
Determinant(Matrix([[1,1,1],[1,z,z^2],[1,z^2,z]]));
```

- (2) Bekanntlich ist  $\langle s_1, s_2 : s_1^2 = 1, s_2^2 = 1, (s_1 s_2)^3 = 1 \rangle \xrightarrow{\sim} \mathcal{S}_3, s_1 \mapsto (1, 2), s_2 \mapsto (2, 3)$ .

Via Magma läßt sich dies wie folgt verifizieren.

```
S3<s1,s2> := Group<S1,S2|S1^2,S2^2,(S1*S2)^3>;
S3P := SymmetricGroup(3);
ph := hom<S3 -> S3P | [S3P!(1,2), S3P!(2,3)] >;
Order(ph(S3));
Order(Kernel(ph));
```

Unser Algebrenmorphismus soll  $(1, 2)$  auf  $(1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1)$  und  $(2, 3) = (1, 2, 3) \circ (1, 2) \circ (1, 2, 3)^{-1}$  auf

$$(1, \begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}, 1)(1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1)(1, \begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}, 1)^{-1} = (1, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, -1)$$

schicken.

Dies ist möglich, da die Relationen für  $s_1$  und  $s_2$  im Bild erfüllt werden, wie folgende Rechnung zeigt.

$$\begin{aligned} (1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1)^2 &= (1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1) \\ (1, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, -1)^2 &= (1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1) \\ ((1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1)(1, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, -1)^3 &= (1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1) \end{aligned}$$

Wir prüfen noch nach, daß  $(1, 2, 3) = (1, 2) \circ (2, 3)$  auf  $(1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1)(1, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, -1) = (1, \begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}, 1)$  abgebildet wird, wie verlangt.

Via Magma verifizieren wir wie folgt, daß die Determinante unseres Algebrenmorphisms nicht verschwindet.

```
S3<s1,s2> := Group<S1,S2|S1^2,S2^2,(S1*S2)^3>;
S3P := SymmetricGroup(3);
ph := hom<S3 -> S3P | [S3P!(1,2), S3P!(2,3)] >;
DP := CartesianProduct([MatrixRing(Integers(),1),MatrixRing(Integers(),2),
                        MatrixRing(Integers(),1)]);
d := [DP!<Matrix([[1]]),Matrix([[ -2,-1],[3,2]]),Matrix([[ -1]])>,
      DP!<Matrix([[1]]),Matrix([[1,1],[0,-1]]),Matrix([[ -1]])>];
mat_seq := [];
for x in S3P do
  x_inv := ElementToSequence(x@@ph);
  prod := DP!<1,1,1>;
  for i in x_inv do
    for j in [1..3] do
      prod[j] := d[i][j];
    end for;
  end for;
  for j in [1..3] do
    mat_seq cat:= ElementToSequence(prod[j]);
  end for;
end for;
ms := RMatrixSpace(Integers(),Order(S3P),Order(S3P));
emb := ms!mat_seq;
print(emb);
print(Determinant(emb));
```

In der Tat ergibt sich diese Determinante zu  $-54$ .

(3) Bekanntlich ist

$$\begin{aligned} \langle s_1, s_2, s_3 : s_1^2, s_2^2, s_3^2, (s_1 s_2)^3, (s_2 s_3)^3, (s_1 s_3)^2, \rangle &\xrightarrow{\sim} \mathcal{S}_4 \\ s_1 &\longmapsto (1, 2) \\ s_2 &\longmapsto (2, 3) \\ s_3 &\longmapsto (3, 4). \end{aligned}$$

Hierbei wurde bei den Relationen jeweils “= 1” unterschlagen.

Via Magma läßt sich dies wie folgt verifizieren.

```
S4<s1,s2,s3> := Group<S1,S2,S3|S1^2,S2^2,S3^2,(S1*S2)^3,(S2*S3)^3,(S1*S3)^2>;
S4P := SymmetricGroup(4);
ph := hom<S4 -> S4P | [S4P!(1,2), S4P!(2,3), S4P!(3,4)] >;
Order(ph(S4));
Order(Kernel(ph));
```

Da  $(2, 3) = (1, 2, 3, 4) \circ (1, 2) \circ (1, 2, 3, 4)^{-1}$  und  $(3, 4) = (1, 2, 3, 4)^2 \circ (1, 2) \circ (1, 2, 3, 4)^{-2}$ , sollte unser Algebrenmorphismus

$$\begin{aligned} (1, 2) &\longmapsto (1, -1, \begin{pmatrix} -11 & -24 & 2 \\ 5 & 11 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -5 & 24 \\ -1 & 5 \end{pmatrix}) \\ (2, 3) &\longmapsto (1, -1, \begin{pmatrix} 19 & 45 & 0 \\ -8 & -19 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -9 \\ 0 & -1 \end{pmatrix}) \\ (3, 4) &\longmapsto (1, -1, \begin{pmatrix} 15 & 32 & 0 \\ -7 & -15 & 0 \\ -4 & -8 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -3 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -5 & 24 \\ -1 & 5 \end{pmatrix}) \end{aligned}$$

abbilden.

Dies ist möglich, da die Relationen für  $s_1$ ,  $s_2$  und  $s_3$  im Bild erfüllt werden, wie wir nachrechnen. Via Magma verifizieren wir wie folgt, daß die Determinante unseres Algebrenmorphismus nicht verschwindet.

```
S4<s1,s2,s3> := Group<S1,S2,S3|S1^2,S2^2,S3^2,(S1*S2)^3,(S2*S3)^3,(S1*S3)^2>;
S4P := SymmetricGroup(4);
ph := hom<S4 -> S4P | [S4P!(1,2), S4P!(2,3), S4P!(3,4)] >;
DP := CartesianProduct(MatrixRing(Integers(),1),MatrixRing(Integers(),1),
    MatrixRing(Integers(),3),MatrixRing(Integers(),3),
    MatrixRing(Integers(),2));
d := [DP!<Matrix([[1]]),Matrix([[ -1]]),Matrix([[ -11,-24,2],[5,11,-1],[0,0,-1]]),
    Matrix([[1,0,0],[1,-1,1],[0,0,1]]),Matrix([[ -5,24],[-1,5]])>,
    DP!<Matrix([[1]]),Matrix([[ -1]]),Matrix([[19,45,0],[-8,-19,0],[0,0,-1]]),
    Matrix([[ -1,1,0],[0,1,0],[0,0,1]]),Matrix([[1,-9],[0,-1]])>,
    DP!<Matrix([[1]]),Matrix([[ -1]]),Matrix([[15,32,0],[-7,-15,0],[-4,-8,-1]]),
    Matrix([[ -1,0,0],[-3,1,0],[-4,0,1]]),Matrix([[ -5,24],[-1,5]])>];
mat_seq := [];
for x in S4P do
  x_inv := ElementToSequence(x@@ph);
  prod := DP!<1,1,1,1,1>;
  for i in x_inv do
    for j in [1..5] do
      prod[j] := d[i][j];
    end for;
  end for;
  for j in [1..5] do
    mat_seq cat:= ElementToSequence(prod[j]);
  end for;
end for;
ms := RMatrixSpace(Integers(),Order(S4P),Order(S4P));
emb := ms!mat_seq;
print(emb);
print(Determinant(emb));
```

In der Tat ergibt sich diese Determinante zu  $-2^{34} \cdot 3^3$ .

(4) Bekanntlich ist

$$\begin{aligned} \mathcal{D}_{10} = \langle a, b : a^5 = 1, b^2 = 1, (ba)^2 = 1 \rangle &\longrightarrow \mathcal{S}_5 \\ a &\longmapsto (1, 2, 3, 4, 5) \\ b &\longmapsto (2, 5)(3, 4) \end{aligned}$$

ein injektiver Gruppenmorphismus.

Hierbei wurde bei den Relationen jeweils “= 1” unterschlagen.

Via Magma läßt sich dies wie folgt verifizieren.

```

D10<a,b> := Group<A,B|A^5,B^2,(B*A)^2>;
S5P := SymmetricGroup(5);
ph := hom<D10 -> S5P | [S5P!(1,2,3,4,5), S5P!(2,5)(3,4)] >;
Order(ph(D10));
Order(Kernel(ph));

```

Wir rechnen nach, daß die Relationen für die angegebenen Bilder gelten. Dazu verfähre man e.g. wie folgt.

```

Q := Rationals();
P<X> := PolynomialRing(Q);
K<th> := ext<Q | X^2 + 5*X + 5>;
MA := Matrix([[1,1],[th,th+1]]);
MB := Matrix([[1,1],[0,-1]]);
NA := Matrix([[1,1],[-th-5,-th-4]]);
NB := Matrix([[1,1],[0,-1]]);
print MA^5, MB^2, (MB*MA)^2;
print NA^5, NB^2, (NB*NA)^2;

```

Also existiert der Algebrenmorphismus in der angegebenen Weise.

Via Magma verifizieren wir wie folgt, daß die Determinante unseres Algebrenmorphismus nicht verschwindet. Um exakt rechnen zu können, können wir  $\mathbf{Q}(\vartheta) \subseteq \mathbf{C}$  verwenden, denn zur Determinantenberechnung macht es keinen Unterschied, ob man die Einträge als in einem Teilkörper liegend betrachtet.

```

D10<a,b> := Group<A,B|A^5,B^2,(B*A)^2>;
S5P := SymmetricGroup(5);
ph := hom<D10 -> S5P | [S5P!(1,2,3,4,5), S5P!(2,5)(3,4)] >;
Q := Rationals();
P<X> := PolynomialRing(Q);
K<th> := ext<Q | X^2 + 5*X + 5>;
MA := Matrix([[1,1],[th,th+1]]);
MB := Matrix([[1,1],[0,-1]]);
NA := Matrix([[1,1],[-th-5,-th-4]]);
NB := Matrix([[1,1],[0,-1]]);
DP := CartesianProduct([MatrixRing(K,1),MatrixRing(K,1),
                        MatrixRing(K,2),MatrixRing(K,2)]);
d := [DP!<Matrix([[1]]),Matrix([[1]]),MA,NA>,DP!<Matrix([[1]]),Matrix([[1]]),MB,NB>];
mat_seq := [];
for x in ph(D10) do
  x_inv := ElementToSequence(x@@ph);
  print x_inv;
  prod := DP!<1,1,1,1>;
  for i in x_inv do
    for j in [1..4] do
      prod[j] := d[Abs(i)][j]^Sign(i);
    end for;
  end for;
  for j in [1..4] do
    mat_seq cat:= ElementToSequence(prod[j]);
  end for;
end for;
ms := RMatrixSpace(K,Order(ph(D10)),Order(ph(D10)));

```

```
emb := ms!mat_seq;
print(emb);
print(Determinant(emb));
```

In der Tat ergibt sich diese Determinante zu  $-6250$ .

### Aufgabe 18

Eine  $\mathbf{Z}$ -lineare Basis der angegebenen Untergruppe  $U \leq \mathbf{Z} \times \mathbf{Z}^{2 \times 2} \times \mathbf{Z}$  ist gegeben durch

$$\left( (1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1), (0, \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}, 0), (0, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 0), (0, \begin{pmatrix} 0 & 0 \\ 3 & 0 \end{pmatrix}, 0), (0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 4), (0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, 6) \right),$$

linear unabhängig nach oberer Dreiecksgestalt, erzeugend nach Konstruktion. Die Determinante der zugehörigen Matrix zeigt, daß der Index von  $U \leq \mathbf{Z} \times \mathbf{Z}^{2 \times 2} \times \mathbf{Z}$  gerade  $2^1 \cdot 3^3$  beträgt.

Der Wedderburnisomorphismus  $\mathbf{CS}_3 \rightarrow \mathbf{C} \times \mathbf{C}^{2 \times 2} \times \mathbf{C}$  aus Aufgabe 17.(2) schränkt ein zu einer Einbettung  $\varphi : \mathbf{ZS}_3 \rightarrow \mathbf{Z} \times \mathbf{Z}^{2 \times 2} \times \mathbf{Z}$ . Deren Matrix aus loc. cit. ist gegeben durch

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & -3 & -2 & 1 \\ 1 & -2 & -1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 0 & -1 & -1 \\ 1 & -2 & -1 & 3 & 2 & -1 \\ 1 & 1 & 0 & -3 & -1 & -1 \end{pmatrix}$$

Das Bild  $\varphi(\mathbf{ZS}_3)$  dieser Einbettung ist eine Untergruppe, die in  $U$  enthalten ist, wie eine direkte Inspektion der  $U$  beschreibenden Kongruenzen ("Bindungen") zeigt. Der Index von  $\varphi(\mathbf{ZS}_3) \leq \mathbf{Z} \times \mathbf{Z}^{2 \times 2} \times \mathbf{Z}$  beträgt  $2^1 \cdot 3^3$ , wie die Determinante  $-54$  dieser Matrix zeigt. Somit ist

$$\varphi(\mathbf{ZS}_3) = U.$$

Es ist  $\varphi(\mathbf{ZS}_3)$  als Bild eines Ringmorphismus ein Teilring von  $\mathbf{Z} \times \mathbf{Z}^{2 \times 2} \times \mathbf{Z}$ , und also ist auch unsere diesem gleiche Untergruppe  $U$  darin ein Teilring.

Schließlich ist  $\varphi^U : \mathbf{ZS}_3 \rightarrow U$  ein Ringisomorphismus.

Alternativ kann man auch den Quotienten beider Einbettungsmatrizen berechnen und direkt erkennen, daß dies ein Element von  $\mathrm{GL}_6(\mathbf{Z})$  ist. Dann hat man auch keine Kongruenzen direkt zu inspizieren.

### Aufgabe 19

$\Leftarrow$ . Sei  $|G|$  kein Vielfaches von  $\mathrm{char} K$ . Wir wollen zeigen, daß  $KG$  halbeinfach ist.

Sei  $M$  ein endlichdimensionaler  $KG$ -Modul. Sei  $N \subseteq M$  ein Teilmodul. Wir haben zu zeigen, daß ein  $KG$ -Teilmodul  $X \subseteq M$  mit  $M = N \oplus X$  existiert. Cf. Definition 20.(4). Sei  $f : M \rightarrow N$  eine  $K$ -lineare Abbildung mit  $f|_N = \mathrm{id}_N$ . Sei

$$\begin{aligned} f' : M &\longrightarrow N \\ m &\longmapsto f'(m) := |G|^{-1} \sum_{g \in G} g f(g^{-1}m). \end{aligned}$$

Es ist  $f'|_N = \mathrm{id}_N$ , da  $f'(n) = |G|^{-1} \sum_{g \in G} g f(g^{-1}n) = |G|^{-1} \sum_{g \in G} g(g^{-1}n) = |G|^{-1} \sum_{g \in G} n = n$  für  $n \in N$ .

Es ist  $f'$  eine  $KG$ -lineare Abbildung, da sie mit der Addition verträglich ist und sich für  $\sum_h r_h h \in KG$  und  $m \in M$

$$\begin{aligned} f'((\sum_h r_h h)m) &= |G|^{-1} \sum_g g f(g^{-1}(\sum_h r_h h m)) \\ &= |G|^{-1} \sum_h r_h \sum_g g f(g^{-1}h m) \\ &\stackrel{y = g^{-1}h}{=} |G|^{-1} \sum_h r_h \sum_y h y^{-1} f(y m) \\ &= \sum_h r_h h |G|^{-1} \sum_y y^{-1} f(y m) \\ &= (\sum_h r_h h) f'(m) \end{aligned}$$

ergibt.

Sei  $X := \text{Kern } f'$ . Dies ist ein  $KG$ -Teilmodul von  $M$  als Kern einer  $KG$ -linearen Abbildung.

Es ist  $N \cap X = 0$ , da für ein  $n \in N \cap X = N \cap \text{Kern } f'$  sich  $n = f'(n) = 0$  ergibt.

Es ist  $M = N + X$ , da wir für  $m \in M$  die Zerlegung  $m = f'(m) + (m - f'(m))$  mit  $f'(m) \in N$  und  $f'(m - f'(m)) = f'(m) - \underbrace{f'(f'(m))}_{\in N} = f'(m) - f'(m) = 0$  ergibt.

Insgesamt ist  $M = N \oplus X$ .

$\Rightarrow$ . Sei  $KG$  halbeinfach. Wir wollen zeigen, daß  $|G|$  kein Vielfaches von  $\text{char } K$  ist, d.h. daß  $|G| \cdot 1_K \stackrel{!}{\neq} 0$ .  
Schreibe  $\sigma := \sum_g g \in KG$ . Es ist  $M := KG$  ein  $KG$ -Modul. Darin ist  $N := KG\sigma$  ein Teilmodul.

Es ist  $h\sigma = \sigma$  für  $h \in G$  und also  $N = K\sigma$ .

Da  $KG$  halbeinfach ist, gibt es einen  $KG$ -Teilmodul  $X \subseteq KG$  mit  $M = N \oplus X$ . Die Projektion  $\pi : M \rightarrow M$ ,  $n + x \mapsto n$ , wobei  $n \in N$  und  $x \in X$ , ist eine  $KG$ -lineare Abbildung. Sie schickt  $1$  nach  $\pi(1) = \lambda\sigma$  für ein  $\lambda \in K$ . Also wird

$$\begin{aligned} \sigma &= \pi(\sigma) \\ &= \pi(\sum_g g) \\ &= \sum_g g \pi(1) \\ &= \sum_g g \lambda\sigma \\ &= \sum_g \lambda\sigma \\ &= |G|\lambda\sigma. \end{aligned}$$

Ein Koeffizientenvergleich bei  $1$  gibt  $1 = |G|\lambda = (|G| \cdot 1_K)\lambda$ . Es folgt  $|G| \cdot 1_K \neq 0$ .

## Aufgabe 20

- (1) Die Aussage ist falsch. Sei e.g.  $G = \mathcal{S}_2$ . Es wird  $(1 + (1, 2))(1 - (1, 2)) = 1 - (1, 2)^2 = 0$ , aber  $1 + (1, 2) \neq 0$  und  $1 - (1, 2) \neq 0$ .
- (2) Die Aussage ist richtig. Sei *angenommen*, es gibt in  $\mathbf{Z}G$  ein Idempotent  $e \notin \{0, 1\}$ . Dann ist  $(e, 1-e)$  eine orthogonale Zerlegung in Idempotenten und also

$$\mathbf{Z}G \stackrel{\text{B.15}}{=} \mathbf{Z}Ge \oplus \mathbf{Z}G(1-e).$$

Es ist  $\mathbf{Z}Ge \neq 0$  und  $\mathbf{Z}G(1-e) \neq 0$ , da  $e \neq 0$  und  $(1-e) \neq 0$ . Insbesondere ist  $0 < \text{rk}_{\mathbf{Z}} \mathbf{Z}Ge < |G|$ .  
Für  $\vartheta \in \mathbf{Z}G$  betrachten wir die Abbildung  $\rho_\vartheta : \mathbf{Z}G \rightarrow \mathbf{Z}G$ ,  $\xi \mapsto \xi\vartheta$ .

Bezüglich der  $\mathbf{Z}$ -linearen Basis  $G$  von  $\mathbf{Z}G$  berechnet, wird

$$\text{tr } \rho_g = |G|\partial_{g,1}$$

für  $g \in G$ , da  $g$  kein Gruppenelement auf sich multipliziert, falls  $g \neq 1$ .

Schreibe  $e = \sum_g r_g g$  mit  $r_g \in \mathbf{Z}$  für  $g \in G$ . Es wird

$$\text{tr } \rho_e = \sum_g r_g \text{tr } \rho_g = \sum_g r_g |G|\partial_{g,1} = |G|r_1.$$

Auf der anderen Seite wird bezüglich der Zerlegung  $\mathbf{Z}G = \mathbf{Z}Ge \oplus \mathbf{Z}G(1-e)$

$$\text{tr } \rho_e = \text{tr} \begin{pmatrix} \rho_e|_{\mathbf{Z}Ge} & 0 \\ 0 & \rho_e|_{\mathbf{Z}G(1-e)} \end{pmatrix} = \text{tr} \begin{pmatrix} \text{id}_{\mathbf{Z}Ge} & 0 \\ 0 & 0 \end{pmatrix} = \text{rk}_{\mathbf{Z}} \mathbf{Z}Ge.$$

Insgesamt ist  $0 < |G|r_1 = \text{rk}_{\mathbf{Z}} \mathbf{Z}Ge < |G|$ , und das ist ein *Widerspruch* zu  $r_1 \in \mathbf{Z}$ .

Wem die  $\mathbf{Z}$ -linearen Spuren suspekt sind, der verwende, daß ein Idempotent in  $\mathbf{Z}G \setminus \{0, 1\}$  auch ein Idempotent in  $\mathbf{Q}G \setminus \{0, 1\}$  ist, und zeige mit einer  $\mathbf{Q}$ -linearen Version obiger Argumente, daß dessen Koeffizient bei 1 echt zwischen 0 und 1 liegen muß.

- (3) Die Aussage ist falsch. Sei  $G$  irgendeine nichtabelsche endliche Gruppe (e.g.  $\mathcal{S}_3$ ). Es ist

$$\mathbf{C}G \simeq \prod_{s \in [1, t]} \mathbf{C}^{n_s \times n_s}$$

als  $\mathbf{C}$ -Algebren, für gewisse  $t \geq 0$  und  $n_s \geq 1$  für  $s \in [1, t]$  cf. Satz 25, Aufgabe 19.

Da  $G$  nichtabelsch ist, ist  $\mathbf{C}G$  kein kommutativer Ring. Somit ist  $n_s \geq 2$  für ein  $s \in [1, t]$ . Das Element von  $\prod_{s \in [1, t]} \mathbf{C}^{n_s \times n_s}$ , das an Position  $s$  die Matrix  $e_{1, n_s}$  als Eintrag hat, und sonst Nullmatrizen, ist nilpotent und ungleich 0. Selbiges gilt also auch für sein Bild in  $\mathbf{C}G$ .

- (4) Die Aussage ist richtig. Es ist

$$\mathbf{C}G \simeq \prod_{s \in [1, t]} \mathbf{C}^{n_s \times n_s}$$

als  $\mathbf{C}$ -Algebren, für gewisse  $t \geq 0$  und  $n_s \geq 1$  für  $s \in [1, t]$  cf. Satz 25, Aufgabe 19.

Da  $G$  abelsch ist, ist  $\mathbf{C}G$  ein kommutativer Ring. Somit ist  $n_s = 1$  für alle  $s \in [1, t]$ , und also

$$\mathbf{C}G \simeq \mathbf{C}^{\times t} := \underbrace{\mathbf{C} \times \cdots \times \mathbf{C}}_{t \text{ Faktoren}} .$$

Ein nilpotentes Element in  $\mathbf{C}^{\times t}$  ist eintragsweise nilpotent, und damit eintragsweise gleich 0. Also gibt es in  $\mathbf{C}^{\times t}$  keine nilpotenten Elemente ungleich 0. Folglich gibt es auch in  $\mathbf{C}G$  keine nilpotenten Elemente ungleich 0.

- (5) Die Aussage ist richtig. Sei  $G$  eine  $p$ -Gruppe. Sei  $S$  ein einfacher  $\mathbf{F}_p G$ -Modul. Wir zeigen die stärkere Aussage, daß  $S$  isomorph ist zu  $\mathbf{F}_p$ , ausgestattet mit der trivialen  $\mathbf{F}_p G$ -Modulstruktur, welche bezüglich  $g \cdot s = s$  ist für  $g \in G$  und  $s \in S$ .

Es ist  $S$  als epimorphes Bild von  $\mathbf{F}_p G$  endlichdimensional.

Es genügt zu zeigen, daß für einen beliebigen endlichdimensionalen  $\mathbf{F}_p G$ -Modul  $M$  ungleich 0 der Teilmodul

$$M^G = \{ m \in M : gm = m \text{ für } g \in G \} \subseteq M$$

ungleich 0 ist. Denn  $M^G$  zerfällt in eine direkte Summe von eindimensionalen trivialen Moduln. In  $S$  ist also zunächst  $S^G = S$ , und sodann  $S$  trivial.

Nach dem Bahnenlemma hat die Bahn eines Elements  $m$  der  $G$ -Menge  $M$  die Länge

$$|G| / |\{ g \in G : gm = m \}| .$$

Diese teilt  $|G|$ , ist also eine Potenz von  $p$ .

Da die Bahn von  $0 \in M$  die Länge 1 hat, und die Summe der Bahnlängen gleich  $p^{\dim_{\mathbf{F}_p} M}$  und also durch  $p$  teilbar ist, muß es in  $M$  eine weitere Bahn von Länge 1 geben, i.e. ein Element von  $M^G \setminus \{0\}$ .

## Aufgabe 21

Wir erinnern daran, daß primitive Idempotente insbesondere ungleich 0 sind.

Nach Aufgabe 12 gibt es in  $A$  eine orthogonale Zerlegung  $\underline{e} = (e_1, \dots, e_n)$  in primitive Idempotente.

Wir haben zu zeigen, daß dies die einzige Zerlegung in primitive Idempotente in  $A$  ist.

Sei  $f$  ein primitives Idempotent in  $A$ . Es genügt zu zeigen, daß  $f \stackrel{!}{=} e_i$  für ein  $i \in [1, n]$ .

Denn dann können in einer Zerlegung  $\tilde{e}$  in primitive Idempotente in  $A$  nur Einträge von  $\underline{e}$  auftreten. Wegen Orthogonalität kann  $\tilde{e}$  jeden Eintrag von  $\underline{e}$  höchstens einmal beinhalten. Da die Summe der Einträge von  $\tilde{e}$  gleich 1 ist, kann auch kein Eintrag von  $\underline{e}$  in  $\tilde{e}$  fehlen. Insgesamt stimmen  $\underline{e}$  und  $\tilde{e}$  dann bis auf Reihenfolge überein.

Betrachten wir also unser  $f$ . Es ist  $f = fe_1 + \dots + fe_n$ . Da  $f \neq 0$ , gibt es ein  $i \in [1, n]$  mit  $fe_i \neq 0$ . Es ist  $f = fe_i + f(1 - e_i)$ . Da  $A$  kommutativ ist, sind  $fe_i$  und  $f(1 - e_i)$  Idempotente. Da  $A$  kommutativ ist, ist  $(fe_i)(f(1 - e_i)) = 0$  und  $(f(1 - e_i))(fe_i) = 0$ . Da  $f$  primitiv ist und da  $fe_i \neq 0$ , folgt  $f(1 - e_i) = 0$ , also  $f = fe_i$ .

Es ist  $e_i = fe_i + (1 - f)e_i$ . Da  $A$  kommutativ ist, sind  $fe_i$  und  $(1 - f)e_i$  Idempotente. Da  $A$  kommutativ ist, ist  $(fe_i)((1 - f)e_i) = 0$  und  $((1 - f)e_i)(fe_i) = 0$ . Da  $e_i$  primitiv ist und da  $fe_i \neq 0$ , folgt  $(1 - f)e_i = 0$ , also  $e_i = fe_i$ .

Insgesamt ist  $f = fe_i = e_i$  gezeigt.

## Aufgabe 22

- (1) Sind Ringe  $A$  und  $B$  gegeben, so behaupten wir, daß  $Z(A \times B) = Z(A) \times Z(B)$  als Teilringe von  $A \times B$ . Sei dazu  $(a, b) \in A \times B$  gegeben. Es ist  $(a, b) \in Z(A \times B)$  genau dann, wenn  $(a, b)(x, y) = (x, y)(a, b)$  für  $(x, y) \in A \times B$ , i.e. genau dann, wenn  $ax = xa$  für  $x \in A$  und  $by = yb$  für  $y \in B$ , i.e. genau dann, wenn  $(a, b) \in Z(A) \times Z(B)$ . Dies zeigt die Behauptung.

Also genügt es faktorweise zu zeigen, daß  $Z(\mathbf{C}^{n_s \times n_s}) \stackrel{!}{=} \mathbf{C}\langle E_{n_s} \rangle$  für  $s \in [1, t]$ .

Zu zeigen ist nur  $\stackrel{!}{\subseteq}$ .

Sei  $\sum_{i,j} \lambda_{i,j} e_{i,j} \in Z(\mathbf{C}^{n_s \times n_s})$ , wobei  $\lambda_{i,j} \in \mathbf{C}$ . Zu zeigen ist  $\lambda_{i,j} \stackrel{!}{=} 0$  für  $i \neq j$  und  $\lambda_{i,i} \stackrel{!}{=} \lambda_{j,j}$  stets. Für  $k, \ell \in [1, n_s]$  ist

$$\sum_j \lambda_{\ell,j} e_{k,j} = e_{k,\ell} \left( \sum_{i,j} \lambda_{i,j} e_{i,j} \right) = \left( \sum_{i,j} \lambda_{i,j} e_{i,j} \right) e_{k,\ell} = \left( \sum_{i,j} \lambda_{i,k} e_{i,\ell} \right)$$

Koeffizientenvergleich bei  $e_{k,k}$  gibt  $\lambda_{\ell,k} = 0$  falls  $k \neq \ell$ .

Koeffizientenvergleich bei  $e_{k,\ell}$  gibt  $\lambda_{\ell,\ell} = \lambda_{k,k}$ .

- (2) Sei  $\xi = \sum_g z_g g \in \mathbf{C}G$ . Es ist  $\xi \in Z(\mathbf{C}G)$  genau dann, wenn  $\xi h = h\xi$  für  $h \in G$ , denn dann vertauscht  $g$  auch mit  $\mathbf{C}$ -Linearkombinationen von Gruppenelementen.

Also ist  $\xi \in Z(\mathbf{C}G)$  genau dann, wenn

$$\sum_g z_g hg = \sum_g z_g gh = \sum_g z_{gh^{-1}} g = \sum_g z_{hgh^{-1}} hg$$

für  $h \in H$ . Koeffizientenvergleich zeigt, daß dies genau dann der Fall ist, wenn  $z_g = z_{hgh^{-1}}$  für alle  $g, h \in G$ , i.e. wenn  $z_g$  auf jeder Konjugationsklasse konstant ist. Das wiederum ist gleichbedeutend zu  $\xi \in \mathbf{C}\langle \sum_{x \in g^G} x : g \in G \rangle$ .

- (3) Aus (2) entnehmen wir die Basis  $\{ \sum_{x \in g^G} x : g \in G \}$  von  $Z(\mathbf{C}G)$ , mithin  $|\{g^G : g \in G\}| = \dim_{\mathbf{C}} Z(\mathbf{C}G)$ .

Aus (1) entnehmen wir, daß  $\dim_{\mathbf{C}} Z(\mathbf{C}G) = \dim_{\mathbf{C}} \mathbf{C}^{\times t} = t$ .

## Aufgabe 23

Schreibe  $n := \chi(1)$ . Sei  $\varphi : \mathbf{C}G \rightarrow \mathbf{C}^{n \times n}$  die zu  $\chi$  gehörige Komponente des gewählten Wedderburnisomorphismus. Sei also  $\chi(g) = \text{tr } \varphi(g)$ . Sei  $S \in \mathbf{C}^{n \times n}$  mit  $J := S\varphi(g)S^{-1}$  in Jordanform. Da  $\varphi(g)^k = E_n$

ist, ist auch  $J^k = E_n$ . Also ist  $J$  eine Diagonalmatrix, und die Diagonaleinträge sind Nullstellen von  $z^k - 1$ . In anderen Worten, es ist

$$J = \begin{pmatrix} \zeta^{m_1} & & \\ & \ddots & \\ & & \zeta^{m_n} \end{pmatrix}$$

für gewisse  $m_i \in [0, k-1]$  für  $i \in [1, n]$ .

(1) Wir erhalten

$$\chi(g) = \operatorname{tr} \varphi(g) = \operatorname{tr} J = \sum_{i \in [1, n]} \zeta^{m_i} = \sum_{j \in [0, k-1]} \underbrace{|\{i \in [1, n] : m_i = j\}|}_{=: x_j} \cdot \zeta^j.$$

(2) Beachte, daß  $\bar{\zeta} = \overline{\exp(2\pi i/k)} = \exp(\overline{2\pi i/k}) = \exp(-2\pi i/k) = \zeta^{-1}$ .

Wir erhalten

$$\begin{aligned} \chi(g^{-1}) &= \operatorname{tr} \varphi(g^{-1}) \\ &= \operatorname{tr} J^{-1} \\ &= \operatorname{tr} \begin{pmatrix} \zeta^{-m_1} & & \\ & \ddots & \\ & & \zeta^{-m_n} \end{pmatrix} \\ &= \sum_{i \in [1, n]} \zeta^{-m_i} \\ &= \overline{\sum_{i \in [1, n]} \zeta^{m_i}} \\ &= \overline{\chi(g)} \end{aligned}$$

(3) Sei  $M$  ein endlichdimensionaler  $\mathbf{C}G$ -Modul.

Sei der Dualraum  $M^* := \operatorname{Hom}_{\mathbf{C}}(M, \mathbf{C})$  ausgestattet mit der Linksmultiplikation

$$(h \cdot f)(m) := f(h^{-1}m)$$

für  $h \in G$  und  $f \in M^*$  und  $m \in M$ . Dies liefert einen Gruppenmorphismus

$$\begin{aligned} G &\longrightarrow \operatorname{GL}(M^*) \\ h &\longmapsto (f \mapsto h \cdot f), \end{aligned}$$

da sich

$$((h\tilde{h}) \cdot f)(m) = f((h\tilde{h})^{-1}m) = f(\tilde{h}^{-1}h^{-1}m) = (\tilde{h} \cdot f)(h^{-1}m) = (h \cdot (\tilde{h} \cdot f))(m)$$

ergibt für  $h, \tilde{h} \in G$ ,  $f \in M^*$  und  $m \in M$ , i.e.  $h\tilde{h} \mapsto (h \cdot (-)) \circ (\tilde{h} \cdot (-))$ .

Dieser kann zu einem  $\mathbf{C}$ -Algebrenmorphismus

$$\begin{aligned} \mathbf{C}G &\longrightarrow \operatorname{End}_{\mathbf{C}}(M^*) \\ \sum_h z_h h &\longmapsto (f \mapsto \sum_h z_h h \cdot f) \end{aligned}$$

fortgesetzt werden; cf. Aufgabe 16.(2). Ein solcher definiert eine  $\mathbf{C}G$ -Modulstruktur auf  $M^*$ .

Allgemein definiert für einen Körper  $K$  auf einem  $K$ -Vektorraum  $V$  ein  $K$ -Algebrenmorphismus  $\psi : A \rightarrow \operatorname{End}_K V$  eine  $A$ -Modulstruktur auf  $V$  via  $a \cdot v := \psi(a)(v)$ .

Sein nun  $M$  einfach. Wir *behaupten*, daß auch  $M^*$  einfach ist.

Denn dann ist zum einen  $\dim_{\mathbf{C}} M^* = \dim_{\mathbf{C}} M > 0$ , also  $M^* \neq 0$ .

Zum anderen, ist  $N \subseteq M^*$  ein Teilmodul, so ist auch

$$N' := \{m \in M : f(m) = 0 \text{ für } f \in N\}$$

ein Teilmodul. Denn es ist ein Teilraum. Und für  $m \in N'$  und  $h \in G$  ist  $hm \in M$ , da  $f(hm) = (h^{-1}f)(m) = 0$  für  $f \in N$ , da mit  $f$  auch  $h^{-1}f$  in  $N$  liegt. Da  $M$  einfach ist, ist  $N' = 0$  oder  $N' = M$ .

Es ist  $\dim_{\mathbf{C}} N' + \dim_{\mathbf{C}} N = \dim_{\mathbf{C}} M$ , wie man mit einer Basis von  $N$ , die zu einer Basis von  $M^*$  ergänzt wird, und deren Dualbasis von  $M$  erkennt. Also ist  $N = 0$  oder  $N = M$ .

Dies zeigt die *Behauptung*.

Sei nun  $M$  so, daß  $\text{tr } \ell_M(h) = \chi(h)$  für  $h \in G$ ; cf. Bemerkung 35.

Nach obigem ist  $\text{tr } \circ \ell_{M^*}$  ein irreduzibler Charakter von  $G$ ; cf. Bemerkung 35.

Sei  $(m_1, \dots, m_s)$  eine Basis von  $M$ . Sei  $(m_1^*, \dots, m_s^*)$  die dazu duale Basis von  $M^*$ . Sei  $h \in G$ . Sei  $h^{-1}m_i = \sum_j z_{j,i} m_j$  für  $i \in [1, s]$ , wobei  $z_{j,i} \in \mathbf{C}$ . Dann ist

$$(hm_k^*)(m_i) = m_k^*(h^{-1}m_i) = \sum_j z_{j,i} m_k^*(m_j) = z_{k,i}$$

für  $i, k \in [1, s]$ , und also  $hm_k^* = \sum_i z_{k,i} m_i^*$ . Es folgt

$$\text{tr } \ell_{M^*}(h) = \sum_i z_{i,i} = \text{tr } \ell_M(h^{-1}) = \chi(h^{-1}) \stackrel{(2)}{=} \overline{\chi(h)}$$

für  $h \in G$ .

## Aufgabe 24

- (1) Die Konjugationsklassen von  $\mathcal{C}_3 := \langle c : c^3 = 1 \rangle$  sind einelementig und also repräsentiert durch 1,  $c$ ,  $c^2$ . Sei  $\zeta = \zeta_3 = \exp(2\pi i/3)$ . Der Wedderburnisomorphismus aus Aufgabe 17.(1) bildet wie folgt ab.

$$\begin{array}{lcl} \mathbf{C}\mathcal{C}_3 & \longrightarrow & \mathbf{C} \times \mathbf{C} \times \mathbf{C} \\ 1 & \longmapsto & (1, 1, 1) \\ c & \longmapsto & (1, \zeta, \zeta^2) \\ c^2 & \longmapsto & (1, \zeta^2, \zeta) \end{array}$$

Spur zu nehmen ändert in  $\mathbf{C}^{1 \times 1} = \mathbf{C}$  nichts. Als Charaktertafel erhalten wir

$$X = X(\mathcal{C}_3) = \begin{array}{c} \chi_1 \\ \chi_2 \\ \chi_3 \end{array} \begin{bmatrix} 1 & c & c^2 \\ 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{bmatrix}$$

Es sind  $\chi_2$  und  $\chi_3$  konjugiert im Sinne von Aufgabe 23.(3).

Magma liefert mit

```
C := sub<SymmetricGroup(3) | (1,2,3)>;
CharacterTable(C);
```

die Charaktertafel

```
Class | 1 2 3
Size  | 1 1 1
Order | 1 3 3
-----
p = 3  1 1 1
```

```

-----
X.1  +   1   1   1
X.2  0   1   J-1-J
X.3  0   1-1-J   J

```

Explanation of Character Value Symbols

J = RootOfUnity(3) ,

die wir unter Beachtung von  $\zeta^2 = -1 - \zeta$  als identisch mit der unsrigen erkennen.

- (2) Die Konjugationsklassen von  $\mathcal{S}_3$  sind repräsentiert durch id, (1, 2), (1, 2, 3). Der Wedderburnisomorphismus aus Aufgabe 17.(2) bildet wie folgt ab.

$$\begin{array}{rcl}
 \mathbf{CS}_3 & \longrightarrow & \mathbf{C} \times \mathbf{C}^{2 \times 2} \times \mathbf{C} \\
 \text{id} & \longmapsto & (1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1) \\
 (1, 2) & \longmapsto & (1, \begin{pmatrix} -2 & -1 \\ 3 & 2 \end{pmatrix}, -1) \\
 (1, 2, 3) & \longmapsto & (1, \begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}, 1)
 \end{array}$$

Die Spur liefert die Charaktertafel

$$X = X(\mathcal{S}_3) = \begin{matrix} & 1 & (1, 2) & (1, 2, 3) \\ \begin{matrix} \chi_1 \\ \chi_2 \\ \chi_3 \end{matrix} & \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{bmatrix} \end{matrix}$$

Magma liefert mit

```
CharacterTable(SymmetricGroup(3));
```

die Charaktertafel

```

Class | 1 2 3
Size  | 1 3 2
Order | 1 2 3
-----
p = 2  1 1 3
p = 3  1 2 1
-----
X.1  +   1   1   1
X.2  +   1  -1   1
X.3  +   2   0  -1 ,

```

die mit der unsrigen übereinstimmt.

- (3) Die Konjugationsklassen von  $\mathcal{S}_4$  sind repräsentiert durch id, (1, 2), (1, 2, 3), (1, 2, 3, 4), (1, 2)(3, 4). Beachte in bezug auf die Erzeuger aus Aufgabe 17.(3), daß

$$\begin{aligned}
 (1, 2, 3) &= (1, 2) \circ (1, 2, 3, 4) \circ (1, 2) \circ (1, 2, 3, 4)^{-1} \\
 (1, 2)(3, 4) &= (1, 2) \circ (1, 2, 3, 4)^2 \circ (1, 2) \circ (1, 2, 3, 4)^2 .
 \end{aligned}$$

Der Wedderburnisomorphismus aus Aufgabe 17.(3) bildet wie folgt ab.

$$\begin{array}{lcl}
 \mathbf{CS}_4 & \longrightarrow & \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{3 \times 3} \times \mathbf{C}^{3 \times 3} \times \mathbf{C}^{2 \times 2} \\
 \text{id} & \longmapsto & (1, 1, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) \\
 (1, 2) & \longmapsto & (1, -1, \begin{pmatrix} -11 & -24 & 2 \\ 5 & 11 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -5 & 24 \\ -1 & 5 \end{pmatrix}) \\
 (1, 2, 3) & \longmapsto & (1, 1, \begin{pmatrix} -17 & -39 & -2 \\ 7 & 16 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -5 & 21 \\ -1 & 4 \end{pmatrix}) \\
 (1, 2, 3, 4) & \longmapsto & (1, -1, \begin{pmatrix} 26 & 57 & 2 \\ -11 & -24 & -1 \\ -4 & -8 & -1 \end{pmatrix}, \begin{pmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ -4 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & -15 \\ 1 & -4 \end{pmatrix}) \\
 (1, 2)(3, 4) & \longmapsto & (1, 1, \begin{pmatrix} -5 & -8 & -2 \\ 2 & 3 & 1 \\ 4 & 8 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ -2 & -1 & 1 \\ -4 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})
 \end{array}$$

Die Spur liefert die Charaktertafel

$$X = X(\mathcal{S}_3) = \begin{array}{c} \begin{matrix} \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \\ \chi_5 \end{matrix} \begin{bmatrix} 1 & (1, 2) & (1, 2, 3) & (1, 2, 3, 4) & (1, 2)(3, 4) \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 3 & -1 & 0 & 1 & -1 \\ 3 & 1 & 0 & -1 & -1 \\ 2 & 0 & -1 & 0 & 2 \end{bmatrix} \end{array}$$

Magma liefert mit

```
CharacterTable(SymmetricGroup(4));
```

die Charaktertafel

Class	1	2	3	4	5
Size	1	3	6	8	6
Order	1	2	2	3	4
-----					
p = 2	1	1	1	4	2
p = 3	1	2	3	1	5
-----					
X.1	+	1	1	1	1
X.2	+	1	1	-1	-1
X.3	+	2	2	0	-1
X.4	+	3	-1	-1	0
X.5	+	3	-1	1	-1

die wir als bis auf Permutation mit der unsrigen übereinstimmend erkennen.

- (4) Die Einteilung von  $\mathcal{D}_{10}$  in Konjugationsklassen ist, in den Bezeichnungen von Aufgabe 17.(4),

$$\mathcal{D}_{10} = \{1\} \sqcup \{a, a^4\} \sqcup \{a^2, a^3\} \sqcup \{b, ba, ba^2, ba^3, ba^4\}.$$

Als Repräsentanten der Konjugationsklassen wählen wir  $1, a, a^2, b$ .

Sei weiterhin  $\vartheta \in \mathbf{C}$  mit  $\vartheta^2 + 5\vartheta + 5 = 0$ .

Der Wedderburnisomorphismus aus Aufgabe 17.(4) bildet wie folgt ab.

$$\begin{array}{lcl}
 \mathbf{CD}_{10} & \longrightarrow & \mathbf{C} \times \mathbf{C} \times \mathbf{C}^{2 \times 2} \times \mathbf{C}^{2 \times 2} \\
 1 & \longmapsto & (1, 1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) \\
 a & \longmapsto & (1, 1, \begin{pmatrix} 1 & 1 \\ \vartheta & \vartheta+1 \end{pmatrix}, \begin{pmatrix} -1 & -5 \\ -\vartheta-5 & -\vartheta-4 \end{pmatrix}) \\
 a^2 & \longmapsto & (1, 1, \begin{pmatrix} \vartheta+1 & \vartheta+2 \\ -3\vartheta-5 & -2\vartheta-4 \end{pmatrix}, \begin{pmatrix} -\vartheta-4 & -\vartheta-3 \\ 3\vartheta+10 & 2\vartheta+6 \end{pmatrix}) \\
 b & \longmapsto & (1, -1, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix})
 \end{array}$$

Die Spur liefert die Charaktertafel

$$X = X(\mathcal{S}_3) = \begin{array}{c} \\ \chi_1 \\ \chi_2 \\ \chi_3 \\ \chi_4 \end{array} \begin{array}{cccc} 1 & a & a^2 & b \\ \left[ \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 2 & \vartheta + 2 & -\vartheta - 3 & 0 \\ 2 & -\vartheta - 3 & \vartheta + 2 & 0 \end{array} \right] \end{array}$$

Es sind  $\chi_3$  und  $\chi_4$  konjugiert im Sinne von Aufgabe 23.(3).

Magma liefert mit

```
D := sub<SymmetricGroup(5) | (1,2,3,4,5), (2,5)(3,4)>;
CharacterTable(D);
```

die Charaktertafel

```
Class | 1 2 3 4
Size | 1 5 2 2
Order | 1 2 5 5
-----
p = 2 1 1 4 3
p = 5 1 2 1 1
-----
X.1 + 1 1 1 1
X.2 + 1 -1 1 1
X.3 + 2 0 Z1 Z1#2
X.4 + 2 0 Z1#2 Z1
```

Explanation of Character Value Symbols

# denotes algebraic conjugation, that is,  
#k indicates replacing the root of unity w by w<sup>k</sup>

```
Z1 = (CyclotomicField(5: Sparse := true)) ! [ RationalField() | -1, 0, -1, -1 ]
```

Sei  $\zeta = \zeta_5 = \exp(2\pi i/5)$ .

Um hier die Übereinstimmung bis auf Permutation mit unserer Charatertafel zu sehen, müssen wir nachweisen, daß  $(-1 - \zeta^2 - \zeta^3) - 2$  eine Nullstelle von  $X^2 + 5X + 5$  ist, denn selbige erhalten wir auch mittels  $-(-1 - \zeta^4 - \zeta^6) - 3 = -\zeta^2 - \zeta^3 - 3$ .

Magma liefert mit

```
P<X> := PolynomialRing(Rationals());
K<zeta> := ext<Rationals() | X^4 + X^3 + X^2 + X^1 + X^0>;
(- 3 - zeta^2 - zeta^3)^2 + 5*(- 3 - zeta^2 - zeta^3) + 5;
```

in der Tat das Resultat 0.

## Aufgabe 25

Sei  $M$  ein endlichdimensionaler  $CG$ -Modul. Wir *behaupten*, daß  $M$  eine direkte Summe einfacher Teilmoduln ist. Zum Beweis machen wir eine Induktion über  $\dim M$ . Im Falle  $\dim M = 0$  ist nichts zu zeigen.

Sei  $\dim M \geq 1$ . Sei  $0 \neq N \subseteq M$  ein Teilmodul minimaler Dimension. Es ist  $N$  einfach. Da  $\mathbf{C}G$  halbeinfach ist, gibt es einen Teilmodul  $X \subseteq M$  mit  $M = N \oplus X$ ; cf. Definition 20.(4), Lemma 27. Nach Induktionsvoraussetzung ist  $X$  direkte Summe einfacher Teilmoduln. Also ist auch  $M$  direkte Summe einfacher Teilmoduln. Dies zeigt die *Behauptung*.

Die Behauptung impliziert nun mit Bemerkung 35, daß die Charaktere von  $G$  gerade die Abbildungen der Form  $G \rightarrow \mathbf{C}, g \mapsto \text{tr}(\ell_M(g))$ , wobei  $M$  ein endlichdimensionaler  $\mathbf{C}G$ -Modul ist, sind; cf. Definition 28.

Schicken wir ferner voraus, daß der Gruppenmorphismus  $\varphi : H \rightarrow G$  den Ringmorphismus

$$\begin{array}{ccc} \mathbf{C}H & \xrightarrow{\hat{\varphi}} & \mathbf{C}G \\ \sum_h z_h h & \mapsto & \sum_h z_h \varphi(h) \end{array}$$

induziert; cf. Aufgabe 16.(2).

- (1) Sei  $M$  ein endlichdimensionaler  $\mathbf{C}G$ -Modul so, daß  $\text{tr} \ell_M(g) = \chi(g)$  für  $g \in G$ , namentlich die direkte Summe der zu den irreduziblen Bestandteilen von  $\chi$  gehörenden einfachen Moduln.

Sei  $M|_\varphi$  als  $\mathbf{C}$ -Vektorraum durch  $M$  gegeben, und mit der Multiplikation

$$\left( \sum_{h \in H} z_h h \right) \cdot m := \hat{\varphi} \left( \sum_{h \in H} z_h h \right) m = \left( \sum_{h \in H} z_h \varphi(h) \right) m$$

ausgestattet, wobei  $z_h \in \mathbf{C}$  für  $h \in H$  und wobei  $m \in M$ .

Dies definiert einen  $\mathbf{C}H$ -Modul  $M|_\varphi$ , wie wir kurz verifizieren wollen. Denn es ist  $(M|_\varphi, +)$  eine abelsche Gruppe. Es operiert  $1_{\mathbf{C}H}$  trivial. Distributivität und Assoziativität vererben sich von  $M$  nach  $M|_\varphi$  unter Verwendung dessen, daß  $\hat{\varphi}$  ein Ringmorphismus ist, denn für  $\xi, \tilde{\xi} \in \mathbf{C}H$  und  $m, \tilde{m} \in M$  wird

$$\begin{aligned} (\xi + \tilde{\xi}) \cdot (m + \tilde{m}) &= \hat{\varphi}(\xi + \tilde{\xi}) \cdot (m + \tilde{m}) \\ &= (\hat{\varphi}(\xi) + \hat{\varphi}(\tilde{\xi})) (m + \tilde{m}) \\ &= \hat{\varphi}(\xi)m + \hat{\varphi}(\xi)\tilde{m} + \hat{\varphi}(\tilde{\xi})m + \hat{\varphi}(\tilde{\xi})\tilde{m} \\ &= \xi \cdot m + \xi \cdot \tilde{m} + \tilde{\xi} \cdot m + \tilde{\xi} \cdot \tilde{m} \end{aligned}$$

und

$$\begin{aligned} \xi \cdot (\tilde{\xi} \cdot m) &= \hat{\varphi}(\xi)(\hat{\varphi}(\tilde{\xi})m) \\ &= (\hat{\varphi}(\xi)\hat{\varphi}(\tilde{\xi}))m \\ &= \hat{\varphi}(\xi\tilde{\xi})m \\ &= (\xi\tilde{\xi}) \cdot m. \end{aligned}$$

Man kann für einen Ring  $R$  allgemein einen  $R$ -Modul definieren als eine abelsche Gruppe  $M$ , zusammen mit einem Ringmorphismus  $R \rightarrow \text{End}_R M$ . Geht man so vor, so kann man hier damit argumentieren, daß das Kompositum eines gegebenen (moduldefinierenden) Ringmorphismus mit dem Ringmorphismus  $\hat{\varphi}$  wieder ein (moduldefinierender) Ringmorphismus ist.

Es ist  $H \rightarrow \mathbf{C}, h \mapsto \text{tr} \ell_{M|_\varphi}(h) = \text{tr} \ell_M(\varphi(h)) = \chi(\varphi(h))$  der zugehörige Charakter.

- (2) Gemäß der Lösung zu (1) müssen wir zeigen, daß aus  $M$  einfach und  $\varphi$  surjektiv folgt, daß  $M|_\varphi$  einfach ist.

Zunächst folgt aus  $M \neq 0$ , daß  $M|_\varphi \neq 0$ .

Sei nun  $N$  ein  $\mathbf{C}H$ -Teilmodul von  $M|_\varphi$ . Es ist mit  $\varphi : H \rightarrow G$  auch  $\hat{\varphi} : \mathbf{C}H \rightarrow \mathbf{C}G$  surjektiv. Es genügt zu zeigen, daß  $N$  ein  $\mathbf{C}G$ -Teilmodul von  $M$  ist, denn dann folgt mit der Einfachheit des  $\mathbf{C}G$ -Moduls  $M$ , daß  $N \in \{0, M\}$ .

Es ist  $0 \in N$ .

Seien  $n, \tilde{n} \in N$ . Seien  $\eta, \tilde{\eta} \in \mathbf{C}G$ . Es gibt  $\xi, \tilde{\xi} \in \mathbf{C}H$  mit  $\hat{\varphi}(\xi) = \eta$  und  $\hat{\varphi}(\tilde{\xi}) = \tilde{\eta}$ . Also wird

$$\eta n + \tilde{\eta} \tilde{n} = \hat{\varphi}(\xi)n + \hat{\varphi}(\tilde{\xi})\tilde{n} = \xi \cdot n + \tilde{\xi} \cdot \tilde{n} \in N.$$

- (3) Wir schreiben Charaktere als Zeilenvektoren, in der Form, in der sie auch in der Charaktertafel in der Lösung von Aufgabe 24 auftauchen.

Der obere Index zeige lediglich die Gruppe an.

Wir haben auf die ersten drei Spalten einzuschränken. Es wird

$$\begin{aligned}\chi_1^{\mathcal{S}_4}|_{\mathcal{S}_3} &= (1\ 1\ 1) = \chi_1^{\mathcal{S}_3} \\ \chi_2^{\mathcal{S}_4}|_{\mathcal{S}_3} &= (1\ -1\ 1) = \chi_2^{\mathcal{S}_3} \\ \chi_3^{\mathcal{S}_4}|_{\mathcal{S}_3} &= (3\ -1\ 0) = \chi_2^{\mathcal{S}_3} + \chi_3^{\mathcal{S}_3} \\ \chi_4^{\mathcal{S}_4}|_{\mathcal{S}_3} &= (3\ 1\ 0) = \chi_1^{\mathcal{S}_3} + \chi_3^{\mathcal{S}_3} \\ \chi_5^{\mathcal{S}_4}|_{\mathcal{S}_3} &= (2\ 0\ -1) = \chi_3^{\mathcal{S}_3} .\end{aligned}$$

- (4) Gemäß Lösung zur Aufgabe 17.(3) genügt es mit  $\sigma_1 := (1, 2)$ ,  $\sigma_2 := (2, 3)$  und  $\sigma_3 := (3, 4)$  zu zeigen, daß

$$\begin{aligned}\varphi(\sigma_1)^2 &\stackrel{!}{=} \text{id} \\ \varphi(\sigma_2)^2 &\stackrel{!}{=} \text{id} \\ \varphi(\sigma_3)^2 &\stackrel{!}{=} \text{id} \\ \varphi(\sigma_1 \circ \sigma_2)^3 &\stackrel{!}{=} \text{id} \\ \varphi(\sigma_2 \circ \sigma_3)^3 &\stackrel{!}{=} \text{id} \\ \varphi(\sigma_1 \circ \sigma_3)^2 &\stackrel{!}{=} \text{id}\end{aligned}$$

Eine Rechnung in  $\mathcal{S}_3$  zeigt, daß dies in der Tat zutrifft.

Es ist  $\varphi$  surjektiv, da bereits  $\mathcal{S}_3 = \langle (1, 2), (2, 3) \rangle = \langle \varphi((1, 2)), \varphi((2, 3)) \rangle = \varphi(\langle (1, 2), (2, 3) \rangle)$  ist.

Es ist

$$\begin{aligned}\varphi(\text{id}) &= \text{id} \\ \varphi((1, 2)) &= (1, 2) \\ \varphi((1, 2, 3)) &= (1, 2, 3) \\ \varphi((1, 2, 3, 4)) &= (1, 3) \\ \varphi((1, 2)(3, 4)) &= \text{id}\end{aligned}$$

Dementsprechend wird

$$\begin{aligned}\chi_1^{\mathcal{S}_3}|_{\varphi} &= (1\ 1\ 1\ 1\ 1) = \chi_1^{\mathcal{S}_4} \\ \chi_2^{\mathcal{S}_3}|_{\varphi} &= (1\ -1\ 1\ -1\ 1) = \chi_2^{\mathcal{S}_4} \\ \chi_3^{\mathcal{S}_3}|_{\varphi} &= (2\ 0\ -1\ 0\ 2) = \chi_5^{\mathcal{S}_4} .\end{aligned}$$

## Aufgabe 26

- (1) Um zu zeigen, daß für  $g \in G$  die Abbildung

$$\begin{array}{ccc} V \otimes_{\mathbf{C}} W & \longrightarrow & V \otimes_{\mathbf{C}} W \\ v \otimes w & \longmapsto & gv \otimes gw \end{array}$$

als  $\mathbf{C}$ -lineare Abbildung wohldefiniert ist, beachten wir, daß

$$\begin{aligned}g(\lambda v + \lambda' v') \otimes gw &= (\lambda gv + \lambda' gv') \otimes gw = \lambda(gv \otimes gw) + \lambda'(gv' \otimes gw) \\ gv \otimes g(\mu w + \mu' w') &= gv \otimes (\mu gw + \mu' gw') = \mu(gv \otimes gw) + \mu'(gv \otimes gw')\end{aligned}$$

für  $v, v' \in V$  und  $w, w' \in W$  und  $\lambda, \lambda', \mu, \mu' \in \mathbf{C}$ .

Dies liefert einen Gruppenmorphismus  $G \longrightarrow \text{U}(\text{End}_{\mathbf{C}}(V \otimes_{\mathbf{C}} W))$ , da

$$g(h(\sum_i v_i \otimes w_i)) = g(\sum_i hv_i \otimes hw_i) = \sum_i ghv_i \otimes ghw_i = (gh)(\sum_i v_i \otimes w_i) ,$$

wobei  $v_i \in V$  und  $w_i \in W$ .

Mit Aufgabe 16.(2) setzt sich dies fort zu einem  $\mathbf{C}$ -Algebrenmorphismus  $\mathbf{C}G \longrightarrow \text{End}_{\mathbf{C}}(V \otimes_{\mathbf{C}} W)$ , was wiederum  $V \otimes_{\mathbf{C}} W$  auf die gewünschte Weise zu einem  $\mathbf{C}G$ -Modul macht.

(2) Sei  $M$  ein endlichdimensionaler  $\mathbf{C}G$ -Modul mit  $\chi(g) = \text{tr } \ell_M(g)$  für  $g \in G$ .

Sei  $N$  ein endlichdimensionaler  $\mathbf{C}G$ -Modul mit  $\psi(g) = \text{tr } \ell_N(g)$  für  $g \in G$ .

Cf. Bemerkung eingangs der Lösung zu Aufgabe 25.

Sei  $g \in G$ .

Sei  $(m_i)_i$  eine  $\mathbf{C}$ -lineare Basis von  $M$ .

Sei  $(\lambda_{i,j})_{i,j}$  die diesbezüglich beschreibende Matrix von  $\ell_M(g)$ .

Sei  $(n_{i'})_{i'}$  eine  $\mathbf{C}$ -lineare Basis von  $N$ .

Sei  $(\mu_{i',j'})_{i',j'}$  die diesbezüglich beschreibende Matrix von  $\ell_N(g)$ .

Es wird

$$g(m_j \otimes n_{j'}) = gm_j \otimes gn_{j'} = \left( \sum_i \lambda_{i,j} m_i \right) \otimes \left( \sum_{i'} \mu_{i',j'} n_{i'} \right) = \sum_{i,i'} \lambda_{i,j} \mu_{i',j'} (m_i \otimes n_{i'}).$$

Also ist die beschreibende Matrix von  $\ell_{M \otimes_{\mathbf{C}} N}(g)$  bezüglich der Basis  $(m_i \otimes n_{i'})_{(i,i')}$  gegeben durch

$$(\lambda_{i,j} \mu_{i',j'})_{(i,i'),(j,j')}.$$

Deren Spur ist gegeben durch

$$\text{tr } \ell_{M \otimes_{\mathbf{C}} N}(g) = \sum_{i,i'} \lambda_{i,i} \mu_{i',i'} = \left( \sum_i \lambda_{i,i} \right) \left( \sum_{i'} \mu_{i',i'} \right) = (\text{tr } \ell_M(g)) (\text{tr } \ell_N(g)) = \chi(g) \cdot \psi(g).$$

Also ist  $\chi \cdot \psi$  der zu  $M \otimes_{\mathbf{C}} N$  gehörige Charakter von  $G$ .

### Aufgabe 27

(1) Es ist

$$\begin{aligned} |\text{id}^{\mathcal{S}_4}| &= 1 \\ |(1,2)^{\mathcal{S}_4}| &= 6 \\ |(1,2,3)^{\mathcal{S}_4}| &= 8 \\ |(1,2,3,4)^{\mathcal{S}_4}| &= 6 \\ |(1,2)(3,4)^{\mathcal{S}_4}| &= 3. \end{aligned}$$

Also wird

$$\begin{aligned} \sum_s \chi_4(g_s) \overline{\chi_4(g_s)} |g_s^{\mathcal{S}_4}| &= 3 \cdot 3 \cdot 1 + 1 \cdot 1 \cdot 6 + 0 \cdot 0 \cdot 8 + (-1) \cdot (-1) \cdot 6 + (-1) \cdot (-1) \cdot 3 = 24 \\ \sum_s \chi_4(g_s) \overline{\chi_5(g_s)} |g_s^{\mathcal{S}_4}| &= 3 \cdot 2 \cdot 1 + 1 \cdot 0 \cdot 6 + 0 \cdot (-1) \cdot 8 + (-1) \cdot 0 \cdot 6 + (-1) \cdot 2 \cdot 3 = 0 \\ \sum_s \chi_5(g_s) \overline{\chi_5(g_s)} |g_s^{\mathcal{S}_4}| &= 2 \cdot 2 \cdot 1 + 0 \cdot 0 \cdot 6 + (-1) \cdot (-1) \cdot 8 + 0 \cdot 0 \cdot 6 + 2 \cdot 2 \cdot 3 = 24 \end{aligned}$$

(2) Es wird  $\chi_4 \cdot \chi_5 = (6 \ 0 \ 0 \ -2) = \chi_3 + \chi_4$ .

(3) Es wird

$$\begin{aligned} \varepsilon_4 &= \frac{n_s}{|G|} \sum_g \chi_s(g^{-1}) g \\ &= \frac{1}{8} (3 \text{id} + (1,2) + (1,3) + (1,4) + (2,3) + (2,4) + (3,4) \\ &\quad - (1,2,3,4) - (1,2,4,3) - (1,3,2,4) - (1,3,4,2) - (1,4,2,3) - (1,4,3,2) \\ &\quad - (1,2)(3,4) - (1,3)(2,4) - (1,4)(2,3)). \end{aligned}$$

Mit Magma kann man wie folgt eine Probe machen, daß  $\varepsilon_4$  in der Tat idempotent ist. Hierzu können wir im Teilring  $\mathbf{QS}_4 \subseteq \mathbf{CS}_4$  rechnen, zur Vermeidung von Dezimalbrüchen.

```
S := SymmetricGroup(4);
R := GroupAlgebra(Rationals(),S);
eps4 := 1/8*(3*R!S!1 + R!S!(1,2) + R!S!(1,3) + R!S!(1,4) + R!S!(2,3) + R!S!(2,4) + R!S!(3,4)
        - R!S!(1,2,3,4) - R!S!(1,2,4,3) - R!S!(1,3,2,4) - R!S!(1,3,4,2) - R!S!(1,4,2,3) - R!S!(1,4,3,2)
        - R!S!(1,2)(3,4) - R!S!(1,3)(2,4) - R!S!(1,4)(2,3));
print eps4^2 - eps4;
```

### Aufgabe 28

Schreibe zunächst

$$\omega'(z^1, \dots, z^t) := \sum_{g \in G} \left( \frac{1}{|G|} \sum_{s \in [1,t]} n_s \operatorname{tr}(\omega^s(g^{-1}) z^s) \right) g \in \mathbf{CG},$$

wobei  $z^s \in \mathbf{C}^{n_s \times n_s}$  für  $s \in [1, t]$ . Wir wollen  $\omega' \stackrel{!}{=} \omega^{-1}$  zeigen. Da wir bereits wissen, daß  $\omega$  ein Isomorphismus ist, genügt es,  $\omega' \circ \omega \stackrel{!}{=} \operatorname{id}_{\mathbf{CG}}$  zu zeigen. Dank  $\mathbf{C}$ -Linearität von  $\omega$  und  $\omega'$  genügt es zu zeigen, daß  $(\omega' \circ \omega)(h) = h$  für  $h \in G$ . In der Tat wird

$$\begin{aligned} (\omega' \circ \omega)(h) &= \sum_{g \in G} \left( \frac{1}{|G|} \sum_{s \in [1,t]} n_s \operatorname{tr}(\omega^s(g^{-1}) \omega^s(h)) \right) g \\ &= \sum_{g \in G} \left( \frac{1}{|G|} \sum_{s \in [1,t]} n_s \operatorname{tr} \omega^s(g^{-1}h) \right) g \\ &= \sum_{g \in G} \left( \frac{1}{|G|} \sum_{s \in [1,t]} n_s \chi_s(g^{-1}h) \right) g \\ &\stackrel{\text{L. 36}}{=} \sum_{g \in G} \partial_{g^{-1}h,1} g \\ &= h. \end{aligned}$$

Natürlich ist das verwandte Lemma 36 ein Spezialfall von Satz 38.(2).

Aufgabe 28 ist die Verallgemeinerung von Lemma 37 von den speziellen Elementen, von denen dort die Urbilder  $\varepsilon_s$  ausgerechnet wurden, zu beliebigen Elementen.

### Aufgabe 29

Sei  $\nu$  der Eigenwert von  $y$ . Es wird

$$\begin{aligned} Ay &\stackrel{1.}{=} \nu y &= \sum_{i \in [1,k]} \nu \mu_i x_i \\ &\stackrel{2.}{=} \sum_{i \in [1,k]} \mu_i Ax_i &= \sum_{i \in [1,k]} \lambda_i \mu_i x_i, \end{aligned}$$

also  $\sum_{i \in [1,k]} (\nu - \lambda_i) \mu_i x_i = 0$ .

Da  $(x_1, \dots, x_k)$  linear unabhängig ist und da  $\mu_i \neq 0$  für  $i \in [1, t]$ , folgt  $\nu = \lambda_i$  für alle  $i \in [1, t]$ .

### Aufgabe 30

// test data

```
p := 3;
n := 4;
V := VectorSpace(GF(p), n);
```

```

M := MatrixRing(GF(p),n);
k := 3;
Mk := CartesianProduct([M : i in [1..k]]); // Mk = M x M x ... x M
A := Mk!<M!DiagonalMatrix([1,0,1,1]),M!DiagonalMatrix([1,1,-1,1]),M!DiagonalMatrix([1,0,1,-1])>;
AA := Mk!<M!DiagonalMatrix([1,0,1,1]),M!DiagonalMatrix([1,1,-1,1]),
      M!Matrix([[1,0,1,-1],[0,-1,0,1],[1,0,0,1],[0,0,1,1]])>;

// function

eigenvector_simult := function(p,n,A)
  k := #A;
  M := MatrixRing(GF(p),n);
  MVN := RMatrixSpace(GF(p),0,n);
  MV := RMatrixSpace(GF(p),1,n);
  V := VectorSpace(GF(p),n);
  eigensp := [V];
  for i in [1..k] do
    eigensp_new := [V]; // to initialise eigensp_new
    Prune(~eigensp_new); // to initialise eigensp_new
    for E in eigensp do
      for ev in Eigenvalues(A[i]) do
        Emeet := E meet Kernel(Transpose(A[i] - ev[1]*M!1));
        if Dimension(Emeet) gt 0 then
          Append(~eigensp_new,Emeet);
        end if;
      end for;
    end for;
    if eigensp_new eq [] then
      break i;
    end if;
  end for;
  eigensp := eigensp_new;
end for;
matrix := MVN!0;
for E in eigensp do
  for x in Basis(E) do
    matrix := VerticalJoin(matrix,MV!x);
  end for;
end for;
return Transpose(matrix);
end function;

// test

print eigenvector_simult(p,n,A);
print eigenvector_simult(p,n,AA);

```

### Aufgabe 31

```

// test data

p := 7;
S := SymmetricGroup(5); // S5

```

```

G := sub< S | (1,2,3,4,5), (2,5)(3,4)>; // D10
GG := sub< S | (1,2,3), (1,2,3,4,5)>; // A5

// function

gamma := function(G,p)
  t := #ConjugacyClasses(G);
  g := [ConjugacyClasses(G)[s][3] : s in [1..t]];
  gG := [{ g[s]^x : x in G } : s in [1..t]];
  M := MatrixRing(GF(p),t);
  Mk := CartesianProduct([M : s in [1..t]]); // Mk = M x M x ... x M
  return Mk!<M!#{x : x in CartesianProduct(gG[r],gG[s]) | x[1]*x[2] eq g[a]} :
    a in [1..t], s in [1..t] : r in [1..t] >, t, g, gG;
end function;

// test

print gamma(S,p);
print gamma(G,p);
print gamma(GG,p);

```

### Aufgabe 32

Halten wir zunächst fest, daß  $\Phi_m(0) \in \{-1, +1\}$  für  $m \geq 1$ , wie aus  $\prod_{d|m} \Phi_d(X) = X^m - 1$  und also  $\prod_{d|m} \Phi_d(0) = -1$  mit Induktion nach  $m \geq 1$  folgt.

Genauer gesagt folgt  $\Phi_m(0) = 1$  für  $m \geq 2$  per Induktion aus  $\prod_{d|m, d \neq 1} \Phi_d(0) = 1$ .

(1) O.E. ist  $n \geq 2$ .

Da  $b \equiv_n 0$ , ist  $\Phi_n(b) \equiv_n \Phi_n(0) \in \{-1, +1\}$ . Also ist  $q$  kein Teiler von  $n$ , da es sonst auch  $-1$  oder  $+1$  teilen würde.

Aus  $\Phi_n(b) \equiv_q 0$  und  $\Phi_n(X) | (X^n - 1)$  folgt, daß  $b^n \equiv_q 1$ .

Sei  $r \geq 1$  maximal mit  $b^n \equiv_{q^r} 1$ . Dies existiert, da zum einen  $b^n \equiv_{q^r} 1$ , und da zum anderen aus  $b \equiv_n 0$  wegen  $n \geq 2$  folgt, daß  $b^n \neq 1$ .

Es ist  $n$  die Ordnung von  $b + q^r \mathbf{Z}$  in  $U(\mathbf{Z}/q^r \mathbf{Z})$ , denn für  $d|n$  mit  $d < n$  ist

$$q | \Phi_n(b) | \frac{b^n - 1}{b^d - 1},$$

und also  $q^r$  kein Teiler von  $b^d - 1$ .

Folglich ist  $n$  ein Teiler von  $|U(\mathbf{Z}/q^r \mathbf{Z})| = q^{r-1}(q-1)$ . Da  $n$  und  $q$  teilerfremd sind, folgt  $n|(q-1)$ , und also  $q \equiv_n 1$ .

Cf. [4, Th. 2.3].

(2) *Angenommen*, die Menge  $\{p \in \mathbf{Z}_{>0} : p \text{ prim}, p \equiv_n 1\}$  ist endlich. Sei  $P$  das Produkt ihrer Elemente (also  $P = 1$ , falls keine vorhanden). Da  $\Phi_n(X)$  ein normiertes Polynom von Grad  $\geq 1$  ist, gibt es ein  $x \in \mathbf{Z}_{\geq 0}$  mit  $\Phi_n(xPn) > 1$ . Sei  $q$  ein Primteiler von  $\Phi_n(xPn)$ . Es ist  $\Phi_n(xPn) \equiv_P \Phi_n(0) \in \{-1, +1\}$ . Also ist  $q$  kein Teiler von  $P$ , da es sonst auch  $+1$  oder  $-1$  teilen würde. Aber mit (1) ist  $q \equiv_n 1$ . Wir haben einen *Widerspruch*, da alle solchen Primzahlen Teiler von  $P$  sind.

Eine (nicht besonders gute) obere Schranke für die jeweils nächste Primzahl  $p$  mit  $p \equiv_n 1$  kann aus diesen Argumenten auch gewonnen werden, wenn man sich noch ein  $t_0$  mit  $\Phi_n(t) > 1$  für  $t > t_0$  beschafft.

Nach dem Satz von Dirichlet ist allgemeiner für  $m \in [1, n - 1]$  mit  $\text{ggT}(m, n) = 1$  die Menge  $\{p \in \mathbf{Z}_{>0} : p \text{ prim, } p \equiv_n m\}$  unendlich. Dies zeigt man mit Mitteln der Funktionentheorie.

### Aufgabe 33

```
// test data

S := SymmetricGroup(5);           // S5
G := sub< S | (1,2,3,4,5), (2,5)(3,4)>; // D10
GG := sub< S | (1,2,3), (1,2,3,4,5)>; // A5

// function

theta_p := function(G)
  e := Exponent(G);
  p := Order(G) + 1; // initialise
  while not IsPrime(p) do
    p += e;
  end while;
  for x in [1..p-1] do
    if Order(GF(p)!x) eq e then
      bzeta := GF(p)!x;
      break x;
    end if;
  end for;
  R := ext<Integers() | CyclotomicPolynomial(e)>;
  if e ge 3 then
    zeta := R.2;
  elif e eq 2 then
    zeta := R!-1;
  else
    zeta := R!1;
  end if;
  th := hom< R -> GF(p) | bzeta > ;
  return R, th, p, e, zeta;
end function;

// test

R, th, p, e, zeta := theta_p(G);
print R, th, p, e, zeta;
R, th, p, e, zeta := theta_p(GG);
print R, th, p, e, zeta;
R, th, p, e, zeta := theta_p(S);
print R, th, p, e, zeta;
```

### Aufgabe 34

- (1) Wir kennen die Funktionen `gamma` von Aufgabe 31, `eigenvector_simult` von Aufgabe 30, und `theta_p` von Aufgabe 33.

Dazuhin schreiben wir folgende Funktion, die zu jedem Index  $s$  in  $[1, t]$  und jedem  $i \in \mathbf{Z}$  den Index der  $i$ -ten Potenz des Konjugationsklassenrepräsentanten  $g_s$  ausgibt.

```
power_index := function(s,i,g,gG)
  for r in [1..#g] do
    if g[s]^i in gG[r] then
      return r;
      break r;
    end if;
  end for;
end function;
```

Nun zum eigentlichen Dixon-Algorithmus. Wir merken dabei die Schritte aus Algorithmus 51 in der dortigen Zählung an.

```
// test data

S := SymmetricGroup(5);           // S5
G := sub< S | (1,2,3,4,5), (2,5)(3,4)>; // D10
GG := sub< S | (1,2,3), (1,2,3,4,5)>; // A5

// function

Dixon := function(G);
  // (1)
  R, th, p, e, zeta := theta_p(G);
  bar_zeta := th(zeta);
  K<zeta> := NumberField(R);
  // (2), takes time
  A,t,g,gG := gamma(G,p);
  // (3)
  beta := Transpose(eigenvector_simult(p,t,A));
  // (4)
  n := [Integers()!(Sqrt(Integers()!(
    (GF(p)!(#G)) / &+[
      beta[r][s] * beta[r][power_index(s,-1,g,gG)] / GF(p)!(#G[s])
    : s in [1..t]]
  ))) : r in [1..t]];
  // (5)
  theta_chi := MatrixRing(GF(p),t)!
  [beta[r][s] * GF(p)!(n[r]) / GF(p)!(#G[s]) : s in [1..t], r in [1..t]];
  // (7) (step (6) done with power_index;)
  // MatrixRing(K,t)-entries look better than MatrixRing(R,t)-entries
  chi := MatrixRing(K,t)![
    &+[Integers()!(
      &+[bar_zeta^(-i*1) * theta_chi[r][power_index(s,i,g,gG)] : i in [0..e-1]]
    /(GF(p)!e) * zeta^1 : 1 in [0..e-1]]
  : s in [1..t], r in [1..t]];
  // swap trivial character to top
  for r in [1..t] do
    if &and[chi[r][s] eq K!1 : s in [1..t]] then
      SwapRows(~chi,r,1);
      break r;
    end if;
  end for;
```

```

    end if;
  end for;
  return MatrixRing(K,t)!chi,e,"\n",g;
end function;

// test

Dixon(G);
Dixon(GG);
Dixon(S);

```

(2) (2.1) Zu  $C_3$ . Unser Programm

```

C3 := sub<SymmetricGroup(3)|(1,2,3)>;
Dixon(C3);

gibt

[      1      1      1]
[      1 -zeta - 1      zeta]
[      1      zeta -zeta - 1]
3
[
  Id(C3P),
  (1, 2, 3),
  (1, 3, 2)
]

```

Dies stimmt mit dem Resultat von `CharacterTable` überein; cf. Aufgabe 24.(1).

(2.2) Zu  $S_3$ . Unser Programm

```

Dixon(SymmetricGroup(3));

gibt

[ 1  1  1]
[ 1 -1  1]
[ 2  0 -1]
6
[
  Id($),
  (1, 2),
  (1, 2, 3)
]

```

Dies stimmt mit dem Resultat von `CharacterTable` überein; cf. Aufgabe 24.(2).

(2.3) Zu  $S_4$ . Unser Programm

```

Dixon(SymmetricGroup(4));

gibt

```

```
[ 1  1  1  1  1]
[ 3 -1 -1  0  1]
[ 2  2  0 -1  0]
[ 3 -1  1  0 -1]
[ 1  1 -1  1 -1]
```

12

```
[
  Id($),
  (1, 2)(3, 4),
  (1, 2),
  (1, 2, 3),
  (1, 2, 3, 4)
]
```

Dies stimmt mit dem Resultat von `CharacterTable` bis auf Permutation der Zeilen überein; cf. Aufgabe 24.(3).

(2.4) Zu  $\mathcal{D}_{10}$ . Unser Programm

```
D10 := sub<SymmetricGroup(5) | (1,2,3,4,5), (2,5)(3,4)>;
Dixon(D10);
```

gibt

```
[          1          1          1          1]
[          2          0 zeta^3 - zeta^2 - 1  -zeta^3 + zeta^2]
[          2          0  -zeta^3 + zeta^2 zeta^3 - zeta^2 - 1]
[          1          -1          1          1]
```

10

```
[
  Id(D10),
  (2, 5)(3, 4),
  (1, 2, 3, 4, 5),
  (1, 3, 5, 2, 4)
]
```

Dies stimmt mit dem Resultat von `CharacterTable` bis auf Permutation der Zeilen überein; cf. Aufgabe 24.(4), da  $\zeta_{10} = -\zeta_5^3$  ist und sich so

$$\zeta_{10}^3 - \zeta_{10}^2 - 1 = -\zeta_5^3 - \zeta_5^2 - 1$$

und

$$-\zeta_{10}^3 + \zeta_{10}^2 = \zeta_5^3 + \zeta_5^2 = -\zeta_5 + (\zeta_5^3 + \zeta_5^2 + \zeta_5^1 + \zeta_5^0) - 1 = -\zeta_5^6 - \zeta_5^4 - 1$$

ergibt.

(3) (3.1) Zu  $\mathcal{S}_6$ . Unser Programm

```
Dixon(SymmetricGroup(6));
```

gibt

```
[ 1  1  1  1  1  1  1  1  1  1  1]
[ 5 -1  3  1 -1  2 -1  1  0 -1  0]
[ 5 -3  1  1  2 -1 -1 -1  0  0  1]
[ 1 -1 -1  1  1  1  1 -1  1 -1 -1]
```

```
[16 0 0 0 -2 -2 0 0 1 0 0]
[ 9 3 3 1 0 0 1 -1 -1 0 0]
[10 2 -2 -2 1 1 0 0 0 -1 1]
[ 5 1 -3 1 -1 2 -1 -1 0 1 0]
[ 5 3 -1 1 2 -1 -1 1 0 0 -1]
[ 9 -3 -3 1 0 0 1 1 -1 0 0]
[10 -2 2 -2 1 1 0 0 0 1 -1]
```

60

```
[
  Id($),
  (1, 2)(3, 4)(5, 6),
  (1, 2),
  (1, 2)(3, 4),
  (1, 2, 3)(4, 5, 6),
  (1, 2, 3),
  (1, 2, 3, 4)(5, 6),
  (1, 2, 3, 4),
  (1, 2, 3, 4, 5),
  (1, 2, 3, 4, 5, 6),
  (1, 2, 3)(4, 5)
]
```

Dagegen gibt `CharacterTable`, bereits nach Umsortieren der Zeilen:

Class		1	2	3	4	5	6	7	8	9	10	11
Size		1	15	15	45	40	40	90	90	144	120	120
Order		1	2	2	2	3	3	4	4	5	6	6
-----												
X.1	+	1	1	1	1	1	1	1	1	1	1	1
X.4	+	5	-1	3	1	-1	2	-1	1	0	-1	0
X.3	+	5	-3	1	1	2	-1	-1	-1	0	0	1
X.2	+	1	-1	-1	1	1	1	1	-1	1	-1	-1
X.11	+	16	0	0	0	-2	-2	0	0	1	0	0
X.7	+	9	3	3	1	0	0	1	-1	-1	0	0
X.10	+	10	2	-2	-2	1	1	0	0	0	-1	1
X.6	+	5	1	-3	1	-1	2	-1	-1	0	1	0
X.5	+	5	3	-1	1	2	-1	-1	1	0	0	-1
X.8	+	9	-3	-3	1	0	0	1	1	-1	0	0
X.9	+	10	-2	2	-2	1	1	0	0	0	1	-1

Das ist dasselbe, wenn wir noch beachten, daß Magma seine eigene Reihenfolge der Konjugationsklassen auch für seine Charaktertafel verwendet.

(3.1) Zu  $\mathcal{A}_6$ . Unser Programm

```
Dixon(AlternatingGroup(6));
```

gibt

```
[1 1 1 1 1 1 1]
[8 0 -1 -1 0 -zeta^14 + zeta^6 + zeta^4 zeta^14 - zeta^6 - zeta^4 + 1]
[9 1 0 0 1 -1 -1]
[8 0 -1 -1 0 zeta^14 - zeta^6 - zeta^4 + 1 -zeta^14 + zeta^6 + zeta^4]
[10 -2 1 1 0 0 0]
```

```
[5 1 -1 2 -1 0 0]
[5 1 2 -1 -1 0 0]
60
[
  Id($),
  (1, 2)(3, 4),
  (1, 2, 3)(4, 5, 6),
  (1, 2, 3),
  (1, 2, 3, 4)(5, 6),
  (1, 2, 3, 4, 5),
  (1, 3, 4, 5, 2)
]
```

Dagegen gibt `CharacterTable`, bereits nach Umsortieren der Zeilen:

Class		1	2	3	4	5	6	7
Size		1	45	40	40	90	72	72
Order		1	2	3	3	4	5	5
-----								
X.1	+	1	1	1	1	1	1	1
X.4	+	8	0	-1	-1	0	Z1	Z1#2
X.6	+	9	1	0	0	1	-1	-1
X.5	+	8	0	-1	-1	0	Z1#2	Z1
X.7	+	10	-2	1	1	0	0	0
X.3	+	5	1	-1	2	-1	0	0
X.2	+	5	1	2	-1	-1	0	0

#### Explanation of Character Value Symbols

-----

# denotes algebraic conjugation, that is,  
 #k indicates replacing the root of unity w by w<sup>k</sup>

Z1 = (CyclotomicField(5: Sparse := true)) ! [ RationalField() | 0, 0, -1, -1 ]

Es ist  $\zeta_{60}^2 = \zeta_{30}$ , und also

$$\begin{aligned} -\zeta_{60}^{14} + \zeta_{60}^6 + \zeta_{60}^4 &= -\zeta_{30}^7 + \zeta_{30}^3 + \zeta_{30}^2 \\ \zeta_{60}^{14} - \zeta_{60}^6 - \zeta_{60}^4 + 1 &= \zeta_{30}^7 - \zeta_{30}^3 - \zeta_{30}^2 + 1. \end{aligned}$$

Wir haben das Kreisteilungspolynom  $\Phi_{30}(X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1$ , wie Magma via `CyclotomicPolynomial(30)` liefert, können also reduzieren zu

$$\begin{aligned} -\zeta_5^2 - \zeta_5^3 &= -\zeta_{30}^{12} - \zeta_{30}^{18} = -\zeta_{30}^7 + \zeta_{30}^3 + \zeta_{30}^2 \\ -\zeta_5^4 - \zeta_5^6 &= -\zeta_{30}^{24} - \zeta_{30}^6 = \zeta_{30}^7 - \zeta_{30}^3 - \zeta_{30}^2 + 1, \end{aligned}$$

wie Magma via

```
R<zeta> := ext<Rationals()|CyclotomicPolynomial(30)>;
- zeta^12 - zeta^18;
- zeta^24 - zeta^6;
```

liefert.

Also stimmen die beiden resultierenden Charaktertafeln überein, wenn wir noch beachten, daß Magma seine eigene Reihenfolge der Konjugationsklassen auch für seine Charaktertafel verwendet.

**Aufgabe 35**

- (1) Sei  $M'' = {}_R\langle m''_1, \dots, m''_t \rangle$  für ein  $t \geq 0$  und für  $m''_i \in M''$  für  $i \in [1, t]$ . Wähle  $m_i \in M$  mit  $p(m_i) = m''_i$  für  $i \in [1, t]$ . Sei  $\text{Kern } p = {}_R\langle m'_1, \dots, m'_s \rangle$  für ein  $s \geq 0$ . Wir behaupten, daß

$$M \stackrel{!}{=} {}_R\langle m'_1, \dots, m'_s, m_1, \dots, m_t \rangle.$$

Sei  $m \in M$  gegeben. Schreibe  $p(m) = w_1 m''_1 + \dots + w_t m''_t$  für gewisse  $w_i \in R$ . Es ist  $p(m - (w_1 m_1 + \dots + w_t m_t)) = 0$ . Also ist  $m - (w_1 m_1 + \dots + w_t m_t) \in \text{Kern } p$ , und wir können  $m - (w_1 m_1 + \dots + w_t m_t) = z_1 m'_1 + \dots + z_s m'_s$  schreiben für gewisse  $z_i \in R$ . Insgesamt wird

$$m = (w_1 m_1 + \dots + w_t m_t) + (z_1 m'_1 + \dots + z_s m'_s).$$

Dies zeigt die *Behauptung*.

- (2) Schreibe  $N = {}_R\langle n_1, \dots, n_\ell \rangle$  mit  $\ell \geq 0$  und mit  $n_i \in N$  für  $i \in [1, \ell]$ .

Wir haben eine surjektive  $R$ -lineare Abbildung

$$\begin{array}{ccc} R^{\oplus \ell} & \xrightarrow{f} & N \\ (r_i)_i & \longmapsto & \sum_{i \in [1, \ell]} r_i n_i \end{array}$$

Also haben wir auch eine surjektive  $R$ -lineare Abbildung

$$f|_{f^{-1}(M)}^M : f^{-1}(M) \longrightarrow M.$$

Können wir zeigen, daß der Teilmodul  $f^{-1}(M)$  von  $R^{\oplus \ell}$  endlich erzeugt ist, so gilt dies auch für  $M$ , da wir die Bilder der gefundenen Erzeuger von  $f^{-1}(M)$  unter  $f$  als Erzeuger von  $M$  verwenden können.

Somit ist o.E.  $M \subseteq R^{\oplus \ell} = N$ .

Wir führen eine Induktion nach  $\ell \geq 0$ . Für  $\ell = 0$  ist nichts zu zeigen. Sei also  $\ell \geq 1$  und die Aussage für  $\ell - 1$  bekannt.

Sei  $R^{\oplus \ell} \xrightarrow{p} R^{\oplus (\ell-1)}$ ,  $(r_1, r_2, \dots, r_\ell) \longmapsto (r_2, \dots, r_\ell)$ . Es ist  $p$  eine  $R$ -lineare Abbildung. Sei  $M'' := \text{Im}(p|_M) \subseteq R^{\oplus (\ell-1)}$ . Als Teilmodul von  $R^{\oplus (\ell-1)}$  ist  $M''$  nach Induktionsvoraussetzung endlich erzeugt. Wir haben eine surjektive  $R$ -lineare Abbildung  $p|_M^{M''} : M \longrightarrow M''$ .

Wir haben die injektive  $R$ -lineare Abbildung

$$\begin{array}{ccc} \text{Kern}(p|_M^{M''}) = \{(r_1, \dots, r_\ell) \in R^{\oplus \ell} : (r_2, \dots, r_\ell) \in M, r_1 = 0 \text{ für } i \in [2, \ell]\} & \longrightarrow & R \\ (r_1, \dots, r_\ell) & \longmapsto & r_1 \end{array}$$

Ihr Bild ist wegen  $R$  Hauptidealbereich von einem Element und also endlich erzeugt. Somit ist auch  $\text{Kern}(p|_M^{M''})$  als zu diesem Bild isomorpher  $R$ -Modul endlich erzeugt.

Somit sind die in (1) gemachten Voraussetzungen an  $M''$  und  $\text{Kern}(p|_M^{M''})$  erfüllt, und wir können schließen, daß  $M$  endlich erzeugt ist.

**Aufgabe 36**

*Vorbemerkung.* Sei  $R$  ein Integritätsbereich. Gebe es eine Abbildung  $f : R \setminus \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$  so, daß es für  $r, s \in R \setminus \{0\}$  ein  $q \in R$  und ein  $p \in R$  mit  $r = sq + p$  und ( $p = 0$  oder  $f(p) \in [0, f(s) - 1]$ ) gibt.

*Behauptung.* Es ist  $R$  ein Hauptidealbereich.

Sei  $\mathfrak{a} \subseteq R$  ein Ideal. Wir haben zu zeigen, daß es ein  $a \in R$  gibt mit  $\mathfrak{a} = \langle a \rangle$ . Sei o.E.  $\mathfrak{a} \neq \{0\}$ . Sei  $a \in \mathfrak{a} \setminus \{0\}$  mit  $f(a)$  minimal. Wir wollen  $\mathfrak{a} \stackrel{!}{=} \langle a \rangle$  zeigen. Zu zeigen ist  $\stackrel{!}{\subseteq}$ . Sei  $b \in \mathfrak{a}$ . Wir wollen  $b \stackrel{!}{\in} \langle a \rangle$  zeigen. O.E. ist  $b \neq 0$ . Schreibe  $b = aq + p$  mit  $q \in R$  und ( $p = 0$  oder  $f(p) \in [0, f(a) - 1]$ ). Es ist  $p = b - aq \in \mathfrak{a}$ . Wäre  $p \neq 0$ , so wäre  $f(p) < f(a)$ , im Widerspruch zur Minimalität von  $f(a)$ . Also ist  $p = 0$  und also  $b = aq \in \langle a \rangle$ . Dies zeigt die *Behauptung*.

- (1) Sei  $g : \mathbf{Q}(i) \rightarrow \mathbf{Q}_{\geq 0}$ ,  $x + yi \mapsto |x + yi|^2 = x^2 + y^2$ , wobei  $x, y \in \mathbf{Q}$ . Wir müssen zeigen, daß  $f := g|_{\mathbf{Z}[i] \setminus \{0\}}$  die in der Vorbemerkung geforderte Eigenschaft hat. Beachte, daß  $g(z \cdot w) = g(z) \cdot g(w)$  für  $z, w \in \mathbf{Q}(i)$ .

Seien  $r = a + bi$ ,  $s = c + di \in \mathbf{Z}[i] \setminus \{0\}$  gegeben, wobei  $a, b, c, d \in \mathbf{Z}$ . In  $\mathbf{Q}(i)$  sei

$$\frac{a + bi}{c + di} =: u + vi$$

mit  $u = (ac + bd)/(c^2 + d^2)$  und  $v = (bc - ad)/(c^2 + d^2)$  aus  $\mathbf{Q}$ .

Seien  $u_0 \in \mathbf{Z}$  und  $u_1 \in \mathbf{Q}$  mit  $u = u_0 + u_1$  und  $|u_1| \leq 1/2$ .

Seien  $v_0 \in \mathbf{Z}$  und  $v_1 \in \mathbf{Q}$  mit  $v = v_0 + v_1$  und  $|v_1| \leq 1/2$ .

Können wir zeigen, daß  $g(u_1 + v_1i) \stackrel{!}{<} 1$ , dann wird

$$a + bi = (u + vi)(c + di) = (u_0 + v_0i)(c + di) + \underbrace{(u_1 + v_1i)(c + di)}_{\in \mathbf{Z}[i]}$$

mit, falls  $u_1 + v_1i \neq 0$ ,

$$f((u_1 + v_1i)(c + di)) = g(u_1 + v_1i) \cdot f(c + di) \stackrel{f(c+di) > 0}{<} f(c + di).$$

In der Tat wird

$$g(u_1 + v_1i) = u_1^2 + v_1^2 \leq (1/2)^2 + (1/2)^2 = 1/2 < 1.$$

- (2) Wir schreiben kurz  $\alpha := \sqrt{-5}$ . Es ist also  $\alpha^2 = -5$ .

Wir wollen zeigen, daß  $\mathbf{z}_{[\alpha]} \langle 1 + \alpha, 2 \rangle$  kein Hauptideal ist. Damit ist dann gezeigt, daß  $\mathbf{Z}[\alpha]$  kein Hauptidealbereich ist.

*Annahme*, es ist  $\mathbf{z}_{[\alpha]} \langle 1 + \alpha, 2 \rangle = \mathbf{z}_{[\alpha]} \langle x + y\alpha \rangle$  für gewisse  $x, y \in \mathbf{Z}$ .

Es ist  $\mathbf{z}_{[\alpha]} \langle x + y\alpha \rangle = \mathbf{z} \langle x + y\alpha, -5y + x\alpha \rangle$ . Der Index der Untergruppe  $\mathbf{z} \langle x + y\alpha, -5y + x\alpha \rangle$  in der abelschen Gruppe  $\mathbf{Z}[\alpha] = \mathbf{z} \langle 1, \alpha \rangle$  ist

$$|\mathbf{Z}[\alpha]/\mathbf{z}_{[\alpha]} \langle x + y\alpha \rangle| = |\det \begin{pmatrix} x & -5y \\ y & x \end{pmatrix}| = x^2 + 5y^2,$$

wie man sich mit dem Elementarteilersatz überlegt; cf. Satz 4. In der Tat gibt es nach loc. cit. eine  $\mathbf{Z}$ -lineare Basis  $(\beta_1, \beta_2)$  von  $\mathbf{Z}[\alpha]$ , für welche die Untergruppe  $\mathbf{z}_{[\alpha]} \langle x + y\alpha \rangle$  die  $\mathbf{Z}$ -lineare Basis  $(z_1\beta_1, z_2\beta_2)$  hat für gewisse  $z_1, z_2 \in \mathbf{Z}$ . Die Faktorgruppe ist damit isomorph zu  $\mathbf{Z}/z_1\mathbf{Z} \oplus \mathbf{Z}/z_2\mathbf{Z}$ , hat also Ordnung  $|z_1z_2|$ . Auf der anderen Seite ist dies die Determinante der Einbettung, die bis auf Vorzeichen von den Basiswahlen unabhängig ist.

Dagegen ist  $\mathbf{z}_{[\alpha]} \langle 1 + \alpha, 2 \rangle = \mathbf{z} \langle 1 + \alpha, 2, -5 + \alpha, 2\alpha \rangle$ . Mittels **SmithForm** erhalten wir

$$\begin{pmatrix} 1 & 2 & -5 & 0 \\ 1 & 0 & 1 & 2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}}_{\in \text{GL}_2(\mathbf{Z})} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 & 1 & -2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{pmatrix}}_{\in \text{GL}_4(\mathbf{Z})}$$

Also ist  $\mathbf{z}_{[\alpha]} \langle 1 + \alpha, 2 \rangle = \mathbf{z} \langle 1 - \alpha, 2 \rangle$  und  $\mathbf{Z}[\alpha]/\mathbf{z}_{[\alpha]} \langle 1 + \alpha, 2 \rangle \simeq \mathbf{Z}/2$  als  $\mathbf{Z}$ -Moduln, insbesondere also  $|\mathbf{Z}[\alpha]/\mathbf{z}_{[\alpha]} \langle 1 + \alpha, 2 \rangle| = 2$ .

Somit ist  $x^2 + 5y^2 = 2$ , wobei  $x, y \in \mathbf{Z}$ . Da dies weder für  $|y| \geq 1$  noch für  $y = 0$  sein kann, sind wir an einen *Widerspruch* gelangt.

(3) Schreibe  $\zeta := \zeta_3$ .

Sei

$$g : \begin{array}{l} \mathbf{Q}(\zeta) \longrightarrow \mathbf{Q}_{\geq 0} \\ x + y\zeta \longmapsto |x + y\zeta|^2 = (x + y\zeta)(x + y\zeta^2) = x^2 - xy + y^2 = (x - y/2)^2 + 3y^2/4, \end{array}$$

wobei  $x, y \in \mathbf{Q}$ . Wir müssen zeigen, daß  $f := g|_{\mathbf{Z}[\zeta] \setminus \{0\}}^{\mathbf{Z}_{>0}}$  die in der Vorbemerkung geforderte Eigenschaft hat. Beachte, daß  $g(z \cdot w) = g(z) \cdot g(w)$  für  $z, w \in \mathbf{Q}(\zeta)$ .

Seien  $r = a + b\zeta, s = c + d\zeta \in \mathbf{Z}[\zeta] \setminus \{0\}$  gegeben, wobei  $a, b, c, d \in \mathbf{Z}$ . In  $\mathbf{Q}(\zeta)$  sei

$$\frac{a + b\zeta}{c + d\zeta} =: u + v\zeta$$

mit  $u (= (ac + bd - ad)/(c^2 - cd + d^2))$  und  $v (= (bc - ad)/(c^2 - cd + d^2))$  aus  $\mathbf{Q}$ .

Seien  $u_0 \in \mathbf{Z}$  und  $u_1 \in \mathbf{Q}$  mit  $u = u_0 + u_1$  und  $|u_1| \leq 1/2$ .

Seien  $v_0 \in \mathbf{Z}$  und  $v_1 \in \mathbf{Q}$  mit  $v = v_0 + v_1$  und  $|v_1| \leq 1/2$ .

Können wir zeigen, daß  $g(u_1 + v_1\zeta) \stackrel{!}{<} 1$ , dann wird

$$a + b\zeta = (u + v\zeta)(c + d\zeta) = (u_0 + v_0\zeta)(c + d\zeta) + \underbrace{(u_1 + v_1\zeta)(c + d\zeta)}_{\in \mathbf{Z}[\zeta]}$$

mit, falls  $u_1 + v_1\zeta \neq 0$ ,

$$f((u_1 + v_1\zeta)(c + d\zeta)) = g(u_1 + v_1\zeta) \cdot f(c + d\zeta) \stackrel{f(c+d\zeta) > 0}{<} f(c + d\zeta).$$

In der Tat wird

$$g(u_1 + v_1\zeta) = (u_1 - v_1/2)^2 + 3v_1^2/4 \leq (3/4)^2 + (3/4)(1/2)^2 = 3/4 < 1.$$

### Aufgabe 37

Es ist

$$\frac{|g_s^G|}{n_r} \chi_r(g_s) \in \mathcal{O}_{\mathbf{Q}(\zeta_e)}$$

für  $r, s \in [1, t]$ ; cf. Bemerkung 45.

Beachte, daß hierfür die Aussage  $\mathcal{O}_{\mathbf{Q}(\zeta_e)} = \mathbf{Z}[\zeta_e]$  aus Satz 89 nicht benötigt wird, sondern nur das Argument zu Bemerkung 45, das, in dortiger Bezeichnung, zeigt, daß  $\beta_{q,r}$  Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten ist.

Also ist

$$\frac{|G|}{n_r} \stackrel{\text{S. 38.(1)}}{=} \frac{1}{n_r} \sum_{g \in G} \chi_r(g) \overline{\chi_r(g)} = \sum_{s \in [1, t]} \frac{|g_s^G|}{n_r} \chi_r(g_s) \overline{\chi_r(g_s)} \stackrel{\text{B. 45, A. 23.(1)}}{\in} \mathcal{O}_{\mathbf{Q}(\zeta_e)} \cap \mathbf{Q} \stackrel{\text{B. 53}}{=} \mathcal{O}_{\mathbf{Q}} \stackrel{\text{Bsp. 60.(1)}}{=} \mathbf{Z}.$$

### Aufgabe 38

(1) Wegen  $R$  Hauptidealbereich läßt sich in  $R \setminus \{0\}$  jedes Element als Produkt von Primelementen aus  $R \setminus \{0\}$  schreiben läßt; cf. Aufgabe 6.(2).

Das ist die einzige Eigenschaft, die wir vom Integritätsbereich  $R$  verwenden werden.

Beachte, daß prime Elemente von  $R \setminus \{0\}$  irreduzibel sind; cf. Lösung zu Aufgabe 6.(1). Der Vollständigkeit halber wiederholen wir hier das Argument. Sei  $y \in R \setminus \{0\}$  prim. Wir wollen zeigen, daß  $y$  irreduzibel ist. *Annahme*, nicht. Zunächst ist  $y$  eine Nichteinheit, da  $R/\langle y \rangle$  als Integritätsbereich ungleich  $\{0\}$  ist. Sei  $y = uv$  mit Nichteinheiten  $u, v \in R$ . Da  $y \neq 0$ , sind auch  $u, v \neq 0$ . Dann ist  $uv \equiv_y 0$ , und also o.E.  $u \equiv_y 0$ , da  $R/\langle y \rangle$  ein Integritätsbereich ist. Somit ist  $u = yw$  für ein  $w \in R$ . Aus  $u = yw = uvw$  folgt  $1 = vw$ , im *Widerspruch* zu  $v$  Nichteinheit.

Ein Polynom  $g(X) = \sum_{i \geq 0} g_i X^i \in R[X] \setminus \{0\}$  heiße *primitiv*, falls es kein Primelement  $p \in R \setminus \{0\}$  gibt, welches  $g_i$  teilt für alle  $i \geq 0$ .

**Vorbemerkung 1.** Jedes Polynom  $w(X) = \sum_{i \geq 0} w_i X^i \in K[X] \setminus \{0\}$  kann geschrieben werden als  $w(X) = q \cdot \tilde{w}(X)$  mit  $q \in Q \setminus \{0\}$  und  $\tilde{w}(X) \in R[X]$  primitiv. Ist  $w(X) \in R[X] \setminus \{0\}$ , so ist auch  $q \in R$ . Ist  $q \cdot \tilde{w}(X) = q' \cdot \hat{w}(X)$  mit  $q, q' \in Q \setminus \{0\}$  und  $\tilde{w}(X), \hat{w}(X) \in R[X]$ , so ist  $qq'^{-1} \in U(R)$ .

*Beweis.* Zur Existenz. Nach Multiplikation mit den Nennern der Koeffizienten dürfen wir  $w(X) \in R[X]$  annehmen. Für  $i \geq 0$  mit  $w_i \neq 0$  schreiben wir

$$w_i = e_i \cdot \prod_{p \in P} p^{n_i(p)},$$

wobei  $P$  eine geeignete endliche Menge von Primelementen von  $R \setminus \{0\}$  ist, in welcher für  $p, p' \in P$  gilt, daß aus  $pp'^{-1} \in U(R)$  bereits  $p = p'$  folgt. Sei

$$q := \prod_{p \in P} p^{\min\{n_i(p) : i \geq 0, w_i \neq 0\}} \in R.$$

Dann ist  $\tilde{w}(X) := q^{-1} \cdot w(X) \in R[X]$ . Schreibe  $\tilde{w}(X) = \sum_{i \geq 0} \tilde{w}_i X^i$ .

Wir behaupten, daß  $w(X)$  primitiv ist. *Annahme*, es gibt ein  $p_1 \in R \setminus \{0\}$  prim, welches  $\tilde{w}_i$  teilt für alle  $i \geq 0$ . Sei nun  $j \geq 0$  mit  $\tilde{w}_j \neq 0$  gewählt. Es ist

$$\tilde{w}_j = e_j \cdot \prod_{p \in P} p^{n_j(p) - \min\{n_i(p) : i \geq 0\}}.$$

Da  $p_1$  prim ist und da  $e_j \in U(R)$  ist, ist  $p_1$  ein Teiler von  $p_0$  für ein  $p_0 \in P$ . Dann aber ist  $p_0 = p_1 s$  für ein  $s \in R$ . Da  $p_0$  prim ist, ist  $p_0$  irreduzibel. Da  $p_1$  prim ist und also Nichteinheit, folgt  $s \in U(R)$ . Also ist auch  $p_0$  ein Teiler von  $\tilde{w}_i$  für alle  $i \geq 0$ .

Es gibt ein  $k \geq 0$  mit  $w_k \neq 0$  und  $n_k(p_0) = \min\{n_i(p_0) : i \geq 0, w_i \neq 0\}$ . Also ist

$$\tilde{w}_k = e_k \cdot \prod_{p \in P} p^{n_k(p) - \min\{n_i(p) : i \geq 0\}} = e_k \cdot \prod_{p \in P \setminus \{p_0\}} p^{n_k(p) - \min\{n_k(p) : k \geq 0\}}.$$

Da  $p_0$  ein Primteiler von  $\tilde{w}_k$  ist und da  $e_j \in U(R)$  ist, ist  $p_0$  ein Teiler eines  $p \in P \setminus \{p_0\}$ . Dann aber ist  $p = p_0 t$  für ein  $t \in R$ . Da  $p$  prim ist, ist  $p$  irreduzibel. Da  $p_0$  prim ist und also Nichteinheit, folgt  $t$  Einheit. Nach Wahl von  $P$  folgt  $p = p_0$ , und wir haben einen *Widerspruch*. Also ist  $\tilde{w}(X)$  primitiv.

Zur Eindeutigkeit bis auf einen Faktor aus  $U(R)$ . Sei  $q \cdot \tilde{w}(X) = q' \cdot \hat{w}(X)$  mit  $q, q' \in Q \setminus \{0\}$  und  $\tilde{w}(X), \hat{w}(X) \in R[X]$ . Schreibe  $q/q' = r/r'$  mit  $r, r' \in R \setminus \{0\}$  ohne gemeinsamen Primteiler. Dann ist  $r \cdot \tilde{w}(X) = r' \cdot \hat{w}(X)$ . *Annahme*, es gibt einen Primteiler  $p$  von  $r$ . Es ist  $p$  ein Teiler von  $r' \cdot \hat{w}(X)$ . Da  $p$  prim und kein Teiler von  $r'$  ist, teilt  $p$  alle Koeffizienten von  $\hat{w}(X)$ , im *Widerspruch* zu  $\hat{w}(X)$  primitiv. Also ist  $r \in U(R)$ . Genauso folgt auch  $r' \in U(R)$ . Folglich ist auch  $q/q' = r/r' \in U(R)$ .  $\square$

**Vorbemerkung 2.** Das Produkt zweier primitiver Polynome  $g(X) = \sum_{i \geq 0} g_i X^i$  und  $h(X) = \sum_{i \geq 0} h_i X^i$  in  $R[X]$  ist wieder primitiv.

*Beweis.* *Annahme*, es gibt ein Primelement  $p \in R$ , welches  $\sum_{i \in [0, k]} g_i h_{k-i}$  teilt für alle  $k \geq 0$ . Sei  $a \geq 0$  maximal mit  $\langle p \rangle \not\subseteq \langle g_a \rangle$ , existent wegen  $g(X)$  primitiv. Sei  $b \geq 0$  maximal mit  $\langle p \rangle \not\subseteq \langle h_b \rangle$ ,

existent wegen  $h(X)$  primitiv. Dann teilt  $p$  das Produkt  $g_i h_{a+b-i}$  für alle  $i \in [0, a+b] \setminus \{a\}$ . Da  $p$  auch  $\sum_{i \in [0, a+b]} g_i h_{a+b-i}$  teilt, teilt  $p$  auch  $g_a h_b$ . Da  $p$  prim ist, folgt daraus, daß  $p$  auch  $g_a$  oder  $h_b$  teilt, im *Widerspruch* zur Wahl von  $a$  oder von  $b$ .  $\square$

**Nun zur Aufgabe.** Schreibe  $u(X) = q' \tilde{u}(X)$  mit  $q' \in \mathbf{Q} \setminus \{0\}$  und  $\tilde{u}(X) \in R[X]$  primitiv; schreibe  $v(X) = q'' \tilde{v}(X)$  mit  $q'' \in \mathbf{Q} \setminus \{0\}$  und  $\tilde{v}(X) \in R[X]$  primitiv; cf. Vorbemerkung 1.

Es ist  $f(X) = u(X) \cdot v(X) = q' q'' \cdot \tilde{u}(X) \cdot \tilde{v}(X)$  mit  $\tilde{u}(X) \cdot \tilde{v}(X)$  primitiv; cf. Vorbemerkung 2. Da  $f(X) \in R[X]$ , ist  $q' q'' \in R$ ; cf. Vorbemerkung 1.

Es ist  $q'^{-1} u(X) = \tilde{u}(X) \in R[X]$ . Es ist  $q' v(X) = (q' q'') q''^{-1} v(X) = (q' q'') \tilde{v}(X) \in R[X]$ .

(2) Ist  $\mu_{\alpha, \mathbf{Q}}(X) \in \mathbf{Z}[X]$ , dann ist  $\alpha \in \mathcal{O}_K$ .

Sei umgekehrt  $\alpha \in \mathcal{O}_K$ . Sei  $f(X) \in \mathbf{Z}[X]$  normiert mit  $f(\alpha) = 0$ . Es ist  $f(X) = \mu_{\alpha, \mathbf{Q}}(X) \cdot g(X)$  für ein  $g(X) \in \mathbf{Q}[X]$ . Da  $f(X)$  und  $\mu_{\alpha, \mathbf{Q}}(X)$  normiert sind, ist auch  $g(X)$  normiert. Nach (1) gibt es ein  $q \in \mathbf{Q} \setminus \{0\}$  mit  $q \cdot \mu_{\alpha, \mathbf{Q}}(X) \in \mathbf{Z}[X]$  und  $q^{-1} \cdot g(X) \in \mathbf{Z}[X]$ . Da  $\mu_{\alpha, \mathbf{Q}}(X)$  und  $g(X)$  normiert sind, ist  $q \in \mathbf{Z}$  und  $q^{-1} \in \mathbf{Z}$ , mithin  $q \in \{-1, +1\}$ . Also ist bereits  $\mu_{\alpha}(X) \in \mathbf{Z}[X]$ .

### Aufgabe 39

Schreibe  $\alpha := \sqrt{d}$ . Es ist also  $\alpha^2 = d$ . Schreibe  $K := \mathbf{Q}(\sqrt{d})$ .

Es ist  $\mathbf{Q}(\alpha) = \mathbf{Q}\langle 1, \alpha \rangle = \{u + v\alpha : u, v \in \mathbf{Q}\}$ .

Sei  $\beta := u + v\alpha \in \mathbf{Q}(\alpha)$  gegeben, wobei  $u, v \in \mathbf{Q}$ .

*Fall*  $v = 0$ . Es ist  $\mu_{\beta, \mathbf{Q}}(X) = X - u \in \mathbf{Z}[X]$  genau dann, wenn  $u \in \mathbf{Z}$ . Also ist diesenfalls  $\beta \in \mathcal{O}_K$  genau dann, wenn  $u \in \mathbf{Z}$ .

*Fall*  $v \neq 0$ . Es ist  $\beta^2 = u^2 + 2uv\alpha + v^2\alpha^2 = (u^2 + dv^2) + 2uv\alpha$ . Also ist

$$\beta^2 - 2u\beta = (u^2 + dv^2) + 2uv\alpha - 2u^2 - 2uv\alpha = dv^2 - u^2,$$

und folglich

$$\mu_{\alpha, \mathbf{Q}}(X) = X^2 - 2uX + (u^2 - dv^2).$$

Nach Aufgabe 38.(2) ist  $\beta \in \mathcal{O}_K$  genau dann, wenn  $2u \in \mathbf{Z}$  und  $u^2 - dv^2 \in \mathbf{Z}$ . Schreibe  $u = u'/2$  mit  $u' \in \mathbf{Z}$ . Es sollte also  $u' \in \mathbf{Z}$  und  $v \in \mathbf{Q}$  noch so sein, daß  $u'^2/4 - dv^2 \in \mathbf{Z}$ . Es sollte jedenfalls  $v^2 \in \frac{1}{4d}\mathbf{Z}$  sein. Da  $d$  quadratfrei ist, muß  $v \in \frac{1}{2}\mathbf{Z}$  liegen. Schreibe  $v = v'/2$  mit  $v' \in \mathbf{Z} \setminus \{0\}$ . Insgesamt ist  $\beta \in \mathcal{O}_K$  genau dann, wenn

$$(*) \quad u'^2 \equiv_4 dv'^2.$$

Ist  $u' \equiv_2 0$ , dann muß wegen  $d \not\equiv_4 0$  auch  $v' \equiv_2 0$  sein. Diesenfalls ist dann  $\beta = (u'/2) + (v'/2)\alpha \in \mathcal{O}_K$ .

Ist  $u' \equiv_2 1$ , dann ist  $u'^2 \equiv_4 1$ , somit notwendig auch  $v' \equiv_2 1$ , also auch  $v'^2 \equiv_4 1$  und mithin die Kongruenz (\*) nur erfüllbar, wenn  $d \equiv_4 1$ . Diesenfalls ist sie erfüllt, falls  $u' \equiv_2 1$  und  $v' \equiv_2 1$ .

Fassen wir nun beide *Fälle* zusammen.

Ist  $d \not\equiv_4 1$ , so ist

$$\begin{aligned} \mathcal{O}_K &= \mathbf{Z} \cup \{u + v\alpha : u \in \mathbf{Z}, v \in \mathbf{Z} \setminus \{0\}\} \\ &= \mathbf{z}\langle 1, \alpha \rangle \\ &= \mathbf{Z}[\alpha]. \end{aligned}$$

Ist  $d \equiv_4 1$ , so ist

$$\begin{aligned} \mathcal{O}_K &= \mathbf{Z} \cup \{u + v\alpha : u \in \mathbf{Z}, v \in \mathbf{Z} \setminus \{0\}\} \cup \{u + v\alpha : u \in \frac{1}{2} + \mathbf{Z}, v \in \frac{1}{2} + \mathbf{Z}\} \\ &= \mathbf{z}\langle 1, \alpha, (1 + \alpha)/2 \rangle \\ &= \mathbf{z}\langle 1, (1 + \alpha)/2 \rangle \\ &= \mathbf{Z}[(1 + \alpha)/2]. \end{aligned}$$

Formulieren wir nochmals in unsere ursprüngliche Notation um.

Ist  $d \not\equiv_4 1$ , so ist  $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\sqrt{d}]$ .

Ist  $d \equiv_4 1$ , so ist  $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[(1 + \sqrt{d})/2]$ .

Insbesondere ist e.g.  $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$  kein Hauptidealbereich; cf. Aufgabe 36.(2).

Ferner ist e.g.  $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[(1 + \sqrt{5})/2] \neq \mathbf{Z}[\sqrt{5}]$ .

#### Aufgabe 40

- (1) Schreibe  $\ell := [K : \mathbf{Q}(\alpha)]$ . Es ist  $n = [K : \mathbf{Q}] = [K : \mathbf{Q}(\alpha)] \cdot [\mathbf{Q}(\alpha) : \mathbf{Q}] = \ell \cdot m$ .

Sei  $(\beta_1, \dots, \beta_\ell)$  eine  $\mathbf{Q}(\alpha)$ -lineare Basis von  $K$ .

Es ist  $(\alpha^0, \dots, \alpha^{m-1})$  eine  $\mathbf{Q}$ -lineare Basis von  $\mathbf{Q}(\alpha)$ .

Nach Algebra ist

$$(\beta_1 \alpha^0, \dots, \beta_1 \alpha^{m-1}, \beta_2 \alpha^0, \dots, \beta_2 \alpha^{m-1}, \dots, \beta_\ell \alpha^0, \dots, \beta_\ell \alpha^{m-1})$$

eine  $\mathbf{Q}$ -lineare Basis von  $K$ . Bezüglich dieser wird die Abbildung  $K \rightarrow K, \gamma \mapsto \alpha\gamma$  durch die Blockdiagonalmatrix

$$\text{diag}(A, \dots, A)$$

mit  $\ell$  Einträgen beschrieben, wobei

$$A = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & 0 & & -a_2 \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & 0 & -a_{m-2} \\ & & & & 1 & -a_{m-1} \end{pmatrix}$$

eine Begleitmatrix von  $\mu_{\alpha, \mathbf{Q}}(X)$  ist.

Da nun  $\text{tr } A = -a_{m-1}$ , folgt  $\text{Tr}_{K|\mathbf{Q}}(\alpha) = \ell \cdot \text{tr } A = -[K : \mathbf{Q}(\alpha)] \cdot a_{m-1}$ .

- (2) Sei nun  $\alpha \in \mathcal{O}_K$ . Nach Aufgabe 38.(2) ist  $\mu_{\alpha, \mathbf{Q}}(X) \in \mathbf{Z}[X]$ . Insbesondere ist also  $a_{m-1} \in \mathbf{Z}$ . Mit (1) folgt somit, daß

$$\text{Tr}_{K|\mathbf{Q}}(\alpha) = -[K : \mathbf{Q}(\alpha)] \cdot a_{m-1} \in \mathbf{Z}.$$

#### Aufgabe 41

Sei  $G = \mathbf{z}\langle \xi_1, \dots, \xi_n \rangle$ . Es ist  $G^\# = \mathbf{z}\langle \xi_1^*, \dots, \xi_n^* \rangle$ , mit  $\xi_i^* \in K$  für  $i \in [1, n]$  so, daß  $\text{Tr}_{K|\mathbf{Q}}(\xi_i \cdot \xi_j^*) = \partial_{i,j}$  für  $j \in [1, n]$ ; cf. Beweis zu Bemerkung 66.(2). Schreibe  $(a_{i,j})_{i,j} := (\text{Tr}_{K|\mathbf{Q}}(\xi_i \cdot \xi_j))_{i,j}$  und  $(a'_{i,j})_{i,j} := (\text{Tr}_{K|\mathbf{Q}}(\xi_i^* \cdot \xi_j^*))_{i,j}$ .

Es ist

$$(*) \quad \xi_i = \sum_j a_{i,j} \cdot \xi_j^*$$

für  $i \in [1, n]$ , da  $\text{Tr}_{K|\mathbf{Q}}(\sum_j a_{i,j} \cdot \xi_j^* \cdot \xi_k) = \sum_j a_{i,j} \partial_{j,k} = a_{i,k} = \text{Tr}_{K|\mathbf{Q}}(\xi_i \cdot \xi_k)$  für  $k \in [1, n]$ .

Genauso folgt auch, daß

$$(**) \quad \xi_i^* = \sum_j a'_{i,j} \cdot \xi_j$$

Insbesondere ist

$$(***) \quad ((a_{i,j})_{i,j})^{-1} = (a'_{i,j})_{i,j} \in \mathrm{GL}_n(\mathbf{Q}).$$

(1) Es ist

$$\Delta(G^\#) = \det((a'_{i,j})_{i,j}) \stackrel{(***)}{=} \det((a_{i,j})_{i,j})^{-1} = \Delta(G).$$

(2) Dank (\*) ist  $G \subseteq G^\#$  gleichbedeutend mit  $(a_{i,j})_{i,j} \in \mathbf{Z}^{n \times n}$ .

Da  $\Delta(G) \cdot (a'_{i,j})_{i,j} \stackrel{(***)}{=} \det((a_{i,j})_{i,j}) \cdot ((a_{i,j})_{i,j})^{-1} \in \mathbf{Z}^{n \times n}$  unter Verwendung der Cramerschen Regel, ist dank (\*\*) auch  $\Delta(G) \cdot G^\# \subseteq G$ .

Schließlich ist  $|G^\# / G|$  gleich dem Produkt der Beträge der Elementarteiler der die Einbettung  $G \hookrightarrow G^\#$  beschreibenden Matrix  $(a_{i,j})_{i,j}$ , also gleich dem Betrag ihrer Determinante, i.e. gleich  $|\Delta(G)|$ .

Auch aus  $|\Delta(G)| = |G^\# / G|$  folgt, daß  $|\Delta(G)| \cdot (G^\# / G) = 0$ , i.e. daß  $|\Delta(G)| \cdot G^\# \subseteq G$ .

#### Aufgabe 42

Schreibe  $\alpha := \sqrt{d}$ . Es ist  $\alpha^2 = d$ .

Fall  $d \not\equiv_4 1$ . Gemäß Aufgabe 39 ist  $\mathcal{O}_K = \mathbf{Z}[\alpha]$ .

Es ist  $(1, \alpha)$  eine  $\mathbf{Z}$ -lineare Basis von  $\mathcal{O}_K$ . Ihrbezüglich rechnen wir

$$\begin{aligned} \mathrm{Tr}_{K|\mathbf{Q}}(1) &= \mathrm{tr} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2 \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha) &= \mathrm{tr} \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} = 0. \end{aligned}$$

Die Grammatrix der Spurbilinearform bezüglich dieser Basis ist also

$$\begin{pmatrix} \mathrm{Tr}_{K|\mathbf{Q}}(1 \cdot 1) & \mathrm{Tr}_{K|\mathbf{Q}}(1 \cdot \alpha) \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha \cdot 1) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha \cdot \alpha) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Also wird  $\Delta_K = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$ .

Ferner ist  $\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/(2d) \end{pmatrix}$ . Also ist eine Dualbasis unserer Basis  $(1, \alpha)$  gegeben durch

$$(1/2 \cdot 1 + 0 \cdot \alpha, 0 \cdot 1 + (2d)^{-1} \cdot \alpha) = \left(\frac{1}{2}, \frac{\alpha}{2d}\right).$$

Fall  $d \equiv_4 1$ . Gemäß Aufgabe 39 ist  $\mathcal{O}_K = \mathbf{Z}[(1 + \alpha)/2]$ .

Es ist  $(1, (1 + \alpha)/2)$  eine  $\mathbf{Z}$ -lineare Basis von  $\mathcal{O}_K$ . Ihrbezüglich rechnen wir

$$\begin{aligned} \mathrm{Tr}_{K|\mathbf{Q}}(1) &= \mathrm{tr} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2 \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha) &= \mathrm{tr} \begin{pmatrix} -1 & (d-1)/2 \\ 2 & 1 \end{pmatrix} = 0. \end{aligned}$$

Die Grammatrix der Spurbilinearform bezüglich dieser Basis ist also

$$\begin{pmatrix} \mathrm{Tr}_{K|\mathbf{Q}}(1 \cdot 1) & \mathrm{Tr}_{K|\mathbf{Q}}(1 \cdot (\alpha+1)/2) \\ \mathrm{Tr}_{K|\mathbf{Q}}((\alpha+1)/2 \cdot 1) & \mathrm{Tr}_{K|\mathbf{Q}}((\alpha+1)/2 \cdot (\alpha+1)/2) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & (d+1)/2 \end{pmatrix}.$$

Also wird  $\Delta_K = \det \begin{pmatrix} 2 & 1 \\ 1 & (d+1)/2 \end{pmatrix} = d$ .

Ferner ist  $\begin{pmatrix} 2 & 1 \\ 1 & (d+1)/2 \end{pmatrix}^{-1} = d^{-1} \begin{pmatrix} (d+1)/2 & -1 \\ -1 & 2 \end{pmatrix}$ . Also ist eine Dualbasis unserer Basis  $(1, (\alpha + 1)/2)$  gegeben durch

$$(d^{-1}((d+1)/2 + (-1)(\alpha+1)/2), d^{-1}(-1 + 2(\alpha+1)/2)) = \left(\frac{1}{2} - \frac{\alpha}{2d}, \frac{\alpha}{d}\right).$$

**Aufgabe 43**

```

// test data

P<X> := PolynomialRing(Rationals());

K<a> := NumberField(X^3 + X + 1);
b1 := [1,a,a^2,1+a];
b2 := [a+a^2,2*a,1+a^2,1/2];

K1<u> := NumberField(X^4 + X + 1);
b3 := [1,u,2*u+u^2,u^2,u^3];
b4 := [1+u+u^2,2*u,u+u^3,1+2*u^2,u^3];

// function

zbasis := function(b,K)
  n := Degree(K);
  m := #b;
  // c := Basis(K); // ElementToSequence gives coefficients wrt c
  X := Transpose(RMatrixSpace(Rationals(),m,n)! [ElementToSequence(b[i]) : i in [1..m]]);
  y := Lcm([Denominator(X[i][j]) : j in [1..m], i in [1..n]]);
  D,S,T := SmithForm(RMatrixSpace(Integers(),n,m)!(y*X));
  return [&+[b[j] * T[j][l] : j in [1..m]] : l in [1..n] ];
end function;

// test

zbasis(b1,K);
zbasis(b2,K);
zbasis(b3,K1);
zbasis(b4,K1);

```

**Aufgabe 44**

Wir verwenden `zbasis` aus Aufgabe 43.

```

// test data

P<X> := PolynomialRing(Rationals());

K1<a> := NumberField(X^3 + X + 1);
b1 := [1,a,a^2];

K2<u> := NumberField(X^4 + X + 1);
b2 := [1,u,u^2,u^3];

K3<zeta> := NumberField(CyclotomicPolynomial(10));
b3 := [1,zeta,zeta^2,zeta^3];

p := 3;

```

```

// function

jacp := function(b,p,K)
  n := Degree(K);
  MQ := MatrixRing(Rationals(),n);
  MF_p := MatrixRing(GF(p),n);
  // c := Basis(K); // ElementToSequence gives coefficients wrt c
  Frob := MF_p!((MQ![ElementToSequence(b[i]^p) : i in [1..n]]
    * (MQ![ElementToSequence(b[i]) : i in [1..n]]^-1)); // wrt basis b in rows
  BK := BasisMatrix(Kernel(Frob^n));
  BKZ := RMatrixSpace(Integers(),NumberOfRows(BK),n)!BK;
  return zbasis([&+[BKZ[i][j] * b[j] : j in [1..n]] : i in [1..NumberOfRows(BKZ)]]
    cat [p*b[i] : i in [1..n]], K);
end function;

// test

Determinant(MatrixRing(Rationals(),Degree(K1))![ElementToSequence(x) : x in jacp(b1,p,K1)]);
Determinant(BasisMatrix(pRadical(Order(b1),p)));
Determinant(MatrixRing(Rationals(),Degree(K2))![ElementToSequence(x) : x in jacp(b2,p,K2)]);
Determinant(BasisMatrix(pRadical(Order(b2),p)));
Determinant(MatrixRing(Rationals(),Degree(K3))![ElementToSequence(x) : x in jacp(b3,p,K3)]);
Determinant(BasisMatrix(pRadical(Order(b3),p)));

```

#### Aufgabe 45

- (1) Sei  $G = \mathbf{z}\langle \xi_1, \dots, \xi_n \rangle$ . Es ist  $G^\# = \mathbf{z}\langle \xi_1^*, \dots, \xi_n^* \rangle$ , mit  $\xi_i^* \in K$  für  $i \in [1, n]$  so, daß  $\text{Tr}_{K|\mathbf{Q}}(\xi_i \cdot \xi_j^*) = \partial_{i,j}$  für  $j \in [1, n]$ ; cf. Bemerkung 66.(1).

Sei  $H = \mathbf{z}\langle \eta_1, \dots, \eta_n \rangle$ . Es ist  $H^\# = \mathbf{z}\langle \eta_1^*, \dots, \eta_n^* \rangle$ , mit  $\eta_i^* \in K$  für  $i \in [1, n]$  so, daß  $\text{Tr}_{K|\mathbf{Q}}(\eta_i \cdot \eta_j^*) = \partial_{i,j}$  für  $j \in [1, n]$ .

Schreibe  $\xi_i = \sum_{j \in [1, n]} \eta_j b_{j,i}$  für  $i \in [1, n]$ , wobei  $B := (b_{i,j})_{i,j} \in \mathbf{Z}^{n \times n}$ .

Wir behaupten, daß für  $i \in [1, n]$

$$\eta_i^* \stackrel{!}{=} \sum_{j \in [1, n]} b_{i,j} \xi_j^*.$$

Für  $k \in [1, n]$  wird auf der einen Seite

$$\text{Tr}_{K|\mathbf{Q}}(\eta_i^* \cdot \xi_k) = \sum_{j \in [1, n]} \text{Tr}_{K|\mathbf{Q}}(\eta_i^* \cdot \eta_j) b_{j,k} = \sum_{j \in [1, n]} \partial_{i,j} b_{j,k} = b_{i,k},$$

auf der anderen Seite

$$\text{Tr}_{K|\mathbf{Q}}(\sum_{j \in [1, n]} b_{i,j} \xi_j^* \cdot \xi_k) = \sum_{j \in [1, n]} b_{i,j} \text{Tr}_{K|\mathbf{Q}}(\xi_j^* \xi_k) = \sum_{j \in [1, n]} b_{i,j} \partial_{j,k} = b_{i,k},$$

also beidesmal dasselbe. Dies zeigt die *Behauptung*.

Es ist  $|H/G|$  gleich dem Produkt der Beträge der Elementarteiler von  $B$ , also gleich  $|\det B|$ .

Dank Behauptung ist  $|G^\#/H^\#|$  gleich dem Produkt der Beträge der Elementarteiler von  $B^t$ , also gleich  $|\det B^t| = |\det B|$ .

Somit ist  $|H/G| = |\det B| = |G^\#/H^\#|$ .

(2) Es ist  $R \subseteq \mathcal{O}_K$ ; cf. Lemma 69. Also ist

$$R \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^\# \subseteq R^\#;$$

cf. Lemma 68. Also ist

$$\Delta(R) \stackrel{A.41}{=} |R^\# / R| = |R^\# / \mathcal{O}_K^\#| \cdot |\mathcal{O}_K^\# / \mathcal{O}_K| \cdot |\mathcal{O}_K / R| \stackrel{(1)}{=} |\mathcal{O}_K^\# / \mathcal{O}_K| \cdot |\mathcal{O}_K / R|^2 \stackrel{A.41}{=} \Delta_K \cdot |\mathcal{O}_K / R|^2.$$

Da  $\Delta(R)$  quadratfrei ist, folgt  $|\mathcal{O}_K / R| = 1$ , und also  $\mathcal{O}_K = R$ .

Eine Chance, auf diese Weise eine  $\mathbf{Z}$ -Ordnung als  $\mathbf{Z}$ -Maximalordnung zu erkennen, hat man natürlich nur, wenn  $\Delta_K$  quadratfrei ist.

(3) Berechnen wir zunächst bezüglich der  $\mathbf{Q}$ -linearen Basis  $(1, \alpha, \alpha^2)$  von  $K$

$$\begin{aligned} \mathrm{Tr}_{K|\mathbf{Q}}(1) &= \mathrm{tr} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 3 \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha) &= \mathrm{tr} \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} = 0 \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2) &= \mathrm{tr} \begin{pmatrix} 0 & -1 & 0 \\ 0 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix} = -2 \end{aligned}$$

Also wird

$$\begin{aligned} \Delta(\mathbf{Z}[\alpha]) &= \det \begin{pmatrix} \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^0 \cdot \alpha^0) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^0 \cdot \alpha^1) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^0 \cdot \alpha^2) \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^1 \cdot \alpha^0) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^1 \cdot \alpha^1) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^1 \cdot \alpha^2) \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2 \cdot \alpha^0) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2 \cdot \alpha^1) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2 \cdot \alpha^2) \end{pmatrix} \\ &= \det \begin{pmatrix} \mathrm{Tr}_{K|\mathbf{Q}}(1) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2) \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha) & \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2) & \mathrm{Tr}_{K|\mathbf{Q}}(-\alpha-1) \\ \mathrm{Tr}_{K|\mathbf{Q}}(\alpha^2) & \mathrm{Tr}_{K|\mathbf{Q}}(-\alpha-1) & \mathrm{Tr}_{K|\mathbf{Q}}(-\alpha^2-\alpha) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & -2 \\ 0 & -2 & -3 \\ -2 & -3 & 2 \end{pmatrix} = -31. \end{aligned}$$

Da  $\Delta(\mathbf{Z}[\alpha])$  quadratfrei ist, können wir mit (2) auf  $\mathbf{Z}[\alpha] = \mathcal{O}_K$  schließen.

#### Aufgabe 46

Sei  $G = \mathbf{z}\langle \xi_1, \dots, \xi_n \rangle$ . Sei  $H = \mathbf{z}\langle \eta_1, \dots, \eta_n \rangle$

Schreibe  $\xi_i = \sum_{j \in [1, n]} \eta_j u_{j, i}$  für  $i \in [1, n]$ , wobei  $(u_{i, j})_{i, j} \in \mathrm{GL}_n(\mathbf{Q})$ .

(1) Es ist  $G \cap H \subseteq G$ . Also genügt es zu zeigen, daß es ein  $a \in \mathbf{Z} \setminus \{0\}$  mit  $aG \stackrel{!}{\subseteq} G \cap H$  gibt; cf. Bemerkung 66.(2).

Sei  $a \in \mathbf{Z} \setminus \{0\}$  so, daß  $a(u_{i, j})_{i, j} \in \mathbf{Z}^{n \times n}$ . Dann ist  $a\xi_i = \sum_{j \in [1, n]} \eta_j a u_{j, i} \in H$  für  $i \in [1, n]$  und also  $aG \subseteq H$ . Insgesamt ist  $aG \subseteq G \cap H$ .

Um eine  $\mathbf{Z}$ -lineare Basis von  $G \cap H$  zu berechnen, können wir dank Satz 4 mit Basiswechsel in  $G$  und in  $H$  annehmen, daß  $(u_{i, j})_{i, j} \in \mathrm{GL}_n(\mathbf{Q})$  eine Diagonalmatrix ist. Schreibe  $u_{i, i} = s_i / t_i$  mit  $s_i, t_i \in \mathbf{Z} \setminus \{0\}$  teilerfremd zueinander für  $i \in [1, n]$ . Es wird

$$G \cap H = \mathbf{z}\langle \eta_1 s_1, \dots, \eta_n s_n \rangle = \mathbf{z}\langle \xi_1 t_1, \dots, \xi_n t_n \rangle.$$

(2) Es ist  $H \subseteq G + H$ . Also genügt es zu zeigen, daß es ein  $a \in \mathbf{Z} \setminus \{0\}$  mit  $G + H \stackrel{!}{\subseteq} a^{-1}H$  gibt; cf. Bemerkung 66.(2).

Sei  $a \in \mathbf{Z} \setminus \{0\}$  so, daß  $a(u_{i, j})_{i, j} \in \mathbf{Z}^{n \times n}$ . In der Lösung zu (1) haben wir bereits gesehen, daß  $aG \subseteq H$ . Also ist  $G \subseteq a^{-1}H$ . Ferner ist  $H \subseteq a^{-1}H$ . Insgesamt ist  $G + H \subseteq a^{-1}H$ .

Um eine  $\mathbf{Z}$ -lineare Basis von  $G + H$  zu berechnen, cf. Bemerkung 65.

(3) Es ist

$$\begin{aligned}
 (G + H)^\# &= \{ \alpha \in K : \text{Tr}_{K|\mathbf{Q}}(\alpha(G + H)) \subseteq \mathbf{Z} \} \\
 &= \{ \alpha \in K : \text{Tr}_{K|\mathbf{Q}}(\alpha G) + \text{Tr}_{K|\mathbf{Q}}(\alpha H) \subseteq \mathbf{Z} \} \\
 &= \{ \alpha \in K : \text{Tr}_{K|\mathbf{Q}}(\alpha G) \subseteq \mathbf{Z} \} \cap \{ \alpha \in K : \text{Tr}_{K|\mathbf{Q}}(\alpha H) \subseteq \mathbf{Z} \} \\
 &= G^\# \cap H^\# .
 \end{aligned}$$

Es folgt

$$(G \cap H)^\# \stackrel{\text{B. 66.(1)}}{=} (G^{\#\#} \cap H^{\#\#})^\# = (G^\# + H^\#)^{\#\#} \stackrel{\text{B. 66.(1)}}{=} G^\# + H^\# .$$

#### Aufgabe 47

(1) // test data

```

P<X> := PolynomialRing(Rationals());

K<a> := NumberField(X^3 + X + 1);
b1 := [1, a, a^2];
b2 := [1, 2*a, 1+a^2];

K1<u> := NumberField(X^4 + X + 1);
b3 := [1, u, u^2, u^3];
b4 := [1+u+u^2, 2*u, 1+2*u^2, u^3];

// function

discriminant := function(b, K)
  n := Degree(K);
  return Determinant(MatrixRing(Rationals(), n)!
    [Trace(b[i]*b[j]) : j in [1..n], i in [1..n]]);
end function;

// test

discriminant(b1, K);
discriminant(b2, K);
discriminant(b3, K1);
discriminant(b4, K1);

```

(2) // test data

```

P<X> := PolynomialRing(Rationals());

K<a> := NumberField(X^3 + X + 1);
b1 := [1, a, a^2];
b2 := [1, 2*a, 1+a^2];
b3 := [3*a, 6*a + 9*a^2, 3 + 3*a^2];

K1<u> := NumberField(X^4 + X + 1);
b4 := [1, u, u^2, u^3];
b5 := [1+u+u^2, 2*u, 1+2*u^2, u^3];

```

```

// function

stab := function(b,K)
  n := Degree(K);
  // c := Basis(K); // ElementToSequence gives coefficients wrt c
  B := (MatrixRing(Rationals(),n)!ElementToSequence(b[i] : i in [1..n]))^-1;
  U := RMatrixSpace(Rationals(),n,n^2)!0;
  for i in [1..n] do
    for j in [1..n] do
      for k in [1..n] do
        v := (VectorSpace(Rationals(),n)!ElementToSequence(b[i]*b[j])) * B;
        U[i][(k-1)*n + j] := v[k];
      end for;
    end for;
  end for;
  w := Lcm([Denominator(U[i][j]) : j in [1..n^2], i in [1..n]]);
  D,S := SmithForm(RMatrixSpace(Integers(),n,n^2)!(w*U));
  return [D[j][j]^-1 * w * &+[S[j][i] * b[i] : i in [1..n]] : j in [1..n]];
  // &+ : summation over sequence
end function;

// test

stab(b1,K);
stab(b2,K);
stab(b3,K);
stab(b4,K1);
stab(b5,K1);

```

#### Aufgabe 48

- (1) Wir verwenden `zbasis` aus Aufgabe 43, `jacp` aus Aufgabe 44, `discriminant` aus Aufgabe 47.(1) und `stab` aus Aufgabe 47.(2).

```

// test data

P<X> := PolynomialRing(Rationals());

K0<a0> := NumberField(X^3 + X + 1);
K1<a1> := NumberField(X^4 + X + 1);
K2<a2> := NumberField(X^6 + X + 5);
K3<a3> := NumberField(CyclotomicPolynomial(9));
K4<a4> := NumberField(X^2 + 3);
K5<a5> := NumberField(X^2 + 108);
// examples K6 and K7 taken from Magma handbook:
K6<a6> := NumberField(X^4 - 420*X^2 + 40000);
K7<a7> := NumberField(X^5 + 5*X^4 - 75*X^3 + 250*X^2 + 65625);
K8<a8> := NumberField(X^3 - 17*X^2 - 8*X - 16);
K9<a9> := NumberField(X^3 + 27*X^2 + 15*X + 29);

// function

// long version, not using the command Order

```

```

zmaxord := function(K)
  n := Degree(K);
  bG := Basis(K);
  bR := stab(bG,K); // basis of a Z-order
  detR := Determinant(MatrixRing(Rationals(),n)!
    [ElementToSequence(bR[i]) : i in [1..n]]);
  P := PrimeDivisors(Integers(!discriminant(bR,K)));
  steps := 0; // only for exercise 45.(2)
  for p in P do
    done := false;
    while not done do
      bRR := stab(jacp(bR,p,K),K);
      detRR := Determinant(MatrixRing(Rationals(),n)!
        [ElementToSequence(bRR[i]) : i in [1..n]]);
      if Abs(detR) gt Abs(detRR) then
        bR := bRR;
        steps += 1; // only for exercise 45.(2)
        detR := detRR;
      else
        done := true;
      end if;
    end while;
  end for;
  return bR, steps; // return steps only for exercise 45.(2)
end function;

// short version, using the command Order

zmaxord := function(K)
  n := Degree(K);
  bG := Basis(K);
  bR := stab(bG,K); // basis of a Z-order
  P := PrimeDivisors(Integers(!discriminant(bR,K)));
  steps := 0; // only for exercise 45.(2)
  for p in P do
    bRR := stab(jacp(bR,p,K),K);
    while Order(bRR) ne Order(bR) do
      steps += 1; // only for exercise 45.(2)
      bR := bRR;
      bRR := stab(jacp(bR,p,K),K);
    end while;
  end for;
  return bR, steps; // return steps only for exercise 45.(2)
end function;

// test

zmaxord(K0);
zmaxord(K1);
zmaxord(K2);
K := K4; a := a4; discriminant([a^i : i in [0..Degree(K)-1]],K);
discriminant(zmaxord(K),K); Discriminant(MaximalOrder(K));

```

```

K := K5; a := a5; discriminant([a^i : i in [0..Degree(K)-1]],K);
      discriminant(zmaxord(K),K); Discriminant(MaximalOrder(K));
K := K8; a := a8; discriminant([a^i : i in [0..Degree(K)-1]],K);
      discriminant(zmaxord(K),K); Discriminant(MaximalOrder(K));
zmaxord(K8);
zmaxord(K9);

```

(2) Wir suchen.

```

P<X> := PolynomialRing(Rationals());
N := 30;
for b in [-N..N] do
  for c in [-N..N] do
    for d in [-N..N] do
      f := X^3 + b*X^2 + c*X + d;
      if IsIrreducible(f) then
        K<a> := NumberField(f);
        bmax,steps := zmaxord(K);
        if steps ge 5 then
          print "steps =", steps, "; f = ", f;
        end if;
        det := Determinant(MatrixRing(Rationals(),3)! [ElementToSequence(x) : x in [1,a,a^2]]);
        detmax := Determinant(MatrixRing(Rationals(),3)! [ElementToSequence(x) : x in bmax]);
        fac := Factorisation(Integers()!(det/detmax));
        if #fac ge 3 then
          print "fac =", [x[1] : x in fac], "; det/detmax = ", det/detmax, "; f = ", f;
        end if;
      end if;
    end for;
  end for;
end for;

```

Alternativ kann man dies zu folgendem verkürzen.

```

P<X> := PolynomialRing(Rationals());
N := 30;
d := 3;
C := CartesianProduct([[-N..N] : i in [0..d-1]]);
for c in C do
  f := X^d + &+[c[i+1] * X^i : i in [0..d-1]];
  if IsIrreducible(f) then
    K<a> := NumberField(f);
    bmax,steps := zmaxord(K);
    if steps ge 5 then
      print "steps =", steps, "; f = ", f;
    end if;
    det := Determinant(MatrixRing(Rationals(),3)! [ElementToSequence(a^i) : i in [0..d-1]]);
    detmax := Determinant(MatrixRing(Rationals(),3)! [ElementToSequence(x) : x in bmax]);
    fac := Factorisation(Integers()!(det/detmax));
    if #fac ge 3 then
      print "fac =", [x[1] : x in fac], "; det/detmax = ", det/detmax, "; f = ", f;
    end if;
  end if;
end for;

```



(2) Es ist

$$|\mathbf{Z}[\zeta]^\# / \mathbf{z}[\zeta] \langle \zeta^q - 1 \rangle| = |\mathbf{Z}[\zeta]^\# / \mathbf{Z}[\zeta]| \cdot |\mathbf{Z}[\zeta] / \mathbf{z}[\zeta] \langle \zeta^q - 1 \rangle| = |\Delta(\mathbf{Z}[\zeta])| \cdot p^q ;$$

cf. (1), Aufgabe 41.(2). Also müssen wir zeigen, daß  $|\mathbf{Z}[\zeta]^\# / \mathbf{z}[\zeta] \langle \zeta^q - 1 \rangle| \stackrel{!}{=} p^{q(p-1)m}$ .

Ist allgemein  $(\alpha_1, \dots, \alpha_n)$  eine  $\mathbf{Z}$ -lineare Basis eines  $\mathbf{Z}$ -Gitters  $G$  und  $(\beta_1, \dots, \beta_n)$  eine  $\mathbf{Z}$ -lineare Basis eines  $\mathbf{Z}$ -Gitters  $H$  in  $K$ , und ist  $G \subseteq H^\#$ , so behaupten wir, daß

$$|H^\# / G| \stackrel{!}{=} |\det((\mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_j))_{i,j})| .$$

Hierzu genügt es zu zeigen, daß  $((\mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_j))_{i,j})$  eine beschreibende Matrix der Einbettung  $G \rightarrow H^\#$  ist. Seien  $\beta_i^* \in K$  so, daß  $\mathrm{Tr}_{K|\mathbf{Q}}(\beta_i^* \beta_j) = \delta_{i,j}$  für  $i, j \in [1, n]$ . Dann ist  $(\beta_1^*, \dots, \beta_n^*)$  eine  $\mathbf{Z}$ -lineare Basis von  $H^\#$ ; cf. Bemerkung 66.(1). Ferner wird in der Tat  $\alpha_i = \sum_j \mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_j) \beta_j^*$  für  $i \in [1, n]$ , da für  $k \in [1, n]$

$$\mathrm{Tr}_{K|\mathbf{Q}}(\sum_j \mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_j) \beta_j^* \beta_k) = \sum_j \mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_j) \mathrm{Tr}_{K|\mathbf{Q}}(\beta_j^* \beta_k) = \sum_j \mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_j) \delta_{j,k} = \mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \beta_k)$$

ist. Dies zeigt die *Behauptung*. Cf. auch Lösung von Aufgabe 41.

Wenden wir diese Behauptung nun auf unsere beiden  $\mathbf{Z}$ -linearen Basen von  $G$  resp.  $H$  an. Für  $i, j \in [0, q-1]$  und  $s, t \in [0, p-2]$  wird

$$\begin{aligned} \mathrm{Tr}_{K|\mathbf{Q}}(\zeta^{s \cdot q + i} \zeta^{-t \cdot q + j}) &= \mathrm{Tr}_{K|\mathbf{Q}}(\zeta^{(s-t+1) \cdot q + (i-j)}) - \mathrm{Tr}_{K|\mathbf{Q}}(\zeta^{(s-t) \cdot q + (i-j)}) \\ &\stackrel{\text{B. 83}}{=} (pq \partial_{(s-t+1) \cdot q + (i-j) + pq\mathbf{Z}, 0} - q \partial_{(s-t+1) \cdot q + (i-j) + q\mathbf{Z}, 0}) \\ &\quad - (pq \partial_{(s-t) \cdot q + (i-j) + pq\mathbf{Z}, 0} - q \partial_{(s-t) \cdot q + (i-j) + q\mathbf{Z}, 0}) \\ &= pq(\partial_{(s-t+1) \cdot q + (i-j) + pq\mathbf{Z}, 0} - \partial_{(s-t) \cdot q + (i-j) + pq\mathbf{Z}, 0}) \\ &= pq \partial_{i,j}(\partial_{s-t+1+p\mathbf{Z}, 0} - \partial_{s-t+p\mathbf{Z}, 0}) \\ &= pq \partial_{i,j}(\partial_{s+1, t} - \partial_{s,t}) . \end{aligned}$$

Beachte hierbei, daß genau dann  $i-j \equiv_q 0$  ist, wenn  $i=j$ ; genau dann  $s-t \equiv_p 0$ , wenn  $s=t$ ; und genau dann  $s-t+1 \equiv_p 0$ , wenn  $s+1=t$ .

Mit der Behauptung ist also  $|\mathbf{Z}[\zeta]^\# / \mathbf{z}[\zeta] \langle \zeta^q - 1 \rangle|$  der Betrag der Determinante einer Blockdiagonalmatrix mit  $q$  Blöcken der Form

$$pq \cdot \begin{pmatrix} -1 & 1 & & & \\ & -1 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & -1 & 1 \\ & & & & & -1 & 1 \\ & & & & & & -1 & 1 \end{pmatrix} \in \mathbf{Q}^{(p-1) \times (p-1)} .$$

Der Betrag der Determinante eines solchen Blocks ist  $(pq)^{p-1}$ .

Es folgt  $|\mathbf{Z}[\zeta]^\# / \mathbf{z}[\zeta] \langle \zeta^q - 1 \rangle| = (pq)^{(p-1)q} = p^{q(p-1)m}$ .

### Aufgabe 50

Da  $\mathrm{char} \mathbf{Q} = 0$ , sind alle auftretenden Körpererweiterungen separabel.

Sei  $F$  die normale Hülle von  $E|\mathbf{Q}$ . Insgesamt ist  $F|E|K|\mathbf{Q}$ . Sei

$$\mathrm{M}_{E|K} := \{ E \xrightarrow{\sigma} F : \sigma \text{ Körpermorphismus, } \sigma(\alpha) = \alpha \text{ für } \alpha \in K \} .$$

Da  $\mathrm{Tr}_{E|K}(\mathcal{O}_E) \subseteq K$  und da  $K \cap \mathcal{O}_F = \mathcal{O}_K$ , genügt es zu zeigen, daß

$$\mathrm{Tr}_{E|K}(\mathcal{O}_E) \stackrel{!}{\subseteq} \mathcal{O}_F ;$$

cf. Bemerkung 53.

Dank Galoistheorie ist

$$\mathrm{Tr}_{E|K}(\alpha) = \sum_{\sigma \in M_{E|K}} \sigma(\alpha)$$

für  $\alpha \in E$ . Also genügt es zu zeigen, daß

$$\sigma(\alpha) \stackrel{!}{\in} \mathcal{O}_E$$

für  $\alpha \in \mathcal{O}_E$  und  $\sigma \in M_{E|K}$ .

Da  $\alpha \in \mathcal{O}_E$ , gibt es ein normiertes Polynom  $f(X) = X^k + \sum_{i \in [0, k-1]} a_i X^i \in \mathbf{Z}[X]$  mit  $f(\alpha) = 0$ . Es wird

$$\begin{aligned} f(\sigma(\alpha)) &= \sigma(\alpha)^k + \sum_{i \in [0, k-1]} a_i \sigma(\alpha)^i \\ &= \sigma(\alpha)^k + \sum_{i \in [0, k-1]} \sigma(a_i) \sigma(\alpha)^i \\ &= \sigma(\alpha^k + \sum_{i \in [0, k-1]} a_i \alpha^i) \\ &= \sigma(f(\alpha)) \\ &= \sigma(0) \\ &= 0, \end{aligned}$$

und folglich  $\sigma(\alpha) \in \mathcal{O}_E$ .

### Aufgabe 51

(1) Sei  $\varphi : \mathbf{Z}[\alpha] \rightarrow \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$ ,  $\xi \mapsto \xi + p\mathbf{Z}[\alpha]$  die Restklassenabbildung. Es ist

$$\mathrm{Jac}_p(\mathbf{Z}[\alpha]) = \varphi^{-1}(\{\xi + p\mathbf{Z}[\alpha] \in \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] : \text{es gibt ein } m \geq 0 \text{ mit } (\xi + p\mathbf{Z}[\alpha])^m = 0\}),$$

i.e. es ist  $\mathrm{Jac}_p(\mathbf{Z}[\alpha])$  das Urbild der Teilmenge der nilpotenten Elemente in  $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$ . Wir müssen zeigen, daß diese gegeben ist durch  $\langle p, g(\alpha) \rangle / p\mathbf{Z}[\alpha] \subseteq \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$ .

Nun ist

$$\begin{array}{ccccccc} \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] & \xleftarrow{\sim} & \mathbf{Z}[X]/\langle p, \mu_{\alpha, \mathbf{Q}}(X) \rangle & \xrightarrow{\sim} & \mathbf{F}_p[X]/\langle \bar{\mu}_{\alpha, \mathbf{Q}}(X) \rangle & \xrightarrow{\sim} & \prod_{i \in [1, k]} \mathbf{F}_p[X]/\langle \bar{f}_i(X)^{e_i} \rangle \\ f(\xi) + p\mathbf{Z}[\alpha] & \longleftarrow & f(X) + \langle p, \mu_{\alpha, \mathbf{Q}}(X) \rangle & \longmapsto & \bar{f}(X) + \langle \bar{\mu}_{\alpha, \mathbf{Q}}(X) \rangle & \longmapsto & (\bar{f}(X) + \langle \bar{f}_i(X)^{e_i} \rangle). \end{array}$$

Für  $i \in [1, k]$  ist in  $\mathbf{F}_p[X]/\langle \bar{f}_i(X)^{e_i} \rangle$  die Teilmenge der nilpotenten Elemente gegeben durch  $\langle \bar{f}_i(X) \rangle / \langle \bar{f}_i(X)^{e_i} \rangle$ .

Transportiert mit dem dritten Isomorphismus zeigt dies, daß in  $\mathbf{F}_p[X]/\langle \bar{\mu}_{\alpha, \mathbf{Q}}(X) \rangle$  die Teilmenge der nilpotenten Elemente gegeben ist durch  $\langle \bar{g}(X) \rangle / \langle \bar{\mu}_{\alpha, \mathbf{Q}}(X) \rangle$ .

Transportiert mit dem zweiten Isomorphismus zeigt dies, daß in  $\mathbf{Z}[X]/\langle p, \mu_{\alpha, \mathbf{Q}}(X) \rangle$  die Teilmenge der nilpotenten Elemente gegeben ist durch  $\langle p, g(X) \rangle / \langle p, \mu_{\alpha, \mathbf{Q}}(X) \rangle$ .

Transportiert mit dem ersten Isomorphismus zeigt dies, daß in  $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$  die Teilmenge der nilpotenten Elemente gegeben ist durch  $\langle p, g(\alpha) \rangle / p\mathbf{Z}[\alpha]$ .

(2) Es genügt zu zeigen, daß  $\mathrm{Stab}(\mathrm{Jac}_p(\mathbf{Z}[\alpha])) \stackrel{!}{=} \mathbf{Z}[\alpha]$ ; cf. Satz 79.(2).

Hierfür genügt es zu zeigen, daß  $\mathrm{Stab}(\mathrm{Jac}_p(\mathbf{Z}[\alpha])) \stackrel{!}{\subseteq} \mathbf{Z}[\alpha]$ .

Sei  $\xi \in \mathbf{Q}(\alpha)$  mit  $\xi \in \mathrm{Stab}(\mathrm{Jac}_p(\mathbf{Z}[\alpha])) \stackrel{(1)}{=} \mathrm{Stab}(\langle p, g(\alpha) \rangle)$  gegeben. Wir haben zu zeigen, daß  $\xi \stackrel{!}{\in} \mathbf{Z}[\alpha]$ .

Wegen  $p \in \langle p, g(\alpha) \rangle$  ist  $\xi p \in \langle p, g(\alpha) \rangle \subseteq \mathbf{Z}[\alpha]$ . Also ist  $\xi = p^{-1}b(\alpha)$  für ein  $b(X) \in \mathbf{Z}[X]$ .

Es genügt zu zeigen, daß  $\bar{\mu}_{\alpha, \mathbf{Q}}(X)$  ein Teiler von  $\bar{b}(X)$  ist. Denn dann können wir  $b(X) = c(X) \mu_{\alpha, \mathbf{Q}}(X) + p d(X)$  mit  $c(X), d(X) \in \mathbf{Z}[X]$  schreiben, und es ergibt sich

$$\xi = p^{-1}b(\alpha) = p^{-1}(c(\alpha) \mu_{\alpha, \mathbf{Q}}(\alpha) + p d(\alpha)) = d(\alpha) \in \mathbf{Z}[\alpha].$$

Da  $\bar{\mu}_{\alpha, \mathbf{Q}}(X) = \bar{f}_1(X)^{e_1} \cdots \bar{f}_k(X)^{e_k}$ , ist also zu zeigen, daß  $\bar{f}_i(X)^{e_i}$  ein Teiler von  $\bar{b}(X)$  ist für  $i \in [1, k]$ .

Da  $b(\alpha) = \xi p \in \langle p, g(\alpha) \rangle$ , ist  $b(X) \in \langle p, g(X), \mu_{\alpha, \mathbf{Q}}(X) \rangle$  und also  $\bar{b}(X) \in \langle \bar{g}(X), \bar{\mu}_{\alpha, \mathbf{Q}}(X) \rangle = \langle \bar{g}(X) \rangle$ , letzteres, da  $\bar{\mu}_{\alpha, \mathbf{Q}}(X)$  ein Vielfaches von  $\bar{g}(X)$  ist. Da  $\bar{g}(X) := \bar{f}_1(X) \cdots \bar{f}_k(X)$ , ist  $\bar{f}_i(X)$  ein Teiler von  $\bar{b}(X)$  für  $i \in [1, k]$ .

Sei  $i \in [1, k]$  mit  $e_i \geq 2$  gegeben. Es bleibt zu zeigen, daß  $\bar{f}_i(X)^{e_i}$  ein Teiler von  $\bar{b}(X)$  ist.

Da wegen  $g(\alpha) \in \langle p, g(\alpha) \rangle$  auch  $p^{-1}b(\alpha)g(\alpha) = \xi g(\alpha) \in \langle p, g(\alpha) \rangle$  ist, ist  $b(\alpha)g(\alpha) \in \langle p^2, p g(\alpha) \rangle$ , mithin

$$b(X)g(X) \in \langle p^2, p g(X), \mu_{\alpha, \mathbf{Q}}(X) \rangle = \langle p^2, p g(X), g(X)h(X) - p a(X) \rangle.$$

Vorsicht,  $p^{-1}b(X)g(X)$  kann nicht als Urbild von  $p^{-1}b(\alpha)g(\alpha) \in \mathbf{Z}[\alpha]$  unter  $\mathbf{Z}[X] \rightarrow \mathbf{Z}[\alpha], X \mapsto \alpha$ , dienen, da nicht bekannt ist, ob es in  $\mathbf{Z}[X]$  liegt.

Wir schreiben dementsprechend

$$(*) \quad b(X)g(X) = p^2 r(X) + p g(X) s(X) + g(X) h(X) t(X) - p a(X) t(X)$$

mit  $r(X), s(X), t(X) \in \mathbf{Z}[X]$ . Es folgt  $\bar{b}(X)\bar{g}(X) = \bar{g}(X)\bar{h}(X)\bar{t}(X)$ , also  $\bar{b}(X) = \bar{h}(X)\bar{t}(X)$ , und daher

$$(**) \quad b(X) = h(X)t(X) + p u(X)$$

für ein  $u(X) \in \mathbf{Z}[X]$ . Setzen wir  $(**)$  in  $(*)$  ein, so wird daraus

$$h(X)t(X)g(X) + p u(X)g(X) = p^2 r(X) + p g(X) s(X) + g(X) h(X) t(X) - p a(X) t(X),$$

i.e.

$$u(X)g(X) = p r(X) + g(X) s(X) - a(X) t(X),$$

woraus

$$(\bar{u}(X) - \bar{s}(X))\bar{g}(X) = -\bar{a}(X)\bar{t}(X)$$

folgt. Wegen  $e_i \geq 2$  ist nach Voraussetzung  $\bar{f}_i(X)$  kein Teiler von  $\bar{a}(X)$ . Da  $\bar{f}_i(X)$  irreduzibel ist, folgt, daß  $\bar{f}_i(X)$  ein Teiler von  $\bar{t}(X)$  ist. Wir schreiben  $\bar{t}(X) = \bar{f}_i(X)\bar{v}(X)$  für ein  $v(X) \in \mathbf{Z}[X]$ . Mit  $(**)$  wird

$$\bar{b}(X) = \bar{h}(X)\bar{t}(X) = \bar{f}_1(X)^{e_1-1} \cdots \bar{f}_k(X)^{e_k-1} \bar{f}_i(X)\bar{v}(X).$$

Es folgt, daß  $\bar{f}_i(X)^{e_i}$  ein Teiler von  $\bar{b}(X)$  ist.

(3) Das in (2) bearbeitete Kriterium stammt von R. Dedekind, daher der Name der folgenden Funktion.

Das in (2) als hinreichend erkannte Kriterium ist auch notwendig. Dies wollen wir hier aber nicht behandeln; cf. [3, Th. 6.1.4.(2)].

Der einzige Nachteil dieses Kriteriums ist, daß es nur auf Ordnungen angewandt werden kann, die von einem Element erzeugt werden.

Wir verwenden **discriminant** aus Aufgabe 47.(1).

```

// test data

PInt<X> := PolynomialRing(Integers());

mu := X^6 + X + 1;
mu1 := X^7 - X^5 + X^2 - 2;

// function, needs a normed polynomial with integer coefficients

is_zmaxord_by_dedekind := function(mu)
  if mu eq 0 or LeadingCoefficient(mu) ne 1 or not IsIrreducible(mu) or
    not &and[IsIntegral(x) : x in Coefficients(mu)] then
    print "The given polynomial is not a minimal polynomial.";
    return false;
  end if;
  PInt<X> := PolynomialRing(Integers());
  d := Degree(mu);
  if d eq 1 then // for Magma-technical reasons
    return true;
  end if;
  K<a> := NumberField(mu);
  b := [a^i : i in [0..d-1]];
  PrDiv := PrimeDivisors(Integers()!discriminant(b,K));
  for p in PrDiv do
    PMod<Y> := PolynomialRing(GF(p));
    f := Factorisation(PMod!mu);
    gh := &*[PInt!(x[1]))^x[2] : x in f];
    a := (mu - gh) div p;
    if &or[((PMod!a) mod x[1] eq 0) and (x[2] ge 2) : x in f] then
      return false;
      break;
    end if;
  end for;
  return true;
end function;

// test

is_zmaxord_by_dedekind(mu);
is_zmaxord_by_dedekind(mu1);

```

- (4) Schreibe  $\zeta := \zeta_{p^m}$ . Die Diskriminante von  $\mathbf{Z}[\zeta]$  ist eine Potenz von  $p$ ; cf. Lemma 84. Also haben wir zu zeigen, daß  $p$  kein Teiler von  $|\mathcal{O}_{\mathbf{Q}(\zeta)}/\mathbf{Z}[\zeta]|$  ist.

Es ist  $\mathbf{Z}[\zeta] = \mathbf{Z}[\zeta - 1]$ . Setzen wir  $\alpha := \zeta - 1$ , so bleibt die Voraussetzung von (2) zu zeigen.

Es ist  $\mu_{\alpha, \mathbf{Q}}(X) = \Phi_{p^m}(X + 1) \equiv_p X^{p^{m-1}(p-1)}$ ; cf. Beweis zu Bemerkung 85. In der obigen Bezeichnung wird also  $k = 1$ ,  $f_1(X) = X$  und  $e_1 = p^{m-1}(p-1)$ .

Folglich wird, in der obigen Bezeichnung,  $a(X) = (\Phi_{p^m}(X + 1) - X^{p^{m-1}(p-1)})/p$ . Nun ist  $a(0) = \Phi_{p^m}(0 + 1)/p = 1$ , und also  $\bar{a}(X)$  nicht durch  $X$  teilbar. Damit ist die für (2) gemachte Voraussetzung erfüllt.

Cf. Lemma 86.

## Literatur

- [1] BERGEMANN, C., *Cantor-Zassenhaus split*, [planetmath.org/encyclopedia/DistinctDegreeFactorization.html](http://planetmath.org/encyclopedia/DistinctDegreeFactorization.html), 2006.
- [2] BOSMA, W.; CANNON, J.J.; FIEKER, C.; STEEL, A. (eds.), *Handbook of Magma functions*, Ed. 2.16, 2010; cf. [magma.maths.usyd.edu.au](http://magma.maths.usyd.edu.au), [magma.maths.usyd.edu.au/calc](http://magma.maths.usyd.edu.au/calc).
- [3] COHEN, H., *A Course in Computational Algebraic Number Theory*, Springer GTM 138, 1993.
- [4] GALLOT, Y., *Cyclotomic Polynomials and Prime Numbers*, manuscript, 2000.
- [5] KIMMERLE, W., *Computeralgebra*, Vorlesung, 1993.
- [6] KOCH, H., *Zahlentheorie*, Vieweg, 1997.
- [7] NEUKIRCH, J., *Algebraische Zahlentheorie*, Springer, 1992.
- [8] SERRE, J.-P., *Linear Representations of Finite Groups*, Springer GTM 42, 1971.