

# Übungen zur Algebra I

F. Lorenz, F. Lemmermeyer

2. April 2007

# Inhaltsverzeichnis

Übungen zu Kapitel 1	2
Übungen zu Kapitel 2	7
Übungen zu Kapitel 3	9
Übungen zu Kapitel 4	13
Übungen zu Kapitel 5	22
Übungen zu Kapitel 6	29
Übungen zu Kapitel 7	33
Übungen zu Kapitel 8	35
Übungen zu Kapitel 9	48
Übungen zu Kapitel 10	52
Übungen zu Kapitel 11	57
Übungen zu Kapitel 12	59
Übungen zu Kapitel 13	61
Übungen zu Kapitel 14	63
Übungen zu Kapitel 15	65
Übungen zu Kapitel 16	66

# Übungen zu Kapitel 1

- 1) Nach F1.2 wurde behauptet, dass  $\mathbb{Q}$  der kleinste Teilkörper von  $\mathbb{C}$  ist. Ist dies klar?

Jeder Teilkörper  $K$  von  $\mathbb{C}$  enthält 0 und 1. Da Körper abgeschlossen bezüglich der Addition sind, muß  $K$  sogar  $\mathbb{Z}$  enthalten. Da  $K$  mit jedem Element  $\neq 0$  auch dessen Inverses enthält, sowie deren ganzzahlige Vielfache, muss  $\mathbb{Q} \subseteq K$  sein, d.h. jeder Teilkörper von  $\mathbb{C}$  enthält  $\mathbb{Q}$ . Da  $\mathbb{Q}$  bereits ein Körper ist, folgt die Behauptung.

- 2) Warum folgt aus F1.3, dass  $\sqrt{m} \in \star M$  für jedes  $m \in \mathbb{Z}$  ist? Dasselbe Argument zeigt auch  $\sqrt{a + b\sqrt{m}} \in \star M$  für  $a, b \in \mathbb{Z}$ , ähnliches gilt für höher verschachtelte Quadratwurzeln.

Da  $0, 1 \in M$  sind, enthält  $M$  wegen (1.5) ganz  $\mathbb{N}$ , und wegen (1.4) dann sogar ganz  $\mathbb{Z}$ . Da  $M$  nach F1.3 quadratisch abgeschlossen ist, ist mit  $m \in M$  für alle  $m \in \mathbb{Z}$  auch immer  $\sqrt{m} \in M$ .

Nach (1.6) ist mit  $\sqrt{m} \in M$  und  $b \in \mathbb{Z}$  auch  $b\sqrt{m} \in M$ , sowie wegen (1.5) auch  $a + b\sqrt{m} \in M$  usw.

- 3) Seien  $E_1/K$  und  $E_2/K$  Körpererweiterungen, und seien  $E_1$  und  $E_2$  isomorph als  $K$ -Vektorräume. Sind  $E_1$  und  $E_2$  dann auch als Körper isomorph?

Nein, es gibt keinen Isomorphismus  $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ . Da für Ringhomomorphismen  $\phi$  nämlich  $\phi(1) = 1$  gilt, muss auch  $\phi(2) = \phi(1 + 1) = 2$  sein (tatsächlich bleibt ganz  $\mathbb{Q}$  unter  $\phi$  fest). Sei nun  $\phi(\sqrt{2}) = a + b\sqrt{3}$  für geeignete  $a, b \in \mathbb{Q}$ . Dann ist  $2 = \phi(2) = \phi(\sqrt{2})^2 = (a + b\sqrt{3})^2$ , und daraus folgt sofort  $b = 0$  und  $a^2 = 2$ , also ein Widerspruch zur Irrationalität von  $\sqrt{2}$ .

- 4) Zeige, dass man den Winkel  $\phi = \frac{\pi}{2}$  mit Zirkel und Lineal dreiteilen kann. Zeige auch  $\mathbb{Q}(e^{i\phi}) = \mathbb{Q}(i)$  und  $\mathbb{Q}(e^{i\phi/3}) = \mathbb{Q}(i, \sqrt{-3})$ ; damit folgt die Behauptung auch aus Satz 1.2.

Eine 6-Teilung des Kreises liefert den Winkel  $\frac{\pi}{3}$ ; damit ist dann  $\frac{\pi}{2} - \frac{\pi}{3} = \frac{\pi}{6}$ .

- 5) Um  $\mathbb{Q}(\sqrt{2}) : \mathbb{Q} = 2$  zu zeigen muss man nachweisen, dass  $\sqrt{2}$  nicht in  $\mathbb{Q}$  liegt, also irrational ist. Wir werden dies (und viel mehr) später direkt aus F5.7 ablesen können. Der bekannte Standardbeweis benutzt die eindeutige Primfaktorzerlegung in  $\mathbb{Z}$ , die wir in Kapitel 4 herleiten werden. Ein Beweis, der ganz ohne Hilfsmittel auskommt, ist der folgende: Ist  $\sqrt{2}$  rational, so gibt es ein  $q \in \mathbb{N}$  mit  $q\sqrt{2} \in \mathbb{N}$ , und wir dürfen annehmen, dass  $q$  die minimale solche Zahl ist. Dann ist  $r := q(\sqrt{2} - 1) < q$  ebenfalls eine natürliche Zahl, und  $r\sqrt{2} = 2q - q\sqrt{2}$  ist wieder ganz. Dies widerspricht der Minimalität von  $q$ .

a) Ergänze die Details.

b) Zeige allgemein, dass  $\sqrt{m}$  für  $m \in \mathbb{N}$  genau dann rational ist, wenn  $m = n^2$  für ein  $n \in \mathbb{N}$  gilt.

a) Sei  $\sqrt{2} = \frac{p}{q}$  mit minimalem  $q \in \mathbb{N}$ . Dann ist  $\sqrt{2} - 1 = \frac{p-q}{q}$  mit  $p - q < q$  (aus  $p^2 = 2q^2 < 4q^2$  folgt sofort  $p < 2q$ ), sowie  $\frac{q}{p-q} = \frac{1}{\sqrt{2}-1} = \sqrt{2} + 1$ , also  $\sqrt{2} = \frac{2q-p}{p-q}$ . Wegen  $p - q < q$  widerspricht diese Darstellung von  $\sqrt{2}$  allerdings der Minimalität von  $q$ .

b) Sei  $m$  kein Quadrat in  $\mathbb{N}$ ; dann gibt es eine natürliche Zahl  $n$  mit  $n^2 < m < (n+1)^2$ , also mit  $0 < \sqrt{m} - n < 1$ . Ist  $\sqrt{m}$  rational, so können wir  $\sqrt{m} = \frac{p}{q}$  mit minimalem  $q \in \mathbb{N}$  schreiben. Dann ist  $r := q(\sqrt{m} - n)$  ebenfalls ganz, und wegen  $0 < \sqrt{m} - n < 1$  ist  $0 < r < q$ . Nun ist aber  $r\sqrt{m} = q(\sqrt{m} - n)\sqrt{m} = mq - nq\sqrt{m}$  ganz, da  $mq$  und  $q\sqrt{m}$  ganz sind; dies widerspricht aber der Minimalität von  $q$ .

- 6) Der eben gegebene Beweis lässt sich verallgemeinern: Sei  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$  mit ganzzahligen  $a_0, a_1, \dots, a_{n-1}$ . Ist  $\alpha$  eine Nullstelle von  $f$ , so zeige man, dass  $\alpha$  entweder eine ganze Zahl oder irrational ist. Insbesondere ist z.B.  $\sqrt[3]{2}$  irrational.

Für nichtreelle  $\alpha$  gibt es nichts zu zeigen. Andernfalls gibt es eine kleinste natürliche Zahl  $q$ , sodass  $q\alpha^j$  für alle  $j = 1, 2, \dots, n-1$  ganzzahlig ist. Ist  $\alpha$  keine ganze Zahl, so gibt es ein  $k \in \mathbb{Z}$  mit  $k < \alpha < k+1$ . Jetzt ist  $p = q(\alpha - k)$  eine ganze Zahl mit  $0 < p < q$ . Allerdings ist nun  $p\alpha^j = q\alpha^{j+1} - kq\alpha^j$  ganzzahlig für alle  $j$  mit  $0 \leq j < n-1$ , und  $p\alpha^{n-1} = q\alpha^n - kq\alpha^{n-1}$  ist ganz, weil  $q\alpha^n = -q(a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0)$  und  $q\alpha^{n-1}$  ganzzahlig sind. Damit haben wir aber wieder einen Widerspruch zur Minimalität von  $q$ .

- 7) Zeige: ist  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$  mit ganzzahligen  $a_0, a_1, \dots, a_{n-1}$ , und gilt  $f(a) = 0$  für ein  $a \in \mathbb{Z}$ , dann ist  $a \mid a_0$ .

Aus  $0 = f(a) = a^n + a_{n-1}a^{n-1} + \dots + a_1a + a_0$  folgt

$$a_0 = -a(a_1 + \dots + a_{n-1}a^{n-2} + a^{n-1}).$$

- 8) Zeige, dass  $\sqrt[3]{2}$  in keiner quadratischen Erweiterung von  $\mathbb{Q}$  enthalten ist.

Angenommen, es wäre  $\sqrt[3]{2} = a + b\sqrt{m}$  für ein  $m \in \mathbb{Z}$ . Dann folgt  $a^3 + 3ab^2m + (3a^2b + b^3)\sqrt{m} = 2$ . Dies geht nur für  $3a^2b + b^3 = 0$  und  $a^3 + 3ab^2m = 2$ . Die erste Gleichung gibt  $b = 0$  oder  $3a^2 + b^2 = 0$ . Also ist in jedem Fall  $b = 0$ , und dies liefert  $a^3 = 2$ , was der Irrationalität von  $\sqrt[3]{2}$  widerspricht.

- 9) Sei  $\omega = \sqrt[3]{2}$  die reelle Kubikwurzel der 2,  $\rho = \frac{-1+\sqrt{-3}}{2}$  eine primitive dritte Einheitswurzel. Zeige, dass die Körper  $\mathbb{Q}(\omega)$  und  $\mathbb{Q}(\rho\omega)$  isomorph, aber nicht gleich sind.

Jedes Element  $\alpha \in \mathbb{Q}(\omega)$  hat die Form  $\alpha = a + b\omega + c\omega^2$  mit  $a, b, c \in \mathbb{Q}$ . Ähnlich kann man jedes Element  $\beta \in \mathbb{Q}(\rho\omega)$  in der Form  $\beta = a + b\rho\omega + c\rho^2\omega^2$  darstellen. Jetzt rechnet man nach, dass die Abbildung

$$a + b\omega + c\omega^2 \mapsto a + b\rho\omega + c\rho^2\omega^2$$

ein Ringhomomorphismus ist, und da sich die Bijektivität ganz von allein zeigt, folgt damit die Behauptung.

- 10) Führe die in (1.14) und (1.15) skizzierte „Berechnung“ von  $\zeta = e^{2\pi i/5}$  explizit durch und weise nach, dass

$$\zeta = \frac{1}{4} \left( -1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}} \right)$$

gilt. Zeige weiter, dass damit

$$\cos \frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4}, \quad \sin \frac{2\pi}{5} = \frac{1}{4} \sqrt{10 + 2\sqrt{5}}$$

ist.

Mit  $z = \zeta + \zeta^{-1}$  wird  $z^2 + z - 1 = 0$ , also  $z = \frac{-1 \pm \sqrt{5}}{2}$ . Aus  $\zeta^2 - z\zeta + 1 = 0$  erhält man dann  $\zeta = \frac{z \pm \sqrt{z^2 - 4}}{2}$ . Da  $\zeta$  und  $\zeta^{-1}$  positiven Realteil haben, muss  $z > 0$ , also  $z = \frac{-1 + \sqrt{5}}{2}$  sein.

Damit ist  $z^2 - 4 = -\frac{5+\sqrt{5}}{2}$ , folglich

$$\zeta = \frac{1}{4} \left( -1 + \sqrt{5} \pm i\sqrt{10 + 2\sqrt{5}} \right).$$

Dass hierbei das positive Vorzeichen richtig ist, ersehen wir aus der Beobachtung, dass  $\zeta$  positiven Imaginärteil hat. Die restlichen Behauptungen ergeben sich jetzt aus der Eulerschen Formel  $e^{it} = \cos t + i \sin t$ .

- 11) Sei  $\zeta = e^{2\pi i/7}$  eine primitive siebte Einheitswurzel. Setze  $\alpha = \zeta + \zeta^{-1}$  und  $\beta = \zeta + \zeta^2 + \zeta^4$ .

- a) Zeige  $\beta^2 + \beta + 2 = 0$ , und genauer, dass  $\beta = \frac{1}{2}(-1 + i\sqrt{7})$  ist.
- b) Zeige  $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$ .
- c) Zeige  $\mathbb{Q}(\alpha) : \mathbb{Q} = 3$ .
- d) Zeige, dass das regelmäßige Siebeneck nicht mit Zirkel und Lineal konstruierbar ist.

- a) Wir finden

$$\begin{aligned} \beta^2 &= (\zeta + \zeta^2 + \zeta^4)^2 = \zeta^2 + \zeta^4 + \zeta^8 + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 \\ &= 2(\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) - (\zeta + \zeta^2 + \zeta^4) \\ &= -2 - \beta. \end{aligned}$$

Hier haben wir benutzt, dass  $S = \sum_{a=0}^{p-1} \zeta_p^a = 0$  ist; dies sieht man am einfachsten ein, indem man nachrechnet, dass  $\zeta S = S$  ist.

Damit ist  $\beta = \frac{-1 \pm i\sqrt{7}}{2}$  für eine geeignete Wahl der Vorzeichen. Eine kleine Zeichnung am Einheitskreis zeigt aber sofort, dass der Imaginärteil von  $\beta$  positiv ist und damit  $\beta = \frac{1}{2}(-1 + i\sqrt{7})$  gelten muss.

- b) Wie eben finden wir

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

- c) Dies folgt aus den Übungen 1.6 und folgendem Resultat: Sei  $f(X) = X^3 + a_2X^2 + a_1X + a_0$  ein Polynom mit ganzzahligen Koeffizienten und ohne ganzzahlige Nullstelle. Ist dann  $\alpha \in \mathbb{C}$  eine Nullstelle von  $f$ , so gilt  $\mathbb{Q}(\alpha) : \mathbb{Q} = 3$ .

Die Elemente  $1, \alpha$  sind über  $\mathbb{Q}$  unabhängig, da  $\alpha$  nach Übung 1.6 irrational ist. Wäre  $\alpha^2 = r\alpha + s$  mit  $r, s \in \mathbb{Q}$ , so würde  $f(X) = (X^2 - rX - s)(X - t)$  für ein

$t \in \mathbb{Q}$  folgen: Polynomdivision zeigt nämlich  $f(X) = (X^2 - rX - s)(X - t) + g(X)$  für ein Polynom  $g$  vom Grad  $\leq 1$ ; Einsetzen von  $\alpha$  gibt  $g(\alpha) = 0$ , und aus der Irrationalität von  $\alpha$  folgt dann, dass  $g = 0$  sein muss.

Andererseits zeigt  $f(X) = (X^2 - rX - s)(X - t)$ , dass  $f$  eine rationale Nullstelle hat; nach Übung 1.6 muss  $t$  ganzzahlig sein, was aber unserer Annahme widerspricht.

Also sind  $1, \alpha, \alpha^2$  linear unabhängig über  $\mathbb{Q}$ . Wegen  $\alpha^3 = -a_2\alpha^2 - a_1\alpha - a_0$  lässt sich aber jedes Element von  $\mathbb{Q}(\alpha)$  als  $\mathbb{Q}$ -Linearkombination von  $1, \alpha, \alpha^2$ , und dies zeigt  $\mathbb{Q}(\alpha) : \mathbb{Q} = 3$ .

d) Sei  $\alpha$  konstruierbar; dann liegt  $\alpha$  nach F1.8 in einer Erweiterung  $E/\mathbb{Q}$  von Zweierpotenzgrad. Die Gradformel F1.7 besagt andererseits, dass  $E : \mathbb{Q}$  durch  $\mathbb{Q}(\alpha) : \mathbb{Q} = 3$  teilbar ist: Widerspruch.

- 12) *Zeige entsprechend, dass das regelmäßige Neuneck nicht mit Zirkel und Lineal konstruierbar ist (auch hier genügt  $\zeta + \zeta^{-1}$  einer kubischen Gleichung).*

Sei  $\zeta = e^{2\pi i/9}$  und  $\alpha = \zeta + \zeta^{-1}$ . Dann finden wir

$$\alpha^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = \rho + \rho^{-1} + 3\alpha,$$

wo  $\rho = \zeta^3 = e^{2\pi i/3}$  ist. Wegen  $1 + \rho + \rho^2 = 0$  ist  $\rho + \rho^{-1} = -1$ , und wir finden  $\alpha^3 = 3\alpha - 1$ . Also ist  $\alpha$  eine Nullstelle von  $X^3 - 3X + 1$ . Wie in der vorangegangenen Übung zeigt man jetzt  $\mathbb{Q}(\alpha) : \mathbb{Q} = 3$ , und dass das regelmäßige Neuneck nicht mit Zirkel und Lineal konstruierbar ist.

# Übungen zu Kapitel 2

- 1) Sei  $E/\mathbb{Q}$  eine algebraische Körpererweiterung und  $z \in \mathbb{R}$  transzendent über  $\mathbb{Q}$ . Ist dann die Erweiterung  $E(z)/\mathbb{Q}(z)$  ebenfalls algebraisch?

Ja. Sei nämlich  $f = \sum_{j=0}^n \alpha_j z^j \in E(z)$ . Dann ist  $\mathbb{Q}(z, f) \subseteq \mathbb{Q}(z, \alpha_0, \alpha_1, \dots, \alpha_n)$ , und dieser Körper ist algebraisch über  $\mathbb{Q}(z)$ . Also ist jedes  $f \in E(z)$  algebraisch über  $\mathbb{Q}(z)$ .

- 2) Gibt es einen Teilkörper  $K$  von  $\mathbb{R}$  mit der Eigenschaft, dass  $K(\pi) : K = 2$  ist?

Ja. Sei  $K = \mathbb{Q}(\pi^2)$ . Da  $\pi$  transzendent ist, ist  $K(\pi) = K(\sqrt{\pi^2})$  eine quadratische Erweiterung.

- 3) Sei  $E/K$  eine algebraische Körpererweiterung und  $K$  abzählbar. Ist dann auch  $E$  abzählbar?

Ja. Jedes Element von  $L$  ist Nullstelle eines Polynoms  $f \in K[X]$ ; es genügt daher zu zeigen, dass alle solchen Polynome abzählbar sind. Wir fixieren nun eine Abzählung von  $K$  und setzen  $c(a) = n$  für  $a \in K$ , wenn  $a$  der  $n$ -te Term in dieser Abzählung ist. Für ein Polynom  $f = \sum_{i=0}^n a_i X^i$  definieren wir jetzt dessen Höhe durch  $h(f) = n + \sum v(a_i)$ . Jetzt überzeugt man sich leicht davon, dass es zu jedem  $m \in \mathbb{N}$  nur endlich viele Polynome  $f \in K[X]$  mit Höhe  $h(f) = m$  gibt. Man kann also die Polynome abzählen, indem man nacheinander diejenigen mit Höhe 1, 2, 3, ... aufschreibt.

- 4) Sei  $E/K$  eine Körpererweiterung und  $E$  abzählbar. Ist dann  $E/K$  algebraisch?

Nein. Sei  $x \in \mathbb{R}$  transzendent über  $\mathbb{Q}$  (z.B.  $x = \pi$ ) und  $E = \mathbb{Q}(x)$ . Da sich jedes Element von  $E$  als Quotient zweier Polynome schreiben lässt und diese abzählbar sind, ist auch  $E$  abzählbar.

- 5) Es seien  $E_1/K$  und  $E_2/K$  Teilerweiterungen einer endlichen Erweiterung  $E/K$ . Sind  $E_1 : K$  und  $E_2 : K$  teilerfremd, dann gilt  $E_1 \cap E_2 = K$ .



Sei  $L = E_1 \cap E_2$ . Die Gradformel besagt, dass  $L : K$  Teiler von  $E_1 : K$  und  $L_2 : K$  ist; da diese beiden Zahlen teilerfremd sind, muss  $L : K = 1$  und damit  $L = K$  sein.

- 6) *Der folgende Beweis der Irrationalität von  $\sqrt{2}$  benutzt etwas Algebra und Analysis: Sei  $\alpha = \sqrt{2} - 1$ ; aus  $0 < \alpha < 1$  folgt  $\lim_{k \rightarrow \infty} \alpha^k = 0$ . Wäre  $\sqrt{2} = \frac{p}{q}$ , so hätten wir, weil  $\mathbb{Z}[\sqrt{2}]$  ein Ring ist,  $0 < \alpha^k = a + b\sqrt{2} = \frac{aq + bp}{q}$ , und die rechte Seite durch  $\frac{1}{q}$  ist nach unten beschränkt.*

*Ergänze die Details und zeige, dass man mit dieser Methode einen neuen Beweis von Übung 1.6 erhält.*

Wir führen den Beweis zuerst für  $n$ -te Wurzeln. Sei dazu  $m \in \mathbb{N}$  keine  $n$ -te Potenz und  $\alpha = \sqrt[n]{m} - a$ , wo  $a$  die natürliche Zahl mit  $0 < \alpha < 1$  ist. Dann gilt sicher  $\lim_{k \rightarrow \infty} \alpha^k = 0$ .

Nun ist  $\alpha$  ein Element des Rings  $\mathbb{Z}[\alpha]$ , somit auch  $\alpha^k = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$  für von  $k$  abhängige ganze Zahlen  $a_j$ . Wäre  $\alpha = \frac{p}{q}$  rational, so auch  $\alpha^k$ : es ist nämlich

$$\alpha^k = a_0 + a_1 \frac{p}{q} + \dots + a_{n-1} \left(\frac{p}{q}\right)^{n-1} = \frac{a_0 q^{n-1} + a_1 p q^{n-2} + \dots + p^{n-1}}{q^{n-1}}.$$

Im Nenner des Bruchs steht eine ganze Zahl; wegen  $\alpha^k > 0$  muss diese  $\geq 1$ , somit  $\alpha^k \geq q^{1-n}$  sein. Lässt man jetzt  $k \rightarrow \infty$  gehen, erhält man den Widerspruch  $0 = \lim \alpha^k \geq q^{1-n}$ .

Sei jetzt  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$  mit ganzzahligen Koeffizienten  $a_0, a_1, \dots, a_{n-1}$ . Wir haben zu zeigen: ist  $\alpha$  eine Nullstelle von  $f$ , so ist  $\alpha$  entweder eine ganze Zahl oder irrational.

Ist  $\alpha$  rational und z.B.  $q\alpha \in \mathbb{Z}$  für ein  $q \in \mathbb{N}$ , so ist  $q^k \alpha^k \in \mathbb{Z}$  für  $k = 1, 2, \dots, n-1$ . Für  $k \geq n$  ist  $\alpha^k$  eine  $\mathbb{Z}$ -Linearkombination von  $1, \alpha, \dots, \alpha^{n-1}$  und damit  $q^{n-1} \alpha^k \in \mathbb{Z}$  für alle  $k \in \mathbb{N}$ .

Ist  $\alpha$  keine ganze Zahl, so gibt es ein  $a \in \mathbb{Z}$  mit  $0 < \alpha - a < 1$ . Mit  $\beta = \alpha - a$  ist dann  $q^{n-1} \beta^k$  ganz für alle  $k \in \mathbb{N}$ ; weil aber  $\beta^k \neq 0$  ist, muss  $|\beta^k| \geq q^{1-n}$  sein. Lässt man jetzt  $k \rightarrow \infty$  gehen, erhält man den gewünschten Widerspruch.

# Übungen zu Kapitel 3

- 1) *Zeige, dass jede additive Untergruppe von  $\mathbb{Z}$  bereits ein Ideal ist.*

Sei  $A$  eine additive Untergruppe. Diese ist per definitionem abgeschlossen bezüglich der Addition. Nun ist aber Multiplikation von  $a \in A$  mit einer natürlichen Zahl nichts anderes als wiederholte Addition von  $a$  zu sich selbst, folglich ist  $A$  abgeschlossen bezüglich Multiplikation mit  $\mathbb{N}$ . Da mit  $a$  auch  $-a$  in  $A$  liegt (wegen der additiven Abgeschlossenheit), folgt die Behauptung.

- 2) *Zeige, dass die Menge der Matrizen  $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$  mit  $a, b, d \in R$  ein Teilring von  $M_2(R)$  ist, aber kein Ideal.*

Die oberen Dreiecksmatrizen sind abgeschlossen gegenüber Addition und Multiplikation, und enthalten die Einheitsmatrix. Damit bilden sie einen Ring (mit Eins).

Andererseits zeigt  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ , dass dieser Teilring nicht gegenüber Multiplikation mit Ringelementen abgeschlossen ist, also kein Ideal bildet.

- 3)  *$\mathbb{Z}$  ist ein Teilring von  $\mathbb{Q}$ , aber kein Ideal.*

$\mathbb{Z}$  ist nicht abgeschlossen bezüglich Multiplikation mit  $\mathbb{Q}$ , da z.B.  $1 \in \mathbb{Z}$ , aber  $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$  gilt.

- 4) *Zeige  $\text{Quot}(\mathbb{Z}[i]) \simeq \mathbb{Q}(i)$ .*

Um  $\text{Quot}(R) = K$  zu zeigen, genügt es nachzuweisen, dass erstens  $K$  ein Körper ist, und zweitens jedes Element von  $K$  die Form  $\frac{r}{s}$  mit  $r, s \in R$  hat.

Dass  $\mathbb{Q}(i)$  Körper ist, sollte klar sein. Ist weiter  $p + qi \in \mathbb{Q}(i)$  gegeben, so können wir  $p = \frac{a}{n}$  und  $q = \frac{b}{n}$  (mit einem gemeinsamen Nenner  $n$ ) schreiben. Dann ist aber  $p + qi = \frac{a+bi}{n}$  der Quotient zweier "ganzer Gaußschen Zahlen"  $a + bi, n \in \mathbb{Z}[i]$ , und damit sind wir fertig.

5) Zeige  $\text{Quot}(\mathbb{Z}[X]) = \mathbb{Q}(X)$ .

Die Elemente von  $\text{Quot}(\mathbb{Z}[X])$  bestehen aus Quotienten  $\frac{f(X)}{g(X)}$  mit  $f, g \in \mathbb{Z}[X]$  und  $g \neq 0$ . Also ist  $\text{Quot}(\mathbb{Z}[X]) \subseteq \mathbb{Q}(X)$ . Sei nun  $\frac{f(X)}{g(X)} \in \mathbb{Q}(X)$ , also  $f, g \in \mathbb{Q}[X]$ . Multipliziert man beide Polnome mit dem Hauptnenner  $m$  der Koeffizienten von  $f$  und  $g$ , so ist  $mf, mg \in \mathbb{Z}[X]$  und damit  $\frac{f(X)}{g(X)} = \frac{mf(X)}{mg(X)} \in \text{Quot}(\mathbb{Z}[X])$ .

6) Zeige  $\mathbb{Z}[X]/(X^2 - 2) \simeq \mathbb{Z}[\sqrt{2}]$ .

Betrachte den Einsetzungshomomorphismus  $\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{2}]$ , der durch  $\phi(f) = f(\sqrt{2})$  definiert wird. Wegen  $f(a + bX) = a + b\sqrt{2}$  ist  $\phi$  offenbar surjektiv. Der Kern von  $\phi$  besteht aus allen  $f \in \mathbb{Z}[X]$  mit  $f(\sqrt{2}) = 0$ ; wir behaupten, dass  $f \in (X^2 - 2)$  ist.

Dazu schreiben wir  $f(X) = (X^2 - 2)q(X) + r(X)$  mit  $\deg r < 2$ . Einsetzen von  $\sqrt{2}$  gibt  $r(\sqrt{2}) = 0$ . Da  $r(X) = a + bX$  für  $a, b \in \mathbb{Z}$  ist, folgt aus der Irrationalität von  $\sqrt{2}$ , dass  $r = 0$  sein muss. Damit folgt Kern  $\phi = (X^2 - 2)$ .

Die Behauptung ergibt sich jetzt aus dem Homomorphiesatz.

7) Sei  $R$  ein Ring. Zeige, dass es einen Ringhomomorphismus  $f : \mathbb{Z} \longrightarrow R$  gibt.

Ist  $R$  ein Ring mit Eins  $1_R$ , so setze man  $f(r) = r \cdot 1_R$  für alle  $r \in \mathbb{Z}$ .

8) Sei  $K$  ein Körper. Zeige, dass es keinen Ringhomomorphismus  $f : K \longrightarrow \mathbb{Z}$  gibt.

Sei  $f$  ein solcher. Da Kern  $f$  ein Ideal in  $K$  ist, muss Kern  $f = 0$  oder Kern  $f = K$  sein. Wegen  $f(1) = 1$  (Ringe mit Eins) kann aber Kern  $f$  nicht gleich  $K$  sein, und es folgt Kern  $f = 0$ . Also ist Bild  $f \simeq K$  ein Teilkörper von  $\mathbb{Z}$ : Widerspruch.

9) Sei  $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$  und betrachte den Ring  $R = \mathbb{F}_2[X]/(f)$ . Setze  $\alpha = X + (f)$  und zeige, dass  $R = \{0, 1, \alpha, \alpha + 1\}$  gilt (wobei wir statt  $0 + (f)$  und  $1 + (f)$  einfach 0 und 1 geschrieben haben). Berechne Additions- und Multiplikationstabellen dieses Rings und folgere, dass  $R$  ein Körper ist (den wir in Kap. 9 mit  $\mathbb{F}_4$  bezeichnen werden).

+	0	1	$\alpha$	$\alpha + 1$
0	0	1	$\alpha$	$\alpha + 1$
1	1	0	$\alpha + 1$	$\alpha$
$\alpha$	$\alpha$	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	$\alpha$	1	0

$\cdot$	1	$\alpha$	$\alpha + 1$
1	1	$\alpha$	$\alpha + 1$
$\alpha$	$\alpha$	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	1	$\alpha$

Da jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt, ist  $\mathbb{F}_4$  in der Tat ein Körper.

- 10) Ist  $E$  ein Teilkörper von  $K$ , dann gilt  $\text{char}(E) = \text{char}(K)$ .

Da  $E$  und  $K$  dasselbe Einselement besitzen, und die Ausdrücke  $n \cdot 1$  alle in  $E$  liegen, müssen beide Körper dieselbe Charakteristik haben.

- 11) Seien  $R, S$  Integritätsringe mit  $R \subseteq S \subseteq \text{Quot}(R)$ . Zeige, dass dann  $\text{Quot}(S) = \text{Quot}(R)$  ist.

Zu zeigen sind die formalen Regeln

- a)  $R \subseteq S \implies \text{Quot}(R) \subseteq \text{Quot}(S)$ .
- b)  $\text{Quot}(\text{Quot}(R)) = \text{Quot}(R)$ .

Wendet man diese auf die Inklusionen  $R \subseteq S \subseteq \text{Quot}(R)$  an, so erhält man  $\text{Quot}(R) \subseteq \text{Quot}(S) \subseteq \text{Quot}(R)$  und damit die Behauptung.

- a)  $R \subseteq S \implies \text{Quot}(R) \subseteq \text{Quot}(S)$  ist mehr oder weniger offensichtlich:  $\text{Quot}(R)$  besteht aus Symbolen  $\frac{r}{r'}$  mit  $r, r' \in R$ ; wegen  $R \subseteq S$  sind diese erst recht in  $\text{Quot}(S)$  enthalten.
- b)  $\text{Quot}(\text{Quot}(R)) = \text{Quot}(R)$ : Wegen  $R \subseteq \text{Quot}(R)$  ist nach a) sicherlich  $\text{Quot}(R) \subseteq \text{Quot}(\text{Quot}(R))$ . Nun haben die Elemente von  $\text{Quot}(\text{Quot}(R))$  die Form  $\frac{r_1/r_2}{r_3/r_4}$  mit  $r_j \in R$ ; wegen  $\frac{r_1/r_2}{r_3/r_4} = \frac{r_1 r_4}{r_2 r_3}$  ist aber auch  $\text{Quot}(\text{Quot}(R)) \subseteq \text{Quot}(R)$ .

- 12) Sei  $\phi : R \longrightarrow R'$  ein Ringhomomorphismus. Zeige, dass sich  $\phi$  eindeutig fortsetzen lässt zu einem Ringhomomorphismus  $\Phi : R[X] \longrightarrow R'[X]$  mit  $\Phi(X) = X$ . Drücke Kern  $\Phi$  und Bild  $\Phi$  durch Kern  $\phi$  bzw. Bild  $\phi$  aus.

Sei  $f(X) = \sum a_j X^j \in R[X]$ . Dann setzen wir  $\Phi(f) = \sum \phi(a_j) X^j$ . Man rechnet sofort nach, dass  $\Phi$  ein Ringhomomorphismus ist, dessen Einschränkung auf  $R$  gleich  $\phi$  ist.

- 13) *Zeige: sind  $R$  und  $S$  Ringe, dann auch  $R \times S$  mit komponentenweiser Addition und Multiplikation. Ist  $R \times S$  ein Integritätsring, wenn  $R$  und  $S$  solche sind?*

Dies ist eine rein formale Verifikation der Axiome, unter Zugrundelegung von  $(r, s) + (r', s') = (r + r', s + s')$  und  $(r, s)(r', s') = (rr', ss')$  für  $r, r' \in R$  und  $s, s' \in S$ .

Sind  $R$  und  $S$  Integritätsringe, dann ist  $R \times S$  keiner: wegen  $(1, 0)(0, 1) = (0, 0)$  ist  $R \times S$  nicht nullteilerfrei.

- 14) *Sind  $I$  und  $J$  Ideale in  $R$ , dann auch  $I \cap J$ ,  $I + J = \{i + j : i \in I, j \in J\}$ , und  $I : J = \{a \in R : aJ \subseteq I\}$ . Zeige weiter, dass  $I \subseteq I + J$ ,  $I \subseteq I : J$ , und  $I : J = I : (I + J)$  gilt.*

Sind  $a, b \in I \cap J$  und  $r, s \in R$ , dann sind  $ra, sb \in I$ ,  $ra, sb \in J$ , daher  $ra, sb \in I \cap J$  und schließlich auch  $ra + sb \in I \cap J$ .

Ist  $a \in I : J$ , so ist  $aJ \subseteq I$ , damit  $raJ \subseteq rI = I$  für jedes  $r \in R$ , und somit  $ra \in I : J$ . Sind  $a, b \in I : J$ , so ist mit  $aJ \subseteq I$  und  $bJ \subseteq I$  auch  $(a + b)J \subseteq I + I = I$ , also  $a + b \in I : J$ . Damit ist  $I : J$  ein Ideal in  $R$ .

Die Inklusion  $I \subseteq I + J$  ist offensichtlich. Weiter ist  $I \subseteq I : J$  wegen  $aJ \subseteq I$  für alle  $a \in I$ . Schließlich ist  $aJ \subseteq I$  äquivalent zu  $a(I + J) \subseteq I$ , und dies zeigt  $I : (I + J) = I : J$ .

Übrigens gilt auch  $I : R = I$ ,  $I : I = I$ , und  $(I : J)J = I$ .

# Übungen zu Kapitel 4

1) *Im Folgenden sei  $M$  ein kommutatives Monoid, also eine Menge, welche mit einer kommutativen und assoziativen Multiplikation ausgestattet ist und ein Einselement besitzt. Außerdem wollen wir annehmen, dass in  $M$  die Kürzungsregel gilt, d.h. dass aus  $ab = ac$  für  $a, b, c \in M$  immer  $b = c$  folgt. Zeige:*

- a) *Ist  $R$  ein Integritätsring, so ist  $M = R \setminus \{0\}$  ein Monoid.*
  - b) *Übertrage den Begriff der Teilbarkeit, wie er in diesem Kapitel für Ringe definiert wurde, auf kommutative Monoide.*
  - c) *Welche der Eigenschaften (4.3)–(4.8) bleiben für Monoide richtig?*
- a) Sind  $a, b \in M = R \setminus \{0\}$ , dann wegen der Nullteilerfreiheit von  $R$  auch  $ab$ . Weiter gilt die Kürzungsregel: ist  $ab = ac$  für  $a, b, c \in M$ , dann gilt diese Gleichung auch im Quotientenkörper  $\text{Quot}(R)$ ; dort liefert Kürzen  $b = c$ , und da wir  $R$  als Teilring von  $\text{Quot}(R)$  auffassen dürfen (hier benutzen wir wieder, dass  $R$  Integritätsring ist), gilt diese Gleichung auch in  $R$  und damit in  $M$ .
- b) Man sagt, es sei  $a \mid b$  für  $a, b \in M$ , wenn es ein  $c \in M$  gibt mit  $b = ac$ .
- c) Alle Aussagen, die in Monoiden sinnvoll bleiben, sind auch richtig. Wenn  $M$  (wie im Falle  $M = R \setminus \{0\}$  keine 0 enthält, ist  $a \mid 0$  natürlich sinnlos. In jedem Fall ist (4.8) sinnlos, da es in Monoiden keine Addition gibt.

2) *Definiere irreduzible und prime Elemente in kommutativen Monoiden, und zeige, dass prime Elemente immer irreduzibel sind (unter Annahme der Kürzungsregel).*

Ein Element  $u \in M$  nennt man eine Einheit, wenn es ein  $v \in M$  mit  $uv = 1$  gilt. Wie für Ringe rechnet man leicht nach, dass die Menge  $M^\times$  aller Einheiten eine Gruppe bildet.

Eine Nichteinheit  $p \in M$  heie irreduzibel, wenn aus  $p = ab$  mit  $a, b \in M$  immer folgt, dass  $a$  oder  $b$  eine Einheit in  $M$  ist.

Eine Nichteinheit  $p \in M$  nennt man prim, wenn aus  $p \mid ab$  mit  $a, b \in M$  immer folgt, dass  $p \mid a$  oder  $p \mid b$  ist.

Sei nun  $p \in M$  prim und  $p = ab$ . Dann ist auch  $p \mid ab$ , also ohne Beschränkung der Allgemeinheit  $p \mid a$ . Dies bedeutet  $a = pc$  für ein  $c \in M$ , und jetzt finden wir  $p = ab = pbc$ . Ausnützen der Kürzungsregel liefert  $1 = bc$ : also ist  $b$  eine Einheit, und damit  $p$  irreduzibel.

- 3) Hilbert führte in seinen Vorlesungen das Monoid  $M = \{1, 6, 11, 16, \dots\}$  aller natürlichen Zahlen  $n \equiv 1 \pmod{5}$  ein. Zeige, dass  $21 \cdot 26 = 6 \cdot 91$  zwei verschiedene Zerlegungen von 4641 in irreduzible Faktoren ist (d.h. das Monoid  $M$  ist nicht faktoriell).

Das Element 21 ist in  $M$  irreduzibel, da die "Faktoren" 3 und 7 nicht in  $M$  enthalten sind. Ähnliches gilt für 6, 26 und 91.

- 4) Zeige allgemein, dass für gegebenes  $m \geq 3$  das Monoid  $M = \{n \in \mathbb{N} : n \equiv 1 \pmod{m}\}$  nicht faktoriell ist.

Dies ist sehr einfach zu zeigen, wenn man einen elementaren Spezialfall des Dirichletschen Primzahlsatzes benutzt, nämlich die Tatsache, dass es unendlich viele Primzahlen  $p$  der Form  $p \equiv -1 \pmod{m}$  gibt. Sind nämlich  $p, q, r, s$  solche Primzahlen, so sind  $pq \cdot rs = pr \cdot qs$  zwei wesentlich verschiedene Faktorisierungen von  $pqrs$  in (in  $M$ ) irreduzible Elemente.

Man kommt aber auch ohne den Dirichletschen Satz zurecht: zuerst überlegt man sich, dass es unendlich viele Primzahlen gibt, die nicht  $\equiv 1 \pmod{m}$  sind. Die Zahl  $2m - 1$  hat nämlich mindestens einen Primfaktor  $p$  mit dieser Eigenschaft; jetzt betrachte  $2mp - 1$  usw.

Da sich diese unendlich vielen Primzahlen auf endlich viele Restklassen aufteilen, gibt es mindestens eine Restklasse, in der sich unendlich viele Primzahlen befinden. Seien nun  $p$  und  $q$  verschiedene Primzahlen mit  $p \equiv q \equiv a \pmod{m}$ , und sei  $f$  der kleinste Exponent mit  $a^f \equiv 1 \pmod{m}$ . Dann sind  $p^f, p^{f-1}q, p^{f-2}q^2, \dots, pq^{f-1}$  und  $q^f$  irreduzible Elemente in  $M$ , und die Faktorisierungen  $p^f \cdot q^f = (p^{f-1}q) \cdot pq^{f-1} = \dots$  zeigen, dass  $M$  nicht faktoriell ist.

- 5) Betrachte den Ring  $R = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$ .

- Bestimme alle Ideale in  $R$ .
- Zeige, dass die Elemente  $\bar{2}$  und  $\bar{3}$  weder Einheiten, noch irreduzibel sind.
- Zeige, dass in  $R$  die Bedingungen F4.8.a) und b) erfüllt sind.
- Man mache sich anhand von  $\bar{2} = \bar{2} \cdot \bar{2} \cdot \bar{2}$  und  $\bar{3} = \bar{3} \cdot \bar{3}$  die Probleme klar, die bei einer Übertragung der Teilbarkeitslehre auf allgemeine kommutative Ringe auftreten.

e) Zeige, dass  $\bar{2}$  und  $\bar{4}$  größte gemeinsame Teiler von  $\bar{2}$  und  $\bar{4}$  sind.

a) Wir beginnen mit den Hauptidealen: diese sind  $(\bar{0})$ ,  $(\bar{1}) = (\bar{5})$ ,  $(\bar{2}) = (\bar{4})$  und  $(\bar{3})$ .

Das sind aber auch schon alle: nimmt man z.B. zu  $(\bar{2})$  ein weiteres Element hinzu (also  $\bar{1}, \bar{3}$  oder  $\bar{5}$ ), so erhält man schon  $(\bar{1})$ . Also ist jedes Ideal von  $R$  Hauptideal (und dennoch  $R$  kein Hauptidealring, da  $R$  kein Integritätsring ist).

b) Offenbar ist  $\bar{2}$  keine Einheit, da aus  $\bar{2}\bar{m} = \bar{1}$  sofort  $2m - 1 = 6t$  für ein  $t \in \mathbb{Z}$  folgt, was aus Paritätsgründen Unsinn ist. Ähnlich zeigt man, dass  $\bar{3}$  keine Einheit ist.

Wegen  $\bar{2} = \bar{2} \cdot \bar{2} \cdot \bar{2}$  und  $\bar{3} = \bar{3} \cdot \bar{3}$  sind  $\bar{2}$  und  $\bar{3}$  aber auch nicht irreduzibel.

c) Da es in  $R$  keine irreduziblen Elemente gibt, ist F4.8.b) trivialerweise erfüllt. Außerdem muss jede aufsteigende Kette von Hauptidealen in  $R$  aus dem einfachen Grund stationär werden, weil es nur endlich viele Hauptideale gibt; also ist auch F4.8.a) erfüllt.

d) Dieser Punkt sollte jetzt klar sein.

e) Die gemeinsamen Teiler von  $\bar{2}$  und  $\bar{4}$  sind  $\bar{2}$  und  $\bar{4}$ : es ist ja  $\bar{2} = \bar{2} \cdot \bar{4}$  und  $\bar{4} = \bar{2} \cdot \bar{2} = \bar{4} \cdot \bar{4}$ . Wegen  $\bar{2} \mid \bar{4}$  und  $\bar{4} \mid \bar{2}$  sind beides größte gemeinsame Teiler.

6) Bestimme alle Ideale  $I$  in  $R = \mathbb{Z}/12\mathbb{Z}$ , sowie die dazugehörigen Quotientenringe  $R/I$ . Welche Ideale sind prim, welche maximal?

In  $R$  sind, wie in allen Ringen  $\mathbb{Z}/m\mathbb{Z}$ , alle Ideale Hauptideale: so ist z.B.  $(\bar{a}, \bar{b}) = (\bar{d})$  für  $d = \text{ggT}(a, b)$ . Also gibt es genau die folgenden Ideale:  $(\bar{0})$ ,  $(\bar{1}) = (\bar{5}) = (\bar{7}) = (\bar{11})$ ,  $(\bar{2}) = (\bar{10})$ ,  $(\bar{3}) = (\bar{9})$ ,  $(\bar{4}) = (\bar{8})$ , und  $(\bar{6})$ .

Die dazugehörigen Quotientenringe sind  $R/(\bar{0}) \simeq R$ ,  $R/(\bar{1}) \simeq 0$  (der Nullring),  $R/(\bar{2}) \simeq \mathbb{Z}/2\mathbb{Z}$  (es gibt genau zwei Restklassen modulo  $\bar{2}$ , und die offensichtliche Abbildung  $R/(\bar{2}) \rightarrow \mathbb{Z}/2\mathbb{Z}$  liefert, wie einfach zu sehen ist, einen Isomorphismus von Ringen mit Eins), sowie allgemein  $R/(\bar{m}) \simeq \mathbb{Z}/m\mathbb{Z}$  für  $m = 2, 3, 4, 6$ .

Damit sind die Ideale  $(\bar{2})$  und  $(\bar{3})$  maximal und damit auch prim; andere Primideale in  $R$  gibt es nicht.

7) Sei  $p$  eine Primzahl und  $R = \mathbb{Z}/p^2\mathbb{Z}$ . Zeige, dass das von  $pX + 1$  in  $R[X]$  repräsentierte Element eine Einheit ist.

Es ist  $(\bar{1} + \bar{p}X)(\bar{1} - \bar{p}X) = \bar{1}$ .

8) Sei  $R$  ein Integritätsring und  $\nu$  eine euklidische Funktion auf  $R$ . Zeige, dass  $\nu(a) = 0$  für  $a \in R$  genau für  $a = 0$  gilt.

Sei  $\nu(a) = 0$ . Wäre  $a \neq 0$ , gäbe es Elemente  $q, r \in R$  mit  $1 = aq + r$  und  $\nu(r) < \nu(a) = 0$ : Widerspruch, da  $\nu$  nur Werte in  $\mathbb{N}_0$  annimmt.



9) Zeige: Körper  $R$  sind euklidische Ringe.

Die Funktion  $\nu$ , welche durch  $\nu(0) = 0$  und  $\nu(a) = 1$  für  $a \in R^\times$  definiert ist, ist ersichtlich euklidisch.

10) Sei  $R$  ein Integritätsring, welcher der Bedingung F4.8.a) genügt, und  $\pi \in R \setminus \{0\}$  eine Nichteinheit.

a) Zeige, dass es zu jedem  $a \in R$  mit  $a \neq 0$  eine ganze Zahl  $w \geq 0$  gibt mit  $\pi^w \mid a$  und  $\pi^{w+1} \nmid a$ .

b) Durch (4.23) wird eine Abbildung  $w_\pi : R \longrightarrow \mathbb{Z} \cup \{\infty\}$  definiert, welche folgende Eigenschaften hat:

$$w_\pi(ab) \geq w_\pi(a) + w_\pi(b), \quad w_\pi(a+b) \geq \min(w_\pi(a), w_\pi(b)).$$

c) Zeige, dass  $w_\pi$  genau dann sogar (4.25) für alle  $a, b \in R$  erfüllt, wenn  $\pi$  ein Primelement ist.

a) Sei  $a \in R \setminus \{0\}$ . Wenn es keinen maximalen Exponenten  $w$  gibt mit  $\pi^w \mid a$ , dann ist  $a = \pi a_1 = \pi^2 a_2 = \pi^3 a_3 = \dots$  für Elemente  $a_j \in R$ . Wegen  $a_{j+1} \mid a_j$  für alle  $j \geq 1$  ist dann aber  $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$ . Nach F4.8.a) muss  $(a_n) = (a_{n+1})$  für einen Index  $n$  gelten; dies bedeutet, dass  $a_n$  und  $a_{n+1}$  assoziiert sind, was wegen  $a_n = a_{n+1}\pi$  bedeuten würde, dass  $\pi$  entgegen der Voraussetzung eine Einheit ist.

b) Ist  $a = \pi^r a'$  für ein  $a' \in R$ , so gilt sicher  $w_\pi(a) \geq r$ . Ist  $a = \pi^r a' = \pi^{r'} a''$  mit  $\pi \nmid a'$  und  $\pi \nmid a''$ , so müssen wir weiter zeigen, dass  $r = r'$  gilt. Aus  $r > r'$  folgt aber  $\pi^{r-r'} a' = a''$ , also  $\pi \mid a''$  im Widerspruch zu unserer Annahme. Also ist  $w_\pi$  wohldefiniert.

Schreiben wir nun  $a = \pi^{w_\pi(a)} a'$ ,  $b = \pi^{w_\pi(b)} b'$  und  $ab = \pi^{w_\pi(ab)} c$  mit  $\pi \nmid a'$ ,  $\pi \nmid b'$  und  $\pi \nmid c$ . Dann ist auch  $ab = \pi^{w_\pi(a)+w_\pi(b)} a' b'$ , und dies impliziert  $w_\pi(ab) \geq w_\pi(a) + w_\pi(b)$ . Ebenso ist  $\pi^{\min(w_\pi(a), w_\pi(b))} \mid (a+b)$ , und dies zeigt  $w_\pi(a+b) \geq \min(w_\pi(a), w_\pi(b))$ .

c) Sei zuerst  $\pi$  ein Primelement, sowie  $a = \pi^{w_\pi(a)} a'$ ,  $b = \pi^{w_\pi(b)} b'$  mit  $\pi \nmid a'$  und  $\pi \nmid b'$ . Dann ist  $ab = \pi^{w_\pi(a)+w_\pi(b)} a' b'$ ; nun kann aber nicht  $\pi \mid a' b'$ , da sonst gegen die Annahme  $\pi$  einen der Faktoren  $a'$  oder  $b'$  teilen müsste. Dies zeigt  $w_\pi(a) + w_\pi(b) = w_\pi(ab)$ .

Sei jetzt  $\pi$  irreduzibel und  $\pi \mid ab$  für  $a, b \in R$ . Wegen  $w_\pi(a) + w_\pi(b) = w_\pi(ab) \geq 1$  muss dann aber  $w_\pi(a) \geq 1$  oder  $w_\pi(b) \geq 1$ , also  $\pi \mid a$  oder  $\pi \mid b$  und damit  $\pi$  prim sein.

11) Sei  $w_p$  die zu der Primzahl  $p$  gehörige Exponentenbewertung von  $\mathbb{Q}$ . Zeige, dass die durch  $|a|_p = p^{-w_p(a)}$  definierte Abbildung  $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{Q}$  die folgenden Eigenschaften mit dem gewöhnlichen Absolutbetrag gemeinsam hat:

- a)  $|a|_p \geq 0$  mit Gleichheit genau für  $a = 0$ ;
- b) Multiplikativität:  $|ab|_p = |a|_p |b|_p$ ;
- c) Dreiecksungleichung:  $|a + b|_p \leq |a|_p + |b|_p$ .

- a)  $|a|_p \geq 0$  folgt aus  $p > 0$ ; weiter ist  $|a|_p = 0$  nur für  $w_p(a) = \infty$  möglich.
- b) Die Multiplikativität  $|ab|_p = |a|_p |b|_p$  ergibt sich direkt aus  $w_p(ab) = w_p(a) + w_p(b)$ .
- c) Die Dreiecksungleichung  $|a + b|_p \leq |a|_p + |b|_p$  ist eine unmittelbare Konsequenz der Ungleichung  $w_p(a + b) \geq \min(w_p(a), w_p(b))$ .

12) Sei  $p$  eine Primzahl. Man bestimme die Einheiten und Primelemente der Teiltringe

$$\mathbb{Z}\left[\frac{1}{p}\right] = \left\{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z}, b \in \{1, p, p^2, \dots\} \right\},$$

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b \right\}$$

von  $\mathbb{Q}$ . Zeige weiter, dass beide Ringe faktoriell sind.

Betrachten wir zuerst  $R = \mathbb{Z}\left[\frac{1}{p}\right]$ . Offenbar sind alle Elemente der Form  $(-1)^m p^n$  mit  $n \in \mathbb{Z}$  Einheiten in  $R$ . Ist umgekehrt  $u \in R^\times$  eine Einheit, so können wir durch Multiplikation von  $u$  mit einer geeigneten Potenz von  $p$  erreichen, dass  $u = \frac{a}{b}$  mit  $p \nmid ab$  ist. Damit  $u \in R$  ist, muss  $b = \pm 1$  sein, und entsprechend folgt  $a = \pm 1$  aus  $\frac{1}{u} \in R$ . Also ist jede Einheit in  $R$  bis auf eine Potenz von  $p$  gleich  $\pm 1$ .

Jetzt behaupten wir, dass jede Primzahl  $q \neq p$  in  $\mathbb{N}$  auch prim in  $R$  ist. Sei nämlich  $q \mid ab$  für  $a, b \in R$ . Wir schreiben nun  $a = \frac{a'}{p^m}$  und  $b = \frac{b'}{p^n}$  mit  $a', b' \in \mathbb{Z}$ . Dann folgt  $q \mid a'b'$  in  $\mathbb{Z}$ , also  $q \mid a'$  oder  $q \mid b'$  in  $\mathbb{Z}$ , und endlich  $q \mid a$  oder  $q \mid b$  in  $R$ .

Schließlich zeigen wir, dass verschiedene Primzahlen  $q, q' \neq p$  in  $R$  nicht assoziiert sein können: sonst wäre nämlich  $q = \pm q' p^m$  in  $\mathbb{Z}$ , was sofort  $m = 0$  und (wegen  $q, q' > 0$ )  $q = q'$  impliziert.

Um zu zeigen, dass  $R$  faktoriell ist, schreiben wir  $a \in R \setminus \{0\}$  in der Form  $a = ua'$  für eine Einheit  $u \in R$  und ein  $a' \in \mathbb{N}$  mit  $p \nmid a'$  in  $\mathbb{N}$ . Da  $a' = \prod q_i^{a_i}$  mit Primelementen  $q_i \in \mathbb{N}$  ist, gilt dasselbe in  $R$ ; auch die Eindeutigkeit folgt sofort.

Sei nun  $R = \mathbb{Z}_{(p)}$ . In  $R$  werden alle Primzahlen  $q \neq p$  zu Einheiten: die Einheitengruppe besteht nämlich aus allen rationalen Zahlen  $\neq 0$ , in deren Primzerlegung  $p$  nicht vorkommt. Dass diese Elemente Einheiten sind, ist klar; ist umgekehrt  $u = \frac{a}{b}$  eine Einheit und  $\text{ggT}(a, b) = 1$ , so muss  $p \nmid b$ , und wegen  $\frac{b}{a} = \frac{1}{u} \in R$  auch  $p \nmid a$  sein.

Damit bleibt nur  $p$  als einzig mögliches Primelement übrig, und in der Tat ist  $p$  prim in  $R$ : aus  $p \mid ab$  in  $R$  mit  $a = \frac{r}{s}$  und  $b = \frac{t}{u}$  folgt  $p \mid rt$  in  $\mathbb{Z}$ ; da  $p$  in  $\mathbb{Z}$  prim ist, gilt  $p \mid r$  oder  $p \mid t$ , und dies wiederum bedeutet  $p \mid a$  oder  $p \mid b$ .

Dass  $R$  faktoriell ist, liegt daran, dass die in einem  $a \in \mathbb{Q}^\times$  aufgehende Potenz von  $p$  eindeutig bestimmt ist.

- 13) Seien  $I_1, I_2$  Ideale in einem Hauptidealring  $R$ . Zeige, dass dann  $I_1 I_2$  gleich der Menge aller Produkte  $xy$  mit  $x \in I_1$  und  $y \in I_2$  ist. Weiter ist  $I_1 I_2 = (ab)$  für  $I_1 = (a)$  und  $I_2 = (b)$ .

Da  $R$  Hauptidealring ist, gilt  $I_1 = (a)$  und  $I_2 = (b)$  für  $a, b \in R$ . Nun besteht  $I_1 I_2$  aus allen endlichen  $R$ -Linearkombinationen  $\sum r_j i_1 i_2$  mit  $r_j \in R, i_1 \in I_1$  und  $i_2 \in I_2$ . Wegen  $i_1 = ar_1$  und  $i_2 = br_2$  für  $r_1, r_2 \in R$  ist aber  $\sum r_j i_1 i_2 = ab \sum r r_1 r_2 = abs$  für ein  $s \in R$ . Wegen  $a \in I_1$  und  $b \in I_2$  folgen daraus alle Behauptungen.

- 14) Man nennt  $e_1, \dots, e_n \in R$  ein vollständiges System paarweiser orthogonaler Idempotente, wenn gilt: a)  $e_i^2 = e_i$ ; b)  $e_i e_j = 0$  für  $i \neq j$ ; c)  $1 = e_1 + \dots + e_n$ . Zeige, dass dann  $R = e_1 R \times \dots \times e_n R$  gilt.

Betrachte man den durch  $\phi(r) = (e_1 r, \dots, e_n r)$  definierten Homomorphismus  $\phi : R \rightarrow e_1 R \times \dots \times e_n R$ . Ist  $r \in \text{Kern } \phi$ , so ist  $e_j r = 0$  für alle  $j$ , somit  $r = 1r = (e_1 + \dots + e_n)r = e_1 r + \dots + e_n r = 0$ . Also ist  $\phi$  injektiv.

Um zu zeigen, dass  $\phi$  surjektiv ist, sein ein Element  $(e_1 r_1, \dots, e_n r_n) \in e_1 R \times \dots \times e_n R$  gegeben. Mit  $r = e_1 r_1 + \dots + e_n r_n$  ist dann  $\phi(r) = (e_1 r, \dots, e_n r) = (e_1^2 r_1 + e_1 e_2 r_2 + \dots + e_1 e_n r_n, \dots) = (e_1 r_1, \dots, e_n r_n)$ , wobei wir die Eigenschaften a) und b) benutzt haben.

- 15) Sei  $\phi : R \rightarrow S$  ein Homomorphismus von Ringen mit Eins. Zeige:  $\phi(R^\times)$  ist eine Untergruppe von  $S^\times$ , und daher vermittelt  $\phi$  einen Gruppenhomomorphismus  $R^\times \rightarrow S^\times$ . Dieser ist ein Isomorphismus, wenn  $\phi$  ein Isomorphismus ist.

Sei  $u \in R^\times$  eine Einheit. Dann gibt es ein  $v \in R^\times$  mit  $uv = 1$ , und Anwenden von  $\phi$  ergibt  $1 = \phi(1) = \phi(uv) = \phi(u)\phi(v)$ . Das erste Gleichheitszeichen ist dabei eine Folge der Annahme, dass  $\phi$  Homomorphismus von Ringen mit Eins ist.

Also ist  $\phi(u)$  eine Einheit in  $S$ , und damit  $\phi(R^\times)$  eine Untergruppe der Einheitsengruppe  $S^\times$  von  $S$ .

Sei nun  $\phi$  ein Isomorphismus, und  $s \in S^\times$  eine Einheit in  $S$ , also  $st = 1$  für ein  $t \in S^\times$ . Die Surjektivität von  $\phi$  gibt uns Elemente  $u, v \in R$  mit  $\phi(u) = s$  und  $\phi(v) = t$ . Dann wird  $1 = st = \phi(u)\phi(v) = \phi(uv)$ , also  $uv = 1$  wegen der Injektivität von  $\phi$ . Dies impliziert aber  $u, v \in R^\times$ .

- 16) Euklid definiert Gleichheit von Proportionen in Buch VII seiner Elemente wie folgt: es sei  $a : b = c : d$  für natürliche Zahlen  $a, b, c, d$  genau dann, wenn es  $m, n, x, y \in \mathbb{N}$  gibt mit  $a = mx, b = nx, c = my, d = ny$ . Dann zeigt er:

a) Es gilt  $a : b = ac : bc$  und  $a : b = ca : cb$ .

b) Gleichheit ist transitiv: aus  $a : b = c : d$  und  $c : d = e : f$  folgt  $a : b = e : f$ .

c) Es ist  $a : b = c : d$  genau dann, wenn  $ad = bc$ .

Hier liegt a) auf der Hand; dass b) zu beweisen ist, hat Euklid übersehen, weswegen sein Beweis für c) auch lückenhaft ist.

Dass der Beweis von b) nicht ganz trivial ist, mache man sich wie folgt klar. In allgemeinen Integritätsringen  $R$  setzen wir  $a : b = c : d$ , wenn es wie oben  $m, n, x, y \in R$  gibt mit  $a = mx$ ,  $b = nx$ ,  $c = my$ ,  $d = ny$ . Zeige, dass die Transitivität der Gleichheit in  $R = \mathbb{Z}[\sqrt{-5}]$  nicht gilt, da zwar

$$\begin{aligned} 2 : (1 + \sqrt{-5}) &= 2(1 - \sqrt{-5}) : (1 + \sqrt{-5})(1 - \sqrt{-5}), \\ 2(1 - \sqrt{-5}) : (1 + \sqrt{-5})(1 - \sqrt{-5}) &= 2(1 - \sqrt{-5}) : (2 \cdot 3) \quad \text{und} \\ 2(1 - \sqrt{-5}) : (2 \cdot 3) &= (1 - \sqrt{-5}) : 3, \end{aligned}$$

aber  $2 : (1 + \sqrt{-5}) \neq (1 - \sqrt{-5}) : 3$  ist.

Sei nun  $R$  ein ggT-Ring, also ein Integritätsring, in welchem jedes Paar  $a, b \in R$  einen größten gemeinsamen Teiler besitzt (jeder faktorielle Ring ist ein ggT-Ring; die Umkehrung gilt aber nicht, wie z.B. der Ring aller ganzen algebraischen Zahlen zeigt). Mit Euklid setzen wir  $a : b = c : d$  für  $a, b, c, d \in R$  genau dann, wenn es  $m, n, x, y \in R$  gibt mit  $a = mx$ ,  $b = nx$ ,  $c = my$ ,  $d = ny$ .

- a) Es ist  $a : b = ac : bc$ ; dazu braucht man nur  $m = a$ ,  $n = b$ ,  $x = 1$  und  $y = c$  zu setzen. Ebenso zeigt man  $a : b = ca : cb$ .
- b) Zum einen kann man das einfach mit c) beweisen: die Voraussetzungen besagen dann  $ad = bc$  und  $cf = de$ ; daraus folgt  $adf = bcf = bde$  und, nach Kürzen von  $d$ , die gewünschte Beziehung  $af = be$ .

Ein direkter Beweis verwendet den folgenden

**Hilfssatz.** Ist  $a : b = c : d$  in einem ggT-Ring  $R$ , so gibt es  $p, q \in R$  mit  $a = p \operatorname{ggT}(a, b)$  und  $b = q \operatorname{ggT}(a, b)$ , und damit gilt  $c = p \operatorname{ggT}(c, d)$  und  $d = q \operatorname{ggT}(c, d)$ .

Die Relation  $a : b = c : d$  liefert die Existenz von  $m, n, x, y \in R$  mit  $a = mx$ ,  $b = nx$ ,  $c = my$ , und  $d = ny$ . Also ist  $x \mid \operatorname{ggT}(a, b)$  und  $y \mid \operatorname{ggT}(c, d)$ , d.h. es gibt  $i, j \in R$  mit  $\operatorname{ggT}(a, b) = ix$  und  $\operatorname{ggT}(c, d) = jy$ . Wir behaupten nun, dass  $i \mid j$  gilt; aus Symmetriegründen ist dann auch  $j \mid i$ , d.h.  $i$  und  $j$  sind assoziiert. Damit gibt es eine Einheit  $e \in R^\times$  mit  $i = ej$ . Andererseits ist  $ix = \operatorname{ggT}(a, b) \mid a = mx$ , also  $i \mid m$ ; daher gibt es ein  $p \in R$  mit  $m = pi$ , und analog findet man  $n = qj$ .

Jetzt folgt  $c = my = piy = epjy = ep \operatorname{ggT}(c, d)$ , sowie  $d = ny = qjy = q \operatorname{ggT}(c, d)$ . Ersetzt man noch  $p$  durch  $ep$ , so erhält man damit die Behauptung. Zu zeigen bleibt noch  $i \mid j$ . Aus  $ix \mid a = mx$  folgt  $i \mid m$ , also  $iy \mid my = c$ . Ähnlich folgt  $iy \mid ny = d$ . Also gilt  $iy \mid \operatorname{ggT}(c, d) = jy$ , und dies liefert die Behauptung.

Jetzt folgt die Transitivität der Gleichheit so: sei  $a : b = c : d$  und  $c : d = e : f$ . Dann gilt  $a = mx$ ,  $b = nx$ ,  $c = my$ ,  $d = ny$  mit  $x = \text{ggT}(a, b)$  und  $y = \text{ggT}(c, d)$ . Der Hilfssatz liefert dann  $c = m \text{ggT}(c, d)$  und  $d = n \text{ggT}(c, d)$ . Wenden wir den Hilfssatz noch einmal an, ergibt sich  $e = m \text{ggT}(e, f)$  und  $f = n \text{ggT}(e, f)$ , und daraus folgt dann sofort  $a : b = e : f$ .

- c) Die Richtung  $\implies$  ist trivial; die andere Richtung können wir unter Zuhilfenahme von b) wie folgt beweisen: ist  $ad = bc$ , so gilt

$$\begin{array}{ll} a : b = ac : bc & \text{nach a)} \\ = ac : ad & \text{wegen } ad = bc \\ = c : d & \text{nach a)} \end{array}$$

Im Ring  $R = \mathbb{Z}[\sqrt{-5}]$  gilt die Transitivität der Gleichheit nicht: die ersten drei angeführten Gleichungen folgen alle aus Teil a), der in beliebigen Integritätsringen gilt. Wäre die Gleichheit transitiv, würde auch  $2 : (1 + \sqrt{-5}) = (1 - \sqrt{-5}) : 3$  gelten, d.h. es gäbe  $m, n, x, y \in R$  mit

$$\begin{array}{ll} 2 = mx, & 1 - \sqrt{-5} = my, \\ 1 + \sqrt{-5} = nx, & 3 = ny. \end{array}$$

Da aber 2 in  $R$  irreduzibel ist (vgl. Aufg. 4.4.a), ist  $m$  oder  $x$  eine Einheit; die einzigen Einheiten in  $R$  sind aber, wovon man sich leicht überzeugt, die Elemente  $\pm 1$ . Aus  $x = \pm 1$  folgt aber  $2 \mid (1 - \sqrt{-5})$ , was nicht richtig ist, und aus  $m = \pm 1$  folgt entsprechend  $2 \mid (1 + \sqrt{-5})$ , was ebenfalls falsch ist. Dieser Widerspruch zeigt  $2 : (1 + \sqrt{-5}) \neq (1 - \sqrt{-5}) : 3$ .

- 17) Sei  $K$  ein Körper. Zeige, dass  $K[X, Y]/(XY) \simeq K[X] \times K[Y]$  als  $K$ -Vektorräume, aber nicht als Ringe isomorph sind.

Jedes Element  $f(X, Y) + (XY) \in K[X, Y]/(XY)$  lässt sich eindeutig in der Form  $g(X) + Yh(Y) + (XY)$  schreiben (man eliminiere alle Vielfachen von  $XY$  und schlage den konstanten Term  $g$  zu). Die Abbildung  $f + (XY) \mapsto (g, h)$  gibt uns dann eine  $K$ -lineare Abbildung  $K[X, Y]/(XY) \rightarrow K[X] \times K[Y]$ , von der man leicht nachrechnet, dass sie bijektiv ist.

Oder so: Die Inklusionen  $K[X] \hookrightarrow K[X, Y]$  und  $K[Y] \hookrightarrow K[X, Y]$  vermitteln Morphismen  $K[X] \hookrightarrow K[X, Y]/(XY)$  und  $K[Y] \hookrightarrow K[X, Y]/(XY)$ , und diese sind offenbar injektiv; also erhält man einen Morphismus der direkten Summe  $K[X] \oplus K[Y] \rightarrow K[X, Y]/(XY)$ , welcher injektiv ist. Wie man sich aber leicht überlegt, ist er auch surjektiv.

Wir wollen nun zeigen, dass  $K[X, Y]/(XY)$  und  $K[X] \times K[Y]$  nicht als Ringe isomorph sind. Dazu nehmen wir an,  $\phi : K[X, Y]/(XY) \rightarrow K[X] \times K[Y]$  sei ein Isomorphismus. Dann gibt es  $F_1, F_2 \in K[X, Y]/(XY)$  mit  $\phi(F_1) = (1, 0)$  und

$\phi(F_2) = (0, 1)$ . Man überlegt sich leicht, dass sich jedes Element in  $K[X, Y]/(XY)$  eindeutig in der Form  $f(X) + g(Y) + (XY)$  mit  $g(0) = 0$  schreiben lässt. Sei daher  $F_j = f_j(X) + g_j(Y)$  für  $j = 1, 2$ , und  $g_j(0) = 0$ . Dann ist  $0 = (0, 0) = (1, 0)(0, 1) = \phi(F_1)\phi(F_2) = \phi(F_1F_2)$ . Da  $\phi$  injektiv ist, muss  $F_1F_2 = 0$  sein, also  $(f_1(X) + g_1(Y))(f_2(X) + g_2(Y)) \in (XY)$ .

Nun ist  $(f_1(X) + g_1(Y))(f_2(X) + g_2(Y)) = f_1(X)f_2(X) + f_2(X)g_1(Y) + f_1(X)g_2(Y) + g_1(Y)g_2(Y)$ . Da die letzten drei Produkte Vielfache von  $Y$  sind, muss dies auch für  $f_1(X)f_2(X)$  gelten, und dies geht nur, wenn  $f_1(X)f_2(X) = 0$  ist. Sei daher oBdA  $f_2 = 0$ . Wegen  $f_1(X)g_2(Y) \equiv f_1(0)g_2(Y) \pmod{XY}$  können wir jetzt schließen, dass  $f_1(0)g_2(Y) + g_1(Y)g_2(Y) \in (XY)$  ist. Auf der linken Seite steht aber jetzt ein Polynom in  $K[Y]$ ; dies kann nur dann durch  $X$  teilbar sein, wenn es verschwindet:  $f_1(0)g_2(Y) + g_1(Y)g_2(Y) = 0$ . Daher ist  $g_2 = 0$  (und damit  $F_2 = 0$  im Widerspruch zu  $\phi(F_2) = (0, 1)$ ) oder  $f_1(0) + g_1(Y) = 0$ ; wegen  $Y \mid g_1(Y)$  folgt daraus aber  $f_1(0) = 0$  und  $g_1 = 0$ .

Damit haben wir  $\phi(f_1(X)) = (1, 0)$  und  $\phi(g_2(Y)) = (0, 1)$ , also  $\phi(1) = (1, 1) = \phi(f_1(X) + g_2(Y))$ . Da  $\phi$  injektiv ist, muss  $f_1(X) + g_2(Y) = 1$  sein. Einsetzen von  $Y = 0$  zeigt  $f(1) = 1$ , also  $g_2 = 0$ : Widerspruch wegen  $\phi(g_2) = (0, 1) \neq 0$ .

Wir bemerken, dass die Abbildung  $\psi$ , welche  $F = f(X) + g(Y)$  auf  $(f(X), f(0) + g(Y))$  abbildet, immerhin einen injektiven Ringhomomorphismus  $K[X, Y]/(XY) \longrightarrow K[X] \times K[Y]$  liefert.

Ein weit einfacherer Beweis, dass  $K[X, Y]/(XY)$  und  $K[X] \times K[Y]$  nicht als Ringe isomorph sein können, geht so: der Ring  $K[X] \times K[Y]$  hat neben dem Einselement  $1 = (1, 1)$  noch die beiden Idempotente  $e = (1, 0)$  und  $1 - e = (0, 1)$ . Der Ring  $K[X, Y]/(XY)$  dagegen hat nur das triviale idempotente Element  $1 = 1 + (XY)$ . Sei nämlich  $f(X) + g(Y)$  ein Repräsentant eines idempotenten Elements, und sei oBdA  $g(0) = 0$ . Dann ist  $(f(X) + g(Y))^2 = f(X)^2 + 2f(X)g(Y) + g(Y)^2 \equiv f(X)^2 + 2f(0)g(Y) + g(Y)^2 \pmod{XY}$ . Da diese Darstellungen eindeutig sind, können wir die Grade der Polynome in  $X$  vergleichen und finden  $f \in K$ . Entsprechend folgt  $g \in K$ , und das einzige Idempotent in  $K$  ist  $e = 1$ .

# Übungen zu Kapitel 5

- 1) Ist  $R$  ein Integritätsring, dann auch  $R[X]$ .

Seien  $f(X) = a_m X^m + \dots + a_0$  und  $g(X) = b_n X^n + \dots + b_0$  Polynome in  $R[X]$  mit Koeffizienten  $a_m, b_n \neq 0$ . Ist dann  $f(X)g(X) = 0$  in  $R[X]$ , so folgt wegen  $f(X)g(X) = a_m b_n X^{m+n} + \text{Terme niederen Grades}$ , dass dann  $a_m b_n = 0$  in  $R$  sein muss. Da  $R$  nullteilerfrei ist, geht das nur, wenn  $a_m = 0$  oder  $b_n = 0$  ist, was unserer Voraussetzung widerspricht.

- 2) Sei  $R = \mathbb{Z}[X]$  und  $S = R[Y]$ . Man berechne  $\text{Inhalt}(f)$  für  $f = X + 2Y \in S$ .

Die Koeffizienten von  $f$  als Element des Polynomrings  $R[Y]$  sind  $X$  und  $2$ ; daher ist  $\text{Inhalt}(f) = \text{ggT}(X, 2) = 1$ .

- 3) Finde möglichst viele Begründungen dafür, dass das Polynom  $X^2 + X$  kein Quadrat in  $K(X)$  ist, wo  $K$  ein beliebiger Körper ist.

1. Der Ring  $K(X)$  ist faktoriell, die Elemente  $X$  und  $X + 1$  zwei verschiedene Prim-elemente. Quadrate in faktoriellen Ringen zeichnen sich aber dadurch aus, dass die Exponenten in ihren Primfaktorzerlegungen sämtlich gerade sind.

2. Sei  $X^2 + X = \frac{f^2}{g^2}$ , wobei wir  $f, g \in K[X]$  als teilerfremd annehmen dürfen. Aus  $f(X)^2 = (X^2 + X)g(X)^2$  folgt  $f(0) = 0$ , also  $f(X) = Xh(X)$  für ein  $h \in K[X]$ . Dann ist aber  $Xh(X) = (X + 1)g(X)^2$ , somit  $g(0) = 0$  und  $X \mid g(X)$ : das widerspricht aber der Teilerfremdheit von  $f$  und  $g$ .

- 4) Sei  $R = \mathbb{Z}[X^2, X^3]$ . Zeige:

a)  $R = \{f \in \mathbb{Z}[X] : f'(0) = 0\}$ .

b)  $R$  ist nicht faktoriell.

c) Es ist  $\text{ggT}(X^4, X^5) = X^2$ , aber  $X^4$  und  $X^5$  besitzen kein kleinstes gemeinsames Vielfaches. Warum widerspricht dies nicht Aufg. 4.9?

- d) Die Elemente  $X^5$  und  $X^6$  haben weder einen größten gemeinsamen Teiler, noch ein kleinstes gemeinsames Vielfaches.

- a) Betrachte die Faktorisierungen  $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$ . Da  $\pm 1$  die einzigen Einheiten in  $R$  sind, unterscheiden sich die Faktoren  $X^2$  und  $X^3$  nicht um eine Einheit. Weiter sind sie irreduzibel: beispielsweise kann  $X^3$  nur das Produkt von Polynomen der Grade 0 und 3, bzw. 1 und 2 sein. Da es keine Polynome vom Grad 1 in  $R$  gibt, kann also höchstens  $X^3 = cg(X)$  für ein  $c \in \mathbb{Z}$  sein: das führt aber sofort auf  $c = \pm 1$ .

Also sind die Faktoren  $X^2$  und  $X^3$  irreduzibel in  $R$ , und damit ist  $X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$  ein Beispiel für nichteindeutige Zerlegung in irreduzible Elemente in  $R$ .

- b) Die Teiler von  $X^4$  sind  $1, X^2, X^4$ ; die Teiler von  $X^5$  sind  $1, X^2, X^3, X^5$ . Damit ist  $X^2$  ein gemeinsamer Teiler, und da die einzigen gemeinsamen Teiler  $1$  und  $X^2$  sind, ist es der größte gemeinsame Teiler.

Die Elemente  $X^7$  und  $X^8$  sind gemeinsame Vielfache von  $X^4$  und  $X^5$ ; der gemeinsame Teiler  $X^5$  dieser Elemente ist aber kein gemeinsames Vielfaches von  $X^4$  und  $X^5$ .

Aufgabe 4.9 besagt, dass kleinste gemeinsame Vielfache existieren, wenn *alle* Elemente einen größten gemeinsamen Teiler besitzen. Die schärfere Aussage, dass zwei Elemente ein kleinstes gemeinsames Vielfaches besitzen, wenn sie einen größten gemeinsamen Teiler haben, ist daher falsch.

- c) Die Teiler von  $X^5$  sind  $1, X^2, X^3$ , diejenigen von  $X^6$  sind  $1, X^2, X^3, X^4$ . Das Element  $X^3$  ist ein gemeinsamer Teiler, aber nicht der größte: es ist nämlich auch  $X^2$  ein gemeinsamer Teiler, aber  $X^2 \nmid X^3$ . Die gemeinsamen Teiler  $1$  und  $X^2$  sind natürlich ebensowenig größte gemeinsame Teiler, da sie keine Vielfachen von  $X^3$  sind.

Unter den gemeinsamen Vielfachen von  $X^5$  und  $X^6$  sind sicherlich  $X^8$  und  $X^9$ ; das kleinste gemeinsame Vielfache müsste also ein gemeinsamer Teiler von  $X^8$  und  $X^9$  sein: aber  $X^6$  ist kein Vielfaches von  $X^5$ , und noch kleinere Potenzen von  $X$  kommen ohnehin nicht in Frage. Also gibt es kein kleinstes gemeinsames Vielfaches.

- 5) Zeige, dass das Ideal  $(2, X)$  im Polynomring  $\mathbb{Z}[X]$  kein Hauptideal ist.

Sei  $(2, X) = (f)$  für ein  $f \in \mathbb{Z}[X]$ . Dann ist  $2 \in (f)$ , also  $2 = fg$  für ein  $g \in \mathbb{Z}[X]$ . Aus Gradgründen muss  $f$  also konstant sein, d.h.  $f \in \mathbb{Z}$ . Wegen  $X \in (f)$  gilt andererseits  $f \mid X$ ; da  $X$  irreduzibel ist, geht das aber wegen  $f \in \mathbb{Z}$  nur für  $f = \pm 1$ . Also muss  $(2, X) = (1)$  sein.



Dies bedeutet aber  $1 = 2r + Xs$  für Polynome  $r, s \in \mathbb{Z}[X]$ . Für  $X = 0$  erhält man daraus  $1 = 2r(0)$  in  $\mathbb{Z}$ : Widerspruch.

Tatsächlich gilt viel mehr: nicht nur ist  $(2, X)$  kein Hauptideal, es lässt sich durch Multiplikation mit von  $(0)$  verschiedenen Idealen auch nicht zu einem Hauptideal machen: aus  $(2, X)I = (f)$  folgt nämlich  $I = (0)$ . Sei dazu  $r \in I$ ; dann ist  $2r \in (2, X)I = (f)$  und  $Xr \in (2, X)I = (f)$ , also  $f \mid 2r$  und  $f \mid Xr$ . Da 2 und  $X$  teilerfremde Primelemente aus  $\mathbb{Z}[X]$  sind, folgt daraus  $f \mid r$ . Also ist  $I \subseteq (f)$ .

Aus  $(f) = (2, X)I \subseteq (2, X)(f)$  folgt aber jetzt  $f = (2r + Xs)f$  für  $r, s \in \mathbb{Z}[X]$ . Kürzen von  $f$  liefert dann  $1 = 2r + Xs$ , woraus sich für  $X = 0$  wieder der gewünschte Widerspruch ergibt.

6) Sei  $f = X^4 + X + 1$  und  $E = \mathbb{Q}(\alpha)$ , wo  $\alpha$  eine Nullstelle von  $f$  ist.

a) Zeige (z.B. mit dem Lemma von Gauß):  $f$  ist irreduzibel über  $\mathbb{Q}$ .

b) Stelle  $\frac{1}{\alpha^2+1} \in E$  als  $\mathbb{Q}$ -Linearkombination der  $\alpha^j$  dar. (Hinweis: wende den Euklidischen Algorithmus auf  $f$  und  $g = X^2 + 1$  an).

a) Ist  $f$  nicht irreduzibel, dann gilt  $f(X) = g(X)h(X)$  für nicht konstante normierte Polynome  $g, h \in \mathbb{Q}[X]$ . Nach dem Lemma von Gauß haben  $g$  und  $h$  ganzzahlige Koeffizienten. Da  $f$  keine ganzzahlige Nullstelle (und damit keinen linearen Teiler) besitzt, müssen  $g$  und  $h$  Grad 2 haben. Ein Ansatz  $f(X) = (X^2 + aX + b)(X^2 + cX + d)$  liefert sofort  $a + c = 0$ , sowie  $b = d = \pm 1$ . Also ist  $f(X) = (X^2 + aX + b)(X^2 - aX + b)$ ; der Koeffizient von  $X$  auf der rechten Seite ist dann aber gleich 0, und dieser Widerspruch zeigt die Behauptung.

b) Der Euklidische Algorithmus liefert  $(2 - X)f(X) + (X^3 - 2X^2 - X + 3)(X^2 + 1) = 5$ ; Einsetzen von  $\alpha$  gibt dann  $(\alpha^3 - 3\alpha^2 - \alpha + 3)(\alpha^2 + 1) = 5$ , also  $\frac{1}{\alpha^2+1} = \frac{\alpha^3 - 3\alpha^2 - \alpha + 3}{5}$ .

7) Sei  $R$  faktoriell,  $a \in R$  und  $f \in R[X]$ . Zeige, dass die folgenden Aussagen äquivalent sind:

(i)  $a \mid f$  in  $R[X]$ ;

(ii)  $a \mid \text{Inhalt}(f)$  in  $R$ .

Sei  $f(X) = a_0 + a_1X + \dots + a_nX^n$  mit  $a_i \in R$ . Ist dann  $a \mid \text{Inhalt}(f)$  in  $R$ , so gilt  $a \mid a_i$  für alle  $0 \leq i \leq n$ , also  $a_i = ab_i$ . Mit  $g(X) = b_0 + b_1X + \dots + b_nX^n$  ist dann  $f(X) = ag(X)$ , also  $a \mid f$  in  $R[X]$ .

Sei nun umgekehrt  $a \mid f$  in  $R[X]$ , also  $f(X) = ag(X)$  für ein  $g$  wie oben. Dann sind alle Koeffizienten von  $f$  durch  $a$  teilbar, folglich  $a \mid \text{Inhalt}(f)$  in  $R$ .

- 8) Sei  $R$  faktoriell und  $p \in R$  prim. Zeige direkt, dass  $p$  auch in  $R[X]$  prim ist.

Sei  $p \mid fg$  für  $f, g \in R[X]$ . Wir schreiben  $f = \sum a_i X^i$  und  $g = \sum b_j X^j$ . Wäre  $p \nmid f$  und  $p \nmid g$ , so gäbe es Koeffizienten von  $f$  und  $g$ , die nicht durch  $p$  teilbar sind. Wir wählen dann  $r, s$  maximal mit  $p \nmid a_r$  und  $p \nmid b_s$ . Der Koeffizient von  $X^{r+s}$  in  $fg$  ist dann gegeben durch  $\sum_{i+j=r+s} a_i b_j$ . In dieser Summe sind alle Terme bis auf  $a_r b_s$  durch  $p$  teilbar; also ist  $fg$  nicht durch  $p$  teilbar im Widerspruch zur Annahme.

- 9) Sei  $R \longrightarrow \bar{R} : a \longmapsto \bar{a}$  ein Ringhomomorphismus, und sei  $\phi : R[X] \longrightarrow \bar{R}[X]$  dessen Fortsetzung auf den entsprechenden Polynomringen (vgl. F5.8). Zeige, dass  $\phi(f)(\bar{a}) = \overline{f(a)}$  für jedes  $f \in R[X]$  gilt.

Mit  $f(X) = \sum a_i X^i$  ist  $\phi(f)(X) = \sum \bar{a}_i X^i$ , somit  $\phi(f)(\bar{a}) = \sum \bar{a}_i \bar{a}^i = \overline{f(a)}$ .

- 10) Sei  $f(X) = X^2 + X + 2 \in \mathbb{Z}[X]$ . Zeige, dass es eine ganze Zahl  $a$  gibt, sodass  $f(X - a)$  ein Eisensteinpolynom bezüglich 7 wird.

Es ist  $f(X - a) = (X - a)^2 + (X - a) + 2 = X^2 + (1 - 2a)X + a^2 - a + 2$ . Für  $a = -3$  wird  $1 - 2a = 7$ , sowie  $a^2 - a + 2 = 14$ .

- 11) Das Polynom  $f(X) = X^5 - 2 \in \mathbb{Z}[X]$  ist ein Eisensteinpolynom bezüglich 2. Zeige, dass es eine ganze Zahl  $a$  gibt, sodass  $f(X - a)$  ein Eisensteinpolynom bezüglich 5 wird.

Es ist  $f(X + a) = X^5 + \dots + a^5 - 2$ ; damit der letzte Koeffizient ein Vielfaches von 5 wird, wählen wir  $a = 2$ . Man rechnet jetzt leicht nach, dass  $f(X + 2)$  tatsächlich ein Eisensteinpolynom bezüglich 5 ist.

- 12) Seien  $a, b, c$  Elemente eines Körpers  $K$ . Zeige, dass  $Y^2 - (X - a)(X - b)(X - c) \in K[X, Y]$  irreduzibel ist. Unter welchen Bedingungen ist  $Y^2 - (X - a)(X - b)$  irreduzibel in  $K[X, Y]$ ?

Wir zeigen allgemein:  $Y^2 - f(X)$  ist genau dann irreduzibel in  $K[X, Y]$ , wenn  $f(X) \in K[X]$  kein Quadrat ist.

Ist  $f(X) = g(X)^2$  ein Quadrat, so ist natürlich  $Y^2 - f(X) = (Y - g(X))(Y + g(X))$  reduzibel.

Sei umgekehrt  $Y^2 - f(X)$  zerlegbar in  $K[X, Y]$ . Fassen wir  $K[X, Y]$  als Polynomring in  $Y$  über  $K[X]$  auf, so müssen die beiden Faktoren von  $Y^2 - f(X)$  entweder beide Grad 1 in  $Y$  haben, oder einer von beiden hat Grad 0. Im letzteren Falle gibt es ein  $g \in K[X]$  mit  $gY^2 - f(X)$ , was offensichtlich nur für  $g \in K^\times$  geht; solche Faktorisierungen sind also immer trivial in dem Sinne, dass einer der beiden Faktoren eine Einheit ist.

Also haben beide Faktoren Grad 1 in  $Y$ , und es muss gelten:  $Y^2 - f(X) = (g_1 Y + g_2)(h_1 Y + h_2)$  mit  $g_j, h_j \in K[X]$ . Koeffizientenvergleich liefert sofort, dass man

$g_1 = h_1 = 1$  annehmen darf. Daher ist  $Y^2 - f(X) = (Y + g_2)(Y + h_2)$ . Substituiert man nun  $Y = -g_2(X)$ , so folgt  $f(X) = g_2(X)^2$ , d.h.  $f$  ist ein Quadrat in  $K[X]$ .

Offensichtlich ist nun  $(X - a)(X - b)(X - c)$  schon aus Gradgründen kein Quadrat in  $K[X]$ , somit  $Y^2 - (X - a)(X - b)(X - c) \in K[X, Y]$  irreduzibel.

Weiter ist  $(X - a)(X - b)$  genau dann ein Quadrat in  $K[X]$ , wenn  $a = b$  ist.

- 13) Betrachte das Polynom  $f = X^5 - X - a$  für  $a \in \mathbb{Z}$ . Zeige, dass  $f$  genau dann einen Linearfaktor besitzt, wenn  $a = m^5 - m$  für ein  $m \in \mathbb{Z}$  gilt. (Die Frage, wann  $f$  irreduzibel in  $\mathbb{Q}[X]$  ist, führt auf eine recht verzwickte diophantische Gleichung, die mit Quadraten in der Fibonaccifolge zu tun hat; es stellt sich heraus, dass  $f$  genau dann reduzibel ist, wenn  $f$  einen linearen Faktor besitzt oder  $a = \pm 15, \pm 22440$  ist.)

Sei  $f(X) = X^5 - X - a = (X - m)g(X)$ ; dann ist  $f(m) = 0$ , also  $a = m^5 - m$ . Hat  $a$  diese Form, ist umgekehrt  $X - m$  ein Faktor von  $f$ .

Ist  $a$  nicht von der Form  $a = m^5 - m$ , so kann  $f$  höchstens in einen quadratischen und einen kubischen Faktor zerfallen:  $f(X) = (X^2 + rX + s)(X^3 + tX^2 + uX + v)$ . Vergleich der Koeffizienten von  $X^4$  zeigt  $t = -r$ , Vergleich der Koeffizienten von  $X^3$  liefert dann  $u = r^2 - s$ , und ein schließlich zeigen die Koeffizienten von  $X^2$ , dass  $v = -r^3 + 2rs$  sein muss. Damit haben wir

$$f(X) = (X^2 + rX + s)(X^3 - rX^2 + (r^2 - s)X - r^3 + 2rs).$$

Vergleicht man jetzt die Koeffizienten des linearen Terms, so findet man  $r^4 - 3r^2s + s^2 = 1$ . Setzt man  $q = r^2$ , ist also  $q^2 - 3qs + s^2 = 1$ . Damit diese quadratische Gleichung in  $q$  eine ganze Lösung hat, muss die Diskriminante  $5s^2 + 4$  ein Quadrat sein, d.h.  $x^2 - 5s^2 = 4$ ; in diesem Fall sind dann  $q = \frac{3s \pm x}{2}$  ganzzahlige Lösungen.

Die Lösungen von  $x^2 - 5s^2 = 4$  lassen sich nun leicht explizit beschreiben: sie sind gegeben durch  $(x, s) = (L_{2n}, F_{2n})$ , wo  $L_n$  und  $F_n$  die durch  $L_0 = 2, L_1 = 1, L_{n+1} = L_n + L_{n-1}$  und  $F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}$  definierten Lucas- und Fibonacci-Zahlen sind.

Damit wird  $\frac{3s \pm x}{2} = F_{2n+2}$ , und da die einzigen Quadratzahlen in der Fibonaccifolge  $F_0 = 0, F_1 = F_2 = 1$ , und  $F_{12} = 144$  sind, ergeben sich in diesem Fall

(i)  $r = \pm 1$  und  $s = 3$ , also  $a = \pm 15$  und z.B.

$$X^5 - X - 15 = (X^2 - X + 3)(X^3 + X^2 - 2X - 5).$$

(ii)  $r = \pm 12$  und  $s = 55$ , also  $a = rs(r^2 - 2s) = \pm 22440$ . In der Tat gilt

$$X^5 - X - 22440 = (X^2 + 12X + 55)(X^3 - 12X^2 + 89X - 408).$$

Wegen  $\frac{3s-x}{2} = F_{2n-2}$  führen diese Werte von  $q$  auf dieselben Lösungen.

- 14) Sei  $K$  ein Körper der Charakteristik  $\neq 2$ . Betrachte das Ideal  $I = (X^2 + Y^2 - 1)$  in  $K[X, Y]$ , und setze  $R = K[X, Y]/I$ . Zeige:

- a) Enthält  $K$  ein Element  $i$  mit  $i^2 = -1$ , so ist  $x = X + I \in R$  reduzibel.
- b) Enthält  $K$  kein Element  $i$  mit  $i^2 = -1$ , so ist  $R$  nicht faktoriell.

Sei  $i \in K$  und setze  $u = x + iy$  und  $v = x - iy$ . Dann ist  $uv = x^2 + y^2 = 1$ , sowie  $x = \frac{u+v}{2}$  und  $y = \frac{u-v}{2i}$ . Dies zeigt  $K[x, y] = K[u, v]$ . Weiter ist  $u$  eine Einheit in  $K[x, y]$ , und wir finden  $x = \frac{u+v}{2} = \frac{u^2+1}{2u} = \frac{1}{2u}(u+i)(u-i)$ . Also ist  $x$  bis auf die Einheit  $\frac{1}{2u}$  das Produkt der Elemente  $u+i$  und  $u-i$ .

Ist  $i \notin K$ , also  $x$  irreduzibel, so ist  $x^2 = 1 - y^2 = (1-y)(1+y)$ . Wir behaupten nun, dass  $x \nmid 1 \pm y$  ist (daraus folgt dann bereits, dass  $R$  nicht faktoriell ist). In der Tat, wäre z.B.  $\frac{1-y}{x} \in R$ , sagen wir  $\frac{1-y}{x} = f(x, y)$ , so würde folgen  $(1-y) = xf(x, y)$  und schließlich  $1 - Y = Xf(X, Y) + (X^2 + Y^2 - 1)g(X, Y)$  für geeignete Polynome  $f, g \in K[X, Y]$ . Setzt man  $X = 0$ , so folgt  $1 - Y = (Y^2 - 1)g(0, Y)$ , also  $1 = -(Y+1)g(0, Y)$ . Dies ist offenbar unmöglich.

- 15) Darf man in Korollar 5.15 auf die Teilerfremdheit von  $x, y, z$  verzichten?

Nein. Multipliziert man irgendeine Lösung von  $x^n + y^n = z^n$  ( $x, y, z \in \mathbb{C}^\times$ ) mit  $X$ , so erhält man eine nichtkonstante Lösung der Fermatgleichung in  $\mathbb{C}[X]$ .

- 16) Welche der folgenden Eigenschaften übertragen sich von einem Integritätsring  $R$  auf den zugehörigen Polynomring  $R[X]$ ?

- a) faktoriell
- b) Hauptidealring
- c) euklidisch

Ist  $R$  faktoriell, so auch  $R[X]$  (Satz von Gauß). Ist  $R$  Hauptidealring, so wird  $R[X]$  in der Regel keiner sein: so ist z.B.  $\mathbb{Z}[X]$  kein Hauptidealring. Dasselbe Beispiel zeigt, dass  $R[X]$  nicht euklidisch zu sein braucht, wenn  $R$  es ist.

- 17) Sei  $R$  ein Integritätsring mit Quotientenkörper  $K$  und  $S$  eine multiplikativ abgeschlossene Teilmenge von  $R \setminus \{0\}$  mit  $1 \in S$ . Zeige: Ist  $R$  faktoriell, dann auch  $S^{-1}R$ .

Wir zeigen zuerst: ist  $p \in R$  irreduzibel in  $R$ , dann ist  $p$  prim oder eine Einheit in  $S^{-1}R$ .

Gibt es ein  $s \in S$  mit  $p \mid s$ , so ist  $p$  eine Einheit. Ist  $p \nmid s$  für alle  $s \in S$ , so behaupten wir, dass  $p$  in  $S^{-1}R$  prim ist. Aus  $p \mid ab$  mit  $a, b \in S^{-1}R$  folgt nämlich  $rp = scd$  für

$s \in S$  und  $r, c, d \in R$ . Da  $p$  prim in  $R$  ist und  $p \nmid s$  gilt, folgt  $p \mid c$  oder  $p \mid d$ . Sei  $p \mid c$  in  $R$ ; dann ist erst recht  $p \mid c$  in  $A$ , also  $p \mid a$ .

Nun kann man jedes von 0 verschiedene  $a \in A = S^{-1}R$  in der Form  $eb$  für eine Einheit  $e \in A^\times$  und ein  $b \in R$  schreiben. Zerlegen wir  $b$  in Primfaktoren aus  $R$ , so sind diese Einheiten oder irreduzible Elemente in  $A$ ; insbesondere existiert eine Zerlegung von  $a$  in irreduzible Elemente.

Seien schließlich  $a = e_1 p_1 \cdots p_m = e_2 q_1 \cdots q_n$  zwei Faktorisierungen von  $a$  in eine Einheit und irreduzible Elemente  $p_i, q_j \in R$ . Da diese auch prim in  $A$  sind, folgt die Eindeutigkeit der Darstellung auf dem üblichen Weg.

- 18) Sei  $R$  ein Integritätsring und  $A = R[X]/X^2$  (im Falle von  $R = \mathbb{R}$  nennt man  $A$  den Ring der dualen Zahlen). Setze  $\varepsilon = X + (X^2)$  und zeige, dass für alle  $f \in A[T]$  gilt:  $\frac{f(T+\varepsilon) - f(T)}{\varepsilon} = f'(T)$ .

Man überzeugt sich zuerst davon, dass beide Seiten  $R$ -linear sind, d.h.: mit

$$\frac{f(T+\varepsilon) - f(T)}{\varepsilon} = f'(T) \quad \text{und} \quad \frac{g(T+\varepsilon) - g(T)}{\varepsilon} = g'(T)$$

gilt auch

$$\frac{h(T+\varepsilon) - h(T)}{\varepsilon} = h'(T)$$

für  $h = rf + sg$ ,  $r, s \in R$ . Daher muss man die Behauptung nur für Polynome  $f(T) = T^n$  zeigen. Für  $f(T) = T^n$  ist aber  $(T + \varepsilon)^n = T^n + nT^{n-1}\varepsilon$  wegen  $\varepsilon^2 = 0$ , somit  $\frac{f(T+\varepsilon) - f(T)}{\varepsilon} = nT^{n-1} = f'(T)$ .

- 19) Ist  $X^2 + Y^2 - Z^2$  irreduzibel in  $\mathbb{C}[X, Y, Z]$ ? In  $K[X, Y, Z]$  für beliebige Körper  $K$ ?

Es ist leicht zu sehen, dass in Körpern der Charakteristik 2 gilt:  $X^2 + Y^2 - Z^2 = (X+Y+Z)^2$  gilt. Über Körpern der Charakteristik  $\neq 2$  ist das Polynom  $X^2 + Y^2 - Z^2$  allerdings irreduzibel.

In der Tat: fassen wir  $Z^2 - X^2 - Y^2$  als Element von  $R[Z]$  mit  $R = K[X, Y]$  auf, so ist  $R$  faktoriell. Das Element  $X^2 + Y^2 \in R$  ist nun entweder irreduzibel (und damit auch prim) oder das Produkt  $(X + iY)(X - iY)$  zweier verschiedener Primelemente in  $R$ . In jedem Fall ist damit  $X^2 + Y^2$  kein Quadrat in  $R$ , und dies zeigt wie in Übung 5.12, dass  $Z^2 - X^2 - Y^2$  irreduzibel in  $K[X, Y, Z]$  ist.

- 20) Eisenstein bemerkt in der Originalarbeit über sein Irreduzibilitätskriterium, dass ein Polynom mit ganzzahligen Koeffizienten auch dann irreduzibel ist, wenn alle Koeffizienten außer dem höchsten teilbar durch  $p$ , aber nicht sämtlich durch  $p^2$  teilbar sind (es also nicht gerade der letzte Koeffizient zu sein braucht, in dem  $p^2$  nicht aufgeht). Man beweise oder widerlege dies.

Für prime  $p > 2$  betrachte man  $(X - p)^2 = X^2 - 2pX + p^2$ .

# Übungen zu Kapitel 6

- 1) Seien  $L_1$  und  $L_2$  Zwischenkörper einer Erweiterung  $E/K$ . Zeige: sind  $L_1/K$  und  $L_2/K$  normale Erweiterungen, so auch ihr Kompositum  $L_1L_2/K$  und ihr Durchschnitt  $L_1 \cap L_2/K$ .

Nach Satz 6.4 gibt es Mengen  $M_1, M_2$  von Polynomen mit Nullstellenmengen  $N_1$  und  $N_2$ , sodass  $L_1 = K(N_1)$  und  $L_2 = K(N_2)$  ist. Dann ist aber  $L_1L_2 = K(N)$ , wo  $N$  die Nullstellenmenge der Polynome aus  $M = M_1 \cup M_2$  ist.

Hat  $f \in K[X]$  eine Nullstelle in  $L_1 \cap L_2$ , dann auch in  $L_1$  und  $L_2$ . Da die Erweiterungen  $L_j/K$  normal sind, zerfällt  $f$  in  $L_1$  und  $L_2$  in Linearfaktoren. Ist  $X - \alpha$  ein solcher Faktor, so ist also  $\alpha \in L_1$  und  $\alpha \in L_2$ , also  $\alpha \in L_1 \cap L_2$ . Daher zerfällt  $f$  bereits in  $L_1 \cap L_2$  in Linearfaktoren.

- 2) Die komplexe Konjugation  $\sigma$  ist ein  $\mathbb{R}$ -Algebrenhomomorphismus  $\mathbb{C} \longrightarrow \mathbb{C}$ . Dies bedeutet:

- a) Die Einschränkung von  $\sigma$  auf  $\mathbb{R}$  ist trivial;
- b)  $\sigma$  ist eine  $\mathbb{R}$ -lineare Abbildung des  $\mathbb{R}$ -Vektorraums  $\mathbb{C}$  in sich, d.h. es gilt  $\sigma(\lambda v + \mu w) = \lambda \sigma(v) + \mu \sigma(w)$  für alle  $\lambda, \mu \in \mathbb{R}$  und alle  $v, w \in \mathbb{C}$ .
- c)  $\sigma$  respektiert die Multiplikation in  $\mathbb{C}$ , d.h. es ist  $\sigma(vw) = \sigma(v)\sigma(w)$ .

Alternativ ist  $\sigma$  ein Ringhomomorphismus  $\mathbb{C} \longrightarrow \mathbb{C}$ , der trivial auf  $\mathbb{R}$  ist. Dagegen ist  $\sigma$  kein  $\mathbb{C}$ -Algebrenhomomorphismus.

Diese Behauptungen sind sehr leicht nachzuweisen: wir haben  $\sigma(x + yi) = x - yi$ , und dies bedeutet:

- a)  $\sigma(x) = x$  für alle  $x \in \mathbb{R}$ ;
- b)  $\sigma(\lambda(x + yi)) = \sigma(\lambda x + \lambda yi) = \lambda x - \lambda yi = \lambda(x - yi) = \lambda \sigma(x + yi)$ . Da  $\sigma$  offenbar additiv ist, folgt die Behauptung.
- c)  $\sigma((x + yi)(u + vi)) = \sigma(xu - yv + (au + yv)i) = xu - yv - (au + yv)i = (x - yi)(u - vi) = \sigma(x + yi)\sigma(u + vi)$ .

Wäre  $\sigma$  ein  $\mathbb{C}$ -Algebrenhomomorphismus, so müsste  $\sigma(i) = i\sigma(1) = i$  gelten, was aber falsch ist.

- 3) Sind  $E_1/K$  und  $E_2/K$  isomorph, so gilt  $E_1 : K = E_2 : K$ .

Jeder  $K$ -Isomorphismus  $\sigma : E_1/K \rightarrow E_2/K$  ist automatisch eine  $K$ -lineare Abbildung  $E_1 \rightarrow E_2$  der  $K$ -Vektorräume  $E_1$  und  $E_2$ . Da  $\sigma$  ein Isomorphismus ist, induziert er einen  $K$ -Vektorraumisomorphismus  $E_1 \simeq E_2$ ; daher haben beide Räume dieselbe  $K$ -Dimension.

- 4) Verifiziere die folgende Tabelle von Zerfällungskörpern einiger Polynome  $f \in \mathbb{Q}[X]$ :

$f$	Zerfällungskörper	$f$	Zerfällungskörper
$X^2 - 2$	$\mathbb{Q}(\sqrt{2})$	$X^4 + 4$	$\mathbb{Q}(i)$
$X^3 - 1$	$\mathbb{Q}(\sqrt{-3})$	$X^4 + 1$	$\mathbb{Q}(i, \sqrt{2})$
$X^3 - 2$	$\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$	$X^4 + X^2 + 1$	$\mathbb{Q}(\sqrt{-3})$

Der Zerfällungskörper von  $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$  ist  $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ .

Entsprechend ist  $X^3 - 1 = (X - 1)(X^2 + X + 1)$ , sodass der Zerfällungskörper von  $X^3 - 1$  mit demjenigen von  $X^2 + X + 1$ , also  $\mathbb{Q}(\sqrt{-3})$ , übereinstimmt.

Bezeichnet  $\rho$  eine primitive dritte Einheitswurzel, so ist  $X^3 - 2 = (X - \sqrt[3]{2})(X - \rho\sqrt[3]{2})(X - \rho^2\sqrt[3]{2})$ . Der Zerfällungskörper von  $X^3 - 2$  enthält mit  $\sqrt[3]{2}$  und  $\rho\sqrt[3]{2}$  auch  $\rho$ , also ganz  $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ ; die andere Inklusion ist klar.

Jetzt gilt  $X^4 + 4 = X^4 + 4X^2 + 4 - 4X^2 = (X^2 + 2)^2 - (2X)^2 = (X^2 + 2X + 2)(X^2 - 2X + 2)$ . Die beiden quadratischen Faktoren haben Nullstellen  $\pm 1 \pm i$ , also ist  $\mathbb{Q}(i)$  der Zerfällungskörper von  $X^4 + 4$ .

Wegender beiden Faktorisierungen  $X^4 + 1 = (X^2)^2 + 1 = (X^2 + i)(X^2 - i)$  und  $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$  enthält der Zerfällungskörper von  $X^4 + 1$  sicherlich  $\mathbb{Q}(i, \sqrt{2})$ . Andererseits liegen die Wurzeln der beiden quadratischen Faktoren  $X^2 \pm \sqrt{2}X + 1$ , nämlich  $\frac{\sqrt{2}}{2}(\pm 1 \pm i)$ , offenbar in  $\mathbb{Q}(i, \sqrt{2})$ .

Schließlich ist  $X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = (X^2 + X + 1)(X^2 - X + 1)$ , und damit folgt die Behauptung wie oben durch Ausrechnen der Wurzeln der beiden quadratischen Faktoren.

- 5) Zeige anhand der Definition, dass die Erweiterung  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  nicht normal ist.

Das Polynom  $X^3 - 2$  hat in  $\mathbb{Q}(\sqrt[3]{2})$  eine Nullstelle; wegen  $X^3 - 2 = (X - \sqrt[3]{2})(X - \rho\sqrt[3]{2})(X - \rho^2\sqrt[3]{2})$ , wo  $\rho$  eine primitive dritte Einheitswurzel bezeichnet, liegen die andern Nullstellen aber nicht in  $\mathbb{Q}(\sqrt[3]{2})$ .

- 6) Zeige, dass  $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$  normal ist,  $\mathbb{Q}(\sqrt{3+\sqrt{2}})/\mathbb{Q}$  dagegen nicht.

Das Minimalpolynom von  $\sqrt{2+\sqrt{2}}$  ist  $f(X) = (X^2 - (2+\sqrt{2}))(X^2 - (2-\sqrt{2})) = X^4 - 4X^2 + 2$ . Die Nullstellen von  $f$  sind  $\pm\sqrt{2+\sqrt{2}}$ , sowie  $\pm\sqrt{2-\sqrt{2}}$ . Nun ist aber  $\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2}$ , also

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in \mathbb{Q}(\sqrt{2+\sqrt{2}}),$$

und damit zerfällt  $f$  über  $\mathbb{Q}(\sqrt{2+\sqrt{2}})$  in Linearfaktoren. Also ist  $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$  normal.

Auf der andern Seite ist  $\sqrt{3+\sqrt{2}}\sqrt{3-\sqrt{2}} = \sqrt{7}$ , also

$$\sqrt{3-\sqrt{2}} = \frac{\sqrt{7}}{\sqrt{3+\sqrt{2}}},$$

und da  $\sqrt{7}$  nicht in  $\mathbb{Q}(\sqrt{3+\sqrt{2}})$  enthalten sein kann (dessen quadratischer Teilkörper ist  $\mathbb{Q}(\sqrt{2})$ ), folgt, dass das Minimalpolynom von  $\sqrt{3+\sqrt{2}}$  über  $\mathbb{Q}(\sqrt{3+\sqrt{2}})$  zwar eine Nullstelle hat, aber nicht in Linearfaktoren zerfällt.

- 7) Seien  $A$  und  $B$  zwei  $K$ -Algebren. Zeige, dass in  $A \otimes B$  folgende Regeln gelten (hierbei seien  $a, a_i \in A$ ,  $b, b_i \in B$  und  $c \in K$ ):

- a)  $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$ ;
- b)  $(ca) \otimes b = c(a \otimes b) = a \otimes (cb)$ ;
- c)  $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2)$ ;
- d)  $a \otimes 0 = 0 = 0 \otimes b$ .

Im Spezialfall  $A = K[X]$  und  $B = K[Y]$  zeige man weiter, dass jedes Element in  $A \otimes B$  eine  $K$ -Linearkombination von endlich vielen Elementen der Form  $X^i \otimes Y^j$  mit  $i, j \in \mathbb{N}_0$  ist.

Wir haben  $M = A \times B$  durch  $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$  zum Monoid gemacht. Das Element  $a \otimes b$  ist definiert als die Nebenklasse  $(a, b) + U$ . Damit gilt dann:

- a) Es ist  $(a_1, b) + (a_2, b) - (a_1 + a_2, b) \in U$ , also  $a_1 \otimes b + a_2 \otimes b - (a_1 + a_2) \otimes b = 0$  in  $A \otimes B$ .
- b) Wegen  $(ca, b) - c(a, b) \in U$  ist  $ca \otimes b = c(a \otimes b)$ .
- c) Nach Definition der Multiplikation in  $KM$  gilt  $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$ . Damit ist insbesondere  $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2)$ .
- d) Nach b) gilt  $a \otimes 0 = 0(a \otimes 0) = 0$ .



Sei nun  $A = K[X]$  und  $B = K[Y]$ . Dann bilden  $M_1 = \{1, X, X^2, \dots\}$  und  $M_2 = \{1, Y, Y^2, \dots\}$   $K$ -Basen von  $A$  und  $B$ ; nach F6.8 ist die Menge  $\{X^i \otimes Y^j : i, j \in \mathbb{N}_0\}$  eine  $K$ -Basis von  $A \otimes B$ .

- 8) Man gehe den Beweis von F6.8 im Spezialfall  $A_1 = K[X]$ ,  $A_2 = K[Y, Z]$  durch. Wie sieht die natürliche Wahl der  $K$ -Basen  $M_1$  und  $M_2$  aus, wie die Basis  $\otimes b_i$ ? Wie sind die Linearformen  $f_i$  hier zu interpretieren?

Eine Basis von  $A_1$  ist gegeben durch  $M_1 = \{1, X, X^2, \dots\}$ , und  $M_2 = \{Y^j Z^k : i, j \in \mathbb{N}_0\}$  ist eine Basis von  $A_2$ . Die dazugehörige  $K$ -Basis von  $A_1 \otimes A_2$  besteht dann aus allen Elementen der Form  $X^i \otimes Y^j Z^k$  mit  $i, j, k \in \mathbb{N}_0$ . Elemente  $a \in M_1$  haben die Form  $a = \sum a_i X^i$ , und die dazugehörige Linearform  $f_1 : A_1 \rightarrow K$  bildet  $a$  auf den Koeffizienten  $a_i$  ab. Ähnlich bildet  $f_2$  ein Polynom  $\sum a_{jk} Y^j Z^k$  auf  $a_{jk}$  ab.

- 9) Man konstruiere den algebraischen Abschluss von  $\mathbb{Q}$  wie folgt.

- a) Zu jedem Polynom  $f \in \mathbb{Q}[X]$  existiert ein Zerfällungskörper. (Satz 3.4 von Kronecker und Induktion.)
- b) Die normierten irreduziblen Polynome in  $\mathbb{Q}[X]$  sind abzählbar.
- c) Sei  $f_1, f_2, \dots$  eine Abzählung wie in b),  $K_0 = \mathbb{Q}$ , sowie  $K_j$  für  $j \geq 1$  der Zerfällungskörper des Produkts  $f_1 \cdots f_j$  über  $\mathbb{Q}$ ; dann ist offenbar  $K_0 \subseteq K_1 \subseteq \dots$ . Setze  $K = \bigcup_j K_j$  und zeige, dass  $K$  eine algebraisch abgeschlossene algebraische Erweiterung von  $\mathbb{Q}$  ist.

- a) Nach dem Satz von Kronecker gibt es zu  $f$  eine Erweiterung  $K/\mathbb{Q}$ , in welchem  $f$  eine Nullstelle  $\alpha$  besitzt. Schreibe  $f(X) = (X - \alpha)g(X)$  und wende den Satz von Kronecker auf  $g$  an. Nach höchstens  $\deg f$  Schritten hat man eine Erweiterung von  $\mathbb{Q}$  gefunden, in welcher  $f$  in Linearfaktoren zerfällt.
- b) Dies haben wir bereits in Übung 2.3 gezeigt.
- c) Offenbar ist  $K$  ein Körper: sind  $\alpha, \beta \in K$ , so gibt es Indizes  $i, j$  mit  $\alpha \in K_i$  und  $\beta \in K_j$ ; also sind  $\alpha, \beta \in K_{\max\{i, j\}}$ , somit  $\alpha \pm \beta$ ,  $\alpha\beta$ , und (falls  $\beta \neq 0$ )  $\alpha/\beta$  ebenfalls Elemente von  $K_{\max\{i, j\}} \subseteq K$ .

Jedes Element von  $K$  ist in einem  $K_j$  enthalten und damit algebraisch über  $\mathbb{Q}$ ; also ist  $K/\mathbb{Q}$  eine algebraische Erweiterung.

Sei  $f$  ein Polynom in  $K[X]$ . Da  $f$  nur endlich viele Koeffizienten hat, gibt es einen Index  $j$  mit  $f \in K_j[X]$ . Sei  $\alpha$  eine Nullstelle von  $f$  in einem Zerfällungskörper  $E$  von  $f$ ; dann ist  $\alpha$  algebraisch über  $\mathbb{Q}$ , also Nullstelle eines normierten irreduziblen Polynoms  $f \in \mathbb{Q}[X]$ . Da der Zerfällungskörper von  $f$  in  $K$  enthalten ist, zerfällt  $f$  über  $K$  in Linearfaktoren. Also ist  $K$  algebraisch abgeschlossen.

# Übungen zu Kapitel 7

- 1) *Gib alle  $K$ -Konjugierten von  $\sqrt{2} + \sqrt{3}$  an, wo  $K = \mathbb{Q}$ ,  $K = \mathbb{Q}(\sqrt{2})$ ,  $K = \mathbb{Q}(\sqrt{3})$ , und  $K = \mathbb{Q}(\sqrt{6})$  ist.*

Die Konjugierten sind die Nullstellen der betreffenden Minimalpolynome; über  $\mathbb{Q}$  ist das wegen  $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$

$$(X^2 - (5 + 2\sqrt{6}))(X^2 - (5 - 2\sqrt{6})) = X^4 - 10X^2 + 1.$$

Die Nullstellen der quadratischen Faktoren sind  $\pm\sqrt{2} \pm \sqrt{3}$ . Über  $\mathbb{Q}(\sqrt{2})$  ist das Minimalpolynom von  $\sqrt{2} + \sqrt{3}$  durch

$$(X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3})) = X^2 - 2\sqrt{2}X - 1$$

gegeben, und die Konjugierten sind  $\sqrt{2} \pm \sqrt{3}$ . Entsprechend ist  $X^2 + 2\sqrt{2}X - 1$  das Minimalpolynom von  $-\sqrt{2} + \sqrt{3}$  über  $\mathbb{Q}(\sqrt{2})$ , und natürlich ist

$$(X^2 + 2\sqrt{2}X - 1)(X^2 - 2\sqrt{2}X - 1) = (X^2 - 1)^2 - 8X^2 = X^4 - 10X^2 + 1.$$

Die Konjugierten von  $\sqrt{2} + \sqrt{3}$  über  $\mathbb{Q}(\sqrt{3})$  sind analog  $\sqrt{2} \pm \sqrt{3}$ , und diejenigen über  $\mathbb{Q}(\sqrt{6})$  schließlich sind  $\pm(\sqrt{2} + \sqrt{3})$ .

- 2) *Sei  $E/K$  eine algebraische Erweiterung. Sind  $E_1/K$  und  $E_2/K$  rein inseparable Zwischenkörper, dann auch deren Durchschnitt  $E_1 \cap E_2/K$  und Kompositum  $E_1E_2/K$ . Insbesondere gibt es für jede algebraische Erweiterung  $E/K$  einen größten Zwischenkörper  $E_i$ , sodass  $E_i/K$  rein inseparabel ist; man nennt  $E_i$  den rein inseparablen Abschluss von  $K$  in  $E$ .*

Seien  $E_1/K$  und  $E_2/K$  rein inseparabel. Dann sind nach F.7.16 alle Elemente aus  $E_1$  und  $E_2$  nur zu sich selbst konjugiert. Da sich jedes Element des Kompositums als  $K$ -Linearkombination von Produkten aus Elementen in  $E_1$  und  $E_2$  schreiben lässt, gilt diese Aussage dann auch für alle Elemente aus  $E_1E_2$ , und nochmalige Anwendung von F.7.16 zeigt dann, dass  $E_1E_2/K$  rein inseparabel ist.

Dass mit einer Erweiterung  $E_1/K$  auch jede Teilerweiterung rein inseparabel ist, folgt sofort aus der Definition D.7.6.

- 3) Sei  $K = \mathbb{F}_2(t)$  und  $f(X) = X^2 + X + t \in K[X]$ . Man zeige mit Vieta, dass die (nach Kronecker existierenden) Wurzeln verschieden sind,  $f$  also separabel ist. (Was passiert, wenn man die Nullstellen von  $f$  mit der quadratischen Formel berechnen will?)

Sei  $f(X) = (X + \beta)(X + \beta')$ . Dann ist  $\beta\beta' = t$  und  $\beta + \beta' = 1$ . Die letzte Gleichung zeigt sofort, dass  $\beta' \neq \beta$  ist, da sonst  $1 = \beta + \beta' = 2\beta = 0$  gelten würde.

Eine Formel wie  $\beta = \frac{-1 \pm \sqrt{1-4t}}{2}$  kann natürlich wegen der  $2 = 0$  im Nenner nicht funktionieren.

- 4) Sei  $K = \mathbb{F}_2(t)$ ,  $E$  der Zerfällungskörper von  $g = X^4 + X^2 + t$ , und  $\alpha$  eine Nullstelle von  $g$ .

- Faktorisiere  $g$  über  $K(\alpha)$  und zeige  $E = K(\alpha)$ .
- Finde den separablen Abschluss  $E_s$  von  $K$  in  $E$ .
- Welches ist die kleinste Potenz  $\alpha^m$  von  $\alpha$ , für welche  $\alpha^m$  separabel ist?
- Finde den rein inseparablen Abschluss  $E_i$  von  $K$  in  $E$ ; ist  $E_s E_i = E$ ?

- a) Mit den Bezeichnungen der vorangehenden Übung ist  $g(X) = X^4 + X^2 + t = (X^2 - \beta)(X^2 - \beta')$ . Ist  $g(\alpha) = 0$ , also z.B.  $\alpha^2 = \beta$ , so wird  $X^2 - \beta = (X - \alpha)^2$ , und  $X^2 - \beta' = X^2 - (1 - \beta) = (X - (\alpha + 1))^2$ . Also finden wir

$$g(X) = X^4 + X^2 + t = (X - \alpha)^2 (X - \alpha - 1)^2.$$

- Offenbar ist  $\alpha$  nicht separabel, also  $E_s$  ein echter Teilkörper von  $K(\alpha)$ . Andererseits ist  $\beta$  separabel über  $K$ , dies zeigt  $E_s = K(\beta)$ .
- Da  $\alpha^2 = \beta$  separabel über  $K$  ist,  $\alpha$  selbst aber nicht, ist  $m = 2$ .
- Um zu sehen, ob  $K$  eine rein inseparable Erweiterung besitzt, machen wir den Ansatz  $\gamma = \sum a_i \alpha^i$  und prüfen, ob wir ein Element mit  $\gamma' = \gamma$  finden können. Koeffizientenvergleich liefert schnell, dass  $\gamma = \alpha + \alpha^2$  ein solches ist; in der Tat ist  $\gamma^2 = \alpha^2 + \alpha^4 = t$ . Also ist  $K(\gamma) = K(\sqrt{t})$  rein inseparabel, und da  $E/K$  nicht rein separabel ist, muss bereits  $E_i = K(\sqrt{t})$  sein.

Wegen  $E_i E_s = K(\alpha + \alpha^2, \alpha^2) = K(\alpha)$  ist hier tatsächlich  $E_i E_s = E$ . Dies ist im allgemeinen jedoch nicht richtig.

- 5) Sei  $K$  ein Körper der Charakteristik  $p$  und  $E/K$  eine endliche Erweiterung. Man zeige: ist  $p \nmid [E : K]$ , dann ist  $E/K$  separabel.

Sei  $E_s$  der separable Abschluss von  $K$  in  $E$ ; einerseits ist nun nach F7.17.c) ist  $E : E_s$  eine Potenz von  $p$ , andererseits ist  $E : E_s$  aber auch ein Teiler von  $E : K$ . Da  $E : K$  nicht durch  $p$  teilbar ist, muss  $E : E_s = 1$  und damit  $E_s = E$  sein.

# Übungen zu Kapitel 8

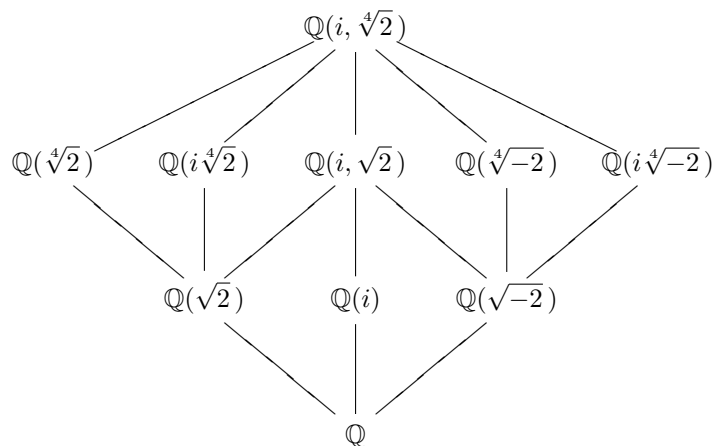
- 1) Zeige  $\sqrt{\alpha} + \sqrt{\beta} = \sqrt{\alpha + \beta + 2\sqrt{\alpha\beta}}$  für positive  $\alpha, \beta \in \mathbb{R}$ .

Dies folgt sofort aus

$$(\sqrt{\alpha} + \sqrt{\beta})^2 = \alpha + \beta + 2\sqrt{\alpha\beta}.$$

Das Ergebnis bleibt in der Form  $\sqrt{\alpha} + \sqrt{\beta} = \pm\sqrt{\alpha + \beta + 2\sqrt{\alpha\beta}}$  über beliebigen Körpern richtig. Damit lassen sich einige hübsche Dinge beweisen.

- a)  $\sqrt{2 + \sqrt{3}} + \sqrt{2 - \sqrt{3}} = \sqrt{6}$ . Wegen  $\sqrt{2 - \sqrt{3}} = 1/\sqrt{2 + \sqrt{3}}$  bedeutet dies, dass  $\sqrt{6} \in \mathbb{Q}(\sqrt{2 + \sqrt{3}})$  ist. Tatsächlich gilt  $\sqrt{2 + \sqrt{3}} = \frac{\sqrt{2} + \sqrt{6}}{2}$ .
- b) Der normale Abschluss  $E$  von  $\mathbb{Q}(\sqrt[4]{m})$  für  $m \in \mathbb{Z}$  enthält  $\sqrt[4]{-4m}$ . Dies folgt aus  $\sqrt{\sqrt{m}} + \sqrt{-\sqrt{m}} = \sqrt[4]{-4m}$ , da  $E$  mit  $\sqrt[4]{m}$  auch  $i\sqrt[4]{m} = \sqrt{-\sqrt{m}}$  enthält. Damit sieht man leicht, dass das Hasse-Diagramm der Teilkörper von  $\mathbb{Q}(\sqrt[4]{2})$  gegeben ist durch



Es ist nämlich  $\mathbb{Q}(\sqrt[4]{-8}) = \mathbb{Q}(\sqrt[4]{-2})$  wegen  $\sqrt[4]{-8}^3 = 4\sqrt[4]{-2}$ . Man beachte auch  $\sqrt[4]{-8} = \sqrt{2}\sqrt[4]{-2} = (1+i)\sqrt[4]{2}$  bei geeigneter Interpretation der Quadratwurzeln.

- c) Der normale Abschluss von  $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$  enthält  $\sqrt{2+2i} = (1+i)\sqrt{1-i}$ . Damit ist es ein Leichtes, das Untergruppendiagramm dieser Diedererweiterung aufzustellen.

- 2) Sei  $K = \mathbb{Q}(\sqrt{2})$  und  $L = \mathbb{Q}(\sqrt{\mu})$  mit  $\mu = 2 + \sqrt{2}$ . Zeige, dass  $L/\mathbb{Q}$  galoissch mit zyklischer Galoisgruppe  $\{1, S, S^2, S^3\}$  der Ordnung 4 ist, dass  $\{1, \sqrt{\mu}, \sqrt{2}, \sqrt{\mu'}\}$  mit  $\mu' = 2 - \sqrt{2}$  eine  $\mathbb{Q}$ -Basis von  $L$  ist, und dass die Operation von  $G(L/\mathbb{Q})$  auf dieser Basis gegeben ist durch

$\nu$	$S(\nu)$	$S^2(\nu)$	$S^3(\nu)$
1	1	1	1
$\sqrt{2 + \sqrt{2}}$	$\sqrt{2 - \sqrt{2}}$	$-\sqrt{2 + \sqrt{2}}$	$-\sqrt{2 - \sqrt{2}}$
$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{2 - \sqrt{2}}$	$-\sqrt{2 + \sqrt{2}}$	$\sqrt{2 - \sqrt{2}}$	$\sqrt{2 + \sqrt{2}}$

Die Konjugierten von  $\sqrt{2 + \sqrt{2}}$  sind  $\pm\sqrt{2 \pm \sqrt{2}}$ . Wegen  $\sqrt{2 + \sqrt{2}}\sqrt{2 - \sqrt{2}} = \sqrt{2}$  ist  $\sqrt{2 - \sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2 + \sqrt{2}}} \in L$ , folglich  $L$  normal über  $\mathbb{Q}$ . Sei  $S$  der Automorphismus, der  $\sqrt{2 + \sqrt{2}}$  auf  $\sqrt{2 - \sqrt{2}}$  abbildet; dann ist  $S(2 + \sqrt{2}) = 2 - \sqrt{2}$ , also  $S$  eine Fortsetzung des nichttrivialen Automorphismus  $\sigma$  von  $K/\mathbb{Q}$ . Um zu zeigen, dass  $L/\mathbb{Q}$  zyklisch ist, genügt der Nachweis, dass  $S^2$  nicht die Identität ist. Nun ist

$$\begin{aligned} S^2(\sqrt{2 + \sqrt{2}}) &= S(\sqrt{2 - \sqrt{2}}) = S\left(\frac{\sqrt{2}}{\sqrt{2 + \sqrt{2}}}\right) = \frac{-\sqrt{2}}{\sqrt{2 - \sqrt{2}}} \\ &= \frac{-\sqrt{2}\sqrt{2 + \sqrt{2}}}{\sqrt{2}} = -\sqrt{2 + \sqrt{2}}, \end{aligned}$$

also  $S$  ein Automorphismus der Ordnung 4 und damit  $G(L/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ .

- 3) Sei  $K = \mathbb{Q}(\sqrt{m})$  ein quadratischer Körper und  $L = K(\sqrt{\mu})$  für  $\mu = a + b\sqrt{m} \neq 0$ .
- Zeige, dass  $L/\mathbb{Q}$  genau dann normal ist, wenn  $N(\mu) := a^2 - mb^2$  ein Quadrat in  $K$  ist.
  - Zeige, dass  $L/\mathbb{Q}$  genau dann zyklisch ist, wenn  $N(\mu)$  ein Quadrat in  $K$ , aber keines in  $\mathbb{Q}$  ist; genauer: genau dann, wenn  $a^2 - mb^2 = mc^2$  für ein  $c \in \mathbb{Q}$  gilt.
  - Zeige, dass sich der quadratische Körper  $K = \mathbb{Q}(\sqrt{m})$  genau dann in eine zyklische Erweiterung  $L/\mathbb{Q}$  vom Grad 4 einbetten lässt, wenn  $m$  die Summe zweier Quadrate in  $\mathbb{Q}$  ist.
- a) Sei  $\sigma$  der nichttriviale Automorphismus von  $K/\mathbb{Q}$ . Die Konjugierten von  $\sqrt{\mu}$  sind dann  $\pm\sqrt{\mu}$  und  $\pm\sqrt{\mu}^\sigma$ , und  $L$  wird genau dann normal über  $\mathbb{Q}$  sein, wenn

$\sqrt{\mu^\sigma} \in L$  ist. Ein Ansatz  $\sqrt{\mu^\sigma} = \alpha + \beta\sqrt{\mu}$  mit  $\alpha, \beta \in K$  liefert sofort  $\alpha = 0$ , und dies bedeutet, dass  $L/\mathbb{Q}$  genau dann normal ist, wenn  $\mu^\sigma = \beta^2\mu$  für ein  $\beta \in K$  gilt. Multiplikation mit  $\mu$  liefert dann wegen  $\mu^\sigma\mu = N(\mu)$  die Behauptung.

- b) Wie in Übung 2 sei  $S$  der Automorphismus von  $L/\mathbb{Q}$ , welcher  $\sqrt{\mu}$  auf  $\sqrt{\mu^\sigma} := \beta\sqrt{\mu}$  abbildet. Dann ist  $S^2(\sqrt{\mu}) = S(\beta\sqrt{\mu}) = \beta^\sigma\beta\sqrt{\mu} = N(\beta)\sqrt{\mu}$ . Nun ist  $\beta^2 = \mu^{\sigma-1}$ , folglich  $N(\beta)^2 = 1$  und daher  $N(\beta) = \pm 1$ . Die Galoisgruppe von  $L/\mathbb{Q}$  wird genau dann zyklisch sein, wenn  $S$  Ordnung 4 hat, wenn also  $S^2$  nicht die Identität ist. Nach unseren Rechnungen ist dies genau dann der Fall, wenn  $N(\beta) = -1$  ist.

Nun ist  $(\beta\mu)^\sigma = \beta^\sigma\beta^2\mu = N(\beta)\beta\mu$ , also genau dann  $\beta\mu \in K$ , wenn  $N(\beta) = +1$  ist. Wegen  $N(\mu) = (\beta\mu)^2$  heißt dies, dass  $N(\mu) \in \mathbb{Q}$  äquivalent ist zu  $N(\beta) = +1$ .

Im Falle  $N(\beta) = -1$  ist  $(\beta\mu)^\sigma = -\beta\mu$ , folglich  $\beta\mu\sqrt{m}$  invariant unter  $\sigma$  und damit  $\beta\mu\sqrt{m} \in \mathbb{Q}$ . Dies bedeutet, dass es ein  $c \in \mathbb{Q}$  gibt mit  $\beta\mu = c\sqrt{m}$ , und dies ist genau die Behauptung.

- c) Ist  $m = r^2 + s^2$ , so ist  $L = K(\sqrt{\mu})$  mit  $\mu = m + r\sqrt{m}$  eine zyklische Erweiterung, die  $K = \mathbb{Q}(\sqrt{m})$  enthält.

Sei umgekehrt  $L = K(\sqrt{\mu})$  eine solche Erweiterung. Dann ist  $\mu = a + b\sqrt{m}$  mit  $a^2 - mb^2 = mc^2$  für  $a, b, c \in \mathbb{Q}$ . Dies liefert  $m = (\frac{mb}{a})^2 + (\frac{mc}{a})^2$  (beachte, dass  $a \neq 0$  ist, da sonst  $-mb^2 = mc^2$  gelten müsste).

- 4) Sei  $K/k$  eine Galoiserweiterung mit Gruppe  $G = G(K/k)$ , und  $L = K(\sqrt{\mu})$  eine quadratische Erweiterung. Zeige: Ist  $L/k$  galoissch, dann auch jede Erweiterung  $L' = K(\sqrt{c\mu})$  mit  $c \in k^\times$ , und falls  $c\mu$  kein Quadrat in  $K$  ist, so gilt  $G(L'/k) \simeq G(L/k)$ .

Sei  $\nu = c\mu$ ; dann ist  $\nu^{\sigma-1} = \mu^{\sigma-1}$  für alle  $\sigma \in G$ ; also sind die "Invarianten"  $\alpha_\sigma$  und insbesondere das Faktorensystem  $\beta : G \rightarrow W_2$  für beide Erweiterungen dieselben. Ist  $c\mu$  kein Quadrat, haben beide Erweiterungen  $L$  und  $L'$  Galoisgruppen derselben Ordnung, welche durch das Faktorensystem eindeutig bestimmt sind; in diesem Fall muss also  $G(L'/k) \simeq G(L/k)$  gelten.

- 5) Die Quaternionenalgebra  $\mathbb{H}$  ist definiert als der  $\mathbb{R}$ -Vektorraum mit Basis  $\{1, i, j, k\}$ , wobei die Multiplikation durch die Relationen  $i^2 = j^2 = k^2 = -1$  und  $ij = k = -ji$  festgelegt ist. Man zeige, dass  $\{\pm 1, \pm i, \pm j, \pm k\}$  eine zur Quaternionengruppe  $Q_8$  isomorphe Gruppe ist.

Man rechnet leicht nach, dass durch  $i \mapsto S$  und  $j \mapsto T$  ein Isomorphismus auf die Gruppe  $Q_8$  definiert wird, deren Elemente sich in der Form  $S^a T^b$  mit  $0 \leq a \leq 3$  und  $0 \leq b \leq 1$  schreiben lassen, und welche den Relationen  $S^2 = T^2$ ,  $S^4 = 1$  und  $TS = S^3T$  genügen.

- 6) Sei  $G = \langle \sigma \rangle$  eine zyklische Gruppe der Ordnung  $n$ ,  $K/k$  eine galoissche Erweiterung mit Galoisgruppe  $G$ , und  $L = K(\sqrt{\mu})$  eine quadratische Erweiterung.

- a) Zeige, dass  $L/k$  genau dann normal ist, wenn  $\mu^{\sigma-1} = \alpha_\sigma^2$  für ein  $\alpha_\sigma \in K$  ist (man muss diese Bedingung also nur für die Erzeugende  $\sigma$  nachprüfen).  
 b) Zeige, dass man in diesem Fall

$$\alpha_{\sigma^j} = \alpha_\sigma^{1+\sigma+\dots+\sigma^{j-1}}$$

wählen kann, und dass der entsprechende 2-Kozykel dann durch

$$\beta(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{falls } i+j < n, \\ \alpha_\sigma^\nu & \text{falls } i+j \geq n. \end{cases}$$

für  $0 \leq i, j < n$  gegeben ist, wobei wir  $\nu = 1 + \sigma + \dots + \sigma^{n-1}$  gesetzt haben.

- c) Ist  $n$  ungerade, so kann man das Vorzeichen von  $\alpha_\sigma$  so wählen, dass  $\alpha_\sigma^\nu = 1$  wird; in diesem Fall ist  $[\beta] = 1$ , und  $G(L/k) \simeq \mathbb{Z}/2 \times \mathbb{Z}/n \simeq \mathbb{Z}/2n$ .  
 d) Ist  $n$  dagegen gerade, so gilt

$$G(L/k) \simeq \begin{cases} \mathbb{Z}/n \times \mathbb{Z}/2 & \text{falls } \alpha_\sigma^\nu = +1, \\ \mathbb{Z}/2n & \text{falls } \alpha_\sigma^\nu = -1. \end{cases}$$

- a) Ist  $\mu^{\sigma-1} = \alpha_\sigma^2$  für ein  $\sigma$ , welches  $G$  erzeugt, dann können wir die  $\alpha_{\sigma^j}$  wie in b) wählen.  
 b) Aus  $\mu^\sigma = \alpha_\sigma^2 \mu$  folgt durch wiederholtes Anwenden von  $\sigma$

$$\begin{aligned} \mu^{\sigma^2} &= (\alpha_\sigma^2 \mu)^\sigma = \alpha_\sigma^{2\sigma} \mu^\sigma = \alpha_\sigma^{2\sigma} \alpha_\sigma^2 \mu, \\ \mu^{\sigma^3} &= (\alpha_\sigma^{2(1+\sigma)} \mu)^\sigma = \alpha_\sigma^{2(\sigma+\sigma^2)} \mu^\sigma = (\alpha_\sigma^{1+\sigma+\sigma^2})^2 \mu, \end{aligned}$$

sodass wir  $\alpha_{\sigma^2} = \alpha_\sigma^{1+\sigma}$ ,  $\alpha_{\sigma^3} = \alpha_\sigma^{1+\sigma+\sigma^2}$  etc. wählen können.

Das dazugehörige Faktorensystem ist gegeben durch  $\beta(\sigma^i, \sigma^j) = \alpha_{\sigma^i}^{\sigma^j} \alpha_{\sigma^j} \alpha_{\sigma^{i+j}}^{-1}$ . Ist  $i+j < n$ , findet man sofort  $\beta(\sigma^i, \sigma^j) = 1$ . Ist  $i+j = n$ , so wird  $\sigma^{i+j} = 1$ , also  $\alpha_{\sigma^{i+j}} = \alpha_1 = 1$  und damit  $\beta(\sigma^i, \sigma^j) = \alpha_\sigma^{1+\sigma+\sigma^2+\dots+\sigma^{n-1}} = \alpha_\sigma^\nu$ . Dieselbe Formel gilt offenbar auch für  $i+j > n$ .

- c) Ist  $n$  ungerade, so ist  $(-\alpha_\sigma)^\nu = -\alpha_\sigma^\nu$ , und wir können das Vorzeichen von  $\alpha_\sigma$  so wählen, dass  $\alpha_\sigma^\nu = 1$  wird. Dann wird aber  $[\beta] = 1$  und  $G(L/k) \simeq \mathbb{Z}/2 \times \mathbb{Z}/n \simeq \mathbb{Z}/2n$ .  
 d) Ist  $n$  gerade und  $\alpha_\sigma^\nu = +1$ , so ist wie eben  $[\beta] = 1$  und  $G(L/k) \simeq \mathbb{Z}/2 \times \mathbb{Z}/n$ . Ist dagegen  $\alpha_\sigma^\nu = -1$ , so wird  $G(L/k) \simeq \mathbb{Z}/2n$ . Ist nämlich  $S$  ein Automorphismus, der  $\sqrt{\mu}$  auf  $\alpha_\sigma \sqrt{\mu}$  abbildet, so ist  $S$  eine Fortsetzung von  $\sigma$  und hat damit Ordnung  $n$  oder  $2n$ ; jetzt findet man  $S^n(\sqrt{\mu}) = \alpha_\sigma^\nu \sqrt{\mu} = -\sqrt{\mu}$ , und folglich hat  $S$  die Ordnung  $2n$ .

Als Anwendung betrachte man z.B.  $\mu = 2 + \sqrt{2}$ ; ist  $\sigma$  der nichttriviale Automorphismus von  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ , so ist

$$\mu^{\sigma-1} = \frac{2 - \sqrt{2}}{2 + \sqrt{2}} = \frac{(2 - \sqrt{2})(2 + \sqrt{2})}{(2 + \sqrt{2})^2} = \left( \frac{\sqrt{2}}{2 + \sqrt{2}} \right)^2.$$

Wir setzen  $\alpha_\sigma = \frac{\sqrt{2}}{2 + \sqrt{2}}$ . Dann folgt

$$\alpha_\sigma^\nu = \alpha_\sigma^{1+\sigma} = \frac{\sqrt{2}}{2 + \sqrt{2}} \frac{-\sqrt{2}}{2 - \sqrt{2}} = \frac{-2}{2} = -1,$$

folglich ist  $G(\mathbb{Q}(\sqrt{2 + \sqrt{2}})/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ .

- 7) Sei  $K/k$  eine Galoiserweiterung mit Gruppe  $G$ ; sei  $H$  eine Untergruppe von  $G$  und  $F$  der Fixkörper von  $H$ . Ist die quadratische Erweiterung  $L = K(\sqrt{\mu})$  galoissch über  $k$ , dann ist  $L$  auch galoissch über  $F$ .

- a) Gehört der 2-Kozykel  $\beta$  zu  $L/k$ , so ist der zu  $L/F$  gehörige 2-Kozykel die Einschränkung von  $\beta$  auf  $H \times H$ .
- b) Die Einschränkung liefert einen Gruppenhomomorphismus

$$\text{res}_{G,H} : H^2(G, W_2) \longrightarrow H^2(H, W_2).$$

- c) Ist  $H = \langle \sigma \rangle$  eine zyklische Untergruppe der geraden Ordnung  $n$ , so wird  $L/F$  genau dann zyklisch sein, wenn  $\alpha_\sigma^\nu = -1$ , also  $\text{res}_{G,H} [\beta] \neq 1$  ist.

- a) Sei  $\bar{\beta}$  der zu  $L/F$  gehörige 2-Kozykel; für alle  $\sigma, \tau \in H$  ist dann nach Definition  $\bar{\beta}(\sigma, \tau) = \beta(\sigma, \tau)$ , also  $\bar{\beta}$  die Einschränkung von  $\beta$  auf  $H \times H$ .
- b) Dies ist eine Folgerung der trivialen Beobachtung, dass es egal ist, ob man Kozykel erst multipliziert und dann einschränkt oder andersherum.
- c) Ist  $n$  ungerade, so ist die Erweiterung  $L/F$  immer zyklisch. Sei also  $n$  gerade; dann haben wir in der vorangegangenen Übung gesehen, dass  $L/F$  genau dann zyklisch ist, wenn  $\bar{\beta}(\sigma, \sigma) = \alpha_\sigma^\nu = -1$ , also  $\bar{\beta} = \text{res}_{G,H} [\beta] \neq 1$  ist.

- 8) Sei  $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ . Zeige dass die durch  $\mu = 2 + \sqrt{2}$ ,  $5 + 2\sqrt{5}$ ,  $10 + 3\sqrt{10}$  definierten Erweiterungen  $L = K(\sqrt{\mu})$  die Galoisgruppe  $G(L/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$  haben, die entsprechenden 2-Kozykel aber nicht äquivalent sind. Insbesondere enthält  $H^2(G(K/\mathbb{Q}), W_2)$  drei verschiedene Elemente  $[\beta]$  mit  $W_2 \times_\beta G \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$ .



Sei  $G = G(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ , und seien  $\sigma, \tau, \sigma\tau$  so gewählt, dass sie  $\sqrt{2}, \sqrt{5}$ , bzw.  $\sqrt{10}$  festlassen. Dann finden wir

$\mu$	$2 + \sqrt{2}$	$5 + 2\sqrt{5}$	$10 + 3\sqrt{10}$
$\alpha_\sigma$	1	$2 + \sqrt{5}$	$3 + \sqrt{10}$
$\alpha_\tau$	$1 + \sqrt{2}$	1	$3 + \sqrt{10}$
$\alpha_{\sigma\tau}$	$1 + \sqrt{2}$	$2 + \sqrt{5}$	1

Die Formel

$$\beta'(\sigma, \tau) = \beta(\sigma, \tau)\gamma(\sigma, \tau) \quad \text{mit} \quad \gamma(\sigma, \tau) = h(\sigma)^\tau h(\tau)h(\sigma\tau)^{-1}$$

auf Seite 137 zeigt im vorliegenden Fall, dass  $\gamma(\sigma, \sigma) = h(\sigma^2) = h(1) = 1$  ist, wenn wir alle Kozykel normiert wählen. Daher sind die Werte  $\beta(\sigma, \sigma)$ ,  $\beta(\tau, \tau)$  und  $\beta(\sigma\tau, \sigma\tau)$  unabhängig von der Wahl der Repräsentanten der Klassen. Die Tabelle

$\mu$	$2 + \sqrt{2}$	$5 + 2\sqrt{5}$	$10 + 3\sqrt{10}$
$\beta(\sigma, \sigma)$	+1	-1	-1
$\beta(\tau, \tau)$	-1	+1	-1
$\beta(\sigma\tau, \sigma\tau)$	-1	-1	+1

zeigt daher, dass die zu den drei Elementen  $\mu$  gehörigen Klassen  $[\beta]$  verschieden sind.

- 9) Sei  $K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$ . Zeige dass die durch  $\mu = 3 + \sqrt{2}, 4 + \sqrt{2}, 3 + \sqrt{7}, 4 + \sqrt{14}$  definierten Erweiterungen  $L = K(\sqrt{\mu})$  die Galoisgruppe  $G(L/\mathbb{Q}) \simeq D_8$  besitzen. Welche der dazugehörigen 2-Kozykel sind äquivalent?

Analog zu oben sei  $G(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ , und  $\sigma, \tau, \sigma\tau$  so gewählt, dass sie  $\sqrt{2}, \sqrt{7}$ , bzw.  $\sqrt{14}$  festlassen. Dann finden wir wie oben

$\mu$	$3 + \sqrt{2}$	$4 + \sqrt{2}$	$3 + \sqrt{7}$	$4 + \sqrt{14}$
$\alpha_\sigma$	1	1	$\frac{3+\sqrt{7}}{\sqrt{2}}$	$2\sqrt{2} + \sqrt{7}$
$\alpha_\tau$	$\frac{3+\sqrt{2}}{\sqrt{7}}$	$\frac{1+2\sqrt{2}}{\sqrt{7}}$	1	$2\sqrt{2} + \sqrt{7}$
$\alpha_{\sigma\tau}$	$\frac{3+\sqrt{2}}{\sqrt{7}}$	$\frac{1+2\sqrt{2}}{\sqrt{7}}$	$\frac{3+\sqrt{7}}{\sqrt{2}}$	1
$\beta(\sigma, \sigma)$	+1	+1	+1	+1
$\beta(\tau, \tau)$	+1	-1	+1	-1
$\beta(\sigma\tau, \sigma\tau)$	-1	+1	-1	+1

Die Berechnung der Galoisgruppe wird nun wie auf S. 139 durchgeführt, und man erhält in allen vier Fällen eine zu  $D_4$  isomorphe Gruppe. Offenbar können nur der

erste und dritte, sowie der zweite und vierte Kozykel zueinander äquivalent sein, und dass dies der Fall ist, rechnet man leicht nach.

Man kann die Äquivalenz auch mittels der Übungen 8.1 und 8.4 nachweisen: zum einen ist nämlich

$$\sqrt{3 + \sqrt{2}} + \sqrt{3 - \sqrt{2}} = \sqrt{2(3 + \sqrt{7})},$$

also  $K(\sqrt{3 + \sqrt{2}}) = K(\sqrt{2(3 + \sqrt{7})})$ , und nach Übung 8.4 haben  $K(\sqrt{3 + \sqrt{7}})$  und diese Erweiterung äquivalente Kozykel.

Es ist im Übrigen nicht schwer zu zeigen, dass die abstrakte Struktur der Galoisgruppe im Falle, dass  $G(K/\mathbb{Q})$  die Kleinsche Vierergruppe ist, nur von der Anzahl der negativen Werte von  $\beta(\sigma, \sigma)$ ,  $\beta(\tau, \tau)$  und  $\beta(\sigma\tau, \sigma\tau)$  abhängt. Man erhält die elementar-abelsche Gruppe  $(\mathbb{Z}/2)^3$ ,  $D_8$ ,  $\mathbb{Z}/4 \times \mathbb{Z}/2$  und  $Q_8$ , je nachdem keines, eines, zwei oder drei der Vorzeichen negativ sind. Weiter ist  $\beta(\rho, \rho)$  genau dann gleich  $-1$ , wenn  $L$  über dem Fixkörper von  $\rho$  zyklisch ist.

- 10) Zeige, dass  $H^2(\mathbb{Z}/2 \times \mathbb{Z}/2, W_2)$  mindestens 8 Elemente besitzt.

Die Ordnung von  $H^2(\mathbb{Z}/2 \times \mathbb{Z}/2, W_2)$  ist eine Zweierpotenz; in den beiden vorhergehenden Übungen haben wir sechs verschiedene Elemente konstruiert. Also hat die Gruppe  $H^2(\mathbb{Z}/2 \times \mathbb{Z}/2, W_2)$  mindestens Ordnung 8.

In der Tat folgt aus den folgenden Übungen, dass sich jede Gruppe der Ordnung 8 mit einer Faktorgruppe vom Typ  $\mathbb{Z}/2 \times \mathbb{Z}/2$  so konstruieren lässt, und dass es nur die Möglichkeiten  $(\mathbb{Z}/2)^3$ ,  $\mathbb{Z}/2 \times \mathbb{Z}/4$ ,  $D_8$  und  $h_8$  gibt. Da zu den Erweiterungen  $(\mathbb{Z}/2)^3$  und  $Q_8$  nur jeweils eine Kozykelklasse gehört, hat  $H^2(\mathbb{Z}/2 \times \mathbb{Z}/2, W_2)$  genau 8 Elemente.

- 11) Zeige, dass die Erweiterung  $\mathbb{Q}(\sqrt{2 + \sqrt{2 + \sqrt{2}}})$  galoissch über  $\mathbb{Q}$  mit zyklischer Galoisgruppe der Ordnung 8 ist. Verallgemeinerung?

Am einfachsten geht dies mit der Beobachtung, dass die Erweiterung in einem Kreiskörper enthalten ist. Es ist nämlich  $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ , und wegen

$$(\zeta_{2^{n+1}} + \zeta_{2^{n+1}}^{-1})^2 = 2 + \zeta_{2^n} + \zeta_{2^n}^{-1}$$

erhält man daraus induktiv  $\zeta_{16} + \zeta_{16}^{-1} = \sqrt{2 + \sqrt{2}}$ ,  $\zeta_{32} + \zeta_{32}^{-1} = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$  etc.

Nun ist der Kreiskörper  $K = \mathbb{Q}(\zeta)$  mit  $\zeta = \zeta_{2^n}$  abelsch über  $\mathbb{Q}$  mit Galoisgruppe  $G \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-2}$ . Da die komplexe Konjugation kein Quadrat sein kann (jeder Automorphismus muss  $i$  auf  $i$  oder  $-i$  abbilden, also ist  $\tau^2(i) = i$ ), dürfen wir  $G = \langle \sigma, \tau \rangle$  schreiben, wo  $\sigma$  die komplexe Konjugation bedeutet. Die Galoisgruppe von  $K/E$  für  $E = \mathbb{Q}(\zeta + \zeta^{-1})$  ist dann  $\langle \sigma \rangle$ , diejenige von  $E/\mathbb{Q}$  also  $G/\langle \sigma \rangle \simeq \langle \tau \rangle$ . Also ist die Erweiterung zyklisch.

Der Nachweis mit den in diesem Kapitel vorgestellten Methoden ist etwas technisch. Wir wissen, dass  $K = \mathbb{Q}(\sqrt{2} + \sqrt{2})$  eine zyklische Erweiterung vom Grad 4 über  $\mathbb{Q}$  ist, deren Galoisgruppe von  $\sigma : \sqrt{2} + \sqrt{2} \mapsto \sqrt{2} - \sqrt{2}$  erzeugt wird. Quadrieren zeigt  $\sigma(\sqrt{2}) = -\sqrt{2}$ , und aus  $\sqrt{2} - \sqrt{2} = \frac{\sqrt{2}}{\sqrt{2} + \sqrt{2}}$  liest man ab, dass  $\sigma^2(\sqrt{2} + \sqrt{2}) = -\sqrt{2} + \sqrt{2}$  ist.

Um die Behauptung zu zeigen, müssen wir zuerst nachrechnen, dass  $\frac{2 + \sqrt{2} - \sqrt{2}}{2 + \sqrt{2} + \sqrt{2}}$  ein Quadrat in  $K$  ist. Dies ist genau dann der Fall, wenn  $(2 + \sqrt{2} - \sqrt{2})(2 + \sqrt{2} + \sqrt{2})$  ein Quadrat ist. Wir finden nun

$$\begin{aligned} (2 + \sqrt{2} - \sqrt{2})(2 + \sqrt{2} + \sqrt{2}) &= 4 + 2(\sqrt{2} - \sqrt{2} + \sqrt{2} + \sqrt{2}) + \sqrt{2} \\ &= 4 + 2\sqrt{4 + 2\sqrt{2}} + \sqrt{2} \\ &= 4 + 2\sqrt{2}\sqrt{2 + \sqrt{2}} + \sqrt{2} \\ &= (\sqrt{2} + \sqrt{2 + \sqrt{2}})^2. \end{aligned}$$

Damit ist die Erweiterung normal über  $\mathbb{Q}$ ; die Berechnung der Galoisgruppe erfordert noch den Nachweis, dass  $\alpha_\sigma^\nu = -1$  ist für

$$\alpha_\sigma = \frac{2 + \sqrt{2} - \sqrt{2}}{2 + \sqrt{2} + \sqrt{2}}.$$

Wegen  $\nu = 1 + \sigma + \sigma^2 + \sigma^3 = (1 + \sigma^2)(1 + \sigma)$  können wir diese Rechnung in zwei Schritte aufteilen:

$$\begin{aligned} \alpha_\sigma^{1+\sigma^2} &= \frac{2 + \sqrt{2} - \sqrt{2}}{2 + \sqrt{2} + \sqrt{2}} \frac{2 - \sqrt{2} - \sqrt{2}}{2 - \sqrt{2} + \sqrt{2}} &= -\frac{\sqrt{2}}{2 + \sqrt{2}} \\ \alpha_\sigma^\nu &= -\frac{\sqrt{2}}{2 + \sqrt{2}} \frac{\sqrt{2}}{2 - \sqrt{2}} &= -1. \end{aligned}$$

- 12) Sei  $K = k(\sqrt{m}, \sqrt{n})$  eine Erweiterung mit Galoisgruppe  $\mathbb{Z}/2 \times \mathbb{Z}/2$ . Seien  $k_j$  ( $j = 1, 2, 3$ ) die drei quadratischen Zwischenkörper von  $K/k$ . Zeige, dass eine quadratische Erweiterung  $L/K$  genau dann normal über  $k$  ist, wenn sie normal über allen  $k_j$  ist.

Sei  $L = K(\sqrt{\mu})$ , und seien  $\sigma_j$  die nichttrivialen Automorphismen von  $K/k_j$ . Da alle  $L/k_j$  normal sind, ist  $\mu^{\sigma_j} = \alpha_j^2 \mu$  für geeignete  $\alpha_j \in K$ . Da aber  $G(K/k) = \{1, \sigma_1, \sigma_2, \sigma_3\}$  ist, folgt dann  $\mu^\sigma = \alpha_\sigma^2 \mu$  für alle  $\sigma \in G$ , und damit ist  $L/k$  normal. Offenbar genügt es anzunehmen, dass  $L/k_j$  über zwei der drei quadratischen Zwischenkörper normal ist.

- 13) Sei  $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$  eine biquadratische Erweiterung von  $\mathbb{Q}$ . Seien weiter  $M = K(\sqrt{\mu})$  und  $N = K(\sqrt{\nu})$  Erweiterungen mit  $G(M/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/4$  und  $G(N/\mathbb{Q}) \simeq D_8$ , wobei  $M$  über  $\mathbb{Q}(\sqrt{m})$  und  $\mathbb{Q}(\sqrt{n})$ , und  $N$  über  $\mathbb{Q}(\sqrt{mn})$  zyklisch ist. Zeige, dass dann  $G(L/\mathbb{Q}) \simeq Q_8$  für  $L = K(\sqrt{\mu\nu})$  gilt.

Die Information darüber, über welchen Körpern  $M$  und  $N$  zyklisch sind, geben uns Auskunft über einige Werte der dazugehörigen Kozykeln: sind  $\sigma, \tau$  und  $\sigma\tau$  die nichttrivialen Automorphismen von  $K/\mathbb{Q}(\sqrt{m})$ ,  $K/\mathbb{Q}(\sqrt{n})$ , bzw.  $K/\mathbb{Q}(\sqrt{mn})$ , dann finden wir

	$\mu$	$\nu$	$\mu\nu$
$\beta(\sigma, \sigma)$	-1	+1	-1
$\beta(\tau, \tau)$	-1	+1	-1
$\beta(\sigma\tau, \sigma\tau)$	+1	-1	-1

Da die Anzahl der negativen Werte unter den Zahlen  $\beta(\rho, \rho)$  für  $\rho \in G(K/\mathbb{Q})$  gleich der Anzahl der Elemente der Ordnung 4 in  $G(L/\mathbb{Q})$  ist, folgt die Behauptung aus der Beobachtung, dass  $(\mathbb{Z}/2)^3$ ,  $D_8$ ,  $\mathbb{Z}/4 \times \mathbb{Z}/2$  und  $Q_8$  genau 0, 1, 2, bzw. 3 Elemente der Ordnung 4 besitzen.

- 14) Zeige, dass  $W_2 \times_{\beta} G$  für jeden 2-Kozykel  $\beta$  durch (8.21) zur Gruppe wird (vgl. die Bemerkung nach F8.11).

Die Abgeschlossenheit bezüglich der Multiplikation ist klar. Sei nun  $\beta$  ein normierter Kozykel.

- Existenz der Eins: es ist  $(s, \sigma)(1, 1) = (s\beta(\sigma, 1), \sigma) = (s, \sigma)$ .
- Existenz des Inversen: es ist  $(s, \sigma)(t, \sigma^{-1}) = (st\beta(\sigma, \sigma^{-1}), 1) = (1, 1)$ , wenn wir  $t = s\beta(\sigma, \sigma^{-1})$  setzen.
- Assoziativität: wir haben

$$\begin{aligned} [(s, \sigma)(t, \tau)](r, \rho) &= (st\beta(\sigma, \tau), \sigma\tau)(r, \rho) = (str\beta(\sigma, \tau)\beta(\sigma\tau, \rho), \sigma\tau\rho), \\ (s, \sigma)[(t, \tau)(r, \rho)] &= (s, \sigma)(tr\beta(\tau, \rho), \tau\rho) = (str\beta(\tau, \rho)\beta(\sigma, \tau\rho), \sigma\tau\rho). \end{aligned}$$

Daher ist die Assoziativität eine Folge der Kozykelrelation

$$\beta(\sigma, \tau)\beta(\sigma\tau, \rho) = \beta(\tau, \rho)\beta(\sigma, \tau\rho).$$

- 15) Sei  $[\beta] \in H^2(G, W_2)$ , und  $\beta' \in [\beta]$ . Dann ist  $\beta'(\sigma, \tau) = \beta(\sigma, \tau)h(\sigma)^{\tau}h(\tau)h(\sigma\tau)$  für eine Abbildung  $h : G \rightarrow W_2$ . Zeige, dass durch  $\phi(s, \sigma) = (sh(\sigma), \sigma)$  ein Gruppenhomomorphismus von  $\Gamma = W_2 \times_{\beta} G$  nach  $\Gamma' = W_2 \times_{\beta'} G$  definiert wird, mit dem

das Diagramm

$$\begin{array}{ccccccccc}
 1 & \longrightarrow & W_2 & \longrightarrow & \Gamma & \xrightarrow{p} & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \phi & & \downarrow & & \\
 1 & \longrightarrow & W_2 & \longrightarrow & \Gamma' & \xrightarrow{p'} & G & \longrightarrow & 1
 \end{array}$$

kommutativ wird, in welchem die Homomorphismen  $W_2 \rightarrow W_2$  und  $G \rightarrow G$  die identischen Abbildungen, und  $p : \Gamma \rightarrow G$  sowie  $p' : \Gamma' \rightarrow G$  die Projektionen auf den zweiten Faktor sind. Zeige auch, dass  $\phi$  ein Isomorphismus ist.

Die Homomorphie-Eigenschaft ist leicht nachzuweisen:

$$\begin{aligned}
 \phi((s, \sigma))\phi((t, \tau)) &= (sh(\sigma), \sigma)(th(\tau), \tau) = (sth(\sigma)h(\tau)\beta'(\sigma, \tau), \sigma\tau) \\
 &= (sth(\sigma)h(\tau)\beta(\sigma, \tau)h(\sigma)h(\tau)h(\sigma\tau), \sigma\tau) \\
 &= (sth(\sigma\tau)\beta(\sigma, \tau), \sigma\tau) = \phi(st\beta(\sigma, \tau), \sigma\tau) \\
 &= \phi((s, \sigma)(t, \tau)).
 \end{aligned}$$

Hierbei haben wir benutzt, dass  $h$  nur die Werte  $\pm 1$  annimmt, also  $h(\rho) = h(\rho)^{-1}$  usw. gilt. Die Kommutativität der beiden Quadrate ist offensichtlich. Damit bleibt noch zu zeigen, dass  $\phi$  ein Isomorphismus ist. Dies lässt sich hier ganz leicht direkt nachweisen, wird aber offensichtlich, wenn man das Schlangenlemma kennt und auf dieses Diagramm anwendet.

16) Ist  $\Gamma$  eine endliche Gruppe und die Sequenz

$$1 \longrightarrow W_2 \longrightarrow \Gamma \xrightarrow{p} G \longrightarrow 1 \quad (8.1)$$

exakt, so kann man wegen der Surjektivität von  $p$  zu jedem  $\sigma \in G$  ein  $a_\sigma \in \Gamma$  wählen mit  $p(a_\sigma) = \sigma$ ; solche Abbildungen  $a : G \rightarrow \Gamma; \sigma \mapsto a_\sigma$  nennt man Schnitte.

- a) Sei  $a : \Gamma \rightarrow G$  ein Schnitt. Dann ist  $a_\sigma a_\tau a_{\sigma\tau}^{-1} \in \text{Kern } p = W_2$ .
- b) Durch  $\beta(\sigma, \tau) = a_\sigma a_\tau a_{\sigma\tau}^{-1}$  wird für jeden Schnitt  $a$  ein 2-Kozykel  $\beta : G \rightarrow W_2$  definiert. Eine andere Wahl des Schnittes liefert einen zu  $\beta$  äquivalenten 2-Kozykel.
- c) Ist  $[\beta]$  das zur Gruppenerweiterung (8.1) gehörige Element von  $H^2(G, W_2)$ , so ist  $W_2 \times_\beta G \simeq \Gamma$ .

- a) Aus  $1 = p(1) = p(a_{\sigma\tau} a_{\sigma\tau}^{-1}) = p(a_{\sigma\tau})p(a_{\sigma\tau}^{-1})$  folgt  $p(a_{\sigma\tau}^{-1}) = (\sigma\tau)^{-1}$ . Daher ist  $p(a_\sigma a_\tau a_{\sigma\tau}^{-1}) = \sigma\tau(\sigma\tau)^{-1} = 1$ .

- b) Es ist nur die Kozykelrelation nachzurechnen. Wir finden

$$\begin{aligned}
 \beta(\sigma, \tau)\beta(\sigma\tau, \rho) &= a_\sigma a_\tau a_{\sigma\tau}^{-1} a_{\sigma\tau} a_\rho a_{\sigma\tau\rho}^{-1} = a_\sigma a_\tau a_\rho a_{\sigma\tau\rho}^{-1}, \\
 \beta(\sigma, \tau\rho)\beta(\tau, \rho) &= a_\sigma a_{\tau\rho} a_{\sigma\tau\rho}^{-1} a_\tau a_\rho a_{\tau\rho}^{-1} = a_\sigma a_\tau a_\rho a_{\sigma\tau\rho}^{-1}.
 \end{aligned}$$

Sei nun  $b : G \longrightarrow \Gamma$  ein weiterer Schnitt. Wegen  $p(b_\sigma) = p(a_\sigma) = 1$  ist dann  $b_\sigma = sa_\sigma$  für ein  $s \in W_2$ , und wir können eine Abbildung  $h : G \longrightarrow W_2$  definieren, indem wir  $h(\sigma) = b_\sigma/a_\sigma$  setzen. Ist dann  $\beta'(\sigma, \tau) = b_\sigma b_\tau b_{\sigma\tau}^{-1}$  der zum Schnitt  $b$  gehörige 2-Kozykel, so gilt

$$\beta'(\sigma, \tau) = b_\sigma b_\tau b_{\sigma\tau}^{-1} = h(\sigma)a_\sigma h(\tau)a_\tau h(\sigma\tau)^{-1}a_{\sigma\tau}^{-1} = \beta(\sigma, \tau)\gamma(\sigma, \tau)$$

für den zerfallenden Kozykel  $\gamma(\sigma, \tau) = h(\sigma)h(\tau)h(\sigma\tau)^{-1}$ .

- c) Wir dürfen annehmen, dass  $a_1 = 1$  ist. Die durch  $\psi : (s, \sigma) \longmapsto sa_\sigma$  definierte Abbildung  $W_2 \times_\beta G \longrightarrow \Gamma$  ist dann ein Isomorphismus. In der Tat gilt

$$\begin{aligned} \psi((s, \sigma)(t, \tau)) &= \psi(st\beta(\sigma, \tau), \sigma\tau) = st\beta(\sigma, \tau)a_{\sigma\tau} = sta_\sigma a_\tau a_{\sigma\tau}^{-1}a_{\sigma\tau} = sta_\sigma a_\tau \\ &= \psi(s, \sigma)\psi(t, \tau), \end{aligned}$$

Also ist  $\psi$  ein Homomorphismus. Da sich jedes Element von  $\Gamma$  in der Form  $sa_\sigma$  schreiben lässt, ist  $\psi$  surjektiv. Endlich ist  $\psi$  auch injektiv wegen  $\text{Kern } \psi = \{(s, \sigma) : sa_\sigma = 1\}$ ; aus  $sa_\sigma = 1$  folgt aber  $1 = p(1) = p(sa_\sigma) = \sigma$ , und  $sa_1 = 1$  impliziert wegen  $a_1 = 1$  dann  $s = 1$ .

17) Betrachte die Gruppenerweiterung

$$1 \longrightarrow W_2 \longrightarrow Q_8 \xrightarrow{p} G \longrightarrow 1, \quad (8.2)$$

wo  $G = \{1, \sigma, \tau, \sigma\tau\} \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$  ist, und  $Q_8$  die von  $S$  und  $T$  erzeugte Gruppe mit den Relationen  $S^2 = T^2$ ,  $S^4 = 1$ ,  $TS = S^{-1}T$ . Die Projektion  $p : Q_8 \longrightarrow G$  sei durch  $p(S) = \sigma$  und  $p(T) = \tau$  definiert. Wähle den Schnitt  $a_1 = 1$ ,  $a_\sigma = S$ ,  $a_\tau = T$  und  $a_{\sigma\tau} = ST$ . Man rechne dann nach, dass der zu diesem Schnitt gehörige (normierte) 2-Kozykel durch folgende Tabelle gegeben ist:

$Q_8$	$\sigma$	$\tau$	$\sigma\tau$
$\sigma$	-1	+1	-1
$\tau$	-1	-1	+1
$\sigma\tau$	+1	-1	-1

Die Untergruppe  $W_2$  von  $Q_8$  mit  $Q_8/W_2 \simeq G$  ist  $W_2 = \{1, S^2\}$ ; wir werden im Folgenden daher  $-1$  mit  $S^2$  identifizieren.

Damit ist dann  $\beta(\sigma, \sigma) = a_\sigma a_\sigma a_1^{-1} = S^2 = -1$ ,  $\beta(\sigma, \tau) = a_\sigma a_\tau a_{\sigma\tau}^{-1} = ST(ST)^{-1} = 1$ , sowie  $\beta(\tau, \sigma) = a_\tau a_\sigma a_{\tau\sigma}^{-1} = TS(ST)^{-1} = TST^{-1}S^{-1} = S^2 = -1$ . Die andern Werte errechnet man ähnlich.

- 18) Betrachte den Grundkörper  $k = F(X)$ , wo  $F$  ein Körper der Charakteristik  $\neq 2$  und  $X$  transzendent über  $F$  ist, und die Erweiterungen  $K = k(\sqrt{X}, \sqrt{1-X})$  und

$L = K(\sqrt{\mu})$  für  $\mu = 1 - \sqrt{X}$ . Zeige, dass  $L/k$  galoissch mit Galoisgruppe  $D_8$  ist. Welche Galoisgruppen erhält man für  $F = \mathbb{Q}$ , wenn man zu  $X = 2, -1, -3$  spezialisiert?

Seien wie üblich  $\sigma, \tau, \sigma\tau$  diejenigen Automorphismen von  $K/k$ , welche  $\sqrt{X}, \sqrt{1-X}$ , bzw.  $\sqrt{X(1-X)}$  festlassen. Dann rechnen wir:

$$\begin{aligned} \mu^{\sigma^{-1}} &= 1, & \text{also} & \quad \alpha_\sigma = 1; \\ \mu^{\tau^{-1}} &= \mu^{\sigma\tau^{-1}} = \frac{(1 - \sqrt{X})^2}{1 - X}, & \text{also} & \quad \alpha_\tau = \alpha_{\sigma\tau} = \frac{1 - \sqrt{X}}{\sqrt{1 - X}}; \end{aligned}$$

Daraus ersehen wir dann  $\beta(\sigma, \sigma) = \beta(\tau, \tau) = 1$  und  $\beta(\sigma\tau, \sigma\tau) = -1$ . Also ist  $G(L/k) \simeq D_8$  die Diedergruppe der Ordnung 8, da dies die einzige der in Frage kommenden Gruppen mit genau einem Element der Ordnung 4 ist.

Spezialisiert man zu  $X = 2$  und  $X = -1$ , erhält man wieder Diedererweiterungen. Im Falle  $X = -3$  dagegen wird  $1 - X = 4$  zum Quadrat, und man überzeugt sich leicht davon, dass dann  $L = F(\sqrt{-3}, \sqrt{-2})$  wird.

- 19) Bestimme die Galoisgruppe von  $\mathbb{Q}(\sqrt[8]{2}, i)$  (das ist der Zerfällungskörper von  $x^8 - 2$ ) über  $\mathbb{Q}$ .

Im Folgenden werden wir die Bestimmung der Galoisgruppe mit den hier vorgestellten Methoden vorführen; wer mit Galoistheorie bereits vertraut ist, wird das Problem auch mit weniger aufwendigen<sup>1</sup> Rechnungen lösen können.

Wir wissen, dass  $K = \mathbb{Q}(\sqrt[4]{2}, i)$  eine Diedererweiterung vom Grad 8 mit Galoisgruppe  $G(K/\mathbb{Q}) \simeq \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$  ist, wobei  $\sigma$  und  $\tau$  wie folgt festgelegt sind:

$$\begin{aligned} \sigma(\sqrt[4]{2}) &= i\sqrt[4]{2}, & \sigma(i) &= i, \\ \tau(\sqrt[4]{2}) &= +\sqrt[4]{2}, & \tau(i) &= -i. \end{aligned}$$

Man beachte, dass  $K$  die primitive achte Einheitswurzel  $\zeta = \frac{\sqrt{2} + i\sqrt{2}}{2}$  enthält. Wegen  $\sigma(\sqrt{2}) = \sigma(\sqrt[4]{2})^2 = -\sqrt{2}$  ist

$$\sigma(\zeta) = -\frac{\sqrt{2} + i\sqrt{2}}{2} = -\zeta, \quad \tau(\zeta) = \frac{\sqrt{2} - i\sqrt{2}}{2} = \zeta^{-1}.$$

Für  $L = K(\sqrt{\mu})$  mit  $\mu = \sqrt[4]{2}$  finden wir jetzt

$$\begin{aligned} \mu^{\sigma^{-1}} &= i = \zeta^2, & \alpha_\sigma &= \zeta, \\ \mu^{\tau^{-1}} &= 1, & \alpha_\tau &= 1 \end{aligned}$$

<sup>1</sup>Anscheinend soll das heutzutage "aufwändig" geschrieben werden, weil man sagt, das Wort käme (oder heißt das kömme, weil es von kommen kommt?) von Aufwand; auswändig kann ich das aber nicht sagen, und ich will dafür auch nicht zuviel Zeit aufwenden.

Dies genügt bereits für den Nachweis, dass  $L/\mathbb{Q}$  normal ist, da sich die andern  $a_\rho$  aus diesen beiden bis auf das Vorzeichen bestimmen lassen. Wir finden, wenn wir die  $a_{\sigma^j}$  wie in Übung 6 wählen (also z.B.  $\alpha_{\sigma^2} = \alpha_\sigma^{1+\sigma} = -\zeta^2$ ):

$$\begin{array}{c|cccccccc} \rho & 1 & \sigma & \sigma^2 & \sigma^3 & \tau & \sigma\tau & \sigma^2\tau & \sigma^3\tau \\ \hline a_\rho & 1 & \zeta & -\zeta^2 & -\zeta^3 & 1 & \zeta^{-1} & \zeta^2 & \zeta \end{array}$$

Damit folgt  $\beta(\sigma, \sigma) = \beta(\sigma^2, \sigma) = 1$ ,  $\beta(\sigma^2, \sigma^2) = a_{\sigma^2}^{1+\sigma^2} = \zeta^4 = -1$ , sodass wir mit  $S = (1, \sigma)$  finden:

$$S^2 = (1, \sigma^2), \quad S^3 = (1, \sigma^3), \quad S^4 = (-1, 1), \quad S^8 = 1.$$

Also hat  $S$  Ordnung 8 und erzeugt zusammen mit  $T = (1, \tau)$  die Galoisgruppe  $\Gamma$  von  $\mathbb{Q}(\sqrt[8]{2}, i)$  über  $\mathbb{Q}$ .

Um die Multiplikationstafel der Gruppe aufstellen zu können, müssen wir noch die Ordnung von  $T$  und den Kommutator  $[S, T]$  ausrechnen. Nun ist  $\beta(\tau, \tau) = 1$ , also  $T^2 = 1$ , sowie  $\beta(\sigma, \tau) = \beta(\tau, \sigma\tau) = 1$ , also  $ST = (1, \sigma\tau)$  und  $TST = (\beta(\tau, \sigma\tau), \tau\sigma\tau) = (1, \sigma^3) = S^3$ . Also ist

$$G = \langle S, T : S^8 = T^2 = 1, TST = S^3 \rangle.$$



# Übungen zu Kapitel 9

- 1) Es gilt  $\mathbb{F}_2 \subseteq \mathbb{F}_4$ , wo  $\mathbb{F}_2$  der Primkörper von  $\mathbb{F}_4$  ist. Gilt auch  $\mathbb{Z}/2 \subseteq \mathbb{Z}/4$ , d.h., gibt es einen injektiven Ringhomomorphismus  $\mathbb{Z}/2 \rightarrow \mathbb{Z}/4$ ?

Einen solchen Ringhomomorphismus  $\phi : \mathbb{Z}/2 \rightarrow \mathbb{Z}/4$  gibt es sicher nicht dann, wenn wir die Ringe als Ringe mit Eins betrachten: dann muss nämlich  $\phi(1 + 2\mathbb{Z}) = 1 + 4\mathbb{Z}$  sein, was sofort auf den Widerspruch  $0 + 4\mathbb{Z} = \phi(0 + 2\mathbb{Z}) = \phi(1 + 2\mathbb{Z}) + \phi(1 + 2\mathbb{Z}) = 2 + 4\mathbb{Z}$  führt.

Lässt man die Bedingung  $\phi(1) = 1$  fallen, so wird durch  $\phi(1 + 2\mathbb{Z}) = 2 + 4\mathbb{Z}$  in der Tat ein injektiver Ringhomomorphismus definiert.

- 2) Zeige: Für jedes  $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$  gilt  $\alpha^2 = \alpha + 1$ .

Jedes von 0 verschiedene  $\alpha \in \mathbb{F}_4$  genügt der Gleichung  $\alpha^3 = 1$ . Ist auch noch  $\alpha \neq 1$ , so folgt die Behauptung aus  $0 = \alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1)$  und der Bemerkung  $-1 = 1$  in  $\mathbb{F}_4$ .

- 3) Man verifiziere folgende Tabelle von Kreisteilungspolynomen:

$n$	$F_n$	$n$	$F_n$
1	$X - 1$	4	$X^2 + 1$
2	$X + 1$	5	$X^4 + X^3 + X^2 + X + 1$
3	$X^2 + X + 1$	6	$X^2 - X + 1$

Es ist wegen F9.10

$$\begin{aligned}
 F_1(X) &= X - 1, & F_4(X) &= \frac{X^4 - 1}{F_1(X)F_2(X)} = X^2 + 1, \\
 F_2(X) &= \frac{X^2 - 1}{F_1(X)} = X + 1, & F_5(X) &= \frac{X^5 - 1}{F_1(X)} = X^4 + X^3 + X^2 + X + 1, \\
 F_3(X) &= \frac{X^3 - 1}{F_1(X)} = X^2 + X + 1, & F_6(X) &= \frac{X^6 - 1}{F_1(X)F_2(X)F_3(X)} = X^2 - X + 1.
 \end{aligned}$$

4) Sei  $p$  eine Primzahl und  $\zeta$  eine primitive  $p$ -te Einheitswurzel. Zeige:

- a)  $1 + \zeta + \zeta^2 + \dots + \zeta^{p-1} = 0$ ;
  - b) für  $p \neq 2$  ist  $1 + \zeta$  eine Einheit in  $\mathbb{Z}[\zeta]$ ;
  - c) es ist  $(1 - \zeta)^{p-1} = \varepsilon p$  für eine Einheit  $\varepsilon$  in  $\mathbb{Z}[\zeta]$ .
- a) Dies folgt sofort aus der Tatsache, dass  $\zeta$  Nullstelle von  $F_p(X) = X^{p-1} + \dots + X + 1$  ist. Ein weiterer Beweis besteht darin, die Summe  $S = 1 + \zeta + \zeta^2 + \dots + \zeta^{p-1}$  mit  $\zeta$  zu multiplizieren und zu bemerken, dass  $\zeta S = S$  ist wegen  $\zeta^p = 1$ .
- b) Es ist  $N = \prod_{r=1}^{p-1} (1 + \zeta^r) = 1$ . In der Tat: die  $\zeta^r$  sind Nullstellen von  $F_p(X)$ , daher sind die  $1 + \zeta^r$  Nullstellen von  $F_p(X - 1)$ . Da  $N$  der konstante Term von  $F_p(X - 1)$  ist, muss  $N = F_p(0 - 1) = F_p(-1) = +1$  sein. Also ist  $1 + \zeta$  eine Einheit.
- c) Wie eben zeigt man  $\prod_{r=1}^{p-1} (1 - \zeta^r) = F_p(1) = p$ . Wegen  $1 - \zeta^r = (1 - \zeta)(1 + \zeta + \zeta^2 + \dots + \zeta^{r-1})$  genügt es zu zeigen, dass die Elemente  $\eta_r = 1 + \zeta + \zeta^2 + \dots + \zeta^{r-1}$  Einheiten sind. Dies geht so am einfachsten: die obige Gleichung zeigt, dass der Quotient  $\eta_r = \frac{1 - \zeta^r}{1 - \zeta} \in \mathbb{Z}[\zeta]$  ist. Sei nun  $s$  eine ganze Zahl mit  $rs \equiv 1 \pmod p$  und  $\sigma_s$  der Automorphismus von  $\mathbb{Q}(\zeta)/\mathbb{Q}$  mit  $\sigma_s(\zeta) = \zeta^s$ . Wegen  $\sigma_s(\varepsilon_r) = \frac{1 - \zeta}{1 - \zeta^s} = \varepsilon_s^{-1}$  ist dann aber auch  $\varepsilon_r^{-1}$  ganz, also  $\varepsilon_r$  eine Einheit.

5) Für  $m \in \mathbb{N}$  sei  $\zeta_m = e^{2\pi i/m}$ . Für welche  $n \in \mathbb{N}$  gilt  $\zeta_{2n} \in \mathbb{Q}(\zeta_n)$ ?

Ist  $n$  ungerade, so ist  $\zeta_{2n} = -\zeta_n^{(n+1)/2}$  wegen  $(-\zeta_n^{(n+1)/2})^2 = \zeta_n^{n+1} = \zeta_n$ , also  $\zeta_{2n} \in \mathbb{Q}(\zeta_n)$ . Alternativ folgt aus Satz S.9.5, dass  $\mathbb{Q}(\zeta_{2n}) : \mathbb{Q} = \phi(2n) = \phi(n) = \mathbb{Q}(\zeta_n) : \mathbb{Q}$  und damit  $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$  ist.

Ist  $n$  gerade, so ist  $\zeta_n$  kein Quadrat in  $\mathbb{Q}(\zeta_n)$ : sei nämlich  $n = 2^a u$  für  $a \geq 1$  und ungerades  $u$ ; dann ist  $\mathbb{Q}(\zeta_n) : \mathbb{Q} = \phi(n) = 2^{a-1} \phi(u)$ , sowie  $\mathbb{Q}(\zeta_{2n}) : \mathbb{Q} = \phi(2n) = 2^a \phi(u) = 2(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ .

6) Sei  $\zeta_n$  eine primitive  $n$ -te Einheitswurzel. Zeige:

- a)  $\sqrt{2} \in \mathbb{Q}(\zeta_n)$ , wenn  $8 \mid n$ ;
  - b)  $\sqrt[4]{2}$  liegt in keinem  $\mathbb{Q}(\zeta_n)$ .
- a) Wegen  $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$  ist  $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ ; weil  $\mathbb{Q}(\zeta_8)$  Teilkörper von  $\mathbb{Q}(\zeta_{8m})$  ist, folgt die Behauptung. Die Umkehrung gilt übrigens auch, lässt sich aber ohne Hilfsmittel aus der algebraischen Zahlentheorie wohl nicht so einfach zeigen.
- b) Der Körper  $\mathbb{Q}(\sqrt[4]{2})$  ist nicht normal, also kann  $\sqrt[4]{2}$  in keiner abelschen Erweiterung von  $\mathbb{Q}$  liegen.

- 7) (A. Scholz) Sei  $m > 2$  eine natürliche Zahl,  $G = (\mathbb{Z}/m)^\times$ , und  $H$  eine echte Untergruppe von  $G$ . Zeige, dass es unendlich viele Primzahlen gibt, deren Restklassen modulo  $m$  nicht in  $H$  liegen.

Wir zeigen zuerst, dass es mindestens eine solche Primzahl gibt. Wären alle Primzahlen modulo  $m$  in  $H$ , so würden alle Restklassen modulo  $m$  in  $H$  liegen, weil jede natürliche Zahl ein Produkt von Primzahlen ist. Wegen  $H \neq G$  kann dies nicht sein.

Haben wir eine solche Primzahl  $p$  gefunden, so kommen wir wie folgt weiter: wir setzen  $m' = pm$ ,  $G = (\mathbb{Z}/m')^\times$ , und  $H' = \{a + mp\mathbb{Z} : a + m\mathbb{Z} \in H, \gcd(a, p) = 1\}$ . Dann finden wir wie oben eine Primzahl  $p' \neq p$ , deren Restklasse mod  $mp$  nicht in  $H'$  (und damit erst recht nicht in  $H$ ) liegt.

- 8) Sei  $K = \mathbb{Q}(\sqrt{m})$  ein quadratischer Zahlkörper. Man bestimme  $W(K)$ .

Beachte  $\mathbb{Q}(\zeta_n) : \mathbb{Q} = \phi(n)$ ; ist  $\zeta_n \in K$ , muss  $\phi(n) \mid 2$  gelten. Dies wiederum ist genau dann der Fall, wenn  $n = 1, 2, 3, 4, 6$  ist, und diese kommen tatsächlich vor: jeder Zahlkörper enthält  $\zeta_2$ , und es gilt  $\zeta_4 \in \mathbb{Q}(\sqrt{-1})$ , sowie  $\zeta_3, \zeta_6 \in \mathbb{Q}(\sqrt{-3})$ .

Die Bestimmung aller  $n$  mit  $\phi(n) = 2$  ist einfach: sei  $n = \prod p^{a(p)}$  die Primfaktorzerlegung von  $n$ . Dann ist  $\phi(n) > 2$ , falls  $a(p) \geq 1$  für ein  $p \geq 5$  ist. Also ist  $n = 2^a 3^b$ . Jetzt sieht man sofort, dass  $a \leq 2$  (wegen  $\phi(8) = 4$ ) und  $b \leq 1$  ist, und Durchprobieren aller verbleibenden Möglichkeiten liefert die Behauptung.

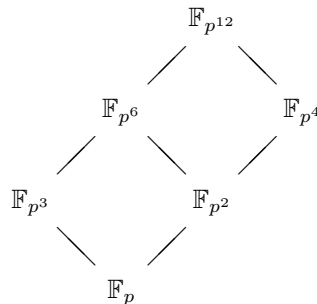
- 9) Sei  $K/\mathbb{Q}$  eine kubische Erweiterung. Man zeige  $W(K) = \{-1, +1\}$ .

Wie eben folgt  $\phi(n) \mid 3$ , falls  $\zeta_n \in K$  ist; da es kein  $n \in \mathcal{N}$  gibt mit  $\phi(n) = 3$ , muss  $n = 1$  oder  $n = 2$  sein.

- 10) Sei  $K$  eine Erweiterung von  $\mathbb{Q}$  vom Grad 10. Zeige  $W_5(K) = \{1\}$ .

Ist  $\zeta_5 \in K$ , so muss  $K : \mathbb{Q}$  durch  $\phi(5) = 4$  teilbar sein.

- 11) Zeige, dass das Körperdiagramm aller Zwischenkörper von  $\mathbb{F}_{p^{12}}/\mathbb{F}$  wie folgt aussieht:



Wir wissen, dass genau dann  $\mathbb{F}_{p^m}$  in  $\mathbb{F}_{p^n}$  enthalten ist, wenn  $m \mid n$  gilt. Da die Teiler von 12 genau 1, 2, 3, 4, 6 und 12 sind, ist alles klar.

- 12) Im Folgenden sei  $\mathbb{F}_q$  ein endlicher Körper mit  $q$  Elementen, und  $\zeta_n$  eine primitive Einheitswurzel im algebraischen Abschluss von  $\mathbb{F}_q$ .

Ist  $q \equiv 2, 5 \pmod{9}$ , so zeige man  $\mathbb{F}_{q^2} = \mathbb{F}_q(\zeta_3)$ ,  $\mathbb{F}_{q^3} = \mathbb{F}_q(\zeta_9 + \zeta_9^{-1})$ , und  $\mathbb{F}_{q^6} = \mathbb{F}_q(\zeta_9)$ .

Mit  $\zeta_3$  ist natürlich eine Wurzel von  $X^2 + X + 1 = 0$  in einem algebraischen Abschluss von  $\mathbb{F}_q$  gemeint. Um  $\mathbb{F}_{q^2} = \mathbb{F}_q(\zeta_3)$  zu zeigen, müssen wir nachrechnen, dass  $X^2 + X + 1$  über  $\mathbb{F}_q$  irreduzibel ist. Für  $q = 2$  ist das klar; wäre aber  $a^2 + a + 1 = 0$  in  $\mathbb{F}_q$  mit  $q > 2$ , so folgte  $(2a + 1)^2 = -3$ . Aber  $-3$  ist kein Quadrat in  $\mathbb{F}_q$  wegen  $(\frac{-3}{q}) = (\frac{q}{3}) = -1$ .

Wegen  $\zeta_9^3 = \zeta_3$  ist als nächstes zu zeigen, dass  $\zeta_3$  in  $\mathbb{F}_{q^2}$  keine dritte Potenz ist. Aus  $\zeta_3 = \gamma^3$  würde aber folgen, dass  $\gamma$  ein Element der Ordnung 9 in  $\mathbb{F}_{q^2}^\times$  ist, und ein solches existiert nicht, da  $q^2 - 1$  zwar durch 3, aber nicht durch 9 teilbar ist.

Das Minimalpolynom von  $\zeta_9 + \zeta_9^{-1}$  ist  $X^3 - 3X + 1$  (vgl. Übung 1.13). Da  $\mathbb{F}_q(\zeta_9)$  eine quadratische Erweiterung von  $\mathbb{F}_q(\zeta_9 + \zeta_9^{-1})$  ist (betrachte die Quadratwurzel von  $(\zeta_9 + \zeta_9^{-1})^2 - 4$ ), muss dieses Polynom irreduzibel und damit  $\mathbb{F}_{q^3} = \mathbb{F}_q(\zeta_9 + \zeta_9^{-1})$  sein.

- 13) Bestimme den Zerfällungskörper von  $X^5 + X + 1$  über  $\mathbb{F}_2$ .

Wir testen  $f(X) = X^5 + X + 1$  auf Irreduzibilität. Wegen  $f(0) = f(1) = 1$  hat  $f$  keinen linearen Faktor. Da  $g(X) = X^2 + X + 1$  das einzige irreduzible Polynom vom Grad 2 über  $\mathbb{F}_2$  ist, müssen wir nur noch testen, ob  $g \mid f$  ist. Eine Polynomdivision zeigt nun  $f(X) = g(X)(X^3 + X^2 + 1)$ .

Der Zerfällungskörper von  $f$  ist also das Kompositum der Zerfällungskörper  $\mathbb{F}_4$  von  $X^2 + X + 1$  und  $\mathbb{F}_8$  von  $X^3 + X^2 + 1$ , nämlich  $\mathbb{F}_{64}$ .

- 14) Bestimme die Anzahl der normierten linearen und die der normierten reduziblen quadratischen Polynome in  $\mathbb{F}_p[X]$ , sowie die Anzahl der normierten irreduziblen quadratischen Polynome in  $\mathbb{F}_p[X]$ .

Offenbar sind die normierten linearen Polynome genau die  $X - a$  mit  $a \in \mathbb{F}_p$ ; davon gibt es genau  $p$ .

Die reduziblen quadratischen Polynome haben die Form  $(X - a)(X - b)$  für  $a, b \in \mathbb{F}_p$ . Davon gibt es  $p$  Stück mit doppelter Nullstelle  $a = b$ , sowie  $\binom{p}{2} = \frac{p(p-1)}{2}$  mit verschiedenen Nullstellen (hier kommt es auf die Reihenfolge der Nullstellen offenbar nicht an).

Da es insgesamt  $p^2$  quadratische Polynome  $X^2 + cX + d$  über  $\mathbb{F}_p$  gibt, ist die Anzahl der normierten irreduziblen Polynome vom Grad 2 gleich  $p^2 - p - \frac{p(p-1)}{2} = \frac{p(p-1)}{2}$ .

# Übungen zu Kapitel 10

- 1) Zeige, dass in Def. 10.4 der Stabilisator  $G_x$  wirklich eine Untergruppe von  $G$  ist.

Sei  $G_x = \{\sigma \in G : \sigma x = x\}$ . Mit  $\sigma, \tau \in G$  ist dann  $(\sigma\tau)x = \sigma(\tau x) = \sigma x = x$ , also auch  $\sigma\tau \in G$ . Weiter ist das Einselement 1 in  $G$  wegen  $1x = x$ . Schließlich enthält  $G$  mit  $\sigma$  auch dessen Inverses: aus  $\sigma x = x$  folgt durch Anwenden von  $\sigma^{-1}$  sofort  $x = \sigma^{-1}x$ .

- 2) Für jede abelsche Gruppe  $G$  endlicher Ordnung beweise man (mit Induktion nach der Gruppenordnung) ganz elementar: Ist  $p$  ein Primteiler von  $|G|$ , so hat  $G$  ein Element der Ordnung  $p$ . Nun zeige man (wieder mit Induktion): Ist  $d \in \mathbb{N}$  ein Teiler von  $n = |G|$ , so hat  $G$  eine Untergruppe der Ordnung  $d$ .

Sei  $|G| = p$ . Da die Ordnung eines Elements die Gruppenordnung teilt und es nur ein Element der Ordnung 1 gibt, enthält  $G$  genau  $p - 1$  Elemente der Ordnung  $p$ .

Sei nun  $|G| = n$  ein Vielfaches von  $p$  und die Behauptung bewiesen für alle abelschen Gruppen kleinerer Ordnung. Sei  $x \in G$  ein Element  $\neq 1$ ; ist dessen Ordnung durch  $p$  teilbar, also z.B. gleich  $pk$  für ein  $k \in \mathbb{N}$ , dann hat  $x^k$  die genaue Ordnung  $p$ . Sei also  $p$  kein Teiler der Ordnung von  $x$  und  $N = \langle x \rangle$ . Da  $G$  abelsch ist, ist  $N$  normal in  $G$ , und  $G/N$  ist eine abelsche Gruppe mit durch  $p$  teilbarer Ordnung. Also enthält  $G/N$  nach Induktionsvoraussetzung ein Element  $yN$  der Ordnung  $p$ . Doch offenbar ist  $\text{ord}(yN)$  ein Teiler von  $\text{ord}(y)$ . Also ist  $p$  ein Teiler von  $\text{ord}(y)$ , und in diesem Fall haben wir bereits gesehen, wie die Behauptung folgt.

Nun zum Beweis der zweiten Behauptung. Sei  $G$  abelsch von der Ordnung  $n$  und  $d|n$ . Für  $d = 1$  ist die Behauptung richtig. Sei also  $d > 1$ . Dann besitzt  $d$  einen Primteiler  $p$ . Da dieser auch in  $n$  aufgeht, gibt es nach der ersten Behauptung ein Element  $x \in G$  mit  $\text{ord}(x) = p$ . Die Ordnung der Gruppe  $G/\langle x \rangle$  hat dann die Ordnung  $n/p < n$ , und  $n/p$  ist teilbar durch  $d/p$ . Per Induktion (wieder nach  $n$ ) können wir annehmen, dass  $G/\langle x \rangle$  eine Untergruppe der Ordnung  $d/p$  besitzt. Diese ist von der Gestalt  $H/\langle x \rangle$  mit einer Untergruppe  $H$  von  $G$ , und  $H$  hat die Ordnung  $d$ .

- 3) Betrachte  $M = \{(x_1, \dots, x_5) : x_i \in \{0, 1\}\}$ . Für  $x = (x_1, \dots, x_5) \in M$  sei  $\sigma(x) = (x_2, \dots, x_5, x_1)$  der durch zyklische Permutation aus  $x$  hervorgehende „Vektor“. Zeige, dass die Bahn jedes Elements genau 5 Elemente hat, mit Ausnahme der von den Elementen  $(0, 0, 0, 0, 0)$  und  $(1, 1, 1, 1, 1)$  erzeugten Bahnen. Schließe daraus, dass  $2^5 \equiv 2 \pmod{5}$  gilt, und verallgemeinere diese Überlegung zu einem Beweis des kleinen Fermatschen Satzes  $a^p \equiv a \pmod{p}$ .

Offenbar ist  $\sigma^5(x) = x$  für alle  $x \in M$ , die Bahnenlänge daher 1 oder 5. Ist sie 1, so muss  $\sigma x = x$  sein, und dies ist genau dann der Fall, wenn  $x_1 = \dots = x_5$  ist. Also gibt es genau 2 Bahnen der Länge 1, während alle anderen Bahnen Länge 5 haben. Folglich ist  $2^5 \equiv 2 \pmod{5}$ .

Lässt man Werte  $x_i \in \{0, 1, \dots, a-1\}$  zu und betrachtet Elemente  $x = (x_1, \dots, x_p)$ , so findet man ganz entsprechend  $a^p \equiv a \pmod{p}$ , da die einzigen Bahnen der Länge 1 von den „konstanten“ Elementen  $(b, b, \dots, b)$  erzeugt werden.

- 4) Eine Gruppe  $G$  operiert von rechts auf einer Menge  $X$ , wenn es eine Abbildung  $X \times G \rightarrow X$ ,  $(x, \sigma) \mapsto x \cdot \sigma$ , gibt mit  $x \cdot 1 = x$  und  $x \cdot (\sigma\tau) = (x \cdot \sigma) \cdot \tau$ . Zeige: operiert  $G$  von rechts auf  $X$ , so definiert  $\sigma x := x \cdot \sigma^{-1}$  eine Operation von links.

Es ist  $1x = x \cdot 1^{-1} = x \cdot 1 = x$ , sowie  $(\sigma\tau)x = x(\sigma\tau)^{-1} = x(\tau^{-1}\sigma^{-1}) = (x\tau^{-1})\sigma^{-1} = \sigma(\tau x)$ .

- 5) Sei  $\text{SL}_2(\mathbb{Z})$  die Gruppe aller  $2 \times 2$ -Matrizen mit ganzzahligen Einträgen und Determinante 1. Zeige:  $\text{SL}_2(\mathbb{Z})$  operiert via  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$  auf der oberen Halbebene  $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ .

Für komplexe Zahlen  $z \in \mathbb{C}$  gilt  $\text{Re } z = \frac{z+\bar{z}}{2}$  und  $\text{Im } z = \frac{z-\bar{z}}{2i}$ . Mit  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  finden wir daher

$$\begin{aligned} \text{Im } Mz &= \text{Im } \frac{az+b}{cz+d} = \text{Im } \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} \\ &= \frac{1}{|cz+d|^2} \text{Im}[(ac+bd) + adz + bc\bar{z}] \\ &= \frac{ad-bc}{|cz+d|^2} \text{Im } z = \frac{\text{Im}(z)}{|cz+d|^2} \end{aligned}$$

wegen  $ad-bc = 1$ . Mit  $\text{Im}(z) > 0$  ist also auch  $\text{Im}(Mz) > 0$ .

Da die Einheitsmatrix auf der oberen Halbebene trivial operiert, müssen wir nur noch zeigen, dass  $(MN)z = M(Nz)$  für  $M, N \in \text{SL}_2(\mathbb{Z})$  gilt. Sei also  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

und  $N = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ ; dann ist

$$\begin{aligned} Nz &= \frac{ez + f}{gz + h}, \\ M(Nz) &= \frac{aN(z) + b}{cN(z) + d} = \frac{a(ez + f) + b(gz + h)}{c(ez + f) + d(gz + h)} \\ &= \frac{(ae + bg)z + af + bh}{(ce + dg)z + cf + dh} = (MN)(z). \end{aligned}$$

- 6) Sei  $Q = AX^2 + BXY + CY^2$  eine quadratische Form und  $A, B, C \in \mathbb{Z}$ . Man nennt  $\Delta = B^2 - 4AC$  die Diskriminante von  $Q$ . Man zeige, dass für  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$  durch  $Q|_M = Q(aX + bY, cX + dY)$  eine Operation von  $\text{SL}_2(\mathbb{Z})$  auf der Menge der quadratischen Formen mit Diskriminante  $\Delta$  definiert ist. Beachte  $Q|_{MN} = (Q|_M)|_N$ , d.h.  $\text{SL}_2(\mathbb{Z})$  operiert von rechts!

Da die Einheitsmatrix trivial operiert, ist nur zu zeigen, dass  $Q|_{MN} = (Q|_M)|_N$  für alle  $M, N \in \text{SL}_2(\mathbb{Z})$  gilt, und dass  $\Delta(Q|_M) = \Delta(Q)$  ist. Das kann man einfach nachrechnen; etwas eleganter ist aber der Zugang mit etwas linearer Algebra.

Dazu ordnen wir jeder quadratischen Form  $Q = AX^2 + BXY + CY^2$  die symmetrische Matrix  $P_Q = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$  zu und beachten, dass  $Q(X, Y) = (X, Y)P_Q(X, Y)^t$ , sowie  $\Delta(Q) = -4 \det P_Q$  gilt. Dann überzeugen wir uns davon, dass  $Q|_M$  zur Matrix  $M^t P_Q M$  gehört (dies ist eine leichte Rechnung), und damit ist einerseits klar, dass  $\Delta(Q|_M) = -4 \det M^2 \det P_Q = \Delta(Q)$  ist (wegen  $\det M = 1$ ), und andererseits folgt, dass  $(Q|_M)|_N$  zur Matrix  $N^t M^t P_Q M N = (MN)^t P_Q M N$  gehört. Damit ist alles bewiesen.

- 7) Ordne jeder quadratischen Form  $Q = AX^2 + BXY + CY^2$  mit negativer Diskriminante  $\Delta = B^2 - 4AC$  und positivem  $A$  die komplexe Zahl  $\tau_Q = \frac{-B + \sqrt{\Delta}}{2A} \in \mathcal{H}$  in der oberen Halbebene zu. Zeige, dass dann  $Q|_M$  dem Element  $M^{-1}\tau_Q$  entspricht.

Sei  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , also  $M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ . Wegen  $Q' := Q|_M = A'X^2 + B'XY + C'Y^2$  mit  $A' = Ar^2 + Brs + Ct^2$ ,  $B' = 2(Ars + Ctu) + B(ru + st)$ , und  $C' = As^2 + Bsu + Cu^2$  ist  $\tau_{Q'} = \frac{-B' + \sqrt{\Delta}}{2A'}$ ; andererseits ist

$$M^{-1}z = \frac{uz - s}{-tz + r} = \frac{(uz - s)(-t\bar{z} + r)}{(-tz + r)(-t\bar{z} + r)} = -\frac{rs + tuz\bar{z} - ruz - st\bar{z}}{(-tz + r)(-t\bar{z} + r)}.$$

Mit  $z = \tau_Q$  gilt aber  $z\bar{z} = C/A$ , sowie

$$\begin{aligned} ruz + st\bar{z} &= \frac{1}{2}(ru + st)(z + \bar{z}) + \frac{1}{2}(ru - st)(z - \bar{z}) \\ &= (ru + st)\frac{B}{2A} + \frac{\sqrt{\Delta}}{2}, \end{aligned}$$

und damit

$$\begin{aligned} M^{-1}z &= -\frac{rs + tu\frac{C}{A} + (ru + st)\frac{B}{2A} - \frac{1}{2}\sqrt{\Delta}}{r^2 + rt\frac{B}{A} + t^2\frac{C}{A}} \\ &= -\frac{2Ars + 2Ctu + B(ru + st) - \sqrt{\Delta}}{2(Ar^2 + Brt + Ct^2)} = \frac{-B' + \sqrt{\Delta}}{A'}. \end{aligned}$$

- 8) Im rationalen Funktionenkörper  $\mathbb{C}(X)$  betrachte man die Funktionen  $f_1(X) = X$ ,  $f_2(X) = -\frac{1}{X+1}$  und  $f_3(X) = -\frac{X+1}{X}$ . Zeige, dass  $G = \{f_1, f_2, f_3\}$  eine Gruppe bezüglich der Komposition von Abbildungen ist, und dass  $G$  auf  $\mathbb{C} \setminus \{0, -1\}$  operiert. Bestimme den Stabilisator  $G_z$  für jedes  $z \in \mathbb{C} \setminus \{0, -1\}$ .

Offenbar ist  $f_1$  die Identität bezüglich Komposition. Weiter ist z.B.

$$\begin{aligned} f_2 \circ f_2 &= -\frac{1}{-\frac{1}{X+1} - 1} = -\frac{X+1}{X} = f_3, \\ f_2 \circ f_3 &= f_3 \circ f_2 = X = f_1, \\ f_3 \circ f_3 &= f_2. \end{aligned}$$

Da 0 und  $-1$  die einzigen Nullstellen der in den Nennern der  $f_i$  auftretenden Polynome ist, operiert  $G$  auf  $\mathbb{C} \setminus \{0, -1\}$ .

Der Stabilisator  $G_z$  besteht aus allen  $f_j$  mit  $f_j(z) = z$ . Nun ist  $f_2(z) = z$  genau dann, wenn  $z^2 + z + 1 = 0$ , also wenn  $z$  eine primitive dritte Einheitswurzel ist, also  $z = \zeta_3$  oder  $z = \zeta_3^2$ . Da sich für  $f_3$  dieselbe Gleichung ergibt, gilt  $G_z = \{f_1\}$  für alle  $z \in \mathbb{C} \setminus \{0, -1, \rho, \rho^2\}$ , und  $G_z = G$  für  $z = \zeta_3, \zeta_3^2$ .

- 9) Für ungerade Primzahlen betrachte man die Menge  $M$  aller Lösungen  $(x, y)$  von  $x^2 + y^2 = 1$  in  $\mathbb{F}_p$ . Zeige, dass die folgenden Abbildungen  $M \rightarrow M$  eine Gruppe  $G$  der Ordnung 8 (welche?) bezüglich der Komposition erzeugen:  $\sigma(x, y) = (-x, y)$ ;  $\tau(x, y) = (x, -y)$ ;  $\rho(x, y) = (y, x)$ . Zeige, dass die Bahnen unter  $G$  bis auf folgende Ausnahmen immer 8 Elemente haben: Die Bahn von  $(0, \pm 1)$  und  $(\pm 1, 0)$  hat Länge 4; außer dieser gibt es noch eine weiteren Bahn der Länge 4 genau dann, wenn 2 ein Quadrat in  $\mathbb{F}_p$  ist.

Man zeige weiter, dass  $|M| = p - 1$  oder  $p + 1$  ist, je nachdem  $-1$  ein Quadrat in  $\mathbb{F}_p$  ist oder nicht. (Hinweis: ist  $x \neq 0$ , so dividiere man  $x^2 + y^2 = 1$  durch  $x^2$ , führe neue Variablen  $Y = y/x$  und  $X = 1/x$  ein und schreibe die Gleichung in der Form  $1 = (X - Y)(X + Y)$ . Deren Lösungen mit  $X \neq 0$  lassen sich leicht zählen). Aus der Bahnengleichung leite man nun ab, dass 2 genau dann ein Quadrat in  $\mathbb{F}_p$  ist, wenn  $p \equiv \pm 1 \pmod{8}$  gilt.

Wenn wir die identische Abbildung auf  $M$  mit 1 bezeichnen, so finden wir  $\sigma^2 = \tau^2 = \rho^2 = 1$ ; setzen wir  $\phi = \tau\rho$ , dann erhalten wir  $\phi^2 = \sigma\tau$  und  $\phi^4 = 1$ , sowie



$\tau\phi\tau = \rho\tau = \phi^3$ . Also ist

$$G = \langle \phi, \tau : \phi^4 = \tau^2 = 1, \tau\phi\tau = \phi^3 \rangle$$

die Diedergruppe  $D_8$  der Ordnung 8.

Die Bahn eines Elements  $(x, y)$  besteht im Allgemeinen aus den 8 Elementen  $(\pm x, \pm y)$ ,  $(\pm y, \pm x)$ . Die Länge der Bahn kann nur dann kleiner sein, wenn irgend zwei dieser Elemente zusammenfallen. Das ist genau dann der Fall, wenn  $x = 0$  oder  $y = 0$  ist (und diese Punkte  $(0, \pm 1)$ ,  $(\pm 1, 0)$  liegen alle in derselben Bahn), oder wenn  $x = \pm y$  gilt. Der letztere Fall tritt genau dann ein, wenn  $x^2 + x^2 = 1$  in  $\mathbb{F}_p$  lösbar ist, was wiederum genau dann der Fall ist, wenn 2 ein Quadrat in  $\mathbb{F}_p$  ist. Es gibt also eine oder zwei Bahnen der Länge 4, je nachdem  $(\frac{2}{p}) = -1$  oder  $(\frac{2}{p}) = +1$  ist. Für die Anzahl der Elemente in  $M$  gibt dies  $|M| \equiv 2 - 2(\frac{2}{p}) \pmod{8}$ .

Als nächstes zählen wir die Elemente von  $M$ . Ist  $x \neq 0$ , so gilt  $1 + (y/x)^2 = (1/x)^2$ , also  $1 = X^2 - Y^2$  mit  $X = 1/x$  und  $Y = y/x$ . Offenbar besteht eine Bijektion zwischen den Punkten  $(x, y)$  mit  $x \neq 0$  und den  $(X, Y)$  mit  $X \neq 0$ , so dass es genügt, letztere zu zählen. Ist  $r \in \mathbb{F}_p^\times$ , so liefert  $Y - X = r$ ,  $Y + X = \frac{1}{r}$  eine Lösung, und jede Lösung kann so geschrieben werden. Also gibt es auf der Hyperbel  $X^2 - Y^2 = 1$  genau  $p - 1$  Punkte mit Koordinaten in  $\mathbb{F}_p$ , und darunter sind genau dann solche mit  $X = 0$  (nämlich 2), wenn  $-1$  ein Quadrat in  $\mathbb{F}_p^\times$  ist. Also gibt es  $p - 2 - (\frac{-1}{p})$  Punkte  $(X, Y)$  mit  $X \neq 0$  (und ebensoviele Punkte  $(x, y)$  mit  $x \neq 0$ ), somit  $p - (\frac{-1}{p})$  Lösungen von  $x^2 + y^2 = 1$  in  $\mathbb{F}_p$ .

Nach dem ersten Teil ist  $|M| \equiv 2 + 2(\frac{2}{p}) \pmod{8}$ , nach dem zweiten dagegen  $|M| = p - (\frac{-1}{p})$ . Ist nun  $p \equiv 1 \pmod{8}$ , so folgt  $2 - 2(\frac{2}{p}) \equiv p - 1 \equiv 0 \pmod{8}$  und damit  $(\frac{2}{p}) = +1$ . Entsprechend ergibt sich  $(\frac{2}{p}) = -1$  für  $p \equiv 3 \pmod{8}$  etc.

- 10) Bestimme das Zentrum der Diedergruppe  $D_8$  und der Quaternionengruppe  $Q_8$ . Welche Struktur haben die dazugehörigen Faktorgruppen?

Es ist

$$\begin{aligned} D_8 &= \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle, \\ Q_8 &= \langle \sigma, \tau : \sigma^4 = 1, \sigma^2 = \tau^2, \tau\sigma\tau = \sigma \rangle. \end{aligned}$$

In beiden Fällen kommutiert  $\sigma^2$  mit allen andern Elementen, während  $\sigma$ ,  $\sigma^3$  und  $\tau$  offenbar nicht im Zentrum liegen. Von den andern Elementen rechnet man dies leicht nach (so ist z.B.  $\sigma\tau$  nicht zentral wegen  $\sigma \cdot \sigma\tau \neq \sigma\tau \cdot \sigma$ ). Also ist  $Z(D_8) = \{1, \sigma^2\}$  und  $Z(Q_8) = \{1, \sigma^2\}$ .

Die Gruppen  $G/Z(G)$  für  $G = D_8$  und  $G = Q_8$  haben beide Ordnung 4 und haben, wie man leicht nachrechnet, nur Elemente der Ordnung 1 und 2 (z.B. ist im Quaternionenfall  $(\tau Z)^2 = \tau^2 Z = \sigma^2 Z = Z$  für  $Z = Z(Q_8)$ ). Also ist  $G/Z(G) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ .

# Übungen zu Kapitel 11

- 1) Ermittle den Wert von  $\alpha = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$  für  $\zeta_p = e^{2\pi i/p}$  in den Fällen  $p = 3$  und  $p = 5$  durch direkte Rechnung.

Sei zuerst  $\zeta = \zeta_3$ , also  $1 + \zeta + \zeta^2 = 0$ . Dann ist  $\alpha = \zeta - \zeta^2$ , also  $\alpha^2 = \zeta^2 - 2 + \zeta^4 = -3$ .

Normiert man jetzt  $\zeta = e^{2\pi i/3}$ , so ist  $\text{Im } \zeta = \frac{1}{2}\sqrt{3}$  und  $\text{Im } \zeta^2 = -\frac{1}{2}\sqrt{3}$ , also  $\text{Im } \alpha > 0$  und damit  $\alpha = i\sqrt{3}$ .

Sei jetzt  $\zeta = \zeta_5$ . Dann ist  $\alpha = \zeta - \zeta^2 - \zeta^3 + \zeta^4$ , also  $\alpha^2 = \zeta^2 + \zeta^4 + \zeta^6 + \zeta^8 - 2\zeta^3 - 2\zeta^4 + 2 + 2 - 2\zeta^6 - 2\zeta^7 = 3 - 2(\zeta + \zeta^2 + \zeta^3 + \zeta^4) = 5$ .

Mit  $\zeta = e^{2\pi i/5}$  rechnet man jetzt nach, dass  $\text{Im } \alpha > 0$  und damit  $\alpha = \sqrt{5}$  ist.

- 2) Sei  $p$  eine Primzahl der Gestalt  $p = a^2 + 4b^2$  mit  $a, b \in \mathbb{Z}$ . Zeige, dass  $\left(\frac{a}{p}\right) = +1$  ist.

Es ist  $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2 + 4b^2}{a}\right) = \left(\frac{4b^2}{a}\right) = +1$ ; hier haben wir das quadratische Reziprozitätsgesetz und  $p \equiv 1 \pmod{4}$  benutzt, sowie die Tatsache  $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right)$  für Zahlen  $r \equiv s \pmod{p}$ .

- 3) Das Jacobisymbol als Funktion seines Nenners: zeige, dass für teilerfremde  $a, b \in \mathbb{N}$ ,  $b$  ungerade, immer  $\left(\frac{a}{b}\right) = \left(\frac{a}{b+4a}\right)$  gilt.

Es ist

$$\left(\frac{a}{b+4a}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}} \left(\frac{b+4a}{a}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}} \left(\frac{b}{a}\right) = \left(\frac{a}{b}\right).$$

- 4) Seien  $p, q$  ungerade Primzahlen mit  $p \neq q$ . Das  $p$ -te Kreisteilungspolynom hat die Diskriminante  $D = p^* p^{p-3}$ . Dann ist  $\left(\frac{p^*}{q}\right) = \left(\frac{D}{q}\right) \equiv D^{(q-1)/2} \equiv \Delta^{q-1} \pmod{qR}$ , wo  $\Delta$  wie in (8.16) definiert ist, und  $R = \mathbb{Z}[\zeta_p]$  ist. Man zeige nun, dass andererseits  $\Delta^q \equiv \left(\frac{q}{p}\right) \Delta \pmod{qR}$  ist, und folgere das quadratische Reziprozitätsgesetz.

Es ist  $\Delta = \prod_{i < j} (\zeta^j - \zeta^i)$ , wo  $\zeta$  eine primitive  $p$ -te Einheitswurzel ist und die Summation über alle  $1 \leq i < j \leq p-1$  geht. Daher ist  $\Delta^q \equiv \prod_{i < j} (\zeta^{qj} - \zeta^{qi}) \pmod{qR}$ .

Reduziert man die Exponenten mod  $p$ , so wird  $qj \equiv j'$  und  $qi \equiv i' \pmod{p}$ , und die Differenzen  $j' - i'$  sind bis auf das Vorzeichen eine Permutation der  $j - i$ . Bezeichnet  $\varepsilon$  die Anzahl der Zeichenwechsel, so ist  $\varepsilon = \left(\frac{q}{p}\right)$ : dies sieht man am einfachsten wohl folgendermaßen ein. Es ist

$$\begin{aligned} \prod_{i < j} (j' - i') &\equiv \prod_{i < j} (qj - qi) \equiv q^{(p-1)(p-2)/2} \prod_{i < j} (j - i) \\ &\equiv \left(\frac{q}{p}\right)^{p-2} \prod_{i < j} (j - i) = \left(\frac{q}{p}\right) \prod_{i < j} (j - i) \pmod{p}. \end{aligned}$$

Also ist  $\prod_{i < j} (\zeta^{qj} - \zeta^{qi}) = \left(\frac{q}{p}\right) \prod_{i < j} (\zeta^j - \zeta^i)$ , und die Behauptung  $\Delta^q \equiv \left(\frac{q}{p}\right) \Delta \pmod{qR}$  folgt.

# Übungen zu Kapitel 12

- 1) Seien  $p_1 : G_1 \longrightarrow \Delta$  und  $p_2 : G_2 \longrightarrow \Delta$  Homomorphismen von Gruppen. Zeige, dass dann

$$G_1 \times_{\Delta} G_2 = \{(g_1, g_2) \in G_1 \times G_2 \mid p_1(g_1) = p_2(g_2)\}$$

eine Gruppe ist. Man nennt diese oft das zu den Homomorphismen  $p_1, p_2$  gehörige Faserprodukt.

Sei  $\Gamma = G_1 \times_{\Delta} G_2$ . Schreiben wir die Gruppen multiplikativ, so ist  $(1, 1) \in \Gamma$  wegen  $p_1(1) = p_2(1) = 1$ , und  $(1, 1)$  ist das neutrale Element in  $\Gamma$ . Ist  $(g_1, g_2) \in \Gamma$ , so gilt  $p_1(g_1) = p_2(g_2)$ , daher auch  $p_1(g_1^{-1}) = p_2(g_2^{-1})$ , und es folgt  $(g_1, g_2)(g_1^{-1}, g_2^{-1}) = (1, 1)$ . Da Assoziativität sich von  $G_1 \times G_2$  auf  $\Gamma$  vererbt, sind wir damit fertig.

- 2) Betrachte (12.12) mit  $K = \mathbb{Q}$  und  $E = \mathbb{Q}(\sqrt{2})$ .

- (i) Zeige, dass die Elemente  $1 \otimes 1$ ,  $1 \otimes \sqrt{2}$ ,  $\sqrt{2} \otimes 1$  und  $\sqrt{2} \otimes \sqrt{2}$  eine  $K$ -Basis von  $E \otimes_K E$  bilden.
- (ii) Schreibe das Element  $(a+b\sqrt{2}) \otimes (c+d\sqrt{2}) \in E \otimes_K E$  als Summe  $1 \otimes c_1 + \sqrt{2} \otimes c_2$  mit  $c_1, c_2 \in E$ .
- (iii) Finde Elemente  $\alpha, \beta \in E \otimes_K E$  mit  $f(\alpha) = 1 + \sigma$  und  $f(\beta) = 1 - \sigma$ .
- (iv) Zeige direkt, dass  $f$  surjektiv ist.

(i) Dies ist ein Spezialfall von F6.8.

(ii) Es ist

$$\begin{aligned} (a + b\sqrt{2}) \otimes (c + d\sqrt{2}) &= a \otimes (c + d\sqrt{2}) + b\sqrt{2} \otimes (c + d\sqrt{2}) \\ &= 1 \otimes a(c + d\sqrt{2}) + \sqrt{2} \otimes b(c + d\sqrt{2}). \end{aligned}$$

(iii) Offenbar ist  $f(1 \otimes 1) = 1 + \sigma$ , sowie  $f(\sqrt{2} \otimes \frac{1}{\sqrt{2}}) = 1 - \sigma$ .

(iv) Da sich jedes Element in  $EG$  als  $E$ -Linearkombination von  $1 + \sigma$  und  $1 - \sigma$  schreiben lässt, folgt dies aus (iii).

3) Sei  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$  der von allen Quadratwurzeln natürlicher Zahlen erzeugte Körper.

- (i) Sei  $p$  prim. Dann gibt es einen Automorphismus  $\sigma_p$  von  $E/\mathbb{Q}$ , welcher  $\sqrt{p}$  auf  $-\sqrt{p}$  abbildet und alle  $\sqrt{q}$  mit  $q \neq p$  fest lässt.
- (ii) Sei  $H$  die von allen  $\sigma_p$  erzeugte Untergruppe der Galoisgruppe  $G$  von  $E/\mathbb{Q}$ . Zeige, dass  $\mathbb{Q}$  der Fixkörper von  $H$  ist.
- (iii) Es gibt einen Automorphismus  $\tau$ , der jedes  $\sqrt{p}$  auf  $-\sqrt{p}$  abbildet.
- (iv) Zeige, dass  $\tau \notin H$  ist.
- (v) Zeige, dass  $G = H^-$  ist.
- (vi) Zeige, dass  $G$  nicht abzählbar ist.
- (vii) Zeige, dass  $G$  überabzählbar viele Untergruppen vom Index 2 besitzt; andererseits sind die quadratischen Teilkörper von  $E$  natürlich abzählbar.

- (i) Sei  $F$  der Körper, der von allen  $\sqrt{q}$  erzeugt wird, wo  $q$  die Primzahlen  $\neq p$  durchläuft. Wegen  $E = F(\sqrt{p})$  ist  $E : F = 2$ , und der nichttriviale Automorphismus von  $E/F$  hat die gewünschte Eigenschaft.
- (ii) Wäre der Fixkörper von  $H$  größer als  $\mathbb{Q}$ , müsste er ein  $\sqrt{n}$  mit einem quadratfreien  $n \geq 2$  enthalten. Ist  $p$  eine Primzahl mit  $p \mid n$ , so ist aber  $\sigma_p(\sqrt{n}) = -\sqrt{n}$ .
- (iii) Dies folgt wie in (i).
- (iv) Jeder Automorphismus in  $H$  bewegt nur endlich viele  $\sqrt{p}$ .
- (v) Dies folgt jetzt sofort aus (12.38).
- (vi) Sei  $\sigma \in G(E/\mathbb{Q})$ ; wir definieren eine Abbildung  $\lambda : G(E/\mathbb{Q}) \rightarrow [0, 1]$ , indem wir jedem  $\sigma \in G(E/\mathbb{Q})$  die reelle Zahl zuordnen, deren binäre Entwicklung durch  $0.a_1a_2a_3\dots$  gegeben ist, wo  $\sigma(\sqrt{p_n}) = (-1)^{a_n}\sqrt{p_n}$  gesetzt ist. Diese Abbildung ist surjektiv, und da die reellen Zahlen im Intervall  $[0, 1]$  nicht abzählbar sind, folgt die Behauptung.
- (vii) Sei  $\sigma_i = \sigma_{p_i}$ ; zu jeder Teilmenge  $S \subseteq \mathbb{N} \setminus \{1\}$  konstruieren wir eine Untergruppe  $H_S$  vom Index 2 wie folgt:  $H_S$  sei erzeugt von allen  $\sigma_1^{a_i}\sigma_i$  mit  $i \geq 2$ , wo  $a_i = \begin{cases} 1 & \text{falls } i \in S \\ 0 & \text{falls } i \notin S \end{cases}$  ist. Wegen  $\langle \sigma_1, H_S \rangle = G$  und  $\sigma_1 \notin H_S$  hat  $H_S$  Index 2. Da verschiedene Mengen  $S$  verschiedenen Untergruppen entsprechen (ist  $j \in S$ , aber  $j \notin T$ , so ist  $\sigma_1\sigma_j \in H_S$ , aber  $\sigma_1\sigma_j \notin H_T$ ), ist damit alles gezeigt.

Übrigens ist  $G \simeq \prod \mathbb{Z}/2$  isomorph zum direkten Produkt abzählbar vieler Kopien von  $\mathbb{Z}/2$ .

# Übungen zu Kapitel 13

- 1) Sei  $m \in \mathbb{Z}$  quadratfrei und  $m \neq 1$ . Man überzeuge sich davon, dass  $M = \mathbb{Q}(\sqrt{m})$  ein freier  $\mathbb{Q}$ -Modul mit Basis  $\{1, \sqrt{m}\}$  ist. Für  $\alpha = a + b\sqrt{m} \in M$  zeige man, dass  $P_{M/\mathbb{Q}}(\alpha; X) = X^2 - 2aX + a^2 - mb^2$  gilt.

Sei nun  $L = \mathbb{Q}(\sqrt{n})$  ein zweiter quadratischer Körper. Man überlege sich, dass dann  $M \otimes_{\mathbb{Q}} L$  mit  $\{\alpha + \beta\sqrt{m} \mid \alpha, \beta \in L\}$  identifiziert werden kann, und rechne nach, dass (13.10) und (13.11) gelten, sich das charakteristische Polynom also nicht ändert.

Dass  $\{1, \sqrt{m}\}$  eine  $\mathbb{Q}$ -Basis von  $M = \mathbb{Q}(\sqrt{m})$  ist, liegt natürlich an der Irrationalität von  $\sqrt{m}$ . Also ist  $M$  ein freier  $\mathbb{Q}$ -Modul vom Rang 2.

Multiplikation durch  $\alpha = a + b\sqrt{m}$  bildet die Basisvektoren 1 und  $\sqrt{m}$  ab auf  $a + b\sqrt{m}$  und  $mb + a\sqrt{m}$ , sodass die dazugehörige Matrix durch  $M_{\alpha} = \begin{pmatrix} a & bm \\ b & a \end{pmatrix}$  gegeben ist. Daher gilt

$$P_{M/\mathbb{Q}}(X) = \det(XI - M_{\alpha}) = X^2 - 2aX + a^2 - mb^2.$$

Nun hat  $M \otimes L$  als  $L$ -Modul nach Definition die  $L$ -Basis  $\{1, \sqrt{m}\}$ ; daher wird die Multiplikation mit  $a + b\sqrt{m}$  durch genau dieselbe Matrix wie eben beschrieben, und damit ändert sich insbesondere das charakteristische Polynom nicht.

- 2) Beweise Hilberts Satz 90 für quadratische Erweiterungen  $E = K(\sqrt{m})$  eines Körpers  $K$  der Charakteristik  $\neq 2$ . Hinweis: sei  $N\gamma = 1$ ; unterscheide zwischen  $\gamma = -1$  und  $\gamma \neq -1$ ; im letzteren Falle betrachte  $\frac{\gamma}{\gamma+1}$ .

Ist  $\gamma = -1$ , so setze man  $\alpha = \sqrt{m}$ . Ist  $\gamma \neq -1$  und  $\alpha = \frac{\gamma}{\gamma+1}$ , so folgt  $\frac{\alpha}{\sigma(\alpha)} = \frac{\gamma(\sigma(\gamma)+1)}{(\gamma+1)\sigma(\gamma)} = \frac{\gamma(\sigma(\gamma)+1)}{\gamma\sigma(\gamma)+\sigma(\gamma)} = \frac{\gamma(\sigma(\gamma)+1)}{1+\sigma(\gamma)} = \gamma$ .

- 3) Finde alle rationalen Lösungen von  $x^2 + y^2 = 1$  mit Hilfe von Hilberts Satz 90. Hinweis: Es ist  $N(x + iy) = 1$ .

Sei  $(x, y)$  eine rationale Lösung von  $x^2 + y^2 = 1$ . Dann ist  $N(x + yi) = 1$  für das Element  $x + yi \in \mathbb{Q}(i)$ ; nach Hilbert 90 gibt es ein  $\beta \in \mathbb{Q}(i)$  mit  $x + yi = \beta'/\beta$ . Mit

$\beta = a + bi$  folgt daraus  $x + yi = \frac{a-bi}{a+bi} = \frac{(a-bi)^2}{a^2+b^2} = \frac{a^2-b^2}{a^2+b^2} - \frac{2ab}{a^2+b^2}i$ . Vergleich von Real- und Imaginärteil liefert dann

$$x = \frac{a^2 - b^2}{a^2 + b^2}, \quad y = -\frac{2ab}{a^2 + b^2}.$$

# Übungen zu Kapitel 14

- 1) Sei  $p$  eine ungerade Primzahl und  $k$  ein Körper der Charakteristik  $\neq p$ . Sei weiter  $K = k(\zeta_p)$  und  $L = K(\sqrt[p]{\mu})$  für ein  $\mu \in K^\times$ . Zeige: Die Erweiterung  $L/k$  ist normal genau dann, wenn es zu jedem  $\sigma \in G(K/k)$  ein  $\alpha_\sigma \in K^\times$  und ein  $a(\sigma) \in \mathbb{Z}$  gibt mit  $\mu^\sigma = \alpha_\sigma^p \mu^{a(\sigma)}$ .

Wir dürfen oBdA annehmen, dass  $\mu$  keine  $p$ -te Potenz ist. Nach Aufg. 14.2 ist  $K(\sqrt[p]{\mu}) = K(\sqrt[p]{\mu}^\sigma)$  genau dann, wenn es ein  $a(\sigma) \in \mathbb{Z}$  gibt mit  $\mu^\sigma = \alpha_\sigma^p \mu^{a(\sigma)}$ . Daraus folgt aber sofort die Behauptung.

- 2) Konstruktion zyklischer kubischer Erweiterungen von  $\mathbb{Q}$ : Sei  $K = \mathbb{Q}(\sqrt{-3})$ ; wähle ein  $\alpha \in K$ , welches keine dritte Potenz in  $K$  ist, und setze  $\mu = \alpha' \alpha^2$ , wo  $\alpha'$  die Konjugierte von  $\alpha$  ist. Zeige:

- $\mu$  ist eine dritte Potenz in  $K$  genau dann, wenn  $\alpha = \alpha'$ , also  $\alpha \in \mathbb{Q}$  ist. Im Folgenden sei dieser Fall ausgeschlossen.
- $L = K(\sqrt[3]{\mu})$  ist abelsch über  $\mathbb{Q}$ .
- Setze  $\beta = \sqrt[3]{\mu} + \sqrt[3]{\mu'}$ , wo die dritten Wurzeln so gewählt sind, dass das Produkt  $m = \sqrt[3]{\mu} \sqrt[3]{\mu'}$  reell (und damit rational) ist. Dann genügt  $\beta$  der Gleichung  $x^3 - 3mx - n$  für  $n = \mu + \mu' \in \mathbb{Q}$ .
- Der kubische Teilkörper von  $L$  ist  $\mathbb{Q}(\beta)$ . Dieser ist zyklisch vom Grad 3 über  $\mathbb{Q}$ .

- Bezeichnet  $\zeta$  eine primitive Einheitswurzel, so ist der Ring  $\mathbb{Z}[\zeta]$  euklidisch bezüglich der Normfunktion, also insbesondere faktoriell. Sei nun oBdA  $\alpha \in \mathbb{Z}[\zeta]$  frei von dritten Potenzen. Ist dann  $\alpha' \alpha^2$  eine dritte Potenz, so muss jeder Primfaktor von  $\alpha'$  auch  $\alpha$  teilen, und umgekehrt. Mit  $\pi \mid \alpha$  ist also auch  $\pi' \mid \alpha$ , und daraus folgt sofort, dass  $\alpha$  bis auf einen Einheitenfaktor rational ist. Da  $\mu$  aber für  $\alpha = \pm \zeta a$  oder  $\alpha = \pm \zeta^2 a$  und rationales  $a$  keine dritte Potenz ist, muss  $\alpha$  rational sein.
- Das ist klar, da hier eine Kummererweiterung vorliegt.



c) Offenbar gilt

$$\beta^3 = (\sqrt[3]{\mu} + \sqrt[3]{\mu'})^3 = \mu + \mu' + 3\sqrt[3]{\mu}\sqrt[3]{\mu'}(\sqrt[3]{\mu} + \sqrt[3]{\mu'}) = n + 3m\beta.$$

d) Wir wissen  $\beta \in L$  und  $\mathbb{Q}(\beta) : \mathbb{Q} \leq 3$ , sowie  $L = K(\beta)$ ; letzteres zeigt aber  $3 = (L : K) \leq (\mathbb{Q}(\beta) : \mathbb{Q})$ , und damit  $\mathbb{Q}(\beta) : \mathbb{Q} = 3$ .

Dass  $L/\mathbb{Q}$  und damit auch  $\mathbb{Q}(\beta)/\mathbb{Q}$  abelsch ist, folgt aus Aufg. 14.14: es ist nämlich, wenn  $\sigma$  den nichttrivialen Automorphismus von  $K/\mathbb{Q}$  bezeichnet, einerseits  $\zeta^\sigma = \zeta^2$ , und andererseits  $\mu^{\sigma-2} = (\alpha'^2\alpha)/(\alpha'\alpha^2)^2 = \alpha^{-3}$  eine dritte Potenz.

# Übungen zu Kapitel 15

- 1) *Der normale Abschluss von  $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$  hat Galoisgruppe  $D_8$  (Diedergruppe der Ordnung 8) und ist auflösbar. Welches sind die möglichen Untergruppenketten in diesem Fall?*

Es ist  $D_8 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ . Die Untergruppe  $V_4 = \langle \sigma^2, \tau \rangle$  ist die einzige normale Untergruppe in  $D_8$  mit zyklischer Faktorgruppe der Ordnung 2. Weiter sind  $C_1 = \langle \sigma^2 \rangle$ ,  $C_2 = \langle \tau \rangle$  und  $C_3 = \langle \sigma^2\tau \rangle$  normal in  $V_4$ , und damit haben wir die folgenden Untergruppenreihen:

$$D_8 \triangleright V_4 \triangleright C_1 \triangleright 1,$$

$$D_8 \triangleright V_4 \triangleright C_2 \triangleright 1,$$

$$D_8 \triangleright V_4 \triangleright C_3 \triangleright 1.$$

- 2) *Zeige, dass das Polynom  $x^6 + x^2 + 1$  durch Radikale auflösbar ist.*

Dies liegt einfach daran, dass die Nullstellen von  $x^6 + x^2 + 1$  Quadratwurzeln der Nullstellen des kubischen Polynoms  $x^3 + x + 1$  sind, und dieses Polynom durch Radikale auflösbar ist.

- 3) *Sei  $\alpha \in \mathbb{A} \setminus \{0, 1\}$  und  $E = \mathbb{Q}(\alpha)$ . Zeige, dass  $E/\mathbb{Q}$  eine Radikalerweiterung ist.*

Setze  $F = \mathbb{Q}(\alpha)$ . Ohne Einschränkung sei  $F \neq \mathbb{Q}$ . Nach Satz 11.1 ist die normale Hülle  $E/\mathbb{Q}$  von  $F/\mathbb{Q}$  eine Galoiserweiterung mit einer 2-Gruppe  $G$  als Galoisgruppe. Sei  $H$  die Untergruppe von  $G$ , die zum Zwischenkörper  $F$  von  $E/\mathbb{Q}$  gehört. Um zu zeigen, dass  $F/\mathbb{Q}$  eine Radikalerweiterung ist, genügt es zu zeigen (Galoistheorie!), dass es eine Kette

$$G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_r = H$$

von Untergruppen  $H_i$  von  $G$  mit  $(H_{i-1} : H_i) = 2$  für alle  $i$  mit  $1 \leq i \leq r$  gibt.

Zum Beweis dieser Tatsache (die entsprechend für eine beliebige endliche  $p$ -Gruppe gilt) sh. Aufgabe 10.5.

# Übungen zu Kapitel 16

- 1) Sei  $R = \mathbb{Z}$  und  $A = \mathbb{Z}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots]$  der von allen  $\sqrt{p}$ ,  $p$  prim, erzeugte Ring. Zeige:  $A/R$  ist ganz, aber nicht endlich.

Jedes Element von  $A$  ist Summe ganzer algebraischer Zahlen, und daher ganz über  $\mathbb{Z}$ . Also ist  $A/\mathbb{Z}$  ganz.

Da die  $\sqrt{p}$  über  $\mathbb{Q}$  linear unabhängig sind, lassen sie sich nicht als  $\mathbb{Z}$ -Linearkombination endlich vieler Elemente schreiben. Also ist  $A/R$  nicht endlich.

- 2) Sei  $R = \mathbb{Z}$  und  $A = \mathbb{Z}[\frac{1}{2}]$ . Ist  $A/R$  endlich? Ist  $A/R$  ganz?

$A$  enthält die Elemente  $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots$ ; wäre  $A$  endlich, müsste es endlich viele  $a_i \in A$  geben, sodass jedes  $a \in A$  eine  $\mathbb{Z}$ -Linearkombination der  $a_i$  ist. Dies kann aber nicht sein: die endlich vielen  $a_i$  haben einen maximalen Nenner  $2^m$ , und alle  $\mathbb{Z}$ -Linearkombinationen der  $a_i$  haben deswegen die Eigenschaft, dass ihr Nenner durch  $2^m$  beschränkt ist. Also kann  $\frac{1}{2^m} \in A$  keine  $\mathbb{Z}$ -Linearkombination dieser  $a_i$  sein.

Wegen F.16.3.ii) ist  $A/R$  damit auch nicht ganz, da  $\mathbb{Z}[\frac{1}{2}]$  als  $\mathbb{Z}$ -Modul nicht endlich erzeugt ist. Direkt kann man das so einsehen: wäre  $\frac{1}{2}$  Nullstelle von  $X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ , so folgt nach Einsetzen von  $X = \frac{1}{2}$  und Durchmultiplizieren mit  $2^n$  die Gleichung  $1 + 2a_{n-1} + \dots + 2^n a_0 = 0$ , was modulo 2 sofort auf einen Widerspruch führt.

- 3) Sei  $R = \mathbb{Z}$  und  $A = \mathbb{Z}[\sqrt{5}]$ . Zeige:  $A/R$  ist endlich und ganz, aber  $A$  ist nicht ganz abgeschlossen in  $\mathbb{Q}(\sqrt{5})$ .

Wegen  $A = \mathbb{Z} \oplus \sqrt{5}\mathbb{Z}$  ist  $A/R$  endlich. Weiter sind alle Elemente von  $A$  ganze algebraische Zahlen, also ist  $A$  auch ganz. Allerdings ist  $A$  nicht ganz abgeschlossen, weil  $\omega = \frac{1+\sqrt{5}}{2}$  im Quotientenkörper von  $A$  liegt und der Ganzheitsgleichung  $\omega^2 - \omega - 1 = 0$  genügt.

- 4) Zeige direkt, dass  $\mathbb{Z}[\sqrt{5}]$  nicht faktoriell ist.

Betrachte  $4 = 2 \cdot 2 = (\sqrt{5} - 1)(\sqrt{5} + 1)$ . Die Faktoren 2 und  $\sqrt{5} \pm 1$  unterscheiden sich nicht nur um Einheiten, da  $\frac{\sqrt{5} \pm 1}{2}$  nicht in  $\mathbb{Z}[\sqrt{5}]$  liegen. Weiter ist 2 irreduzibel in  $\mathbb{Z}[\sqrt{5}]$ : dazu führen wir für  $\alpha = a + b\sqrt{5}$  die Norm  $N(\alpha) = \alpha\alpha' = a^2 - 5b^2$  ein, wo  $\alpha' = a - b\sqrt{5}$  die Konjugierte von  $\alpha$  ist. Eine leichte Rechnung zeigt, dass die Norm multiplikativ ist.

Aus  $2 = \alpha\beta$  folgt dann  $4 = N\alpha N\beta$ . Da es keine Elemente der Norm  $\pm 2$  in  $\mathbb{Z}[\sqrt{5}]$  gibt ( $a^2 - 5b^2 = \pm 2$  liefert  $a^2 \equiv \pm 2 \pmod{5}$ , und diese Kongruenz hat keine Lösung), muss  $N\alpha = \pm 1$  oder  $N\beta = \pm 1$  sein. Dies impliziert aber, dass  $\alpha$  oder  $\beta$  Einheit ist: dies kann man an  $\pm 1 = N(\alpha) = \alpha\alpha'$  nämlich direkt ablesen.

Andererseits ist 2 nicht prim, da es zwar das Produkt  $(\sqrt{5} - 1)(\sqrt{5} + 1)$ , aber keinen der beiden Faktoren teilt. Daher ist  $\mathbb{Z}[\sqrt{5}]$  nicht faktoriell.

5) Sei  $K$  ein Körper. Ist der Ring  $R = K[X^2, X^3]$  ganz abgeschlossen?

Der Quotientenkörper von  $R$  enthält  $X = \frac{X^3}{X^2}$  und ist daher  $K(X)$ . Das Polynom  $T - X \in R[T]$  ist normiert und hat  $X$  als Nullstelle; also ist  $X$  ganz, folglich ist  $K[X]$  der ganze Abschluss von  $R$ . Dies erklärt auch, warum der Ring  $R$  nicht faktoriell sein kann.

Algebra 1

Körper und Galoistheorie

Lorenz, F.; Lemmermeyer, F.

2007, X, 390 S., Softcover

ISBN: 978-3-8274-1609-4