Lösungvorschläge zu den ausgewählten Aufgaben

der

VL Algebra I

Prof. U. Kühn SS 2005

von

Anna Posingies[1], Markus Hihn[2]

4. Juli 2005

[1]email: Anna(dot)Posingies(at)gmx(dot)de
[2]email: mhihn(at)mathematik(dot)hu-berlin(dot)de

I.2

a) Man betrachtet einfach $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/5\mathbb{Z}$ bzgl. Addition und rechnet sich die Tabellen per Hand aus.

b) Gruppen der Ordnung 4 ist $\mathbb{Z}/4\mathbb{Z}$ und die kleinsche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (kleinste Gruppe, die nicht zyklisch ist)

Gruppen der Ordnung 6 sind die Gruppe $\mathbb{Z}/6\mathbb{Z}$ abelscher Fall und die Symmetriegruppe des gleichseitigen Dreiecks D_3 diese entspricht der S_3 nicht abelscher Fall.

c) Die Fälle 1,2,3,5 sind uninteressant, weil sie Primenzahlen sind. Diese sind als abelsche Gruppen bis auf Isomorphie eindeutig bestimmt sind. Durch Ausprobieren stellt man im Fall 4 und 6 fest, dass die unter b) genannten die einzigen sind.

Aufgabe II.1

a) Das Zentrum von $\mathrm{GL}_n(\mathbb{R})$ ist λI. Angenommen es wären noch weitere Matrizen A im Zentrum, dann haben diese außerhalb der Hauptdiagonale einen von Null verschieden Eintrag. Es reicht also zu überprüfen, das diese Matrizen nicht im Zentrum liegen. Sei $I_{k,l}$ die Einheitsmatrix mit einer weiteren 1 in der k-ten Zeile und l-ten Spalte, dann ist $I_{k,l} \in \mathrm{GL}_n(\mathbb{R})$. Es reicht zu zeigen, daß bei geeignerter Wahl von k, l gilt $AI_{k,l} \neq I_{k,l}A$

$$(AI_{k,l})_{ij} = \sum_{r=1}^{n} A_{ir}\delta_{kr}\delta_{lj} = A_{ik}\delta_{lj}$$

$$(I_{k,l}A)_{ij} = \sum_{r=1}^{n} A_{rj}\delta_{ki}\delta_{rj} = A_{jj}\delta_{ki}$$

Das ist offensichtlich nicht das selbe (Setze k = l, i = j z.B.)

b) Das Zentrum $Z(S_4)$ ist trivial. Angenommen es existiere $id \neq \sigma \in Z(S_4)$ mit $\sigma(i) \neq i$ für ein $i = 1, ...4$. Es gibt offensichtlich ein $\tau \in S_4$ mit $\tau(i) = i$ und $\tau(\sigma(i)) \neq \sigma(i)$. Weil σ im Zentrum von S_4 ist gilt nun $\sigma\tau = \tau\sigma$ und so erhalten wir den Widerspruch

$$\sigma(i) = \sigma(\tau(i)) = \tau(\sigma(i)) \neq \sigma(i).$$

III.4

- (a) Bew.:

  Z.z.: $[G,G]$ ist ein Normalteiler in G, d.h. z.z. ist, dass für alle $h \in G$ gilt: $h[G,G]h^{-1} = [G,G]$. Sei $h \in G$ beliebig, dann gilt für $[a,b] \in [G,G]$:

  $$h[ab]h^{-1} = haba^{-1}b^{-1}h = (hah^{-1})(hbh^{-1})(ha^{-1}h^{-1})(hb^{-1}h^{-1})$$

  $$= (hah^{-1})(hbh^{-1})(hah^{-1})^{-1}(hbh^{-1})^{-1} = [cac^{-1}, cbc^{-1}]$$

  .

  Z.z.: $G/[G,G]$ ist eine abelsche Gruppe. Seinen $a, b \in G$, dann ist wegen $ab[b^{-1}a^{-1}] = abb^{-1}a^{-1}ba = ba$ auch $ab[G,G] = ba[G,G]$, also ist die Gruppe abelsch.

- (b) Bew.: Es genügt zu zeigen, dass $[G,G]$ im Kern von φ liegt, denn dann gibt es nach der universellen Eigenschaft der Faktorgruppe den gewünschten Morphismus. Sei $[ab] \in [G,G]$, so gilt $\varphi([a,b]) = \varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = \varphi(a)\varphi(a^{-1})\varphi(b)\varphi(b^{-1}) = 0$, wobei das erste und das letzte $=$ gilt, da φ ein Homomorphismus ist und das dritte $=$ gilt, da H abelsch ist.

  Also liegt $[G,G]$ im Kern der Abbildung und der Morphismus h existiert.

V.1

Es sei $\varphi : R \to R'$ ein Hom. von Ringen.

- (a) Z.z. ist, dass $im(\varphi)$ ein Unterring von R' ist.

  Bew.: Da $im(\varphi) \subset R'$ ist, folgen die Assoziativität von "+" und "$\cdot$", die Kommutativität von "+" und die Distributivität aus der Tatsache, dass R' ein Ring ist.

  Z.z. bleiben: Die Operationen sind abgeschlossen: Seien $a, b \in im(\varphi)$ mit $a = \varphi(a'), b = \varphi(b')$, dann gilt

  $$a + b = \varphi(a') + \varphi(b') = \varphi(a' + b') \in im(\varphi)$$

$$a \cdot b = \varphi(a') \cdot \varphi(b') = \varphi(a' \cdot b') \in im(\varphi).$$

Die Null und die Eins liegen im Bild: Dies gilt, da Ringhomomorphismen Null auf Null abbilden und $\varphi(1) = 1$.

Die Existenz eines Inversen bzgl. "$+$" : Sei $a \in im(\varphi)$ mit $a = \varphi(a')$. Dann ist $b := \varphi(-a')$ das Inverse zu a, da

$$a + b = \varphi(a') + \varphi(-a') = \varphi(a' - a') = \varphi(0) = 0.$$

Also ist $im(\varphi)$ ein Unterring.

- (b) Z.z. ist, dass $ker(\varphi) \subset R$ ein Ideal ist.

  Bew.: Z.z. ist:

  Der Kern ist abgeschlossen bzgl. "$+$" und $R \cdot ker(\varphi) \subseteq ker(\varphi)$. Seien $a, b \in ker(\varphi), r \in R$. So gilt:

  $$\varphi(a + b) = \varphi(a) + \varphi(b) = 0 + 0 = 0 \Rightarrow a + b \in ker(\varphi)$$

  $$\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0 \Rightarrow r \cdot a \in ker(\varphi).$$

  Daraus folgt auch, dass $0 = 0 \cdot a \in ker(\varphi)$ und $-a = -1 \cdot a \in ker(\varphi)$, wobei $a \in ker(\varphi)$.

  Also ist $ker(\varphi)$ ein Ideal.

V.2

- (a) Bew.:

  1. Sei $\mathbb{Z}/n\mathbb{Z}$ ein Körper, dann folgt, n ist prim. Äquivalent dazu kann man zeigen, dass, wenn n keine Primzahl ist, folgt ,dass $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist. Sei also n keine Primzahl, d.h es exsistieren $l, m \in \mathbb{Z} \setminus \{1\}$ mit $l \cdot m = n$. Dann gilt in $\mathbb{Z}/n\mathbb{Z}$ die Identität $[l] + [m] = [0]$, d.h. $\mathbb{Z}/n\mathbb{Z}$ ist kein Körper, da es Nullteiler gibt.

  2. Sei p eine Primzahl, dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper.

  Wir benutzen folgenden Satz: Sei R ein Ring und $\mathfrak{m} \subset R$ ein Ideal. Dann ist $R/\mathfrak{m}$ ein Körper g.d.w., $\mathfrak{m}$ maximal ist.

Wir Zeigen, dass $p\mathbb{Z}$ ist maximal: Angenommen $\mathfrak{a}$ sei ein Ideal mit $p\mathbb{Z} \subsetneq \mathfrak{a}$. Dann gibt es ein $a \in \mathfrak{a}$ mit $ggT(p,a) = 1$ und wegen $\mathfrak{a} \supseteq (p,a) = (ggT(p,a)) = (1) = \mathbb{Z}$ folgt die Behauptung.

- (b) da $\mathbb{Z}$ faktoriell ist, ist $\mathbb{Z}[x]$ auch faktoriell. Es genügt also zu zeigen, dass $f(x) = x^2+x+1$ irreduzibel ist in $\mathbb{Z}[x]$, denn faktoriellen Ringen sind irred. Elemente prim. Da $f(x)$ nur vom Grad 2 ist und keine Nullstellen in $\mathbb{Z}$ hat, ist es irreduzibel. Also ist $(f(x))$ ein Primideal.

- (c) Wie in (b) genüg es zu zeigen, dass p prim ist. Bekannterweise hat p keine Zerlegung in $\mathbb{Z}$. Ein Polynom vom Grad größer Null kann aber kein Faktor von p sein, da das Produkt von Polynomen vom Grad $\geqslant 1$ auch ein solches ist. Also gibt es keine Zerlegung von p und (p) ist ein Primideal.

- (d) Sei $\mathfrak{a} = (5, x^2+x+1)$, so ist $\mathbb{Z}[x]/\mathfrak{a} = \left\{ax + b : a, b \in \mathbb{Z}/5\mathbb{Z}, x^2 = -x - 1\right\}$ (da $5 \equiv 0$ und $x^2 + x + 1 \equiv 0$). Dies ist ein Körper, da $x^2 + x + 1$ über $\mathbb{F}_5 = \mathbb{Z}/(5)$ irreduzibel ist, also ist $\mathfrak{a}$ ein maximales Polynom.

VI.1

- (a) Finden Sie die kleinste Zahl $x \in \mathbb{N}$ mit $x \equiv 3 \; mod \; 4$, $x \equiv 1 \; mod \; 9$ und $x \equiv 4 \; mod \; 5$.

  Ergebnis: 19 (z.B. durch durchgehen der Zahlen $x \equiv 1 \; mod \; 9$ und Überprüfung der anderen Bedingungen.)

- (b) Was sind der ggT und der kgV von 17201 und 13861?

  Bew.: Mit den euklidischen Algorithmus folgt $17201 = 13861+3340$, $13861 = 3340 \cdot 4 + 501$, $3340 = 501 \cdot 6 + 334$, $501 = 334 + 167$, $334 = 167 \cdot 2 + 0$, also ist 167 der ggT der beiden Zahlen. Für den kgV folgt: $kgV(a,b) = \frac{a \cdot b}{ggT(a,b)}$, also ist der kgV der beiden Zahlen $\frac{17201 \cdot 13861}{167} = 142843$.

- (c) Man berechne mit Hilfe des euklidischen Algorithmus den ggT der folgenden Polynome aus $\mathbb{Q}[x]$:

$$f = x^3 + x^2 + x - 3, \; g = x^6 - x^5 + 6x^2 - 13x + 7.$$

Bew.: Mit den Polynomdivision brechnet man $f = qg + r$, dann $g = q'r + r'$ und so weiter, bis der Rest (r^j) Null ist. Der $ggT(f, g)$ ist dann r^{j-1}.

Hier erhält man: $g = f \cdot (x^3 - 2x^2 + x + 4) + (-5x^2 - 14x + 19)$, $f = (-5x^2 - 14x + 19)(-\frac{1}{5}x + \frac{9}{25}) + (-\frac{246}{25}x + \frac{246}{25})$ und schließlich $-5x^2 - 14x + 19 = (-\frac{246}{25}x + \frac{246}{25})(\frac{5 \cdot 25}{246}x + \frac{9 \cdot 25}{246}) + 0$. Also ist der $ggT(f, g)$ das Polynom $-\frac{246}{25}x + \frac{246}{25}$, d.h. $x - 1$.

Aufgabe VI.2

a)

Die Lösung findet man im Artin auf Seite 455:

$\mathbb{Z}[i]$ bildet ein Gitter.Ein Ideal erzeugt durch $a = e^{i\theta}$ ist geometrisch nichts anderes als $\mathbb{Z}[i]$ um den Winkel θ gestreckt und um den Faktor $|a|$ gestreckt. Zu jedem $b\ in\mathbb{C}$ ist der Quadrat des Abstandes zu dem so erhaltenen Gitter $1/2|a|^2$. Sei $r = b - aq$, wobei b nicht auf dem Gitter liegt, offensichtlich aq jedoch. Dann ist $|r|^2 \leqslant 1/2|a|^2 < |a|^2$, was die Bedingung für einen euklidischen Ring ist.

b)

Beides erhält man durch den euklidischen Algorithmus

VI.3

- (a) $\mathfrak{p} = (2, 1 + \sqrt{5})$ ist ein Primideal, da $R/\mathfrak{p} \equiv \mathbb{F}_3$ ist: Im Faktorring gibt ausser Null nur die Elemente 1 und $\sqrt{5} \equiv -1$ ($\mathfrak{p}$). Alle anderen Elemente aus R lassen sich duch diese beiden und $\mathfrak{p}$ darstellen.

  $\mathfrak{p}$ kann nicht von einem Element s erzeugt werden, denn s müsste beide Erzeuger teilen. Insbesondere bedeutet dies, dass $Nm(s)$ die Normen von 2 und $1+\sqrt{5}$ teilen muss. $Nm(2) = 2^2 = 4$ und $Nm(1+\sqrt{5}) = 1^2+5 \cdot 1^2 = 6$. In einer Zerlegung von 4 oder 6 taucht immer die 2 auf und es gibt in R kein Element der Norm 2, also sind 2 und $1 + \sqrt{5}$ irreduzibel. Ausserdem sind 2 und $1 + \sqrt{5}$ nicht assoziiert, da sie unterschiedliche Normen haben.

- (b) In faktoriellen Ringen sind Faktorisierungen in irreduzible Elemente eindeutig. In R gilt: $6 = 2 \cdot 3 = (1 + \sqrt{5}) \cdot (1 - \sqrt{5})$. 2 und $1 + \sqrt{5}$

sind nach (a) irreduzibel und nicht assoziiert. Die 3 und $1-\sqrt{5}$ sind mit den Normen 9 und 6 auch irreduzibel (es gibt kein Elemant der Norm 3 in R) und auch zu einander nicht assoziiert, da $R^* = \{\pm 1\}$ ist. (Wegen $Nm(a+b\sqrt{5}) = a^2 + 5 \cdot b^2$, sind ± 1 die einzigen Elemente, die Norm 1 haben).

Aufgabe VII.2

a) $\Leftarrow$: Ist klar, weil $(a) = Ra$ und R Integritätsbereich

$\Rightarrow$: $\mathfrak{A}$ ist frei, deswegen ist $\mathfrak{A} = \oplus Ra_i$, wobei $Ra_i \cap Ra_j = 0$ falls $i \neq j$. Da $\mathfrak{A}$ ein Ideal ist, d.h. $\mathfrak{A} = \oplus Ra_i \subseteq R$, sind die $a_i \in R$. Da jedoch dann immer $Ra_iaj \subset (Ra_i \cap Ra_j)$ gilt, muss $\mathfrak{A}$ ein Hauptideal sein.

b) Das Ideal aus Aufgabe $VI.3$ erfüllt zum Beispiel die genannten Eigenschaften.

Aufgabe VII.3

Folgende Operationen dürfen wir auf die Matrix anwenden:

1. Ein Ganzzahliges Vielfaches einer Zeile zu einer anderen addieren oder ein ganzzahliges Vielfaches einer Spalte zu einer anderen addieren.
2. zwei Zeilen oder zwei Spalten vertauschen
3. eine Zeile oder eine Spalte mit ± 1 multiplizieren.

Mit Hilfe dieser Operation versucht man möglichst kleine Einträge in der linken oberen Ecke u bekommen.

$$\begin{pmatrix} 2 & 6 & 8 \\ 3 & 1 & 2 \\ 9 & 5 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 & 2 \\ 6 & 2 & 8 \\ 5 & 9 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 & 2 \\ 0 & -16 & -4 \\ 0 & -6 & -6 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -12 & 4 \\ 0 & 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -12 & 20 \\ 0 & 0 & -6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -12 & 2 \\ 0 & 0 & -6 \end{pmatrix} \rightsquigarrow$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -12 \\ 0 & -6 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 36 \end{pmatrix}$$

Um sich zu vergewissern, dass man richtig gerechnet hat. Kann man sein Ergebnis z.B. mit dem Computeralgebraprogramm GAP nachrechnen.

mat:= [[2,6,8],[3,1,2],[9,5,4]] ElementaryDivisorsMat(mat);

Den detailierten Algorithmus findet man in "Algebra", von M. Artin in Kapitel 12.4. Dort findet man auch ein Beispiel.

Die andere Aufgabe geht analog

VIII.2

- (a) Die restlichen Polynome vom Grad 2 in $\mathbb{F}_2$ sind:

$$X^2 = X \cdot X$$

$$X^2 + 1 = (X+1)(X+1)$$

$$X^2 + X = X(X+1)$$

  Wie gesehen, sind sie alle reduzibel. Da für $f(X) = X^2 + X + 1$ $f(0) = f(1) = 1$ ist, ist f irreduzibel über $\mathbb{F}_2$.

- (b) Das Polynom ist irreduzibel nach dem Kriterium von Eisenstein: 3 teilt 3, 144, -6, 3, doch 9 teilt nicht 3^2.

- (c) $X^m + 1$ ist irred. g.d.w. $(X+1)^m + 1$ irred. ist.

$$\begin{aligned}(X+1)2^n + 1 &= ((X+1)^2)^{2^{n-1}} + 1 \\ &= ((X^2+2X+1)^2)^{2^{n-2}} + 1 \\ &= (X^4 + 4X^3 + 6X^2 + 4X + 1)^{2^{n-2}} + 1 \\ &= \cdots\end{aligned}$$

  Man sieht, dass das Polynom bis auf den Leitkoeffizient nur gerade Koeffeffizienten hat und der letzte mit 2 der kleinste ist. Somit ist das Polynom nach Eisenstein (mit 2) irreduzibel.

- (d) Wir zeigen, dass das Polynom über $\mathbb{Z}[X]$ irred. ist. Nach den Satz von Gauß ist es dann auch über $\mathbb{Q}[X]$ irred.

  Falls $f(X) = g(X) \cdot h(X)$ ist, dann erfüllen g und h die drei Bedingungen:

  - $g(-17) = h(-17) = \pm 1$

- $g(-5) = h(-5) = \pm 1$
- g und h sind normiert.

Damit sind die Polynome eindeutig bestimmt und es gilt $g = h$. Also ist $f(X) = (g(X))^2$ und $f(a)$ ist für alle $a \in \mathbb{Z}$ ein Quadrat. Nun ist aber $f(-6) = 11^2 \cdot 1^2 + 1 = 122$, was kein Quadrat in $\mathbb{Z}$ ist. Also lässt sich $f(X)$ nicht zerlegen.

VIII.3

Angenommen, es gäbe nur endlich viele prime Hauptideale, die von $q, p_1, ..., p_n$ erzeugt werden. Betrachte dann $r := q \cdot p_1 \cdot ... \cdot p_n + 1$. Nach Voraussetzung ist r keine Einheit und nicht Null, da $r \equiv 1(q)$. Das Elemant r lässt sich aber nicht zerlegen und ist auch keines der schon bekannten Primelemente, da für alle Primelemente p_i gilt: $r \equiv 1(p_i)$. Also ist r irreduzibel und da R ein faktorieller Ring ist r auch prim. Dies ist ein Widerspruch zur Annahme!

Aufgabe IX.1

Aufgabe a)

b) ist Minimalpolynom für a) und ist separabel.

Aufgabe b)

Ansatz

$$X = \sqrt{2} + \sqrt{-23}$$
$$X^2 = 2 + 2\sqrt{-46} - 23$$
$$(X^2 + 21)^2 = -4 \cdot 46$$
$$= X^4 + 42X^2 + 257$$

Weil 257 Primenzahl ist, kann man das Eisenstein-Kriterum anwenden, und damit ist obengenanntes Polynom irreduzibel. Es hat offensichtlich die gewünschte Nullstelle und ist normiert, ist also das Minimalpolynom.

Aufgabe IX.4

a) $3^{2/9} = \sqrt[9]{3^2}$ ist ganz. Summe ganzer Zahlen ist ganz. b) $23X^2 - 1$ ist nicht normiert, also $\frac{1}{\sqrt{23}}$ nicht ganz. c) Der Nenner ist ist eine Einheit, der Zähler ist offensichtlich ganz (die Norm ist 1). Also ist der Bruch ganz. d) Nach der Eulerformel ist $\cos x = 1/2(e^{ix} + e^{-ix})$. Die Zahl beschreibt also eine Einheitswurzel.

X.1

- 1. Über $\mathbb{Q}$ ist das Polynom irreduzibel. Die Nullstellen über $\mathbb{C}$ sind $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. D.h. das Polynom zerfällt erst über $\mathbb{Q}(\sqrt[4]{2}, i)$.

- 2. Über $\mathbb{F}_3$ ist

  $$X^4 - 2 \equiv (X^2 + 2X + 2)(X^2 + X + 2) \equiv ((X+1)^2 + 1)((X-1)^2 + 1)$$
  $$\equiv ((X+1) - \alpha)((X+1) + \alpha)((X-1) - \alpha)((X-1) + \alpha),$$

  wobei $\alpha^2 = -1$. Also zerfällt das Polynom über $\mathbb{F}_3(\alpha)$.

  Man braucht nur ein Element vom Grad 2 zu adjungieren, da $-1 \equiv 2\ (3)$ und $(1+\alpha)^4 \equiv -1\ (3)$ ist.

- 3. Über $\mathbb{F}_5$ ist das Polynom irreduzibel. Doch mit α, so dass $\alpha^4 = -2$ ist, gilt

  $$X^4 - 2 = (X + \alpha)(X + 2\alpha)(X + 3\alpha)(x + 4\alpha).$$

  Also zerfällt das Polynom über $\mathbb{F}_5(\alpha)$.

  Man benötigt nur die $\sqrt[4]{2}$, da in $\mathbb{F}_5$ gilt: $3^2 \equiv -1\ (5)$.

X.2

Da t in $\mathbb{F}_3(t)$ irreduzibel, d.h. auch Prim ist, ist $f(X)$ nach Eisenstein irreduzibel. Für die Nullstellen gilt: $(X - \sqrt[3]{t})^3 = X^3 - 3 \cdot X^2 \sqrt[3]{t} + 3 \cdot X(\sqrt[3]{t})^2 - t = X^3 - t$.

X.3

- (a) Das primitive Element ist $\sqrt[6]{2}$, da wegen $\sqrt[3]{2} = (\sqrt[6]{2})^2$ und $\sqrt{2} = (\sqrt[6]{2})^3$ die Inklusion $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$ gilt und wegen $\frac{\sqrt{2}}{\sqrt[3]{2}} = \sqrt[6]{2}$ ist auch $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

- (b) Siehe (a).

XI.3

Das Polynom ist nach Eisenstein irreduzibel. Das Polynom ist als Funktion monoton wachsend und die Diskriminante ist ungleich 0, wonach es keine mehrfachen Nullstellen hat. Es gibt nur eine Gruppe der Ordnung 3: $\mathbb{Z}/3\mathbb{Z}$

XI.4

Man bestimmt durch allgemeinen Ansatz das Minimalpolynom und stellt fest, dass die Körpererweiterung separabel ist. Die Körpererweiterung ist normal, da alle endlichen Körpererweiterungen über $\mathbb{Q}$ normal sind. Die Körperautomorphismen sind zum einen die komplexe Konjugation zum anderen durch $\{\pm id\}$ bestimmt, also ist $G(K|\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, also die Kleinsche Vierergruppe.