Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

14. Übungsblatt – Lösungsskizze

Körpererweiterungen, Polynomringe und Galoistheorie

1. Wir wissen, dass $\mathbb{Q}$ und i konstruierbar sind und dass die konstruierbaren Zahlen einen Körper bilden. Es ist also auch $\mathbb{Q}(i)$ konstruierbar. Da $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt und $\mathbb{C} = \mathbb{R}(i)$, ist auch $\mathbb{Q}(i)$ dicht in $\mathbb{C}$.

2. Seien k, l, f wie in der Aufgabe. Es ist f injektiv genau dann, wenn $\ker(f) = \{0_k\}$. Angenommen, es gilt $f(a) = 0_l$ für ein $a \in k \setminus \{0_k\}$. Weil k ein Körper ist, gibt es zu a ein Inverses mit $aa^{-1} = 1_k$. Wir haben dann wegen der Homomorphismuseigenschaft von f

$$1_l = f(1_k) = f(aa^{-1}) = f(a)f(a^{-1}) = 0_l \cdot f(a^{-1}) = 0_l$$

   Das ist natürlich ein Widerspruch, also ist f injektiv.

3. Es sind E und F Vektrorräume gleicher Dimension, also isomorph. Sei $\varphi\colon E \to F$ ein k-linearer Isomorphismus und $a \in E$. Da E endlich-dimensional über k ist, ist a algebraisch und es sei m_a, k das Minimalpolynom von a über k. Dann ist $m_{a,k}$ auch das Minimalpolynom von $\varphi(a)$, denn

$$m_{a,k}(\varphi(a)) = \sum_{i=0}^{n} \lambda_i \varphi(a)^i = \sum_{i=0}^{n} \varphi(\lambda_i)\varphi(a)^i = \varphi(\sum_{i=0}^{n} \lambda_i a^i) = \varphi(0) = 0$$

   und $m_{\varphi(a),k}$ ist durch Nullstelle, Irreduzibilität und Normiertheit eindeutig festgelegt. Nach Aufgabe P15 gibt es einen Körperisomorphismus $k(a) \to k(\varphi(a))$, der auf k die Identität ist. Falls $k(a) = E$, so sind wir fertig (aus Dimensionsgründen muss dann auch $k(\varphi(a)) = F$) gelten. Falls nicht, dann kann man obige Konstruktion induktiv fortsetzen.

4. Mit "Raten" einer Nullstelle und dem Euklidischen Algorithmus erhält man

$$p_1 = (X-1)(X+2)(X-3)$$
$$p_3 = (X-1)(X-1)(X+1)(X+1).$$

   und Es ist p_2 irreduzibel, das sieht man z. B. mit dem Eisensteinkriterium.

5. Da $\deg(p) = 3$, besitzt p mindestens eine Nullstelle in $\mathbb{R}$ und ist nach Aufgabe P9 nicht irreduzibel. Mit Satz I.3.7 folgt dann direkt die Behauptung. Über $\mathbb{Q}$ gibt es irreduzible Polynome vom Grad 3, z.B. $p(X) = X^3 - 2$. Dann ist $\mathbb{Q}[X]/p \cdot \mathbb{Q}[X]$ ein Körper, ebenfalls nach Satz I.3.7.

6. Das ist genau Aufgabe P12 mit $k = \mathbb{Q}$ und $a = \sqrt{3}$.

7. Es gilt $\mathrm{NS}(p) = \{a, \xi_3 a, \xi_3^2 a\}$ mit $a = \sqrt[3]{2}$ und $\xi_3 = e^{\frac{2\pi i}{3}}$. Das $\mathrm{Gal}_{\mathbb{Q}}(p) = S_3$ ist folgt dann aus Satz III.1.8. Man sieht hier aber noch etwas genauer, was hinter Satz III.1.8 steckt: Die komplexe

Konjugation liefert ein Element $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(p)$. Da $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(a, \xi_3)$, $[\mathbb{Q}(a, \xi_3) : \mathbb{Q}(a)] = 3$ und $[\mathbb{Q}(a) : \mathbb{Q}] = 2$ folgt

$$|\operatorname{Gal}_{\mathbb{Q}}(p)| = [\mathbb{Q}(a, \xi_3) : \mathbb{Q}] = 6.$$

Also muss $\mathrm{Gal}_{\mathbb{Q}}(p)$ ein Element τ der Ordnung 3 enthalten (nach dem Staz von Lagrange). Damit gilt $\tau = (123)$ (in Zykelschreibweise für eine geeignete Nummerierung) oder $\tau = (132)$. Da das Produkt $\sigma\tau$ Ordnung 6 hat muss (nach Aufgabe P20) haben wir also alle 6 Permutationen in $\mathrm{Gal}_{\mathbb{Q}}(p)$. Damit muss $\mathrm{Gal}_{\mathbb{Q}}(p) = S_3$ gelten.

Gruppen

1. Dreimalige Komposition von α mit sich selbst ergibt:

$$\begin{aligned}
1 &\longmapsto 2 \longmapsto 3 \longmapsto 4 \longmapsto 1,\\
2 &\longmapsto 3 \longmapsto 4 \longmapsto 1 \longmapsto 2,\\
3 &\longmapsto 4 \longmapsto 1 \longmapsto 2 \longmapsto 3,\\
4 &\longmapsto 1 \longmapsto 2 \longmapsto 3 \longmapsto 4.
\end{aligned}$$

Hieraus lesen wir ab, dass $\alpha^2 = (1\ 3)(2\ 4)$, $\alpha^3 = (1\ 4\ 3\ 2)$ und $\alpha^4 = \mathrm{Id}$ gilt. Somit ist $\alpha^n \neq \mathrm{Id}$ für $1 \leq n \leq 3$, aber $\alpha^4 = \mathrm{Id}$ und somit $\mathrm{ord}(\alpha) = 4$. Eine Komposition von β mit sich selbst ergibt:

$$\begin{aligned}
1 &\longmapsto 1 \longmapsto 1,\\
2 &\longmapsto 4 \longmapsto 2,\\
3 &\longmapsto 3 \longmapsto 3,\\
4 &\longmapsto 2 \longmapsto 4.
\end{aligned}$$

Hieraus lesen wir ab, dass $\beta^2 = \mathrm{Id}$ und somit $\mathrm{ord}(\beta) = 2$ gilt. Schlussendlich berechnen wir $\alpha\beta$ mittels des folgenden Diagramms (in welchem zuerst β und dann α auf $\{1, 2, 3, 4\}$ wirkt):

$$\begin{aligned}
1 &\longmapsto 1 \longmapsto 2,\\
2 &\longmapsto 4 \longmapsto 1,\\
3 &\longmapsto 3 \longmapsto 4,\\
4 &\longmapsto 2 \longmapsto 3.
\end{aligned}$$

Außerdem berechnen wir $\beta\alpha^{-1} = \beta\alpha^3$ mittels des folgenden Diagramms (in welchem zuerst α^3 und dann β auf $\{1, 2, 3, 4\}$ wirkt):

$$\begin{aligned}
1 &\longmapsto 4 \longmapsto 2,\\
2 &\longmapsto 1 \longmapsto 1,\\
3 &\longmapsto 2 \longmapsto 4,\\
4 &\longmapsto 3 \longmapsto 3.
\end{aligned}$$

Es ergibt sich also insgesamt, dass $\alpha\beta = (1\ 2)(3\ 4) = \beta\alpha^3 = \beta\alpha^{-1}$ gilt.

2. Es enthält X das neutrale Element $\mathrm{id} = \beta^0\alpha^0$. Aus $\alpha\beta = \beta\alpha^{-1}$ folgt induktiv

$$\alpha^n\beta = \beta\alpha^{-n}.$$

Bezeichnet $r(z)$ den Rest einer ganzen Zahl r beim Teilen durch 4, so gilt

$$\beta^m\alpha^n\beta^{m'}\alpha^{n'} = \begin{cases} \alpha^{r(n+n')} & \text{falls } m = m = 0 \\ \beta\alpha^{r(n'-n)} & \text{falls } m = 0, m' = 1 \\ \beta\alpha^{r(n+n')} & \text{falls } m' = 0.m = 1 \\ \alpha^{r(n'-n)} & \text{falls } m' = m = 1 \end{cases}.$$

Damit ist das Produkt zweier Elemente von X wieder ein Element von X, also X abgeschlossen unter Multiplikation. Aus dem letzten Fall folgt auch $(\beta\alpha^n)^{-1} = \beta\alpha^{-n} \in X$ und $(\alpha^n)^{-1} = \alpha^{r(-n)} \in X$ gilt sowieso. Also ist X auch abgeschlossen unter dem Bilden von Inversen. Damit ist X eine Untergruppe.

3. Aus X Untergruppe und $\alpha, \beta \in X$ folgt $G \subseteq X$ und aus $\mathrm{ord}(\alpha) = 4$ und $\mathrm{ord}(\beta) = 2$ folgt

$$X = \{\beta^m\alpha^n \mid 0 \leq n \leq 3 \,\text{und}\, 0 \leq m \leq 1\} \subseteq G.$$

Insgesamt also $G = X$. Nun nehmen wir n, m, n', m' mit $0 \leq n, n' \leq 3$ und $0 \leq m, m' \leq 1$, sodass $\beta^{m'}\alpha^{n'} = \beta^m\alpha^n$. Dann gilt:

$$\begin{aligned} \mathrm{Id} &= (\beta^{m'}\alpha^{n'})(\beta^m\alpha^n)^{-1} = \beta^{m'}\alpha^{n'-n}\beta^{-m} = \beta^{m'}(\beta^m\alpha^{n-n'})^{-1} \\ &= \beta^{m'}(\alpha^{(-1)^m\cdot(n-n')}\beta^m)^{-1} = \beta^{m'-m}\alpha^{(-1)^m\cdot(n'-n)}. \end{aligned}$$

Also gilt $\beta^{m-m'} = \alpha^{(-1)^m\cdot(n'-n)}$. Aus der Rechnung in Aufgabenteil 1 sehen wir nun, dass diese Gleichung nur erfüllt sein kann, wenn $m' - m = 0$ und $n' - n = 0$ gelten, d.h. wenn $m' = m$ und $n' = n$. Daraus wiederum folgt, dass für alle n, m, n', m' mit $0 \leq n, n' \leq 3$ und $0 \leq m, m' \leq 1$ und $n \neq n'$ und $m \neq m'$ gilt, dass $\beta^m\alpha^n \neq \beta^{m'}\alpha^{n'}$. Somit erhalten wir, dass

$$|G| = |\{\beta^m\alpha^n \mid 0 \leq n \leq 3 \,\text{und}\, 0 \leq m \leq 1\}| = 8.$$

4. Die Gruppe G ist nicht abelsch. Wie in Aufgabenteil 3 bewiesen wurde, gilt etwa $\alpha^3\beta \neq \alpha\beta$ und somit

$$\alpha\beta \neq \alpha^3\beta = \beta\alpha^{-3} = \beta\alpha.$$

5. G ist nicht normal. Z. B. gilt $(12)\beta(12) = (14)$, und diese Permutation ist nicht in G enthalten.

6. Es ist $\beta^m\alpha^n \in Z(G)$ für $0 \leq m \leq 1$ und $0 \leq n \leq 3$ genau dann, wenn für alle m', n' mit $0 \leq m' \leq 1$ und $0 \leq n' \leq 3$ gilt, dass

$$\beta^{m+m'} \cdot \alpha^{(-1)^{m'}\cdot n+n'} = (\beta^m\alpha^n)(\beta^{m'}\alpha^{n'}) = (\beta^{m'}\alpha^{n'})(\beta^m\alpha^n) = \beta^{m+m'} \cdot \alpha^{(-1)^m\cdot n'+n}$$

Dies wiederum ist genau dann der Fall, wenn für alle m', n' wie oben gilt, dass

$$(-1)^{m'} \cdot n + n' \equiv (-1)^m \cdot n' + n \pmod 4,$$

was äquivalent ist zu

$$((-1)^{m'} - 1)n \equiv ((-1)^m - 1)n' \pmod 4.$$

Wenn $m = 1$ ist, kann obige Bedingung nicht erfüllt sein. In diesem Falle lautet sie, dass für alle m', n' mit $0 \leq m' \leq 1$ und $0 \leq n' \leq 3$ gilt, dass

$$((-1)^{m'} - 1)n \equiv 2n' \pmod 4.$$

Um dies zu wiederlegen, wählen wir $m' = 1$ und $n' = n + 1$. Dann gilt:

$$((-1)^{m'} - 1)n \equiv 2n \not\equiv 2(n+1) \equiv 2n' \pmod 4.$$

Somit ist $\beta^m \alpha^n \notin Z(G)$, wenn $m = 1$ ist. Es bleibt nun, zu bestimmen, für welche n mit $0 \leq n \leq 3$ es gilt, dass $\alpha^n \in Z(G)$. Zunächst bemerken wir, dass $\alpha \notin Z(G)$, wie wir bereits in der Lösung zu Aufgabenteil 3 gezeigt haben. Mit einem analogen Argument zeigt man, dass $\alpha^3 \notin Z(G)$. Andererseits ist es klar, dass $\mathrm{Id} \in Z(G)$. Weiterhin ist $\alpha^2 \in Z(G)$, da für alle m', n' mit $0 \leq m' \leq 1$ und $0 \leq n' \leq 3$ gilt, dass

$$\alpha^2(\beta^{m'}\alpha^{n'}) = \beta^{m'}\alpha^{2\cdot(-1)^{m'}}\alpha^{n'} = \beta^{m'}\alpha^2\alpha^{n'} = \beta^{m'}\alpha^{2+n'} = (\beta^{m'}\alpha^{n'})\alpha^2,$$

wobei wir verwendet haben, dass $\alpha^{-2} = \alpha^2$ gilt, da $\mathrm{ord}(\alpha) = 4$ ist. Insgesamt erhalten wir also, dass $Z(G) = \{\mathrm{Id}, \alpha^2\} = \langle\alpha^2\rangle$.

7. Für n, n' mit $0 \leq n, n' \leq 3$ rechnen wir direkt nach, dass

$$\begin{aligned}
[\alpha^n, \alpha^{n'}] &= \mathrm{Id}, \\
[\alpha^n, \beta\alpha^{n'}] &= \alpha^n\beta\alpha^{n'}\alpha^{-n}\alpha^{-n'}\beta^{-1} = \alpha^{n-n'+n+n'}\beta\beta^{-1} = \alpha^{2n}, \\
[\beta\alpha^n, \alpha^{n'}] &= ([\alpha^{n'}, \beta\alpha^n])^{-1} = \alpha^{2n'}, \\
[\beta\alpha^n, \beta\alpha^{n'}] &= \beta\alpha^n\beta\alpha^{n'}\alpha^{-n}\beta^{-1}\alpha^{-n'}\beta^{-1} = \alpha^{-n}\beta\beta\alpha^{n'}\alpha^{-n}\beta^{-1}\beta^{-1}\alpha^{n'} = \alpha^{2(n'-n)}
\end{aligned}$$

gilt. Somit erhalten wir, dass $G' = \langle\alpha^2\rangle = \{\mathrm{Id}, \alpha^2\} = Z(G)$.

8. Die Gruppe $G' = \langle\alpha^2\rangle$ ist abelsch und somit gilt, dass $G^{(2)} = \{\mathrm{Id}\}$. Daraus folgt, dass G auflösbar ist. Alternativ argumentiert man, dass S_4 auflösbar ist und somit auch G als Untergruppe von S_4.