

Lösungsvorschlag zur Aufgabe 1: (a) w, (b) f, (c) f, (d) w, (e) w, (f) f, (g) w, (h) w, (i) f, (j) w

Lösungsvorschlag zur Aufgabe 2: Zu (a). Seien $x_1, x_2 \in X$ mit $Gx_1 = Gx_2$. Dann gilt $x_1 \in Gx_2$, also gibt es $g \in G$ mit $x_1 = gx_2$. Bezeichne H_i die Standgruppe von x_i ($i \in \{1, 2\}$). Wir behaupten, $H_1 = gH_2g^{-1}$.

Wir zeigen zunächst $H_1 \subseteq gH_2g^{-1}$. Sei hierzu $h \in H_1$. Wegen $h = g(g^{-1}hg)g^{-1}$, reicht es $g^{-1}hg \in H_2$ zu zeigen. Nach Definition von H_2 , ist hierzu $(g^{-1}hg)x_2 = x_2$ zu zeigen. Nun gilt aber

$$\begin{aligned}(g^{-1}hg)x_2 &= (g^{-1}h)(gx_2) = (g^{-1}h)x_1 = g^{-1}(hx_1) \\ &= g^{-1}x_1 = g^{-1}(gx_2) = (g^{-1}g)x_2 = 1x_2 = x_2.\end{aligned}$$

Nun zeigen wir $gH_2g^{-1} \subseteq H_1$. Dazu sei $h \in H_2$ und wir zeigen $ghg^{-1} \in H_1$. Nach Definition von H_1 ist hierzu $(ghg^{-1})x_1 = x_1$ zu zeigen. Tatsächlich gilt

$$(ghg^{-1})x_1 = (gh)(g^{-1}x_1) = (gh)x_2 = g(hx_2) = gx_2 = x_1.$$

Zu (b). Ist G irgendeine Gruppe und X irgendeine Menge, so ist

$$G \times X \rightarrow X, (g, x) \mapsto x$$

eine Gruppenwirkung von G auf X mit lauter einelementigen Bahnen. Die Standgruppen sind dann alle gleich G , also insbesondere immer konjugiert zueinander. Wenn X mehr als ein Element enthält, erhalten wir ein Beispiel, welches zeigt, daß die Umkehrung im Allgemeinen nicht gilt.

Lösungsvorschlag zur Aufgabe 3: Zu (a) und (b). Diese Polynome sind primitiv und daher nach dem Kriterium von Eisenstein (angewandt mit der Primzahl 3) irreduzibel in $\mathbb{Z}[X]$.

Zu (c). Dieses Polynom läßt sich in $\mathbb{Z}[X]$ als das Produkt

$$2(X^4 + 2X^3 - 27X^2 + 9X + 3)$$

der beiden Nichteinheiten 2 und $X^4 + 2X^3 - 27X^2 + 9X + 3$ schreiben und ist daher reduzibel in $\mathbb{Z}[X]$.

Zu (d) und (e). Für jedes $a \in \mathbb{Z}$ ist

$$\mathbb{Z}[X] \rightarrow \mathbb{Z}[X], p \mapsto p(X + a)$$

ein Automorphismus des Ringes $\mathbb{Z}[X]$, denn diese Abbildung ist ein (Einsetzungs-)Homomorphismus und besitzt die Umkehrabbildung

$$\mathbb{Z}[X] \rightarrow \mathbb{Z}[X], p \mapsto p(X - a),$$

die ebenfalls ein Ringhomomorphismus ist. Daher ist für jedes $p \in \mathbb{Z}[X]$ und $a \in \mathbb{Z}$ das Polynom p irreduzibel in $\mathbb{Z}[X]$ genau dann, wenn

$p(X + a)$ irreduzibel in $\mathbb{Z}[X]$ ist. Mit (a) und $a = 1$, $a = 2$ erhält man also, daß die Polynome aus (d) und (e) auch irreduzibel sind.

Lösungsvorschlag zur Aufgabe 4: Die Behauptung ist äquivalent zu

$$(I \not\subseteq \mathfrak{p} \text{ und } J \not\subseteq \mathfrak{p}) \implies IJ \not\subseteq \mathfrak{p}$$

und damit trivial, denn wenn $x \in I \setminus \mathfrak{p}$ und $y \in J \setminus \mathfrak{p}$, so ist $xy \in IJ \setminus \mathfrak{p}$ (wäre $xy \in \mathfrak{p}$, so folgte $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$).

Lösungsvorschlag zur Aufgabe 5: Zu (a). Da

$$\sqrt{(-3)^2 - 4 \cdot 2} = \sqrt{1} = 1 \in \mathbb{Q},$$

hat das Polynom nach der Lösungsformel für quadratische Gleichungen nur rationale Nullstellen, weshalb der Zerfällungskörper gleich \mathbb{Q} ist und damit den Grad 1 über \mathbb{Q} hat.

Zu (b). Da

$$\sqrt{(-2)^2 - 4(-2)} = \sqrt{4 + 8} = \sqrt{12} = 2\sqrt{3},$$

ist der Zerfällungskörper nach der Lösungsformel für quadratische Gleichungen gleich $\mathbb{Q}(\sqrt{3})$ und hat den Grad 2 über \mathbb{Q} .

Zu (c). Es gilt $X^4 + 2X^2 + 1 = (X^2 + 1)^2 = (X + i)^2(X - i)^2$, weshalb der Zerfällungskörper gleich $\mathbb{Q}(i)$ ist und den Grad 2 über \mathbb{Q} hat.

Lösungsvorschlag zur Aufgabe 6: Zu (a). Es gilt

$$(1 + 1)^2 = 1 + 1 + 1 + 1 = 0$$

in K , da die Ordnung von 1 in der additiven Gruppe ein Teiler der Gruppenordnung (nämlich 4) sein muß. Da K ein Körper ist, folgt daraus $1 + 1 = 0$.

Zu (b). Sei $x \in K$ mit $x^2 = 1$. Dann gilt

$$(x - 1)^2 = (x - 1)(x + 1) = x^2 - 1 = 0$$

wegen $-1 = 1$, was sofort aus (a) folgt. Also $x - 1 = 0$ und somit $x = 1$.

Zu (c).

$+$	0	1	a	b	\cdot	0	1	a	b
0	0	1	a	b	0	0	0	0	0
1	1	0	b	a	1	0	1	a	b
a	a	b	0	1	a	0	a	b	1
b	b	a	1	0	b	0	b	1	a

Lösungsvorschlag zur Aufgabe 7: Sei \leq ein Anordnung des Körpers K und $a \in K$. Gilt $a \geq 0$, so gilt nach der Monotonie der Multiplikation $a^2 = aa \geq 0$. Gilt $a \leq 0$, so gilt nach der Monotonie der Addition $0 = a - a \leq -a$ und daher nach dem gerade gezeigten wieder $a^2 = (-a)^2 \geq 0$. Da die Ordnung total ist, gilt in jedem Fall $a^2 \geq 0$.

Zu (a). Wäre \leq eine Anordnung von $\mathbb{Q}(i)$, so folgte demnach $0 \leq i^2 = -1$, also $1 \leq -1 + 1 = 0 \leq 1^2 = 1$ und somit $0 = 1$, was absurd ist.

Mit den Quadraten sind wegen der Monotonie der Addition auch beliebige Quadratsummen in K nichtnegativ.

Zu (b). Wäre \leq eine Anordnung von $\mathbb{Q}(X)(\sqrt{-(1+X^2)})$, so folgte $0 \leq X^2 + (\sqrt{-(1+X^2)})^2 = X^2 - (1+X^2) = -1$, also wieder

$$1 \leq -1 + 1 = 0 \leq 1^2 = 1$$

und somit $0 = 1$, was absurd ist.

Lösungsvorschlag zur Aufgabe 8: Der Körper L entsteht aus K durch n -maliges Adjungieren einer Wurzel. Bei jedem Adjungieren einer Wurzel kann der Körpergrad nach der Gradformel sich entweder verdoppeln oder gleichbleiben. Die Voraussetzung $[L : K] = 2^n$ besagt gerade, daß sich der Grad jeweils in jedem Schritt verdoppelt hat. Das wäre natürlich nicht so, wenn $\sqrt{a_1}, \dots, \sqrt{a_n}$ linear abhängig wären über K . Also sind $\sqrt{a_1}, \dots, \sqrt{a_n}$ linear unabhängig über K , insbesondere $\neq 0$.

Zu (a). $L|K$ ist Zerfällungskörper des Polynoms $\prod_{i=1}^n (X^2 - a_i)$. Dieses Polynom ist separabel, da $X^2 - a_i = (X - \sqrt{a_i})(X + \sqrt{a_i})$ und

$$\sqrt{a_i} = -\sqrt{a_i}$$

$1 = -1$ implizieren würde im Widerspruch zur Voraussetzung $2 \neq 0$.

Zu (b). Sei $\sigma \in \text{Gal}(L|K(x))$. Da σ für jedes $i \in \{1, \dots, n\}$ die Nullstellen von $X^2 - a_i \in K[X]$ permutiert, gibt es $\delta_1, \dots, \delta_n \in \{-1, 1\}$ mit $\sigma(a_i) = \delta_i \sqrt{a_i}$ für jedes $i \in \{1, \dots, n\}$. Dann gilt

$$\sum_{i=1}^n \sqrt{a_i} = x = \sigma(x) = \sum_{i=1}^n \delta_i \sqrt{a_i}.$$

Wegen der linearen Unabhängigkeit von $\sqrt{a_1}, \dots, \sqrt{a_n}$ über K folgt $\delta_i = 1$ und somit $\sigma(a_i) = \sqrt{a_i}$ für alle $i \in \{1, \dots, n\}$. Wegen

$$L = K(\sqrt{a_1}, \dots, \sqrt{a_n})$$

folgt $\sigma = \text{id}_L$.

Zu (c). Es gilt nach (b)

$$\text{Gal}(L|K(x)) = \{\text{id}_L\} = \text{Gal}(L|L)$$

und somit nach dem Hauptsatz der Galoistheorie $K(x) = L$.