WS 05/06
Priv.-Doz. Dr. S. Wewers
Andreas Martin

Algebra I

12. Übungsblatt

Aufgabe 1: ($6 \cdot 1$ P) Sei $\zeta = \zeta_7 = \exp(2\pi i/7)$ und $K := \mathbb{Q}[\zeta]$. Wir nehmen an, dass $K/\mathbb{Q}$ eine Galois-Erweiterung ist und dass es einen Gruppenisomorphismus

$$(\mathbb{Z}/7)^\times \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}), \quad a \mapsto \sigma_a$$

gibt, der bestimmt ist durch die Gleichung $\sigma_a(\zeta) = \zeta^a$.

(a) Bestimmen Sie alle Untergruppen von $(\mathbb{Z}/7)^\times$.

(b) Sei $\alpha := \zeta + \zeta^{-1} \in K$. Bestimmen Sie alle Elemente $a \in (\mathbb{Z}/7)^\times$ mit $\sigma_a(\alpha) = \alpha$.

(c) Sei
$$\beta := \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6 \in K.$$
Bestimmen Sie alle Elemente $a \in (\mathbb{Z}/7)^\times$ mit $\sigma_a(\beta) = \beta$.

(d) Zeigen Sie: $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, $[\mathbb{Q}[\beta] : \mathbb{Q}] = 2$ und $K = \mathbb{Q}[\alpha, \beta]$. (Hinweis: benutzen Sie den Hauptsatz der Galoistheorie.)

(e) Bestimmen Sie die Minimalpolynome über $\mathbb{Q}$ von α und β. (Hinweis: vergleiche mit Aufgabe 3 (a) vom 10. Blatt.)

(f) Ist $\mathbb{Q}[\alpha]/\mathbb{Q}$ eine Galois-Erweiterung? Wenn ja, bestimmen Sie ihre Galois-Gruppe.

Lösung: Wir bezeichnen den angegbenen Isomorphismus durch

$$\sigma : (\mathbb{Z}/7\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}),\ a \mapsto \sigma_a\ .$$

(a) Die Gruppe ist zyklisch, also sind auch alle ihre Untergruppen zyklisch. Diese sind
$$\begin{array}{lcl} \langle 1\rangle & = & \{1\}\ , \\ \langle 2\rangle = \langle 4\rangle & = & \{1,2,4\}\ , \\ \langle 6\rangle & = & \{1,-1\}\ , \\ \langle 3\rangle = \langle 5\rangle & = & (\mathbb{Z}/7\mathbb{Z})^\times\ . \end{array}$$

(b) Wegen $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(7) = 6$ sind die Elemente $1, \zeta, \ldots, \zeta^6$ linear unabhängig über $\mathbb{Q}$. Ferner gilt $\sigma_a(\alpha) = \zeta^a + \zeta^{-a} = \zeta^a + \zeta^{7-a}$. Also gilt für $a \in \{1, \ldots, 6\}$

$$\sigma_a(\alpha) \ = \ \alpha \iff \zeta^a + \zeta^{7-a} \ = \ \zeta + \zeta^{-1} \iff a \in \{1, 6\}\ .$$

Mit anderen Worten, es ist

$$\mathrm{Gal}(K/\mathbb{Q}[\alpha]) \ = \ \{\sigma_1, \sigma_6\}\ .$$

(c) Es gilt

$$\{\tau \in \mathrm{Gal}(K/\mathbb{Q}) |\, \tau(\beta) = \beta\} \;=\; \mathrm{Gal}(K/\mathbb{Q}[\beta]) \;\leq\; \mathrm{Gal}(K/\mathbb{Q}) \;,$$

und

$$H \;:=\; \{a \in (\mathbb{Z}/7\mathbb{Z})^\times |\, \sigma_a(\beta) = \beta\} \;=\; \sigma^{-1}(\mathrm{Gal}(K/\mathbb{Q}[\beta])) \;\leq\; (\mathbb{Z}/7\mathbb{Z})^\times \;.$$

Nun ist

$$\begin{array}{rcl} \sigma_2(\beta) &=& \zeta^2+\zeta^4-\zeta^6+\zeta-\zeta^3-\zeta^5 \quad = \quad \beta \;, \\ \sigma_3(\beta) &=& \zeta^3+\zeta^6-\zeta^2+\zeta^5-\zeta-\zeta^4 \quad \neq \quad \beta \;. \end{array}$$

Also gilt $2 \in H$ und $3 \notin H$. Wegen $H \leq (\mathbb{Z}/7\mathbb{Z})^\times$ folgt mit Teil (a) daher

$$H \;=\; \{1, 2, 4\} \;.$$

(d) K ist galoissch über $\mathbb{Q}[\alpha]$ und $\mathbb{Q}[\beta]$, daraus folgt

$$[K : \mathbb{Q}[\alpha]] \;=\; |\,\mathrm{Gal}(K/\mathbb{Q}[\alpha])| \;=\; 2 \;,\;\; [K : \mathbb{Q}[\beta]] \;=\; |\,\mathrm{Gal}(K/\mathbb{Q}[\beta])| \;=\; 3 \;.$$

Wegen $[K : \mathbb{Q}] = 6$ folgt aus dem Gradsatz, daß

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] \;=\; 3 \;,\;\; [\mathbb{Q}[\beta] : \mathbb{Q}] \;=\; 2 \;.$$

Daher ist nach dem Gradsatz $[\mathbb{Q}[\alpha, \beta] : \mathbb{Q}]$ ein Vielfaches von 2 und von 3, also auch von 6. Aus $\mathbb{Q}[\alpha, \beta] \subseteq K$ und $[K : \mathbb{Q}] = 6$ folgt demnach $K = \mathbb{Q}[\alpha, \beta]$.

(e) Es wird

$$\begin{array}{lcl} \alpha^2 &=& \zeta^2+\zeta^{-2}+2 \;, \\ \zeta^3+\zeta^{-3} &=& \zeta^3+\zeta^4 \;=\; -1-\zeta-\zeta^2-\zeta^5-\zeta^6 \\ &=& -1-\zeta-\zeta^{-1}-\zeta^2-\zeta^{-2} \\ &=& -\alpha^2-\alpha+1 \;, \\ \alpha^3 &=& \zeta^3+3\zeta+3\zeta^{-1}+\zeta^{-3} \\ &=& -\alpha^2+2\alpha+1 \;. \end{array}$$

Also ist α Nullstelle des normierten Polynoms $X^3 + X^2 - 2X - 1$. Wegen $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ folgt

$$\mathrm{minpol}_{\mathbb{Q}}(\alpha) \;=\; X^3 + X^2 - 2X - 1 \;.$$

Ferner wird

$$\begin{array}{rcl} \beta^2 &=& (\zeta+\zeta^2-\zeta^3+\zeta^4-\zeta^5-\zeta^6)^2 \\ &=& \zeta^2+\zeta^4+\zeta^6+\zeta+\zeta^3+\zeta^5+2\zeta^3-2\zeta^4+2\zeta^5-2\zeta^6-2-2\zeta^5 \\ && +2\zeta^6-2-2\zeta-2+2\zeta+2\zeta^2-2\zeta^2-2\zeta^3+2\zeta^4 \\ &=& -6+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6 \\ &=& -7 \;. \end{array}$$

Also ist β Nullstelle des normierten Polynoms $X^2 + 7$. Wegen $[\mathbb{Q}[\beta] : \mathbb{Q}] = 2$ folgt

$$\mathrm{minpol}_{\mathbb{Q}}(\beta) \;=\; X^2 + 7 \;.$$

(f) Die Gruppe $\mathrm{Gal}(K/\mathbb{Q})$ ist abelsch, da sie isomorph zu $(\mathbb{Z}/7\mathbb{Z})^\times$ ist. Es gilt also

$$\mathrm{Gal}(K/\mathbb{Q}[\alpha]) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q}) ,$$

und nach dem Hauptsatz der Galoistheorie folgt, daß $\mathbb{Q}[\alpha]$ galoissch über $\mathbb{Q}$ ist. Daraus folgt

$$|\,\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})| = [\mathbb{Q}[\alpha] : \mathbb{Q}] = 3 ,$$

d.h. es gilt

$$\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) \cong A_3 .$$

Man kann die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ sogar explizit bestimmen. Mit α sind auch noch

$$\begin{aligned} \sigma_2(\alpha) &= \zeta^2 + \zeta^{-2} &&= \alpha^2 - 2 , \\ \sigma_3(\alpha) &= \zeta^3 + \zeta^{-3} &&= -\alpha^2 - \alpha + 1 \end{aligned}$$

Nullstellen von $\mathrm{minpol}_{\mathbb{Q}}(\alpha)$. Es gilt also

$$\mathrm{minpol}_{\mathbb{Q}}(\alpha) = (X - \alpha)(X - (\alpha^2 - 2))(X - (-\alpha^2 - \alpha + 1)) ,$$

und es gibt genau 3 Automorphismen τ_0, τ_1, τ_2 von $\mathbb{Q}[\alpha]$, festgelegt durch

$$\begin{aligned} \tau_0(\alpha) &= \alpha \\ \tau_1(\alpha) &= \alpha^2 - 2 \\ \tau_2(\alpha) &= -\alpha^2 - \alpha + 1 . \end{aligned}$$

Dann gilt $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) = \{\tau_0, \tau_1, \tau_2\}$.

Aufgabe 2: (1+1+1=3 P) Die Diskriminante des Polynoms $f = X^3 + pX + q \in \mathbb{Q}[X]$ ist $D = -4p^3 - 27q^2$. Zeigen Sie:

(a) Die folgenden Bedingungen sind äquivalent:

(i) f hat drei verschiedene reelle Nullstellen.

(ii) $D > 0$.

(iii) Die Ableitung f' hat zwei reelle Nullstellen $\alpha, \beta \in \mathbb{R}$ mit $f(\alpha) > 0$ und $f(\beta) < 0$.

(b) Angenommen, f sei irreduzibel über $\mathbb{Q}$ und habe mindestens eine nichtreelle Nullstelle. Dann ist die Galoisgruppe von f isomorph zu S_3.

(c) Bestimmen Sie die Galoisgruppen von

$$X^3 + X + 1, \quad X^3 + X^2 - 2X - 1, \quad X^3 + X^2 - 2X - 3.$$

Lösung:

(a) Es sei $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ die Zerlegung von f in $\mathbb{C}[X]$. Dann gilt nach Vorlesung

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 .$$

- „(i) $\Longrightarrow$ (ii)“: Das ist klar nach obiger Darstellung von D.

- „(ii) $\Longrightarrow$ (iii)“: Es sei $y := -p/3$. Dann gilt

  $$4y^3 \;=\; -\frac{4p^3}{27} \;=\; \frac{D}{27} + q^2 \;>0\;,$$

  also $y > 0$. Die Nullstellen von $f' = 3X^2 + p$ sind $\pm\sqrt{y}$. Nun gilt

  $$f(\pm\sqrt{y}) \;=\; \pm y\sqrt{y} \pm p\sqrt{y} + q \;=\; \mp 2y\sqrt{y} + q\;.$$

  Wegen

  $$(2y\sqrt{y})^2 \;=\; 4y^3 \;=\; \frac{D}{27} + q^2 \;>\; q^2$$

  gilt $f(-\sqrt{y}) > 0$ und $f(+\sqrt{y}) < 0$.
- „(iii) $\Longrightarrow$ (i)“: Klar nach Analysis.

(b) Es sei G die Galoisgruppe von f über $\mathbb{Q}$. Nach Vorlesung gibt es einen injektiven Gruppenhomomorphismus $G \hookrightarrow S_3$, d.h. G ist isomorph zu einer Untergruppe H von S_3. Die komplexe Konjugation $z \mapsto \bar{z}$ bildet Nullstellen von f wieder auf Nullstellen von f ab, d.h. sie bildet den Zerfällungskörper von f auf sich selbst ab. Die entsprechende Nullstellenpermutation ist also eine Transposition, da die angenommene nichtreelle Nullstelle z mit $\bar{z}$ vertauscht wird. Ferner ist die Operation von G auf $\{1,2,3\}$ nach Vorlesung transitiv, d.h. H enthält mindestens ein weiteres nichttriviales Element. Daraus folgt $H = S_3$.

(c) Wir berechnen jeweils die Diskriminante. Diese ändert sich nicht, sofern X durch $X - a$ substituiert wird für ein $a \in \mathbb{Q}$.

$$\begin{array}{lcl}
D(X^3 + X + 1) & = & -31\;, \\
D(X^3 + X^2 - 2X - 1) & = & D((X-\tfrac{1}{3})^3 + (X-\tfrac{1}{3})^2 - 2(X-\tfrac{1}{3}) - 1) \\
 & = & D(X^3 - \tfrac{7}{3}X - \tfrac{7}{27}) \\
 & = & 49\;, \\
D(X^3 + X^2 - 2X - 3) & = & D(X^3 - \tfrac{7}{3}X - \tfrac{61}{27}) \\
 & = & -87\;.
\end{array}$$

Nach Teil (a) haben also $X^3 + X + 1$ und $X^3 + X^2 - 2X - 3$ je mindestens eine nichtreelle Nullstelle, und die Galoisgruppe ist nach (b) isomorph zu S_3.

Das Polynom $X^3 + X^2 - 2X - 1$ hat hingegen drei verschiedene reelle Nullstellen $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, und es gilt

$$\delta \;:=\; (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \;=\; \pm 7\;.$$

Wäre die Nullstellenpermutation $(1\;2)$ ein Element der Galoisgruppe, so würde diese die Zahl δ auf $-\delta$ abbilden; das ist jedoch unmöglich wegen $\delta \in \mathbb{Q}$. Also enthält die Galoisgruppe keine Transpositionen der Nullstellen. Andererseits wirkt sie transitiv auf der Menge $\{1,2,3\}$. Daraus folgt, daß die Galoisgruppe isomorph zu A_3 ist.

Aufgabe 3: (1+1+1+1=4 P) Beweisen oder widerlegen Sie die folgenden Aussagen.

(a) Sei G eine Gruppe, die auf der Menge $X = \{1,2,3,4\}$ treu und transitiv operiert. Dann ist G genau dann isomorph zu S_4, wenn es ein Element $x \in X$ gibt mit nichttrivialem Stabilisator, $G_x \neq \{1\}$.

(b) Jeder faktorielle Ring ist ein Hauptidealring.

(c) Sei K ein Körper, L/K eine Körpererweiterung, $f, g \in K[X]$ nichtkonstante Polynome und $\alpha \in L$ eine gemeinsame Nullstelle von f und g. Wenn f irreduzibel über K ist, dann ist f ein Teiler von g in dem Ring $K[X]$.

(d) Sei L/K eine endliche Körpererweiterung und $K \subset M \subset L$ ein Zwischenkörper. Wenn L/M und M/K Galoiserweiterungen sind, dann ist auch L/K eine Galoiserweiterung.

Lösung:

(a) Die Aussage ist i.a. falsch. Man betrachte z.B. die volle Symmetriegruppe des Quadrats
$$G \; := D_4 \; = \; \langle (1\,2), (1\,2\,3\,4) \rangle \; \leq \; S_4 \; ,$$
Jedes Element $x \in \{1, 2, 3, 4\}$ hat einen nichttrivialen Stabilisator. Es gilt z.B. $G_1 = \{\mathrm{id}, (2\,4)\}$.

(b) Die Aussage ist falsch. Z.B. ist der Ring $\mathbb{Z}[X]$ ein faktorieller Ring nach dem Satz von Gauß, aber kein Hauptidealring. Denn das Ideal (X) ist Primideal, aber kein maximales Ideal, da $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ kein Körper ist.

(Allgemein gilt für einen Integritätsbereich R, daß $R[X]$ genau dann ein Hauptidealring ist, wenn R ein Körper ist. Dies folgt aus $R[X]/(X) \cong R$ und der Tatsache, daß in einem Hauptidealring das irreduzible Element X ein maximales Ideal (X) erzeugen würde.)

(c) Wir können annehmen, daß f normiert ist. Dann ist f normiert, irreduzibel und erfüllt $f(\alpha) = 0$. Daraus folgt $f = \mathrm{minpol}_K(\alpha)$. Aus $g(\alpha) = 0$ folgt dann sofort $f | g$ in $K[X]$.

(d) Die Aussage ist i.a. falsch. Man betrachte z.B. die Körpererweiterungskette
$$\mathbb{Q} \; \subseteq \; M := \mathbb{Q}[\sqrt{2}] \; \subseteq \; L := \mathbb{Q}[\sqrt[4]{2}] \; .$$
Offenbar gilt $[M : \mathbb{Q}] = [L : M] = 2$. Alle obigen Erweiterungen sind separabel, da sie $\mathbb{Q}$ enthalten. Ferner sind Erweiterungen vom Grad 2 stets normal, da ein Polynom vom Grade 2, welches eine Nullstelle hat, bereits zerfällt. Daher sind die Erweiterungen $M/\mathbb{Q}$ und L/M jeweils galoissch. Andererseits ist $L/\mathbb{Q}$ nicht normal, da das Polynom $X^4 - 2$ eine Nullstelle in L hat, aber wegen $L \subseteq \mathbb{R}$ nicht über L zerfällt. Daher ist $L/\mathbb{Q}$ nicht galoissch.