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

10. Übungsblatt – Lösungsskizze

Aufgabe H26

Sei k mit $\mathbb{Q} \subseteq k \subseteq \mathbb{C}$ ein Körper. Dann gilt $\mathbb{Q}[X] \subseteq k[X]$ und somit $p \in k[X]$. Wir zeigen nun die folgende Aussage: Wenn p über dem Körper k reduzibel ist, dann sind $u, w \in k$, wobei u und w die beiden Nullstellen von p sind.
Sei also p reduzibel über k. Dann gibt es $q, r \in k[X]$, sodass $\deg(q) = \deg(r) = 1$ und somit gibt es $a_0, b_0 \in k$ und $a_1, b_1 \in k \setminus \{0\}$, sodass $p = (a_1X + a_0)(b_1X + b_0) = a_1b_1(X + \frac{a_0}{a_1})(X + \frac{b_0}{b_1})$. Aber dann sind $-\frac{a_0}{a_1}$ und $-\frac{b_0}{b_1}$ Nullstellen von p. Da $\deg(p) = 2$, sind dies schon alle Nullstellen von p, d.h. $\left\{-\frac{a_0}{a_1}, -\frac{b_0}{b_1}\right\} = \{u, w\}$. Somit ist $\{u, w\} \subseteq k$, wie behauptet.
Nun nehmen wir an, dass p eine Nullstelle u in $\mathbb{Q}$ hat. Dann teilt $(X - u) \in \mathbb{Q}[X]$ das Polynom p und somit ist p reduzibel über $\mathbb{Q}$. Wie bereits gezeigt wurde, liegen dann aber beide Nullstellen von p in $\mathbb{Q}$.
Für den zweiten Teil der Aussage zeigen wir nur, dass $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(u)$, da die Aussage $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(w)$ komplett analog ist. Aus der Tatsache, dass $u \in \mathrm{NS}(p)$ gilt, folgt sofort, dass $\mathbb{Q}(u) \subseteq \mathbb{Q}(\mathrm{NS}(p))$. Für die andere Richtung bemerken wir wieder, dass $(X - u) \in \mathbb{Q}(u)$ das Polynom p teilt. Somit liegen beide Nullstellen von p in $\mathbb{Q}(u)$. Daraus folgt, dass $\mathbb{Q}(\mathrm{NS}(p)) \subseteq \mathbb{Q}(u)$.

Aufgabe H27

1. Wir rechnen leicht nach, dass $\pm\sqrt{2}$ und $\pm\sqrt{3}$ Nullstellen von p sind. Da $\deg(p) = 4$ ist, sind dies schon alle Nullstellen, d.h. $\mathrm{NS}(p) = \{\pm\sqrt{2}, \pm\sqrt{3}\}$. Somit ist $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Aus Aufgabe **H5** wissen wir allerdings, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

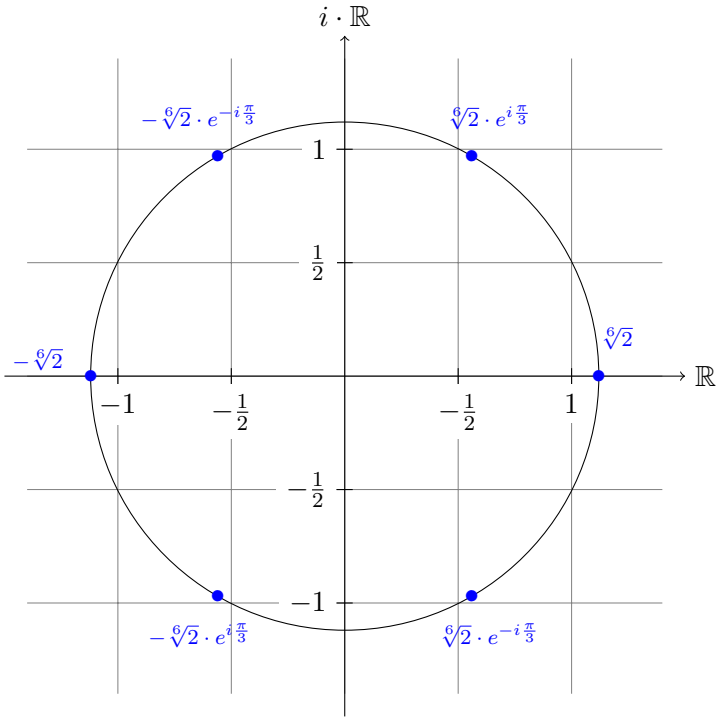
   Um zu sehen, dass $\sqrt{2}+\sqrt{3}$ keine Nullstelle von p ist, bemerken wir, dass $\sqrt{2}+\sqrt{3} = \sqrt{5 + 2\sqrt{6}}$ und rechnen aus, dass

   $$(5 + 2\sqrt{6})^2 - 5 \cdot (5 + 2\sqrt{6}) + 6 = 10 \cdot \sqrt{6} + 30 > 0.$$

2. Wir zählen $\mathrm{NS}(p)$ auf als $x_1 := \sqrt{2}$, $x_2 := -\sqrt{2}$, $x_3 := \sqrt{3}$, $x_4 := -\sqrt{3}$. Aus Aufgabe **H5** wissen wir, dass $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Mit dem Hauptsatz der Galois-Theorie folgt somit, dass $|\mathrm{Gal}_{\mathbb{Q}}(p)| = 4$. Es gilt, dass $p = (X^2 - 2)(X^2 - 3)$ und nach dem Eisenstein-Kriterium sind diese Faktoren irreduzibel. Nach Satz III.1.6 kann nun kein Element von $\mathrm{Gal}_{\mathbb{Q}}(p)$ Nullstellen von $(X^2 - 2)$ auf Nullstellen von $(X^2 - 3)$ abbilden oder umgekehrt. Somit ist also $\mathrm{Gal}_{\mathbb{Q}} \subseteq \{\mathrm{id}, (x_1\ x_2), (x_3\ x_4), (x_1\ x_2)(x_3\ x_4)\}$. Da $|\mathrm{Gal}_{\mathbb{Q}}| = 4$ gilt, ist dann aber schon $\mathrm{Gal}_{\mathbb{Q}} = \{\mathrm{id}, (x_1\ x_2), (x_3\ x_4), (x_1\ x_2)(x_3\ x_4)\}$. Da diese Gruppe Elemente der Ordnung 2 enthält, ist sie gemäß Aufgabe **H19** isomorph zu $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Aufgabe H28

1. Die blau eingezeichneten Punkte sind die Nullstellen von p:



2. Mit $\zeta := e^{\frac{2\pi i}{6}}$ und $\varepsilon := \sqrt[6]{2}$ gilt, dass $\mathrm{NS}(p) = \{\varepsilon \cdot \zeta^n \mid n \in \{0, \dots 6\}\}$. Man rechnet jedoch leicht nach (vgl. die Skizze in Aufgabenteil 1), dass

$$\begin{aligned}\zeta^2 &= -\overline{\zeta},\\ \zeta^3 &= -1,\\ \zeta^4 &= -\zeta,\\ \zeta^5 &= \overline{\zeta}.\end{aligned}$$

Damit erhalten wir, dass $\mathrm{NS}(p) = \{\varepsilon, -\varepsilon, \varepsilon\zeta, -\varepsilon\zeta, \varepsilon\overline{\zeta}, -\varepsilon\overline{\zeta}\}$ gilt. Somit folgt, dass $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(\varepsilon, \zeta, \overline{\zeta})$. Nun bemerken wir, dass $\zeta = \cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3}) = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, woraus bereits folgt, dass $\zeta \in \mathbb{Q}(i\sqrt{3})$. Analog zeigen wir, dass $\overline{\zeta} \in \mathbb{Q}(i\sqrt{3})$. Damit folgt, dass $\mathbb{Q}(\varepsilon, \zeta, \overline{\zeta}) \subseteq \mathbb{Q}(\varepsilon, i\sqrt{3})$. In die andere Richtung gilt, dass $i\sqrt{3} = 2 \cdot \zeta - 1$ und somit $i\sqrt{3} \in \mathbb{Q}(\zeta)$, was bereits zeigt, dass $\mathbb{Q}(\varepsilon, i\sqrt{3}) \subseteq \mathbb{Q}(\varepsilon, \zeta, \overline{\zeta})$. Somit erhalten wir insgesamt, dass $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(\varepsilon, i\sqrt{3})$, wie behauptet.

Wir zeigen nun, dass $[\mathbb{Q}(\varepsilon, i\sqrt{3}) : \mathbb{Q}] = 12$: Zunächst sehen wir, dass $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 6$, da nach dem Eisensteinkriterium $m_{\varepsilon,\mathbb{Q}} = X^6 - 2$ gilt. Ferner gilt, dass $\mathbb{Q}(\varepsilon) \subseteq \mathbb{R}$ und somit $i\sqrt{3} \notin \mathbb{Q}(\varepsilon)$. Damit ist $m_{i\sqrt{3},\mathbb{Q}(\varepsilon)} = X^2 + 3$ und somit $[\mathbb{Q}(\varepsilon, i\sqrt{3}) : \mathbb{Q}(\varepsilon)] = 2$. Somit erhalten wir insgesamt, dass $[\mathbb{Q}(\varepsilon, i\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon, i\sqrt{3}) : \mathbb{Q}(\varepsilon)] \cdot [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2 \cdot 6 = 12$.

Schließlich zeigen wir noch, dass $\mathbb{Q}(\varepsilon, i\sqrt{3}) = \mathbb{Q}(\varepsilon, \zeta)$. Dazu bemerken wir zunächst, dass $\mathbb{Q}(\varepsilon, \zeta) \subseteq \mathbb{Q}(\varepsilon, \zeta, \overline{\zeta}) = \mathbb{Q}(\varepsilon, i\sqrt{3})$. In die andere Richtung bemerken wir einfach, dass $\overline{\zeta} = \frac{1}{2} - \frac{i\sqrt{3}}{2}$ und somit $\zeta, \overline{\zeta} \in \mathbb{Q}(\varepsilon, i\sqrt{3})$ gilt, woraus folgt, dass $\mathbb{Q}(\varepsilon, i\sqrt{3}) \subseteq \mathbb{Q}(\varepsilon, \zeta)$.

3. Nach Aufgabenteil 2 ist $\mathbb{Q}(\mathrm{NS}(p)) = \mathbb{Q}(\varepsilon, \zeta)$ und somit gibt es einen eindeutig bestimmten Homomorphismus $\tau : \mathbb{Q}(\mathrm{NS}(p)) \to \mathbb{Q}(\mathrm{NS}(p)$, sodass $\tau|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, $\tau(\varepsilon) = \varepsilon \cdot \zeta$ und $\tau(\zeta) = \zeta$. Wir zeigen, dass τ ein Automorphismus ist. Dazu bemerken wir, dass es einen eindeutig bestimmten Homomorphismus $\tau' : \mathbb{Q}(\mathrm{NS}(p)) \to \mathbb{Q}(\mathrm{NS}(p))$ gibt, sodass $\tau'|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, $\tau'(\varepsilon) = \varepsilon \cdot \zeta^{-1}$ und $\tau'(\zeta) = \zeta$ und dass dieser beidseitig invers zu τ ist. Da wegen $\tau|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ und $\tau|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ beide Abbildungen $\mathbb{Q}$-linear sind, reicht es dafür aus, für alle $n, m \in \mathbb{N}$ zu zeigen, dass $\tau'(\tau(\varepsilon^n \cdot \zeta^m)) = \varepsilon^n \cdot \zeta^m = \tau(\tau'(\varepsilon^n \cdot \zeta^m))$. Wir zeigen nur die erste Gleichung; die zweite ist analog:

$$\tau'(\tau(\varepsilon^n \cdot \zeta^m)) = \tau'(\tau(\varepsilon)^n \cdot \tau(\zeta)^m) = \tau'(\varepsilon^n \cdot \zeta^n \cdot \zeta^m) = \tau'(\varepsilon)^n \cdot \tau'(\zeta)^{n+m} = \varepsilon^n \cdot \zeta^{-n} \cdot \zeta^{n+m} = \varepsilon^n \cdot \zeta^m$$

Somit ist $\tau \in \mathrm{Aut}(\mathbb{Q}(\mathrm{NS}))$ und da $\tau|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, also $\tau \in \mathrm{Gal}_{\mathbb{Q}}(p)$. Ferner ist τ von Ordnung 6. Dies sehen wir entweder durch direktes Nachrechnen oder dadurch, dass wir überprüfen, dass $\tau^2(\varepsilon) \neq \varepsilon$ und $\tau^3(\varepsilon) \neq \varepsilon$ und daraus folgern, dass $\mathrm{ord}(\tau) \notin \{2, 3\}$, woraus nach dem Satz von Lagrange schon folgt, dass $\mathrm{ord}(\tau) = 6$.

Es sei σ die Einschränkung der komplexen Konjugation auf $\mathbb{Q}(\mathrm{NS}(p))$, d.h. der eindeutige Homomorphismus $\sigma : \mathbb{Q}(\mathrm{NS}(p)) \to \mathbb{Q}(\mathrm{NS}(p)$ mit $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, $\tau(\varepsilon) = \varepsilon$ und $\tau(\zeta) = \overline{\zeta}$. τ ist ein injektiver Homomorphismus, da die komplexe Konjugation auf $\mathbb{C}$ ein injektiver Homomorphismus ist. Ferner ist τ surjektiv, da $\overline{\zeta} \in \mathbb{Q}(\mathrm{NS}(p)$ und $\zeta = \sigma(\overline{\zeta})$ und somit $\mathbb{Q} \cup \{\varepsilon\} \cup \{\zeta\} \subseteq \mathrm{im}(\sigma)$. Damit ist $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(p)$. Ferner ist $\mathrm{ord}(\sigma) = 2$, da die komplexe Konjugation zu sich selbst invers ist.

Schließlich zeigen wir, dass für alle $n \in \{0, \ldots, 5\}$ gilt, dass $\tau^n \neq \sigma$. Wenn $n = 0$ gilt, so ist dies klar, da $\tau^0 = \mathrm{id}_{\mathbb{Q}(\mathrm{NS}(p))}$. Andernfalls hat τ^n die Eigenschaft, dass für jedes $x \in \mathrm{NS}(p)$ gilt, dass $\tau^n(x) \neq x$, da τ als Element der Ordnung 6 als 6-Zyklus operiert. Somit gilt auch für je zwei $n, m \in \{0, \ldots, 5\}$, dass $\tau^n \neq \sigma\tau^m$, da ansonsten $\sigma = \tau^{n-m}$ gälte. Aus dem Hauptsatz der Galois-Theorie zusammen mit Aufgabenteil 4 ergibt sich, dass $|\mathrm{Gal}_Q(p)| = 12$ und somit haben wir, dass

$$\mathrm{Gal}_Q(p) = \{\mathrm{id}, \tau, \tau^2, \tau^3, \tau^4, \tau^5, \sigma\tau, \sigma\tau^2, \sigma\tau^3, \sigma\tau^4, \sigma\tau^5\}.$$

Es bleibt nun zu zeigen, dass für alle $i \in \{0, \ldots, 5\}$ gilt, dass $\sigma \cdot \tau^i = \tau^{-i} \cdot \sigma$. Wir zeigen dies durch Induktion über i. Der Fall $i = 0$ ist klar, also beginnen wir mit $i = 1$. Jedes Element von $\mathrm{Gal}_{\mathbb{Q}}(p)$ ist durch seine Wirkung auf $\mathrm{NS}(p)$ bestimmt. Wir rechnen zunächst für $j \in \{0, \ldots, 5\}$:

$$\sigma(\tau(\varepsilon\zeta^j)) = \sigma(\varepsilon\zeta^{j+1}) = \varepsilon\overline{\zeta}^{j+1} = \varepsilon\overline{\zeta} \cdot \overline{\zeta}^j = \varepsilon\zeta^{-1}\overline{\zeta}^j = \tau^{-1}(\varepsilon\overline{\zeta}^j) = \tau^{-1}(\sigma(\varepsilon\zeta^j)),$$

wobei wir benutzt haben, dass $\zeta^{-1} = \zeta^5 = \overline{\zeta}$. Dies zeigt, dass $\sigma \cdot \tau = \tau^{-1} \cdot \sigma$. Nun nehmen wir für ein festes $i \in \{0, \ldots, 5\}$ an, dass $\sigma \cdot \tau^i = \tau^{-i} \cdot \sigma$. Dann berechnen wir für $i + 1$:

$$\sigma \cdot \tau^{i+1} = \sigma \cdot \tau^i \cdot \tau = \tau^{-i} \cdot \sigma \cdot \tau = \tau^{-i} \cdot \tau^{-1} \cdot \sigma = \tau^{-(i+1)} \cdot \sigma.$$

4. Ein allgemeines Element in $\mathrm{Gal}_{\mathbb{Q}}(p)$ ist von der Form $\sigma^k \cdot \tau^i$ mit $k \in \{0, 1\}$ und $\tau \in \{0, 1, \ldots, 5\}$. Um die Kommutatoren solcher Elementes auszurechnen unterscheiden wir den Fall $k = 0$ und den Fall $k = 1$. Für $i, j \in \{0, 1, \ldots, 5\}$ erhalten wir dann:

$$\begin{aligned}
[\tau^i, \tau^j] &= \tau^{i+j} \cdot \tau^{-i-j} = \mathrm{id}\,. \\
[\sigma\tau^i, \tau^j] &= \sigma \cdot \tau^{i+j} \cdot (\tau^j \cdot \sigma \cdot \tau^i)^{-1} = \tau^{-(i+j)} \cdot \sigma \cdot (\tau^{j+i} \cdot \sigma)^{-1} = \tau^{-2i} = \tau^{6-2i}. \\
[\tau^i, \sigma\tau^j] &= ([\sigma\tau^j, \tau^i])^{-1} = \tau^{2j}. \\
[\sigma\tau^i, \sigma\tau^j] &= \sigma\tau^i \cdot \sigma\tau^j \cdot (\sigma\tau^j\sigma\tau^i)^{-1} = \tau^{-i}\sigma\sigma\tau^j \cdot (\tau^{-j}\sigma\sigma\tau^i)^{-1} = \tau^{j-i} \cdot \tau^{j-i} = \tau^{2(j-i)}.
\end{aligned}$$

Damit ist $(\mathrm{Gal}_{\mathbb{Q}}(p))' = \{\mathrm{id}, \tau^2, \tau^4\} = \langle \tau^2 \rangle$ und somit kommutativ. Daraus folgt, dass $(\mathrm{Gal}_{\mathbb{Q}}(p))^{(2)} = \{\mathrm{id}\}$ und somit, dass $\mathrm{Gal}_{\mathbb{Q}}(p)$ auflösbar ist.