Algebra - Übungszettel 12 (Abgabe: 22.01.20)

Aufgabe 1. Sei $L/\mathbb{Q}$ ein Zerfällungskörper des Polynoms $X^3 - 7 \in \mathbb{Q}[X]$.

(a) Zeige, dass die Galoisgruppe $G(L/\mathbb{Q})$ isomorph zur symmetrischen Gruppe S_3 ist.

(b) Finde ein $\alpha \in L$ mit $L = \mathbb{Q}(\alpha)$.

(c) Bestimme alle Untergruppen von $G(L/\mathbb{Q})$ und die zugehörigen Zwischenkörper von $L/\mathbb{Q}$.

Lösung. (a) Dies lässt sich sofort an der Diskriminante ablesen, wir hatten diese aber noch nicht eingeführt, als die Aufgabe gestellt wurde. Also direkt: Das Polynom $f(X) = X^3 - 7$ ist irreduzibel, da es keine Nullstelle in $\mathbb{Q}$ hat. Die Nullstellen von f in $\mathbb{C}$ sind $\alpha_1 = \sqrt[3]{7}$, $\alpha_2 = \zeta\sqrt[3]{7}$, und $\alpha_3 = \zeta^2\sqrt[3]{7}$ wobei ζ eine primitive dritte Einheitswurzel ist. Damit ist der Zerfällungskörper gegeben durch $L = \mathbb{Q}(\sqrt[3]{7}, \zeta) \subset \mathbb{C}$. Die Einheitswurzel ζ ist eine Nullstelle des Polynoms $X^2 + X + 1$, welches in $\mathbb{R}$ und damit auch in $\mathbb{Q}(\sqrt[3]{7})$ keine Nullstelle hat, also ein irreduzibles Polynom in $\mathbb{Q}(\sqrt[3]{7})[X]$ ist. Wir folgern, dass die Erweiterungen $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$ und $L/\mathbb{Q}(\sqrt[3]{7})$ primitiv sind, mit $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$ und $[L : \mathbb{Q}(\sqrt[3]{7})] = 2$. Also gilt $[L : \mathbb{Q}] = 6$. Weiterhin operiert die Galoisgruppe $G(L/\mathbb{Q})$ treu auf den Nullstellen von f lässt sich also mit einer Untergruppe von S_3 identifieren. Da $|G(L/\mathbb{Q})| = [L : \mathbb{Q}]$ gilt muss dann aber gelten $G(L/\mathbb{Q}) \cong S_3$.

(b) Wir wissen aus vorherigem Übungszettel: Für alle bis auf endlich viele $\lambda \in K$, gilt $L = \mathbb{Q}(\sqrt[3]{7} + \lambda\zeta)$. Wir probieren $\lambda = 1$. Um zu zeigen, dass $\alpha := \sqrt[3]{7} + \zeta$ in keinem echten Teilkörper von L enthalten ist, genügt es zu zeigen, dass α von keinem $\mathrm{id} \neq \sigma \in G(L/\mathbb{Q})$ fixiert wird (Galoiskorrespondenz). Wir identifizieren die Galoisgruppe mit S_3 und rechnen

$$\begin{aligned}(12).\alpha &= \zeta\sqrt[3]{7} + \zeta^2\\ (13).\alpha &= \zeta^2\sqrt[3]{7} + \zeta^2\\ (23).\alpha &= \sqrt[3]{7} + \zeta^2\\ (123).\alpha &= \zeta\sqrt[3]{7} + \zeta\\ (132).\alpha &= \zeta^2\sqrt[3]{7} + \zeta.\end{aligned}$$

Die Tatsache, dass keines dieser Elemente mit α übereinstimmt lässt sich zum Beispiel leicht nachvollziehen, indem man verwendet, dass

$$1, \sqrt[3]{7}, \sqrt[3]{7}^2, \zeta, \zeta\sqrt[3]{7}, \zeta\sqrt[3]{7}^2$$

eine $\mathbb{Q}$-Basis von L bildet und $\zeta^2 + \zeta + 1 = 0$ gilt.

(c) Die echten Zwischenkörper sind gegeben durch

$$\begin{aligned}L^{\langle(12)\rangle} &= \mathbb{Q}(\zeta^2\sqrt[3]{7})\\ L^{\langle(13)\rangle} &= \mathbb{Q}(\zeta\sqrt[3]{7})\\ L^{\langle(23)\rangle} &= \mathbb{Q}(\sqrt[3]{7})\\ L^{\langle(123)\rangle} &= \mathbb{Q}(\zeta).\end{aligned}$$

□

Aufgabe 2. Es seien $p_1, p_2, \ldots, p_n$ paarweise verschiedene Primzahlen. Sei $L/\mathbb{Q}$ ein Zerfällungskörper des Polynoms

$$(X^2 - p_1)(X^2 - p_2) \cdots (X^2 - p_n) \in \mathbb{Q}[X].$$

Zeige, dass $L/\mathbb{Q}$ galoissch ist und bestimme die Galoisgruppe $G(L/\mathbb{Q})$.

Lösung. Wir wollen zunächst zeigen, dass $[L : \mathbb{Q}] = 2^n$ gilt. Wir zeigen dies, indem wir induktiv beweisen, dass das Polynom $X^2 - p_r$ im Körper $L_{r-1} := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{r-1}})$ keine Nullstelle hat, also anders gesagt, dass das die Primzahl p_r in L_{r-1} keine Quadratwurzel besitzt. Für den Beweis ist es vorteilhaft eine etwas stärkere Aussage zu zeigen, nämlich, dass auch jedes $\frac{p_r}{a}$ mit $a \in \mathbb{N}$ und $\mathrm{ggT}(a, p_r) = 1$ in L_{r-1} keine Quadratwurzel hat.

Induktionsanfang: $r = 1$. Eine Zahl $\frac{p_1}{a}$ mit $a \in \mathbb{N}$ und $\mathrm{ggT}(a, p_1) = 1$ hat in $\mathbb{Q}$ keine Quadratwurzel. Dies ist klar, denn sei $\frac{u}{v} \in \mathbb{Q}$ ein gekürzter Bruch, also $\mathrm{ggT}(u, v) = 1$, dann impliziert $(\frac{u}{v})^2 = \frac{p_1}{a}$ schon $u^2 = p_1$, da beide Brüche gekürzt sind. Dies steht aber im Widerspruch, zur Annahme, dass p_1 eine Primzahl ist.

Induktionsschritt: $r \rightsquigarrow r + 1$. Zu zeigen: Eine Zahl $\frac{p_{r+1}}{a}$ mit $a \in \mathbb{N}$ und $\mathrm{ggT}(a, p_{r+1}) = 1$ hat in L_r keine Quadratwurzel. Per Induktionshypothese, wissen wir, dass $1, \sqrt{p_r}$ eine Basis von L_r/L_{r-1} ist, denn $X^2 - p_r$ ist irreduzibel über L_{r-1}. Sei also $x = y + z\sqrt{p_r} \in L_r$ beliebig mit $y, z \in L_{r-1}$. Dann impliziert die Gleichung $x^2 = \frac{p_{r+1}}{a}$ die Gleichungen

$$y^2 + p_r z^2 = \frac{p_{r+1}}{a}$$
$$2yz = 0.$$

1. Fall: $z = 0$. Dann muss also gelten $y^2 = \frac{p_{r+1}}{a}$ was durch die Induktionshypothese ausgeschlossen ist, da $y \in L_{r-1}$, also $\frac{p_{r+1}}{a}$ in diesem Körper keine Quadratwurzel hat.
2. Fall: $y = 0$. Dann muss gelten $z^2 p_r = \frac{p_{r+1}}{a}$, also $z^2 = \frac{p_{r+1}}{a p_r}$ was wieder durch die Induktionshypothese ausgeschlossen ist, da $z \in L_{r-1}$, also $\frac{p_{r+1}}{a p_r}$ in diesem Körper keine Quadratwurzel hat.

Wir bestimmen nun die Galoisgruppe wie folgt: Wie in der Vorlesung gezeigt, operiert die Galoisgruppe $G(L/\mathbb{Q})$ auf den Nullstellen jedes irreduziblen Faktors $X^2 - p_i$, also erhalten wir einen Homomorphismus

$$G(L/\mathbb{Q}) \longrightarrow S_{\{\pm\sqrt{p_1}\}} \times \cdots \times S_{\{\pm\sqrt{p_n}\}} \cong (C_2)^n$$

und dieser ist injektiv (wenn $\sigma \in G(L/\mathbb{Q})$ alle Nullstellen $\sqrt{p_i}$ fixiert, dann gilt $\sigma = \mathrm{id}$, wie in Vorlesung diskutiert). Nun ist aber $|G(L/\mathbb{Q})| = [L : \mathbb{Q}] = 2^n = |(C_2)^n|$, also muss $G(L/\mathbb{Q}) \cong (C_2)^n$ gelten. □

Aufgabe 3. Sei L/K eine Erweiterung endlicher Körper. Zeige: Es gibt ein Element $\alpha \in L$ so dass $L = K(\alpha)$. Tipp: Bestimme per Galoiskorrespondenz alle Zwischenkörper von L/K, und zeige die Existenz von α durch Abzählen derjenigen Elemente von L, welche in echten Zwischenkörpern enthalten sind.

Beweis. Sei $\mathrm{char}(K) = p$, dann gilt $\mathbb{F}_p \subset K \subset L$, also auch $\mathrm{char}(L) = p$. Es genügt nun zu zeigen, dass es $\alpha \in L$ gibt mit $L = \mathbb{F}_p(\alpha)$, dann gilt nämlich natürlich auch $L = K(\alpha)$. Wir verwenden nun, dass die Erweiterung $L/\mathbb{F}_p$ galoissch ist, mit zyklischer Galoisgruppe $G(L/\mathbb{F}_p) = \langle F \rangle$ erzeugt vom Frobeniusautomorphismus F. Per Galoiskorrespondenz gibt es zu jeder Untergruppe von $G(L/\mathbb{F}_p)$ genau einen Zwischenkörper von $L/\mathbb{F}_p$. Wir haben gezeigt, dass die Untergruppen einer zyklischen Gruppe der Ordnung n genau zu den Teilern von n korrespondieren: Im gegebenen Fall ist jede Untergruppe von $G(L/\mathbb{F}_p)$ von der Form $\langle F^k \rangle$ wobei $k|n$. Per Galoiskorrespondenz gilt dann für den Fixkörper M von $\langle F^k \rangle$ dass $[L : M] = \frac{n}{k}$ und $[M : \mathbb{F}_p] = k$, also $|M| = p^k$ und damit auch $M \cong \mathbb{F}_{p^k}$. Zusammenfassend gibt es also zu jedem Teiler $k|n$ genau einen Zwischenkörper M von $L/\mathbb{F}_p$ und dieser hat p^k Elemente.

Wir zeigen nun durch ein Abschätzung der Anzahl der Elemente von L welche in echten Teilkörpern enthalten sind, dass die Vereinigung dieser echten Teilkörper nicht ganz L sein kann. Jedes α im Komplement dieser Vereinigung erfüllt dann per Konstruktion $L = \mathbb{F}_p(\alpha)$. Die Abschätzung ist die folgende:

$$|\bigcup_{\mathbb{F}_p \subset M \subset L} M| \leq \sum_{\substack{k|n \\ k \neq n}} p^k \leq \sum_{k=0}^{n-1} p^k = \frac{p^n - 1}{p - 1} < p^n = |L|$$

□

Aufgabe 4. Sei $L/\mathbb{Q}$ der Zerfällungskörper des Polynoms $X^8 - 1 \in \mathbb{Q}[X]$. Bestimme die Galoisgruppe $G(L/\mathbb{Q})$, das Gitter der Untergruppen von $G(L/\mathbb{Q})$ und die zugehörigen Zwischenkörper von $L/\mathbb{Q}$.

Lösung. Die Nullstellen des Polynoms $f(X) = X^8 - 1$ in $\mathbb{C}$ sind die 8-ten Einheitswurzeln. Diese zerlegen sich in eine primitive 1-te Wurzel (1), eine primitive 2-te Wurzel (-1), zwei primitive 4-te Wurzeln (i und $-i$) und 4 primitive 8-te Wurzeln ($\exp(2\pi ik/4)$ für $k = 1, 3, 5, 7$). Diese Zerlegung korrespondiert zur Faktorisierung von f in seine irreduziblen Faktoren

$$f(X) = (X - 1)(X + 1)(X^2 + 1)(X^4 + 1) \in \mathbb{Q}[X],$$

welche genau die m-ten Kreisteilungspolynome für $m = 1, 2, 4, 8$ sind. Aber dies haben wir erst nach dem Übungszettel in der Vorlesung besprochen, die obige Zerlegung, und die Tatsache, dass $X^4 + 1$ irreduzibel ist, rechnet man einfach direkt nach: Da $X^4 + 1$ keine Nullstelle in $\mathbb{Q}$ (sogar $\mathbb{R}$) hat, ist die verbleibende Möglichkeit, dass sich $X^4 + 1$ als Produkt von irreduziblen Polynomen in $\mathbb{Z}[X]$ (Gauss-Lemma) vom Grad 2 schreiben lässt, also als $(X^2 + aX + b)(X^2 + cX + d)$. Dies impliziert:

$$\begin{aligned} a + c &= 0 \\ ac + d + f &= 0 \\ df &= 1 \end{aligned}$$

Auflösen der Gleichungen zeigt, dass $a^2 = \pm 2$ gelten muss, ein Widerspruch, so dass $X^4 + 1$ irreduzibel ist.

Mit $\zeta = \exp(2\pi i/4)$ ist also der Zerfällungskörper $L = \mathbb{Q}(\zeta)/\mathbb{Q}$ primitiv wobei das Minimalpolynom von ζ genau $X^4 + 1$ ist, also $L \cong \mathbb{Q}[T]/(T^4 + 1)$. Es gibt demnach also für jede der Nullstellen $\zeta, \zeta^3, \zeta^5, \zeta^7$ genau einen Automorphismus $\sigma \in G(L/\mathbb{Q})$, eindeutig bestimmt durch $\sigma(\zeta) = \zeta^k$, $k = 1, 3, 5, 7$. Es folgt zunächst eine Bijektion von Mengen $G(L/\mathbb{Q}) \cong \{1, 3, 5, 7\} = (\mathbb{Z}/8\mathbb{Z})^*$ welche aber auch ein Gruppenhomomorphismus ist, denn es gilt für $\sigma(\zeta) = \zeta^k$ und $\tau(\zeta) = \zeta^l$, dass $\sigma\tau(\zeta) = \zeta^{kl}$.

Weiterhin ergibt direktes Nachrechnen $(\mathbb{Z}/8\mathbb{Z})^* \cong C_2 \times C_2$. Also ist die Galoisgruppe von $L/\mathbb{Q}$ isomorph zur Kleinschen Vierergruppe.

Die nichttrivialen Untergruppen der Galoisgruppe sind die drei zyklischen Gruppen der Ordnung 2 erzeugt von 3, 5, und 7. Die zugehörigen Zwischenkörper, welche also quadratische Erweiterungen von $\mathbb{Q}$ sein müssen, lassen sich zum Beispiel beschreiben als $\mathbb{Q}(\zeta + \zeta^3) = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\zeta\zeta^5) = \mathbb{Q}(i)$, $\mathbb{Q}(\zeta + \zeta^7) = \mathbb{Q}(\sqrt{2})$.

□