Algebra - Übungszettel 13 (Abgabe: 29.01.20)

Aufgabe 1. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3 welches genau eine reelle Nullstelle besitzt. Zeige, dass die Galoisgruppe des Zerfällungskörpers von f isomorph zur symmetrischen Gruppe S_3 ist.

Lösung. Da f irreduzibel ist, ist die Galoisgruppe von f isomorph zu einer transitiven Untergruppe von S_3, also A_3 oder S_3. Um den Zerfällungskörper von f zu konstruieren betrachten wir zunächst die primitive Erweiterung $M = \mathbb{Q}[T]/(f(T))$ von $\mathbb{Q}$. Da f eine reelle Nullstelle $\alpha \in \mathbb{R}$ besitzt, erhalten wir einen Einsetzungshomomorphismus $M \hookrightarrow \mathbb{R}, g(T) \mapsto g(\alpha)$ mit $[M : \mathbb{Q}] = 3$. M kann noch nicht der Zerfällungskörper von f sein, da f auch komplexe Nullstellen besitzt, also gilt für den Zerfällungskörper $[L : \mathbb{Q}] > 3$, so dass also die Galoisgruppe isomorph zu S_3 sein muss. □

Aufgabe 2. Sein K ein Körper. Man führe unter Anwendung der induktiven Strategie im Beweis des Hauptsatzes über symmetrische Funktionen folgende Rechnungen aus:

(1) Drücke das symmetrische Polynom

$$X_1^2 + X_2^2 + \cdots + X_n^2 \in K[X_1, \ldots, X_n],$$

$n \geq 1$ als Polynom in den elementarsymmetrischen Polynomen $e_1, \ldots, e_n$ aus.

(2) Drücke das symmetrische Polynom

$$(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2 \in K[X_1, X_2, X_3]$$

als Polynom in den elementarsymmetrischen Polynomen e_1, e_2, e_3 aus. Folgere, dass die Diskriminante eines Polynoms

$$f(X) = X^3 + pX + q \in K[X]$$

durch die Formel $D = -4p^3 - 27q^2$ gegeben ist.

Lösung. (1) Es gilt

$$X_1^2 + X_2^2 + \cdots + X_n^2 = e_1^2 - 2e_2.$$

(2) Anwenden des induktiven Algorithmus aus der Vorlesung liefert

$$(X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2 = e_1^2e_2^2 - 4e_2^3 - 4e_1^3e_3 - 27e_3^2 + 18e_1e_2e_3$$

also gilt mit $e_1 = 0$, $e_2 = p$ und $e_3 = -q$, die Formel

$$D = -4p^3 - 27q^2.$$

□

Aufgabe 3. Sei L'/K eine Körpererweiterung mit Zwischenkörpern $K \subset L \subset L'$ und $K \subset K' \subset L'$ so dass es keine echten Teilkörper von L' gibt, welche L und K' enthalten. Sei L/K eine Galoiserweiterung.

(1) Zeige, dass die Erweiterung L'/K' galoissch ist.

(2) Zeige, dass die Restriktionsabbildung einen Isomorphismus

$$G(L'/K') \cong G(L/L \cap K')$$

definiert und folgere, dass sich die Galoisgruppe $G(L'/K')$ mit einer Untergruppe von $G(L/K)$ identifizieren lässt.

Tipp: Jede Galoiserweiterung ist Zerfällungskörper eines separablen Polynoms.

Lösung. (1) Sei L/K Zerfällungskörper des separablen Polynoms $f(X) \in K[X]$. Dann ist, per Annahme, L'/K' der Zerfällungskörper von $f(X) \in K'[X]$, also galoissch.

(2) Sei nun $\alpha \in L$ ein primitives Element, also $L = K(\alpha)$ (Existenz wurde auf vorigen Übungszetteln bewiesen). Dann ist das Polynom

$$g(X) = \prod_{\sigma \in G(L/L\cap K')} (X - \sigma(\alpha)) \in (L \cap K')[X] \tag{1}$$

irreduzibel und separabel. Es gilt

$$L \cong (L \cap K')[T]/(g(T))$$

insbesondere also $[L : (L \cap K')] = \mathrm{grad}(g)$. Es gilt natürlich auch $L' = K'(\alpha)$. Desweiteren behaupten wir, dass $g(X) \in K'[X]$ irreduzibel ist. Denn wäre dies nicht der Fall, also

$$g(X) = p(X)q(X) \in K'[X].$$

Doch wegen (1) müssen sowohl $p(X)$ und $q(X)$ ein Produkt von Linearfaktoren der Form $(X - \sigma(\alpha))$ sein, haben also beide Koeffizienten in L. Doch die ist ein Widerspruch zur Irreduzibilität von $g(X) \in (L \cap K')[X]$. Insbesondere gilt also auch

$$L' \cong K'[T]/(g(T))$$

also $[L' : K'] = \mathrm{grad}(g) = [L : (L \cap K')]$.

Wir behaupten nun, dass sich jeder Automorphismus $\sigma \in G(L'/K')$ einschränkt auf einen Automorphismmus $\sigma|L \in G(L/K' \cap L)$. Dazu beachte, dass zunächst die Einschränkung eine Einbettung $\sigma|L : L \hookrightarrow L'$ über $K' \cap L$ definiert. Es gibt aber nach dem Dedekind Lemma höchstens $[L : K' \cap L]$ paarweise verschiedene solcher Einbettungen und, da $L/K' \cap L$ Galoissch ist, müssen also alle Einbettungen L auf sich selbst abbilden. Wir erhalten demnach einen wohldefinierten Homomorphismus

$$\pi : G(L'/K') \longrightarrow G(L/L \cap K'),\ \sigma \mapsto \sigma_{|L}.$$

Falls $\sigma \in \ker(\pi)$, dann muss gelten $\sigma(\alpha) = \alpha$. Da aber $L' = K'(\alpha)$ gilt dann schon $\sigma = \mathrm{id}_{L'}$. Daher ist also π injektiv. Die Surjektivität folgt nun wegen

$$|G(L'/K')| = [L' : K'] = [L : (L \cap K')] = |G(L/L \cap K')|.$$

□

Aufgabe 4. Sei $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})})$. Zeige:

(1) Die Körpererweiterung $L/\mathbb{Q}$ ist galoissch und $G(L/\mathbb{Q})$ is isomorph zur Quaternionengruppe Q_8.

(2) Bestimme das Gitter aller Zwischenkörper von $L/\mathbb{Q}$.

(3) Bestimme ein Polynom $f \in \mathbb{Q}[X]$ so dass L der Zerfällungskörper von f über $\mathbb{Q}$ ist.

Lösung. Wir zeigen (1). Wir zeigen dass $[L : \mathbb{Q}] = 8$ ist, konstruieren 8 paarweise verschiedene Automorphismen in $G(L/\mathbb{Q})$ und zeigen schliesslich, wie sich $G(L/\mathbb{Q})$ mit Q_8 identifizieren lässt. Wir betrachten den Turm von primitiven Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})}).$$

Wir behaupten zunächst, dass jede dieser Erweiterungen Grad 2 hat. Dies ist klar für die ersten beiden Erweiterungenen (vorheriges Übungsblatt). Für die Erweiterung

$$M = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})}) = L$$

müssen wir zeigen, dass $(2+\sqrt{2})(3+\sqrt{3})$ keine Quadratwurzel in M besitzt. Das folgende schöne Argument hierfür ist von Leonhard Reichenbach und Karim Ritter von Merkl: Angenommen es gäbe eine solche Wurzel, also $\alpha \in M$ mit

$$\alpha^2 = (2+\sqrt{2})(3+\sqrt{3})$$

Sei $\sigma \in G(M/\mathbb{Q})$ der Automorphismus mit $\sigma(\sqrt{2}) = -\sqrt{2}$ und $\sigma(\sqrt{3}) = \sqrt{3}$. Dann gilt

$$\sigma(\alpha^2) = (2-\sqrt{2})(3+\sqrt{3})$$

also auch

$$\sigma(\alpha)^2 = \frac{(2-\sqrt{2})^2}{2}\alpha^2$$

wegen

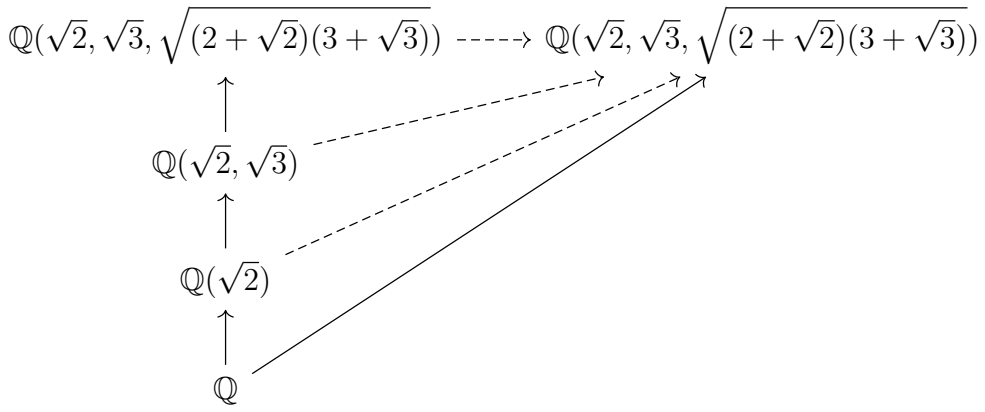
$$(2-\sqrt{2})(2+\sqrt{2}) = 2.$$

Daher folgt, dass gelten muss

$$\sigma(\alpha) = \pm\frac{(2-\sqrt{2})}{\sqrt{2}}\alpha = \pm(\sqrt{2}-1)\alpha$$

Doch dann gilt $\sigma^2(\alpha) = -\alpha$ und dies ist ein Widerspruch, denn $\sigma^2 = \mathrm{id}$. Dies zeigt also, dass auch die Erweiterung $M \subset L$ eine primitive Erweiterung vom Grad 2 ist, so dass also wie behauptet gilt $[L : \mathbb{Q}] = 8$.

Wir konstruieren nun die gewünschten 8 Automorphismen in $G(L/\mathbb{Q})$ in dem wir iterativ Einbettungen



konstruieren. Da der vertikale Turm eine Kette von primitiven Erweiterungen bildet, können wir diese Einbettungen wie in der Vorlesung konstruieren, indem wir jeweils den primitiven Erzeuger auf eine Nullstelle seines Minimalpolynoms in L abbilden. Es geht also nun um die Frage, ob wir jeweils genügend Nullstellen finden, um alle 8 potentiell möglichen Automorphismen zu konsturieren. Es ist klar, dass wir entlang der ersten beiden primitiven Erweiterungen genau 4 Einbettungen $M \hookrightarrow L$ konstruieren können, die gegeben sind durch

$$\sqrt{2} \mapsto \pm\sqrt{2}$$
$$\sqrt{3} \mapsto \pm\sqrt{3}.$$

Diese Einbettungen bilden M auf sich selbst ab und liefern so die 4 Automorphismen in $G(M/\mathbb{Q})$. Wir befassen uns nun mit der Konstruktion von Fortsetzungen entlang $M \subset L$ dieser 4 Automorphismen von M zu Automorphismen von L. Dazu berechnen wir zunächst

$$(2+\sqrt{2})(2-\sqrt{2}) = 2$$
$$(3+\sqrt{3})(3-\sqrt{3}) = 6$$

woraus sich die Formeln

$$\begin{aligned}
\sqrt{(2-\sqrt{2})(3+\sqrt{3})} &= \frac{\sqrt{2}(3+\sqrt{3})}{\sqrt{(2+\sqrt{2})(3+\sqrt{3})}} \\
\sqrt{(2+\sqrt{2})(3-\sqrt{3})} &= \frac{\sqrt{2}\sqrt{3}(2+\sqrt{2})}{\sqrt{(2+\sqrt{2})(3+\sqrt{3})}} \\
\sqrt{(2-\sqrt{2})(3-\sqrt{3})} &= \frac{2\sqrt{3}}{\sqrt{(2+\sqrt{2})(3+\sqrt{3})}}
\end{aligned} \tag{2}$$

ableiten lassen. Da also jede der Quadratwurzeln auf der linken Seite dieser Gleichungen in L existiert, lassen sich die 4 obigen Automorphismen von $G(M/\mathbb{Q})$ zu Automorphismen

von $L/\mathbb{Q}$ fortsetzen mit den Formeln:

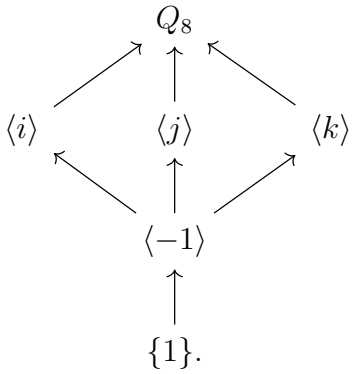
$$\begin{aligned}\sqrt{2} &\mapsto \pm\sqrt{2}\\ \sqrt{3} &\mapsto \pm\sqrt{3}\\ \sqrt{(2+\sqrt{2})(3+\sqrt{3})} &\mapsto \pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}\end{aligned}$$

wobei die Vorzeichen vor $\sqrt{2}$ und $\sqrt{3}$ in der letzten Zeile dieselben wie die entsprechenden Vorzeichen in der ersten und zweiten Zeile sind. Dies liefert 8 Automorphismen in $G(L/\mathbb{Q})$, insbesondere ist $L/\mathbb{Q}$ also galoissch. Da $\alpha := \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ von keinem $\sigma \in G(L/\mathbb{Q})$ festgehalten wird muss gelten $L = \mathbb{Q}(\alpha)$, so dass also jedes $\sigma \in G(L/\mathbb{Q})$ durch $\sigma(\alpha)$ bestimmt ist. Wir bezeichnen nun die folgenden Automorphismen in $G(L/\mathbb{Q})$:

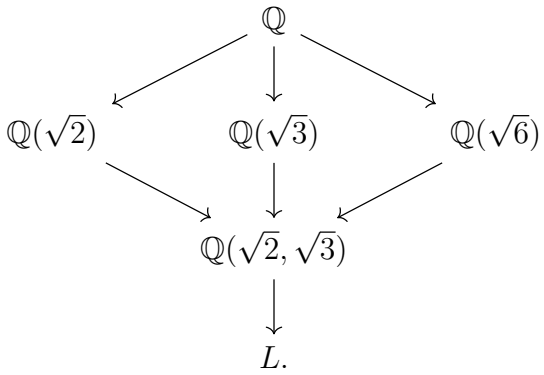
$$\begin{aligned}i :&\sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2+\sqrt{2})(3-\sqrt{3})}\\ j :&\sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2-\sqrt{2})(3+\sqrt{3})}\\ k :&\sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2-\sqrt{2})(3-\sqrt{3})}.\end{aligned}$$

Mittels der Relationen (2) zeigt man nun leicht, dass diese Automorphismen genau die Relationen der Quaternionengruppe Q_8 erfüllen, also insbesondere, da diese von i, j, k erzeugt ist, gilt auch $G(L/\mathbb{Q}) \cong Q_8$.

Das Gitter der Untergruppen wurde schon auf einem vorigen Übungszettel untersucht:



Das dazu korrespondierende Gitter von Zwischenkörpern lässt sich wie folgt beschreiben:



Schließlich beschreiben wir noch ein Polynom dessen Zerfällungskörper genau $L/\mathbb{Q}$ ist. Dazu verwenden wir $L = \mathbb{Q}(\alpha)$ und definieren

$$f(X) = \prod_{\sigma \in G(L/\mathbb{Q})} (X - \sigma(\alpha)).$$

Wir führen die Notation

$$\begin{aligned} a &= (2 + \sqrt{2}) \\ \overline{a} &= (2 - \sqrt{2}) \\ b &= (3 + \sqrt{3}) \\ \overline{b} &= (3 - \sqrt{3}) \end{aligned}$$

ein und rechnen

$$\begin{aligned} f(X) &= (X^2 - ab)(X^2 - \overline{a}\overline{b})(X^2 - \overline{a}b)(X^2 - a\overline{b}) \\ &= (X^4 - (ab + \overline{a}\overline{b})X^2 + 12)(X^4 - (\overline{a}b + a\overline{b})X^2 + 12) \\ &= X^8 - (ab + \overline{a}\overline{b} + \overline{a}b + a\overline{b})X^6 + (24 + (ab + \overline{a}\overline{b})(\overline{a}b + a\overline{b}))X^4 \\ &- 12(ab + \overline{a}\overline{b} + \overline{a}b + a\overline{b})X^2 + 144 \\ &= X^8 - 24X^6 + 84X^4 - 288X^2 + 144. \end{aligned}$$

□