

## Übungsblatt 14 zur Algebra I

Abgabetermin entscheidet ihr!

### Aufgabe 1. Illustrationen des Hauptsatzes

- Zeige, dass die einzigen Zwischenerweiterungen von  $\mathbb{Q}(\sqrt{2})$  über  $\mathbb{Q}$  die beiden trivialen (ganz  $\mathbb{Q}(\sqrt{2})$  und nur  $\mathbb{Q}$ ) sind.
- Finde ein normiertes separables Polynom  $f(X)$  mit rationalen Koeffizienten, sodass der Index der Untergruppe  $\text{Gal}_{\mathbb{Q}(\sqrt[3]{2})}(x_1, \dots, x_n)$  in  $\text{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)$  gleich 3 ist. Dabei seien  $x_1, \dots, x_n$  die Nullstellen von  $f(X)$ . Ist diese Untergruppe ein Normalteiler?
- Sei  $f(X)$  ein normiertes separables Polynom mit rationalen Koeffizienten, welches mindestens eine echt komplexe Nullstelle besitzt. Zeige, dass die Galoisgruppe der Nullstellen von  $f(X)$  mindestens ein Element der Ordnung 2 besitzt.

### Lösung.

- Variante über den Hauptsatz:* Das Polynom  $X^2 - 2$  hat die Nullstellen  $\pm\sqrt{2}$ ; ein primitives Element der Nullstellen ist  $\sqrt{2}$ , und daher können wir den Hauptsatz verwenden, um Auskunft über die Zwischenerweiterungen von  $\mathbb{Q}(\sqrt{2})$  zu erhalten: Diese stehen in 1:1-Korrespondenz zu den Untergruppen der Galoisgruppe der beiden Nullstellen. Diese ist  $\{\text{id}, \sigma\}$ , wobei  $\sigma = (1, 2)$ ; es gibt also genau zwei Untergruppen, entsprechend den Zwischenerweiterungen  $\mathbb{Q}$  und  $\mathbb{Q}(\sqrt{2})$ .

*Direkte Variante:* Sei  $\mathbb{Q}(\sqrt{2}) \supseteq L \supseteq \mathbb{Q}$  eine Zwischenerweiterung. Nach der Gradformel muss  $[L : \mathbb{Q}]$  gleich 2 oder 1 sein. Im ersten Fall gilt  $L = \mathbb{Q}(\sqrt{2})$ , im zweiten  $L = \mathbb{Q}$ .

- Wir setzen  $f(X) = X^3 - 2$ . Die Nullstellen sind

$$x_1 = \sqrt[3]{2}, \quad x_2 = \omega \sqrt[3]{2}, \quad x_3 = \omega^2 \sqrt[3]{2},$$

wobei  $\omega = \exp(2\pi i/3)$ . Da  $x_1$  kein primitives Element für  $\mathbb{Q}(x_1, x_2, x_3)$  ist, folgt mit Aufgabe 2b) von Blatt 11, dass  $G := \text{Gal}_{\mathbb{Q}}(x_1, x_2, x_3) = S_3$ .

Nun gibt es die Zwischenerweiterung  $\mathbb{Q}(x_1, x_2, x_3) \supseteq \mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ . Ihr Grad über  $\mathbb{Q}$  ist 3, daher ist der Index der zugehörigen Untergruppe  $H$  der Galoisgruppe ebenfalls 3. Explizit ist sie nach Aufgabe 5b) von Blatt 13 durch

$$H = \{\text{id}, (2, 3)\}$$

gegeben. Damit kann man nachrechnen, dass  $H$  kein Normalteiler in  $G$  ist: Denn die Konjugation von  $(2, 3) \in H$  durch  $(1, 2) \in G$  ist

$$(1, 2) \circ (2, 3) \circ (1, 2)^{-1} = (1, 3)$$

und liegt also nicht in  $H$ .

*Bemerkung:* Man kann sich auch die Motivation über die Zwischenerweiterung sparen und direkt die Untergruppe  $H$  angeben.

- c) Seien  $x_1, \dots, x_n$  die Nullstellen von  $f(X)$ . Dann definieren wir eine Permutation  $\sigma \in S_n$  durch die Forderung

$$x_{\sigma(i)} = \overline{x_i}$$

für  $i = 1, \dots, n$ . Diese Permutation liegt tatsächlich in der Galoisgruppe: Denn gilt  $H(x_1, \dots, x_n) = 0$  für ein Polynom  $H \in \mathbb{Q}[X_1, \dots, X_n]$ , so gilt auch

$$H(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = H(\overline{x_1}, \dots, \overline{x_n}) = \overline{H(x_1, \dots, x_n)} = \overline{0} = 0.$$

Nun gilt  $\sigma^2 = \text{id}$ , denn es gilt

$$x_{\sigma^2(i)} = x_{\sigma(\sigma(i))} = \overline{\overline{x_{\sigma(i)}}} = \overline{\overline{x_i}} = x_i$$

für alle  $i = 1, \dots, n$ . Damit ist also die Ordnung von  $\sigma$  gleich 1 oder 2. Die Voraussetzung, dass mindestens eine Nullstelle echt komplex ist, garantiert nun, dass  $\sigma \neq \text{id}$  ist; also hat  $\sigma$  Ordnung 2.

*Bemerkung:* Unter der der Korrespondenz des Hauptsatzes entspricht die Untergruppe  $\{\text{id}, \sigma\}$  der Zwischenerweiterung  $\mathbb{Q}(x_1, \dots, x_n) \cap \mathbb{R}$ . Wenn man  $\mathbb{Q}(t) = \mathbb{Q}(x_1, \dots, x_n)$  schreibt, kann man Erzeuger dieser Zwischenerweiterung explizit bestimmen:

$$\mathbb{Q}(t)^{\{\text{id}, \sigma\}} = \mathbb{Q}(t + \bar{t}, t \cdot \bar{t}) = \mathbb{Q}(2\text{Re}(t), \text{Re}(t)^2 + \text{Im}(t)^2) = \mathbb{Q}(\text{Re}(t), \text{Im}(t)^2).$$

Man kann auch explizit das Minimalpolynom von  $t$  über  $\mathbb{Q}(t)^{\{\text{id}, \sigma\}}$  angeben: Es lautet

$$X^2 - (t + \bar{t})X + t \cdot \bar{t}.$$

## Aufgabe 2. Wurzelausdrücke

- Sei  $x$  eine durch Wurzeln ausdrückbare Zahl und  $x'$  ein galoissch konjugiertes von  $x$ . Zeige, dass  $x'$  ebenfalls durch Wurzeln ausdrückbar ist, und zwar durch denselben Wurzel Ausdruck wie  $x$ .
- Zeige, dass jede primitive  $n$ -te Einheitswurzel durch Wurzeln, deren Exponenten höchstens  $\max\{2, \frac{n-1}{2}\}$  sind, ausgedrückt werden kann.

## Aufgabe 3. Normalteiler

- Sei  $G$  eine Gruppe mit  $G \neq \{\text{id}\}$ . Finde zwei verschiedene Normalteiler in  $G$ .
- Sei  $G$  eine beliebige Gruppe. Zeige, dass das Zentrum von  $G$  ein Normalteiler in  $G$  ist.
- Ist die symmetrische Gruppe  $S_5$  einfach?

## Lösung.

- Stets sind die Untergruppen  $\{\text{id}\}$  und  $G$  Normalteiler (wieso?). Nach Voraussetzung sind das zwei verschiedene.
- Das Zentrum enthält diejenigen Elemente  $\tau \in G$ , für die für alle  $\sigma \in G$  die Identität  $\sigma \circ \tau \circ \sigma^{-1} = \tau$  gilt (äquivalent:  $\sigma \circ \tau = \tau \circ \sigma$ ).

Zum Nachweis der Normalteilereigenschaft sei  $\tau \in Z(G)$  und  $\sigma \in G$  beliebig gegeben. Dann müssen wir zeigen, dass  $\sigma \circ \tau \circ \sigma^{-1}$  ebenfalls in  $Z(G)$  liegt. Das ist klar, denn wie bemerkt ist dieses Element gerade gleich  $\tau \in Z(G)$ .

- c) Nein, denn die Untergruppe  $A_5 \subseteq S_5$  ist ein Normalteiler: Sei  $\tau \in A_5$  und  $\sigma \in S_5$ . Dann gilt

$$\operatorname{sgn}(\sigma \circ \tau \circ \sigma^{-1}) = \operatorname{sgn} \sigma \cdot \operatorname{sgn} \tau \cdot (\operatorname{sgn} \sigma)^{-1} = \operatorname{sgn} \tau = 1,$$

also liegt das konjugierte Element  $\sigma \circ \tau \circ \sigma^{-1}$  wieder in  $A_5$ .

*Bemerkung:* Völlig analog zeigt man, dass auch die Gruppen  $S_n$ ,  $n \geq 3$  jeweils nicht einfach sind.

#### Aufgabe 4. Diedergruppen

- Bestimme explizit die Symmetriegruppe eines ebenen regelmäßigen  $n$ -Ecks in der Ebene, die sog. *Diedergruppe*  $D_n \subseteq S_n$ . Zeige, dass diese von zwei Elementen erzeugt werden kann und insgesamt  $2n$  Elemente enthält.
- Zeige, dass der Index von  $D_4$  in  $S_4$  gleich 3 ist.
- Zeige, dass  $D_4$  kein Normalteiler in  $S_4$  ist.

#### Aufgabe 5. Auflösbarkeit von Gleichungen

- Finde ein normiertes irreduzibles Polynom  $f(X)$  fünften Grads mit rationalen Koeffizienten, sodass die Gleichung  $f(X) = 0$  lösbar ist.
- Zeige, dass die Gleichung  $X^5 - 23X + 1 = 0$  nicht lösbar ist.

#### Lösung.

- Ein Beispiel ist das Polynom  $f(X) = X^5 - 2$ . Dessen Nullstellen sind nämlich  $\zeta^i \sqrt[5]{2}$ ,  $i = 0, \dots, 4$ , wobei  $\zeta$  eine primitive fünfte Einheitswurzel ist. Da primitive Einheitswurzeln durch Wurzeln ausdrückbar sind (Satz 5.25) und die Zahl  $\sqrt[5]{2}$  sogar ganz sicher durch Wurzeln ausdrückbar ist, sind die Lösungen der Gleichung  $f(X) = 0$  also durch Wurzeln ausdrückbar.
- Wir zeigen, dass das Polynom  $f(X) = X^5 - 23X + 1$  irreduzibel ist und genau zwei nicht reelle Nullstellen besitzt. Dann folgt nämlich aus Hilfssatz 5.39, dass die Galoisgruppe der Nullstellen die volle  $S_5$  ist, und diese ist nicht lösbar (siehe Seite 196 oben).

*Nachweis der Irreduzibilität:* Rationale Nullstellen besitzt  $f(X)$  keine, denn diese könnten nur Teiler von 1 sein, aber  $\pm 1$  sind keine Nullstellen. Bleibt zu zeigen, dass  $f(X)$  nicht in Faktoren der Grade 2 und 3 zerfällt. Nach dem Satz von Gauß genügt es, Faktoren mit ganzzahligen Koeffizienten auszuschließen. Aus dem Ansatz

$$f(X) = (a + bX + cX^2) \cdot (d + eX + fX^2 + gX^3)$$

mit ganzzahligen Koeffizienten  $a, b, c, d, e, f, g$  folgen die Gleichungen

$$\begin{aligned} 1 &= ad, \\ -23 &= ae + bd, \\ 0 &= be + af + cd, \\ 0 &= ag + bf + ce, \\ 0 &= cf + bg, \\ 1 &= cg. \end{aligned}$$

Mit einigem Rechnen sieht man:  $a = d = \pm 1$ ,  $c = g = \pm 1$ ,  $f = -b$ ,  $e = cb^2 - a$ ,  $cb^2 - a + b = \mp 23$ . Daraus erhält man die Beziehung

$$b \cdot (cb + 1) = \mp 22.$$

Daraus folgen nur acht Fälle für  $b$ :  $b = 1$ ,  $b = 2$ ,  $b = 11$ ,  $b = 22$  und jeweils mit negativem Vorzeichen. Alle Fälle führen zu einem Widerspruch.

*Nachweis der Nullstelleneigenschaft:* Am einfachsten zeigt man das numerisch: Die Nullstellen sind

$$x_1 \approx -2,20,$$

$$x_2 \approx 0,04,$$

$$x_3 \approx 2,18,$$

$$x_4 \approx -0,01 - 2,19i,$$

$$x_5 \approx -0,01 + 2,19i.$$

Alternativ führt man eine Kurvendiskussion, kann sich so den groben Verlauf des reellen Graphen erschließen und daraus auch ablesen, dass es genau drei reelle Nullstellen gibt.

#### **Aufgabe 6.** *Kriterium für Konstruierbarkeit*

Sei  $x$  eine algebraische Zahl und  $t$  ein primitives Element zu allen galoissch Konjugierten von  $x$ . Zeige, dass  $x$  genau dann konstruierbar ist, wenn der Grad von  $t$  eine Zweierpotenz ist.

**Lösung.** Seien  $t_1, \dots, t_n$  alle galoissch Konjugierten von  $t$ . Nach Proposition 4.4 sind diese ebenfalls primitive Elemente für  $x_1, \dots, x_n$ , d. h. es gilt jeweils  $\mathbb{Q}(t_i) = \mathbb{Q}(t)$ . Folglich gilt insbesondere  $t_1, \dots, t_n \in \mathbb{Q}(t)$ ; also sind alle galoissch Konjugierten von  $t$  in  $t$  rational und es greift Proposition 4.34: Die Zahl  $t$  ist genau dann konstruierbar, wenn der Grad von  $t$  eine Zweierpotenz ist. Mit diesem Vorwissen zeigen wir nun die beiden Richtungen:

„ $\Leftarrow$ “: Klar: Da  $t$  konstruierbar ist, ist auch  $x$  konstruierbar, da  $x$  ja eine in  $t$  rationale Zahl ist.

„ $\Rightarrow$ “: Da  $x$  konstruierbar ist, ist auch jedes galoissch Konjugiertes von  $x$  konstruierbar (wieso?! Mir fehlt ein Beweis dafür, aber die Aussage stimmt). Da  $t$  ein primitives Element dieser galoissch Konjugierten ist, ist  $t$  daher ebenfalls konstruierbar.