Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie
Prof. Marc Nieper-Wißkirchen

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 14 zur Algebra I

Abgabetermin entscheidet ihr!

Aufgabe 1. *Illustrationen des Hauptsatzes*

a) 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.

b) Finde ein normiertes separables Polynom $f(X)$ mit rationalen Koeffizienten, sodass der Index der Untergruppe $\mathrm{Gal}_{\mathbb{Q}(\sqrt[3]{2})}(x_1, \ldots, x_n)$ in $\mathrm{Gal}_{\mathbb{Q}}(x_1, \ldots, x_n)$ gleich 3 ist. Dabei seien $x_1, \ldots, x_n$ die Nullstellen von $f(X)$. Ist diese Untergruppe ein Normalteiler?

c) 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.

a) *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 $\{\mathrm{id}, \sigma\}$, 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 $L = \mathbb{Q}$.

b) 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 $\omega = \exp(2\pi\mathrm{i}/3)$. Da x_1 kein primitives Element für $\mathbb{Q}(x_1, x_2, x_3)$ ist, folgt mit Aufgabe 2b) von Blatt 11, dass $G := \mathrm{Gal}_{\mathbb{Q}}(x_1, x_2, x_3) = \mathrm{S}_3$.

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

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

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 $x_1, \ldots, x_n$ die Nullstellen von $f(X)$. Dann definieren wir eine Permutation $\sigma \in \mathrm{S}_n$ durch die Forderung

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

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

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

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

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

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

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

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

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

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

Aufgabe 2. *Wurzelausdrücke*

a) 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 Wurzelausdruck wie x.

b) 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*

a) Sei G eine Gruppe mit $G \neq \{\mathrm{id}\}$. Finde zwei verschiedene Normalteiler in G.

b) Sei G eine beliebige Gruppe. Zeige, dass das Zentrum von G ein Normalteiler in G ist.

c) Ist die symmetrische Gruppe S_5 einfach?

Lösung.

a) Stets sind die Untergruppen $\{\mathrm{id}\}$ und G Normalteiler (wieso?). Nach Voraussetzung sind das zwei verschiedene.

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

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*

a) 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.

b) Zeige, dass der Index von D_4 in S_4 gleich 3 ist.

c) Zeige, dass D_4 kein Normalteiler in S_4 ist.

Aufgabe 5. *Auflösbarkeit von Gleichungen*

a) Finde ein normiertes irreduzibles Polynom $f(X)$ fünften Grads mit rationalen Koeffizienten, sodass die Gleichung $f(X) = 0$ auflösbar ist.

b) Zeige, dass die Gleichung $X^5 - 23\,X + 1 = 0$ nicht auflösbar ist.

Lösung.

a) Ein Beispiel ist das Polynom $f(X) = X^5 - 2$. Dessen Nullstellen sind nämlich $\zeta^i \sqrt[5]{2}$, $i = 0, \ldots, 4$, wobei ζ 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.

b) Wir zeigen, dass das Polynom $f(X) = X^5 - 23\,X + 1$ 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 auflösbar (siehe Seite 196 oben).

Nachweis der Irreduzibilität: Rationale Nullstellen besitzt $f(X)$ keine, denn diese könnten nur Teiler von 1 sein, aber ± 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: $a = d = \pm 1$, $c = g = \tilde{\pm} 1$, $f = -b$, $e = cb^2 - a$, $cb^2 - a + b = \mp 23$. 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

$$\begin{aligned} x_1 &\approx -2{,}20, \\ x_2 &\approx 0{,}04, \\ x_3 &\approx 2{,}18, \\ x_4 &\approx -0{,}01 - 2{,}19\,\mathrm{i}, \\ x_5 &\approx -0{,}01 + 2{,}19\,\mathrm{i}. \end{aligned}$$

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.