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

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 10 zur Algebra I

Abgabe bis 24. Juni 2013, 17:00 Uhr

Aufgabe 1. *Weitere Anwendungen der Gradformel*

a) Sei z eine algebraische Zahl und seien $x, y \in \mathbb{Q}(z)$. Zeige, dass

$$[\mathbb{Q}(z) : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}] = [\mathbb{Q}(z) : \mathbb{Q}(y)] \cdot [\mathbb{Q}(y) : \mathbb{Q}],$$

und gib ein Diagramm zur Veranschaulichung an.

b) Sei a eine algebraische Zahl und $y \in \mathbb{Q}(a)$. Sei f ein normiertes Polynom mit Koeffizienten aus $\mathbb{Q}(y)$, das über $\mathbb{Q}(y)$ auch irreduzibel ist. Sei der Grad von f mindestens 2 und teilerfremd zu $\deg_{\mathbb{Q}(y)} a$. Zeige, dass keine Zahl aus $\mathbb{Q}(a)$ Nullstelle von f sein kann.

c) Beweise oder widerlege: Sei z ein primitives Element zu algebraischen Zahlen x, y. Dann ist $\deg_{\mathbb{Q}} z$ ein Teiler von $\deg_{\mathbb{Q}} x \cdot \deg_{\mathbb{Q}} y$.

Lösung.

a) Aus der Voraussetzung folgt $\mathbb{Q}(x) \subseteq \mathbb{Q}(z)$ und $\mathbb{Q}(y) \subseteq \mathbb{Q}(z)$. Daher kann man das Diagramm

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(z) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(x) \arrow[dr, dash] & & \mathbb{Q}(y) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

zeichnen. Die Behauptung liefert nun einfach die Gradformel, angewendet auf den linken bzw. rechten Zweig.

b) Sei $x \in \mathbb{Q}(a)$ mit $f(x) = 0$. Dann ist f das Minimalpolynom von x über $\mathbb{Q}(y)$, also gilt $\deg_{\mathbb{Q}(y)} x = [\mathbb{Q}(y, x) : \mathbb{Q}(y)] = \deg f$; die Situation können wir in dem Diagramm

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(a) \arrow[d, dash] & \\ & \mathbb{Q}(x, y) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(x) \arrow[dr, dash] & & \mathbb{Q}(y) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

veranschaulichen. Mit der Gradformel folgt die Beziehung

$$\deg_{\mathbb{Q}(y)} a = [\mathbb{Q}(a) : \mathbb{Q}(y)] = [\mathbb{Q}(a) : \mathbb{Q}(x, y)] \cdot [\mathbb{Q}(x, y) : \mathbb{Q}(y)] = [\mathbb{Q}(a) : \mathbb{Q}(x, y)] \cdot \deg f,$$

die wegen $\deg f \geq 2$ ein Widerspruch zur Teilerfremdheitsvoraussetzung ist (sonst wäre $\deg f$ ein echter Teiler von $\deg_{\mathbb{Q}(y)} a$).

Bemerkung: Allgemein gilt für den Grad einer algebraischen Zahl w über einer weiteren algebraischen Zahl u die Formel

$$\deg_{\mathbb{Q}(u)} w = [\mathbb{Q}(u,w) : \mathbb{Q}(u)] = \text{Grad des Minimalpolynoms von } u \text{ über } \mathbb{Q}(w).$$

Nur falls $u \in \mathbb{Q}(w)$, gilt $\mathbb{Q}(u,w) = \mathbb{Q}(w)$, sodass sich dann die Formel noch ein wenig vereinfacht.

c) Das stimmt im Allgemeinen nicht: Setze $x = \sqrt[3]{2}$ und $y = \omega \cdot \sqrt[3]{2}$, wobei $\omega = \exp(2\pi\mathrm{i}/3)$ ist. Dann gilt

$$\begin{aligned} \deg_{\mathbb{Q}} z &= [\mathbb{Q}(z) : \mathbb{Q}] = [\mathbb{Q}(x,y) : \mathbb{Q}] = [\mathbb{Q}(x,\omega) : \mathbb{Q}] \\ &= [\mathbb{Q}(x,\omega) : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}] = 2 \cdot 3 = 6, \\ \deg_{\mathbb{Q}} x \cdot \deg_{\mathbb{Q}} &= 3 \cdot 3 = 9, \end{aligned}$$

aber 6 ist kein Teiler von 9. Dabei war der Wert des hinteren Faktors in der zweiten Zeile der Rechnung klar (Minimalpolynom ist $X^3 - 2$ nach Eisenstein), und dass der vordere Faktor gleich 2 ist, kann man wie folgt begründen: Das Polynom $X^2 + X + 1$ besitzt bekanntermaßen ω als Nullstelle und ist über $\mathbb{Q}(x) \subset \mathbb{R}$ irreduzibel, da es vom Grad 2 ist und seine Nullstellen ω und ω^2 echt komplex sind.

Bemerkung: Obige Lösung benötigt gar keine explizite Darstellung des primitiven Elements z.

Bemerkung: Eine ähnliche und richtige Behauptung ist $\deg_{\mathbb{Q}} z \leq \deg_{\mathbb{Q}} x \cdot \deg_{\mathbb{Q}} y$, denn

$$\begin{aligned} \deg_{\mathbb{Q}} z = [\mathbb{Q}(x,y) : \mathbb{Q}] &= [\mathbb{Q}(x,y) : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}] \\ &\leq [\mathbb{Q}(y) : \mathbb{Q}] \cdot [\mathbb{Q}(x) : \mathbb{Q}] = \deg_{\mathbb{Q}} y \cdot \deg_{\mathbb{Q}} x. \end{aligned}$$

(Wieso gilt die Abschätzung?)

Aufgabe 2. *Galoissche Konjugierte*

a) Finde zwei algebraische Zahlen, die nicht zueinander galoissch konjugiert sind.

b) Wie viele galoissch Konjugierte hat die Zahl $\sqrt[4]{3}$?

c) Seien p und q zwei verschiedene Primzahlen. Finde alle galoissch Konjugierten von $\sqrt{p} + \sqrt{q}$.

d) Seien x, y, z algebraische Zahlen, sodass x zu y und y zu z galoissch konjugiert ist. Zeige, dass dann auch x galoissch konjugiert zu z ist.

e) Sei t eine algebraische Zahl. Zeige, dass die Summe von t mit all seinen galoisschen Konjugierten eine rationale Zahl ist. Wie steht es mit dem Produkt?

Lösung.

a) Es gibt [abzählbar] unendlich viele Beispiele. Eines ist $(x,y) = (0,1)$ mit den Minimalpolynomen X bzw. $X - 1$.

b) Die Zahl $\sqrt[4]{3}$ hat insgesamt genau so viele galoissch Konjugierte, wie ihr Grad angibt. Dieser ist 4, denn das Minimalpolynom ist $X^4 - 3$ – die Irreduzibilität ist wegen des Eisenstein-Kriteriums sofort klar. Explizit sind die vier galoissch Konjugierten

$$\sqrt[4]{3}, \quad \mathrm{i}\sqrt[4]{3}, \quad -\sqrt[4]{3}, \quad -\mathrm{i}\sqrt[4]{3}.$$

c) Wir suchen zunächst ein Polynom mit rationalen Koeffizienten, dass $z := \sqrt{p} + \sqrt{q}$ als Nullstelle besitzt:

$$\begin{aligned}
&& z &= \sqrt{p} + \sqrt{q} \\
\Longrightarrow && z^2 &= p + 2\sqrt{p}\sqrt{q} + q^2 \\
\Longleftrightarrow && z^2 - (p+q) &= 2\sqrt{p}\sqrt{q} \\
\Longrightarrow && \Big(z^2 - (p+q)\Big)^2 &= 4pq \\
\Longleftrightarrow && 0 &= z^4 - 2(p+q)^2 z^2 + (p-q)^2
\end{aligned}$$

Kandidat für's Minimalpolynom von z ist also $X^4 - 2(p+q)^2\,X^2 + (p-q)^2$. Die vier Nullstellen dieses Polynoms sind

$$x_1 = \sqrt{p} + \sqrt{q}, \quad x_2 = \sqrt{p} - \sqrt{q}, \quad x_3 = -\sqrt{p} + \sqrt{q}, \quad x_4 = -\sqrt{p} - \sqrt{q};$$

wenn wir seine Irreduzibilität nachgewiesen haben, erkennen wir genau diese Zahlen als die galoissch Konjugierten von z.

Irreduzibilitätsnachweis mit dem Verfahren der Vorlesung:

- Keine der Nullstellen ist ganzzahlig (wieso?), also kann kein Linearfaktor abspalten.
- Für jede zweielementige Auswahl der Nullstellen sind stets nicht beide elementarsymmetrischen Funktionen in den Nullstellen ganzzahlig:

$$\begin{aligned}
&e_1(x_1, x_2) = 2\sqrt{p} \notin \mathbb{Z} \\
&e_1(x_1, x_3) = 2\sqrt{q} \notin \mathbb{Z} \\
&e_1(x_1, x_4) = 0 \in \mathbb{Z}, \qquad \text{aber } e_2(x_1, x_4) = -(p + q + 2\sqrt{p}\sqrt{q}) \notin \mathbb{Z}
\end{aligned}$$

- Kubische Faktoren können nicht abspalten, da die komplementären Faktoren Linearfaktoren wären.

Irreduzibilitätsnachweis mit einem Gradformelargument: Wir haben die Inklusionen $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Dabei gilt $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ (klar) und $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = \deg_{\mathbb{Q}(\sqrt{p})} \sqrt{q} = 2$ (zeigt man wie bei Aufgabe 5 von Blatt 9). Also folgt mit der Gradformel $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Da z ein primitives Element für diese Erweiterung ist (wieso?), ist also der Grad von z über $\mathbb{Q}$ gleich 4. Somit muss obiges Polynom irreduzibel sein – es kann kein Polynom niedrigeren Grads geben, das ebenfalls normiert ist, rationale Koeffizienten hat und z als Nullstelle besitzt.

Bemerkung: Reduktion modulo p (oder q) funktioniert nicht: Modulo p erhält man das reduzible Polynom $(X^2 - q)^2$. Auch kann nicht aus der Irreduzibilität von $g(X) = X^2 - 2(p+q)\,X + (p-q)^2$ die des eigentlich zu untersuchenden Polynoms $g(X^2)$ gefolgert werden. Ein einfaches Gegenbeispiel, das die Unmöglichkeit eines solchen Schlusses zeigt, ist das Polynom $h(X) = X - 1$: Dieses ist irreduzibel, aber $h(X^2) = X^2 - 1 = (X+1) \cdot (X-1)$ ist reduzibel.

d) *Variante 1 (mit Vieta):* Sei $m(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ das Minimalpolynom von t und $t_1, \ldots, t_n$ seine Nullstellen (also alle galoissch Konjugierten von t). Nach dem Vietaschen Satz gilt dann

$$\begin{aligned}
(-1)^n a_0 &= e_n(t_1, \ldots, t_n) = t_1 \cdots t_n, \\
a_{n-1} &= e_1(t_1, \ldots, t_n) = t_1 + \cdots + t_n,
\end{aligned}$$

also sind Summe und Produkt der galoissch Konjugierten bis auf Vorzeichen durch die Koeffizienten a_0 bzw. a_{n-1} des Minimalpolynoms gegeben und daher rational.

Variante 2 (mit Wirkung der galoisschen Gruppe): Seien $t_1, \ldots, t_n$ alle galoissch Konjugierten von t, also die Nullstellen des Minimalpolynoms von t. Dann wollen wir zeigen, dass die Summe der t_i invariant unter der Wirkung der galoisschen Gruppe ist und daher rational sein muss: Sei also $\sigma \in \mathrm{Gal}(t_1, \ldots, t_n)$ beliebig. Dann gilt in der Tat

$$\sigma \cdot (t_1 + \cdots + t_n) = t_{\sigma(1)} + \cdots + t_{\sigma(n)} = t_1 + \cdots + t_n.$$

Analog kann man mit dem Produkt verfahren.

e) Seien m_x, m_y und m_z die Minimalpolynome von x, y bzw. z. Dann gilt nach Voraussetzung $m_x = m_y$ und $m_y = m_z$, also auch $m_x = m_z$. Damit sind x und z zueinander galoissch konjugiert.

Aufgabe 3. *Eine konkrete Galoisgruppe*

Bestimme die Galoisgruppe der vier Nullstellen des Polynoms $X^4 + 1$.

Lösung.

1. Die vier Nullstellen sind

$$x_1 = \xi, \quad x_2 = \xi^3, \quad x_3 = \xi^5, \quad x_4 = \xi^7,$$

wobei $\xi = \exp(2\pi \mathrm{i}/8)$ eine primitive achte Nullstelle ist.

2. Es gilt

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\xi, \xi^3, \xi^5, \xi^7) = \mathbb{Q}(\xi),$$

also ist $t := \xi$ ein primitives Element.

3. Für die vier Nullstellen gilt jeweils $x_i = h_i(t)$, wobei

$$\begin{aligned} h_1(X) &= X, \\ h_2(X) &= X^3, \\ h_3(X) &= X^5, \\ h_4(X) &= X^7. \end{aligned}$$

4. Das Minimalpolynom von t ist $f(X) = X^4 + 1$: Die Irreduzibilität bestätigt das Eisenstein-Kriterium angewendet auf

$$f(X+1) = X^4 + 4\,X^3 + 6\,X^2 + 4\,X + 2$$

mit $p = 2$. (Alternative Irreduzibilitätsbegründung: Das Polynom $f(X)$ ist gerade das achte Kreisteilungspolynom.)

5. Die vier galoissch Konjugierten von t sind daher gerade die obigen vier Nullstellen:

$$t_1 = \xi, \quad t_2 = \xi^3, \quad t_3 = \xi^5, \quad t_4 = \xi^7.$$

6. Damit können wir die Elemente der Galoisgruppe auflisten:

t_i	$h_1(t_i)$	$h_2(t_i)$	$h_3(t_i)$	$h_4(t_i)$	σ_i
t_1	x_1	x_2	x_3	x_4	id
t_2	x_2	x_1	x_4	x_3	$(1,2) \circ (3,4)$
t_3	x_3	x_4	x_1	x_2	$(1,3) \circ (2,4)$
t_4	x_4	x_3	x_2	x_1	$(1,4) \circ (2,3)$

Aufgabe 4. *Polynome sind blind für galoissch Konjugierte*

a) Zeige, dass zwei algebraische Zahlen t und t' genau dann zueinander konjugiert sind, wenn jedes Polynom mit rationalen Koeffizienten, welches t als Nullstelle hat, auch t' als Nullstelle hat.

b) Seien t und t' zueinander konjugierte algebraische Zahlen und f ein Polynom mit rationalen Koeffizienten. Zeige, dass dann auch $x := f(t)$ und $x' := f(t')$ zueinander konjugiert sind.

Lösung.

a) „$\Longleftarrow$“: Sei m_t das Minimalpolynom von t. Dieses hat sicherlich t als Nullstelle. Nach Voraussetzung ist daher auch t' eine Nullstelle. Also haben t und t' beide m_t als Minimalpolynom und sind daher galoissch Konjugierte.

„$\Longrightarrow$“ (schon im Skript als Proposition 4.2): Sei m_t das gemeinsame Minimalpolynom von t und t' und sei $f \in \mathbb{Q}[X]$ ein Polynom, das t als Nullstelle hat. Dann haben f und m_t also die gemeinsame Nullstelle t. Da m_t irreduzibel ist, folgt mit dem abelschen Irreduzibilitätssatz (Satz 3.10), dass f ein Vielfaches von m_t ist. Somit ist jede Nullstelle von m_t, insbesondere t', auch Nullstelle von f.

b) Es ist klar, dass x und x' wieder algebraische Zahlen sind. Sei m_x das Minimalpolynom von $x = f(t)$. Dann gilt

$$0 = m_x(x) = m_x(f(t)) = (m_x \circ f)(t),$$

das Polynom $m_x \circ f$ besitzt also t als Nullstelle. Nach Teilaufgabe a) besitzt dieses Polynom dann auch t' als Nullstelle, also gilt

$$m_x(x') = m_x(f(t')) = (m_x \circ f)(t') = 0.$$

Somit ist x' ebenfalls Nullstelle des Minimalpolynoms von x und somit zu x galoissch konjugiert.

Aufgabe 5. *Gegenbeispiele*

Zeige an jeweils einem Beispiel, dass

a) Hilfssatz 4.3 auf Seite 118

b) Proposition 4.4 auf Seite 119

falsch werden, wenn man von den dort vorkommenden Zahlen $x_1, \ldots, x_n$ nicht voraussetzt, dass sie die gesamten Lösungen (mit Vielfachheiten) einer Polynomgleichung mit rationalen Koeffizienten sind, sondern stattdessen beliebige algebraische Zahlen erlaubt.

Lösung.

a) Hilfssatz 4.3 lautet:

> Seien $x_1, \ldots, x_n$ die Lösungen (mit Vielfachheiten) einer Polynomgleichung mit rationalen Koeffizienten. Ist dann $V(X_1, \ldots, X_n)$ ein Polynom mit rationalen Koeffizienten, so sind die galoissch Konjugierten von $t = V(x_1, \ldots, x_n)$ alle von der Form $t' = V(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, wobei σ eine n-stellige Permutation ist.

Es gibt zahlreiche Gegenbeispiele, wenn man die Voraussetzung, dass die x_i *alle* Lösungen *einer* Polynomgleichung mit rationalen Koeffizienten sind, fallen lässt. Sei etwa $n = 1$, $x_1 = \mathrm{i}$ und $V(X_1) = X_1$. Dann stimmt es nicht, dass alle galoissch Konjugierten von $t = V(x_1) = \mathrm{i}$

von der (wegen $n = 1$ einzig möglichen) Form $t' = V(x_1)$ sind. Denn $-\mathrm{i}$ ist ja auch noch ein galoissch Konjugiertes von t.

Ein komplizierteres Gegenbeispiel ist $n = 2$, $x_1 = 17$, $x_2 = \mathrm{i}$, $V(X_1, X_2) = X_2$.

b) Proposition 4.4 lautet:

> Seien $x_1, \ldots, x_n$ die Lösungen (mit Vielfachheiten) einer Polynomgleichung mit rationalen Koeffizienten. Ist dann t ein primitives Element zu $x_1, \ldots, x_n$, so ist auch jedes galoissch Konjugierte t' von t ein primitives Element von $x_1, \ldots, x_n$.

Auch hier gibt es zahlreiche Gegenbeispiele, wenn man die Voraussetzung fallen lässt. Sei etwa $n = 1$, $x_1 = \omega\sqrt[3]{2}$ und $t = x_1$, wobei $\omega = \exp(2\pi\mathrm{i}/3)$ eine primitive dritte Einheitswurzel ist. Dann stimmt es nicht, dass das galoissch Konjugierte $t' = \sqrt[3]{2}$ ebenfalls ein primitives Element von $\mathbb{Q}(x_1)$ ist: Denn $\mathbb{Q}(t') \subseteq \mathbb{R}$, aber $\mathbb{Q}(x_1) \not\subseteq \mathbb{R}$.