Mathematisches Institut der Universität München
Wintersemester 2009/10

Stefan Gille
Lukas-Fabian Moser

Algebra – Lösungsideen zum 13. Übungsblatt

Aufgabe 1.

i) Das Polynom $f = X^3 - 3X - 3$ ist irreduzibel in $\mathbb{Q}[X]$ nach Eisenstein (oder mangels rationaler Nullstelle). Ich behaupte, daß f genau eine einzige reelle Nullstelle a besitzt: Es gibt mindestens eine nach dem Zwischenwertsatz, und mit einer gewöhnlichen Kurvendiskussion sieht man, daß es keine weitere geben kann. (Alle Nullstellen sind einfach, da f als irreduzibles Polynom in Charakteristik 0 automatisch separabel ist.) Es sei $K = \mathbb{Q}(a)$. Dann ist $K \subset \mathbb{R}$, also zerfällt f über K noch nicht. Den Zerfällungskörper L erhält man also erst durch Adjunktion einer (und damit beider) Nullstellen b, c des quadratischen Polynoms $f/(X - a) \in K[X]$ an K, also hat L Grad 2 über K und damit Grad 6 über $\mathbb{Q}$.
Da ein Element von $\mathrm{Gal}(L/\mathbb{Q})$ die Nullstellen a, b, c permutiert und durch die Wirkung auf die Nullstellen eindeutig bestimmt ist, haben wir einen injektiven Restriktionshomomorphismus $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\{a, b, c\})$. Letztere Gruppe ist aber isomorph zur S_3 und hat insbesondere 6 Elemente, ebenso wie die Galoisgruppe. Also folgt $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

ii) Das Polynom $f = X^4 - X^2 - 3 \in \mathbb{F}_5[X]$ ist irreduzibel: Denn es hat keine Nullstelle (ausprobieren!) und ist auch nicht Produkt zweier Polynome vom Grad 2, wie man durch einen Ansatz sieht: Aus

$$f = (X^2 + aX + b)(X^2 + cX + d) = X^4 + (a + c)X^3 + (ac + b + d)X^2 + (ad + bc)X + bd$$

folgt $c = -a$, $a(d - b) = 0$, $b + d - a^2 = -1$, $bd = -3$. Der Fall $d = b$ kann nicht sein, da sonst 3 ein Quadrat wäre; also ist $a = 0$, und es folgt $b + d = -1$, also $d = -(1 + b)$ und damit $3 = b(1 + b) = b^2 + b$. Die Diskriminante dieser quadratischen Gleichung ist aber 3, und das ist kein Quadrat, d.h. die Gleichung besitzt keine Lösung.[1]
Sei nun L der Körper, der aus $\mathbb{F}_5$ durch Adjunktion einer Nullstelle a von f entsteht (also etwa $L = \mathbb{F}_5[X]/(f)$ mit $a := \overline{X}$). Ich behaupte, daß L bereits der Zerfällungskörper von f ist: Dazu genügt es zu zeigen, daß $L/\mathbb{F}_5$ normal ist, aber laut Vorlesung ist *jede* Erweiterung zwischen endlichen Körpern galoissch und insbesondere normal. Die Galoisgruppen sind immer zyklisch, also hier isomorph zu $\mathbb{Z}/4\mathbb{Z}$, erzeugt vom Frobeniushomomorphismus $x \mapsto x^5$.

Aufgabe 2.

i) Nach Vorlesung sind die Nullstellen von Φ_n genau die primitiven n-ten Einheitswurzeln in $\mathbb{C}$. Das normierte Polynom, dessen Nullstellen *alle* n-ten Einheitswurzeln sind, ist $X^n - 1$, und jede n-te Einheitswurzel ist primitive d-te Einheitswurzel für genau ein $d \mid n$. Daraus folgt die angegebene Formel.

ii) Dem Tip folgend, zeige ich zuerst $\Phi_{pn} \mid \Phi_n(X^p)$ und muß dafür zeigen: Ist ζ eine primitive pn-te Einheitswurzel, so ist $\Phi_n(\zeta^p) = 0$, d.h. ζ^p ist primitive n-te Einheitswurzel. Das folgt aus $\mathrm{ord}(\zeta^p) = (\mathrm{ord}\,\zeta)/p = n$ wegen $p \mid \mathrm{ord}\,\zeta = np$.

[1] Dieses immergleiche Argument könnte man einmal zu einem allgemeinen Irreduzibilitätskriterium für Polynome der Form $X^4 + pX^2 + q$ auszubauen versuchen!

Ist $p \nmid n$, so gilt auch $\Phi_n \mid \Phi_n(X^p)$: Denn ist ζ eine primitive n-te Einheitswurzel, so auch ζ^p, denn aus $1 = (\zeta^p)^m = \zeta^{pm}$ folgt $n \mid pm$, also $n \mid m$. – Da aber Φ_n und Φ_{pn} teilerfremd sind (sie sind irreduzibel und verschieden), folgt zusammen sogar $\Phi_{pn} \mid \Phi_n(X^p)/\Phi_n$.
Um nun die behaupteten Gleichheiten zu beweisen, müssen wir (da die Polynome alle normiert sind und einander teilen) nur die Grade vergleichen. Aber es ist $\deg \Phi_n = \varphi(n)$, und die Formeln $\varphi(pn) = p\varphi(n)$ für $p \mid n$ und $\varphi(pn) = p\varphi(n) - \varphi(n) = (p-1)\varphi(n)$ für $p \nmid n$ folgen aus den Rechenregeln für φ aus der Vorlesung.

iii) Man erhält

$$\begin{aligned}
\Phi_5 &= \frac{\Phi_1(X^5)}{\Phi_1} = \frac{X^5-1}{X-1} = X^4+X^3+X^2+X+1,\\
\Phi_6 &= \frac{\Phi_2(X^3)}{\Phi_2} = \frac{X^3+1}{X+1} = X^2-X+1,\\
\Phi_{12} &= \Phi_6(X^2) = X^4-X^2+1,\\
\Phi_{15} &= \frac{\Phi_5(X^3)}{\Phi_5} = \frac{X^{12}+X^9+X^6+X^3+1}{X^4+X^3+X^2+X+1} = \cdots = X^8-X^7+X^5-X^4+X^3-X+1.
\end{aligned}$$

Aufgabe 3.

i) $L \subset M$ folgt daraus, daß $\sigma_i = \mathrm{id}$ ist für ein bestimmtes i. Jedes L_i ist endlich über K, und wegen $M = K(L_1)(L_2)\dots(L_n)$ folgt $[M:K] < \infty$.
Für die Normalität zeige ich zunächst: Ist $a \in L$ mit Minimalpolynom $f \in K[X]$, und ist $b \in \overline{K}$ eine weitere Nullstelle von f, so gibt es ein i mit $\sigma_i(a) = b$ (insbesondere gilt also $b \in M$). Das sieht man so: Es gibt einen K-Homomorphismus $\varphi : K(a) \to \overline{K}$ mit $a \mapsto b$. Dieser läßt sich fortsetzen zu einem Homomorphismus $\widetilde{\varphi} : L \to \overline{K}$, und dann muß $\widetilde{\varphi} = \sigma_i$ für ein geeignetes i sein.
Jetzt behaupte ich: M wird über K erzeugt von den Nullstellen *aller* Minimalpolynome von Elementen von L. Sei nämlich M' der von diesen Nullstellen erzeugte Körper. Nach dem gerade Bewiesenen gilt $M' \subset M$. Umgekehrt gilt aber $L_i \subset M'$ für alle i (und damit $M \subset M'$), denn für jedes $a \in L$ und jedes i ist $\sigma_i(a)$ eine Nullstelle des Minimalpolynoms von a, liegt also in M'. Insgesamt ist also $M = M'$, und M'/K ist normal nach Satz III.3.2 der Vorlesung.

ii) Es genügt zu zeigen, daß $L_i \subset M'$ gilt für alle i. Aber für $a \in L$ und jedes i ist einerseits $a \in M'$, andererseits liegt $\sigma_i(a)$ als weitere Nullstelle des Minimalpolynoms von a ebenfalls wieder in M' (denn M'/K ist ja normal), und das zeigt die Behauptung.

iii) Jedes L_i ist isomorph zu L, also ebenfalls separabel über K und damit auch über jedem größeren Körper. Also entsteht M durch sukzessive Adjunktion von separablen Elementen und ist damit wieder separabel über K.

iv) Das kann man so ähnlich beweisen wie in i), oder aber direkt: Wegen $L = K(a)$ ist $L_i = K(a_i)$ mit $a_i = \sigma_i(a)$. Die a_i sind außerdem genau die Nullstellen des Minimalpolynoms von a, und wegen $L = K(a_1, \dots, a_n)$ folgt die Behauptung.

Aufgabe 4. Der Satz von Artin besagt ja: Ist L ein Körper und G eine endliche Gruppe von Automorphismen von L, so ist L/L^G eine endliche Galoiserweiterung mit Galoisgruppe G (insbesondere $[L : L^G] = |G|$). Es genügt also, einen Körper zu konstruieren, dessen Automorphismengruppe eine zu S_n isomorphe Untergruppe besitzt.
Dafür nehmen wir einen beliebigen Grundkörper K und setzen $L := K(X_1, \dots, X_n)$ (der Quotien-

tenkörper des Polynomrings $K[X_1, \ldots, X_n]$). Für jedes $\sigma \in S_n$ ist der Ringhomomorphismus

$$\begin{aligned} \varphi_\sigma : K[X_1, \ldots, X_n] &\to K[X_1, \ldots, X_n], \\ X_i &\mapsto X_{\sigma(i)} \end{aligned}$$

bijektiv (wegen $\varphi_{\sigma^{-1}} = \varphi_\sigma^{-1}$) und induziert damit einen Automorphismus $\tau_\sigma : L \to L$. Die Vorschrift $\sigma \mapsto \tau_\sigma$ liefert einen injektiven Gruppenhomomorphismus $S_n \to \mathrm{Aut}(L)$ (nachrechnen!).
Die resultierende Galoiserweiterung $L^{S_n} \subset L$ läßt sich so deuten: L besteht aus allen rationalen Funktionen in den Unbestimmten $X_1, \ldots, X_n$, der Fixkörper L^{S_n} nur aus denjenigen, die in den X_i symmetrisch sind.

Zusatzaufgabe.

i) $\mathbb{Q}(\zeta)$ ist $\mathbb{Q}$-Vektorraum mit Basis $1, \zeta, \ldots, \zeta^{s-1}$. Insbesondere kann man jedes Element schreiben als $g(\zeta)$ mit einem eindeutigen $g \in \mathbb{Q}[X]$, $\deg g < s$. Um aber $g \in \mathbb{Z}[X]$ zu zeigen, muß man dieses Argument ein wenig variieren: Statt $\mathbb{Q}(\zeta)$ betrachten wir nur den Ring $\mathbb{Z}[\zeta]$. Dieser besitzt als abelsche Gruppe die Basis $1, \zeta, \ldots, \zeta^{s-1}$, und damit kann man jedes Element schreiben als $g(\zeta)$ mit einem eindeutigen $g \in \mathbb{Z}[X]$, $\deg g < s$. Man muß nur noch einsehen, daß $f(\zeta^d) \in \mathbb{Z}[\zeta]$ ist. Dafür genügt es sicherlich, $f \in \mathbb{Z}[X]$ zu zeigen, und das steht schon in der Vorlesung: Ein normiertes Polynom über $\mathbb{Q}$, das ein normiertes Polynom über $\mathbb{Z}$ teilt, liegt in $\mathbb{Z}[X]$; das wendet man auf $f \mid X^n - 1$ an. (Für $d < 0$ benötigen wir auch, daß ζ in $\mathbb{Z}[\zeta]$ invertierbar ist, aber das liegt an $\zeta^n = 1$.)
Außerdem hängt g_d nur von ζ^d ab, und wegen $\zeta^n = 1$ hängt dieses seinerseits nur von der Klasse von d in $\mathbb{Z}/n\mathbb{Z}$ ab.

ii) Wir rechnen jetzt in $\mathbb{Z}[\zeta]/(p)$: Dies ist ein $\mathbb{Z}/p\mathbb{Z}$-Vektorraum mit Basis $\overline{1}, \ldots, \overline{\zeta}^{s-1}$ (das folgt aus der entsprechenden Aussage für $\mathbb{Z}[\zeta]$). Es ist aber $\overline{g_p(\zeta)} = \overline{f(\zeta^p)} = \overline{f(\zeta)}^p = 0$ nach dem Satz vom Frobeniushomomorphismus (der auf $\mathbb{Z}/p\mathbb{Z}$ selbst als Identität wirkt). Also hat das Polynom $\overline{g_p} \in (\mathbb{Z}/p\mathbb{Z})[X]$ verschwindende Koeffizienten, d.h. $p \mid g_p$.

iii) Die g_d, $d \in \mathbb{Z}$, sind nach i) nur endlich viele verschiedene Polynome. Unter ihren endlich vielen Koeffizienten gibt es also einen betragsmäßig größten; nennen wir ihn N. Ist nun $p > N$ eine Primzahl, so ist jeder Koeffizient von g_p nach ii) durch p teilbar, aber auf jeden Fall im Betrag kleiner als p, und das geht nur, wenn $g_p = 0$ ist.

iv) Das ist eine rein zahlentheoretische Aussage ohne Bezug zu Einheitswurzeln: Wir müssen zu r ein geschickt gewähltes Vielfaches von n dazuaddieren, um eine Zahl r' zu bekommen, die durch keine Primzahl $\leqslant N$ teilbar ist.
Das bekommt man durch die Festlegung

$$r' := r + n \prod_{\substack{p \leqslant N \text{ prim} \\ p \nmid r}} p.$$

Ist nämlich $p \leqslant N$ eine Primzahl, so kann sie kein Teiler von r' sein: denn entweder es gilt $p \mid r$, dann teilt p nicht den zweiten Summanden (beachte $p \nmid n$ wegen $\mathrm{ggT}(r, n) = 1$). Oder es gilt $p \nmid r$, dann teilt p den zweiten Summanden. In jedem Fall teilt p nur genau einen der beiden Summanden, also keinesfalls die Summe r'.

v) In iii) haben wir bewiesen: Es gibt ein N, so daß $f(\zeta^p) = 0$ ist, wenn $p > N$ prim ist. Das gilt nun aber für *alle* Nullstellen von f (wir haben von ζ nichts weiter verwendet, als daß $f(\zeta) = 0$ ist; nicht einmal die g_d und N hängen von der bestimmten Wahl der Nullstelle ab). Insgesamt haben wir also gezeigt: Ist ζ eine Nullstelle von f, so auch ζ^p, wenn p eine Primzahl $> N$ ist. Insbesondere folgt durch wiederholte Anwendung, daß auch ζ^m Nullstelle von f ist, wenn m nur Primfaktoren $> N$ hat, und mit iv) folgt $f(\zeta^r) = f(\zeta^{r'}) = 0$.

Jede primitive n-te Einheitswurzel hat nach Vorlesung die Form ζ^r mit einem zu n teilerfremden r. Also sind alle primitiven n-ten Einheitswurzeln Nullstellen von f; da umgekehrt jede Nullstelle von f primitive n-te Einheitswurzel sein muß (denn sie ist Bild von ζ unter einem Körperautomorphismus von $\mathbb{Q}(\zeta)$), sind die Nullstellen von f genau die primitiven n-ten Einheitswurzeln. Von ihnen gibt es $\varphi(n)$ Stück, und da f als irreduzibles Polynom über $\mathbb{Q}$ separabel ist, folgt $\deg f = \varphi(n)$.