Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Frühjahr 2004, Thema Nr. 2

Aufgabe 1 (*Frühjahr 2004*) Geben Sie eine Untergruppe der Ordnung 21 der symmetrischen Gruppe S_7 an.

Lösung. Wir wählen eine Untergruppe U und einen Normalteiler N von S_7 mit $|U| = 3$ und $|N| = 7$ (und $U \cap N = \{e\}$). Es ist dann bekanntlich UN eine Untergruppe von S_7 mit $|UN| = 21$. Das Problem: Was wählen wir für N?
Andere Lösung: Wir wählen zwei Untergruppen U und N von S_7 mit $|U| = 3$ und $|N| = 7$ (und $U \cap N = \{e\}$) und $UN = NU$. Es ist dann bekanntlich UN eine Untergruppe von S_7 mit $|UN| = 21$.
Wegen der Primzahlordnungen von U und N sind beide Gruppen zyklisch, $U = \langle\sigma\rangle$ und $N = \langle\tau\rangle$; und die Bedingung $UN = NU$ lautet dann: Zu (i, j) gibt es (r, s) mit

$$\sigma^i\tau^j = \tau^r\sigma^s.$$

Dies folgt bereits aus

$$\sigma\tau\sigma^{-1} = \tau^k \text{ für ein } k.$$

Wir wählen nun $\tau = (1234567)$ und bestimmen σ so, daß $\sigma\tau\sigma^{-1} = \tau^k$ für ein k gilt: Wir probieren es zuerst mit

$$\tau^2 = (1357246).$$

Wegen

$$\sigma\tau\sigma^{-1} = (\sigma(1)\,\sigma(2)\,\sigma(3)\,\sigma(4)\,\sigma(5)\,\sigma(6)\,\sigma(7)) = (1357246)$$

erhalten wir

$$\sigma = (235)\,(476),$$

ein Element der Ordnung 3.
Mit $U = \langle\sigma\rangle$ und $N = \langle\tau\rangle$ erhalten wir durch UN eine Untergruppe der S_7 von der Ordnung 21.

Aufgabe 2 (*Frühjahr 2004*) Der Ring $R = \{n + m\sqrt{-2} \,|\, n, m \in \mathbb{Z}\}$ ist bekanntlich ein euklidischer Ring bezüglich der Norm $N(n + m\sqrt{-2}) = n^2 + 2m^2$.

(a) Zeigen Sie, daß 11 ein zerlegbares und 13 ein unzerlegbares Element in R ist.

(b) Zeigen Sie, daß der Restklassenring $R/13R$ ein Körper ist. Aus wieviel Elementen besteht er?

(c) Verwenden Sie den chinesischen Restsatz, um $R/11R$ als direktes Produkt von zwei Körpern darzustellen.

Lösung. (a) Für die 11 können wir eine Zerlegung angeben:

$$11 = (3+\sqrt{-2})\,(3-\sqrt{-2})\,,$$

dabei sind die Elemente $3\pm\sqrt{-2}$ keine Einheiten, es gilt nämlich $N(3\pm\sqrt{-2}) = 11$ und Einheiten haben die Norm 1 ($1 = N(1) = N(aa^{-1}) = N(a)N(a^{-1})$, beachte: $N(a) \in \mathbb{N}_0$).
Angenommen, das Element 13 ist zerlegbar, $13 = ab$ mit Nichteinheiten a und b. Dann gilt

$$13 \cdot 13 = 169 = N(13) = N(a)N(b)\,, \;\text{ also }\; N(a) = 13 \;\text{ und }\; N(b) = 13\,.$$

Aber es gibt kein Element $n+m\sqrt{-2} \in R$ mit $n^2+2m^2 = 13$. Somit ist 13 unzerlegbar.

(b) Da 13 unzerlegbar ist, ist $(13) = 13R$ ein maximales Ideal. Somit ist $R/(13)$ ein Körper. Offenbar gilt $|R/(13)| = 169$.

(c) Wir betrachten die Ideale $I = (3+\sqrt{-2})$ und $J = (3-\sqrt{-2})$ von R. Wegen $N(3\pm\sqrt{-2}) = 11$ sind I und J maximal und R/I und R/J Körper. Wegen der Maximalität und der Verschiedenheit von I und J gilt $I+J = R$, so daß I und J teilerfremd sind. Weiter gilt $I \cap J = (11)$, da $I \cap J = IJ = (11)$. Nach dem chinesischen Restsatz erhalten wir

$$R/(11) \cong R/I \times R/J\,.$$

Aufgabe 3 (*Frühjahr 2004*)

(a) Geben Sie die Anzahl und die Grade der irreduziblen Teiler des Polynoms $X^{45}-1$ im Polynomring $\mathbb{Z}[X]$ an. Wie lautet der irreduzible Teiler vom Grad 6?

(b) Die Einheitswurzeln $\xi = \mathrm{e}^{\frac{2\pi\mathrm{i}}{9}}$ bzw. $\alpha = \mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}$ erzeugen die Körper

$$K_9 = \mathbb{Q}(\xi) \;\text{ bzw. }\; K_3 = \mathbb{Q}(\alpha)\,.$$

Geben Sie die Bahn von ξ unter den Galoisgruppen $G = \mathrm{Gal}(K_9/\mathbb{Q})$ bzw. $H = \mathrm{Gal}(K_9/K_3)$ an.

(c) Geben Sie die Zerlegung des Polynoms X^6+X^3+1 in irreduzible Faktoren im Polynomring $K_3[X]$ an.

Lösung. Bekanntlich ist X^n-1 ein Produkt von Kreisteilungspolynomen, es gilt

$$X^n - 1 = \prod_{0<d|n} \Phi_d\,,$$

wobei Φ_d das d-te Kreisteilungspolynom vom Grad $\varphi(d)$ ist; seine Wurzeln sind die primitiven d-ten Einheitswurzeln. Damit haben wir

$$X^{45}-1 = \Phi_1\Phi_3\Phi_5\Phi_9\Phi_{15}\Phi_{45}\,.$$

Das Polynom hat damit 6 Teiler mit den Graden $\varphi(1) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(9) = 6$, $\varphi(15) = 8$, $\varphi(45) = 24$. Da die Kreisteilungspolynome über $\mathbb{Q}$ irreduzibel sind, haben wir alle irreduziblen Teiler bestimmt. Der irreduzible Teiler vom Grad 6 lautet

$$\Phi_9 = \frac{X^9-1}{\Phi_1\Phi_3} = \frac{X^9-1}{(X-1)(X^2+X+1)} = X^6+X^3+1\,.$$

(b) Es sind $K_9/\mathbb{Q}$ und K_9/K_3 galoissch mit $[K_9:\mathbb{Q}] = \varphi(9) = 6$ und $[K_9:K_3] = \frac{\varphi(9)}{2} = 3$. Es gilt somit $|G| = 6$ und $|H| = 3$. Genauer gilt

$$G = \{\xi \mapsto \xi,\ \xi \mapsto \xi^2,\ \xi \mapsto \xi^4,\ \xi \mapsto \xi^5,\ \xi \mapsto \xi^7,\ \xi \mapsto \xi^8\}\,.$$

und

$$H = \{\xi \mapsto \xi,\ \xi \mapsto \xi^4,\ \xi \mapsto \xi^7\},$$

da diese Elemente aus G die Ordnung 1 bzw. 3 haben und dies somit die eindeutig bestimmte Untergruppe der Ordnung 3 von G ist.
Die Gruppen G und H operieren auf der Menge $\{1, \xi, \xi^2, \ldots, \xi^8\}$, wir erhalten als Bahnen von ξ:

$$G \cdot \xi = \{\xi,\ \xi^2,\ \xi^4,\ \xi^5,\ \xi^7, \xi^8\} \text{ und } H \cdot \xi = \{\xi,\ \xi^4,\ \xi^7\}.$$

(c) Wegen $\xi^3 = \alpha$ hat das Polynom $P = X^3 - \alpha \in K_3[X]$ das Element $\xi \in K_9$ als Wurzel. Da P normiert und über K_3 irreduzibel ist (die Wurzeln ξ, ξ^4, ξ^7 von P liegen nicht in K_3, ist P das Minimalpolynom von ξ und somit ein (irreduzibler) Teiler von $X^6 + X^3 + 1$. Eine Polynomdivision liefert

$$X^6 + X^3 + 1 = (X^3 - \alpha)(X^3 + 1 + \alpha).$$

Jetzt ist höchstens noch eine Zerlegung von $X^3 + 1 + \alpha$ denkbar. Jede solche echte Zerlegung würde aber eine Wurzel von $X^6 + X^3 + 1$ liefern; diese Wurzeln sind die primitiven 9-ten Einheitswurzeln $\xi,\ \xi^2,\ \xi^4,\ \xi^5,\ \xi^7, \xi^8$; die Existenz einer echten Zerlegung hätte also zur Folge, daß eine und damit alle primitiven 9-ten Einheitswurzeln in K_3 liegen – ein Widerspruch, $X^3 + 1 + \alpha$ ist somit irreduzibel.

Aufgabe 4 (*Frühjahr 2004*) Für Primzahlpotenzen q bezeichne F_q den Körper aus q Elementen.

(a) Bestimmen Sie die kleinste Zweierpotenz $q = 2^m$, so daß der Körper F_q eine primitive 17-te Einheitswurzel enthält.

(b) Es sei α ein erzeugendes Element der multiplikativen Gruppe des Körpers F_{256}. Welchen Grad hat das Minimalpolynom f von α über F_2? Welche Potenzen von α sind Nullstellen von f?

(c) Es sei α wie in (b). Zeigen Sie unter Benutzung der Galois-Theorie, daß das Polynom

$$g(X) = (X - \alpha)(X - \alpha^4)(X - \alpha^{16})(X - \alpha^{64})$$

Koeffizienten in F_4 hat.

Lösung. (a) Ein Element $\xi \in F_q$ ist genau dann eine primitive 17-te Einheitswurzel, wenn $\xi^{17} = 1$ und $\xi \neq 1$. Ein solches Element existiert genau dann in $F_q^\times$, wenn

$$17 \mid |F_q^\times| = q - 1 = 2^m - 1.$$

Wir testen dies für die ersten möglichen m:

$$17 \nmid 2^1 - 1,\ 17 \nmid 2^2 - 1,\ 17 \nmid 2^3 - 1,\ 17 \nmid 2^4 - 1,\ 17 \nmid 2^5 - 1,\ 17 \nmid 2^6 - 1,\ 17 \nmid 2^7 - 1,\ 17 \mid 2^8 - 1.$$

Damit ist $q = 256$ für $m = 8$ die gesuchte Zahl.

(b) Wegen $F_2(\alpha) = F_{2^8}$ gilt $\deg f = 8$. Weiter ist die Körpererweiterung F_{2^8}/F_2 galoissch, wobei die Galoisgruppe Γ vom Frobenius-Automorphismus $\tau : x \mapsto x^2$ erzeugt wird, $\Gamma = \{\mathrm{id}, \tau, \tau^2, \ldots, \tau^7\}$. Es sind somit α, α^2, α^4, α^8, α^{16}, α^{32}, α^{64}, α^{128} Konjugierte von α und damit Nullstellen von f.

(c) Multipliziert man $g(X)$ aus, so sieht man, daß die Koeffizienten von $g(X)$ Summen von Produkten der Elemente α, α^4, α^{16} und α^{64} sind. Die Behauptung folgt also, wenn wir begründen können, daß diese vier Elemente in F_4 liegen, es liegen dann auch Summen von Produkten dieser Elemente in F_4.
Der Zwischenkörper F_4 von F_{2^8}/F_2 ist der Fixkörper von $\Gamma' = \{\mathrm{id}, \tau^2, \tau^4, \tau^6\}$. Wegen

$$\tau^2(\alpha) = \alpha^4,\ \tau^2(\alpha^4) = \alpha^{16},\ \tau^2(\alpha^{16}) = \alpha^{64},\ \tau^2(\alpha^{64}) = \alpha$$

hält τ^2 und damit auch alle anderen Elemente von Γ' die Koeffizienten von $g(X)$ fest. Damit folgt, daß diese in F_4 liegen.