Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Herbst 2003, Thema Nr. 1

Aufgabe 1 (*Herbst 2003*) Es sei G eine Gruppe der Ordnung n. Zeigen Sie:

(a) G ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

(b) Ist $n = 2u$ mit ungeradem u, so hat G einen Normalteiler vom Index 2.

Lösung: (a) Das ist der *Satz von Cayley*: Betrachte zu $a \in G$ die Abbildung

$$\tau_a : G \to G,\ g \mapsto a\,g\,.$$

Es ist τ_a eine Bijektion von G, d. h. $\tau_a \in S_G$. Weiter ist die Abbildung

$$\tau : G \to S_G,\ a \mapsto \tau_a$$

offenbar ein Monomorphismus. Damit ist G zu einer Untergruppe von S_G isomorph. Da die Gruppen S_n und S_G isomorph sind, ist somit G zu einer Untergruppe von S_n isomorph.
(b) Nach dem Teil (a) ist G zu einer Untergruppe U von S_{2u} isomorph. Einen Isomorphismus von G auf U bezeichnen wir mit σ. Bekanntlich ist A_{2u} ein Normalteiler vom Index 2 in S_{2u}. Wir betrachten nun $N := \sigma^{-1}(A_{2u})$ und begründen, daß N ein Normalteiler vom Index 2 in G ist.
Bekanntlich ist N ein Normalteiler von G. Es bleibt also zu zeigen, daß der Index von N in G gleich 2 ist. Nach dem Satz von Cauchy gibt es in G ein Element a der Ordnung 2. Wir betrachten nun das Element $\sigma(a)$ der Ordnung 2 in S_{2u}. Es ist $\sigma(a)$ ein Produkt von elementfremden Transpositionen, und zwar von genau u Stück, da nämlich $\sigma(a)$ keinen Fixpunkt hat, es wäre nämlich sonst $a = e$ (betrachte $\tau_a : g \mapsto a\,g$). Damit ist also $\sigma(a) \in S_{2u}$ eine ungerade Permutation, d. h. $\sigma(G) = U \not\subseteq A_{2u}$ (d. h. $a \in G \setminus N$, woraus folgt, daß der Index von N in G größer gleich 2 ist – das werden wir aber nicht brauchen). Wir wenden nun den ersten Isomorphiesatz an: Da $\sigma(a) \in U \setminus A_{2u}$ und da A_{2u} ein Normalteiler vom Index 2 in S_{2u} ist, gilt $U\,A_{2u} = S_{2u}$. Betrachte $V := U \cap A_{2u}$. Nach dem 1. Isomorphisatz gilt

$$V = U \cap A_{2u} \trianglelefteq U \ \text{ und } \ U\,A_{2u}/A_{2u} \cong U/U \cap A_{2u}\,,$$

woraus wegen $S_{2u} = U\,A_{2u}$ die Behauptung folgt.

Aufgabe 2 (*Herbst 2003*) Beweisen Sie:

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}\,.$$

Lösung. Es ist

$$\zeta := \mathrm{e}^{2\pi\mathrm{i}/5} = \cos\frac{2\pi}{5} + \mathrm{i}\sin\frac{2\pi}{5} \neq 1$$

eine Wurzel von $X^5 - 1$, also eine Wurzel von $X^4 + X^3 + X^2 + X + 1$, d. h.

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0\,.$$

Die Zahlen $1, \zeta, \zeta^2, \zeta^3, \zeta^4$ bilden die Ecken eines regulären Fünfecks am Einheitskreis. Die reelle Zahl $\cos\frac{2\pi}{5}$ erhält man dabei als die Hälfte von $\zeta+\zeta^4$:

$$\cos\frac{2\pi}{5} = \frac{1}{2}(\zeta+\zeta^4)\,.$$

Gesucht ist nun ein quadratisches Polynom, dessen Nullstelle $\zeta+\zeta^4$ ist, dabei sollen die Nullstellen lauten:

$$\frac{-1\pm\sqrt{5}}{2}\,.$$

Als Polynom kommt also nur $p = X^2+X-1$ in Frage. Zu begründen bleibt damit nur, daß $\zeta+\zeta^4$ eine Nullstelle von p ist:

$$(\zeta+\zeta^4)^2+(\zeta+\zeta^4)-1 = \zeta^2+2\zeta^5+\zeta^8+\zeta+\zeta^4-1 = \zeta^2+1+\zeta^3+\zeta+\zeta^4 = 0\,.$$

Damit ist die Gleichung

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$$

begründet.

Aufgabe 3 (*Herbst 2003*) Begründen oder widerlegen Sie die folgenden Aussagen:

(a) Ist p eine Primzahl, sind $1 \le i \le j$ natürlichen Zahlen, sind K bzw. L Körper mit p^i bzw. p^j Elementen, so ist K zu einem Teilkörper von L isomorph.

(b) Für jede Primzahl p und jede natürliche Zahl a gilt: Ist $X^2 \equiv a \mod p$ lösbar in $\mathbb{Z}$, so auch $X^4 \equiv a \mod p$.

(c) Die Zahl $\zeta_{13} = \mathrm{e}^{2\pi\mathrm{i}/13}$ ist mit Zirkel und Lineal konstruierbar.

(d) Es seien $\alpha_1, \alpha_2 \in \mathbb{C}$ algebraische Zahlen und $K_i = \mathbb{Q}(\alpha_i)$, weiter sei $L = \mathbb{Q}(\alpha_1, \alpha_2)$ und es gelte $K_1 \cap K_2 = \mathbb{Q}$. Dann gilt

$$[L:\mathbb{Q}] \text{ teilt } [K_1:\mathbb{Q}]\cdot[K_2:\mathbb{Q}]\,.$$

Lösung.

(a) Falsch: Der Körper $\mathbb{F}_{2^2}$ ist nicht isomorph zu einem Teilkörper von $\mathbb{F}_{2^3}$, es gilt nämlich

$$[\mathbb{F}_{2^2}:\mathbb{F}_2] = 2 \text{ und } [\mathbb{F}_{2^3}:\mathbb{F}_2] = 3\,.$$

(b) Falsch: Gesucht ist ein $a \in \mathbb{N}$ mit $X^2 \equiv a \mod p$ ist lösbar und $X^4 \equiv a \mod p$ ist nicht lösbar für eine Primzahl p.

Nach Probieren stellt man fest, daß $p = 2$ kein Gegenbeispiel liefert, ebenso $p = 3$; schließlich kommt $p = 5$. Hier stellt man fest (indem man die Zahlen 0, 1, 2, 3, 4 einsetzt:

$$X^4 \equiv 0, 1 \mod 5\,.$$

Gesucht ist nun ein $a \neq 0, 1$, so daß $X^2 \equiv a \mod 5$ lösbar ist. Mit Hilfe des quadratischen Reziprozitätsgesetzes (oder durch Probieren) findet man, daß $X^2 \equiv 4 \mod 5$ lösbar ist. Man beachte, daß $X^4 \equiv 4 \mod 5$ nicht lösbar ist.

(c) Falsch: Die Zahl ζ_{13} ist Nullstelle des irreduziblen Polynoms $X^{12}+X^{11}+\cdots+X+1 \in \mathbb{Q}[X]$. Damit hat $\mathbb{Q}(\zeta_{13})$ den Grad 12 über $\mathbb{Q}$. Konstruierbare Elemente haben aber eine Zweierpotenz als Grad über $\mathbb{Q}$.

(d) Falsch: Es sind $\alpha_1 := \sqrt[3]{2}$ und $\alpha_2 := \sqrt[3]{2}e^{2\pi i/3}$ zwei Nullstellen des über $\mathbb{Q}$ irreduziblen Polynoms $p = X^3 - 2$. Für $K_1 = \mathbb{Q}(\alpha_1)$ und $K_2 = \mathbb{Q}(\alpha_2)$ und $L = \mathbb{Q}(\alpha_1, \alpha_2)$ gilt

$$[K_1 : \mathbb{Q}] = 3\,,\ [K_2 : \mathbb{Q}] = 3\,,\ [L : \mathbb{Q}] = 6\,,\ K_1 \cap K_2 = \mathbb{Q}\,,\ \text{ aber } 6 \nmid 9\,.$$

Aufgabe 4 (*Herbst 2003*) Es seien K ein Körper mit 81 Elementen und G die Gruppe aller Automorphismen von K. Bestimmen Sie:

(a) die Länge der Bahnen der Operation von G auf K, sowie

(b) die Anzahl der Bahnen gegebener Länge.

Lösung. Es ist $K = \mathbb{F}_{3^4}$. Es gilt $[\mathbb{F}_{3^4} : \mathbb{F}_3] = 4$. Damit ist die Galoisgruppe G zyklisch von der Ordnung 4; sie wird vom Frobeniusautomorphismus $\Phi : x \mapsto x^3$ erzeugt: $G = \{\mathrm{Id}, \Phi, \Phi^2, \Phi^3\}$. Der Körper $\mathbb{F}_3$ ist der Fixkörper von G, der Körper $\mathbb{F}_{3^2}$ ist der Fixkörper von $H = \langle \Phi^2 \rangle$.
(a) Die Operation von G auf K ist gegeben durch

$$\cdot : \begin{cases} G \times K & \to & K \\ (\Phi^i, x) & \mapsto & \Phi^i(x) \end{cases} .$$

Die Bahnlängen sind $|G \cdot x|$ für die Bahnen $G \cdot x = \{\mathrm{Id}(x), \Phi(x), \Phi^2(x), \Phi^3(x)\}$, $x \in K$. Dabei ist bekanntlich die Bahnlänge ein Teiler der Gruppenordnung, hier kommen also nur 1, 2 und 4 in Frage.
Ist $x \in \mathbb{F}_3$, so ist x im Fixkörper von G, d. h. $G \cdot x = \{x\}$; die Bahnlänge ist also 1.
Ist $x \in \mathbb{F}_{3^2} \setminus \mathbb{F}_3$, so ist x im Fixkörper von H, d. h. $G \cdot x = \{x, x^3\}$; die Bahnlänge ist also 2.
Ist $x \in \mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}$, so ist x im Fixkörper von $\{\mathrm{Id}\}$, d. h. $G \cdot x = \{x, x^3, x^9, x^{27}\}$; die Bahnlänge ist also 4, falls wir erklären können, daß die vier Elemente x, x^3, x^9, x^{27} verschieden sind: Da $x \in K^\times$, gilt $o(x) \mid 80$. Wäre zum Beispiel $x^9 = x^{27}$, so folgte $18 \mid 80$, was nicht möglich ist. Man beachte, daß $x = x^9$ auch ausgeschlossen ist, da x nicht im Fixkörper von H ist.
(b) Die Bahnen bilden eine Partition von K.
Eine Bahn $G \cdot x$ hat genau dann die Länge 1, wenn $x \in \mathbb{F}_3$ liegt. Also gibt es genau $3 = |\mathbb{F}_3|$ Bahnen der Länge 1.
Eine Bahn $G \cdot x$ hat genau dann die Länge 2, wenn $x \in \mathbb{F}_{3^2} \setminus \mathbb{F}_3$ liegt. Also gibt es genau $3 = \frac{1}{2}|\mathbb{F}_{3^2} \setminus \mathbb{F}_3|$ Bahnen der Länge 2.
Eine Bahn $G \cdot x$ hat genau dann die Länge 4, wenn $x \in \mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}$ liegt. Also gibt es genau $18 = \frac{1}{4}|\mathbb{F}_{3^4} \setminus \mathbb{F}_{3^2}|$ Bahnen der Länge 4.