Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Herbst 2004, Thema Nr. 1

Aufgabe 1 Bestimmen Sie je eine 2-Sylowgruppe in

(a) der symmetrischen Gruppe S_4,

(b) der alternierenden Gruppe A_5,

(c) der alternierenden Gruppe A_6.

Lösung: (a) Es gilt $|S_4| = 2^3 \cdot 3$. Eine 2-Sylowgruppe hat daher 8 Elemente. Die Gruppe $D = \langle (1234), (13) \rangle$ ist eine Untergruppe von S_4 der Ordnung 8 (sie ist zur Diedergruppe isomorph).

(b) Es gilt $|A_5| = 2^2 \cdot 3 \cdot 5$. Eine 2-Sylowgruppe hat daher 4 Elemente. Die Gruppe $V = \langle (12)(34), (13)(24) \rangle$ ist eine Untergruppe von A_4 der Ordnung 4 (sie ist zur Kleinschen Vierergruppe isomorph).

(c) Es gilt $|A_6| = 2^3 \cdot 3^2 \cdot 5$. Eine 2-Sylowgruppe hat daher 8 Elemente. Die Gruppe

$$W = \langle (12)(34), (13)(24), (12)(56) \rangle$$

ist eine Untergruppe von A_6 der Ordnung 8, es gilt nämlich

$$\begin{aligned} &\langle (12)(34), (13)(24), (12)(56) \rangle = \\ &\qquad = \{(1), (12)(34), (13)(24), (12)(56), (14)(23), (34)(56), (1234)(56), (1423)(56)\}. \end{aligned}$$

Aufgabe 2 Bestimmen Sie alle natürlichen Zahlen n im Intervall $0 \leq n \leq 999$ mit

$$n^2 \equiv 500 \mod 1000.$$

Lösung: Beachte, daß $1000 = 2^3 \cdot 5^3$. Falls $n^2 \equiv 500 \mod 1000$, so folgt $2 \mid n^2 - 500$ und $5 \mid n^2 - 500$, also $n^2 \equiv 0 \mod 2$ und $n^2 \equiv 0 \mod 5$. Es folgt $n \in 10\mathbb{Z}$. Damit gilt

$$n \in \{10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, \ldots, 990\}.$$

Es gilt

$$(10+100)^2 = 10^2 + 2 \cdot 1000 + 100^2 \equiv 10^2 \mod 1000,$$

so daß wir also modulo 1000 nur die Zahlen $10, 20, \ldots, 90$ untersuchen müssen. Und hier gilt

$$\begin{aligned} &10^2 \not\equiv 500 \mod 1000, 20^2 \not\equiv 500 \mod 1000, 30^2 \not\equiv 500 \mod 1000, \\ &40^2 \not\equiv 500 \mod 1000, 50^2 \equiv 500 \mod 1000, 60^2 \not\equiv 500 \mod 1000, \\ &70^2 \not\equiv 500 \mod 1000, 80^2 \not\equiv 500 \mod 1000, 90^2 \not\equiv 500 \mod 1000. \end{aligned}$$

Damit erhalten wir also genau die Zahlen

$$n \in \{50, 150, 250, \ldots, 950\}\,.$$

Aufgabe 3 Bestimmen Sie im Polynomring $\mathbb{Q}[X]$ den größten gemeinsamen Teiler der beiden Polynome

$$f(X) = X^5 - X^3 - X^2 + 1 \text{ und } g(X) = X^4 - 2X^3 + 2X - 1\,.$$

Lösung: Division mit Rest liefert:

$$f(X) = g(X)\,(X+2) + 3\,(X^3 - X^2 - X + 1)\,,$$
$$g(X) = 3\,(X^3 - X^2 - X + 1)\,\frac{1}{3}\,(X-1)$$

sodaß also $3\,(X^3 - X^2 - X + 1)$ ein ggT von $f(X)$ und $g(X)$ ist.

Aufgabe 4 Bestimmen Sie die Ordnung der Galoisgruppe des Polynoms

$$X^4 - 4X^3 + 4X^2 - 2$$

über $\mathbb{Q}$.
Hinweis: Beseitigen Sie durch geeignete Substitution den Term dritter Ordnung.

Lösung: Nach Eisenstein mit $p = 2$ ist das Polynom $f = X^4 - 4X^3 + 4X^2 - 2$ irreduzibel über $\mathbb{Q}$ und somit Minimalpolynom seiner vier verschiedenen Wurzeln im Zerfällungskörper $L \subseteq \mathbb{C}$ von f über $\mathbb{Q}$. Gesucht ist der Grad $[L : \mathbb{Q}]$ von L über $\mathbb{Q}$, dieser Grad ist die Ordnung der Galoisgruppe, die gesucht ist. Dazu bestimmen wir die Wurzeln von f mithilfe des Hinweises: Es gilt

$$g = f(X+1) = (X+1)^4 - 4\,(X+1)^3 + 4\,(X+1)^2 - 2 = \ldots = X^4 - 2X^2 - 1\,.$$

Die Wurzeln von g erhalten wir einfach, es sind dies

$$\sqrt{1+\sqrt{2}},\ -\sqrt{1+\sqrt{2}},\ \sqrt{1-\sqrt{2}},\ -\sqrt{1-\sqrt{2}}\,.$$

Damit lauten wegen $0 = g(a) = f(a+1)$ die Wurzeln von f

$$a_1 = \sqrt{1+\sqrt{2}}+1\,,\ a_2 = -\sqrt{1+\sqrt{2}}+1\,,\ a_3 = \sqrt{1-\sqrt{2}}+1\,,\ a_4 = -\sqrt{1-\sqrt{2}}+1\,.$$

Beachte, daß die Wurzel a_1 und a_2 reell sind, a_3 und a_4 hingegen imaginär sind. Außerdem gilt $L = \mathbb{Q}(a_1, a_3)$ und damit

$$[L : \mathbb{Q}] = [\mathbb{Q}(a_1, a_3) : \mathbb{Q}(a_1)] \cdot [\mathbb{Q}(a_1) : \mathbb{Q}]\,.$$

Nachdem wir bereits festgestellt haben, daß f das Minimalpolynom von a_1 ist, gilt $[\mathbb{Q}(a_1) : \mathbb{Q}] = 4$, es bleibt also $[\mathbb{Q}(a_1, a_3) : \mathbb{Q}(a_1)]$ zu bestimmen. Dazu ermitteln wir das Minimalpolynom von a_3 über $\mathbb{Q}(a_1)$, es gilt

$$(a_3 - 1)^2 = 1 - \sqrt{2} = 1 - [(a_1 - 1)^2 - 1]\,,$$

so daß a_3 Wurzel des Polynoms $X^2 - 2X + a_1^2 - 2a_1 \in \mathbb{Q}(a_1)$ ist. Da a_3 imaginär ist, ist dies zwingend das Minimalpolynom von a_3, es folgt

$$[L : \mathbb{Q}] = [\mathbb{Q}(a_1, a_3) : \mathbb{Q}(a_1)] \cdot [\mathbb{Q}(a_1) : \mathbb{Q}] = 2 \cdot 4 = 8\,.$$

Damit ist begründet, daß die Galoisgruppe die Ordnung 8 hat.

Aufgabe 5 Es sei $K = \mathbb{F}_{3^3}$ der Körper mit 27 Elementen.

(a) Was ist die Ordnung der Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{F}_3)$? In wieviele und wie lange Bahnen zerfällt K unter der Operation von G?

(b) Wieviele normierte Polynome vom Grad 3 in $\mathbb{F}_3[X]$ sind irreduzibel?

(c) Zeigen Sie: Das Polynom $X^3 + aX^2 + bX + c$ ist genau dann irreduzibel, wenn das Polynom $X^3 - aX^2 + bX - c$ irreduzibel ist.

(d) Zerlegen Sie das Polynom

$$p(X) = X^{26} - 1 \in \mathbb{F}_3[X]$$

in irreduzible Faktoren im Ring $\mathbb{F}_3[X]$.

Lösung: (a) Jede endliche Erweiterung endlicher Körper ist galoissch (mit zyklischer Galoisgruppe, die vom Frobeniusautomorphismus $\tau : a \mapsto a^3$ erzeugt wird), somit ist die Ordnung der Galoisgruppe der Grad der Körpererweiterung: Wegen $[K : \mathbb{F}_3] = 3$ ist die Ordnung der Galoisgruppe damit 3.
Die Galoisgruppe besteht aus den drei Elementen

$$\mathrm{Id} : a \mapsto a\,,\ \tau : a \mapsto a^3\,,\ \tau^2 : a \mapsto a^9\,.$$

Die Galoisgruppe operiert auf K vermöge

$$\cdot : G \times K \to K\,,\ (\varphi, a) \mapsto \varphi(a)\,.$$

Wir unterscheiden zwei Fälle:

(i) $a \in \mathbb{F}_3$. Dann gilt für die Bahn $G \cdot a$ wegen $a^3 = a$

$$G \cdot a = \{a\} \ \text{ und damit } \ |G \cdot a| = 1\,.$$

Wegen $|\mathbb{F}_3| = 3$ gibt es drei solcher Bahnen.

(ii) $a \in K \setminus \mathbb{F}_3$. Dann gilt für die Bahn $G \cdot a$ wegen $a^3 \neq a$, $a^9 \neq a$, $a^9 \neq a^3$

$$G \cdot a = \{a, a^3, a^9\} \ \text{ und damit } \ |G \cdot a| = 3\,.$$

Wegen $|K \setminus \mathbb{F}_3| = 24$ gibt es $\frac{24}{3} = 8$ solcher Bahnen.

(b) Es gibt insgesamt $3^3 = 27$ normierte Polynome vom Grad 3. Da ein Polynom vom Grad 3 genau dann irreduzibel über $\mathbb{F}_3$ ist, wenn es keine Wurzel in $\mathbb{F}_3$ hat, sind genau die Polynome unter den 27 existierenden irreduzibel, die weder 0 noch 1 noch -1 als Wurzel haben. Wir zählen die Polynome vom Grad 3, die 0 oder 1 oder -1 als Wurzel haben: Jedes solche Polynom ist ein Produkt eines quadratischen Polynoms mit einem Linearfaktor, d. h.

$$(*) \qquad X^3 + aX^2 + bX + c = (X - d)\,(X^2 + eX + f)\,.$$

Von den neun normierten quadratischen Polynomen sind genau 6 reduzibel: drei mit einer doppelten Wurzel und $\binom{3}{2} = 3$ mit zwei verschiedenen Wurzeln.
Damit erhalten wir $3 \cdot 3 = 9$ verschiedene normierte reduzible Polynome der Art $(*)$ mit irreduziblem quadratischem Faktor $X^2 + eX + f$.
Und ist der Faktor $X^2 + eX + f$ reduzibel, so ist das Polynom in $(*)$ ein Produkt von drei Linearfaktoren; von diesen gibt es 3 mit einer dreifachen Wurzel, 1 mit drei verschiedenen Wurzeln und 6 mit zwei verschiedenen Wurzeln, wobei eine doppelt und eine einfach ist. Das ergibt insgesamt 10 Polynome der Art $(*)$ mit reduziblem quadratischen Faktor.
Damit sind insgesamt 19 reduzibel und somit 8 irreduzibel.

(c) Wir setzen $g = X^3 - aX^2 + bX - c$. Da das Polynom $f = X^3 + aX^2 + bX + c$ genau dann irreduzibel ist, wenn es keine Wurzel in $\mathbb{F}_3$ hat, gilt:

$$\begin{aligned} f \text{ irreduzibel } &\Leftrightarrow \begin{cases} f(0) &= c \neq 0 \\ f(1) &= 1+a+b+c \neq 0 \\ f(2) &= 2+a+2b+c \neq 0 \end{cases} \Leftrightarrow \begin{cases} -c &\neq 0 \\ 1-a+b-c &\neq 0 \\ 2-a+2b-c &\neq 0 \end{cases} \\ &\Leftrightarrow g \text{ irreduzibel } . \end{aligned}$$

(d) Da $\mathbb{F}_{27}$ der Zerfällungskörper von $X^{27} - X$ ist, sind die Wurzeln von $X^{26} - 1$ die von Null verschiedenen Elemente von $\mathbb{F}_{27}$. Damit haben wir bereits

$$X^{26} - 1 = (X-1)(X-2)g$$

mit einem Polynom g vom Grad 24, dessen Wurzeln in $\mathbb{F}_{27}$ liegen. Daher ist g ein Produkt von 8 verschiedenen irreduziblen Polynomen vom Grad 3 über $\mathbb{F}_3$. Mit Probieren erhalten wir vier Stück, weitere vier Stück finden wir mit dem Teil (c):

$$\begin{aligned} g_1 &= X^3 + 2X + 1 \text{ und } g_2 = X^3 + 2X + 2 \\ g_3 &= X^3 + 2X^2 + 1 \text{ und } g_4 = X^3 + X^2 + 2 \\ g_5 &= X^3 + X^2 + 2X + 1 \text{ und } g_6 = X^3 + 2X^2 + 2X + 2 \\ g_7 &= X^3 + X^2 + X + 2 \text{ und } g_2 = X^3 + 2X^2 + X + 1 . \end{aligned}$$

Damit gilt:

$$X^{26} - 1 = (X-1)(X-2)g_1 \cdots g_8 .$$