

Repetitorium zur Algebra

Frühjahr 2004, Thema Nr. 3

Aufgabe 1

- (a) Es sei $K = F_2$ der Körper mit 2 Elementen. Finden Sie ein Polynom f in $K[x]$, das die Kongruenz

$$(x^4 + x^3 + x^2 + 1) \cdot f \equiv x^2 + 1 \pmod{(x^3 + 1)}$$

in $K[x]$ erfüllt.

- (b) Es sei $K = F_3$ der Körper mit 3 Elementen. Gibt es dann zu jedem $g \in K[x]$ ein $f \in K[x]$, so daß die Kongruenz

$$(x^2 + 1) \cdot f \equiv g \pmod{(x^3 + 1)} \quad (*)$$

erfüllt ist?

- (c) Finden Sie in der Kongruenz $(*)$ für $g = 1$ eine Lösung $f \in F_3[x]$.

Lösung: (a) Durch Probieren findet man schnell, daß $f = 0$ und $f = 1$ nicht taugen, $f = x$ hingegen schon:

$$(x^5 + x^4 + x^3 + x^2 + x + 1) \equiv 0 \pmod{(x^3 + 1)}.$$

- (b) Die Frage ist, ob es zu jedem Polynom g Polynome f und h gibt, sodaß

$$(x^2 + 1) \cdot f + (x^3 + 1) \cdot h = g$$

gilt. Das sieht nach dem euklidischen Algorithmus aus: Die Polynome $x^2 + 1$ und $x^3 + 1$ sind teilerfremd. Damit existieren $\tilde{f}$ und $\tilde{h}$ mit

$$(x^2 + 1) \cdot \tilde{f} + (x^3 + 1) \cdot \tilde{h} = 1.$$

Multiplikation dieser Gleichung mit g liefert f und h , nämlich $f = g \cdot \tilde{f}$ und $h = g \cdot \tilde{h}$.

- (c) Hier benötigen wir konkret das Polynom $\tilde{f}$, das hier gleich f ist. Der euklidische Algorithmus liefert:

$$x^3 + 1 = (x^2 + 1) \cdot x - x + 1 \quad \text{und} \quad x^2 + 1 = (-x + 1) \cdot (-x - 1) + 2$$

und damit

$$2 = (x + 1) \cdot (x^3 + 1) + (1 - x - x^2) \cdot (x^2 + 1),$$

d. h.

$$1 = (2x + 2) \cdot (x^3 + 1) + (2 + x + x^2) \cdot (x^2 + 1),$$

damit taugt $f = 2 + x + x^2$.

Aufgabe 2 Es sei $K = F_2$ und $f = x^4 + x^3 + x^2 + x + 1 \in K[x]$. Bestimmen Sie die Galoisgruppe von f über K .

Lösung: Wegen

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

Ist der 5-te Kreisteilungskörper K_5 über K (das ist der Zerfällungskörper von $x^5 - 1$ über K) auch der Zerfällungskörper von f über K . Bekanntlich ist K_n/K dann galoissch, wenn $\text{Char}K \nmid n$. Das ist hier erfüllt, $n = 5$ und $\text{Char}K = 2$. Bekanntlich ist die Galoisgruppe zu einer Untergruppe von $\mathbb{Z}_n^\times$ isomorph und genau dann zu $\mathbb{Z}_n^\times$ isomorph, wenn f irreduzibel über K ist (vgl. Lemma 28.8, Karpfinger/Meyberg, Algebra, 2. Auflage).

Wir begründen nun, daß f irreduzibel über K ist: Wegen $f(0) \neq 0 \neq f(1)$ hat, f keine Wurzel in K . Falls f einen Teiler vom Grad 2 hat, so hat f auch einen irreduziblen Teiler vom Grad 2. Das einzige irreduzible Polynom vom Grad 2 lautet $x^2 + x + 1$. Eine Division mit Rest liefert:

$$f = (x^2 + x + 1)x^2 + x + 1.$$

Damit ist begründet, daß f irreduzibel ist. Damit ist die Galoisgruppe von f über K zu $\mathbb{Z}_5^\times$ isomorph.

Aufgabe 3 Die Diedergruppe D_6 , also die Symmetriegruppe des regulären Sechsecks, und die alternierende Gruppe A_4 haben beide zwölf Elemente.

- (a) Zeigen Sie, daß die Gruppen D_6 und A_4 nicht isomorph sind.
- (b) Geben Sie eine weitere nichtabelsche Gruppe der Ordnung 12 an, die zu den beiden genannten Gruppen nicht isomorph ist.

Lösung: (a) In der Gruppe D_6 gibt es ein Element der Ordnung 6, nämlich $\alpha : \zeta \mapsto e^{\frac{2\pi i}{6}} \zeta$. Die A_4 besteht bekanntlich neben dem Einselement (1) aus den Doppeltranspositionen (12)(34), (13)(24), (14)(23) und den 3-Zyklen (123), (132), (243), (234), (124), (142), (134), (143). Keines der Elemente in der A_4 hat die Ordnung 6. Die beiden Gruppen können also nicht isomorph sein.

(b) Es gibt bekanntlich genau drei nichtisomorphe nichtabelsche Gruppen der Ordnung 12. Das sind D_6 , A_4 und $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$. Das semidirekte Produkt $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ besteht dabei aus den Elementen

$$\mathbb{Z}_3 \times \mathbb{Z}_4 = \{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (2,3)\}.$$

Weiter betrachten wir den Homomorphismus $\theta : \mathbb{Z}_4 \rightarrow \text{Aut}(\mathbb{Z}_3)$, gegeben durch

$$0 \mapsto \text{Id}, \quad 1 \mapsto \alpha : \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 2 \\ 2 \mapsto 1 \end{cases}, \quad 2 \mapsto \alpha^2 : \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 1 \\ 2 \mapsto 2 \end{cases}, \quad 3 \mapsto \alpha^3 : \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 2 \\ 2 \mapsto 1 \end{cases}.$$

Die Verknüpfung $\circ$ in $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ ist erklärt als

$$(a,b) \circ (c,d) := (a + \alpha^b(c), b + d).$$

Hierdurch wird $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ bekanntlich zu einer Gruppe mit 12 Elementen.

Die Gruppe $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ ist nicht abelsch, da z. B.

$$(1,1) \circ (1,0) = (0,1) \neq (2,1) = (1,0) \circ (1,1).$$

Die Gruppe $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ ist auch nicht isomorph zu A_4 bzw. D_6 , da $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ eine zyklische Untergruppe $U = \{(0,0), (0,1), (0,2), (0,3)\}$ der Ordnung 4 hat, die Gruppen A_4 bzw. D_6 jedoch nicht.

Aufgabe 4 Für ein Polynom $f \in \mathbb{R}[x]$ bezeichne f' die Ableitung. Es seien $a_1, \dots, a_n \in \mathbb{R}$ verschiedene reelle Zahlen, und es sei I die Menge aller Polynome $f \in \mathbb{R}[x]$ mit

$$f(a_i) = f'(a_i) = 0 \quad \text{für } i = 1, \dots, n.$$

Zeigen Sie:

- (a) I ist ein Ideal im Polynomring $\mathbb{R}[x]$.
- (b) I wird erzeugt von dem Polynom $\prod_{i=1}^n (x - a_i)^2$.
- (c) Wieviele Ideale besitzt der Faktoring $\mathbb{R}[x]/I$?

Lösung: (a) Da das Nullpolynom in I liegt, ist I nicht leer. Sind f und g aus I und $h \in \mathbb{R}[x]$, so gilt

$$\begin{aligned} (f - g)(a_i) &= f(a_i) - g(a_i) = 0 \quad \text{und} \quad (hf)(a_i) = h(a_i)f(a_i) = 0 \quad \text{und} \\ (f - g)'(a_i) &= f'(a_i) - g'(a_i) = 0 \quad \text{und} \quad (hf)'(a_i) = h'(a_i)f(a_i) + h(a_i)f'(a_i) = 0, \end{aligned}$$

so daß $f - g$ und hf wieder in I liegen. Wegen der Kommutativität von $\mathbb{R}[x]$ ist I ein Ideal von $\mathbb{R}[x]$.

(b) Zu zeigen ist $I = (\prod_{i=1}^n (x - a_i)^2)$.

Es sei $f \in I$. Wegen $f(a_i) = 0 = f'(a_i)$ hat f die n doppelten Wurzeln $a_1, \dots, a_n$. Damit ist $\prod_{i=1}^n (x - a_i)^2$ ein Teiler von f , es folgt $f \in (\prod_{i=1}^n (x - a_i)^2)$.

Es sei $f \in (\prod_{i=1}^n (x - a_i)^2)$. Dann ist f von der Form $f = g \prod_{i=1}^n (x - a_i)^2$ mit einem Polynom $g \in \mathbb{R}[x]$. Offenbar gilt $f(a_i) = 0$ für alle $i = 1, \dots, n$. Wir ermitteln $f'(a_i)$, dazu setzen wir $h := \prod_{i=1}^n (x - a_i)^2$ und beachten, daß $h'(a_i) = 0$; damit erhalten wir:

$$f'(a_i) = g'(a_i)h(a_i) + g(a_i)h'(a_i) = 0.$$

Damit ist die Gleichheit $I = (\prod_{i=1}^n (x - a_i)^2)$ gezeigt.

(c) Wegen $\text{ggT}((x - a_i)^2, (x - a_j)^2) = 1$ für $i \neq j$ sind die Ideale $I_1 = ((x - a_1)^2), \dots, I_n = ((x - a_n)^2)$ paarweise teilerfremd; es gilt $I_i + I_j = \mathbb{R}[x]$ für $i \neq j$. Weiter gilt

$$I = ((x - a_1)^2 \cdots (x - a_n)^2) = ((x - a_1)^2) \cup \cdots \cup ((x - a_n)^2).$$

Nach dem (allgemeinen) chinesischen Restsatz gilt nun:

$$(*) \quad \mathbb{R}[x]/I \cong \mathbb{R}[x]/I_1 \times \cdots \times \mathbb{R}[x]/I_n.$$

Jeder Faktor $\mathbb{R}[x]/I_j$ hat nach dem Korrespondenzsatz genau drei verschiedene Ideale, da jedes solche Ideale mit einem Ideal in $\mathbb{R}[x]$ *korrespondiert*, das $((x - a)^2)$ umfaßt, und hierfür kommen genau die Ideale (1) , $(x - a_j)$, $((x - a_j)^2)$ in Frage. Damit hat der Ring rechts in $(*)$ genau 3^n Ideale. Der Ring $\mathbb{R}[x]/I$ hat wegen der Isomorphie genauso viele.