Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Herbst 2004, Thema Nr. 2

Aufgabe 1 Es seien p, q Primzahlen mit $p < q$. Zeigen Sie:

(a) Im Fall $p \nmid (q-1)$ ist jede Gruppe der Ordnung pq abelsch.

(b) Jede abelsche Gruppe der Ordnung pq ist zyklisch.

(c) Im Fall $p \mid (q-1)$ gibt es eine nichtabelsche Gruppe der Ordnung pq.

Lösung: (a) Ist G eine Gruppe der Ordnung pq, so gilt für die Anzahl n_p der p- bzw. n_q der q-Sylowgruppen:

$$n_p \in \{1, 1+p, 1+2p, \ldots\} \text{ und } n_p \mid q \text{ bzw. } n_q \in \{1, 1+q, 1+2q, \ldots\} \text{ und } n_q \mid p.$$

Wegen $p < q$ folgt aus den Bedingungen für n_q sofort $n_q = 1$. Wegen $n_p \mid q$ gilt $n_p = 1$ oder $n_p = q$. Im Fall $n_p = q$ folgte wegen der ersten Bedingung an n_p sogleich $1 + kp = q$ für ein $k \in \mathbb{N}$ im Widerspruch zu $p \nmid (q-1)$; also gilt auch $n_p = 1$.
Sind P bzw. Q die (einzig existierenden) p- bzw. q-Sylowgruppen von G, die wegen $n_p = 1 = n_q$ Normalteiler von G sind, so ist G wegen der Teilerfremdheit von p und q das innere direkte Produkt der abelschen, da zyklischen Normalteiler P und Q, $G = P \otimes Q$. Da die Faktoren abelsch sind, ist die Gruppe G abelsch.

(b) Ist G eine abelsche Gruppe der Ordnung pq, so ist G nach dem Hauptsatz über endliche abelsche Gruppen isomorph zu $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$; und diese Gruppe ist zyklisch.
Zur Begründung kann man auch den Teil (a) heranziehen: Da G abelsch ist, gilt ebenso $n_p = 1 = n_q$, somit ist $G = P \otimes Q$ für die (einzig existierende) p-Sylowgruppe P bzw. q-Sylowgruppe Q. Da P und Q zyklisch sind mit teilerfremden Ordnungen, ist auch $P \otimes Q$ zyklisch.

(c) Ist p ein Teiler von $q-1$, so gibt es nach dem Satz von Cauchy ein Element $\varphi \in \mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_q^\times$ der Ordung p. Das semidirekte Produkt von $\mathbb{Z}_p$ mit $\mathbb{Z}_q$ mittels des in diesem Fall existierenden nichttrivialen Homomorphismus ist nicht abelsch.

Aufgabe 2 Gegeben ist der Ring $R = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$. Zeigen Sie:

(a) ± 1 sind die einzigen Einheiten in R.

(b) 2 ist ein irreduzibles Element in R aber kein Primelement.

(c) R ist kein faktorieller Ring.

Lösung: (a) Wegen $1 \cdot 1 = 1 = (-1) \cdot (-1)$ sind ± 1 Einheiten in R. Wir zeigen, daß es keine weiteren Einheiten gibt: Ist x eine Einheit in R, so existiert ein $y \in R$ mit $xy = 1$, wegen der Multiplikativität der Normabbildung

$$N : R \setminus \{0\} \to \mathbb{N},\ x = a + b\sqrt{-3} \mapsto a^2 + 3b^2$$

folgt $N(x) = a^2 + 3b^2 = 1$ für die Einheit $x = a + b\sqrt{-3}$. Es folgt somit $b = 0$ und $a = \pm 1$, d. h. $x = \pm 1$.

(b) Angenommen, die $2 \in R$ ist reduzibel, $2 = xy$ mit Nichteinheiten $x, y \in R$. Anwenden der Norm liefert $4 = N(x)N(y)$, also $N(x) = 2$. Das ist aber für $x = a + b\sqrt{-3}$ nicht möglich, da die Gleichung $2 = a^2 + 3b^2$ keine Lösung in $\mathbb{Z}^2$ hat. Somit ist die 2 irreduzibel in R.
Die 2 ist ein Teiler von 4, also gilt

$$2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Aber die 2 teilt weder $1 + \sqrt{-3}$ noch $1 - \sqrt{-3}$; damit ist die 2 kein Primelement in R.

(c) Wäre R faktoriell, so wäre jedes irreduzible Element auch ein Primelement. Das ist nach (b) nicht der Fall in R, also ist R nicht faktoriell.

Aufgabe 3 Zeigen Sie, daß die folgenden Polynome irreduzibel sind:

(a) $5X^3 + 63X^2 + 168$ in $\mathbb{Z}[X]$.

(b) $X^4 + X + 1$ in $\mathbb{F}_2[X]$.

(c) $X^9 + XY^7 + Y$ in $\mathbb{Z}[X, Y]$.

Lösung: (a) Wegen $\mathrm{ggT}(5, 63) = 1$ kann man keine Konstante $\neq \pm 1$ ausklammern. Wegen Eisenstein mit $p = 3$ ist das Polynom in (a) auch irreduzibel über $\mathbb{Q}$ und somit über $\mathbb{Z}$.

(b) Das Polynom in (b) hat keine Nullstelle in $\mathbb{F}_2$. Eine Zerlegung in quadratische Faktoren wäre nur dann möglich, wenn die Faktoren irreduzibel über $\mathbb{F}_2$ sind. Da aber $X^2 + X + 1$ das einzige über $\mathbb{F}_2$ irreduzible quadratische (normierte) Polynom über $\mathbb{F}_2$ ist und

$$(X^2 + X + 1)^2 = X^4 + X^2 + 1$$

ungleich dem Polynom in (b) ist, ist das Polynom in (b) irreduzibel.

(c) Das Polynom $f = X^9 + XY^7 + Y \in (\mathbb{Z}[Y])[X]$ über dem faktoriellen Ring $\mathbb{Z}[Y]$ ist nach Eisenstein mit dem Primelement $p = Y$ aus $\mathbb{Z}[Y]$ über dem Quotientenkörper von $\mathbb{Z}[Y]$ irreduzibel, also wegen der Teilerfremdheit der Koeffizienten von f auch über $\mathbb{Z}[Y]$.

Aufgabe 4 Es seien p und q verschiedene Primzahlen.

(a) Zeigen Sie, daß die Körper $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ nicht isomorph sind.

(b) Zeigen Sie, daß der Körper $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ vom Grad 4 über $\mathbb{Q}$ ist.

(c) Bestimme Sie das Minimalpolynom von $\alpha = \sqrt{p} + \sqrt{q}$ über $\mathbb{Q}$.

Lösung: (a) Angenommen, es existiert ein Isomorphismus $\varphi : \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(\sqrt{q})$ mit $\varphi(\sqrt{p}) = a + b\sqrt{q}$. Es folgt dann

$$p = \varphi(p) = \varphi(\sqrt{p}\sqrt{p}) = \varphi(\sqrt{p})\varphi(\sqrt{p}) = (a + b\sqrt{q})^2 = a^2 + 2ab\sqrt{q} + b^2 q.$$

In jedem der Fälle $a=0$, $b=0$, $ab\neq 0$ folgt ein Widerspruch zu der Tatsache, daß p und q Primzahlen sind:

$$\begin{aligned} a=0 &\Rightarrow\ p=b^2q \\ b=0 &\Rightarrow\ p=a^2 \\ ab\neq 0 &\Rightarrow\ \sqrt{q}=\frac{p-a^2-b^2q}{2ab}\,. \end{aligned}$$

(b) Es sind $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ beides Oberkörper von $\mathbb{Q}$ vom Grad 2, da X^2-p und X^2-q nach Eisenstein irreduzibel über $\mathbb{Q}$ sind und $\sqrt{p}$ und $\sqrt{q}$ Wurzeln davon sind. Damit gilt

$$[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}]\in\{2,4\}\,.$$

Angenommen, $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}]=2$. Dann gilt $\sqrt{q}\in\mathbb{Q}(\sqrt{p})$, sodaß $\mathbb{Q}(\sqrt{q})=\mathbb{Q}(\sqrt{p})$ im Widerspruch zum Teil (a).

(c) Es gilt

$$\begin{aligned} \alpha^2=p+2\sqrt{pq}+q\ &\Rightarrow\ \frac{1}{4}(\alpha^2-p-q)^2=pq \\ &\Rightarrow\ \alpha^4-2\alpha^2(p+q)+(p+q)^2=4pq \\ &\Rightarrow\ \alpha^4-2\alpha^2(p+q)+(p+q)^2-4pq=0\,, \end{aligned}$$

so daß α Wurzel des normierten Polynoms

$$f=X^4-2(p+q)X^2+(p-q)^2\in\mathbb{Q}[X]$$

ist. Da $\alpha=\sqrt{p}+\sqrt{q}$ bekanntlich den Grad 4 über $\mathbb{Q}$ hat (bekanntlich gilt $\mathbb{Q}(\sqrt{p},\sqrt{q})=\mathbb{Q}(\sqrt{p}+\sqrt{q})$), ist f das Minimalpolynom von α über $\mathbb{Q}$.

Aufgabe 5 Es sei p eine Primzahl und ζ_p eine primitive p-te Einheitswurzel. Zeigen Sie:

(a) Zu jedem natürlichen Teiler n von $p-1$ gibt es genau einen Teilkörper K_n von $\mathbb{Q}(\zeta_p)$ mit

$$[K_n:\mathbb{Q}]=n\,.$$

(b) Der einzige über $\mathbb{Q}$ quadratische Teilkörper von $\mathbb{Q}(\zeta_5)$ ist $\mathbb{Q}(\sqrt{5})$.

Lösung: (a) Es gilt $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$, da ζ_p Wurzel des über $\mathbb{Q}$ irreduziblen Kreisteilungspolynom $X^{p-1}+\cdots+X+1\in\mathbb{Q}[X]$ ist. Bekanntlich ist die Körpererweiterung $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ zyklisch, d. h. $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong\mathbb{Z}_{p-1}$. Bekanntlich hat eine zyklische Gruppe zu jedem Teiler n der Gruppenordnung (hier $p-1$) genau eine Untergruppe vom Index n. Aufgrund des Hauptsatzes der Galoistheorie existiert daher zu jedem solchen Teiler n von $p-1$ genau ein Teilkörper K_n mit $[K_n:\mathbb{Q}]=n$.

(b) Nach dem Teil (a) gibt es zu dem Teiler 2 von $5-1$ genau einen quadratischen Teilkörper K_2 von $\mathbb{Q}(\zeta_5)$ über $\mathbb{Q}$. Es ist nur noch zu begründen, daß $K_2=\mathbb{Q}(\sqrt{5})$ gilt, dazu reicht es aus zu zeigen, daß $\sqrt{5}\in\mathbb{Q}(\zeta_5)$. Wir können ohne Einschränkung voraussetzen, daß $\zeta_5=\mathrm{e}^{\frac{2\pi\mathrm{i}}{5}}$ (ansonsten potenziere ζ_5 entsprechend). Mit ζ_5 liegt auch das Element

$$\zeta_5+\zeta_5^4=2\cos(\frac{2\pi}{5})$$

in $\mathbb{Q}(\zeta_5)$. Und wegen

$$(\zeta_5+\zeta_5^4)^2=\zeta_5^2+2+\zeta_5^3=-\zeta_5^4-\zeta_5+1$$

ist $\zeta_5+\zeta_5^4$ eine Wurzel des quadratischen Polynoms

$$X^2+X-1\in\mathbb{Q}[X]\,,$$

dessen Wurzeln $\frac{-1\pm\sqrt{5}}{2}$ sind. Somit gilt $\sqrt{5}\in\mathbb{Q}(\zeta_5)$.