Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Herbst 2003, Thema Nr. 3

Aufgabe 1 (*Herbst 2003*) Es sei G eine endliche Gruppe der Ordnung $n > 1$. Es sei p der kleinste Primteiler von n und P eine zyklische, normale p-Sylowgruppe von G.

(a) Zeigen Sie: Ist p^m die Ordnung von P, so ist $p^{m-1}(p-1)$ die Ordnung der Automorphismengruppe $\mathrm{Aut}(P)$ von P.

(b) Die Konjugation von G auf P liefert einen Homomorphismus

$$\alpha : G \to \mathrm{Aut}(P)\,,\ \alpha(g) : x \mapsto g\,x\,g^{-1}$$

für $g \in G$ und $x \in P$.

Zeigen Sie: Der Index $[G : \ker(\alpha)]$ ist ein Teiler von $p^{m-1}(p-1)$ und nicht durch p teilbar.

(c) Zeigen Sie, daß P im Zentrum von G enthalten ist.

Lösung. (a) Da P eine zyklische Gruppe der Ordnung p^m ist, gilt $P \cong \mathbb{Z}_{p^m}$. Es folgt $\mathrm{Aut}(P) \cong \mathrm{Aut}\,\mathbb{Z}_{p^m} = \mathbb{Z}_{p^m}^{\times}$. Damit hat die Automorphismengruppe von P die Ordnung $\varphi(p^m) = p^{m-1}(p-1)$.

(b) Nach dem Homomorphiesatz ist $G/\ker\alpha$ isomorph zu einer Untergruppe von $\mathrm{Aut}\,P$ und damit ist $|G/\ker\alpha| = [G : \ker\alpha]$ nach Lagrange ein Teiler von $p^{m-1}(p-1)$. Weiter liegt P im Kern von α, so daß $|G/P| = |G/\ker\alpha|\,|\ker\alpha/P|$. Da p kein Teiler von $|G/P|$ ist (beachte, daß P eine p-Sylowgruppe ist), ist p also auch kein Teiler von $|G/\ker\alpha| = [G : \ker\alpha]$.

(c) Da $|G/\ker\alpha| = [G : \ker\alpha]$ nach (b) ein Teiler von $p-1$ ist und bekanntlich ein Teiler von $|G|$ ist, p aber andererseits der kleinste Primteiler von $|G|$ ist, bleibt nur $[G : \ker\alpha] = 1$, d. h. $G = \ker\alpha$, d. h. P liegt im Zentrum von G.

Aufgabe 2 (*Herbst 2003*) Es sei R der Unterring des Matrizenringes $\mathbb{Q}^{2\times 2}$, der aus den Matrizen $\begin{pmatrix} z & a \\ 0 & z \end{pmatrix}$ mit $z \in \mathbb{Z}$, $a \in \mathbb{Q}$ besteht.

(a) Zeigen Sie, daß jedes Primideal von R die Elemente

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \ \text{ für } \ a \in \mathbb{Q}$$

enthält, und daß diese Elemente ein Ideal N von R bilden, für das $R/N \cong \mathbb{Z}$ gilt.

(b) Bestimmen Sie alle Primideale von R.

Lösung. (a) Es sei P ein Primideal. Für jedes Element $x \in N$ gilt $x^2 = 0 \in P$, so daß also $x \in P$ gilt (P ist ein Primideal $\Leftrightarrow P \neq R$ und $ab \in P$ impliziert $a \in P$ oder $b \in P$).
Wir betrachten den Homomorphismus

$$\varphi : R \to \mathbb{Z}, \begin{pmatrix} z & a \\ 0 & z \end{pmatrix} \mapsto z.$$

Offenbar ist φ surjektiv. Der Kern von φ ist offensichtlich N. Mit dem Homomorphiesatz folgt

$$R/N \cong \mathbb{Z}.$$

Als Kern eines Homomorphismus ist N ein Ideal von R.

(b) Der Korrespondenzsatz liefert eine inklusionserhaltende Bijektion $A \mapsto \varphi(A)$ von der Menge aller Ideale von R *über* N (beachte den Teil (a)) auf die Menge aller Ideale von $\mathbb{Z}$. Hierbei entsprechen den Primidealen von R die Primideale von $\mathbb{Z}$. Und die Primideale von $\mathbb{Z}$ kennt man, es sind dies die Ideale (p) mit $p = 0$ oder $p =$ prim.
Wir erhalten für jedes solche p also das Primideal

$$N_p := \left\{ \begin{pmatrix} pz & a \\ 0 & pz \end{pmatrix} \mid z \in \mathbb{Z}, a \in \mathbb{Q} \right\} \subseteq R.$$

Aufgabe 3 (*Herbst 2003*) Es sei F der Körper mit zwei Elementen. Zeigen Sie:

(a) Ist $n > 1$ eine natürliche Zahl, ist $2^n - 1$ eine Primzahl und ist $f \in F[X]$ ein irreduzibles Polynom vom Grad n, dann erzeugt die Restklasse $X + (f)$ die multiplikative Gruppe des Körpers $F[X]/(f)$.

(b) Für $g = X^4 + X^3 + X^2 + X + 1 \in F[X]$ ist $K = F[X]/(g)$ ein Körper, und die Restklasse $X + (g)$ in $K^\times$ hat die Ordnung 5.

Lösung. (a) Der Körper $K = F[X]/(f)$ hat 2^n Elemente. Das Element $X + (f)$ liegt in der multiplikativen Gruppe $K^\times$ und ist ungleich 1. Die Ordnung von $X + (f)$ ist damit $2^n - 1$, da dies eine Primzahl ist. Somit ist $X + (f)$ ein erzeugendes Element von $K^\times$.
(b) Das Polynom g ist als fünftes Kreisteilungspolynom irreduzibel. Somit ist $K = F[X]/(g)$ ein Körper, der zu $\mathbb{F}_{16}$ isomorph ist. Wegen $X^5 - 1 = (X - 1)\, g$ ist die Ordnung von $X + (g)$ in $K^\times$ gleich 5.

Aufgabe 4 (*Herbst 2003*) Gegeben sei das Element $z = X^2 + X^{-2}$ des rationalen Funktionenkörpers $\mathbb{Q}(X)$.

(a) Zeigen Sie, daß $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ endlich vom Grad ≤ 4 ist.

(b) Bestimmen Sie die Gruppe aller Automorphismen von $\mathbb{Q}(X)$, die z festlassen.

(c) Zeigen Sie, daß $\mathbb{Q}(X)$ über $\mathbb{Q}(z)$ galoissch ist und geben Sie alle Körper zwischen $\mathbb{Q}(X)$ und $\mathbb{Q}(z)$ an.

Lösung. (a) Wegen $zX^2 = X^4 + 1$ ist X eine Wurzel des Polynoms $Y^4 - zY^2 + 1$ über $\mathbb{Q}(z)$. Somit gilt $[\mathbb{Q}(X) : \mathbb{Q}(z)] \leq 4$.

(b) Es sei φ ein Automorphismus von $\mathbb{Q}(X)$, der z festläßt. Wegen $X^4 - zX^2 + 1 = 0$ erhalten wir $\varphi(X)^4 - z\varphi(X)^2 + 1 = 0$, so daß neben X auch $\varphi(X)$ eine Wurzel des Polynoms $Y^4 - zY^2 + 1$ ist. Da dieses

Polynom die vier verschiedenen Wurzeln $\pm X$ und $\pm X^{-1}$ hat, erhalten wir die vier verschiedenen $\mathbb{Q}(z)$-Automorphismen

$$\varphi_1 : X \to X\,,\ \varphi_2 : X \to -X\,,\ \varphi_3 : X \to X^{-1}\,,\ \varphi_4 : X \to -X^{-1}\,.$$

Damit ist $\Gamma = \{\varphi_1, \ldots, \varphi_4\}$ die gesuchte Gruppe.

(c) $\mathbb{Q}(X)$ ist als Zerfällungskörper von $Y^4 - zY^2 + 1$ über $\mathbb{Q}(z)$ normal. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist $\mathbb{Q}(X)/\mathbb{Q}(z)$ separabel. Somit ist die Erweiterung galoissch. Nach dem Teil (b) ist der Grad der Körpererweiterung 4, und die Galoisgruppe ist die Kleinsche Vierergruppe. Die drei Untergruppen $U_i = \langle \varphi_i \rangle$ mit $i = 2, 3, 4$ liefern alle echten Zwischenkörper, es gilt

$$U_2 \;\leftrightarrow\; \mathbb{Q}(z, X^2)\,,\ U_3 \;\leftrightarrow\; \mathbb{Q}(z, X + X^{-1})\,,\ U_4 \;\leftrightarrow\; \mathbb{Q}(z, X - X^{-1})\,.$$