Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Frühjahr 2012, Thema Nr. 2

Aufgabe 1 Welche der folgenden Aussagen sind richtig bzw. falsch? Geben Sie jeweils eine **kurze** Begründung an:

(a) Die Gruppen $Z_6 \times Z_{10}$ und $Z_2 \times Z_{30}$ sind isomorph (Z_n bezeichne dabei die zyklische Gruppe der Ordnung n).

(b) Die alternierende Gruppe A_4 ist eine einfache Gruppe.

(c) In der symmetrischen Gruppe S_5 sind alle Elemente der Ordnung 2 konjugiert.

(d) In $\mathbb{Z}[X]$ ist (X) ein Primideal.

Lösung. (a) Richtig. Nach dem Hauptsatz über endliche abelsche Gruppen gilt

$$Z_6 \times Z_{10} \cong Z_2 \times Z_3 \times Z_2 \times Z_5\,,$$
$$Z_2 \times Z_{30} \cong Z_2 \times Z_2 \times Z_3 \times Z_5\,.$$

(b) Falsch. Es ist

$$\{(1)\,,\ (12)(34)\,,\ (13)(24)\,,\ (14)(23)\}$$

ein nichttrivialer Normalteiler der A_4.
(c) Falsch. Es sind (12) und $(12)(34)$ zwei Elemente der S_5 der Ordnung 2, die nicht zueinander konjugiert sind.
(d) Richtig. Das Ideal (X) ist der Kern des surjektiven Homomorphismus $\varepsilon : \mathbb{Z}[X] \to \mathbb{Z}$, $f \mapsto f(0)$. Nach dem Homomorphiesatz ist $\mathbb{Z}[X]/(X)$ zum Integritätsbereich $\mathbb{Z}$ isomorph. Das besagt, dass (X) ein Primideal ist.

Aufgabe 2 Es seien G eine endliche Gruppe und p eine Primzahl. Begründen Sie, dass die Anzahl der Elemente der Ordnung p in G durch $p-1$ teilbar ist, d. h.,

$$|\{a \in G \,|\, \mathrm{ord}(a) = p\}| = (p-1)\cdot k \ \text{ für ein } \ k \in \mathbb{N}\,.$$

(Hinweis: Betrachten Sie die Mengen $M_a = \{a, a^2, \ldots, a^{p-1}\}$ für $a \in G$ mit $\mathrm{ord}(a) = p$.)
Lösung: Zur Abkürzung setzen wir $M := \{a \in G \,|\, \mathrm{ord}(a) = p\}$, und für jedes $a \in G$ schreiben wir $M_a = \langle a\rangle \backslash \{e\}$ wie im Hinweis angegeben. Wir müssen also zeigen, dass $p-1$ ein Teiler von $|M|$ ist.

(i) Für alle $a \in M$ gilt: $\mathrm{ord}(a) = p$, also $|\langle a\rangle| = p$, also $|M_a| = p-1$.

(ii) Es sei $a \in M$. Für alle $\alpha \in M_a$ ist dann nach dem Satz von Lagrange $\mathrm{ord}(a) = |\langle\alpha\rangle|$ ein Teiler von p, also $\mathrm{ord}(\alpha) = 1$ oder $= p$. Wegen $\alpha \neq e$ ist also $\mathrm{ord}(\alpha) = p$ und somit $\alpha \in M$. Wir erhalten:

$$M = \bigcup_{a \in M} M_a.$$

(iii) Es seien $a, b \in M$ mit $M_a \neq M_b$. Dann gilt also $\langle a\rangle \neq \langle b\rangle$. Somit ist $\langle a\rangle \cap \langle b\rangle$ eine echte Untergruppe der Gruppe $\langle a\rangle$. Da $|\langle a\rangle| = p$ eine Primzahl ist, folgt aus dem Satz von Lagrange: $\langle a\rangle \cap \langle b\rangle = \{e\}$ und somit $M_a \cap M_b = \emptyset$.

Aus (i), (ii), (iii) folgt:

$$|M| = (p-1) \cdot \text{Anzahl der verschiedenen } M_a\text{'s.}$$

Insbesondere ist $p-1$ ein Teiler von M.

Aufgabe 3 Bestimmen Sie alle Teiler von 6 im Ring in $\mathbb{Z}[\sqrt{-6}] = \{a + \sqrt{-6} \cdot b \,|\, a, b \in \mathbb{Z}\}$.
Lösung. Ist $a = u + \sqrt{-6}v \in \mathbb{Z}[(\sqrt{-6}]$ ein Teiler von 6, so gilt $N(a) \mid N(6) = 36$. Folglich gilt $N(a) = u^2 + 6v^2 \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.

$$\begin{aligned}
&N(a) = 1 \;\Rightarrow\; a = \pm 1\,,\\
&N(a) \in \{2, 3, 12, 18\} \;\Rightarrow\; N(a) = u^2 + 6v^2 \text{ ist nicht lösbar,}\\
&N(a) = 4 \;\Rightarrow\; a = \pm 2\,,\\
&N(a) = 6 \;\Rightarrow\; a = \pm\sqrt{-6}\,,\\
&N(a) = 9 \;\Rightarrow\; a = \pm 3\,,\\
&N(a) = 36 \;\Rightarrow\; a = \pm 6\,.
\end{aligned}$$

Folglich sind $\pm 1, \pm 2, \pm\sqrt{-6}, \pm 3, \pm 6$ die Kandidaten für die Teiler. Wegen $6 = -\sqrt{-6}^2 = 2 \cdot 3$ ist $\{\pm 1, \pm 2 \pm \sqrt{-6}, \pm 3, \pm 6\}$ die Menge aller Teiler von 6.

Aufgabe 4 Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper von $f = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$.

(a) Begründen Sie, warum f irreduzibel ist.

(b) Warum ist die Körpererweiterung $L/\mathbb{Q}$ galoissch?

(c) Es sei $\alpha \in L$ eine Nullstelle von f. Begründen Sie, warum $\beta := \alpha^3 + 3\alpha$ eine Nullstelle von f ist.

(d) Begründen Sie, warum $\mathbb{Q}(\alpha) = L$ gilt.

(e) Wieviele Elemente enthält die Galoisgruppe $\mathrm{Gal}(L/\mathbb{Q})$?

(f) Ist die Galoisgruppe zyklisch? Begründen Sie Ihre Antwort. (Hinweis: Betrachten Sie den $\mathbb{Q}$-Automorphismus σ, der durch $\sigma(\alpha) = \beta$ gegeben ist und bestimmen Sie $\sigma^2(\alpha)$.)

Lösung: (a) Nach dem Eisenstein-Kriterium mit $p = 2$ ist f irreduzibel.

(b) Die algebraische Körpererweiterung $L/\mathbb{Q}$ ist normal (da L Zerfällungskörper eines Polynoms über $\mathbb{Q}$ ist) und separabel (da $\mathbb{Q}$ die Charakteristik 0 hat). Damit ist $L/\mathbb{Q}$ galoissch.

(c) Mit Hilfe von Polynomdivision sieht man

$$\begin{aligned}
f(\beta) = (\alpha^3 + 3\alpha)^4 + 4(\alpha^3 + 3\alpha)^2 + 2 = \alpha^{12} + 12\alpha^{10} + 54\alpha^8 + 112\alpha^6 + 105\alpha^4 + 36\alpha^2 + 2 =\\
(\alpha^8 + 8\alpha^6 + 20\alpha^4 + 16\alpha^2 + 1)\underbrace{(\alpha^4 + 4\alpha^2 + 2)}_{=f(\alpha)=0} = 0.
\end{aligned}$$

(d) Es sind α, β, $-\alpha$, $-\beta$ Nullstellen von f, die paarweise verschieden sind, da $\{1, \alpha, \alpha^2, \alpha^3\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\alpha)$ ist. Also ist $\mathbb{Q}(\alpha)$ ein Zerfällungskörper von f und somit $\mathbb{Q}(\alpha) = L$.
(e) Wegen (d) ist $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = \deg(f) = 4$.
(f) Da α, β Nullstellen von f sind und f irreduzibel ist, existiert ein $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ mit $\sigma : \alpha \mapsto \beta$. Es gilt $\sigma^2(\alpha) = \beta^3 + 3\beta = -\alpha \neq \alpha$, also $|\langle\sigma\rangle| = 4$. Also ist $\mathrm{Gal}(L/\mathbb{Q})$ zyklisch von der Ordnung 4, somit $\mathrm{Gal}(L/\mathbb{Q}) \cong Z_4$.