Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Herbst 2004, Thema Nr. 3

Aufgabe 1 (*Herbst 2004*) Es sei G eine Gruppe der Ordnung p^2q, wobei p und q Primzahlen bezeicnen. Zeigen Sie, daß G einen nichttrivialen Normalteiler hat.

Lösung. *1. Fall:* $p = q$. Da G eine p-Gruppe ist, hat G ein nichttriviales Zentrum Z. Das Zentrum Z ist damit ein nichttrivialer Normalteiler von G, falls $Z(G) \neq G$. Im Fall $Z(G) = G$ ist G abelsch und somit ist jede echte Untergruppe ein nichttrivialer Normalteiler.

2. Fall: $p \neq q$. Nichttriviale Normalteiler sind Sylowgruppen, die *einzeln* auftreten. Es seien n_p die Anzahl der p-Sylowgruppen und n_q die Anzahl der q-Sylowgruppen. Bekanntlich gilt

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

Ist $n_p = 1$ oder $n_q = 1$, so ist die p-Sylowgruppe oder q-Sylowgruppe ein nichttrivialer Normalteiler. Wir zeigen, daß der Fall $n_p \neq 1 \neq n_q$ nicht auftreten kann.
Angenommen, es gilt $n_p \neq 1 \neq n_q$. Dann gibt es zwei Möglichkeiten:

Fall 2a: $n_p = q$ und $n_q = p$. In diesem Fall gilt $p \mid q-1$ und $q \mid p-1$. Das kann nicht sein.

Fall 2b: $n_p = q$ und $n_q = p^2$. In diesem Fall gilt $p \mid q-1$ und $q \mid p^2-1$. Es folgt $q \mid p+1$, da $q \mid p-1$ nach dem Fall 2a nicht möglich ist. Wegen $q \mid p+1$ und $p \mid q-1$ muß $p = 2$ und $q = 3$ gelten, d. h. $|G| = 12$. Wir zählen nun die Elemente der Sylowgruppen: 4 Sylowgruppen der Ordnung 3 liefern acht Elemente der Ordnung 3 und 3 Sylowgruppen der Ordnung 4 liefern mehr als vier Elemente. Das kann nicht sein.

Aufgabe 2 (*Herbst 2004*)

(a) Es sei p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \nmid a$. Zeigen Sie, daß die Kongruenz

$$x^2 - ay^2 \equiv b \mod p$$

eine Lösung in ganzen Zahlen $x, y \in \mathbb{Z}$ hat.

[Hinweis: Zählen Sie die Elemente der Form $ay^2 + b$ in F_p.]

(b) Beweisen Sie, daß die Gleichung

$$x^2 - 43y^2 = 29$$

keine Lösung in ganzen Zahlen $x, y \in \mathbb{Z}$ hat.

Lösung. (a) Die Quadratmenge $F_p^{(2)} = \{a^2 \,|\, a \in F_p\}$ hat die Ordnung $\frac{p+1}{2}$, falls $p \neq 2$. Für beliebige $a, b \in F$ mit $a \neq 0$ ist die Abbildung $q \mapsto aq + b$ von $F_p^{(2)}$ in $aF_p^{(2)} + b \subseteq F_p$ eine Bijektion, es folgt

$$|aF_p^{(2)} + b| = \frac{p+1}{2} = |F_p^{(2)}|\,,$$

so daß $(aF_p^{(2)}+b)\cap F_p^{(2)}\neq\emptyset$. Es folgt die Behauptung in diesem Fall. Im Fall $p=2$ stimmt die Behauptung auch: Hier ist $a=1$, die Gleichung $x^2=y^2+b$ ist für jedes b lösbar.

(b) Angenommen, x und y lösen die Gleichung $x^2-43y^2=29$. Modulo 43 gilt dann

$$x^2\equiv 29 \mod 43\,,\ \text{d. h.}\ \left(\frac{29}{43}\right)=1\,;$$

aber tatsächlich gilt für das Legendresche Restsymbol

$$\left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)=-\left(\frac{7}{29}\right)=-\left(\frac{29}{7}\right)=-\left(\frac{1}{7}\right)=-1\,,$$

so daß obige Gleichung keine Lösung haben kann.

Aufgabe 3 (*Herbst 2004*) Bestimmen Sie den Isomorphietyp der Galoisgruppe des Polynoms $f(X)=X^5-4X+2$ über $\mathbb{Q}$.

Lösung. Die Galoisgruppe eines Polynoms f über $\mathbb{Q}$ ist die Galoisgruppe des Zerfällungskörpers L von f über Q, $\Gamma(f)=\Gamma(L/\mathbb{Q})$. Bekanntlich gilt der Satz (vgl. Lemma 27.5, Algebra, 2. Auflage, Karpfinger/Meyberg): *Ist $f\in\mathbb{Q}[X]$ irreduzibel vom Primzahlgrad p und hat f genau zwei nichtreelle Wurzeln, so gilt $\Gamma(f)\cong S_p$.*
Wir begründen, daß unser Polynom f vom Primzahlgrad 5 irreduzibel ist und genau zwei nichtreelle Wurzeln in $\mathbb{C}$ hat, oder anders formuliert, genau drei reelle Wurzeln in $\mathbb{R}$ hat.
Das Polynom f ist nach Eisenstein mit $p=2$ irreduzibel. Da ein Polynom vom Grad 5 entweder genau eine oder genau drei oder genau fünf reelle Wurzeln hat, können wir unsere Begründung abschließen, wenn wir zeigen können, daß f genau zwei lokale Extrema hat:
Wegen

$$f'=5X^4-4=5\left(X^2-\sqrt{\frac{4}{5}}\right)\left(X^2+\sqrt{\frac{4}{5}}\right)\ \text{ und }\ f''=20X^3$$

und

$$f''\left(\sqrt[4]{\frac{4}{5}}\right)\neq 0\ \text{ und }\ f''\left(-\sqrt[4]{\frac{4}{5}}\right)\neq 0$$

hat f genau zwei lokale Extrema (eines muß ein Minimum, das andere ein Maximum sein). Es folgt $\Gamma(f)\cong S_5$.

Aufgabe 4 (*Herbst 2004*) Es sei K eine Galoiserweiterung von k und $a\in K$ ein Element, für das $\sigma(a)\neq a$ für alle Automorphismen $\sigma\neq 1$ der Galoisgruppe von K über k gilt. Zeigen Sie, daß $K=k(a)$ gilt.

Lösung. Die Erweiterung $K/k(a)$ ist bekanntlich galoissch. Betrachte:

$$\begin{tikzcd}
K \arrow[d, dash] & \{1\} \arrow[d, dash] \\
k(a) \arrow[d, dash] & \Gamma(K/k(a)) \arrow[d, dash] \\
k & \Gamma(K/k)
\end{tikzcd}$$

Da $k(a)$ der Fixkörper von $\Gamma(K/k(a))$ ist,

$$k(a) = \mathcal{F}(\Gamma(K/k(a)) = \{x \in K \mid \sigma(x) = x \text{ für alle } \sigma \in \Gamma(K/k(a))\},$$

erhalten wir

$$\sigma(a) = a \;\text{ für alle }\; \sigma \in \Gamma(K/k(a)) \subseteq \Gamma(K/k).$$

Nach Voraussetzung gilt $\sigma = 1$, d. h. $|\Gamma(K/k(a))| = 1$, es folgt $[K : k(a)] = 1$, d. h. $K = k(a)$.

Aufgabe 5 (*Herbst 2004*) Bestimmen Sie alle Zwischenkörper der Erweiterung $\mathbb{Q}(\sqrt[4]{5})$ von $\mathbb{Q}$.

Lösung. Neben den trivialen Zwischenkörpern $\mathbb{Q}(\sqrt[4]{5})$ und $\mathbb{Q}$ ist offenbar $\mathbb{Q}(\sqrt{5})$ ein Zwischenkörper mit $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Jeder weitere Zwischenkörper hat nach dem Gradsatz ebenfalls den Grad 2 über $\mathbb{Q}$. Ist K ein solcher Zwischenkörper, so gilt bekanntlich $K = \mathbb{Q}(\sqrt{a})$ für ein $a \in \mathbb{Q}$. Im Fall $\mathbb{Q}(\sqrt{5}) \neq \mathbb{Q}(\sqrt{a})$ gilt $\mathbb{Q}(\sqrt[4]{5}) = \mathbb{Q}(\sqrt{5}, \sqrt{a})$, das ist ein Widerspruch, da $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ nicht normal ist, die Erweiterung $\mathbb{Q}(\sqrt{5}, \sqrt{a})/\mathbb{Q}$ hingegen schon.