Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger



# Repetitorium zur Algebra

Frühjahr 2004, Thema Nr. 1

**Aufgabe 1** (*Frühjahr 2004*) Es sei $G$ eine endliche Gruppe der Ordnung $n = a \cdot b$ mit teilerfremden $a, b > 1$. Zeigen Sie:

(a) Es gibt einen minimalen Normalteiler $N$ in $G$ mit zu $b$ teilerfremdem Index $[G : N]$.

(b) Der Normalteiler in (a) ist die von der Teilmenge $\{g^a \mid g \in G\}$ erzeugte Untergruppe von $G$.

(c) Es gibt eine endliche Gruppe $H$ und einen Homomorphismus $u : G \to H$ mit den folgenden Eigenschaften

(i) Die Ordnung von $H$ ist teilerfremd zu $b$.

(ii) Jeder Gruppenhomomorphismus $f : G \to A$ in eine endliche Gruppe $A$ mit zu $b$ teilerfremder Ordnung faktorisiert eindeutig über $u$, d. h. ist von der Gestalt $f = h \circ u$ mit einem wohlbestimmten Homomorphismus $h : H \to A$.

**Lösung.** (a) Sind $N_1$ und $N_2$ Normalteiler von $G$ mit zu $b$ teilerfremden Indizes, so ist auch $N_1 \cap N_2$ ein Normalteiler von $G$ mit zu $b$ teilerfremden Index (das ist bekannt bzw. betrachte man den (wohldefinierten) injektiven Homomorphismus $\varphi : G/N_1 \cap N_2 \to G/N_1 \times G/N_2$, $a(N_1 \cap N_2) \mapsto (aN_1, aN_2)$; hieraus folgt: $[G : N_1 \cap N_2] \mid [G : N_1] \cdot [G : N_2]$).
Dies ist auf endlich viele solche Normalteiler verallgemeinerbar, man erhält: Der Durchschnitt aller Normalteiler $N$ mit zu $b$ teilerfremden Indizes ist ein Normalteiler, der einen zu $b$ teilerfremden Index hat; offenbar ist dieser minimal bzgl. der Inklusion.

(b) Den minimalen Normalteiler aus dem Teil (a) bezeichnen wir mit $N$, die von $\{g^a \mid g \in G\}$ erzeugte Untergruppe von $G$ bezeichnen wir mit $N'$. Offenbar ist $N'$ ein Normalteiler von $G$, da $xg^a x^{-1} = (xgx^{-1})^a$. Falls wir begründen können, daß $N'$ einen zu $b$ teilerfremden Index hat und $N' \subseteq N$ gilt, folgt wegen der Minimalität von $N$ die Behauptung.
Da $N$ nach dem Teil (a) einen zu $b$ teilerfremden Index hat, gilt $b \mid |N|$. Somit sind alle Elemente von $G$, deren Ordnung ein Teiler von $b$ ist, in $N$ enthalten. Also sind auch die Elemente $g^a$ des Erzeugendensystems von $N'$ wegen $(g^a)^b = e$ in $N$ enthalten. Es folgt $N' \subseteq N$.
Da für jedes $gN' \in G/N'$ die Potenz $g^a N' = N'$ das neutrale Element ist, ist die Ordnung von $G/N'$ ein Teiler von $a$. Folglich ist der Index $[G : N']$ teilerfremd zu $b$.

(c) (i) Man wähle $H = G/N$ mit dem Normalteiler $N = N'$ aus dem Teil (b), für $u$ wähle man den kanonischen Epimorphismus $g \mapsto gN$.
(ii) Es sei $f$ ein solcher Homomorphismus von $G$ in $A$ mit $\operatorname{ggt}(|A|, b) = 1$. Der Kern von $f$ ist ein Normalteiler von $G$, der wegen des Homomorphiesatzes einen Index in $G$ hat, der zu $b$ teilerfremd ist; es folgt $N \subseteq \ker(f)$. Wir betrachten die Abbildung

$$h : G/N \to A,\ gN \mapsto f(g)\,.$$

Die Abbildung ist wohldefiniert: $gN = hN \Rightarrow h^{-1}g \in N \Rightarrow f(h^{-1}g) = e \Rightarrow f(g) = f(h)$, da $N \subseteq \ker f$. Offenbar ist $h$ ein Homomorphismus; und es gilt $f = h \circ u$.

**Aufgabe 2** (*Frühjahr 2004*) Zeigen Sie: Sind $a, b, c \in \mathbb{Z}$ ungerade, so ist das Polynom $aX^4 + bX^3 + c$ irreduzibel in $\mathbb{Q}[X]$.

**Lösung.** Wir fassen das Polynom als ein Polynom über $\mathbb{Z}$ auf und reduzieren modulo 2. Das reduzierte Polynom

$$X^4 + X^3 + 1 \in \mathbb{Z}_2[X]$$

hat keine Nullstelle in $\mathbb{Z}_2$. Und eine Zerlegung in quadratische Faktoren

$$X^4 + X^3 + 1 = (X^2 + aX + b)\,(X^2 + cX + d)$$

liefert das folgende nicht lösbare Gleichungssystem:

$$\begin{aligned} a + c &= 1\,, \\ ac + b + d &= 0\,, \\ ad + bc &= 0\,, \\ bd &= 1\,. \end{aligned}$$

Damit ist das Polynom über $\mathbb{Z}$ irreduzibel und somit auch über $\mathbb{Q}$.

**Aufgabe 3** (*Frühjahr 2004*) Es sei $k$ ein Körper, der keine Galoiserweiterung vom Grad 3 hat. Kann $k$ dann eine Galoiserweiterung vom Grad 225 haben?

**Lösung.** Die Antwort muß offenbar „Nein“ sein, sonst müßte man einen Körper $k$ mit den angegebenen Eigenschaften angeben – das scheint schwierig zu sein. Die einzig naheliegende Idee, die Aufgabe zu lösen, besteht in dem Ansatz: Angenommen, es gibt eine Galoiserweiterung $K$ von $k$ vom Grad 225. Wenn wir hieraus folgern können, daß dann auch eine Galoiserweiterung $L$ von $k$ vom Grad 3 existiert, haben wir einen Widerspruch gefunden: Es kann dann keine solche Erweiterung vom Grad 225 geben.
Mit ein bißchen Hintergrundwissen geht das ganz einfach: Nach dem Hauptsatz der Galoistheorie ist ein Zwischenkörper $L$ von $K/k$ genau dann galoissch über $k$, falls die zugehörige Galoisgruppe $\Gamma(K/L)$ ein Normalteiler von $\Gamma$ ist; in diesem Fall ist der Grad der Körpererweiterung $L/k$ gleich dem Index von $\Gamma(K/L)$ in $\Gamma$, also

$$[L : k] = [\Gamma : \Gamma(K/L)]\,.$$

Wenn wir also zeigen können, daß $\Gamma$ mit $|\Gamma| = 225 = 3^2 \cdot 5^2$ einen Normalteiler vom Index 3 hat, sind wir fertig. Und das sieht man wie folgt: Es gibt genau eine 5-Sylowgruppe $P_5$ wegen $s_5 = 1 + 5k$ und $s_5 \mid 9$. Die Faktorgruppe $\Gamma/P_5$ hat die Ordnung 9 und ist abelsch. Somit hat $\Gamma/P_5$ einen Normalteiler $V$ vom Index 3. Dieser Normalteiler $V$ ist von der Form $N/P_5$ mit einem Normalteiler $N$ von $\Gamma$ vom Index 3, der $P_5$ umfaßt (das besagt der Korrespondenzsatz). Damit ist alles gezeigt.

**Aufgabe 4** (*Frühjahr 2004*) Es sei $K/k$ eine Galoiserweiterung, deren Galoisgruppe isomorph zur symmetrischen Gruppe $S_n$ ist. Zeigen Sie:

(a) $K$ enthält $n$ zueinander konjugierte Zwischenkörper vom Grad $n$ über $k$, die zusammen $K$ über $k$ erzeugen.

(b) $K$ ist der Zerfällungskörper eines Polynoms vom Grad $n$ aus $k[X]$ über $k$.

**Lösung.** (a) Zu jedem Zwischenkörper $L_i$ von $K/k$ vom Grad $n$ über $k$ gehört eine Untergruppe $\Gamma_i$ von $\Gamma \cong S_n$ vom Index $n$, das sind Untergruppen von der Ordnung $(n-1)!$ von $S_n$. Die $n$ Fixgruppen

$$S_n^{(i)} = \{\sigma \in S_n \,|\, \sigma(i) = i\}$$

jeweils eines Elements $i \in \{1,\ldots,n\}$ sind Untergruppen der $S_n$ der Ordnung $(n-1)!$. Die $n$ Fixkörper dieser Fixgruppen sind $n$ Zwischenkörper vom Grad $n$ über $k$.
Wegen

$$\Gamma(K/(L_1 \cdots L_n)) = \Gamma(K/L_1) \cap \cdots \Gamma(K/L_n) = \{\mathrm{id}\}$$

(beachte etwa Lemma 26.5, Algebra, 2. Auflage, Karpfinger/Meyberg) erhalten wir $K = L_1 \cdots L_1$.
Wir begründen nun noch, daß je zwei solche Zwischenkörper $L_i$ und $L_j$ konjugiert sind, d. h. $L_j = \varphi(L_i)$ für ein $\varphi \in \Gamma(K/k)$ und $i, j \in \{1,\ldots,n\}$. Da zueinander konjugierte Untergruppen der Galoisgruppe zueinander konjugierte Zwischenkörper liefern, folgt die Behauptung, wenn wir begründen können, daß je zwei Fixgruppen $S_n^{(i)}$ und $S_n^{(j)}$ konjugiert sind. Das folgt aber mit der Transposition $\sigma = (i\,j)$, die die Zahlen $i$ und $j$ vertauscht, es gilt offenbar

$$S_n^{(i)} = \sigma^{-1} S_n^{(j)} \sigma .$$

Falls nicht bekannt sein sollte, daß zueinander konjugierte Untergruppen der Galoisgruppen zueinander konjugierte Zwischenkörper liefern, hier der Nachweis dieser Tatsache: Es gelte $U = \varphi^{-1} W \varphi$ für zwei Untergruppen $U$ und $W$ von $\Gamma$, $\varphi \in \Gamma$; und $L_U$ bzw. $L_W$ seien die Fixkörper von $U$ bzw. $W$. Dann gilt

$$\begin{aligned} x \in L_U &\Leftrightarrow \sigma(x) = x \ \text{ für alle } \sigma \in U \\ &\Leftrightarrow \varphi^{-1}\tau\varphi(x) = x \ \text{ für alle } \tau \in W \\ &\Leftrightarrow \tau\varphi(x) = \varphi(x) \ \text{ für alle } \tau \in W \\ &\Leftrightarrow \varphi(x) \in L_W , \end{aligned}$$

d. h. $\varphi(L_U) = L_W$.

(b) Wir behalten die Bezeichnungen aus Teil (a) bei. Wir wählen ein primitives Element $a$ von $L_1/k$, d. h. $L_1 = k(a)$, und betrachten das Minimalpolynom $m_{a,k}$ von $a$ über $k$ vom Grad $n$. Wir begründen, daß $K = L_1 \cdots L_n$ der Zerfällungskörper von $m_{a,k}$ ist. Diese Idee ist naheliegend, da $m_{a,k}$ wegen der Normalität von $K/k$ über $K$ zerfallen muß.
Da $L_1$ zu den anderen $L_j$ nach dem Teil (a) konjugiert ist, gibt es zu jedem $j$ ein $\varphi \in \Gamma \cong S_n$ mit $\varphi(a) \in L_j$. Da $\varphi$ ein $k$-Automorphismus von $K$ ist, ist $\varphi(a)$ ein primitives Element von $L_j$, das ebenfalls eine Wurzel von $m_{a,k}$ ist. Damit gilt $K = L_1 \cdots L_n = k(a_1,\ldots,a_n)$, wobei $a_1,\ldots,a_n$ die $n$ verschiedenen Wurzeln von $m_{a,k}$ bezeichnen.

**Aufgabe 5** (*Frühjahr 2004*) Es sei $n > 2$ und $\zeta$ eine primitive $n$-te Einheitswurzel über $\mathbb{Q}$. Zeigen Sie:

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{1}{2}\varphi(n) ,$$

wobei $\varphi$ die Eulersche $\varphi$-Funktion bezeichnet.

**Lösung.** Bekanntlich gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Der Gradsatz besagt

$$\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \cdot [\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] .$$

Hiernach ist *nur* $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ zu begründen. Wegen

$$\zeta(\zeta + \zeta^{-1}) = \zeta^2 + 1$$

ist $\zeta$ eine Wurzel des Polynoms $T^2 - (\zeta + \zeta^{-1})\,T + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[T]$; somit gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$. Im Fall $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 1$ wäre aber $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta + \zeta^{-1})$. Das ist nicht möglich, da $\zeta \in \mathbb{C} \setminus \mathbb{R}$ und $\zeta + \zeta^{-1} \in \mathbb{R}$. Somit gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$.