Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie
Prof. Marc Nieper-Wißkirchen

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 12 zur Algebra I

Abgabe bis 8. Juli 2013, 17:00 Uhr

Aufgabe 1. *Allgemeines zu Gruppen*

a) Gibt es in der Permutationsgruppe S_5 eine Untergruppe mit 70 Elementen?

b) Sei G eine Gruppe. Sei H eine Untergruppe von G und K eine Untergruppe von H. Wieso ist K dann auch eine Untergruppe von G?

c) Sei G eine Gruppe und $\sigma \in G$. Zeige, dass $\sigma^i \circ \sigma^j = \sigma^{i+j}$ für beliebige *ganze* Zahlen i, j.

Lösung.

a) Nein, denn nach dem Satz von Lagrange wäre 70 dann ein Teiler der Ordnung von S_5. Diese ist aber $5! = 120$.

b) Zur Erinnerung die nötigen Definitionen:

> Eine *Gruppe* G ist eine Teilmenge einer S_n, die die Identitätspermutation enthält und außerdem unter Komposition und Inversenbildung abgeschlossen ist.
>
> In dieser Situation ist eine *Untergruppe* L von G eine Teilmenge derselben symmetrischen Gruppe S_n, welche die Identitätspermutation enthält und außerdem unter Komposition und Inversenbildung abgeschlossen ist, und außerdem eine Teilmenge von G ist.

Dann ist die Behauptung klar: Zu zeigen ist, dass $K \subseteq G$ und dass K die Identitätspermutation enthält und unter Komposition und Inversenbildung abgeschlossen ist. Letzteres gilt nach Voraussetzung, und ersteres folgt aus $K \subseteq H$ und $H \subseteq G$.

c) Wir unterscheiden mehrere Fälle. Falls $i = 0$ oder $j = 0$, ist die Behauptung klar (wieso?). Für $i, j > 0$ gilt

$$\sigma^i \circ \sigma^j = \underbrace{\sigma \circ \cdots \circ \sigma}_{i \text{ Faktoren}} \circ \underbrace{\sigma \circ \cdots \circ \sigma}_{j \text{ Faktoren}} = \underbrace{\sigma \circ \cdots \circ \sigma}_{i+j \text{ Faktoren}} = \sigma^{i+j}.$$

Für $i, j < 0$ gilt

$$\sigma^i \circ \sigma^j = \underbrace{\sigma^{-1} \circ \cdots \circ \sigma^{-1}}_{-i \text{ Faktoren}} \circ \underbrace{\sigma^{-1} \circ \cdots \circ \sigma^{-1}}_{-j \text{ Faktoren}} = \underbrace{\sigma^{-1} \circ \cdots \circ \sigma^{-1}}_{-(i+j) \text{ Faktoren}} = \sigma^{i+j}.$$

Für $i > 0, j < 0, i > -j$ gilt

$$\sigma^i \circ \sigma^j = \underbrace{\sigma \circ \cdots \circ \sigma}_{i \text{ Faktoren}} \circ \underbrace{\sigma^{-1} \circ \cdots \circ \sigma^{-1}}_{-j \text{ Faktoren}} = \underbrace{\sigma \circ \cdots \circ \sigma}_{i+j \text{ Faktoren}} = \sigma^{i+j}.$$

Analog behandelt man den Fall $i > 0, j < 0, i < -j$ und den Fall $i < 0, j > 0$.

Aufgabe 2. *Elementordnungen*

a) Sei G eine Gruppe und $\sigma \in G$ ein Element der Ordnung n. Zeige, dass die Ordnung einer beliebigen Potenz σ^m durch $n \,/\, \mathrm{ggT}(n, m)$ gegeben ist.

b) Bestimme die Ordnungen aller Elemente der zyklischen Gruppe C_n.

c) Bestimme alle Erzeuger der zyklischen Gruppe C_n.

Lösung.

a) Wir müssen also folgende Frage beantworten: Für welchen Exponenten $k \geq 1$ ist $(\sigma^m)^k$ das erste Mal gleich der Identitätspermutation? Da für eine ganze Zahl ℓ genau dann $\sigma^\ell = \mathrm{id}$ gilt, wenn ℓ ein Vielfaches von n ist, können wir die Frage äquivalent umformulieren: Für welchen Exponenten $k \geq 1$ ist $m \cdot k$ das erste Mal ein Vielfaches von n? Diese Frage nun können wir mit Schulwissen beantworten: Das ist dann der Fall, wenn $m \cdot k$ das kleinste gemeinsame Vielfache von n und m ist, also wenn $k = \mathrm{kgV}(n, m) \,/\, m = nm \,/\, (\mathrm{ggT}(n, m) \cdot m) = n \,/\, \mathrm{ggT}(n, m)$ ist.

b) Die zyklische Gruppe ist durch

$$\mathrm{C}_n = \{\tau^0, \ldots, \tau^{n-1}\}$$

gegeben, wobei $\tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} \in \mathrm{S}_n$. Diese Permutation τ hat Ordnung n. Daher folgt für die Ordnungen nach Teilaufgabe a)

$$\mathrm{ord}\, \tau^m = n \,/\, \mathrm{ggT}(n, m).$$

c) Ein *Erzeuger* einer endlichen Gruppe G ist ein solches Element $\sigma \in G$, sodass alle Elemente von G gewisse Potenzen von σ sind. Das ist gleichbedeutend damit, dass die Ordnung von σ gleich der Gruppenordnung ist: Denn in der unendlichen Liste

$$\ldots, \sigma^{-2}, \sigma^{-1}, \sigma^0, \sigma^1, \sigma^2, \ldots$$

kommen genau $(\mathrm{ord}\, g)$ viele verschiedene Gruppenelemente vor.

Mit dieser allgemeinen Überlegung können wir die Frage der Aufgabe klären: Ein beliebiges Element $\tau^m \in \mathrm{C}_n$ ist genau dann ein Erzeuger von C_n, wenn seine Ordnung $n/\,\mathrm{ggT}(n, m)$ gleich n ist, also wenn n und m zueinanander teilerfremd sind.

Aufgabe 3. *Kreisteilungspolynome*

a) Berechne die Kreisteilungspolynome $\Phi_3(X)$, $\Phi_6(X)$ und $\Phi_9(X)$.

b) Zerlege das Polynom $X^3 + X^2 + X + 1$ über den rationalen Zahlen in irreduzible Faktoren.

Lösung.

a) Bekanntermaßen gilt $\Phi_1 = X - 1$ und $\Phi_2 = X + 1$. Dann folgt jeweils mit Polynomdivision:

$$\begin{aligned} X^3 - 1 &= \Phi_1 \cdot \Phi_3 & &\Longrightarrow \Phi_3 = X^2 + X + 1 \\ X^6 - 1 &= \Phi_1 \cdot \Phi_2 \cdot \Phi_3 \cdot \Phi_6 & &\Longrightarrow \Phi_6 = X^2 - X + 1 \\ X^9 - 1 &= \Phi_1 \cdot \Phi_3 \cdot \Phi_9 & &\Longrightarrow \Phi_9 = X^6 + X^3 + 1 \end{aligned}$$

b) Wir fügen zunächst künstlich den Faktor $(X-1)$ hinzu:

$$(X^3 + X^2 + X + 1) \cdot (X - 1) = X^4 - 1 = \Phi_1 \cdot \Phi_2 \cdot \Phi_4 = (X-1) \cdot (X+1) \cdot (X^2+1).$$

Dann können wir ihn wieder kürzen, und erhalten so die Zerlegung

$$X^3 + X^2 + X + 1 = (X+1) \cdot (X^2+1).$$

Die auftretenden Faktoren sind (wie alle Kreisteilungspolynome) irreduzibel über den rationalen Zahlen.

Aufgabe 4. *Etwas Zahlentheorie*

Sei p eine Primzahl.

a) Gib eine Primfaktorzerlegung von $X^{p-1} - 1$ modulo p an.

b) Zeige, dass der Binomialkoeffizient $\binom{p^2}{p}$ durch p, aber nicht durch p^2 teilbar ist.

Lösung.

a) Nach dem kleinen Satz von Fermat gilt für alle ganzen Zahlen a die Beziehung

$$a^p \equiv a \mod p.$$

Für solche ganze Zahlen a, die modulo p invertierbar sind (d. h. die teilerfremd zu p sind), kann man a auf beiden Seiten einmal kürzen, sodass man die Beziehung

$$a^{p-1} \equiv 1 \mod p$$

erhält. Folglich besitzt das gegebene Polynom modulo p die $p-1$ verschiedenen Nullstellen $1, 2, \ldots, p-1$. Aus Gradgründen folgt dann schon:

$$X^{p-1} - 1 \equiv (X-1)(X-2) \cdots (X-(p-1)) \mod p.$$

Bemerkung: Der kleine Satz von Fermat besagt *nicht*, dass die Polynomkongruenzen $X^p \equiv X$ oder $X^{p-1} \equiv 1$ gelten.

b) Wir rechnen:

$$\begin{aligned}\binom{p^2}{p} &= \frac{p^2 \cdot (p^2-1) \cdots (p^2-p+2) \cdot (p^2-p+1)}{p \cdot (p-1) \cdots 2 \cdot 1} \\ &= p \cdot \frac{(p^2-1) \cdot (p^2-2) \cdots (p^2-p+2) \cdot (p^2-p+1)}{(p-1) \cdot (p-2) \cdots 2 \cdot 1} \\ &= p \cdot \binom{p^2-1}{p-1}\end{aligned}$$

Da der hintere Faktor wie jeder Binomialkoeffizient eine ganze Zahl ist, ist daher p ein Teiler von $\binom{p^2}{p}$. Ferner ist p^2 aber kein Teiler, da im Zähler des hinteren Faktors die Primzahl p kein einziges Mal vorkommt (wieso?) [im Nenner auch nicht, aber das tut nichts zur Sache].

Aufgabe 5. *Primitive Wurzeln*

a) Gib alle primitiven Wurzeln *modulo* 5 an.

b) Sei X die Menge der n-ten *komplexen* Einheitswurzeln. Zeige, dass die Abbildung

$$\sigma_d : X \longrightarrow X,\ \zeta \longmapsto \zeta^d$$

genau dann eine Bijektion ist, wenn die feste natürliche Zahl d teilerfremd zu n ist.

Lösung.

a) Eine *primitive Wurzel modulo* p ist eine solche $(p-1)$-te Einheitswurzel in $\mathbb{Z}/(p)$, sodass jede $(p-1)$-te Einheitswurzel in $\mathbb{Z}/(p)$ eine gewisse Potenz von ihr ist.

Von den Zahlen $0, 1, 2, 3, 4$ sind genau die Zahlen $1, 2, 3, 4$ vierte Einheitswurzeln, denn es gilt

$$0^4 \equiv 0, \qquad 1^4 \equiv 1, \qquad 2^4 \equiv 1, \qquad 3^4 \equiv 1, \qquad 4^4 \equiv 1$$

modulo 5. Zur Überprüfung der Primitivität legen wir folgende Tabelle an:

ξ	ξ^0	ξ^1	ξ^2	ξ^3	ξ^4	ξ^5	$\cdots$
1	1	1	1	1	1	1	$\cdots$
2	1	2	4	3	1	2	$\cdots$
3	1	3	4	2	1	3	$\cdots$
4	1	4	1	4	1	4	$\cdots$

Also sind 2 und 3 primitive Wurzeln modulo 5, da in ihren Zeilen *alle* vierten Einheitswurzeln vorkommen. Die Zahlen 1 und 4 sind zwar vierte Einheitswurzeln, aber nicht primitive vierte Einheitswurzeln.

b) *Fall 1:* d ist teilerfremd zu n. Dann gibt es eine Bézoutdarstellung $1 = ad + bn$. Folglich ist σ_a Umkehrabbildung zu σ_d: Für alle $\zeta \in X$ gilt

$$(\sigma_a \circ \sigma_d)(\zeta) = (\zeta^d)^a = \zeta^{1-bn} = \zeta \cdot (\zeta^n)^{-b} = \zeta \cdot 1 = \zeta$$

und analog gilt $(\sigma_d \circ \sigma_a)(\zeta) = \zeta$.

Fall 2: d ist nicht teilerfremd zu n. Dann gibt es also einen gemeinsamen Teiler $k \geq 2$, sodass $d = pk$ und $n = qk$ für gewisse $p, q \geq 0$. Sei ζ_0 eine feste primitive n-te Einheitswurzel. Dann folgt

$$\sigma_d(\zeta_0^q) = \zeta_0^{qd} = \zeta_0^{qpk} = \zeta_0^{np} = (\zeta_0^n)^p = 1^p = 1 = \sigma_d(1),$$

also ist σ_d nicht injektiv (es gilt $\zeta_0^q \neq 1 = \zeta_0^0$) und somit insbesondere nicht bijektiv.

Zur Erinnerung: **Algebra-Treffen** am 10. Juli um 18:30 Uhr