

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

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 $n / \text{ggT}(n, m)$ gegeben ist.
- b) Bestimme die Ordnungen aller Elemente der zyklischen Gruppe C_n .
- c) Bestimme alle Erzeuger der zyklischen Gruppe C_n .

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:

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

b) Wir fügen zunächst künstlichen 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 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.

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

$$a^p \equiv a \pmod{p}.$$

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

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

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

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

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

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

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

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

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

ξ	ξ^0	ξ^1	ξ^2	ξ^3	ξ^4	ξ^5	\dots
1	1	1	1	1	1	1	\dots
2	1	2	4	3	1	2	\dots
3	1	3	4	2	1	3	\dots
4	1	4	1	4	1	4	\dots

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.

Zur Erinnerung: **Algebra-Treffen** am 10. Juli um 18:30 Uhr in Raum 2004/L1.