Moritz Mossböck, 11820925
Andreas Archer, 11816749

Übungsblatt № 2

Eine kleine Anmerkung: Die disjunkte Vereinigung von Mengen schreiben wir als $\uplus$ an. Des weiteren schreiben wir in allgemeinen Gruppen $(G, \circ)$ Verknüpfungen $a \circ b$ als ab an. Für $X, Y \subseteq G$, schreiben wir $X \circ Y = \{xy | x \in X, y \in Y\}$ als XY an.

Aufgabe 2.1: Untergruppen endlicher Gruppen

a) Zeigen Sie: Für eine endliche Gruppe $(G, \circ)$ ist eine Teilmenge U von G genau dann eine Untergruppe von G, wenn $1 \in U$ und $\forall a, b \in U : ab \in U$
b) Gilt die Aussage aus a) auch noch, wenn man von $(G, \circ)$ nicht mehr voraussetzt, endlich zu sein?

Zu a): $\Rightarrow$. Sei $U \leq G$. Da U eine Gruppe ist, folgt laut Definition $\forall a, b \in U : ab \in U$. Es bleibt zu zeigen, dass $1 \in U$. Sei 1_U das neutrale Element von $(U, \circ|_{U^2})$. Dann folgt:

$$1_U 1_U = 1_U \qquad 1_G 1_U = 1_U \Rightarrow 1_U 1_U = 1_G 1_U$$

Nach den Kürzungsregeln folgt $1_U = 1_G \in U$.

$\Leftarrow$: Sei $a \in U$, dann gilt $\forall n \in \mathbb{N}: a^n \in U$. Da G endlich ist, ist auch U endlich. Angenommen, $\nexists k \in \mathbb{N}: a^k = 1$, dann gilt $\forall k, l \in \mathbb{N}: a^k \neq a^{k+l}$. Das ist aber ein Widerspruch dazu, dass U endlich ist. Es gibt also ein $k \in \mathbb{N}$, sodass $a^k = 1$, womit aus der Assoziativität folgt:

$$aa^{k-1} = a^{k-1}a = 1$$

Sprich $a^{k-1} = a^{-1} \in U$. Somit gilt:

1. $\forall a, b \in U : ab \in U$
2. $\exists 1 \in U : \forall a \in U : 1a = a1 = a$
3. $\forall a, b, c \in U : (ab)c = (ab)c$
4. $\forall a \in U : \exists a^{-1} \in U : aa^{-1} = a^{-1}a = 1$

Daher ist $(U, \circ)$ eine Gruppe.

Zu b): Wir finden ein Gegenbeispiel. $(\mathbb{Z}, +)$ ist eine Gruppe. Allerdings gilt für $N_0 \subseteq \mathbb{Z}$, dass $\forall m, n \in \mathbb{N}_0 : m+n \in \mathbb{N}_0$, allerdings ist $(\mathbb{N}_0, +)$ keine Gruppe, sondern nur ein Monoid.

Aufgabe 2.2: Turmsatz für den Index

Es sie $(G, \circ)$ eine Gruppe mit Untergruppen $V \leq U \leq G$. Ferner seien

$$G = \biguplus_n a_n U \qquad U = \biguplus_m b_m V$$

disjunkte Zerlegungen von G und U in Linksnebenklassen. Die Indices m und n mögen hier jeweils über geeignete Indexmengen N und M durchlaufen. Zeigen Sie:

a)

$$G = \biguplus_{n,m} a_n b_m V$$

b) Ist G endlich, so gilt:

$$[G : V] = [G : U][U : V]$$

Zu a):

Sei $a \in G$ und X, Y seien verschiedene Linksnebenklassen von $V \subseteq G$. Wir wollen zeigen, dass $aX \cap aY = \emptyset$. Angenommen, es gäbe $b \in aX \cap aY$, dann gilt aber $\exists x \in X, y \in Y$, sodass:

$$ax = b = ay$$

Nach den Kürzungsregeln folgt damit $x = y$, womit $X = Y$. Wir wollen nun das folgende zeigen:

$$a(X \uplus Y) = aX \uplus aY$$

Dazu sei $t \in X \uplus Y$. Da $aX \cap aY = \emptyset$, folgt $at \in aX \dot\vee at \in aY$, bzw. $at \in aX \uplus aY$, hernach also $a(X \uplus Y) \subseteq aX \uplus aY$.

Sei nun $at \in aX \uplus aY$, ergo $at \in aX \dot\vee at \in aY$, womit $t \in X \dot\vee t \in Y$, ergo $at \in a(X \uplus Y)$. Damit erhalten wir $aX v aY \subseteq a(X \uplus Y)$, somit aber auch $a(X \uplus Y) = aX \uplus aY$. Seien nun V_i für $i \in I$ paarweise verschiedene Linksnebenklassen von V, dann gilt

$$a \biguplus_{i \in I} V_i = a \left(V_n \uplus \left(\biguplus_{i \in I \setminus \{n\}} V_i \right) \right) = aV_n \uplus a \biguplus_{i \in I \setminus \{n\}} V_i = aV_n \uplus \biguplus_{i \in I \setminus \{n\}} aV_i = \biguplus_{i \in I} aV_i$$

Hernach:

$$G = \biguplus_{n \in N} a_n \biguplus_{m \in N} b_m V = \biguplus_{n \in N} \biguplus_{m \in M} a_n b_m V = \biguplus_{n \in N, m \in M} a_n b_m V$$

Zu b):

$$|G| = \left| \biguplus_{m \in M, n \in N} a_n b_m V \right| = \sum_{n \in N} \sum_{m \in M} |a_n b_m V| = \sum_{n \in N} \sum_{m \in M} |V| = \sum_{n \in N} |V| [U : V] = |V| \cdot [G : U][U : V]$$

Nach dem Satz von Lagrange gilt nun (und weil G endlich ist):

$$[G : V] = \frac{|G|}{|V|} = [G : U][U : V]$$