DS1-Zentralübung – 20.11.03 (WS03/04)
(Dr. P. Ullrich)

Wiederholung. Ist G eine Gruppe und H ein Normalteiler von G, so ist die *Faktorgruppe* $(G/H, \cdot)$ wie folgt definiert:

1) $G/H = \{aH : a \in G\}$ = Menge aller Linksnebenklassen von H.

2) $\cdot : G/H \times G/H \to G/H$, $(aH, bH) \mapsto aH \cdot bH := abH$.

Man rechnet leicht nach, dass $(G/H, \cdot)$ alle Gruppenaxiome erfüllt. Insbesondere ist $H = 1H$ das Einselement, und $(aH)^{-1} = a^{-1}H$. Da H ein Normalteiler ist, ist die Verknüpfung (binärer Operator) "$\cdot$" wohldefiniert. Zudem gilt $aH = Ha$ für alle $a \in G$, d.h. G/H ist auch die Menge aller Rechtsnebenklassen von G.

Satz (1. Isomorphiesatz)
Sei $f : G \to G'$ ein Gruppenhomomorphismus, und sei $H = \ker(f)$. Dann ist

$$\bar{f} : G/H \to \mathrm{im}(f),\ aH \mapsto f(a)$$

ein Gruppenisomorphismus.

Beweis. Zunächst müssen wir zeigen, dass die Abbildung $\bar{f}$ wohldefiniert ist, d.h. dass $f(a) = f(b)$ aus $aH = bH$ folgt (ansonsten wäre $\bar{f}$ keine Funktion, sondern nur eine Relation). Gilt $aH = bH$ für $a, b \in G$, so folgt $ab^{-1} \in H$. Da $H = \ker(f)$ gilt, ist $f(ab^{-1}) = 1_{G'}$. Da f ein Homomorphismus ist, gilt $f(ab^{-1}) = f(a)f(b)^{-1}$. Somit folgt $f(a)f(b)^{-1} = 1_{G'}$ und wir erhalten $f(a) = f(b)$.
Als nächstes zeigen wir, dass $\bar{f}$ ein Gruppenhomomorphismus ist. Seien $aH, bH \in G/H$ gegeben. Dann ist

$$\bar{f}(aH \cdot bH) = \bar{f}(abH) = f(ab) = f(a)f(b) = \bar{f}(aH) \cdot \bar{f}(bH);$$

hierbei haben wir ausgenutzt, dass f ein Gruppenhomomorphismus ist.
Da $\bar{f}$ ein Gruppenhomomorphismus ist, ist "Injektivität" äquivalent zu "$\ker(\bar{f}) = \{1_{G/H}\}$". Sei demnach $aH \in \ker(\bar{f})$, d.h. $\bar{f}(aH) = 1_{G'}$. Wegen $\bar{f}(aH) = f(a)$ folgt $f(a) = 1_{G'}$, also $a \in \ker(f)$. Wegen $H = \ker(f)$ ist dann $aH = H$. Es ist $H = 1_{G/H}$ das Einselement von G/H. Somit haben wir $\ker(\bar{f}) = \{1_{G/H}\}$ gezeigt, also ist $\bar{f}$ injektiv.
Die Surjektivität ist offensichtlich, denn sei $b \in \mathrm{im}(f)$. Wählt man $a \in G$ mit $f(a) = b$, so gilt $\bar{f}(aH) = f(a) = b$.

Bemerkung. Ist $f : G \to G'$ ein Gruppenhomomorphismus, so sagt der 1.Isomorphiesatz (es gibt noch weitere) aus, dass die Gruppe G eine ähnliche Gestalt hat, wie eine Untergruppe von G'. Gibt es somit einen Homomorphismus von einer Gruppe G in eine Gruppe G', so kann man eine ähnliche Struktur von G in G' wieder erkennen; daher auch der Name "Homomorphismus". Betrachtet man das Bild $H' = \mathrm{im}(f)$ von f, so ist H' eine Untergruppe von G'. G und H' haben eine ähnliche Gruppenstruktur. Jedoch entsprechen sich die Punkte von G und H' i.a. nicht eineindeutig. Zwar gibt es zu jedem $a' \in H'$ ein $a \in G$ mit $f(a) = a'$, jedoch kann es i.a. noch weitere Elemente $b \in G$ mit $f(b) = a'$ geben. Man kann leicht zeigen, dass die Nebenklasse aH, wobei $H = \ker(f)$ ist, gleich der Menge aller Punkte $b \in G$ ist, die unter f auf $a' = f(a)$ abgebildet werden (Übung!), d.h. $aH = f^{-1}(f(a)) = \{b \in G : f(b) = f(a)\}$. Fasst man die aH $(a \in G)$ als Punkte einer neuen Menge auf – wir hatten diese neue Menge mit G/H bezeichnet –, so erhält man eine 1-zu-1 Korrespondenz. Definiert man auf G/H obige Gruppenstruktur (siehe Faktorgruppe), so ist diese 1-zu-1 Korrespondenz ein Isomorphismus.

Beispiel. Betrachte den Gruppenhomomorphismus $f : \mathbb{Z} \to \mathbb{Z}_n$, $m \mapsto m \mod n$. Dieser ist surjektiv und es gilt $\ker(f) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Nach dem 1. Isomorphiesatz ist die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ isomorph zu $\mathbb{Z}_n$.

Lemma. Sei G eine Gruppe. Für $a \in G$ gelte $\mathrm{ord}(g) = mk$, $(1 \leq m, k \in \mathbb{N})$. Dann gilt $\mathrm{ord}(a^k) = m$.

Beweis. Es gilt $(a^k)^m = a^{km} = 1$. Sei $1 \leq q < m$. Dann ist $1 \leq kq < km$, und wegen $\mathrm{ord}(a) = km$ gilt $a^{kq} \neq 1$, also gilt auch $(a^k)^q \neq 1$.