Proseminar Körpertheorie

Elemente der Gruppentheorie

Marcus Kühn

20. Juni 2013
Prof. Dr. K. Wingberg, K. Hübner

1 Der Satz von Lagrange

1.1 Satz von Lagrange:

Sei G eine endliche Gruppe und sei H eine Untergruppe von G. Dann teilt die Ordnung von H die Ordnung von G:

$$\#H | \#G$$

Insbesondere teilt auch die Ordnung jedes Elements der Gruppe G die Ordnung von G:

$$\forall g \in G : ord(g) | \#G$$

(die Ordnung eines Elements ist die kleinste natürliche Zahl $n \in \mathbb{N}$ mit $g^n = e_G$, wobei e_G hier und im Folgenden das neutrale Element in der Gruppe G bezeichne.)

Beweis:
Sei G eine Gruppe und H eine Untergruppe von G. Definition einer Äquivalenzrelation auf G:
Sei für $g, g' \in G$:

$$g \sim g' :\Leftrightarrow \exists h \in H : g' = g \cdot h$$

Dies ist eine Äquivalenzrelation:

Reflexivität: Sei $g \in G$.

Es ist:

$$\begin{aligned} & g = g \cdot e_G \\ \Rightarrow\ & g \sim g && \text{'}H \text{ Untergruppe von } G \end{aligned}$$

Symmetrie: Seien $g, g' \in G$ mit $g \sim g'$

Es ist:

$$\begin{aligned}
& g \sim g' \\
\Leftrightarrow\ & g' = g \cdot h && \text{'für geeignetes } h \in H \\
\Leftrightarrow\ & g \cdot h^{-1} = g' && \text{'} h \in G \\
\Rightarrow\ & g' \sim g && \text{'} H \text{ ist Gruppe} \Rightarrow h^{-1} \in H
\end{aligned}$$

Transitivität: Seien $g, g', g'' \in G$ mit $g \sim g'$ und $g' \sim g''$

Es ist:

$$\begin{aligned}
& (g \sim g' \wedge g' \sim g'') \\
\Leftrightarrow\ & (g' = g \cdot h \wedge g'' = g' \cdot h') && \text{'für geeignete } h, h' \in H \\
\Rightarrow\ & g'' = (g \cdot h) \cdot h'' \\
\Leftrightarrow\ & g'' = g \cdot (h \cdot h'') \\
\Rightarrow\ & g \sim g'' && \text{'} H \text{ ist Gruppe} \Rightarrow (h \cdot h' \in H)
\end{aligned}$$

Betrachten der Äquivalenzklassen:

Für $g \in G$ ist:

$$[g] = \{g \cdot h | h \in H\} =: gH$$

Sei $\varphi : H \to gH; h \mapsto g \cdot h$. φ ist eine Bijektion:

Surjektivität: φ ist nach Konstruktion von gH surjektiv
Injektivität: Seien $h, h' \in H$.

Es ist:

$$\begin{aligned}
& \varphi(h) && = \varphi(h') \\
\Leftrightarrow\ & g \cdot h && = g \cdot h' \\
\Leftrightarrow\ & h && = h' && \text{'} G \text{ ist Gruppe}
\end{aligned}$$

Folglich ist φ injektiv.

Da φ bijektiv ist folgt:

$$\#gH = \#H$$

Äquivalenzklassen bilden eine Partition. G ist also die disjunkte Vereinigung aller Äquivalenzklassen. Sei nun $n \in \mathbb{N}$ die Anzahl der paarweise verschiedenen Äquivalenzklassen. Diese bilden nun eine Partition von G, also folgt:

$$\begin{aligned} & \#G = n \cdot \#gH \\ \Leftrightarrow\ & \#G = n \cdot \#H && \text{'\#gH=\#H} \end{aligned}$$

Die Ordnung von G ist also ein Vielfaches der Ordnung von H. Die Ordnung von H teilt also die von G.
Die Ordnung n eines Elements g der Gruppe G teilt die der Gruppe G, da die Ordnung n eines Gruppenelements $g \in G$ der Mächtigkeit der von diesem Element erzeugten Untergruppe $\langle g \rangle$ entspricht:

$$\begin{aligned} & \#\langle g \rangle \\ = & \#\{e_G, g, g^2, \ldots, g^{n-1}\} && 'g^z := \underbrace{g \ldots g}_{z\text{-mal}} \\ = & n \end{aligned}$$

□

1.2 Definition:

Sei G eine Gruppe und H eine Untergruppe von G sowie $g \in G$ ein Element aus G. Die rechte Nebenklasse gH von H nach g ist dann wie folgt definiert:

$$gH := \{g \cdot h | h \in H\}$$

Analog wird die linke Nebenklasse Hg von H nach g definiert:

$$Hg := \{h \cdot g | h \in H\}$$

1.3 Definition:

Sei G eine Gruppe und H eine Untergruppe von G. Dann notiert man die Menge aller rechten Nebenklassen von H bezüglich Gruppenelementen aus G mit G/H:

$$G/H := \{gH | g \in G\}$$

Analog wird die Menge aller linken Nebenklassen von H bezüglich Gruppenelementen aus G mit $H\backslash G$ notiert:

$$H\backslash G := \{Hg | g \in G\}$$

1.4 Bemerkung:

Sei G eine endliche Gruppe und H eine Untergruppe von G. Dann gilt:

$$\#(G/H) = \#(H\backslash G)$$

Beweis:
Sei G eine endliche Gruppe und H eine Untergruppe von G. Sei $\varphi : G/H \to H\backslash G; gH \mapsto Hg$.
Die Abbildung φ ist bijektiv:

> *Surjektivität:* φ ist nach Konstruktion von G/H und $H\backslash G$ surjektiv
> *Injektivität:* Seien $gH, g'H \in G/H$.
>
> Es ist:
>
> $$\begin{aligned} &\varphi(gH) &&= \varphi(g'H) && \\ \Leftrightarrow\ &Hg &&= Hg' && \\ \Rightarrow\ &g &&\in Hg' && \text{'}H \text{ Untergruppe von } G \Rightarrow e_G \in H \\ \Rightarrow\ &\exists h' \in H : g &&= g' \cdot h' && \end{aligned}$$

Es folgt:

$$
\begin{aligned}
& g'H && = (g \cdot h')H \\
\Leftrightarrow\ & g'H && = \{(g \cdot h') \cdot h | h \in H\} \\
\Leftrightarrow\ & g'H && = \{(g \cdot (h' \cdot h) | h \in H\} \\
\Leftrightarrow\ & g'H && = \{(g \cdot h) | h \in H\} && \text{'}H \text{ ist Gruppe} \\
\Leftrightarrow\ & g'H && = gH
\end{aligned}
$$

Folglich ist φ injektiv.

□

1.5 Definition:

Sei G eine endliche Gruppe und H eine Untergruppe von G. Der Index $(G : H)$ von H in G ist definiert als die Mächtigkeit der Menge aller rechten Nebenklassen von H bezüglich Gruppenelementen aus G bzw. der Mächtigkeit der Menge aller linken Nebenklassen von H bezüglich Gruppenelementen aus G:

$$(G : H) := \#(G/H) = \#(H \backslash G)$$

2 Operationen auf einer Menge

2.1 Definition:

Sei X eine Menge und G eine Gruppe. Eine Operation der Gruppe G auf der Menge X ist eine Abbildung $\varphi : G \times X; (g,x) \mapsto \varphi((g,x))$, wobei $\varphi((g,x))$ auch als $g \cdot x$ oder gx notiert wird, für die gilt:

(i) $\forall x \in X : e_G \cdot x = x$

(ii) $\forall x \in X : g(hx) = (gh)x$

2.2 Definition:

Sei X eine Menge und G eine auf X operierende Gruppe. Die Bahn Gx eines Elements x der Menge X bezüglich der auf X operierenden Gruppe G ist wie folgt definiert:

$$Gx := \{gx | g \in G\}$$

2.3 Definition:

Sei X eine Menge und G eine auf X operierende Gruppe. Der Stabilisator G_x eines Elements x der Menge X bezüglich der auf X operierenden Gruppe G ist wie folgt definiert:

$$G_x := \{g \in G | gx = x\}$$

2.4 Definition:

Sei X eine Menge und G eine auf X operierende Gruppe. Ein Element $x \in X$ heißt Fixpunkt eines Elements $g \in G$, wenn gilt:

$$gx = x$$

Ist ein Element $x \in X$ Fixpunkt aller Gruppenelemente, so heißt x Fixpunkt der Operation oder Fixpunkt von G.

3 Klassengleichung

3.1 Bemerkung:

Sei X eine Menge und G eine auf X operierende Gruppe. Der Stabilisator G_x eines Elements $x \in X$ ist eine Untergruppe von G.

Beweis:
Sei X eine Menge und G eine auf X operierende Gruppe und G_x der Stabilisator eines Elements x der Menge X. Es ist zu zeigen, dass G_x bezüglich der Gruppenverknüpfung von G abgeschlossen ist, dass diese Gruppenverknüpung auch in G_x assoziativ ist, sowie, dass es zu jedem Element aus G_x ein bezüglich genannter Verknüpfung Inverses in G_x gibt, und dass $e_G \in G_x$ gilt:

Assoziativität: Es gilt: $G_x = \{g \in G | gx = x\} \subset G$. Die Verknüpfung ist auf ganz G assoziativ, also auch auf G_x.

Abgeschlossenheit: Seien $g, h \in G_x$

Es ist:

$$\begin{aligned}
&(gh)x \\
&= g(hx) && \text{'Gruppenoperation} \\
&= gx && \text{'}h \in G_x \\
&= x && \text{'}g \in G_x
\end{aligned}$$

Es folgt:

$$gh \in G_x$$

Existenz des neutralen Elements:

Es ist:

$$\begin{aligned}
&e_G x = x \\
&\Rightarrow e_G \in G_X
\end{aligned}$$

Existenz von Inversen: Sei $g \in G_x$

Es ist:

$$
\begin{aligned}
& g^{-1}x \\
&= g^{-1}(gx) && \text{'}g \in G_x \\
&= (g^{-1}g)x && \text{'Gruppenoperation} \\
&= x
\end{aligned}
$$

Es folgt:

$$g^{-1} \in G_x$$

□

3.2 Bemerkung:

Sei X eine Menge und G eine auf X operierende Gruppe. Sei x ein Element der Menge X. Für zwei Elemente g und g' aus der Gruppe G gilt folgende Äquivalenz:

$$gx = g'x \Leftrightarrow g' \in gG_x \Leftrightarrow g'G_x = gG_x$$

(Die Notation gG_x ist sinnvoll, da gG_x nach Bemerkung 3.1 eine Untergruppe von G ist)
Die Abbildung $\varphi_x : G \to X; g \mapsto gx$ induziert also eine Bijektion zwischen der Menge rechter Nebenklassen G/G_x des Stabilisators von x und der Bahn Gx von x.

Beweis:
Sei $x \in X$ und seien $g, g' \in G$.

Es ist:

$$
\begin{aligned}
& g'x = gx \\
\Leftrightarrow\ & g^{-1}g'x = x \\
\Leftrightarrow\ & g^{-1}g' \in G_x \\
\Leftrightarrow\ & g' \in gG_x \\
\Leftrightarrow\ & \exists h \in G_x : g' = g \cdot h \\
\Leftrightarrow\ & g'G_x = (g \cdot h)G_x \\
\Leftrightarrow\ & g'G_x = g(hG_x) \\
\Leftrightarrow\ & g'G_x = gG_x
\end{aligned}
$$

$\square$

3.3 Bemerkung:

Sei X eine Menge und G eine auf X operierende Gruppe. Aus der Existenz der in Bemerkung 3.2 erwähnten Bijektion ergibt sich bei einer endlichen auf X operierenden Gruppe G für jedes Element x der Menge X:

$$\#Gx = \#(G/G_x) = (G : G_x) = \tfrac{\#G}{\#G_x}$$

Beweis:
Sei X eine Menge und G eine auf X operierende Gruppe. Die in Bemerkung 3.2 erwähnte Bijektion zeigt unmittelbar:

$$\#Gx = \#(G/G_x)$$

Nach Definition des Index (Definition 1.5) gilt:

$$\#(G/G_x) = (G : G_x)$$

Gemäß des vorangegangen Beweis des Satzes von Lagrange (Satz 1.1), insbesondere nach Betrachtung der dort eingeführten Äquivalenzrelation, gilt:

$$\begin{aligned}
& \#G = \#(G/G_x) \cdot \#G_x \\
\Leftrightarrow\ & \tfrac{\#G}{\#G_x} = \#(G/G_x) && \text{'}G_x \text{ Gruppe} \Rightarrow \#G_x \neq 0 \\
\Leftrightarrow\ & (G : G_x) = \tfrac{\#G}{\#G_x} && \text{'Indexdefinition (Definition 1.5)}
\end{aligned}$$

□

3.4 Bemerkung:

Sei X eine Menge und G eine auf X operierende Gruppe.

(i) Die Menge X ist die Vereinigung aller ihrer Bahnen.

(ii) Für zwei Elemente x und y aus der Menge X sind die Bahnen Gx und Gy disjunkt oder gleich.

Beweis:
Sei X eine Menge und G eine auf X operierende Gruppe.
(i) Es ist:

$$\begin{aligned}
& \forall x \in X : Gx = \{gx | g \in G\} \\
\Rightarrow\ & \forall x \in X : Gx \subset X && \text{'Die Zielmenge der Gruppenoperation ist } X \\
\Rightarrow\ & \textstyle\bigcup_{x \in X} Gx \subset X
\end{aligned}$$

Zudem:

$$\begin{aligned}
& \forall x \in X : x = e_G x \\
\Rightarrow\ & \forall x \in X : x \in \{gx | g \in G\} \\
\Leftrightarrow\ & \forall x \in X : x \in Gx \\
\Rightarrow\ & X \subset \textstyle\bigcup_{x \in X} Gx
\end{aligned}$$

Also:

$$\textstyle\bigcup_{x \in X} Gx = X$$

(ii) Seien $x, y \in X$ mit $Gx \cap Gy \neq \emptyset$. Es ist nun zu zeigen, dass solche nicht disjunkten Bahnen Gx und Gy gleich sind wenn sie existieren.
Seien $g, h \in G$ so gewählt, dass $gx = hy$ gilt. (diese Elemente aus G existieren, da $Gx \cap Gy \neq \emptyset$)
Es ist:

$$\begin{aligned} & gx = hy \\ \Leftrightarrow\ & h^{-1}gx = y \end{aligned}$$

und:

$$\begin{aligned} & gx = hy \\ \Leftrightarrow\ & x = g^{-1}hy \end{aligned}$$

Es folgt:

$$\begin{aligned} & Gy \\ & = \{g'y | g' \in G\} \\ & = \{g'h^{-1}gx | g' \in G\} \\ & \subset \{g'x | g' \in G\} && \text{'}G \text{ Gruppe} \Rightarrow g'h^{-1}g \in G \\ & = Gx \end{aligned}$$

und:

$$\begin{aligned} & Gx \\ & = \{g'x | g' \in G\} \\ & = \{g'h^{-1}gy | g' \in G\} \\ & \subset \{g'y | g' \in G\} && \text{'}G \text{ Gruppe} \Rightarrow g'h^{-1}g \in G \\ & = Gy \end{aligned}$$

also:

$$Gx = Gy$$

□

3.5 Klassengleichung:

Aus den Bemerkungen 3.1 bis 3.4 folgt: Für jedes Element aus der Menge der Bahnen der Elemente der Menge X kann Gx_i als Repräsentant dieser Bahn gewählt werden und es wird gelten (Bemerkung 3.4 (i)):

$$X = \bigcup_i Gx_i$$

Und somit folgt mit den Bemerkungen 3.4(ii) und Bemerkung 3.3 die Klassengleichung:

$$\#X = \sum_i \#Gx_i = \sum_i \frac{\#G}{\#G_{x_i}}$$

4 Das Zentrum einer p-Gruppe

Sei G eine endliche Gruppe mit p^2 Elementen wobei p eine Primzahl ist. Dann ist G abelsch.

Beweis:
Sei $Z := \{z \in G | \forall g \in G : gz = zg\}$ das Zentrum von G. Z ist eine Untergruppe von G:

Assoziativität: Es gilt: $Z = \{z \in G | \forall g \in G : gz = zg\} \subset G$. Die Verknüpfung ist auf ganz G assoziativ, also auch auf Z.

Abgeschlossenheit: Seien $z_1, z_2 \in Z$ und $g \in G$

Es ist:

$$
\begin{aligned}
&(z_1 z_2)g \\
&= z_1 z_2 g && \text{'Assoziativität der Gruppenverknüpfung} \\
&= z_1 g z_2 && \text{'}z_2 \in Z \\
&= g z_1 z_2 && \text{'}z_1 \in Z \\
&= g(z_1 z_2)
\end{aligned}
$$

Es folgt:

$$(z_1 z_2) \in Z$$

Existenz des neutralen Elements:

Es ist:

$$
\begin{aligned}
&\forall g \in G : g e_G = e_G g \\
&\Rightarrow e_G \in Z
\end{aligned}
$$

Existenz von Inversen: Sei $z \in Z$, $g \in G$

Es ist:

$$\begin{aligned} & z^{-1}g \\ &= z^{-1}gzz^{-1} \\ &= z^{-1}zgz^{-1} && \text{'}z \in Z \\ &= gz^{-1} \end{aligned}$$

Es folgt:

$$z^{-1} \in Z$$

Nach dem Satz von Lagrange folgt somit:

$$\begin{aligned} & \#Z|\#G \\ \Rightarrow\ & \#Z|p^2 \\ \Rightarrow\ & \#Z = \{1, p, p^2\} && \text{'}p \text{ ist Primzahl} \end{aligned}$$

Betrachte $\#Z = 1$:

Hier ist $Z = \{e_G\}$, denn für ein beliebiges Element G der Gruppe G gilt:

$$\begin{aligned} & ge_G = e_G g \\ \Rightarrow\ & e_G \in Z \end{aligned}$$

Operiere G auf G mit der Konjugation $\varphi : G \times G \to G; (g_1, g_2) \mapsto g_1 g_2 g_1^{-1}$. Dies ist eine Operation, denn für $g, h, x \in G$ gilt:

$$\begin{aligned} & \varphi(e_G, g) \\ &= e_G g e_G^{-1} \\ &= g \end{aligned}$$

und:

$$\begin{aligned}
&\varphi(gh, x) \\
=\ &(gh)x(gh)^{-1} \\
=\ &ghxh^{-1}g^{-1} \\
=\ &g\varphi(h, x)g^{-1} \\
=\ &\varphi(g, \varphi(h, x))
\end{aligned}$$

Bezüglich dieser Operation gilt für eine beliebige Bahn Gx eines Elements x der Menge G:

$$\begin{aligned}
&\#Gx = \tfrac{\#G}{\#G_x} && \text{'Bemerkung 3.3} \\
\Rightarrow\ &\#Gx \in \{\tfrac{p^2}{1}, \tfrac{p^2}{p}, \tfrac{p^2}{p^2}\} && \text{'Bemerkung 3.1; Satz von Lagrange} \\
\Leftrightarrow\ &\#Gx \in \{1, p, p^2\}
\end{aligned}$$

Für alle Bahnen Gx mit $\#Gx = 1$ gilt:

$$\begin{aligned}
&e_G x e_G^{-1} = x \\
\Rightarrow\ &x \in Gx \\
\Leftrightarrow\ &Gx = \{x\} && \text{'}\#Gx = 1 \\
\Leftrightarrow\ &\{gxg^{-1} | g \in G\} = \{x\} \\
\Leftrightarrow\ &\forall g \in G : gxg^{-1} = x \\
\Leftrightarrow\ &\forall g \in G : gx = xg \\
\Leftrightarrow\ &x \in Z \\
\Leftrightarrow\ &x = e_G && \text{'}Z = \{e_G\} \\
\Rightarrow\ &Gx = Ge_G
\end{aligned}$$

Mit der Klassengleichung ergibt sich also:

$$p^2 = 1 + \textstyle\sum_i p^{n_i} \qquad \text{mit} \qquad n_i \in \{1, 2\}$$

Ist p eine Primzahl, so darf die rechte Summe über alle i nicht leer sein, da $p^2 \neq 1$ ist. Weiterhin muss für alle n_i $n_i \neq 2$ gelten, da $p^2 < 1 + p^2$. folglich müsste nach der Klassengleichung gelten:

$$
\begin{aligned}
& p^2 = 1 + n \cdot p \qquad \text{mit} \qquad n \in \mathbb{N} \\
\Leftrightarrow\ & p - \tfrac{1}{p} \in \mathbb{N}
\end{aligned}
$$

Die untere Aussage ist für eine Prizahl p aber offensichtlich unerfüllaber. Folglich ist $\#Z \neq 1$.

Betrachte $\#Z = p$

Sei $x \in G \backslash Z$, $Z(x) := \{g \in G | gx = xg\}$ der Zentralisator von x.
Es ist:

$$
\begin{aligned}
& \forall z \in Z : \forall g \in G : gz = zg \\
\Rightarrow\ & \forall z \in Z : gx = xg \\
\Leftrightarrow\ & \forall z \in Z : z \in Z(x) \\
\Leftrightarrow\ & Z \subset Z(x)
\end{aligned}
$$

und:

$$
\begin{aligned}
& xx = xx \\
\Leftrightarrow\ & x \in Z(x)
\end{aligned}
$$

mit $x \in G \backslash Z$, also $x \notin Z$ folgt dann:

$$\#Z(x) > \#Z$$

Des weiteren ist $Z(x)$ eine Untergruppe von G:

Assoziativität: Es gilt: $Z(x) = g \in G | gx = xg\} \subset G$. Die Verknüpfung ist auf ganz G assoziativ, also auch auf Z.

Abgeschlossenheit: Seien $z_1, z_2 \in Z(x)$

Es ist:

$$
\begin{aligned}
& (z_1 z_2) x \\
= \ & z_1 z_2 x && \text{'Assoziativität der Gruppenverknüpfung} \\
= \ & z_1 x z_2 && {}'z_2 \in Z(x) \\
= \ & x z_1 z_2 && {}'z_1 \in Z(x) \\
= \ & x (z_1 z_2)
\end{aligned}
$$

Es folgt:

$$(z_1 z_2) \in Z(x)$$

Existenz des neutralen Elements:

Es ist:

$$\begin{aligned} &\forall g \in G : g e_G = e_G g \\ \Rightarrow\ & e_G \in Z(x) \end{aligned}$$

Existenz von Inversen: Sei $z \in Z(x)$

Es ist:

$$\begin{aligned} & z^{-1}x \\ =\ & z^{-1}xzz^{-1} \\ =\ & z^{-1}zxz^{-1} && \text{'}z \in Z(x) \\ =\ & xz^{-1} \end{aligned}$$

Es folgt:

$$z^{-1} \in Z(x)$$

Nach dem Satz von Lagrange gilt also: $\#Z(x) \in \{1, p, p^2\}$, mit $\#Z(x) > \#Z$ folgt dann aber $\#Z = p^2$ und damit $x \in Z$, dies ist aber ein Widerspruch zur Wahl von x. Also gilt $\#Z \neq p$

Es folgt also schließlich $\#Z = p^2 = \#G$, alle Elemente der Gruppe G vertauschen also mit allen Elementen der Gruppe G, G ist also abelsch.
$\square$

5 Normalteiler

5.1 Definition:

Eine Untergruppe H einer Gruppe G heißt normal, wenn gilt:

$$\forall g \in G : \forall h \in H : g^{-1}hg \in H$$

5.2 Beispiele:

(i) Sei G eine Gruppe. $\{e_G\}$ und G sind normale Untergruppen von G
(ii) Untergruppen abelscher Gruppen sind normal.
(iii) Das Zentrum einer Gruppe ist normal.

5.3 Satz:

Der Kern eines Gruppenhomomorphismusses $\varphi : G \to G'$ ist eine normale Untergruppe von G.
Beweis:
Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. $ker\varphi$ ist eine Untergruppe:

Assoziativität: Es gilt: $ker\varphi = \{g \in G|\varphi(g) = e_{G'}\} \subset G$. Die Verknüpfung ist auf ganz G assoziativ, also auch auf Z.

Abgeschlossenheit: Seien $g, g \in ker\varphi$

Es ist:

$$\begin{aligned} & \varphi(gh) && \\ &= \varphi(g)\varphi(h) && \text{'}\varphi \text{ ist Gruppenhomomorphismus} \\ &= \varphi(h) && \text{'}g \in ker\varphi \\ &= e_{G'} && \text{'}h \in ker\varphi \end{aligned}$$

Es folgt:

$$(gh) \in ker\varphi$$

Existenz des neutralen Elements: Da φ ein Gruppenhomomorphismus ist gilt $e_G \in ker\varphi$

Existenz von Inversen: Sei $g \in ker\varphi$

Es ist:

$$
\begin{aligned}
& \varphi(g^{-1}) \\
&= \varphi(g^{-1}) \cdot \varphi(g) && g \in ker\varphi \\
&= \varphi(e_G) && \text{'}\varphi \text{ ist Gruppenhomomorphismus} \\
&= e_{G'} && e_G \in ker\varphi
\end{aligned}
$$

Es folgt:

$$g^{-1} \in ker\varphi$$

$ker\varphi$ ist normal:

Seien $g \in G$, $h \in ker\varphi$
Es ist:

$$
\begin{aligned}
& \varphi(g^{-1}hg) \\
&= \varphi(g)^{-1}\varphi(h)\varphi(g) && \text{'}\varphi \text{ ist Gruppenhomomorphismus} \\
&= \varphi(g)^{-1}\varphi(g) && \text{'}h \in ker\varphi \\
&= e_{G'}
\end{aligned}
$$

Es folgt:

$$g^{-1}hg \in ker\varphi$$

□

5.4 Definition einer Gruppenverknüpfung auf G/H für eine normale Untergruppe H

Sei G eine Gruppe und H eine Untergruppe von G. Man definiere eine Gruppenverknüpung auf G/Hq wie folgt:

$$\cdot : \qquad (G/H) \times (G/H) \to G/H \qquad ; \qquad (gH, g'H) \mapsto gg'H$$

Diese Verknüpfung ist wohldefiniert (Repräsentantenunabhängig):
Seien $g_1H, g_2H, g_1'H, g_2'H \in (G/H)$ mit $g_1H = g_2H$ und $g_1'H = g_2'H$. Es ist:

$$\begin{aligned} & g_1H && = g_2H \\ \Rightarrow\ & g_1e && \in g_2H \\ \Rightarrow\ & \exists hh \in H : g_1 && = g_2h \end{aligned}$$

analog:

$$\exists h \in H : g_1' = g_2'h'$$

Seien $h, h' \in H$ mit $g_1 = g_2h$ und $g_1' = g_2'h'$. Es ist:

$$\begin{aligned} & g_1H \cdot g_1'H \\ = & g_1'g_1H \\ = & (g_2hg_2'h')H \\ = & g_2hg_2'h'H \\ = & g_2hg_2'H \\ = & g_2g_2'g_2'^{-1}hg_2'H \\ = & g_2g_2'(g_2'^{-1}hg_2')H \\ = & g_2g_2'H && \text{'}H \text{ ist normal} \Rightarrow g_2'^{-1}hg_2' \in H \\ = & g_2H \cdot g_2'H \end{aligned}$$

Somit ist die Repräsentantenunabhängigkeit und damit die Wohldefiniertheit gezeigt. Mit dieser Verknüpfung wird G/H zu einer Gruppe:

Assoziativität: Seien $g_1H, g_2H, g_3H \in (G/H)$.

Es gilt:

$$\begin{aligned}
&(g_1Hg_2H)g_3H \\
&= g_1g_2Hg_3H \\
&= g_1g_2g_3H \\
&= g_1Hg_2g_3H \\
&= g_1H(g_2Hg_3H)
\end{aligned}$$

Abgeschlossenheit: Seien $gH, g'H \in (G/H)$

Es ist:

$$\begin{aligned}
&gHg'H \\
&= gg'H \\
&\in (G/H) && \text{'}gg' \in G
\end{aligned}$$

Es folgt:

$$gHg'H \in (G/H)$$

Existenz des neutralen Elements:

Es ist:

$$\forall gH \in (G/H) : gH \cdot eH = gH$$

Folglich ist $e_{G/H} = eH = H$.

Existenz von Inversen: Sei $gH \in (G/H)$

Es ist:

$$\begin{aligned}
&gH \cdot g^{-1}H \\
&= eH \\
&= e_{G/H}
\end{aligned}$$

Also ist $g^{-1}H = gH^{-1}$. Des Weiteren ist $g^{-1} \in G$ und somit $gH^{-1} = g^{-1}H \in (G/H)$.

Die Abbildung $\pi : G \to (G/H); g \mapsto gH$ ist somit ein surjektiver Gruppenhomomorphismus mit $ker\pi = H$:

Surjektivität: π ist nach Konstrutkion von G/H surjektiv.
Gruppenhomomorphismus: Seien $g, g' \in G$

Es ist:

$$\begin{aligned} &\pi(gg') \\ &= gg'H \\ &= gH \cdot g'H \\ &= \pi(g)\pi(g') \end{aligned}$$

$ker\pi = H$: Sei $g \in G$

Es ist:

$$\begin{aligned} &\pi(g) && = e_{G/H} \\ &\Leftrightarrow gH && = H \\ &\Leftrightarrow g && \in H && \text{'}H \text{ ist Untergruppe} \end{aligned}$$

Folglich ist $ker\pi = H$.

5.5 Satz:

Sei G eine Gruppe und H eine normale Untergruppe von G. Sei $\pi : G \to (G/H); g \mapsto gH$ der kanonische Morphismus von G nach G/H und $f : G \to G'$ ein Gruppenhomomorphismus mit $H \subset kerf$.
Dann existiert ein eindeutiger Gruppenhomomorphismus $\varphi : (G/H) \to G'$ so dass gilt $\varphi \circ \pi = f$. Des weiteren ist $ker\varphi = \pi(kerf)$, φ ist also genau dann injektiv wenn $kerf = H$ gilt. Zudem ist φ genau dann surjektiv wenn f surjektiv ist.
Beweis:
Sei G eine Gruppe und H eine normale Untergruppe von G. Sei $\pi : G \to (G/H); g \mapsto gH$ der kanonische Morphismus von G nach G/H und $f : G \to G'$ ein Gruppenhomomorphismus mit $H \subset kerf$.
Seien $g, g' \in G$.

Es gilt folgende Äquivalenz:

$$\begin{aligned}
&\pi(g) &&= \pi(g') \\
\Leftrightarrow\ &gH &&= g'H \\
\Leftrightarrow\ &g &&\in g'H \\
\Leftrightarrow\ &\exists h \in H : g &&= g'h && \text{'}H \text{ ist Untergruppe}
\end{aligned}$$

Sei $h \in H$ mit $g = g'h$
Es folgt:

$$\begin{aligned}
&f(g) \\
&= f(g'h) \\
&= f(g')f(h) && \text{'}f \text{ ist Gruppenhomomorphismus} \\
&= f(g') && \text{'}h \in H \subset kerf
\end{aligned}$$

Sei nun $\varphi : (G/H) \to G'; gH \mapsto f(g)$. Diese Abbildung ist wegen der oben gezeigten Implikation $gH = g'H \Rightarrow f(g) = f(g')$ vom Repräsentanten der Nebenklasse unabhängig, also wohldefiniert.
Nach Konstruktion von φ gilt: $\varphi \circ \pi = f$. Außerdem ist φ ein Gruppenhomomorphismus:

$$\begin{aligned}
&\varphi(gH \cdot g'H) \\
&= \varphi(gg'H) \\
&= f(gg') \\
&= f(g)f(g') \\
&= \varphi(gH)\varphi(g'H)
\end{aligned}$$

Für Elemente gH im Kern von φ gilt:

$$\begin{aligned}
&gH && \in ker\varphi \\
\Leftrightarrow\ &f(g) && = e_{G'} \\
\Leftrightarrow\ &g && \in kerf
\end{aligned}$$

Also: $ker\varphi = \pi(kerf)$

Bezüglich der Injektivität von φ gilt:
φ injektiv $\Rightarrow ker f = H$:

Sei $g \in ker f$
Es ist:

$$\begin{aligned} \varphi(gH) = f(g) &= e_{G'} \\ \Leftrightarrow gH &\in ker\varphi \\ \Leftrightarrow gH &= H && \text{'}\varphi \text{ injektiv} \Rightarrow ker\varphi = \{H\} \\ \Leftrightarrow g &\in H \end{aligned}$$

Es folgt $ker f \subset H$ und schließlich mit $H \subset ker f$: $ker f = H$

$ker f = H \Rightarrow \varphi$ injektiv:

Sei $g \in G$ so dass $gH \in ker\varphi$
Es ist:

$$\begin{aligned} gH &\in ker\varphi \\ \Leftrightarrow \varphi(gH) &= e_{G'} \\ \Rightarrow f(g) &= e_{G'} \\ \Leftrightarrow g &\in ker f \end{aligned}$$

Also $g \in H$, denn $ker f = H$ und somit $gH = H = e_{G/H}$, also die Injektivität von φ.

Für die Surjektivität von φ gilt offensichtlich, dass φ genau dann surjektiv ist, wenn f surjektiv ist, denn es gilt $\varphi \circ \pi = f$ wobei π surjektiv ist.
□

5.6 Satz:

Sei G eine Gruppe, H eine normale Untergruppe von G und $\pi : G \to (G/H); g \mapsto gH$ der kanonische Morphismus mit Kern H. Dann gilt:

(i) Für jede Untergruppe K in G/H ist $\pi^{-1}(K)$ eine Untergruppe in G die H enthält und jede solche Untergruppe in G kann als solches Urbild einer Untergruppe in G/H erhalten werden.

(ii) Ist K eine normale Untergruppe von G/H dann ist die Komposition kanonischer Projektionen $f : G \to (G/H) \to ((G/H)/K)$ ein surjektiver

Gruppenmorphismus mit Kern $\pi^{-1}(K)$. Dies induziert einen Isomorphismus

$$(G/\pi^{-1}(K) \simeq ((G/H)/K)$$

Beweis:
Sei G eine Gruppe, H eine normale Untergruppe von G und $\pi : G \to (G/H); g \mapsto gH$ der kanonische Morphismus mit Kern H.

(i) Sei K eine Untergruppe in G/H mit $H \subset K$. Wie jedes Urbild einer Untergruppe unter einem Gruppenhomomorphismus ist $\pi^{-1}(K)$ eine Untergruppe. Zudem gilt mit $e_{G/H} \in K$ und $\pi^{-1}(e_{G/H})$: $H \subset \pi^{-1}(K)$. Alle Untergruppen von von G die H enthalten sind Urbilder von Untergruppen in G/H:

Sei U eine Untergruppe von G mit $H \subset U$. Dann ist $\pi(U)$ eine Untergruppe in G/H und es gilt:

$$U \subset \pi^{-1}(\pi(U))$$

Sei $v \in \pi^{-1}(\pi(U)$. Es folgt $\pi(v) \in \pi(U)$. Folglich gilt $\exists u \in U : \pi(v) = \pi(u)$. Sei nun $u \in U$ mit $\pi(v) = \pi(u)$.
Es gilt dann:

$$\begin{aligned} &\pi(v) &&= \pi(u) \\ \Leftrightarrow\ &\pi(vu^{-1}) &&= e_{G/H} \\ \Leftrightarrow\ &vu^{-1} &&\in ker\pi \\ \Leftrightarrow\ &vu^{-1} &&\in H && 'ker\pi = H \end{aligned}$$

Da $H \subset U$ folgt $v = (vu^{-1})u \in U$. Es gilt also:

$$\pi^{-1}(\pi(U)) \subset U$$

und schließlich:

$$U = \pi^{-1}(\pi(U))$$

(ii) Sei K eine normale Untergruppe von G/H Sei $f : G \to (G/H) \to ((G/H)K)$ die Verkettung der entsprechenden kanonischen Projektio-

nen $\pi : G \to (G/H)$ und $\pi' : (G/H) \to ((G/H)/K)$.
f ist als Komposition surjektiver Gruppenmorphismen ein surjektiver Gruppenmorphismus.
Sei $g \in G$.
Es gilt:

$$
\begin{array}{lll}
g & \in ker f & \\
\Leftrightarrow f(g) & = e_{((G/H)/K)} & \\
\Leftrightarrow \pi'(\pi(g)) & = e_{((G/H)/K)} & \\
\Leftrightarrow \pi(g) & \in ker \pi' & \\
\Leftrightarrow \pi(g) & \in K & \text{'} ker \pi' = K
\end{array}
$$

also:

$$ker f = \pi^{-1} K$$

Wendet man nun Satz 5.5 auf folgende Situation an:

$$
\begin{tikzcd}
G \arrow[rr, "\pi"] \arrow[dr, "f"'] & & (G/H)/K \arrow[dl, "\varphi"] \\
& G/\pi^{-1}(K) &
\end{tikzcd}
$$

so ergibt sich die Existenz von φ, die surjektivität von φ aus der gezeigten Surjektivität von f und die Injektivität von φ aus $ker f = \pi^{-1}(K)$.
Damit ist φ bijektiv, $G/\pi^{-1}(K)$ und $(G/H)/K$ sind also isomorph:

$$(G/\pi^{-1}(K) \simeq ((G/H)/K)$$

□

6 Quellen:

- Antoine Chambert-Loir A Field Guide to Algebra 2005
- Michael Artin Algebra 1998
- http://www.mathematik.tu-dortmund.de/ algebra/Algebra_2012/ Skript/algebra_kap2_4.pdf