Proseminar Körpertheorie

Einstieg in die Theorie der Körper

Alexa Rieger

20.06.2013

Prof. Dr. K. Wingberg, K. Hübner

8. Vortrag – Elemente der Gruppentheorie

1. Satz von Lagrange

Satz (Satz von Lagrange)***:***
Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann gilt: #H | #G

Beweis: Sei $g \sim g' :\Leftrightarrow \exists h \in H:\ g' = gh \ \ (g, g' \in G)$ eine Relation in G. Dies ist sogar eine Äquivalenzrelation, denn es gilt:

(i) $\forall g \in G$ gilt $g = g e_G$, $e_G \in H \ \Rightarrow g \sim g$

(ii) Sei $g \sim g'$ und $h \in H$ derart, dass $g' = gh \overset{h^{-1} \in H}{\Rightarrow} g' h^{-1} = g \Rightarrow g' \sim g$

(iii) Sei $g \sim g'$, $g' \sim g''$ und $h, h' \in H$ derart, dass $g' = gh$, $g'' = g'h'$
$\Rightarrow g'' = (gh)h' = g(\underbrace{hh'}_{\in H}) \Rightarrow g \sim g''$

Die Äquivalenzklasse eines Elements $g \in G$ ist also genau die Menge
$gH = \{gh \mid h \in H\}$.
Betrachte nun die offensichtlich bijektive Abbildung $H \to gH,\ h \to gh.$ Aus H und gH endlich (G endl.) folgt #H = #gH $\forall g \in G$.
Eine Gruppe ist die disjunkte Vereinigung all ihrer Äquivalenzklassen. Existieren nun $N \in \mathbb{N}$ viele Äquivalenzklassen in G, so folgt $\#G = N \cdot \#H$.
$\Rightarrow \#H \mid \#G$

Def.: Der Index einer Untergruppe H einer endlichen Gruppe G ist der Quotient $\frac{\#G}{\#H}$ und wird mit (G:H) bezeichnet. Wie im Beweis deutlich geworden, ist er stets eine natürliche Zahl.

Die oben definierten Äquivalenzklassen gH werden Linksnebenklassen genannt. Für die Menge $\#G/H = \{gH \mid g \in G\}$ der Linksnebenklassen gilt insbesondere $\#G/H = (G:H)$.

2. Operationen auf Mengen, Klassengleichung

Def.: Sei X eine Menge, G eine Gruppe. Die Abb. $\varphi: G \times X \to X,\ (g,x) \to gx$ operiert auf X, wenn gilt:
(i) $1x = x\ \forall x \in X$, wobei 1 das neutrale Element e_G ist
(ii) $(gg')x = g(g'x)\ \forall g, g' \in G$ und $x \in X$

Außerdem: $Gx := \{gx \mid g \in G\} \subseteq X$ Bahn (bzw. Orbit) von $x \in X$
$Stab_G(x) := \{g \in G \mid gx = x\} \subseteq G$ Stabilisator von $x \in X$
$F := \{x \in X \mid gx = x\} \subseteq X$ Fixpunkte

Anm.: $Stab_G(x) \subseteq G$ ist sogar eine Untergruppe von G, denn:
(i) $\forall x \in X$ gilt $1x = x \Rightarrow 1 \in Stab_G(x)$
(ii) $\forall g \in G$ gilt $gx = x \Leftrightarrow x = g^{-1}x \Rightarrow g^{-1} \in Stab_G(x)$
(iii) $g, g' \in Stab_G(x) : g(g'x) = gx = x = \underbrace{(gg')}_{\in Stab_G(x)} x$

Außerdem gilt: $gx = g'x \Leftrightarrow g^{-1}g'x = x \Leftrightarrow g^{-1}g' \in Stab_G(x) \Leftrightarrow g' \in gStab_G(x)$
$\Leftrightarrow g'Stab_G(x) = gStab_G(x)$
Diese Äquivalenzumformungen liefern sowohl die Wohldefiniertheit als auch die Injektivität der Abbildung $G/Stab_G(x) \to Gx$, $gStab_g(x) \to gx$. Aus deren offensichtlicher Surjektivität erschließt sich, dass die Abbildung sogar bijektiv ist.
$\overset{\text{endl. Mengen}}{\Rightarrow} \#Gx = \#G/Stab_G(x) \overset{G/Stab_G(x)\text{ Nebenklasse}}{=} (G : Stab_G(x)) = \dfrac{\#G}{\#Stab_G(x)}$.

Ähnlich wie im Beweis zum Satz von Lagrange kann gezeigt werden, dass X die disjunkte Vereinigung all ihrer Bahnen ist, indem man Äquivalenzrelationen auf X mittels der Bahn (beispielsweise der Form $x \sim y :\Leftrightarrow \exists g \in G : y = gx$ für $x, y \in X$) definiert.
$\Rightarrow X = \dot{\bigcup}_i Gx_i$
$\Rightarrow \#X = \sum_i \#Gx_i = \sum_i \dfrac{\#G}{\#Stab_G(x_i)}$ ***(Klassengleichung)***

3. Zentrum einer $p-$Gruppe

Def.: Sei G eine endliche Gruppe. Die Ordnung eines Elements $g \in G$ ist die kleinste Zahl $n \in \mathbb{N}$, $n \geq 1$, sodass $g^n = 1$. Gibt es ein solches n nicht, gilt $ord(g) = \infty$.

Def.: Sei $p \in \mathbb{N}$ eine feste Primzahl, G eine Gruppe und $n \in \mathbb{N}$ bel. Eine $p-$Gruppe ist eine Gruppe, in der $\forall g \in G$ $ord(g) = p^n$ gilt. In anderen Worten: $\forall g \in G : g^{p^n} = 1$. Insbesondere ist $\#G = p^n$

Beh.: Sei G eine Gruppe. Für $\#G=p^2$ gilt: G ist eine kommutative Gruppe.

Beweis: Hierfür müssen erst ein paar Definitionen betrachtet werden:

$Z(G):=\{g\in G\mid gh=hg\ \forall h\in G\}$ Zentrum von G

$C_G(g):=\{h\in G\mid gh=hg\}$ Zentralisator von $g\in G$

Anm.: **$C_G(g)\subseteq G$ und $Z(G)\subseteq G$ sind Untergruppen**

Beweis: (i) $\forall h\in G$ gilt: $1\cdot h=h=h\cdot 1\Rightarrow 1\in Z(G)$

(ii) $g\in Z(G)\Rightarrow \forall h\in G: gh=hg\Leftrightarrow h=g^{-1}hg\Leftrightarrow hg^{-1}=g^{-1}h$
$\Rightarrow g^{-1}\in Z(G)$

(iii) $x,y\in Z(G)\Rightarrow \forall g\in G: (xy)g=x(yg)=x(gy)=(xg)y=g(xy)$
$\Rightarrow xy\in Z(G)$
$\Rightarrow (x(yz))g=xg(yz)=(xy)gz=((xy)z)g$

Analog für $C_G(g)$.

Es gilt zu zeigen: $\#Z(G)=p^2$, denn wenn das Zentrum einer Gruppe komplette Gruppe ist, so kommutiert diese.

$\#G=p^2$, $Z(G)\subseteq G$ Untergruppe $\overset{\text{Satz v. Lagrange}}{\Rightarrow}$ $\#Z(G)\in\{1,p,p^2\}$

Zunächst zu zeigen: $\#Z(G)\neq 1$ (Also das Zentrum ist nicht trivial)

Betr. die Operation von G auf sich selbst mit $(g,g')\to gg'g^{-1}$ **(Konjugation)**

Dies ist eine Operation, denn: (i) $1\cdot g'=1\cdot g'\cdot 1=g'$ und

(ii) $(g_1g_2)x=(g_1g_2)x(g_1g_2)^{-1}=(g_1g_2)x(g_2^{-1}g_1^{-1})$
$=g_1(g_2x)g_1^{-1}=g_1(g_2x)$

Die Bahn $Gg'=\{gg'g^{-1}\mid g\in G\}$ von $g'\in G$ heißt Konjugationsklasse von g'.

$\mathrm{Stab}_G(g')=\{g\in G\mid gg'g^{-1}=g'\}=\{g\in G\mid gg'=g'g\}=C_G(g')$.

$F=\{g'\in G\mid gg'g^{-1}=g'\ \forall g\in G\}=\{g'\in G\mid gg'=g'g\ \forall g\in G\}=Z(G)$.

Anm.: Fixpunkte einer Operation besitzen Bahnen der Länge 1 (d.h. $\#Gx=1$ für x Fixpunkt)!

$$G \text{ endlich } \overset{\text{Klassengleichung für Konjugation}}{\Rightarrow} \#G=\sum_i \#Gx_i=\#\{x\mid x \text{ Fixpunkt}\}+\underbrace{\sum_j \#Gx_j}_{\text{Bahnen d. Länge}\geq 2} \quad (*)$$

$x_j\notin Z(G)\ \forall j\Rightarrow C_G(x_j)\subset G$, d.h. $p\mid \dfrac{\#G}{\#C_G(x_j)}$.

$$\overset{(*)\bmod p}{\Rightarrow} 0\equiv\#G=\#Z(G)+\sum_j \#Gx_j=\#Z(G)+\sum_j \frac{\#G}{\#C_G(x_j)}\equiv\#Z(G)+0$$

$\Rightarrow p\mid \#Z(G)\Rightarrow \#Z(G)\neq 1\Rightarrow \#Z(G)\in\{p,p^2\}$

Anm.: In diesem Teil des Beweises wurde zu keiner Zeit verwendet, dass $\#G=p^2$ gilt, also wurde sogar für allgemeine p−Gruppen gezeigt, dass ihr Zentrum nicht trivial ist!

Angenommen $\#Z(G)=p. \Rightarrow \exists x\in G: x\notin Z(G) \overset{\text{x kommutiert mit sich selbst}}{\underset{x\notin Z(G)}{\Rightarrow}} Z(G)\subset \underbrace{C_G(x)}_{x\in}$

$\Rightarrow p=\#Z(G) < \#C_G(x) \leqslant p^2 \overset{C_G(x)\subseteq G \text{ Untergrp.}}{\Rightarrow} \#C_G(x)=p^2$

$\Rightarrow C_G(x)=G$ **Widerspruch**, denn $x\notin Z(G)\subset C_G(x)$

$\Rightarrow \#Z(G)=p^2 \Rightarrow$ G kommutiert!

4. Normalteiler und Faktorgruppen

Def.: Eine Untergruppe $H\subseteq G$ einer Gruppe G heißt Normalteiler (ist normal), wenn $\forall g\in G,\ h\in H$ gilt: $g^{-1}hg\in H$

Satz: Für $H\subseteq G$ Untergruppe sind folgende Aussagen äquivalent:
(i) H ist normal
(ii) $g^{-1}Hg=H\ \forall g\in G$
(iii) $Hg=gH\ \forall g\in G$

Beweis: (i) $\Leftrightarrow$ (iii): $\Leftarrow$: $g\in G,\ h\in H$ bel. $\Rightarrow gh\in gH \overset{gH=Hg}{\Rightarrow} gh\in Hg$
$\Rightarrow \exists h'\in H$ mit $gh=h'g \Rightarrow ghg^{-1}=h' \Rightarrow ghg^{-1}\in H$
$\Rightarrow$: $\subseteq$: $ghg^{-1}\in H$ für $g\in G,\ h\in H$ bel.
$x\in gH \Rightarrow \exists h\in H$ mit $x=gh \Rightarrow xg^{-1}=ghg^{-1}\in H$
$\Rightarrow xg^{-1}\in H$. Wegen $x=xg^{-1}g$ folgt $x\in Hg \Rightarrow gH\subseteq Hg$
$\supseteq$: analog.
(iii) $\Leftrightarrow$ (ii) trivial durch Multiplikation mit dem Inversen.

Satz: Der Kern jedes Gruppenhomomorphismus ist ein Normalteiler
Beweis: Sei $\varphi: G\to G'$ Gruppenhomomorphismus. $\forall g\in G,\ h\in \operatorname{Ker}\varphi$:
$\varphi(g^{-1}hg)=\varphi(g)^{-1}\varphi(h)\varphi(g)=1 \Rightarrow g^{-1}hg\in \operatorname{Ker}\varphi$

Def.: G Gruppe, $H\subseteq G$ Normalteiler. Durch $*: G/H\times G/H\to G/H,\ gH*g'H:=(gg')H$ $\forall g,g'\in G$ ist eine Verknüpfung auf der Menge der Nebenklassen gH definiert. $(G/H,*)$ wird Faktorgruppe genannt.
$*$ ist wohldefiniert, denn: Seien $g_1H=g'_1H,\ g_2H=g'_2H \Rightarrow g_1\in g_1H=g'_1H$
$g_2\in g_2H=g'_2H$
$\Rightarrow \exists h_1, h_2\in H: g_1=g'_1h_1,\ g_2=g'_2h_2 \Rightarrow (g_1g_2)H=(g'_1h_1g'_2h_2)H=(g'_1g'_2\underbrace{h_1h_2}_{\in H})H$
$=g'_1g'_2(h_1h_2H)=(g'_1g'_2)H$
$\Rightarrow *$ ist repräsentantenunabhängig und damit wohldefiniert.

Satz: $(G/H,*)$ ist eine Gruppe
Beweis: (i) $e_{G/H}=H\in G/H$ klar, denn $\forall gH\in G/H: gH\cdot H=gH$
(ii) $\forall gH\in G/H: (gH)^{-1}=g^{-1}H\in gH$ klar, denn: $gH*g^{-1}H=(gg^{-1})H=H$
(iii) $g_1H*(g_2H*g_3H)=g_1H*(g_2g_3)H=(g_1g_2g_3)H=(g_1g_2)H*g_3H$
$=(g_1H*g_2H)*g_3H$ gilt $\forall g_1H,\ g_2H,\ g_3H\in G/H$

Beispiele: a) Sei G Gruppe. Die trivialen Untergruppen $\{1\}$ und G sind Normalteiler. Eine Gruppe, die nur diese Normalteiler enthält, heißt **einfach.**
b) Untergruppen einer kommutativen Gruppe sind automatisch normal.
c) Sei $Z(G)$ das Zentrum einer Gruppe G. $Z(G)$ ist ein Normalteiler, denn für $h\in Z(G)$, $g\in G$ gilt: $g^{-1}hg=g^{-1}gh=h\in Z(G)$.

Bem.: Für $H\subseteq G$ Normalteiler ist die Abb. $\pi: G\to G/H$ ein surjektiver Gruppenhom mit $\operatorname{Ker}\pi=H$.
π ist ein Gruppenhom., da $\forall g,g'\in G$ gilt: $\pi(gg')=(gg')H=gH*g'H=\pi(g)*\pi(g')$.

Satz (Homomorphiesatz)***:***
Seien G, G' Gruppen, $H\subseteq G$ Normalteiler, π obige Abb. Sei $f: G\to G'$ Gruppenhom. mit $H\subseteq\operatorname{Ker}f$.
Dann existiert ein eindeutiger Gruppenhom. $\varphi: G/H\to G'$, sodass $\varphi\circ\pi=f'$ mit $\operatorname{Ker}\varphi=\pi(\operatorname{Ker}f)$, φ surj. $\Leftrightarrow$ f surj. und φ inj. $\Leftrightarrow \operatorname{Ker}f=H$

Beweis: (i) $\forall gH\in G/H: \varphi(gH)=\varphi(\pi(g))=f(g)$
$\Rightarrow g'H=gH \Rightarrow g'^{-1}g\in H\subseteq\operatorname{Ker}f \Rightarrow f(g'^{-1}g)=1 \overset{\text{f Gruppenhom.}}{\Rightarrow} f(g)=f(g')$
$\Rightarrow \varphi(gH)=\varphi(g'H) \overset{\text{Repräsentantenunabh.}}{\Rightarrow}$ φ wohldefiniert und eindeutig.
(ii) $\forall gH\in G/H$ gilt $gH\in\operatorname{Ker}\varphi \Leftrightarrow f(g)=1$
$\Rightarrow \operatorname{Ker}\varphi=\{gH\mid g\in\operatorname{Ker}f\} \overset{\text{offensichtlich nach Def. v. }\pi}{=} \pi(\operatorname{Ker}f)$
(iii) Z.z.: φ surj. $\Leftrightarrow$ f surj.
klar aus der Surjektivität von π und $f=\varphi\circ\pi$ (Surjektiv als Komposition surjektiver Funktionen)
Z.z.: φ inj. $\Leftrightarrow \operatorname{Ker}f=H$
$\Rightarrow$: φ inj. $\Rightarrow \varphi(gH)=1$ $\forall gH=H$ (neutr. Element v. G/H) $\Rightarrow g\in H$
$\Rightarrow \operatorname{Ker}f\subseteq H$, $H\subseteq\operatorname{Ker}f$ (Vorauss.) $\Rightarrow$ $\operatorname{Ker}f=H$
$\Leftarrow$: $\operatorname{Ker}f=H$, $g\in G$: $gH\in\operatorname{Ker}\varphi \Rightarrow \varphi(gH)=f(g)=1 \Rightarrow g\in\operatorname{Ker}f$
$\Rightarrow g\in H$ und $gH=e_{G/H}$ $\Rightarrow$ φ ist injektiv

Satz (2. Isomorphiesatz)***:***
Sei G Grp., $H\subseteq G$ Normalteiler, $\pi: G\to G/H$, $g\to gH$ mit $\operatorname{Ker}\pi=H$ (siehe oben).
Dann gilt: Ist $K\subseteq G/H$ Normalteiler, so ist $G\overset{\pi}{\to}G/H\to(G/H)/K$ ein Gruppenhom. mit Kern $\pi^{-1}(K)$. Dies induziert $G/\pi^{-1}(K)\simeq(G/H)/K$

Beweis: $\pi^{-1}(K)\subseteq G$ Normalteiler, wenn $\pi^{-1}(K)$ Kern eines Gruppenhom. ist.
Sei $f: G\to(G/H)/K$ eine surjektive Abb. als Komposition surj. Gruppenhom.
Es gilt $g\in\operatorname{Ker}f \Leftrightarrow \pi(g)\in K \Rightarrow \operatorname{Ker}f=\pi^{-1}(K)$.
$\overset{\text{Homomorphiesatz}}{\Rightarrow}$ $\exists\varphi: G/\pi^{-1}(K)\to(G/H)/K$, φ surj. (f surj.) und φ inj. ($\operatorname{Ker}f=\pi^{-1}(K)$)
$\Rightarrow$ φ bijektiv
$\Rightarrow$ $G/\pi^{-1}(K)\simeq(G/H)/K$

Literatur: *Chambert−Loir, Antoine: A field guide to Algebra, Springer, 2000*

Anmerkung : *In dieser Ausarbeitung wurde mangels passenderer Operatoren des Formeleditors $\subset$ als Bezeichung für eine echte Teilmenge und $\subseteq$ als Bezeichung für eine nicht unbedingt echte Teilmenge verwendet.*
Aus demselben Grund wurde der normale Rechtspfeil $\rightarrow$ anstatt eines Zuordnungspfeils bei definierten Abbildungen verwendet.