Westfälische
Wilhelms-Universität
Münster

Fachbereich 10
Mathematik und
Informatik

Einführung in die Algebra

Aufarbeitung der Vorlesungsnotizen

Tobias Wedemeier

30. Oktober 2014
gelesen von
Prof. Dr. Kramer

Hierbei handelt es sich um eine Aufarbeitung der Vorlesungsnotizen von **Prof. Dr. Kramer**, WWU Münster, aus der Vorlesung **Einführung in die Algebra** im Wintersemester 2014/15. Dies ist kein Skript der Vorlesung und keine eigene Arbeit des Autors.

Für Fehler in der Aufarbeitung wird keine Haftung übernommen. Hinweise auf Fehler sind gerne gesehen, hierfür kann man mich in der Uni ansprechen oder alternativ eine e-Mail an:
tobias.wedemeier@gmx.de
Auch ist eine Mitarbeit über Github möglich.

Wenn Teile aus der Vorlesung selber fehlen, können diese gerne an meine e-Mail versandt werden. Ich werde diese dann einarbeiten.

Inhaltsverzeichnis

1 Elementare Gruppentheorie

Erinnerung: eine **Verknüpfung** auf einer nicht leeren Menge X ist eine Abbildung

$$X \times X \to X, (x, y) \mapsto m(x, y).$$

Häufig schreibt man $m(x, y) = xy$ oder $m(x, y) = x + y$, je nach Kontext. Die Schreibweise $m(x, y) = x + y$ wird eigentlich nur für kommutative Verknüpfungen benutzt, d.h. wenn $\forall x, y \in X$ gilt $m(x, y) = m(y, x)$.

1.1 Definition Gruppe

Eine **Gruppe** $(G, \cdot)$ besteht aus einer Verknüpfung $\cdot$ auf einer nicht leeren Menge G, mit folgenden Eigenschaften:

(G1) Die Verknüpfung ist assoziativ, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt $\forall x, y, z \in G$.
(Folglich darf man Klammern weglassen.)

(G2) Es gibt ein neutrales Element $e \in G$, d.h. es gilt $e \cdot x = x \cdot e = x \forall x \in G$

(G3) Zu jedem $x \in G$ gibt es ein Inverses $y \in G$, d.h. $xy = e = yx$.
man schreibt dann auch $y = x^{-1}$ für das Inverse zu x.

Fordert man von der Verknüpfung nur (G1) und (G2), so spricht man von einer Halbgruppe mit Eins oder einem **Monoid**. Fordert man nur (G1), so spricht man von einer Halbgruppe.

1.2 Beispiel 1

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ sind kommutative Gruppen.
- $(\mathbb{Z}, \cdot), (\mathbb{N}, \cdot), (\mathbb{N}, +)$ sind Monoide.

1.3 Beobachtungen

a) Das Neutraleelement (einer Verknüpfung) ist eindeutig bestimmt: sind e, e' beides Neutralelemente, so folgt: $e = ee' = e'$

b) Das Inverse zu x ist eindeutig bestimmt:
$xy = e = xy' = y'x \Rightarrow y' = y'e = y'xy = ey = y$

1.4 Lemma 1 (Sparsame Definition von Gruppen)

Sei $G \times G \to G$ eine assoziative Verknüpfung. Dann ist G schon eine Gruppe, wenn gilt:

(i) es gibt $e \in G$ so, dass $ex = x \; \forall x \in G$ gilt.

(ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$

Beweis
Sei $yx = e$, es folgt $yxy = y$. Wähle z mit $zy = e$, es folgt $\underbrace{zy}_{=e} xy = zy = e \Rightarrow xy = e$

Weiter gilt $xe = xyx = ex = x$. □

1.5 Beispiel 2

Sei X eine nicht leere Menge, sei $X^X = \{f : X \to X\}$ die Menge aller Abbildungen von X nach X. Als Verknüpfung auf X nehmen wir die Komposition von Abbildungen. Dann gilt wegen $f = id_X \circ f = f \circ id_X$, dass id_X ein Neutralelement ist.
Damit haben wir ein Monoid $(X_X, \circ)$.
Sei $Sym(X) = \{f : X \to X | f \text{ bijektiv}\}$. Zu jedem $f \in Sym(X)$ gibt es also eine Umkehrabbildung $g : X \to X$ mit $f \circ g = g \circ f = id_X$. Folglich ist $(Sym(X), \circ)$ eine Gruppe, die **Symmetrische Gruppe**.
Wenn X endlich ist mit n Elementen, so gibt es genau $n! = n(n-1)(n-2) \cdot \dots \cdot 2 \cdot 1$ Permutationen, also hat $Sym(X)$ dann genau $n!$ Elemente.

Für $X = \{1, 2, 3, \dots, n\}$ schreibt man auch $Sym(X) = Sym(n) \Big(= S_n \Big)$.

1.6 Definition zentralisieren

Sei $G \times G \to G$ eine Verknüpfung. Wir sagen, $x, y \in G$ vertauschen oder kommutieren oder x **zentralisiert** y, wenn gilt $xy = yx$.
Eine Gruppe, in der alle Elemente vertauschen heißt kommutativ oder **abelsch**.

1.7 Beispiel 3

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \cdots)$ sind abelsche Gruppen.

(b) K Körper, $G = Gl_2(K) = \{X \in K^{2\times 2} \mid det(X) \neq 0\}$ Gruppe der invertierbaren 2×2 Matrizen.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$\Rightarrow$ nicht abelsch, genauso $Gl_n(K)$ für $n \geq 2$.

(c) $Sym(2)$ ist abelsch, aber $Sym(3)$ nicht. Allgemein ist $Sym(X)$ nicht abelsch, falls $\#X \geq 3$ gilt.

1.8 Definition Untergruppe

Sei G eine Gruppe, sei $H \subseteq G$. Wir nennen H **Untergruppe** von G, wenn gilt:

(UG1) $e \in H$

(UG2) $x, y \in H \Rightarrow xy \in H$

(UG3) $x \in H \Rightarrow x^{-1} \in H$

Offensichtlich ist eine Untergruppe dann wieder eine Gruppe, mit der von G vererbten Verknüpfung.

Bsp
(a) $(\mathbb{Q}, +)$. $\mathbb{Z}$ ist Untergruppe, denn $0 \in \mathbb{Z}, m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}$ und $n \in \mathbb{Z} \Rightarrow -n \in \mathbb{Z}$

(b) $(\mathbb{Q}^*, \cdot)$. $\mathbb{Z}^*$ ist keine Untergruppe, kein Inverses.

1.9 Lemma 2

Sei G eine Gruppe und sei U eine nicht leere Menge von Untergruppen von G. Dann ist auch
$\bigcap U = \{g \in G | \forall H \in U \text{ gilt } g \in H\}$
eine Untergruppe von G.
Beweis
Für alle $H \in U$ gilt $e \in H$, also $e \in \bigcap U$. Angenommen $x, y \in \bigcap U$. Dann gilt für alle $H \in U$, dass $xy \in H$ sowie $x^{-1} \in H$. Es folgt $xy \in \bigcap U$ sowie $x^{-1} \in \bigcap U$. □

1.10 Definition $\langle X \rangle$

Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Wir setzen:

$$\langle X \rangle = \bigcap \{H \subseteq G | H \text{ Untergruppe und } X \subseteq H\}$$

Ist nicht leer, da mindestens G enthalten ist.

- Es gilt z.B. $\langle \emptyset \rangle = \{e\}$, denn $\{e\}$ ist Untergruppe.
- Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $X \subseteq \langle X \rangle \subseteq H$, insb. also $\langle H \rangle = H$.

Satz

Sei $X \subseteq G$ und sei $W = \{x_1 \cdot x_2, \cdot \cdots \cdot x_s | s \geq 1, x_i \in X \text{ oder } x_i^{-1} \in X \ \forall i = 1, \ldots, s\}$.
Dann gilt: $\langle X \rangle = \{e\} \cup W$.
Beweis
Wegen $X \subseteq \langle X \rangle$ und $e \in \langle X \rangle$ folgt $\{e\} \cup W \subseteq \langle X \rangle$. Ist $f, g \in W$, so folgt $fg \in W$ sowie $f^{-1} \in W$, also ist $H = \{e\} \cup W$ eine Untergruppe von G, mit $X \subseteq H$. Es folgt $\langle X \rangle \subseteq H = \{e\} \cup W$. □

1.11 Definition zyklische Gruppe

Sei G eine Gruppe und sei $g \in G$. Für $n \geq 1$ setze $g^n = \underbrace{g \cdot \cdots \cdot g}_{n-mal}$ sowie $g^{-n} = \underbrace{g^{-1} \cdot \cdots \cdot g^{-1}}_{n-mal}$ und $g^0 = e$.
Dann gilt $\forall k, l \in \mathbb{Z}$, dass $g^k \cdot g^l = g^{k+l}$.
Sei $\langle g \rangle = \langle \{g\} \rangle \overset{1.10}{=} \{g^n | n \in \mathbb{Z}\}$. Man nennt $\langle g \rangle$ die von g erzeugte **zyklische Gruppe**. Wenn für ein $n \geq 1$ gilt $g^n = e$, so heißt n ein **Exponent** von g. DIe **Ordnung** von g ist der kleinste Exponent von g,

$$o(g) = min\left(\{n \geq 1 | g^n = 1\} \cup \{\infty\}\right)$$

$o(g) = \infty$ bedeutet: $g^n \neq e \ \forall n \geq 1$
$o(g) = 1$ bedeutet: $g^n = g = e$

1.12 Zyklische Gruppen

Eine Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$. Wegen $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ gilt: zyklische Gruppen sind abelsch.

Satz

Sei $G = \langle g \rangle$ zyklisch mit $o(g) = n < \infty$. Dann gilt $\#G = n$ und $G = \{g, g^1, g^2, g^3, \ldots, g^n\}$. **Beweis**
Jedes $m \in \mathbb{Z}$ lässt sich schreiben als $m = kn + l$ mit $0 \leq l < n$ (Teilen mit Rest), also $g^m = \underbrace{g^{kn}}_{=e} . g^l = g^l$.

Es folgt $G \subseteq \{g, g^2, \dots, g^n\}, g^n = g^0$. Ist $g^k = g^l$ für $0 \leq k \leq l < n$, so gilt $e = g^0 = g^{l-k}$, also $l - k = 0$ (wegen$l < n$), also $\#\{g, g^2, \dots, g^n = g^0\} = n$. □

Folgerung
Ist G endlich mit $\#G = n$ und ist $h \in G$ mit $O(h) = n$, so folgt $\langle h \rangle = G$. Insbesondere ist dann G eine zyklische Gruppe. □

1.13 Nebenklassen

Sei G eine Gruppe und sei H eine Untergruppe. Sei $a \in G$. Wir definieren:

$$aH = \{ah | h \in H\} \subseteq G$$

$$Ha = \{ha | h \in H\} \subseteq G$$

Man nennt aH die **Linksnebenklassen** von a bzgl. H (und Ha die **Rechtsnebenklassen**). In nicht abelschen Gruppen gilt im allgemeinen $aH \neq Ha$.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G und $a, b \in G$.
Dann sind äquivalent:

(i) $b \in aH$

(ii) $bH = aH$

(iii) $bH \cap aH \neq \emptyset$

Beweis

- $(i) \Rightarrow (ii):\ b \in aH \Rightarrow b = ah$ für ein $h \in H \Rightarrow bH = \{ahh' | h' \in H\}$ $\overset{H \text{ Untergruppe}}{=} \{ah'' | h'' \in H\} = aH$
- $(ii) \Rightarrow (iii)$: klar
- $(iii) \Rightarrow (i)$: Sei $g \in bH \cap aH,\ g = bh = ah' \Rightarrow b = ah'h^{-1} \in aH$, da H Untergruppe

□

Folgerung
Jedes $g \in G$ liegt in genau einer Linksnebenklasse bzgl. H, nämlich $g \in gH$. Entsprechendes gilt natürlich für Rechtsnebenklassen. Man setzt:
${}^{G}/_{H} = \{gH \mid g \in G\}$ Menge der Linksnebenklasse, Rechtsnebenklassen analog.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G, sei $a \in G$.
Dann ist die Abbildung $H \to gH, h \mapsto gH$ bijektiv.
Beweis
SSurjektivïst klar nach Definition von gH. Angenommen, $gh = gh' \Rightarrow h = g^{-1}gh' = h'$ □

1.14 Satz von Lagrange

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wenn zwei der drei Mengen $G, H, {}^{G}/_{H}$ endlich sind, dann ist die dritte ebenfalls endlich und es gilt:

$$\#G = \#H \cdot \#{}^{G}/_{H}$$

Insbesondere ist dann $\#H$ eine **Teiler** von $\#G$.

Beweis
Wenn G endlich ist, dann sind auch H und ${}^{G}/_{H}$ endlich.
Angenommen, ${}^{G}/_{H}$ und H sind endlich. Dann ist auch $G = \bigcup {}^{G}/_{H} = \bigcup\{gH \mid gH \in {}^{G}/_{H}\}$ endlich, da $\#gH = \#H$ nach 1.13.
Jetzt zählen wir genauer: sei $\#{}^{G}/_{H} = m; \#H = n$ etwa ${}^{G}/_{H} = \{g_1H, g_2H, \dots g_mH\}$.
$g_iH \overset{1.13}{=} n \qquad g_iH \cap g_jH = \emptyset$ für $i \neq j$ nach 1.13.
$G = g_1 \cap \#g_2H \cap \dots \cap g_mH \Rightarrow \#G = m \cdot n$ □

Bem

(1) Eine entsprechende Aussage gilt für Rechtsnebenklassen.

(2) Die Abbildung $G \to G, \quad g \mapsto g^{-1}$ bildet die Linksnebenklassen bijektiv auf die Rechtsnebenklassen ab:

$$(gH)^{-1} = \{(gh)^{-1} \mid h \in H\} \overset{\text{Achtung!}}{=} \{h^{-1}g^{-1} \mid h \in H\} = \{hg^{-1} \mid h \in H\} = Hg^{-1} \qquad \text{(ÜA)}$$

Korollar A (Lagrange)

Sei G eine endliche Gruppe und sei $g \in G$. Dann teilt $o(g)$ die Zahl $\#G$.
Beweis
Da G endlich ist, folgt $o(g) < \infty$. Nach dem Satz von Lagrange ist $\#\langle g\rangle = o(g)$ ein Teiler von $\#G$. □

Korollar B

Sei G eine endliche Gruppe, sei p eine **Primzahl** (d.h. die einzigen Teiler von p sind 1 und p) und $p > 1$. Wenn gilt $\#G = p$, dann ist G zyklisch. Für jedes $g \in G \backslash \{e\}$ gilt $\langle g\rangle = G$.
Beweis
Sei $g \in G\backslash\{e\}$. Dann ist $o(g) > 1$ und $o(g)$ teilt p. Es folgt $o(g) = p$, also $G = \langle g\rangle$ vgl. 1.12. □
Für endliche Gruppen sind Teilbarkeitseigenschaften wichtig, wie wir sehen werden.
Die Zahl $\#{}^{G}/_{H} := [G : H]$ nennt man auch den **Index von H in G**.

Wichtige Rechenregeln in Gruppen

(a) Man darf kürzen

$$ax = ay \Rightarrow x = y$$
$$xa = ya \Rightarrow x = y$$

(multipliziere beide Seiten von links/rechts mit a^{-1})

(b) Es gilt $(x^{-1})^{-1} = x$ ($x^{-1}x = e = xx^{-1} \Rightarrow (x^{-1})^{-1} = x$)

(c) Beim Invertieren darf die Reihenfolge umgedreht werden:

$$(ab)^{-1} = b^{-1}a^{-1} \left(ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab \Rightarrow (ab)^{-1} = b^{-1}a^{-1}\right)$$

(in abelschen Gruppen gilt natürlich damit $(ab)^{-1} = a^{-1}b^{-1}$)

1.15 Homomorphismen

Seien G, K Gruppen. Eine Abbildung $\varphi : G \to K$ heißt <u>**(Gruppen-)Homomorphismus**</u>, wenn $\forall x, y \in G$ gilt

$$\varphi \underbrace{(x \cdot y)}_{\text{Verküpfung in G}} = \underbrace{\varphi(x)\varphi(y)}_{\text{Verknüpfung in K}}$$

Bsp

(a) $id_G : G \to G$ ist Homomorphismus

(b) $H \subseteq G$ Untergruppe $i : H \hookrightarrow G, \quad h \mapsto h$ Inklusion, ist Homomorphismus.

(c) $(G, \cdot) = (\mathbb{Z}, +)$ $m \in \mathbb{Z}$ $\varphi : \mathbb{Z} \to \mathbb{Z}, x \mapsto mx$ ist Homomorphismus, denn $\phi(x + y) = m(x + y) = mx + my = \varphi(x) + \varphi(y)$

(d) G Gruppe, $a \in G$, $a \neq e$, $\lambda_a(x) = ax$.
$\lambda : G \to G$ ist kein Homomorphismus, denn $\lambda_a(e) = a, \lambda(ee) = a$, aber $\lambda_a(e)\lambda_a(e) = aa \neq a$

Lemma

Sei $\varphi : G \to K$ ein Homomorphismus von Gruppen. Dann gilt $\varphi(e_G) = e_K$ und $\varphi(x^{-1}) = \varphi(x)^{-1}$ $\forall x \in G$. (e_G Neutralelement in G und e_K Neutralelement in K)

<u>**Beweis**</u>

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \overset{\text{kürzen}}{\Rightarrow} e_K = \varphi(e_G)$$

$$e_K = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})$$

$\square$

<u>Achtung:</u> $\varphi(x)^{-1}$ ist das Inverse in K von $\varphi(x)$ <u>nicht</u> die Umkehrabbildung!

Das <u>**Bild**</u> eines Homomorphismus $\varphi : G \to K$ ist $\varphi(G) \subseteq K$,
der <u>**Kern**</u> ist $ker(\varphi) = \{x \in G \mid \varphi(x) = e_K\} \subseteq G$

1.16 Satz Gruppenhomomorphismen

Bild und Kern von Gruppenhomomorphismen sind Untergruppen.

<u>**Beweis**</u>

Setze $H = \varphi(G) \subseteq K$. Es folgt $e_K \in H$. Für $\varphi(x), \varphi(y) \in H$ gilt $\varphi(x)\varphi(y) = \varphi(xy) \in H$ sowie $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$, also ist H Untergruppe. Betrachte jetzt $ker(\varphi) \subseteq G$. Es gilt $\varphi(e_G) = e_K$, also $e_G \in ker(\varphi)$. Ist $x, y \in ker(\varphi)$, so folgt

$$\varphi(xy) = \varphi(x)\varphi(y) = e_K \cdot e_K = e_K \text{ , also } xy \in ker(\varphi)$$

$$\varphi(x^{-1}) = \varphi(x)^{-1} = e_K^{-1} = e_K \text{ , also } x^{-1} \in ker(\varphi)$$

$\square$

Bemerkung:

<u>Jede</u> Untergruppe von $H \subseteq G$ ist Bild eine geeigneten Homomorphismus (nämlich der Inklusion $H \hookrightarrow G$). Wir werden sehen, dass im allgemeinen <u>nicht</u> jede Untergruppe $H \subseteq G$ Kern eines Homomorphismus ist.

1.17 Normalteiler

Sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. Wir nennen N **normal** in G oder **Normalteiler** in G, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) für alle $a \in G$ gilt $aN = Na$ (Rechtsnebenklassen sind Linksnebenklassen)

(ii) für alle $a \in G$ gilt $aNa^{-1} = N(aNa^{-1} = \{ana^{-1} \mid n \in N\})$

(iii) für alle $a \in G$ gilt $aN \subseteq Na$

(iv) für alle $a \in G$ gilt $aNa^{-1} \subseteq N$

Beweis:
(i) und (ii) sind äquivalent: multipliziere von rechts mit a^{-1} bzw. a. Genauso sind (iii) und (iv) äquivalent.
Klar: (iv) $\Rightarrow$ (iii) ($\checkmark$)
Zeige (iv) $\Rightarrow$ (ii): Setze $b = a^{-1}$, es folgt aus (iv), dass $bNb^{-1} \subseteq N \rightsquigarrow N \subseteq b^{-1}Nb = aNa^{-1}$. Also gilt für alle $a \in G$, dass $N \subseteq aNa^{-1}$ und $aNa^{-1} \subseteq N$, damit gilt (ii) $\square$

Lemma

Ist $\varphi : G \to K$ ein Homomorphismus von Gruppen, dann ist $ker(\varphi)$ ein Normalteiler in G.
Beweis:
Sei $N = ker(\varphi) = \{n \in G \mid \varphi(n) = e\}$, sei $a \in G$. Dann gilt

$$\varphi(ana^{-1}) = \varphi(a)\underbrace{\varphi(n)}_{=e}\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = e$$

also gilt $aNa^{-1} \subseteq N \quad \forall a \in G$. $\square$

Achtung:
Bilder von Homomorphismen sind nicht immer Normalteiler, nach Beispiel 1.15 (b) ist jede Untergruppe Bild eines Homomorphismus, aber nicht jede Untergruppe ist normal.

Beispiel:
$G = Sym(3)$, $g = (1,2)$ Transposition, die 1 und 2 vertauscht. $g^2 = id$, $\langle g \rangle = \{g, id\} \subseteq Sym(3)$ ist Untergruppe, aber für $h = (2,3)$ gilt

$$h\langle g \rangle h^{-1} = \{hgh^{-1}, h\ id\ h^{-1}\} = \{\underbrace{(2,3)(1,2)(2,3)}_{=(3,1)}, id\} \not\subseteq \langle g \rangle$$

also ist $\langle g \rangle$ kein Normalteiler in $Sym(3)$.

Schreibweise: Ist $N \subseteq G$ ein Normalteiler, schreibt man kurz $N \trianglelefteq G$

Beachte: Ist G abelsch, dann sind alle Untergruppen $H \subseteq G$ automatisch normal.

1.18 Definition Teilmengen assoziativ

Für Teilmengen $X, Y, Z \subseteq G$ in einer Gruppe schreibe kurz:

$$XY = \{xy \mid x \in X,\ y \in Y\} \subseteq G$$
$$X^{-1} = \{x^{-1} \mid x \in X\} \subseteq G$$

Es gilt dann $(XY)Z = X(YZ)$, (weil die Verknüpfung assoziativ ist).

Satz

Sei $N \trianglelefteq G$ Normalteiler in der Gruppe G. Dann ist ${}^{G}/_{N} = \{gN \mid g \in G\}$ eine Gruppe mit der Verknüpfung $(gN) \cdot (hN) = ghN$
Das Neutralelement ist $eN = N$, das Inverse zu gN ist $g^{-1}N$.
<u>**Beweis:**</u>
Da N Normalteiler ist, gilt für $g, h \in G$

$$gNhN = g(Nh)N \overset{1.17}{=} g(hN)N = ghNN \overset{N \text{ Gruppe}}{=} ghN$$

Die Verknüpfung ist also einfach gegeben durch

$$gN \cdot hN = gNhN = ghN$$

und damit assoziativ nach obiger Bemerkung. Es gilt $NgN = gNN = gN = gNN$, also ist N ein Neutralelement. Weiter gilt:

$$gNg^{-1}N = gg^{-1}N = N = g^{-1}gN = g^{-1}NgN$$

□

1.19 Definition π_H

Ist G eine Gruppe und H eine Untergruppe, so definieren wir $\pi_H : G \to {}^{G}/_{H}$ durch $\pi_H(g) = gH$.

Satz

Ist $N \trianglelefteq G$ ein Normalteiler, dann ist $\pi_N : G \to {}^{G}/_{N}$ ein surjektiver Homomorphismus mit Kern $N = ker(\pi_N)$.
<u>**Beweis:**</u>
π_N ist nach Definition surjektiv und

$$\pi_N(gh) = ghN = gNhN = \pi_N(g)\pi_N(h)$$

Weiter gilt

$$\pi_N(g) = N \iff gN = N \overset{1.13}{\iff} g \in N$$

□

Folgerung:
Jeder Normalteiler ist auch ein Kern eines Homomorphismus.

1.20 Der Homomorphiesatz

Sei $G \overset{\varphi}{\to} K$ ein Homomorphismus von Gruppen, sei $N \trianglelefteq G$ ein Normalteiler. Wenn gilt $N \subseteq ker(\varphi)$, dann gibt es <u>genau einen</u> Homomorphismus $\overline{\varphi} : {}^{G}/_{H} \to K$ mit $\overline{\varphi} \circ \pi_H = \varphi$.

$$\begin{tikzcd}
G \arrow[rr, "\varphi"] \arrow[dr, "\pi_N"'] & & K \\
& {}^{G}/_{N} \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

Abbildung 1: Homomorphiesatz

Beweis:
Existenz von $\overline{\varphi}$:
Für $g \in G$ setze $\overline{\varphi}(gN) = \varphi(g)$. Das ist eine wohldefinierte Abbildung, denn angenommen,

$$gN = g'N \Rightarrow g^{-1}g' \in N \subseteq ker(\varphi) \Rightarrow \varphi(g^{-1}g') = e \Rightarrow \varphi(g) = \varphi(g')$$

Es gilt damit

$$\overline{\varphi}(gNhN) = \overline{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(gN)\overline{\varphi}(hN)$$

also ist $\overline{\varphi}$ ein Homomorphismus.

Eindeutigkeit von $\overline{\varphi}$:
Sei $\psi : {}^{G}/_{N} \to K$ ein Homomorphismus mit $\psi \circ \pi_N = \varphi$.
Es folgt

$$\psi(gN) = \psi(\pi_N(g)) = \varphi(g) = \overline{\varphi}(gN) \quad \forall g \in G$$

Bemerkung:
In der Situation vom Homomorphiesatz gilt:

(i) $ker(\varphi) = \pi_N^{-1}\ ker(\overline{\varphi})$

(ii) $ker(\overline{\varphi}) = \pi_N\ ker(\varphi)$

(iii) $\varphi(G) = \overline{\varphi}({}^{G}/_{N})$

Beweis:
(iii) ist klar nach Konstruktion, $\overline{\varphi}(gN) = \varphi(g)$
(ii) $\overline{\varphi}(gN) = e = \varphi(g) \Leftrightarrow g \in ker(\varphi)$, also $ker(\overline{\varphi}) = \pi_N(ker(\varphi))$
(i) $\varphi(g) = e \Rightarrow g \in ker(\varphi) \Rightarrow \pi_N(g) \in ker(\overline{\varphi}) \Rightarrow \varphi(g) = e$ □

1.21 Definition Isomorphismus

Ein Gruppenhomomorphismus $\varphi : G \to K$ heißt **Mono/Epi/Isomorphismus**, wenn φ injektiv/surjektiv/bijektiv ist.
(Klar: φ Epimorphismus $\Leftrightarrow \varphi(G) = K$)
Für einen Mono / Epi / Isomorphismus schreibt man auch:
$\overset{\varphi}{\rightarrowtail}$ $\overset{\varphi}{\twoheadrightarrow}$ und $\overset{\cong}{\to}$.

Lemma

Ein Gruppenhomomorphismus $G \overset{\varphi}{\to} K$ ist genau dann injektiv, wenn gilt $ker(\varphi) = \{e_G\}$.

Beweis:
Wenn φ injektiv ist, dann ist $ker(\varphi) = \{e_G\}$ (klar). Angenommen, $ker(\varphi) = \{e_G\}$ und $a, b \in G$ mit $\varphi(a) = \varphi(b) \rightsquigarrow \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) = e_K \Rightarrow ab^{-1} = e_G \Rightarrow a = b$ □

1.22 Satz Eigenschaften von Gruppenhomomorphismen

Sei $G \overset{\varphi}{\to} K$ ein Gruppenhomomorphismus. Dann gilt folgendes:

(i) Ist $H \subseteq G$ Untergruppe, so ist $\varphi(H) \subseteq K$ Untergruppe. Wenn $H \trianglelefteq G$, so gilt $\varphi(H) \trianglelefteq \varphi(G)$

(ii) Ist $L \subseteq K$ Untergruppe, so ist $\varphi^{-1}(L) \subseteq G$ Untergruppe. Ist $L \trianglelefteq K$, so gilt $\varphi^{-1}(L) \trianglelefteq G$.

Beweis:

(i) Sei $a, b \in H$ und $g \in G$. Es gilt $\varphi(a)\varphi(b) = \varphi(ab) \in H$, $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$. $\varphi(e_G) = e_K \in \varphi(H) \Rightarrow \varphi(H)$ Untergruppe.
Ist $H \trianglelefteq G$, so folgt $\varphi(g)\varphi(H)\varphi(g)^{-1} = \varphi(gHg^{-1}) \overset{H \trianglelefteq G}{=} \varphi(H)$ □

(ii) Sei $a, b \in \varphi^{-1}(L)$, $g \in G$ (also $\varphi(a), \varphi(b) \in L$). Es folgt $\varphi(ab) \in L$, $\varphi(a^{-1}) = \varphi(a)^{-1} \in L$ und $\varphi(e_G) = e_K \Rightarrow ab, a^{-1}, e_G \in \varphi^{-1}(L) \rightsquigarrow$ Untergruppe.
Angenommen, $L \trianglelefteq K$. Es folgt $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) \in L$, also $g\varphi^{-1}(L)g^{-1} \subseteq \varphi^{-1}(L)$. □

Beispiele
Gruppe $(\mathbb{Z}, +)$, $\varphi : \mathbb{Z} \to \mathbb{Z}$ Homomorphismus, $\varphi(z) = m \cdot z$, $m \in \mathbb{Z}$ fest.
$\varphi(\mathbb{Z}) = m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\} = (-m)\mathbb{Z}$
z.B. $m = 2 \rightsquigarrow 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$ gerade Zahlen
$ker(\varphi) = \begin{cases} \{0\}, & \text{wenn } m \neq 0 \\ \mathbb{Z}, & \text{wenn } m = 0. \end{cases}$ φ surjektiv $\Leftrightarrow$ $m = \pm 1$
φ injektiv $\Leftrightarrow$ $m \neq 0$

Angenommen, $m > 0$, $a, b \in \mathbb{Z}$
$a + m\mathbb{Z} = b + m\mathbb{Z}$ Nebenklassen $\overset{1.13}{\Leftrightarrow} a \in b + m\mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$
Folglich $\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$ insbesondere $\#\mathbb{Z}/m\mathbb{Z} = m$.
Schreibe $\overline{k} = k + m\mathbb{Z}$ **Kongruenzklasse** von k **modulo** m.
$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ wird erzeugt von $\overline{1} \rightsquigarrow \mathbb{Z}/m\mathbb{Z} = \langle \overline{1} \rangle$ zyklische Gruppe der ordnung m. $o(\overline{1}) = m$.
Später mehr dazu.

1.23 Die Isomorphiesätze

Lemma

Sei G eine Gruppe, seien $H, N \subseteq G$ Untergruppen. Wenn $N \trianglelefteq G$ gilt, dann ist $HN = NH \subseteq G$ eine Untergruppe.

Beweis:
Es gilt $e = e \cdot e \in N \cdot H$. Weiter gilt für $h_1, h_2 \in H$, $n_1, n_2 \in N$, dass

$$h_1 n_1 h_2 n_2 = \underbrace{h_1 h_2}_{\in H} \underbrace{h_2^{-1} n_1 h_2}_{\in N} n_2 \in HN$$

$$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} \underbrace{h_1 n_1^{-1} h_1^{-1}}_{\in N} \in HN$$

$$(HN)^{-1} = N^{-1} H^{-1} = NH \subseteq HN \text{ genauso } HN \subseteq NH$$

□

Satz

Sei $G \overset{\varphi}{\to} K$ ein Epimorphismus von Gruppen. Sei $N = ker(\varphi)$. Dann ist die Abbildung $\overline{\varphi} : G/N \to K$ aus dem Homomorphisatz 1.20 ein Isomorphismus.

Beweis:
$\overline{\varphi}(G/N) = \varphi(G)$ und $ker(\overline{\varphi}) = \{N\}$ nach dem Beweis von 1.20. Den Isomorphismus $\overline{\varphi} : G/ker(\varphi) \overset{\cong}{\to} K$ nennt man **kanonisch** oder **natürlich**.

Theorem: 1. Isomorphiesatz

Sei G eine Gruppe, seien $H, N \subseteq G$ Untergruppen mit $N \trianglelefteq G$. Dann gilt $H \cap N \trianglelefteq H$, $N \trianglelefteq NH$ und die Abbildung

$$\begin{aligned} {}^{H}\!/_{H\cap N} &\to {}^{NH}\!/_{N} \\ aH &\mapsto aNH \end{aligned}$$

ist ein Isomorphismus. ("Kürzungsregel")

Beweis:

Index

Die Seitenzahlen *sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar!*

Abbildungsverzeichnis