Algebra I

Stand vom 22. Oktober 2014

Dozent: Prof. Dr. Christopher Voll
voll@math.uni-bielefeld.de

Autor: Jonas Betzendahl
jbetzend@techfak.uni-bielefeld.de

Inhaltsverzeichnis

-1 Organisatorisches etc.

Dozent ist Prof. Dr. Christopher Voll
voll@math.uni-bielefeld.de
Büro: UHG V5-238, Sprechstunde noch im Flux

Vorlesungen finden an Montagen von 08.30 Uhr bis 10.00 Uhr und Mittwochs von 14.15 Uhr bis 15.45 Uhr statt.

Es wird darauf hingewiesen, dass die Übungen bei Dr. Doang in Englisch abgehalten werden.

Voraussetzung für die Zulassung zur Prüfung sind das Erreichen von mindestens 50 % der Punkte und mindestens zwei Mal eine aktive Teilnahme an den Übungen (Vorrechnen) abgeleistet zu haben.

Bücher:	Einführung in die Algebra (F. Lorenz, Spektrum)	
	Algebra 1 (S. Bosch, Springer)	
	Algebra (S. Lang, Springer)	
	Algebra (Hungerford)	
	Algebra (v.d. Waerden)	(Ein Klassiker)
	Algebra (E. Artin)	

Übungszettel gibt es immer am Mittwoch der Woche n, bearbeiten werden müssen diese bis Mittwoch der Woche n+1 (Abgabe vor der Vorlesung im Postfach des Tutors), besprochen werden sie in der Woche n+2 in den Tutorien.

0 Algebra - die Kunst, Gleichungen zu lösen (Einführung)

Lineare Algebra:
$a_{11}x_1 + a_{12}x_2 + \cdots + a_{nm}x_m = b_1$
$\ldots$
$a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = b_n$

Alle Fragen können in Form $a_{ij}, b_i \in \mathcal{K}$ beantwortet werden.
Verallgemeinerung: $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$ (polynom. Gleichung von Grad $n(a_n \neq 0)$.
„Struktur" der Lösungen solcher Gleichungen treibt Menschen seit Jahrtausenden um.
Spezialfall: Quadratische Gleichungen

$$x^2 + bx + c = 0 \Leftrightarrow \frac{-b \pm \sqrt{b^2 - 4c}}{21}$$

durch Wurzeln lösbar. Kubische Gleichungen:

$$x^3 + bx^2 + cx + d = 0 \Leftrightarrow \ldots$$

ebenfalls durch Wurzeln lösbar. Im 16. Jahrhundert wurde bekannt, dass auch quartische Gleichungen ($n = 4$) durch Wurzelausdrücke lösbar sind.
Was nicht ins Weltbild des 16. Jahrhundert passte: Im 19. Jahrhundert zeigte Abel: Nicht jede quintische Gleichung ($n = 5$) kann durch Wurzelausdrücke gelöst werden.
Galois: Lösungen von Polynomen sind nicht einfach Mengen ohne Struktur sondern Mengen *mit* Struktur ($\rightarrow$ Gruppentheorie). Auflösbarkeit von $f = 0$ durch Wurzel $\Rightarrow$ Galois-Gruppe(f) auflösbar.
Ziel der Vorlesung: Einführung in die Sprache der modernen Algebra, sowohl durch Anerkennen der Theorie als auch durch das Praktizieren.

1 Fundamente der Gruppentheorie

1.1 Monoide & Gruppen

Definition 1 *Ein* Monoid *ist eine Menge M zusammen mit einer Verknüpfung $\cdot : M \times M \to M$, die die Eigenschaften erfüllt:*

- `(ASS)` $\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Assoziativität)*
- `(NEU)` $\exists\, e = e_M \in M\ \forall a \in M,\ e \cdot a = a = a \cdot e$ *(Existenz eines neutralen Elementes)*

Bemerkung: Die Notation ist oft einfach nur „ab" statt „$a \cdot b$", oft auch bei mehreren Monoiden gleichzeitig. Ausgelassen wird immer die passende Verknüpfung. Es wird auch die Schreibweise $\prod_{i=1}^{n} a_i$ für den Ausdruck $a_1 \cdot a_2 \cdot \ldots a_n,\ a_i \in M$ verwendet. Weiterhin gelten per Konvention: $\prod_{i=1}^{n} a_i = e$ für $n \leq 0$ und $a^m = \underbrace{a \cdot a \cdot \ldots a}_{\text{m-mal, } m \in \mathbb{N}}$.

Behauptung: $e \in M$ ist eindeutig (siehe unten).

Sei $a \in M$. Wir nennen $b \in M$ *invers zu a* falls $a \cdot b = b \cdot a = e$ gilt. Falls (!) solch ein b existiert, ist es eindeutig (siehe unten). In diesem Fall ist die Notation oft a^{-1} für b: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition 2 *Eine* Gruppe *ist ein Monoid $(G, \cdot)$ mit der folgenden Eigenschaft:*

`(INV)` $\forall a \in G\ \exists\, a^{-1} \in G$ *sodass* $a \cdot a^{-1} = a^{-1} \cdot a = e$ *(Existenz eines inversen Elements)*

G heißt kommutativ *oder synonym dazu* abelsch *falls folgende Eigenschaft gilt:*

`(KOM)` $\forall a, b \in G : a \cdot b = b \cdot a$ *(Kommutativität)*

Vektorräume zum Beispiel sind abelsche Gruppen, die interessante Struktur ist hier aber nicht die abelsche Eigenschaft sondern die Multiplikation mit Skalaren, die sich gut mit der Gruppenstruktur verträgt.

Die *Ordnung* einer Gruppe ist $(G, \cdot)$ ist die Kardinalität $|G|$ von G.

Konvention: „Gruppe G", falls $\cdot$ klar ist. Ist G abelsch, so schreibt man oft $+$ für $\cdot$ (die Monoidverknüpfung) und man redet von „additiver Schreibweise" im Gegensatz zu „multiplikativer Schreibweise". Bei additiver Schreibweise schreibt man oft 0 für e, bzw. bei multiplikativer Schreibweise 1.

Beispiele 1.3:

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sind abelsche Gruppen. Ebenso $(\mathcal{K}, +)$ wenn $(\mathcal{K}, +, \cdot)$ ein Körper ist.
2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^*, \mathbb{C}^*, \mathcal{K}^* = \mathcal{K} \setminus \{0\}$, mit $1 = e$ als Einselemnent, sind abelsche Gruppen
3. $GL_n(R) = \{x \in Mat_n(R) | \det(x) \neq 0\}$ mit R beliebiger Körper, invertierbare Matrizen über R, $SL_n(R) = \{x \in GL_n(R) | \det x = 1 \in R\}$, ($1_n$ = Einheitsmatrix) sind Gruppen bezüglich der Matrixmultiplikation, mit Einselement jeweils 1_n, allerdings für $n > 1$ <u>nicht</u> abelsch.
4. $\mathbb{N}_0 = \mathbb{N} \cup 0$, $\mathbb{N} = \{1, 2, 3, \ldots\}$. Sowohl $(\mathbb{N}_0, +)$ als auch $(\mathbb{N}, \cdot)$ sind Monoide aber keine Gruppen ($2x = 1$ unlösbar).
5. $Mat_n(R)$ (R Körper) ist ein Monoid ($\cdot$ = Multiplikation, $e = 1_n$).
6. $A \in Mat_n(\mathbb{Z}), L_A = \{x \in {\mathbb{N}_0}^n | xA = 0\}$ ist ein Monoid mit Nullvektor als Einselement.

   Notation: R Ring, dann $R^n = \{(r_1, \ldots, r_n) | r_i \in R\}$ (n-Tupel).
7. Symmetrische Gruppen: Sei X beliebige Menge. $Sym(X) := \{f : X \to X | f \text{ Bijektion }\}$ ist eine Gruppe mit Verknüpfung von Abbildungen als „Multiplikation". ($f, g \in Sym(X) : f \circ g : X \to X$ Bijektion!), mit $id : X \to X$ als Einselement.

   Rekapitulation der Leibnitz-Formel: K- Körper: $a_{ij} = A \in Mat_n(K)$.

   $$\det(A) = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.$$

Wichtiger Spezialfall: $X = \{1, 2, \ldots, n\}, n \in \mathbb{N}$. Setze $S_n = Sym(X)$„ , symmetrische Gruppe vom Grad n“. (Dies erlaubt es, dass jede endliche Gruppe als Unterobjekt verstanden werden kann) Ordnung $|S_n| = n!$. Nicht abelsch falls $n > 2$.

$f \in S_n$:

Matrixschreibweise $\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$

oder Zykelschreibweise: $(1, f(1), f(f(1)) \ldots)$, $(a, f(a), f^2(a) \ldots), \underbrace{(b, f(b), f^2(b) \ldots)}_{\text{„Zykel“}}$ für $a \notin \{ f^n(1) \,|\, n = \{1, 2, 3, \ldots\} \}$

$\subseteq \{1, \ldots, n\}$ und $b \notin \{ f^n(1) \,|\, dots \} \cup \{ f^n(a) \,|\, n \in \mathbb{N} \}$

Konvention: Zykel der Länge 1 weg.

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \Leftrightarrow (1)(2)(3)$ (A)

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \Leftrightarrow (12)(3)$ (B)

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \Leftrightarrow (123)$ (C)

...

8. Sei X eine beliebige Menge und G eine Gruppe. Dann ist $G^X := Abb(X, G) = \{q : X \to G\}$ mit der folgenden Verknüpfung eine Gruppe:

   Gegeben $\varphi, \psi \in G^X$, definiere für $x \in X$ $\phi \circ \psi := \phi(x) \cdot \psi(x) \in G$ Dies nennt sich „komponentenweise Multiplikation“.

9. Sei X eine beliebige Menge, $\{G_x\}_{x \in X}$, Familie von Gruppen. Dann ist $\prod_{x \in X} G_x = \{ (g_x)_{x \in X} \,|\, \forall x : g_x \in G_x \}$ mit der Verknüpfung $(g_x)_{x \in X} \cdot (h_x)_{x \in X} := (g_x \cdot h_x)_{x \in X}$ – Produkt der Gruppen $G_x, x \in X$.

1.2 Untergruppen und Homomorphismen

Definition 3 *Sei G ein Monoid, $H \subseteqq G$ Teilmenge. H heißt* Untermonoid *von G, falls*

- $e \in H$
- $a, b \in H \Rightarrow ab \in H$

Ist G eine Gruppe, so heißt H Untergruppe*, falls zusätzlich*

- $a \in H \Rightarrow a^{-1} \in H$

.

Schreibe gegebenenfalls „$H \leqslant G$“ oder „$H < G$“. Schreibe „$H \lneqq G$“ für Untergruppen $H \neq G$.

Beispiel (1.5):

1. G Gruppe $\Rightarrow H = G \leqslant G$, $\{e\} = G$ heißen *triviale Untergruppen.*
2. $G = (\mathbb{Z}, +), m \in \mathbb{Z}$. $H = m\mathbb{Z} = \{ mx \,|\, x \in \mathbb{Z} \} \leqslant \mathbb{Z}$.

   (a) @1: $0 = m0 \in H$
   (b) @2: $mx(\in H) + my(\in H) = m(x + y) \in H$, $x, y \in \mathbb{Z}$
   (c) @3: Inverses von mx ist $-mx(mx + (-mx) = 0 = e_{\mathbb{Z}})$.

   Tatsache (Beweis später): Jede Untergruppe von Z ist von der Form mZ. $\mathbb{Z} = (-1)Z = 1Z, 0\mathbb{Z} = e_{\mathbb{Z}}$. Schreibe $(m) = m\mathbb{Z}$.

   Echte Untergruppen: $\{A, B\}, \{A, D, E\}, \{A, C\}, \{A, F\}$.

3. G Gruppe, $g \in G$, $H :=< g >:= \{ g^n \,|\, n \in \mathbb{Z} \} \leqslant G$ (!!).

(a)
(b) $g^n \cdot g^m = g^{n+m}$
(c) $(g^n)^{-1} = g^{-n}$

„Die von g erzeugte (zyklische) Untergruppe“ = die kleinste Untergruppe von G, die g enthält (braucht g, g^2, g^3, $\ldots$, g^{-1}, $\ldots$).

4. $SL_n(K) \leqslant GL_n(K)$, K Körper
   LHS $= \{\, x \in Mat_n(K) \,|\, det(x) = 1 \,\}$ RHS $= \{\, x \in Mat_n(K) \,|\, det(x) \neq 0 \,\}$
   Für alle „vernünftigen“ Körper und alle $n > 1$ ist das eine nicht-triviale Teilmenge.

Definition 4 *(1.6) Seien G, G' Monoide, mit Einselementen $e \in G$ und $e' \in G'$. Ein* Monoidhomomorphismus *ist eine Abbildung $\varphi : G \to G'$, derart, dass*

- $\varphi(e) = e'$
- $\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Sind G, G' Gruppen, spricht man von einem Gruppenhomomorphismus *(oder oft einfach nur Homomorphismus).*

Bemerkung: Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus, dann gilt
(Übungsaufgaben:)

1. $\forall a \in G : (\varphi(a))^{-1} = \varphi(a^{-1})$. Nach der zweiten Eigenschaft von oben gilt $\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(e) = e$
2. $\ker(\varphi) \coloneqq \{\, g \in G \,|\, \varphi(g) = e' \,\} \leqslant G$.
3. $img(\varphi) = \{\, \varphi(g) \,|\, g \in G \,\} \leqslant G'$

Definition 5 *(1.7) Ein Gruppenhomomorphismus $\varphi : G \to G'$ heißt*

- Monomorphismus*, falls er injektiv ist.* ($\Leftrightarrow \ker(\varphi) = \{e\}$),
- Epimorphismus*, falls er surjektiv ist.* ($\Leftrightarrow im(\varphi) = G'$),
- Isomorphismus*, falls er sowohl ein Epimorphismus als auch ein Monomorphismus ist,*
- Endomorphismus *von G, falls $G' = G$,*
- Automorphismus *von G, falls $G' = G$ und φ ein Isomorphismus ist.*

Sprechweise: Gegeben ein Isomorphismus heißen G und G' *isomorph zu einander*. Man schreibt $G \cong G'$. Beispiel: $G = \mathbb{Z}, H = 2\mathbb{Z} \leqslant G$.
Behauptung: $G \to G$, $g \mapsto 2g(= g + g)$ ist Isomorphismus. Also schreibt man $\mathbb{Z} \cong 2\mathbb{Z}$. Isomorphie ist transitiv $(G \cong G'), (G' \cong G'') \Rightarrow G \cong G''$.

Beispiele (1.8):

1. Sei G ein Monoid, $g \in G$, dann ist $\varphi : \mathbb{N}_0 \to G, n \mapsto g^n$ ein Monoidhomomorphismus. (Übungsaufgabe!) φ ist sozusagen bestimmt durch $\varphi(1)$.
2. Ist G sogar eine Gruppe, dann bestimmt $n \mapsto g^n$ einen Gruppenhomomorphismus: $\varphi : \mathbb{Z} \to G$. $im(\varphi) = \{\, g^n \,|\, n \in Z \,\} =< g >$.
   Übungsaufgabe: Wenn $| < g > | = \infty$, dann ist $\phi : \mathbb{Z} \to im(\varphi)$ ein Isomorphismus.
3. Sei G eine Gruppe, $g \in G$. Dann ist $\psi_g \coloneqq G \to G, h \mapsto ghg^{-1}$ ein Gruppen<u>automorphismus</u> (Übungsaufgabe: Checken und was ist das Inverse zu ψ_g?).
   $\psi_g(h \cdot h') = ghh'g^{-1} = gheh'g^{-1} = (ghg^{-1})(gh'g^{-1}) = \psi_g(h)\psi_g(h')$. Dies nennt sich „Konjugation mit g“.
   Prüfen: $Aut(G) = \{\, \psi : G \to G \,|\, \phi Automorphismus \,\}$ bildet Gruppe unter Verknüpfung.
   $\{\, \phi_g \,|\, g \in G \,\} < Aut(G) =$ Ïnnere Automorphismen von G”.

1.3 Nebenklassen

Definition 6 *Sei G eine Gruppe, $H \leqslant G$. Eine Menge der folgenden Form: $gH = \{ g \cdot H \mid h \in H \} \subseteq G, g \in G$ heißt* Linksnebenklasse *(LNK) (left coset) von H in G.*
Dementsprechend: $Hg = \{ h \cdot g \mid h \in H \}$ heißt Rechtsnebenklasse (RNK) von H in G.

Nebenklassen „pflastern“ die Gruppe.
Lemma (1.10): Seien gH und $g'H$, mit $g, g' \in H$ Linksnebenklassen von $H \leqslant G$. Dann sind Äquivalent:

1. $gH = g'H$
2. $gH \cap g'H \neq \varnothing$
3. $g \in g'H$
4. $g'^{-1}g \in H$

Beweis:

1. klar: $gH \ni ge = g \Rightarrow gH \neq \varnothing$
2. $gh \in g'H$ für ein $h \in H$. $\Rightarrow \exists h' \in H : gh = g'h' \Leftrightarrow g \underbrace{hh^{-1}}_{e} = g' \underbrace{h'h^{-1}}_{\in H} \Leftrightarrow g \in g'H$.
3. $g \in g'H \Leftrightarrow \exists h \in H : g = g'h \Rightarrow (g')^{-1} \cdot g = h \in H$.
4. $(g')^{-1}g \in H$, etwa $(g')^{-1}g = h \in H \Rightarrow g = g' \cdot h$. $gH = \{ g\tilde{h} \mid \tilde{h} \in H \} = \{ g' \cdot (h\tilde{h}) \mid \tilde{h} \} = g'H$ □

Satz (1.11): Je zwei Linksnebenklassen von H in G sind in Bijektion zueinander. Verschiedene LNK sind disjunkt. Insbesondere ist G disjunkte Vereiningung der Linksnebenklassen von H in G. **Beweis:** @Bijektion: Gegeben gH, $g'H$, $g, g' \in G$.
$gH \underbrace{\cong}_{(bijektiv)} H$. $(gH \cong eH = H \cong g'H)$
Es reicht zu zeigen: $H \to gH, h \mapsto gh$ ist Bijektiv. $gh = gh' \leftrightarrow g^{-1}gh = g^{-1}gh' \leftrightarrow h = h'$. □

Definition 7 *(1.12) Sei G eine Gruppe, $H \leqslant G$. Schreibe $G/H = \{ gH \mid g \in G \}$ für die Menge der Linksnebenklassen von H in G und $H\ G = \{ Hg \mid g \in H \}$ für die Menge der Rechtsnebenklassen von H in G.*

Bemerkung: $G/H \to H\ G, gH \mapsto Hg$ ist Bijektion.
ÜA: $(gH = g'H \Leftrightarrow g \cdot (g')^{-1} \in H \Leftrightarrow Hg = Hg')$

Definition 8 *(1.13) Setze $|G : H| (= [G : H] = (G : H)) = |G/A| = = |H\ G|$ genannt der* Index *von H in G.*

Informell: $|G : H|$ „inverse Dichte“ von H in G. $\frac{1}{|G:H|}$ =„$P(g \in H)$“.
z.B.: $G = \mathbb{Z}, H = m\mathbb{Z}. \to |G : H| = m$.
Beispiel (1.14) :

1. $H = \{e\} : G/H \cong H\ G \cong G \Rightarrow |G : H| = |G|$.
2. $H = G : G/G = G$
   $G = \{\cdot\} \Rightarrow |G : G| = 1$.
3. Drittes Beispiel siehe oben.

Korrollar (1.5) (Satz von Lagrange): Sei G eine <u>endliche</u> Gruppe, $H \leqslant$. Dann gilt $|G| = |H| \cdot |G : H|$. $(\frac{|G|}{|H|} = |G : H|)$.
(1.16) Insbesondere teilt $|H|$ stets $|G|$!
Achtung: $\exists$ endliche Gruppen G mit der Eigenschaft, dass einige Teiler ihrer Ordnung von von Untergruppen H realisiert werden. (ÜA: Eleganter formulieren.)
z.B: Ist p eine Primzahl, $|G| = p^e, e \in \mathbb{N}_0$, so heißt G *p-Gruppe.* Aus Langrange folgt: $\forall H \leqslant G, H$ ist p-Gruppe.

1.4 Normalteiler & Isomorphiesätze

Definition 9 *(1.17) Sei G eine Gruppe, $H \leqslant G$ heißt* Normalteiler *(oder synonym dazu: normale Untergruppe), wenn $\forall g \in G\ gH = Hg$. Gegebenenfalls heißt gH die von g bestimmte Nebenklasse von H in G. Gegebenenfalls schreibe $(H \trianglelefteq G) \Leftrightarrow H \triangleleft G$.*

Bemerkung: g, H, G wie in (1.17): $gH = Hg \Leftrightarrow gHg^{-1} = H$.
Um zu verifizieren, ob $H \leqslant G$ ein Normalteiler ist, reicht es zu testen, ob $\forall g. gHg^{-1} \subseteq H$ (*).
In der Tat. Angenommen (*) gilt, so gilt auch $\forall g \in G. gH \subseteq Hg$. Aber es gilt $g^{-1}Hg^{-1^{-1}} = g^{-1}Hg \subseteq H$, d.h. $Hg \subseteq gH$
$\Rightarrow gH = Hg$
Beispiel (1.18):

1. $\{e\} \triangleleft G$. $(\forall g : g\{e\} = \{e\}g = \{g \cdot e\} = \{g\})$. Ebenso: $G \triangleleft G : gG = G = Gg$.

2. Ist G abelsch, ist jede Untergruppe Normalteiler.

3. $G = S_3$. Die Untergruppen H von S_3 die von $\{e\}$ und S_3 selbst verschieden sind, sind $\{<(12)>, <(13)>, <(23)>, <(123)>\}$ (Untergruppen der Ordnung 2,2,2 und 3. Lagrange sagt dass es keine anderen geben kann.) Übungsaufgabe: Von diesen 4 Untergruppen ist nur $<(123)>$ normal.

4. Ist $\varphi : G \to G'$ Gruppenhomomorphismus, dann ist $ker(\varphi) = \{g \in G | \varphi(g) = e_{G'}\} \triangleleft G$.
   Z.z. $\forall g \in G. g(ker\varphi)g^{-1} \subseteq ker\varphi$. Sei gkg^{-1} mit $k \in ker\varphi$. Reicht zu zeigen: $\varphi(gkg^{-1}) = e_{G'}$. Aber

$$\begin{aligned} \varphi(gkg^{-1} &= \varphi(g)\varphi(h)\underbrace{\varphi(g^{-1})}_{=\varphi(g)^{-1}} \\ &= \varphi(g)e_{G'}\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} = e_{G'} \end{aligned}$$

Sei $N \triangleleft G$. Wollen Gruppenstruktur auf $G/N = \{gN | g \in G\}$.
Allgemein $X, Y \subseteq G : XY := \{xy | x \in X, y \in Y\} \subseteq G$
Definiere $\cdot : G/N \times G/N \to G/N, (gN, kN) \mapsto ghN$
$gN = g'N \Leftrightarrow g(g')^{-1} \in N$

Seien also $g' \in G, k' \in G$ mit $gN = g'N, kN = k'N$. Wir wissen, $g(g')^{-1} =: n_1 \in N, k(k')^{-1} =: n_2 \in N$.
Zu zeigen: $gkN = g'k'N$, d.h. $gh(g'h')^{-1} \in N$. Nun ist

$$\begin{aligned} gh(g'h')^{-1} &= g\underbrace{h(h')^{-1}}_{n_2}(g')^{-1} \\ &= gn_2(g')^{-1} \\ &= gn_2g^{-1}\underbrace{g(g')^{-1}}_{n_1} \\ &= \underbrace{gn_2g^{-1}}_{\in N, da N \triangleleft G} n_1 \in N \end{aligned}$$

Übungsaufgabe: Verifiziere, dass $\cdot$ eine Gruppenoperation ist.
Bemerkung: $N \triangleleft G$. Die Gruppe G/N („G modulo N") heißt „Faktorengruppe von G nach N".
$\pi : G \to G/N, g \mapsto gN$ heißt die „natürliche Reduktion", „natürlicher Homomorphismus", „natürliche Surjektion", „Reduktionmodulo N".
π ist Epimorphismus. $(g, k \in G : \underbrace{\pi(gh)}_{ghN} = \underbrace{\pi(g)\pi(h)}_{gN \cdot hN})$

Satz 1 (1.19) *„Homomorphiesatz" Sei $\varphi : G \to G'$ Homomorphismus von Gruppen G, G' und sei $N \triangleleft G$ mit $N \leq ker\varphi$. Dann existiert* genau ein *Homomorphismus $\bar{\varphi} : G/N \to G'$, derart, dass $\varphi = \bar{\varphi} \circ \pi$. *malt ein kommutierendes Diagramm**
Es gilt:

- $im(\bar{\varphi}) = im(\varphi)$
- $ker(\bar{\varphi}) = \pi(ker(\varphi)) \triangleleft G/N$
- $ker(\varphi) = \pi^{-1}(ker(\bar{\varphi})) \triangleleft G$

Beweis: Eindeutigkeit. Angenommen $\bar{\varphi}$ mit $\varphi = \bar{\varphi} \circ \pi$ existiert $\forall g \in G. \bar{\varphi}(gN) = \bar{\varphi}(\pi(g)) = \varphi(g) \Box$
Existenz: Gegeben $gN \in G/N$. Definiere $\bar{\varphi}(gN) := \varphi(g)$. Wohldefiniert?
In der Tat, seien $g, g' \in G : gN = g'N$, das heißt $g = g'n \exists n \in N$. Zu zeigen: $\varphi(g = \varphi(g')$.
$\varphi(g) = \varphi(g'n) = \varphi(g')\varphi(n) = \varphi(g')$, da $N \leq her\varphi$.
Homomorphieeigenschaft: Seien $gN, hN \in G/N$.
$\bar{\varphi}(gN \cdot hN) = \bar{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \bar{\varphi}(gN) \cdot \bar{\varphi}(hN)$

1. $ker\varphi = \pi^{-1}(ker(\bar{\varphi}))$, da $\varphi = \bar{\varphi} \circ \pi$
2. $im(\bar{\varphi}) = im(\varphi), ker\bar{\varphi} = \pi(ker\varphi)$, da π *surjektiv* ist.$\Box$

Beachte: $\bar{\varphi}$ Monomorphismus gdw. $ker\bar{\varphi} = N$ gdw. $ker\varphi = N$
Nenne $\bar{\varphi}$ den von φ auf G/N *induzierten* Homomorphismus.

Korrolar 1 (1.20) *Ist φ ein Epimorphismus, dann gilt $G/ker(\varphi) \to G'$ ist Isomorphismus von Gruppen.*

Satz 2 (1.21) *1. Isomorphiesatz Sei G Gruppe, $H \leq G$, $N \lhd G$.*

- *$HN \leq G$ ist Untergruppe (nicht nur Teilmenge). $N \lhd HN$*
- *$H \cap N \lhd H$*
- *$\varphi : H/H \cap N \to HN/N, h(H \cap N) \mapsto hN$ ist Isomorphismus*

Beweis:
Übungsaufgabe: G Gruppe, $X \subseteq G$: $X \leq G$ gdw. 1. $X \neq \emptyset$, 2. $\forall x, y \in X : x(y)^{-1} \in X$
@1: $HN \ni e \cdot e = e, \Rightarrow HN \neq \emptyset$
$h_1n_1, h_2n_2 \in HN, h_i \in H, n_i \in N$

Zu zeigen: $h_1n_1(h_1n_1)^{-1} \in HN$. In der Tat $h_1n_1n_2^{-1}h_2^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}(\overbrace{h_2 \underbrace{n1n_2^{-1}}_{\in N} h_2^{-1}}^{\in N, da N \lhd G}) \in HN$
$N \leq HN, N \lhd G$ impliziert, dass $N \lhd HN$:
$N \lhd G \Leftrightarrow \forall g \in G : gNg^{-1} \subseteq N \Rightarrow \forall k \in HN : kNk^{-1} \subseteq N \Leftrightarrow N \trianglelefteq HN$
Bemerkung: $(HN)/N nicht \cong H$. Z.B. $HH/H = H/H = \{e\}$

2 Übungsaufgaben

2.1 13/10/2014

Eindeutigkeit des Neutralen: Sei M ein Monoid. Zeige, dass $e \in M$ eindeutig ist.

Angenommen, es gäbe ein zweites neutrales Element e' mit $e \neq e'$. Dann würde gelten $e = e \cdot e' = e' \to \perp$ $\square$

Eindeutigkeit der Inversen: Sei M ein Monoid. Zeige, dass $a^{-1} \in M$, falls es existiert, eindeutig ist.

Angenommen, zu einem $a \in M$ gäbe es zwei inverse Elemente a', a'' mit $a' \neq a''$. Dann gilt $a' \cdot a \cdot a'' = a' \cdot e = a'$ als auch $(a' \cdot a) \cdot a'' = e \cdot a'' = a''$. Es folgt $a' = a'' \to \perp$ $\square$

2.2 15/10/2014

Aufgabe: Sei G eine Gruppe mit $g \in G$. Zeige: $\psi_g \coloneqq G \to G, h \mapsto ghg^{-1}$ ist ein Gruppenautomorphismus.