EINFÜHRUNG IN DIE ALGEBRA, SOMMERSEMESTER 2014

KARIN BAUR

Zusammenfassung. Einführung in die Algebra, Sommersemester 2014.
Mo 12.15 – 14.00, Do 12:00 – 13:15, jeweils im HS 10.11.

Inhaltsverzeichnis

Vorbemerkungen. Dieses Vorlesungsskript beinhaltet den Stoff der Einführung in die Algebra vom Sommersemester 2014. In der Vorlesung werden dazu weitere Aspekte diskutiert und insofern ergänzen sich der Besuch der Vorlesung und das Durcharbeiten des Materials (wie hier im Skript) sehr gut.

Als Literatur zur Vorlesung empfehle ich die Literaturliste von G. Lettl, zu finden unter
`http://www.uni-graz.at/~lettl/lehre/einfalgebralit-s10.html`

Danke für die Hinweise bzgl. Schreibfehler etc. im Skript!

1. Algebraische Grundbegriffe

[Vorlesung 1, 4.3. 2014]

1.1. Verknüpfungen.

Definition 1.1. Sei $\varnothing \neq M$ eine nichtleere Menge.

a) Eine *Verknüpfung* (oder *binäre Operation*) auf M ist eine Abbildung

$$f : M \times M \longrightarrow M, \quad (x, y) \longmapsto f(x, y)$$

Meist wird dann f mit einem Operationssymbol bezeichnet, etwa $*$ (oder konkret $+$, $-$, $\cdot$, $:$, $\circ$, $\wedge$, $\vee$, etc.), also

$$f(x, y) = x * y$$

$x * y$ heisst das *Verknüpfungsergebnis* (*Operationsergebnis*) *von* x *und* y *unter* $*$.
$(M, *)$ (mit $M \neq \varnothing$) heisst ein *Verknüpfungsgebilde* (*Magma, Menge mit Verknüpfung, Gruppoid*).

Beispiel 1.1. a) sub: $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(x, y) \longmapsto \text{sub}(x, y) := x - y$.

b) add: $\mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$, $(x, y) \longmapsto \text{add}(x, y) := x + y$.

c) mult: $M_{2,2}(\mathbb{R}) \times M_{2,2}(\mathbb{R}) \longrightarrow M_{2,2}(\mathbb{R})$, $(A, B) \longmapsto \text{mult}(A, B) := A \cdot B$ (Matrizenprodukt)

d) Ist M "klein", so kann eine Verknüpfung $*$ auf M explizit angegeben werden mit einer Verknüpfungstafel (d.h. einer Wertetabelle der Funktion $*$):
$M_1\{x_1, \ldots, x_n\}$ mit $*_1$, $M_2 := \{\triangle, \square, \circ\}$ mit $*_2$

$*_1$	x_1	x_2	x_3	$\cdots$	x_n
x_1	$x_1 *_1 x_1$	$x_1 *_1 x_2$			$x_1 *_1 x_n$
x_2	$x_2 *_1 x_1$	$\ddots$			
$\vdots$	$\vdots$			$\ddots$	
x_n	$x_1 *_n x_1$		$\cdots$		$x_n *_1 x_n$

$*_2$	$\triangle$	$\square$	$\circ$
$\triangle$	$\triangle$	$\square$	$\triangle$
$\square$	$\square$	$\square$	$\square$
$\circ$	$\triangle$	$\square$	$\circ$

Frage: was ist die Verknüpfung $*_2$?

e) $\max : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$, $(x, y) \longmapsto \max\{x, y\}$.

f) N eine beliebige Menge, sei $M := \mathcal{P}(N)$ die Potenzmenge von N. $\cap : M \times M \longrightarrow M$, $(A, B) \longmapsto A \cap B$. (Ebenso: $\cup$, $\setminus$).

Nun setzen wir die Definition 1.1 fort.

Definition (**1.1**, Forts.). b) Sei $*$ eine Verknüpfung auf M und seien $\varnothing \neq N, N' \subseteq M$ nichtleere Teilmengen von M. Dann sei

$$N * N' := \{x * y \mid x \in N, y \in N'\}.$$

N heisst *abgeschlossen unter* $*$, falls für alle $x, y \in N$ gilt: $x * y \in N$ (anders gesagt: $N * N \subseteq N$). Ist N abgeschlossen unter $*$, so induziert die Einschränkung von $*$ auf $N \times N$ eine Verknüpfung auf N; $(N, *)$ heisst dann *Teil-* oder *Unterstruktur* von $(M, *)$ (*Teilmagma*, *Teilgruppoid*).

c) Sei $(M, *)$ Verknüpfungsgebilde. Dann heisst $*$
- *assoziativ*, falls für alle $x, y, z \in M$ gilt: $(x * y) * z = x * (y * z)$
- *kommutativ*, falls für alle $x, y \in M$ gilt: $x * y = y * x$.

Ein Element $e \in M$ heisst $\left\{\begin{array}{l}\text{links-neutrales}\\ \text{rechts-neutrales}\\ \text{neutrales}\end{array}\right\}$ Element für die Operation $*$, falls $\forall x \in M$ gilt: $\left\{\begin{array}{l} e * x = x \\ x * e = x \\ e * x = x * e = x \end{array}\right\}$

Ist $*$ assoziativ und existiert ein neutrales Element $e \in M$ für $*$, so nennt man $(M, *)$ eine *Halbgruppe*.

Existiert ein für $*$ neutrales Element $e \in M$, so nennt man ein Element $a \in M$ *invertierbar* (bzgl. $*$), falls ein $a' \in M$ existiert mit $a * a' = a' * a = e$. a' heisst dann *Inverses* zu a (und a Inverses zu a').
Die Menge aller invertierbaren Elemente von M wird geschrieben als

$$M^\times := (M, *)' := \{a \in M \mid a \text{ ist invertierbar bzgl. } *\}.$$

Bemerkung: Es ist $\{e\} \subseteq M^\times$.

Zurück zu den Beispielen 1 a)-f):

a) 0 ist re-neutral, es gibt kein li-neutrales. $-$ ist nicht assoziativ, nicht kommutativ.
b) $+$ ist assoz., komm., 0 ist neutral, $-x$ ist invers zu x.
c) Matrizenmult. ist assoziativ, nicht kommutativ, $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ ist neutral. Invertierbare Elemente: $\mathrm{GL}_2(\mathbb{R})$.
d) $(M_2, *_2)$: assoziativ, komm., $\circ$ ist neutral, $M^\times = \{\circ\}$.
e) assoz., komm., es existiert kein neutrales Element.
f) $\cap$, $\cup$ sind assoz., komm.. Neutralelement bzgl. $\cap$: N, bzgl. $\cup$: $\varnothing$. Dies ist jeweils das einzige invertierbare Element. Wie sieht es mit $\setminus$ aus?

Übungsbeispiel 1. Auf $\mathbb{R}$ sei die folgende Verknüpfung $\diamond$ definiert: $x \diamond y := x+3y$. Man überlege sich: $\diamond$ ist weder komm. noch assoz., bzgl. $\diamond$ existiert ein re-neutrales Element, kein li-neutrales Element.

Übungsbeispiel 2. Für $x \in \mathbb{R}$ sei $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$ (die floor-Funktion). Auf $\mathbb{R}$ definiere man $\circ$ durch

$$x \circ y := \lfloor x + y \rfloor$$

Behauptung: $\circ$ ist kommutativ, ist nicht assoziativ. Frage: existiert ein Neutralelement bzgl. $\circ$?

Übungsbeispiel 3. Wie viele verschiedene Operationen gibt es für eine n-elementige Menge ($n \in \mathbb{N}$)? Konvention der Vorlesung: $\mathbb{N} = \{1, 2, 3, \dots\}$
Sei M eine Menge mit drei Elementen. Wie viele verschiedene mögliche Verknüpfungen gibt es auf M?
Wieviele davon besitzen ein fix vorgegebenes Element von M als neutrales Element? Wieviele sind kommutativ? (Tipp: man benutze die Verknüpfungstafel.)

Lemma 1.2. *Sei $(M, *)$ ein Verknüpfungsgebilde.*

a) *Ist $e_1 \in M$ li-neutral und $e_2 \in M$ re-neutral, so ist $e_1 = e_2$ und $e_1 = e_2$ ist neutral. Insbesondere gibt es höchstens ein neutrales Element.*
b) *Ist $*$ assoziativ und hat $(M, *)$ ein neutrales Element $e \in M$, so besitzt jedes invertierbare Element genau ein Inverses und die Menge $M^\times$ ist abgeschlossen unter $*$ (d.h. $(M^\times, *)$ ist Verknüpfungsgebilde).*

Beweis. a) $e_1 \overset{e_2\text{re-neutral}}{=} e_1 * e_2 \overset{e_1\text{li-neutral}}{=} e_2$ ist li- und re-neutral.
b) Seien a' und a'' Inverse zu a. Dann ist

$$a' = a' * e = a' * (a * a'') \overset{*\text{assoz.}}{=} (a' * a) * a'' = e * a'' = a''$$

Zur Abgeschlossheit: seien $x, y \in M^\times$ mit Inversen x' und y'. Zu zeigen ist, dass $x * y$ auch in $M^\times$ liegt. Wir tun das, indem wir zeigen, dass $y' * x'$ invers zu $x * y$ ist, d.h., dass $x * y$ auch invertierbar ist.

Es ist dann

$$(x * y) * (y' * x') \overset{*\text{assoz.}}{=} x * (y * y') * x' = x * x' = e$$

Analog sieht man, dass $(y' * x') * (x * y) = e$ ist. □

Definition 1.2. Sei $(M, *)$ ein Verknüpfungsgebilde, $n \in \mathbb{N}$, $a_1, \dots, a_n \in M$. Man definiert $\ast_{i=1}^n a_i$ rekursiv durch

$$\ast_{i=1}^1 a_i = a_1,$$
$$\text{und für } \quad 1 < k \leq n: \quad \ast_{i=1}^k a_i = (\ast_{i=1}^{k-1} a_i) * a_k = (\cdots((a_1 * a_2) * a_3) * a_4 \cdots) * a_k$$

Ist $e \in M$ ein neutrales Element bzgl. $*$, so definiert man

$$\ast_{i=1}^0 a_i = e$$

Statt $\ast_{i=1}^n a_i$ schreibt man auch $\prod_{i=1}^n a_i$ falls $* = \cdot$ und $\sum_{i=1}^n a_i$ falls $* = +$.

(Achtung: Reihenfolge der Klammern spielt eine Rolle!)

[Vorlesung 2, 6.3.2014]

Bemerkung. Hat M mindestens 3 Elemente, so kann "die Berechnung" auf verschiedene Arten erfolgen (verschiedene Klammerungen bzw. verschiedene Reihenfolge der Auswertung von $*$):

$$(a_1 * a_2) * a_3 \overset{\text{i.A.}}{\neq} a_1 * (a_2 * a_3)$$

Lemma 1.3. *Sei $(M, *)$ ein assoz. Gruppoid, $2 \leq n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{N}$. Dann gilt:*

a) *Allgemeines Assoziativgesetz: Der Ausdruck "$a_1 * a_2 * \cdots * a_n$" ist unabhängig von der Reihenfolge der Auswertungen der Operation.*
b) *Allgem. Kommutativgesetz: Ist $*$ zudem kommutativ, so ist $a_1 * \cdots * a_n$ unabhängig von der Reihenfolge der a_i (d.h. für jede Permutation $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ ist $a_1 * \cdots * a_n = a_{\sigma 1} * \cdots * a_{\sigma n}$).*

Beweis. (a) Mit vollständiger Induktion nach $n \geq 2$ zeigt man, dass jede beliebige Reihenfolge der Operationsauswertung für $a_1 * \cdots * a_n$ dasselbe Ergebnis wie $\ast_{i=1}^{n} a_i$ liefert.
$n = 2$: nur 1 Möglichkeit
($n = 3$: Assoziativität, Voraussetzung)
$n - 1 \rightsquigarrow n$ ($n \geq 3$):
Sei eine beliebige Reihenfolge für die Auswertung von $a_1 * \cdots * a_n$ gegeben. Es existiert ein Index $j \in \{1, 2, \ldots, n-1\}$, so dass die erste Operation in der Klammerung die von a_j mit a_{j+1} ist, setzen $b := a_j * a_{j+1}$:

$$a_1 * \cdots * \overbrace{a_j * a_{j+1}}^{\text{erste Operation},b} * \cdots * a_n$$

Also ist

$$\begin{aligned} \underbrace{a_1 * \cdots * a_n}_{\text{geg. Reihenfolge}} &= \underbrace{a_1 * \cdots * a_{j-1} * b * a_{j+2} * \cdots * a_n}_{n-1 \text{ Operanden}} \\ &\overset{\text{I.V.:Reihenfolge wählbar}}{=} (((\ast_{i=1}^{j-1} a_i) * b) * a_{j+2}) * \cdots * a_n \\ &= ((\ast_{i=1}^{j+1} a_i) * a_{j+2}) * \cdots * a_n = \ast_{i=1}^{n} a_i \end{aligned}$$

b) Mit vollst. Induktion nach $n \geq 2$.
$n = 2$ klar (kommutativ - es gibt nur eine nicht-triviale Permuation von $\{1, 2\}$)
$(n-1) \rightsquigarrow n$: Sei σ eine beliebige vorgegebene Permutation von $\{1, 2, \ldots, n\}$. Sei $j \in \{1, \ldots, n\}$ der Index mit $\sigma(j) = n$.

$$\begin{aligned} a_{\sigma 1} * \cdots * a_{\sigma n} &= (\underbrace{a_{\sigma 1} * \cdots * a_{\sigma(j-1)}}_{=:A} * a_n) * (\underbrace{a_{\sigma(j+1)} * \cdots * a_{\sigma(n)}}_{=:B}) \\ &\overset{* \text{ kommut.}}{=} B * A * a_n \end{aligned}$$

Man überlege sich, dass das in den Fällen $j = 1$ und $j = n$ auch funktioniert (dann wird A nicht definiert bzw. B nicht definiert).

Nun definiert man zu σ eine Permutation σ' der Elemente $\{1, \dots, n-1\}$ wie folgt:

$$\sigma' : \{1, \dots, n-1\} \to \{1, \dots, n-1\}, \quad \sigma'(i) := \begin{cases} \sigma(i) & 1 \leq i \leq j-1 \\ \sigma(i+1) & j \leq i \leq n-1 \end{cases}$$

Das ist eine Permutation von $\{1, \dots, n-1\}$, da $\sigma(i)$ für $i \neq j$ nie $= n$ ist.

Damit erhält man

$$\begin{aligned} B * A * a_n &= \big(\underbrace{a_{\sigma'(j)} * \cdots * a_{\sigma'(n-1)}}_{B} * \underbrace{a_{\sigma'(1)} * \cdots * a_{\sigma'(j-1)}}_{A}\big) * a_n \\ &\overset{\text{Ind. Vor.}}{=} a_1 * \cdots * a_{n-1} * a_n \end{aligned}$$

□

Übungsbeispiel 4. Sei $*$ eine Operation auf der Menge $M \neq \varnothing$, seien a_1, a_2, a_3, $a_4 \in M$.
Behauptung: es gibt 6 verschiedene Reihenfolgen, in denen die Operation zur Berechnung von $a_1 * a_2 * a_3 * a_4$ durchgeführt werden kann, aber nur 5 verschiedene Klammerungen für den Ausdruck.

1.2. **Produkte und Homomorphismen.**

Definition 1.3. Sei $I \neq \varnothing$ eine (Index-)Menge und $(M_i = (M_i, *_i))_{i \in I}$ eine Familie von Verknüpfungsgebilden. Dann definiert man auf der Produktmenge

$$M := \prod_{i \in I} M_i$$

eine Operation $*$ (*komponentenweise Verknüpfung*) folgendermassen: ist $a = (a_i)_{i \in I} \in M$ und $b = (b_i)_{i \in I} \in M$, so ist

$$a * b := (a_i *_i b_i)_{i \in I}$$

$(M, *)$ heisst dann das (*äussere*) *direkte Produkt* der Familie $(M_i)_{i \in I}$. Ist insbesondere $I = \{1, 2, \dots, n\}$ für ein $n \in \mathbb{N}$, so ist

$$\begin{aligned} M &= M_1 \times \cdots \times M_n \\ a * b &= (a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n) \end{aligned}$$

Bemerkung.
- Existiert $\forall i \in I$ ein neutrales Element $e_i \in M_i$ bzgl. $*_i$, so ist $e := (e_i)_{i \in I}$ Neutralelement in M bzgl. $*$. Analog für invertierbare Elemente.
- Ist $*_i$ assoziativ (kommutativ) $\forall i \in I$, so ist auch $*$ assoziativ (kommutativ).

Beispiel. $(\mathbb{R}^n, +)$ ist das direkte Produkt der Familie $(M_i = (\mathbb{R}, +))_{1 \leq i \leq n}$.

Übungsbeispiel 5. Wählen Sie drei verschiedene konkrete Verknüpfungsgebilde und bilden Sie deren direktes Produkt. Wie sieht die komponentenweise Verknüpfung in Ihrem konkreten Beispiel aus?

[Vorlesung 3, 13.3.2014]

Definition 1.4. $(M, *)$ und $(N, \circ)$ seien Verknüpfungsgebilde. Eine Abbildung $\varphi : M \to N$ heisst *Homomorphismus*, falls für alle $x, y \in M$ gilt:

$$\varphi(x * y) = \varphi(x) \circ \varphi(y)$$

$\varphi : M \to N$ ist ein $\left\{ \begin{array}{l} Monomorphismus \\ Epimorphismus \\ Isomorphismus \end{array} \right\}$, wenn $\varphi \left\{ \begin{array}{l} \text{injektiv} \\ \text{surjektiv} \\ \text{bijektiv} \end{array} \right\}$ ist.

M und N heissen zueinander *isomorph*, $M \cong N$, falls es einen Isomorphismus $\varphi : M \to N$ gibt.

Beispiel. $(\{\triangle, \square, \circ\}, *) \cong (\{0, 3, 4\}, \max) \cong (\{1, 2, 3\}, \min)$ unter den Zuordnungen

$$\begin{array}{ccccc} \circ & \longleftrightarrow & 0 & \longleftrightarrow & 3 \\ \triangle & \longleftrightarrow & 3 & \longleftrightarrow & 2 \\ \square & \longleftrightarrow & 4 & \longleftrightarrow & 1 \end{array}$$

Übungsbeispiel 6. Welche "konkreten" Beispiel von Homomorphismen haben Sie bis jetzt im Studium kennen gelernt? Geben Sie die entsprechenden Verknüpfungsgebilde an (M und $*$).

Übungsbeispiel 7. Auf $\mathbb{R}$ seien $\wedge$ und $\vee$ definiert durch

$$\begin{aligned} x \wedge y &:= \min\{x, y\} \\ x \vee y &:= \max\{x, y\} \end{aligned}$$

Zu zeigen: Die Abbildung $\mu : \mathbb{R} \to \mathbb{R}$, $\mu(x) = -x$ ist ein Isomorphismus $(\mathbb{R}, \wedge) \to (\mathbb{R}, \vee)$.
Frage: Ist die Umkehrabbildung μ^{-1} ein Isomorphismus $(\mathbb{R}, \vee) \to (\mathbb{R}, \wedge)$?

Satz 1.4. *Seien $(M, *)$ und $(N, \circ)$ Verknüpfungsgebilde, sei $\varphi : M \to N$ ein Homomorphismus.*

a) *Ist φ ein Epimorphismus, so gilt:*
   (i) *Ist $*$ assoziativ (kommut.), so ist auch $\circ$ assoz. (komm.)*
   (ii) *Ist $e \in M$ Neutralelement bzgl. $*$, so ist $\varphi(e)$ Neutralelement in N bzgl. $\circ$.*

b) *Seien $e \in M$, $f \in N$ neutrale Elemente bzgl. $*$ resp. bzgl. $\circ$, sei $\varphi(e) = f$. Dann gilt $\forall a \in M$: Ist $a' \in M$ invers zu a bzgl. $*$, so ist $\varphi(a')$ invers zu $\varphi(a)$ bzgl. $\circ$.*
   (M.a.W.: ist $a \in M^\times$, so ist $\varphi(a) \in N^\times$).

c) *Ist $f \in N$ neutrales Element und $\varphi^{-1}(f) := \{b \in M \mid \varphi(b) = f\} \neq \varnothing$, so ist φ^{-1} ein Teilmagma von $(M, *)$.*

Beweis. a) $\varphi : M \to N$ ist surjektiv. Seien $x, y, z \in N$ beliebig. Man wählt $a, b, c \in M$ mit $\varphi(a) = x$, $\varphi(b) = y$ und $\varphi(c) = z$. Die tun's:

(i) $*$ sei assoz.

$$\begin{array}{rcl} (x \circ y) \circ y & = & (\varphi(a) \circ \varphi(b)) \circ \varphi(c) \overset{\varphi \text{ Homomorph.}}{=} \varphi(a * b) \circ \varphi(c) \\ & \overset{\varphi \text{ Homom.}}{=} & \varphi((a * b) * c) \overset{\text{assoz. in } M}{=} \varphi(a * (b * c)) \overset{\varphi \text{ Homom.}}{=} \varphi(a) \circ \varphi(b * c) \\ & \overset{\varphi \text{ Homom.}}{=} & \varphi(a) \circ (\varphi(b) \circ \varphi(c)) = x \circ (y \circ z). \end{array}$$

analog für die Kommutativität.

(ii) Sei $e \in M$ neutral. Für alle $x \in N$ ist dann

$$\varphi(e) \circ x \overset{\text{surj.}}{=} \varphi(e) \circ \varphi(a) \overset{\varphi \text{ Homom.}}{=} \varphi(e * a) = \varphi(a) = x,$$

analog sieht man $x \circ \varphi(e) = \cdots = x$.

b) Seien $\varphi(e) = f$, e, f neutral in M bzw. in N. Seien $a * a' = e = a' * a$ für a, $a' \in M$. Dann gilt

$$\begin{array}{rcl} f = \varphi(e) & = & \varphi(a * a') = \varphi(a) \circ \varphi(a') \\ \text{und} \quad \varphi(e) & = & \varphi(a' * a) = \varphi(a') \circ \varphi(a) \end{array}$$

und damit hat man die Behauptung.

c) Seien $b, b' \in \varphi^{-1}(f)$. Zu zeigen: $b * b' \in \varphi^{-1}(f)$

$$\begin{array}{rcl} \varphi(b) = f = \varphi(b') & \Longrightarrow & \varphi(b * b') = \varphi(b) \circ \varphi(b') = f \circ f = f \\ & \Longrightarrow & b * b' \in \varphi^{-1}(f) \end{array}$$

□

Beispiel. Ist φ nicht surjektiv, so ist a)ii) im obigen Satz im allgemeinen falsch:

- Sei $\varphi : (\mathbb{Z}, \cdot) \to (\mathbb{Z}, \cdot)$, $n \mapsto 0$ die konstante Abbildung. φ ist ein Homomorphismus, 1 ist neutral in $(\mathbb{Z}, \cdot)$ und $\varphi(1) \neq 1$!
- Sei $\varphi : (\mathbb{R}, \cdot) \to (M_{2,2}(\mathbb{R}), \cdot)$, $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$.
  Auch hier ist $\varphi(1)$ nicht das Neutralelement vom (zweiten) Verknüpfungsgebilde, $\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Definition 1.5 (Strukturtransport)**.** Sei $(M, *)$ ein Verknüpfungsgebilde.

a) Sei N Menge, $\varphi : N \to M$ bijektiv. Definiert man für beliebige $n, n' \in N$

$$n \circ n' := \varphi^{-1}(\varphi(n) * \varphi(n'))$$

so ist $\circ$ eine Operation auf N und

$$\varphi : (N, \circ) \to (M, *)$$

ist ein Isomorphismus. Man nennt $\circ$ die *mittels φ von M auf N transportierte Verknüpfung*[1].

b) Sei $X \neq \varnothing$ eine Menge. $\mathrm{Abb}(X, M) := \{f : X \to M\}$ sei die Menge aller Abbildungen von X nach M. Für $f, g \in \mathrm{Abb}(X, M)$ sei

$$f \circledast g : X \to M, \quad x \mapsto f(x) * g(x)$$

Dann definiert $\circledast$ eine Operation auf $\mathrm{Abb}(X, M)$. $\circledast$ heisst die *von M auf $\mathrm{Abb}(X, M)$ übertragene Verknüpfung* (oder die von $*$ *induzierte Verknüpfung auf* $\mathrm{Abb}(X, M)$).

Bemerkung. Zu Definition 1.5 a): Satz 1.4 liefert für "transportierte Verknüpfungen":
Ist $*$ assoziativ (kommut.), so ist auch $\circ$ assoz. (kommut.).
Ist $e \in M$ neutral bzgl. $*$, so ist $\varphi^{-1}(e) \in N$ neutral bzgl. $\circ$; es ist $\varphi^{-1}(M^\times) = N^\times$.
Zu Definition 1.5 b): Ist $*$ assoz. (kommut.), so auch $\circledast$.
Ist $e \in M$ neutral bzgl. $*$, so ist die konstante Abbildung $\mathcal{E} : X \to M$, $x \mapsto e$ neutrales Element von $(\mathrm{Abb}(X, M), \circledast)$.

Übungsbeispiel 8. Sei $(\mathbb{R}, \cdot)$ die übliche Multplikation reeller Zahlen und $\varphi : \mathbb{R} \to \mathbb{R}$ gegeben durch $\varphi(x) = x + 2$. Geben Sie die mittels φ^{-1} von $\mathbb{R}$ auf $\mathbb{R}$ transportierte Verknüpfung $\circ$ and und untersuchen Sie, welche Eigenschaften $\circ$ besitzt.
(Vergleichen Sie mit Aufgabe 4 auf dem ersten Übungszettel).

Übungsbeispiel 9. Überlegen Sie sich, dass die in Analysis und lin.Alg. definierten Rechenoperationen für Funktionen (bzw. von linearen Abbildungen) Beispiele für Übertragung von Verknüpfungen nach Definition 1.5b) sind.

1.3. **Relationen.**

Definition 1.6. Sei $\varnothing \neq M$ eine Menge.
a) Eine (binäre) *Relation* auf M ist eine Teilmenge $\mathcal{R} \subseteq M \times M$. Oft beeichnet man eine Relation $\mathcal{R} \subseteq M \times M$ mit einem Symbol R (oder $\sim$, $\cong$, $=$, $\subseteq$, $|$, $<$, $\geq$, $\equiv$, $\dots$) und schreibt für $x, y \in M$

$$xRy \iff (x, y) \in \mathcal{R}$$

(li: gekürzte Schreibweise). In Worten: "x steht in Relation R zu y".

Beispiel.
- "$<$" auf $\mathbb{R} \times \mathbb{R}$, $\mathcal{R} = \{(x, y) \in \mathbb{R}^2 \mid x < y\}$.
- "teilt" auf $\mathbb{N} \times \mathbb{N}$, $\mathcal{R} = \{(m, n) \in \mathbb{N}^2 \mid \ m|n\}$.

Definition (1.6, Forts.). $M \neq \varnothing$ Menge, R Relation auf M.
b) Die Relation R auf M heisst

[1] Hier drei Dinge zu überlegen: die Definition von $\circ$ ist i.O., das ist eine Verknüpfung. Und: dass φ ein Homomorphismus ist: $\varphi(n \circ n') \overset{\text{nach Def.}}{=} \varphi(\varphi^{-1}(\varphi(n) * \varphi(n'))) = \varphi(n) * \varphi(n')$. Dass φ bijektiv ist, ist klar.

(i) *reflexiv*, falls $\forall x \in M$ gilt: xRx (in andern Worten: $(x,x) \in \mathcal{R}\ \forall x \in M$)
(ii) *symmetrisch*, falls $\forall x, y \in M$ gilt: $xRy \Longrightarrow yRx$.
(ii') *antisymmetrisch*, falls $\forall x, y \in M$ gilt: xRy und $yRx \Longrightarrow x = y$
(iii) *transitiv*, falls $\forall x, y, z \in M$ gilt: (xRy und yRz) $\Longrightarrow xRz$.

Eine Relation R auf M heisst *Äquivalenzrelation*, wenn sie reflexiv, symmetrisch und transitiv ist. Sie heisst *Ordnungsrelation* (oder Teilordnung, Halbordnung, partielle Ordnung), wenn sie reflexiv, antisymmetrisch und transitiv ist.

Beispiele von Ordnungsrelationen: $\subseteq$, $\geq$, $|$ (letztere Relation z.B. auf $\mathbb{N}$) (Frage: sind dies "Totalordnungen", i.e. sind je zwei Elemente der entsprechenden Grundmenge vergleichbar?)

[Vorlesung 4, 17.3.2014]

Beispiel.
- Jeder Abbildung $f : M \to M$ lässt sich eine Relation $\mathcal{R}_f := \{(x, f(x) \mid x \in M\}$ zuordnen: $x, y \in M$, $(x,y) \in \mathcal{R}_f \Leftrightarrow y = f(x)$. (i.A. hat $\mathcal{R}_f$ keine der Eigenschaften aus der Definition 1.6b).
  $\mathcal{R}_f$ ist eine linksseitige Relation (d.h. für alle $x \in M$ $\exists!\ y \in M$ mit $(x,y) \in \mathcal{R}_f$). Und jeder linksseitigen Relation $\mathcal{R} \subseteq M \times M$ lässt sich eine Funktion $f_{\mathcal{R}} : M \to M$ zuordnen mit $\mathcal{R} = \mathcal{R}_{f_{\mathcal{R}}}$.
- Jeder Abbildung $f : M \to N$ lässt sich eine Relation $\sim_f$ auf M zuordnen: Für $x_1, x_2 \in M$ sei $x_1 \sim_f x_2 :\Longleftrightarrow f(x_1) = f(x_2)$.
  $\mathcal{R} = \{(x_1, x_2) \in M \times M \mid f(x_1) = f(x_2)\}$.
  Übung: $\sim_f$ ist eine Äquivalenzrelation!

Definition (**1.6**, Forts.). $M \neq \varnothing$ Menge.
c) Sei $\sim$ eine Äquivalenzrelation auf M. Dann heisst für $x \in M$

$$[x]_\sim := \{y \in M \mid x \sim y\}$$

die *Äquivalenzklasse von* x. Jedes $x' \in [x]_\sim$ heisst ein *Repräsentant* dieser Äquivalenzklasse. Die Menge aller Äquivalenzklassen wird mit

$$M/\sim := \{[x]_\sim \mid x \in M\}$$

bezeichnet. Eine Teilmenge $Z \subseteq M$ heisst *Repräsentantensystem für* $\sim$, wenn es zu jeder Äquivalenzklasse $[x]_\sim \in M/\sim$ genau ein $z \in Z$ gibt mit $[x]_\sim = [z]_\sim$.

Übungsbeispiel 10. Auf $\mathbb{N}$ sei die "Teilbarkeitsrelation" gegeben, d.h. a ist in Relation zu b genau dann, wenn a durch b teilbar ist oder b durch a teilbar ist.

Welche Eigenschaften aus Definition 1.6 b) besitzt diese Relation? Ist es eine Äquivalenzrelation, eine Ordnungsrelation?

Übungsbeispiel 11. Auf $\mathbb{N}$ sei die Relation $\square$ gegeben, die folgendermassen definiert ist. Für $a, b \in \mathbb{N}$ ist

$$a \square b \quad \Longleftrightarrow \quad \forall p \in \mathbb{P} \text{ gilt } p \mid a \Leftrightarrow p \mid b$$

(d.h. a und b besitzen die gleichen Primteiler).
Sind $4\square 6$, $4\square 1024$, $6\square 36$, $376\square 1$, $189\square 21$, $1980\square 21$?
Behauptung: a) $\square$ ist eine Äquivalenzrelation auf $\mathbb{N}$.
b) Bis auf eine (welche?) enthält jede Äquivalenzklasse unendlich viele Zahlen.
Wie sieht ein Repräsentantensystem dafür aus?

Übungsbeispiel 12. Sei $\mathbb{R}[x]$ die Menge aller (reellen) Polynomfunktionen und für $f \in \mathbb{R}[x]$ sei $gr(f) \in \mathbb{N}_0 \cup \{-\infty\}$ der Grad von f (das Nullpolynom $f = 0$ hat Grad $-\infty$). Auf $\mathbb{R}[x]$ definiert man Relationen $\sim$, $\preceq$ für $f, g \in \mathbb{R}[x]$ wie folgt:

$$\begin{aligned} f \sim g &:\Leftrightarrow gr(f) = gr(g) \\ f \preceq g &:\Leftrightarrow gr(f) \leq gr(g) \end{aligned}$$

Behauptung: $\sim$ ist Äquivalenzrelation.
Frage: was ist ein Repräsentantensystem dafür?
Welche Eigenschaften von Definition 1.6b) besitzt $\preceq$? Ist $\preceq$ eine Ordnungsrelation?

Satz 1.5. *Sei $M \neq \varnothing$ eine Menge.*

a) *Sei $\sim$ eine Äquivalenzrelation auf M.*
   (i) *Für $x, y \in M$ ist* $\begin{array}{ll} [x]_\sim = [y]_\sim & \Longleftrightarrow \ x \sim y \\ [x]_\sim \cap [y]_\sim = \varnothing & \Longleftrightarrow \ x \not\sim y \end{array}$
   (ii) *Es existieren $z_i \in M$ ($i \in I$, I eine Indexmenge) mit $M = \dot{\bigcup}_{i \in I} [z_i]_\sim$.*

b) *Sei $M = \dot{\bigcup}_{i \in I} A_i$ eine Partition von M in nichtleere Teilmengen A_i. Definiert man für $x, y \in M$*

$$x \sim y :\Longleftrightarrow \exists i \in I : \{x, y\} \subseteq A_i,$$

so ist $\sim$ eine Äquivalenzrelation auf M, und für jedes $x \in A_i$ ist

$$A_i = [x]_\sim$$

Beweis. a)i) Beh.: Für $x, y \in M$ hat man die folgenden Implikationen:
$[x]_\sim \cap [y]_\sim \neq \varnothing \Rightarrow x \sim y \Rightarrow [x]_\sim = [y]_\sim \Rightarrow x \sim y$.
Bew. Beh.: Es sei $z \in [x]_\sim \cap [y]_\sim$.

$$x \sim z \wedge y \sim z \overset{\text{Symmetrie}}{\Rightarrow} x \sim z \wedge z \sim y \overset{\text{Transitivität}}{\Rightarrow} x \sim y$$

Damit ist die erste Implikation gezeigt.
Sei nun $x \sim y$. Dann gilt für jedes $z \in [y]_\sim$: $y \sim z \wedge x \sim y$, woraus $x \sim z$ folgt, d.h. $z \in [x]_\sim$ und somit ist $[y]_\sim \subseteq [x]_\sim$.
Analog folgt für $z \in [x]_\sim$, dass $z \in [y]_\sim$, also ist $[x]_\sim \subseteq [y]_\sim$, d.h. die beiden Äquivalenzklassen sind gleich, die zweite Implikation ist gezeigt.

Für die dritte Implikation: sei $[x]_\sim = [y]_\sim$. Dann ist $y \in [x]_\sim$, also $x \sim y$.
Die Behauptung ist beweisen.

Diese Behauptung liefert $\Leftrightarrow$ im 1. Teil von i) und $\Leftarrow$ im 2. Teil von i)
Es bleibt zu zeigen: $[x]_\sim \cap [y]_\sim = \varnothing \Rightarrow \ x \not\sim y$.
Ersteres impliziert $y \notin [x]_\sim$, damit hat man auch dies gezeigt.

ii) klar. (Benötigt, falls die $M_{i\in I}$ unendlich viele Mengen sind, das Auswahlaxiom. Dieses sagt, kurz formuliert, dass es möglich ist, aus jeder Menge von nichtleeren Mengen ein Element auszusuchen. D.h. es existiert eine Auswahlfunktion, die aus jeder der nichtleeren M_i ein Element aussucht.)

b) Übung (Reflexiv: klar, symm. klar, transitiv auch klar). □

Beispiel. Die Äquivalenzklassen von $\sim_f$ aus dem Beispiel nach Definition 1.6 b) sind genau die nichtleeren Urbildmengen

$$f^{-1}(\{n\}) = \{m \in M \mid f(m) = n\}, \quad \text{für } n \in f(M) \subseteq N$$

2. Elementare Gruppentheorie

2.1. Definitionen, Untergruppen, Nebenklassen.

Definition 2.1. Eine *Gruppe* ist eine Halbgruppe $(G, \cdot)$ mit $G = G^\times$ (d.h. jedes Element ist bzgl. $\cdot$ invertierbar). $(G, \cdot)$ heisst

- *abelsch* (*kommutativ*), falls $\cdot$ kommutativ ist.
- *endlich*, falls $|G| < \infty$ ist.

Bemerkung. a) Ein Verknüpfungsgebilde $(G, *)$ ist genau dann eine Gruppe, wenn gilt:

$$\begin{cases} (G1) & * \text{ ist assoziativ} \\ (G2) & \exists \text{ neutrales Element } e \in G \\ (G3) & \forall\, g \in G\ \exists\, g' \in G \text{ mit } g * g' = g' * g = e. \end{cases}$$

b) Übliche Schreibweise für Gruppen:

multiplikativ	(auch wenn sie nicht abelsch sind)
$\cdot$	für die Operation
e (oder 1 oder ...)	für das neutrale Element
g^{-1}	für das Inverse zu g

Ist $g \in G$, $n \in \mathbb{N}$, so schreibt man $g^n = \underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ mal}}$, $g^0 = 1$

Beispiele. (1) Ist $(G, \cdot)$ eine Halbgruppe, so ist $(G^\times, \cdot)$ eine Gruppe (benutzt Lemma 1.2).

(2) $(2\,\mathbb{N}, \cdot)$ ist assoziatives und kommutatives Verknüpfungsgebilde.
$(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{N}_0 = \mathbb{N} \cup \{0\}, +)$ sind (kommut.) Halbgruppen.
$(\mathbb{Q}_{>0}, \cdot)$, $(\mathbb{Z}, +)$ sind (komm.) Gruppen.
$(\mathbb{Q}, \cdot)$ ist *keine* Gruppe ($0 \cdot ? = 1$).

(3) Es sei $X \neq \varnothing$ eine Menge. Man definiert $\Sigma(X)$ als $\{\varphi : X \to X \mid \varphi \text{ bij.}\}$, $\circ$ sei das Hintereinanderausführen von Abbildungen. Dann ist $(\Sigma(X), \circ)$ eine Gruppe, genannt die *symmetrische Gruppe auf* X:

- $\circ$ ist assoziativ (also (G1) erfüllt)
- $\mathrm{id}_X : X \to X$ ist neutrales Element, da für alle $\varphi \in \Sigma(X)$ gilt: $\varphi \circ \mathrm{id}_X = \mathrm{id}_X \circ \varphi = \varphi$ (damit ist (G2) erfüllt)
- $\forall\, \varphi \in \Sigma(X)$ ist $\varphi^{-1} : X \to X$ Inverses zu φ bzgl. $\circ$ (also ist (G3) ok).

Bemerkung: Die symmetrische Gruppe ist für $|X| \geq 3$ nicht abelsch. Dies kann man leicht zeigen:
Behauptung: $(\Sigma(X), \circ)$ ist nicht abelsch für $|X| \geq 3$: Sei $X = \{x_1, x_2, x_3, \dots\}$. Seien φ_1 und φ_2 zwei Elemente von $\Sigma(X)$, die wie folgt die ersten drei Elementen x_1, x_2, x_3 abbilden:

$$\begin{array}{lll} \varphi_1: & x_1 \mapsto x_2 & \\ & x_2 \mapsto x_1 & \\ & x_3 \mapsto x_3 & \\ & \text{Rest beliebig} & \end{array} \qquad \begin{array}{lll} \varphi_2: & x_1 \mapsto x_1 & \\ & x_2 \mapsto x_3 & \\ & x_3 \mapsto x_2 & \\ & \text{Rest bel.} & \end{array}$$

Dann ist

$$(\varphi_2 \circ \varphi_1)(x_1) = x_3 \quad (\varphi_1 \circ \varphi_2)(x_1) = x_2,$$

also $\varphi_1 \circ \varphi_2 \neq \varphi_2 \circ \varphi_1$.

Als Übung überlege man sich, dass für $|X| = 1, 2$ gilt, dass $|\Sigma(X)| = |X|$ und dass $\circ$ in diesen beiden Fällen kommutativ ist.

Ist $X = \{1, 2, \dots, n\}$, so schreibt man für $\Sigma(X)$ meistens S_n (oder Σ_n). Es gilt: Die Gruppe S_n hat $n!$ Elemente. (Warum?)

Satz 2.1. *Ein assoziatives Verknüpfungsgebilde $(G, \cdot)$ ist eine Gruppe*
$\iff$ *es gilt* $\forall\ g, h \in G$ $\begin{cases} (i) & \exists!\ x \in G \quad mit \quad g \cdot x = h \\ (ii) & \exists!\ y \in G \quad mit \quad y \cdot g = h \end{cases}$

Beweis. $\Longrightarrow$: G sei Gruppe, $g, h \in G$ beliebig. Man zeigt: $x := g^{-1}h$ ist das einzige Element von G mit $gx = h$.

Annahme, es existiert ein $x' \in G$ mit $gx' = h$. Dann folgt

$$\begin{array}{rll} & gx = h = gx' & \mid \quad g^{-1} \cdot (\dots) \\ \Rightarrow & x = g^{-1}gx = g^{-1}h = g^{-1}gx' = x' & \text{also gilt i)} \end{array}$$

ii) zeigt man analog, mit $y := hg^{-1}$.

$\Longleftarrow$: Zu $g_0 \in G$ fest existiert $e \in G$ mit $eg_0 = g_0$ (nach ii), mit $g = g_0$ und $h = g_0$). Für beliebiges $g \in G$ gilt dann (wenn man i) benutzt mit $g = g_0$ und $h = g$): es existiert h mit $g_0 \cdot h = g$.

$$\Rightarrow \quad e \cdot g \overset{g_0h=g}{=} eg_0h \overset{eg_0=g_0}{=} g_0h = g,$$

also ist e links-neutral. Analog zeigt man: es existiert e', das re-neutral ist. Dann folgt mit Lemma 1.2 a), dass $e = e'$ ist und dass das neutral ist. Also ist (G2) erfüllt. Wir brauchen noch die Existenz von Inversen (da $*$ nach Voraussetzung assoziativ ist, hat man (G1) bereits).

Nach i) gilt: für jedes $g \in G$ existiert $g' \in G$ mit $gg' = e$. Daher:

$g = e \cdot g = gg'g = g(g'g)$
$\overset{i)}{\Rightarrow} x = g'g$ ist die (einzige!) Lösung von $g = gx$ (i) mit $g = g_0$, $h = g$)
$\Rightarrow\ g'g = e$
$\Rightarrow\ g'$ ist Inverses zu g

□

Übungsbeispiel 13. Wie findet man in der Verknüpfungstafel einer Gruppe das neutrale Element? Was bedeutet Satz 2.1 für die Verknüpfungstafel einer Gruppe? (Tipp: wie oft muss/darf ein Gruppenelement in jeder Zeile/Spalte vorkommen?) Wie erkennt man in der Verknüpfungstafel das Inverse zu einem Gruppenelement? Woran erkennt man, dass die Gruppe abelsch ist?

Definition 2.2. Sei $(G, \cdot)$ eine Gruppe.

a) Eine *Untergruppe* H von G (geschrieben $H \leq G$) ist eine Unterstruktur $(H, \cdot)$ von $(G, \cdot)$, die wieder eine Gruppe ist.
b) Sei $M \subseteq G$, $\mathcal{M} := \{H \mid H \leq G, M \subseteq H\}$ die Menge aller Untergruppen von G, die M enthalten. Dann heisst
$$\langle M \rangle := \bigcap_{H \in \mathcal{M}} H$$
die *von M erzeugte Untergruppe von G*.
c) G heisst *endlich erzeugt*, falls eine endliche Teilmenge $M \subseteq G$ existiert mit $\langle M \rangle = G$.

Bemerkung.
- $\{e\}$ und G sind Untergruppen von G (die *trivialen Untergruppen*) ($\varnothing$ ist kein Verknüpfungsgebilde nach Definition 1.1 a)).
- $\langle M \rangle$ ist eine Untergruppe von G (Satz 2.2 b) unten).
- Ist $M = \{g_1, \ldots, g_n\}$ endlich, so schreibt man auch
$$\langle M \rangle = \langle g_1, \ldots, g_n \rangle$$
Für $M = \varnothing$: es ist $\langle \varnothing \rangle = \{e\} = \langle e \rangle$

Übungsbeispiel 14. Ist eine endliche Gruppe auch endlich erzeugt? Kennen Sie Beispiele von endlich erzeugten Gruppen, die nicht endlich sind?

Übungsbeispiel 15. Geben Sie die von $M_1 := \{3, 1\}$ erzeugte Untergruppe von $(\mathbb{Q}_+, \cdot)$ an. Dabei ist $\mathbb{Q}_+ = \{a \in \mathbb{Q} \mid a > 0\}$. Und geben Sie die von $M_2 := \{10, 12\}$ erzeugte Untergruppe von $(\mathbb{Z}, +)$ an.

[Vorlesung 5, 20.3. 2014]

Satz 2.2. *Sei $(G, \cdot)$ eine Gruppe.*

a) (Untergruppenkriterium) *Für eine Teilmenge $\varnothing \neq H \subseteq G$ gilt:*
$$H \text{ ist Untergruppe von } G \iff \forall g, h \in H \text{ ist } gh^{-1} \in H.$$

b) *Sei $I \neq \varnothing$ eine Indexmenge, für alle $i \in I$ sei $H_i \leq G$ eine Untergruppe. Dann gilt*

$$\bigcap_{i\in I} H_i \leq G \quad \textit{(ist eine Untergruppe von } G\textit{).}$$

c) *Sei $M \subseteq G$. Dann gilt für jede Untergruppe $U \leq G$:*

$$M \subseteq U \iff \langle M\rangle \subseteq U$$

d.h. bzgl. $\subseteq$ ist $\langle M\rangle$ die kleinste Untergruppe von G, die M enthält.

Beweis. a) $\underline{\Longrightarrow}$: Sei $H \leq G$, seien $g, h \in H$ beliebig. Dann ist $h^{-1} \in H$ und $gh^{-1} \in H$.
$\underline{\Longleftarrow}$: Sei $a \in H$ ($H \neq \varnothing$ nach Voraussetzung). Dann ist $e = aa^{-1} \in H$ (man wählt $g = a$ und $h = a$) und $ea^{-1} = a^{-1} \in H$ (hier wählt man $g = e$ und $h = a$).
Ausserdem: sind $a, b \in H$, so ist $b^{-1} \in H$
$\Rightarrow\ a \cdot (b^{-1})^{-1} = a \cdot b \in H$ (man wählt $g = a$, $h = b^{-1}$).
Also ist $(H, \cdot)$ Untergruppe von $(G, \cdot)$.
b) Für alle $i \in I$ ist $e \in H_i$, also folgt $e \in H := \bigcap_{i\in I} H_i$ und insbesondere ist $H \neq \varnothing$. Nun verwendet man Teil a):

$$g, h \in H \Rightarrow \forall i \in I \text{ sind } g,\, h \in H_i \overset{H_i \text{ sind U'Gr.}}{\Rightarrow} gh^{-1} \in H_i\ \forall i \in I$$

Damit ist $gh^{-1} \in H$, also $H \leq G$.
c) Sei $\mathcal{M} := \{H \leq G \mid M \subseteq H\}$. Es ist $G \in \mathcal{M}$, also ist $\mathcal{M} \neq \varnothing$.
$\underline{\Longrightarrow}$: Sei $M \subseteq U \Rightarrow U \in \mathcal{M} \Rightarrow \langle M\rangle \overset{\text{def.}}{=} \bigcap_{H\in\mathcal{M}} H \subseteq U$.
$\underline{\Longleftarrow}$: Sei $\langle M\rangle \subseteq U$. Es gilt $M \subseteq H$ für alle $H \in \mathcal{M}$. Also gilt:

$$M \subseteq \langle M\rangle = \bigcap_{H\in\mathcal{M}} H \overset{\text{Voraussetzung}}{\subseteq} U$$

□

Übungsbeispiel 16. Welche zu Satz 2.2 analogen Ergebnisse für Vektorräume kennen Sie aus der linearen Algebra? (Vektorräume sind abelsche Gruppen, nicht umgekehrt)

Lemma 2.3. *Seien $(G, \cdot)$ eine Gruppe, $H \leq G$ Untergruppe.*

a) *Man definiert für $g, g' \in G$ die Relation $\underset{Hl}{\sim}$ durch*

$$g \underset{Hl}{\sim} g' \quad :\iff g^{-1}g' \in H$$

Dann ist $\underset{Hl}{\sim}$ eine Äquivalenzrelation auf G mit Äquivalenzklassen

$$[g]_{\underset{Hl}{\sim}} = gH = \{gh \mid h \in H\}$$

b) *Analog sei für* $g, g' \in G$ $\underset{Hr}{\sim}$ *definiert durch*

$$g \underset{Hr}{\sim} g' \quad :\Longleftrightarrow \quad g(g')^{-1} \in H$$

Dann ist $\underset{Hr}{\sim}$ *eine Äquivalenzrelation auf* G *mit Äquivalenzklassen*

$$[g]_{\underset{Hr}{\sim}} = Hg = \{hg \mid h \in H\}$$

Beweis. Behauptung: $\underset{Hl}{\sim}$ ist Äquivalenzrelation. Seien $g, g', g'' \in G$ beliebig.

(i) (refl.) $e = g^{-1}g \in H \Rightarrow g \underset{Hl}{\sim} g$.

(ii) (symm.) Sei $g \underset{Hl}{\sim} g'$, also $g^{-1}g' \in H \Rightarrow (g^{-1}g')^{-1} = (g')^{-1}g$ und das ist in H (Lemma 1.2 b)), also $g' \underset{Hl}{\sim} g$.

(iii) (trans.) Seien $g \underset{Hl}{\sim} g'$, $g' \underset{Hl}{\sim} g''$, also $g^{-1}g' \in H$, $(g')^{-1}g'' \in H$.
Damit ist $(g^{-1}\underbrace{g')((g')^{-1}}_{=e} g'') = g^{-1}g'' \in H \Rightarrow g \underset{Hl}{\sim} g''$.

Für $g' \in G$ gilt:

$$g' \in [g]_{\underset{Hl}{\sim}} \Leftrightarrow g \underset{Hl}{\sim} g' \Leftrightarrow \exists h \in H : g^{-1}g' = h \Leftrightarrow \exists h \in H : g' = gh \Leftrightarrow g' \in gH$$

□

Definition 2.3. Sei $(G, \cdot)$ eine Gruppe, $H \leq G$ eine Untergruppe.
a) Für $g \in G$ heisst die Äquivalenzklasse $[g]_{\underset{Hl}{\sim}} = g \cdot H$ die *durch* g *bestimmte Linksnebenklasse von* G *nach* H. Jedes $g' \in [g]_{\underset{Hl}{\sim}}$ heisst ein *Repräsentant* dieser Nebenklasse, $G/H := \{gH \mid g \in G\}$ bezeichnet die Menge aller Linksnebenklassen von G nach H. Eine Teilmenge $R \subset G$ heisst ein *Repräsentantensystem* für G/H (oder *Linkstransversale von* H *in* G), wenn es für jedes $gH \in G/H$ genau ein $r \in R$ gibt mit $gH = rH$; es ist also

$$G = \dot{\bigcup}_{r \in R} rH.$$

b) Für $g \in G$ ist $[g]_{\underset{Hr}{\sim}} = Hg$ die *durch* g *bestimmte Rechtsnebenklasse von* G *nach* H, jedes $g' \in [g]_{\underset{Hr}{\sim}}$ heisst *Repräsentant* dieser Nebenklasse, $H\backslash G := \{Hg \mid g \in G\}$ bezeichnet die Menge aller Rechtsnebenklassen von G nach H. Eine Teilmenge $R \subset G$ heisst ein *Repräsentantensystem* für $H\backslash G$ (oder *Rechtstransversale von* H *in* G), wenn es für jedes $Hg \in H\backslash G$ genau ein $r \in R$ gibt mit $Hg = Hr$; es ist also

$$G = \dot{\bigcup}_{r \in R} Hr.$$

[Vorlesung 6, 24.3. 2014 (Beispiele 2.5 schon in Lektion 5 angeschaut.]

c) Sei $e \in G$ das neutrale Element von $(G, \cdot)$.
$(G : H) := |G/H| \in \mathbb{N} \cup \{\infty\}$ ist der *Index von* H *in* G,
$\mathrm{ord}(G) := (G : \{e\}) = |G|$ ist die *Ordnung* der Gruppe G.

Bemerkung 2.4. Sei $H \leq G$. Man kann zeigen, dass es eine bijektive Abbildung

$$\begin{aligned} \Psi: \quad G/H &\longrightarrow H\backslash G \\ gH &\longmapsto Hg^{-1} \quad \text{gibt.} \end{aligned}$$

(Ausgehend von der bijektiven Abbildung $G \to G$, $g \mapsto g^{-1}$.)
Daher hat man $|G/H| = |H\backslash G|$ und es gilt:
ist R ein Repräsentantensystem für G/H, so ist
$R^{-1} := \{r^{-1} \mid r \in R\}$ ein Repräsentantensystem für $H\backslash G$.

Beispiele 2.5.

- $\{e\} \leq G$: $G/\{e\} = \{\{g\} \mid g \in G\}$, jede Äquivalenzklasse hat genau 1 Element.
- $G \leq G$: $G/G = \{G\}$, ganz G bildet die einzige Äquivalenzklasse.
- $\Sigma_3 \ni \pi = \begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix}$. Es ist $\Sigma_3 = \{\mathrm{id}, \tau_1, \tau_2, \sigma_1, \sigma_2, \sigma_3\}$.

$$\mathrm{id}: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_1: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \tau_2: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_1: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_2: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_3: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Sei $U := \langle \sigma_1 \rangle = \{\mathrm{id}, \sigma_1\}$, $\sigma_1 \circ \sigma_1 = \mathrm{id}$. Es ist (nachrechnen)

$$\begin{aligned} \sigma_2 U &= \{\sigma_2, \sigma_2 \circ \sigma_1\} = \{\sigma_2, \tau_2\} \\ U\sigma_2 &= \{\sigma_2, \sigma_1 \circ \sigma_2\} = \{\sigma_2, \tau_1\} \end{aligned}$$

und

$$\begin{aligned} \sigma_3 U &= \{\sigma_3, \sigma_3 \circ \sigma_1\} = \{\sigma_3, \tau_1\} \\ U\sigma_3 &= \{\sigma_3, \sigma_1 \circ \sigma_3\} = \{\sigma_3, \tau_2\} \end{aligned}$$

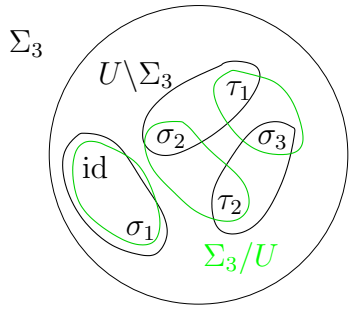
sowie

$$\begin{aligned} \tau_2 U &= \{\tau_2, \tau_2 \circ \sigma_1\} = \{\tau_2, \sigma_2\} \\ U\tau_2 &= \{\tau_2, \sigma_1 \circ \tau_2\} = \{\tau_2, \sigma_3\} \end{aligned}$$

$R := \{\mathrm{id}, \sigma_2, \sigma_3\}$ ist Repräsentantensystem für Σ_3/U und für $U\backslash\Sigma_3$,
d.h. $\Sigma_3 = \dot{\bigcup}_{\pi \in R} \pi U$ und $\Sigma_3 = \dot{\bigcup}_{\pi \in R} U\pi$

$R' := \{\mathrm{id}, \sigma_2, \tau_2\}$ ist Repräsentantensystem für $U\backslash\Sigma_3$ **nicht** für Σ_3/U
also $\Sigma_3 = \dot{\bigcup}_{\pi \in R'} U\pi$

(Man beachte: $R = R^{-1}$, sowie $(R')^{-1} \neq R'$! Das soll mit der Bemerkung 2.4 verglichen werden.)



- Ist $H \leq G$ U'Gruppe, so besitzt jede Re-/Li-Nebenklasse aH bzw. Ha "genausoviele" Elemente wie H. (Übung: $H \to aH$, $h \mapsto ah$, ist bijektiv.)

Übungsbeispiel 17. Zeigen Sie: Ist $(G, \cdot)$ abelsche Gruppe, $H \leq G$ U'Gruppe, so ist für jedes $g \in G$ $gH = Hg$.
Stimmen dann auch die Äquivalenzrelationen $\underset{Hl}{\sim}$ und $\underset{Hr}{\sim}$ überein, d.h. gilt $G/H = H\backslash G$?

Übungsbeispiel 18. $(G, \cdot)$ sei Gruppe, $H \leq G$ mit $(G : H) = 2$. Man zeige, dass dann gilt: $G/H = H\backslash G$. (Das benötigt nicht, dass G abelsch ist!)

Übungsbeispiel 19. Sei $G = (\mathbb{R}^2, +)$, H sei ein eindimensionaler UVRaum von $\mathbb{R}^2$.
Zeige: H ist U'Gruppe von G.
Frage: Was sind die Elemente von G/H (explizit)?
Was ist die geometrische Bedeutung der Elemente von G/H?

Satz 2.6 (Satz von Lagrange)**.** *Sei $(G, \cdot)$ eine Gruppe, seien $H_0 \leq H \leq G$ Untergruppen. Dann gilt:*

$$\begin{aligned} (G : H_0) &= (G : H) \cdot (H : H_0) \\ \text{und} \qquad |G| &= (G : H) \cdot |H| \end{aligned}$$

Insbesondere gilt für alle $H \leq G$: $|H| \mid |G|$.

Beweis. Sei R ein Repräsentantensystem für G/H,
S ein Repräsentantensystem für H/H_0. Also hat man

$$G = \dot{\bigcup}_{r \in R} rH, \quad H = \dot{\bigcup}_{s \in S} sH_0 \quad \Longrightarrow G = \dot{\bigcup}_r \dot{\bigcup}_s (rsH_0)$$

Dann ist $R_0 := \{r \cdot s \mid \underbrace{(r, s)}_{\text{paarw. versch.}} \in R \times S\}$ ein Repräsentantensystem[2] für G/H_0.

[2]Dazu muss man sich Folgendes überlegen: ist $r_i s_j H_0 \cap r_k s_l H_0 \neq \varnothing$, mit $r_i, r_k \in R$ und $s_j, s_l \in S$, so existieren $h \in s_j H_0 \subseteq H$ und $\tilde{h} \in s_l H_0 \subseteq H$ mit $r_i h = r_k \tilde{h}$. Also ist $r_i H \cap r_k H \neq \varnothing$. Daher muss $r_i = r_k$ sein (denn beides sind Repräsentanten). Dann multipliziert man $r_i s_j H_0$ und $r_i s_k H_0$ von links mit r_i^{-1} und erhält, dass $s_j H_0 \cap s_l H_0 \neq \varnothing$ ist. Das geht nur, wenn $s_j = s_l$ ist.

$\Longrightarrow (G : H_0) = |R_0| = |R \times S| = |R| \cdot |S| = (G : H) \cdot (H : H_0)$
Der zweite Teil folgt mit $H_0 := \{e\}$. □

2.2. **Ordnung von Gruppenelementen, zyklische Gruppen.**

Definition 2.4. Sei $(G, \cdot)$ eine Gruppe mit Neutralelement e.
a) Für $g \in G$ ist
$\operatorname{ord}(g) := \inf\{n \in \mathbb{N} \mid g^n = e\} \in \mathbb{N} \cup \{\infty\}$ die *Ordnung des Gruppenelements* g ($\inf(\varnothing) = \infty$). $g \in G$ heisst *Torsionselement* von G, wenn $\operatorname{ord}(g) \in \mathbb{N}$ ist (i.e. wenn g endliche Ordnung hat).

b) Für $g \in G$ heisst $\langle g \rangle \leq G$ die *von* g *erzeugte zyklische Untergruppe* von G. G heisst *zyklische Gruppe*, wenn ein $g \in G$ existiert mit $G = \langle g \rangle$.

Übungsbeispiel 20. $(GL_2, \mathbb{R}), \cdot)$ (Matrizenmultiplikation). Was sind die Ordnungen von $A_1 := \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$, $A_2 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $A_3 := A_1 \cdot A_2$? Welche davon sind Torsionselemente?

Beispiele 2.7.
- $\operatorname{ord}(g) = 1 \Leftrightarrow g = e$, $\{e\} = \langle e \rangle$ ist eine zyklische Gruppe.
- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$
- $(G, \cdot) := (\mathbb{Q} \setminus \{0\})$, $\langle 2 \rangle = \{2^k \mid k \in \mathbb{Z}\} = \{\dots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$
- $(\mathbb{C} \setminus \{0\}, \cdot)$, sei $n \in \mathbb{N}$, $r \in \mathbb{R}_{>0}$. Für welche $0 \neq z = r \cdot e^{i\varphi} \in \mathbb{C}$ ist $z^n = 1$?

$$\begin{aligned} z^n = 1 &\Leftrightarrow r^n = 1 \text{ und } n \cdot \varphi \in 2k\pi\,\mathbb{Z} \\ &\Leftrightarrow r = 1 \text{ und } \varphi = \frac{2\pi k}{n} \text{ für } k \in \mathbb{Z} \end{aligned}$$

Setze $\xi_n := e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ die *primitive* n*-te Einheitswurzel*.
$\mu_n := \{e^{\frac{2\pi i k}{n}} \mid 1 \leq k \leq n\}$ ist Lösungsmenge von $z^n = 1$ und $\mu_n = \langle \xi_n \rangle$, $|\mu_n| = n$.

Damit erhält man, dass die Torsionselemente von $(\mathbb{C} \setminus \{0\}, \cdot)$ die folgende Menge ist: $\bigcup_{n \in \mathbb{N}} \mu_n = \{e^{2\pi i r} \mid r \in \mathbb{Q}\}$.

Aber für jedes $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ist $e^{2\pi\alpha}$ **kein** Torsionselement.

Satz 2.8. *Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $e \in G$, sei $g \in G$.*
a) $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.
b) *Ist* $\operatorname{ord}(g) = \infty$*, so ist für alle $k, l \in \mathbb{Z}$ mit $k \neq l$ auch $g^k \neq g^l$ und $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, g^0 = e, g, g^2, \dots\}$ eine unendliche Menge.*
c) *Ist* $\operatorname{ord}(g) = n \in \mathbb{N}$*, so gilt:*
   (i) *für $k, l \in \mathbb{Z}$:* $g^k = g^l \Leftrightarrow n \mid (l - k)$
   insbesondere: $g^l = e \Leftrightarrow n \mid l$.
   (ii) $|\langle g \rangle| = n = \operatorname{ord}(g)$ *und* $\langle g \rangle = \{g, g^2, g^3, \dots, g^n = e\}$.
   (iii) *für $m \in \mathbb{Z}$ ist* $\operatorname{ord}(g^m) = \frac{n}{\operatorname{ggT}(m,n)}$.
d) *Ist G endlich, so gilt* $\operatorname{ord}(g) \mid \operatorname{ord}(G)$.

e) *Ist* $|G| = p \in \mathbb{P}$ *prim, so ist* G *zyklisch und es gilt* $\langle g\rangle = G \Leftrightarrow g \neq e$.
f) *Ist* G *zyklisch, so ist auch jede Untergruppe von* G *zyklisch.*

[Vorlesung 7, 27.3. 2014 (Beweis von a) und b) bereits in Lektion 6.]

Beweis. a) $\subseteq$: Die Menge $\{g^k \mid k \in \mathbb{Z}\}$ ist U'Gruppe von G und g liegt da drin.
$\supseteq$: $\langle g\rangle$ ist U'Gruppe von G, muss daher $g, g^2, g^3, \ldots, e = g^0, g^{-1}, g^{-2}, \ldots$ enthalten.

b) O.E. sei $k < l$, also $l - k \in \mathbb{N}$.

Aus $\operatorname{ord} g = \infty$ folgt $g^{l-k} \neq e$. $\overset{|\cdot g^k}{\Longrightarrow}$ $g^l \neq g^k$ (Kürzungsregel), damit ist $\langle g\rangle$ eine unendliche Menge.

c) i) $\Rightarrow$: Aus $g^k = g^l$ folgt $e = g^{l-k}$.
Division von $l - k$ durch n mit Rest liefert $l - k = 1 \cdot n + r$, $q \in \mathbb{Z}$, $0 \leq r < n$.

$$e = g^{l-k} = g^{nq+r} = (\underbrace{g^n}_{e})^q \cdot g^r = g^r$$

Und daraus folgt (mit $\operatorname{ord}(g) = n$ und $r < n$): der Rest r muss 0 sein, also $n \mid l-k$.
$\Leftarrow$: $n \mid (l - k)$, also $l - k = i \cdot n$ mit $i \in \mathbb{Z}$. Dann ist

$$g^l = g^{k+in} = g^k(\overbrace{g^n}^{e})^i = g^k$$

Der zweite Teil in i) folgt mit $k = 0$.

ii) Aus i) hat man $|\{g, g^2, g^3, \ldots, g^n = e\}| = n$. Mit a) ist z.z.:

$$\{g^k \mid k \in \mathbb{Z}\} = \{g, g^2, g^3, \ldots, g^n = e\}$$

Die Inklusion $\supseteq$ ist klar. Zur Inklusion $\subseteq$: Sei $k \in \mathbb{Z}$, $k = q \cdot n + r$ mit $0 \leq r < n$. Dann ist $g^k = g^r$, also hat man diese Inklusion auch.

iii) Sei $d := \operatorname{ggT}(m, n) \in \mathbb{N}$, $n = d \cdot n'$, $m = d \cdot m'$, also $\operatorname{ggT}(n', m') = 1$. Sei $k := \operatorname{ord}(g^m)$. Es ist zu zeigen: $k = n'$ $(= \frac{n}{d})$.

$$(g^m)^{n'} = (g^m)^{\frac{n}{d}} = (g^n)^{\frac{m}{d}} = e \overset{i)}{\Rightarrow} k \mid n'$$
$$e = (g^m)^k = g^{mk} \overset{i)}{\Rightarrow} n \mid mk,\ n'd \mid dm'k \quad \Rightarrow n' \mid m'k \overset{(**)}{\Rightarrow} n' \mid k$$

$(**)$ benutzt folgende Aussage: sind $a, b \in \mathbb{Z}$ mit $\operatorname{ggT}(a, b) = 1$ und gilt $a \mid bc$, so folgt $a \mid c$.

d) (Mit Satz 2.6:)

$$|\langle g\rangle| \cdot (G : \langle g\rangle) = \operatorname{ord}(G)$$

e) Sei $|G| = p \in \mathbb{P}$. $g \neq e \Leftrightarrow 1 < \operatorname{ord}(g) \mid p \overset{p\in\mathbb{P}}{\Longleftrightarrow} \operatorname{ord}(g) = p \Leftrightarrow \langle g\rangle = G$

f) Sei $G = \langle a\rangle$ zyklisch, sei $U \leq G$. z.z.: U ist zyklisch. $\{e\}$ ist zyklisch, also ist O.E. $\{e\} \subsetneq U$.

Setze $K := \{k \in \mathbb{N} \mid a^k \in U\}$. Da $\{e\} \subseteq U$ existiert $0 \neq j \in \mathbb{Z}$:

$$a^j \in U,\ a^{-j} \in U \quad (U \text{ ist U'Gruppe}) \ \text{ also ist } K \neq \varnothing$$

Damit existiert $m := \min(K) \in \mathbb{N}$.

Behauptung: $U = \langle a^m \rangle$ (also zyklisch).
Die Inklusion $\supseteq$ ist klar. Zur Inklusion $\subseteq$:

Sei $a^j \in U$ beliebig ($j \in \mathbb{Z}$). Division mit Rest: $j : q \cdot m + r$ mit $q \in \mathbb{Z}$, $0 \leq r < m$. Es sind a^j und $(a^m)^q$ in U, also ist mit dem Untergruppenkriterium

$$a^j \cdot (a^{mq})^{-1} = a^{j-mq} = a^r \in U \quad \overset{\text{Def. von } m}{\Longrightarrow} r = 0$$

also $a^j = (a'm)^q \in \langle a^m \rangle$. □

(Zur Illustration von Satz 2.8, insbesondere c) und d), kann man sich $\mathbb{Z}/(12\,\mathbb{Z})$ anschauen.)

Bemerkung. Sei $\operatorname{ord}(g) = n \in \mathbb{N}$. Mit Satz 2.8 c), ii), iii) folgt für $m \in \mathbb{N}$:

$$\langle g \rangle = \langle g^m \rangle \overset{(ii)}{\Longleftrightarrow} \operatorname{ord}(g^m) = n \overset{(iii)}{\Longleftrightarrow} \operatorname{ggT}(m, n) = 1$$

Also ist die Anzahl der Elemente $g \in \langle g \rangle$ mit $\langle h \rangle = \langle g \rangle$ gleich

$$|\{m \in \mathbb{N} \mid 1 \leq m \leq n \ \text{ und } \ \operatorname{ggT}(m, n) = 1\}| = \Phi(n)$$

die sogenannte Euler'sche Phi-Funktion.

Übungsbeispiel 21. Geben Sie die zyklischen Untergruppen $a_i \leq \mathrm{GL}_2(\mathbb{R})$ (für $i = 1, 2, 3$) für die Matrizen aus dem Übungsbeispiel 20 an.

Übungsbeispiel 22. Sei G zyklische Gruppe der Ordnung 10,

$$G = \{a, a^2, a^3, \ldots, a^9, a^{10} = e\} \text{ für ein passendes } \ a \in G.$$

Geben Sie alle Gruppenelemente der Ordnung $1, 2, 5, 10$ an. Zeigen Sie: zu jedem positiven Teiler d von 10 existiert genau eine Untergruppe der Ordnung d.
$d = 1 : \{e\}$. $d = 2 : \{a^5, e\}$, $d = 5 : \{a^2, a^4, a^6, a^8, e\}$, $d = 10 : G$ selbst.

Übungsbeispiel 23. Verallgemeinern Sie Übungsbeispiel 21 und zeigen Sie:
Ist $(G, \cdot)$ zyklisch, $\operatorname{ord}(G) = n$, so besitzt G für jeden positiven Teiler $d \mid n$ genau eine Untergruppe U_1 der Ordnung d und genau eine Untergruppe U_2 mit Index $(G : U_2) = d$.
(Tipp: Wie viele Gruppenelemente besitzt G deren Ordnung d teilt?)

Übungsbeispiel 24. Sei $(G, \cdot)$ abelsch, seien g, h Torsionselemente mit $\operatorname{ord}(g) = m$ und $\operatorname{ord}(h) = n$.
Beh.: gh ist Torsionselement und $\operatorname{ord}(gh) \mid \operatorname{kgV}(m, n)$.
(So: $g^m = h^n = e$, $(g \cdot h)^{mn} = g^{mn} \cdot h^{mn} = (g^m)^n (h^n)^m = e^n e^m = e$.)

Können Sie ein Beispiel angeben, wo $\operatorname{ord}(gh) \neq \operatorname{kgV}(m,n)$ gilt?
$(\mathbb{Z}_6,+)$ mit $g = 2+6\,\mathbb{Z}$, $h = 4+6\,\mathbb{Z}$, $\operatorname{ord}(g) = \operatorname{ord}(h) = 3$, $\operatorname{ord}(g+h) = 1$, $\operatorname{kgV}(g,h) = 3$.
Oder analog das Beispiel mit μ_6, den 6.ten Einheitswurzeln, mit Multiplikation, aus Beispiel 2.7

Bemerkung. Übungsbeispiel 21 zeigt, dass die Aussage von Übungsbeispiel 24 für nicht abelsche Gruppen i.A. falsch ist.

2.3. **Konjugation und Normalteiler.**

Definition 2.5. Sei $(G,\cdot)$ eine Gruppe.

a) Für $a \in G$ heisst die Abbildung $\kappa_a : G \to G$, $g \mapsto aga^{-1}$ die *Konjugation mit dem Elemente* $a \in G$. Zwei Elemente $g,h \in G$ heissen *zueinander konjugiert*, wenn es ein $a \in G$ gibt mit $h = \kappa_a(g) = aga^{-1}$.

"Zueinander konjugiert sein" definiert eine Äquivalenzrelation auf G. Ihre Äquivalenzklassen werden die *Klassen konjugierter Elemente* genannt. Zwei Untergruppen $U,V \leq G$ heissen *zueinander konjugiert*, wenn es ein $a \in G$ gibt mit

$$V = \kappa_a(U) = aUa^{-1} = \{aua^{-1} \mid u \in U\}.$$

Bemerkung.

- "Konjugiert sein" ist eine Äquivalenzrelation:
  Es gilt $g = ege^{-1}$, also ist die Reflexivität erfüllt.
  $h = aga^{-1} \Rightarrow g = (a^{-1})h(a^{-1})^{-1}$, damit ist die Symmetrie gegeben.
  Aus $h = aga^{-1}$ und $k = bhb^{-1}$ folgt $k = b(aga^{-1})b^{-1} = (ba)g(ba)^{-1}$, die Transitivität ist auch erfüllt.
- Aus $e = axa^{-1}$ folgt $a^{-1}\cdot a = x \Rightarrow x = e$, also ist $\{e\}$ die Konjugationsklasse von e.
  Analog: ist G abelsch, so ist für jedes $g \in G$
  $$\kappa_a(g) = aga^{-1} = aa^{-1}g = g, \quad \text{also } \kappa_a = \mathrm{id}.$$
  Damit besteht jede Konjugationsklasse aus nur einem Element.
- Beh.: κ_a ist bijektiv:

Sei $\kappa_a(g) = \kappa_a(h) \Rightarrow aga^{-1} = aha^{-1} \overset{a^{-1}\cdot|\cdots|\cdot a}{\Longrightarrow} g = h$ also ist κ_a injektiv
Sei $x \in G$. Gesucht ist g mit $\kappa_a(g) = x$:
$aga^{-1} = x \implies g = a^{-1}xa$, d.h. $\kappa_a(a^{-1}xa) = x$ also ist κ_a surjektiv
Umkehrabbildung: $(\kappa_a)^{-1} = \kappa_{a^{-1}}$.

- $U \leq G \Longrightarrow aUa^{-1} \leq G$.
- $(\mathrm{GL}_n(\mathbb{R}),\cdot)$, konjugierte Elemente sind "ähnliche" Matrizen, Konjugationsklassen: Jordan'sche Normalform.

Definition (2.5, Forts.). b) Eine Untergruppe $H \leq G$ heisst *Normalteiler von* G, $H \triangleleft G$, wenn für alle $a \in G$ gilt:

$$H = \kappa_a(H)$$

(d.h. H bleibt bei Konjugation mit beliebigem $a \in G$ invariant).

Bemerkung.
- $\{e\}$ und G sind (triviale) Normalteiler von G.
- Ist G abelsch, so ist $\kappa_a = \mathrm{id}$ für jedes $a \in G$, damit ist jede Untergruppe ein Normalteiler.

[Vorlesung 8, 31.3. 2014]

Übungsbeispiel 25. Sei $(G, \cdot)$ abelsch. Man zeige: κ_a ist die Identität für jedes $a \in G$. Wie sehen die Klassen zueinander konjugierter Elemente aus? Warum ist jede Untergruppe von $(G, \cdot)$ ein Normalteiler?

Übungsbeispiel 26. Behauptung: Sind zwei Elemente einer Gruppe zueinander konjugiert, so haben sie dieselbe Ordnung.
Frage: Welche Gruppen besitzen nur eine einzige Klasse konjugierter Elemente?

Satz 2.9. *Sei $(G, \cdot)$ eine Gruppe, $H \leq G$ Untergruppe. Dann sind äquivalent:*

a) $H \triangleleft G$
b) *Für jedes $a \in G$ ist $aH = Ha$.*
c) $H\backslash G = G/H$.
d) *Für alle $a, b \in G$ ist $aH \cdot bH = abH$*
e) $\forall\ a \in G\ \forall\ h \in H$ *ist* $aha^{-1} \in H$.

Beweis. a) $\Rightarrow$ b): Für jedes $a \in G$ ist $H = \kappa_a(H) = aHa^{-1} \overset{|\cdot a}{\Longrightarrow} Ha = aH$.

b) $\Leftrightarrow$ c): Es ist $M \in H\backslash G \Leftrightarrow \exists a \in G$: $M = Ha \overset{aH=Ha}{\Longleftrightarrow} \exists a \in G : M = aH \Leftrightarrow M \in G/H$.

b) $\Rightarrow$ d): $(aH) \cdot (bH) = a \cdot (\underbrace{Hb}_{=bH}) \cdot H = ab\underbrace{HH}_{=H} = abH$.

d) $\Rightarrow$ e): Sei $a \in G$ beliebig. Man benutzt d) mit $b := a^{-1}$:

$$\begin{aligned} & aHa^{-1}H = aa^{-1}H = H \\ \forall\ h \in H : \quad & \underbrace{aha^{-1}}_{\in aHa^{-1}} e = h' \in H \end{aligned}$$

e) $\Rightarrow$ a): Sei $a \in G$ beliebigt. Es ist $aHa^{-1} \subseteq H$. Und für a^{-1} anstelle von a: $a^{-1}Ha \subseteq H \underset{\cdot a|\cdots|\cdot a^{-1}}{\Longrightarrow} H \subseteq aHa^{-1}$.

Damit hat man $\kappa_a(H) = aHa^{-1} = H$. □

Übungsbeispiel 27. Zeigen Sie: ist $(G, \cdot)$ eine Gruppe, $H \leq G$ Untergruppe vom Index $(G : H) = 2$, so ist $H \triangleleft G$. (Tipp: benutze Beispiel 18 und Satz 2.9.)

Definition 2.6 (Bemerkung und Definition)**.** Sie $(G, \cdot)$ eine Gruppe, $N \triangleleft G$ ein Normalteiler von G. Dann wird durch

$$(aN) \cdot (bN) := (ab)N \quad (a, b \in G)$$

eine Operation auf G/N definiert und $(G/N, \cdot)$ ist eine Gruppe mit Neutralelement N $(= eN)$.

$(G/N, \cdot)$ heisst die *Faktorgruppe von G nach N.*

Lemma 2.10 (Restklassen von $\mathbb{Z}$ modulo m)**.** a) *Zu jeder Untergruppe U von $(\mathbb{Z}, +)$ $\exists!$ $m \in \mathbb{N}_0$ mit*

$$U = \langle m \rangle = m \cdot \mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}.$$

b) *Sei $m \in \mathbb{N}$, $U = \langle m \rangle = m \cdot \mathbb{Z}$ (hier ist $m \neq 0$!)*
Für $a, b \in \mathbb{Z}$ sind äquivalent:
(i) $m \mid (b - a)$
(ii) $a + U = b + U$
(iii) *a und b haben unter der "Division durch m mit Rest" den gleichen Rest in $\{0, 1, \ldots, m-1\}$.*

Zu b): Die Nebenklassen von $\mathbb{Z}$ nach $U = \langle m \rangle$ (mit $m \neq 0$) nennt man auch die *Restklassen von $\mathbb{Z}$ modulo m.*
In den Fällen (i)-(ii) sagt man, *a ist zu b kongruent modulo m,*
geschrieben $a \equiv b \mod (m)$.

Beweis. a) Wie in Satz 2.8 f): $(G, \cdot) = (\mathbb{Z}, +) = \langle 1 \rangle$ ist zyklisch.
Ist $U = \{0\} = \langle 0 \rangle$ die triviale Untergruppe, so nimmt man $m = 0$.
Ist $\{0\} \subsetneq U$, so nimmt man $m := \min(U \cap \mathbb{N})$, dies erzeugt U.

b) (i)$\Rightarrow$ (ii): $\exists j \in \mathbb{Z}$: $b - a = j \cdot m$. Daraus folgt: $b = a + jm$, also ist $b \in a + U$, es folgt $b + U = a + U$.
(ii)$\Rightarrow$ (iii): $a \in b + U$, daher existiert $j \in \mathbb{Z}$ mit $a = b + jm$.
Division durch m mit Rest liefert

$$a = q_1 m + r_1, \quad b = q_2 m + r_2 \text{ mit } 0 \leq r_i \leq m-1$$

$$\Longrightarrow q_1 m + r_1 = q_2 m + r_2 + jm$$

$$r_1 - r_2 = \underbrace{(q_2 + j - q_1)}_{\in \mathbb{Z}} \underbrace{m}_{\in \mathbb{N}} \qquad \text{also gilt: } m \mid r_1 - r_2$$

$$\left.\begin{array}{r} 0 \leq r_1 \leq m-1 \\ -(m-1) \leq -r_2 \leq 0 \end{array}\right\} + \quad -(m-1) \leq r_1 - r_2 \leq m-1 \quad \overset{m \mid (r_1 - r_2)}{\Longrightarrow} r_1 - r_2 = 0,$$

d.h. $r_1 = r_2$

(iii)$\Rightarrow$ (i): $a = q_1 m + r$, $b = q_2 m + r$ mit $0 \leq r \leq m-1$.
Dann ist $b - a = (q_2 - q_1)m$.

□

Beispiel 2.11. $m = 7$, $U = \langle 7 \rangle = \{\ldots, -14, -7, 0, 7, 14, 21, \ldots\} \leq \mathbb{Z}$.

$$\mathbb{Z}/U = \{\overline{0} := 0 + U, \overline{1} := 1 + U, \overline{2} = 2 + U, \ldots, \overline{6} = 6 + U$$

Es ist etwa $\overline{2} = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$ die Nebenklasse von 2 (oder von 23 oder von -12) mod 7, das sind alle Zahlen mit "Rest 2" (bei Division durch 7).

$$\overline{4} + \overline{6} = (4 + U) + (6 + U) = 10 + U = 3 + U = \overline{3}$$

$\mathbb{Z}/\langle 7\rangle$ ist bzgl. + eine Gruppe mit 7 Elementen.
Zahlentheoretische Sprache: $4 + 6 = 10 \equiv 3 \mod (7)$.

Übungsbeispiel 28.
- Treffen folgende Relationen zu oder nicht?
  $14 \equiv 39 \mod (5)$, $-14 \equiv 39 \mod (7)$, $-3 \equiv 30 \mod (11)$
- Gilt für $a, b \in \mathbb{Z}$ beliebig, dass $a \equiv b \mod (1)$?
- Wie lässt sich die Eigenschaft, gerade/ungerade zu sein $\mod (2)$ ausdrücken? Welche Zahlen bilden die beiden Restklassen modulo 2?

Übungsbeispiel 29. Beweisen Sie: für $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ beliebig gilt:

$$\begin{array}{l}\text{aus } a \equiv b \mod (m) \\ \text{und } c \equiv d \mod (m)\end{array} \quad \text{folgt} \quad a + c \equiv b + d \mod (m)$$

2.4. **Gruppenhomomorphismen.**

Definition 2.7. Seien $(G, \cdot)$ und $(G', *)$ zwei Gruppen.

a) Ein *Gruppenhomomorphismus* φ von G nach G' ist ein Homomorphismus nach Definition 1.4 (d.h. eine Abbildung, die verträglich mit den Strukturen $\cdot, *$ ist).
Ist φ ein Gruppenhomomorphismus, der ein Mono- (Epi-, Iso-)morphismus ist (nach Definition 1.4), so heisst φ *Gruppen-mono- (-epi-, -iso-) morphismus*.
Existiert ein Gruppenisomorphismus $\varphi : G \to G'$, so heissen G und G' zueinander *isomorph*, geschrieben $G \cong G'$.

Beispiele 2.12.
- Ist $e' \in G'$ neutral, so ist $\varphi : G \to G'$, $g \mapsto e'$ (die konstante Abbildung auf e') ein (Gruppen)Homomorphismus (der *triviale Homomorphismus*).

G' additiv: $e' = 0$	Nullhomomorphismus
G' multiplikativ: $e' = 1$	Einshomomorphismus

- Determinantenfunktion: $n \in \mathbb{N}$, $\det : (\mathrm{GL}_n(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus \{0\})$, $A \mapsto \det(A)$ ist ein Gruppenhomomorphismus (denn $\det(A \cdot B) = \det(A) \cdot \det(B)$).
- Exponentialfunktion $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, $x \mapsto \exp(x)$ ist bijektiv und es ist $\exp(x+y) = \exp(x) \cdot \exp(y)$. Also ist exp ein Gruppenisomorphismus. Die Umkehrfunktion ist $\log : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$, $y \mapsto \log(y)$ ist auch ein Gruppenisomorphismus.
- Allgemein: Ist $\varphi : (G, \cdot) \to (G', *)$ ein Gruppenisomorphismus, so ist auch die Umkehrabbildung $\varphi^{-1} : G' \to G$ ein Gruppenisomorphismus.
- Die Konjugation $\kappa_a : G \to G$ ist ein Gruppenisomorphismus:
  $\kappa_a(g)\kappa_a(h) = aga^{-1}aha^{-1} = agha^{-1} = \kappa_a(gh)$, also ist κ_a ein Homomorphismus.
  Wegen der Bemerkung nach Definition 2.5 ist κ_a bijektiv, mit $(\kappa_a)^{-1} = \kappa_{a^{-1}}$.

- Sind in $G \xrightarrow{\varphi_1} G' \xrightarrow{\varphi_2} G''$ φ_1 und φ_2 Gruppenhomomorphismen, so auch $\varphi_2 \circ \varphi_1 : G \to G''$.

Definition (**2.7**, Forts.). b) Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus und $e' \in G'$ das neutrale Element, so heisst

$$\ker(\varphi) := \varphi^{-1}(\{e'\}) = \{g \in G \mid \varphi(g) = e'\}$$

der *Kern von* φ und

$$\mathrm{im}(\varphi) := \varphi(G) = \{\varphi(g) \mid g \in G\}$$

das *Bild von* φ.

c) Ist $N \triangleleft G$ ein Normalteiler von G, so heisst $\pi : (G, \cdot) \to (G/N, \cdot), g \mapsto gN$ der *(kanonische) Restklassenhomomorphismus* (die *natürliche Projektion*) von G auf die Faktorgruppe von G nach N.

Bemerkung. Sei $N \triangleleft G$, $\pi : G \to G/N$ wie oben. π ist ein Homomorphismus, surjektiv, also Gruppenepimorphismus. Es ist $\ker(\pi) = \{g \in G \mid \pi(g) = N\} = N$. Insbesondere existiert zu jedem Normalteiler $N \triangleleft G$ eine Gruppe G' und ein Gruppenepimorphismus $\varphi : G \to G'$ mit $\ker(\varphi) = N$ (z.B.:) $G' := G/N$, $\varphi = \pi$.

Übungsbeispiel 30. Zeigen Sie: Sind $(G, \cdot)$, $(G', *)$ zwei Gruppen, $\varphi : G \to G'$ ein Gruppenisomorphismus. Dann ist die Umkehrabbildung $\varphi' : G' \to G$ auch ein Gruppenisomorphismus.

Satz 2.13. *Seien $(G, \cdot)$, $(G', *)$ Gruppen, $\varphi : G \to G'$ ein Gruppenhomomorphismus. Dann gilt:*

a) *Ist $e \in G$ bzw. $e' \in G'$ neutrales Element, so gilt $\varphi(e) = e'$.*
b) *Für jedes $g \in G$ ist $\varphi(g^{-1}) = (\varphi(g))^{-1}$.*
c) *Ist $H \leq G$ U'Gruppe, so auch $\varphi(H) \leq \varphi(G)$.*
d) *Ist $H \triangleleft G$ ein Normalteiler, so ist $\varphi(H) \triangleleft \varphi(G) = \mathrm{im}(\varphi)$.*
e) *Ist $H' \leq G'$ (bzw. $H' \triangleleft G'$), so ist $\varphi^{-1}(H') \leq G$ (bzw. $\varphi^{-1}(H') \triangleleft G$).*

[Vorlesung 9, 3.4. 2014]

Beweis. a) $e \cdot e = e \Rightarrow \varphi(e) * \varphi(e) = \varphi(e)$. Aus Satz 2.1 folgt $\exists!\ x \in G'$ mit $\varphi(e) * x = \varphi(e)$ (nämlich gerade $x = e'$) $\Rightarrow \varphi(e) = e'$. (Gruppeneigenschaft! Vgl. mit Satz 1.4 a)ii).)

b) Das folgt aus Satz 1.4 b).

c) Man zeigt $\varphi(H) \leq G'$ (und in $\varphi(G)$ mit dem Untergruppenkriterium (Satz 2.2 a)): Es ist $H \neq \varnothing$, also $\varphi(H) \neq \varnothing$.
Seien $g', h' \in \varphi(H)$. z.z.: $g' * (h')^{-1} \in \varphi(H)$.
Wähle $g, h \in H$ mit $\varphi(g) = g'$ und $\varphi(h) = h'$. Wegen $H \leq G$ ist $gh^{-1} \in H$.

$$\Longrightarrow \varphi(H) \ni \varphi(gh^{-1}) = \varphi(g) * \varphi(h^{-1}) \overset{b)}{=} g' * \varphi(h)^{-1} = g * (h')^{-1}.$$

d) $\varphi(H) \leq G'$, $\varphi(H) \leq \varphi(G)$ (nach c)).
z.z.: $\forall\ g' \in \varphi(G)\ \forall\ h' \in \varphi(H)$: $g' * h' * (g')^{-1} \in \varphi(H)$. Dazu wählt man $g \in G$, $h \in H$ mit $\varphi(g) = g'$ und $\varphi(h) = h'$.
Wegen $H \lhd G$ ist $ghg^{-1} =: h_0 \in H$. Damit:

$$\varphi(H) \ni \varphi(h_0) = \varphi(ghg^{-1}) = \varphi(g) * \varphi(h) * \varphi(g^{-1}) = g' * h' * (g')^{-1}.$$

e) Zur Aussage über Untergruppen: Es seien $g, h \in \varphi^{-1}(H')$.

$$\Rightarrow \varphi(gh^{-1}) = \underbrace{\varphi(g)}_{\in H'} * \underbrace{\varphi(h)^{-1}}_{\in H'} \in H' \Rightarrow gh^{-1} \in \varphi^{-1}(H')$$

Zur Aussage über Normalteiler: Sei $g \in G$, $h \in \varphi^{-1}(H')$:

$$\varphi(ghg^{-1}) = \underbrace{\varphi(g)}_{\in G'} * \underbrace{\varphi(h)}_{\in H'} * \underbrace{\varphi(g)^{-1}}_{\in G'} \in \underset{\text{da } H' \lhd G'}{H'} \Rightarrow ghg^{-1} \in \varphi^{-1}(H')$$

□

Übungsbeispiel 31. $(G, \cdot)$, $(G', *)$ Gruppen, $\varphi : G \to G'$ Gruppenhomomorphismus, $N \lhd G$ Normalteiler.
Behauptung:
Durch $\overline{\varphi}(gN) := \varphi(g)\varphi(N)$ (für $g \in G$) wird ein Gruppenhomomorphismus $\overline{\varphi} : G/N \to \varphi(G)/\varphi(N)$ definiert.
(Dabei ist auch nachzuweisen, dass $\overline{\varphi}$ unabhängig von der Wahl des Repräsentanten g der Restklasse gN ist.)
(Tipp: man benutze Satz 2.13 d).)

Korollar 2.14. *Seien $(G, \cdot)$, $(G', *)$ Gruppen, $e \in G$ Neutralelement, $\varphi : G \to G'$ Gruppenhomomorphismus. Dann gilt:*

a) $\ker(\varphi) \lhd G$.
b) *Ist $g \in G$, $\varphi(g) = g'$, so ist* $\varphi^{-1}(\{g'\}) = g \cdot \ker(\varphi)$.
c) *φ ist Monomorphismus* $\Longleftrightarrow \ker(\varphi) = \{e\}$.

Beweis. a) $\{e'\} \lhd G' \overset{\text{Satz 2.13e)}}{\Longrightarrow} \ker(\varphi) = \varphi^{-1}(\{e'\}) \lhd G$.
b) $\supseteq$: (z.z.: es ist $g \cdot h \in \varphi^{-1}(\{g'\})$ für alle $h \in \ker(\varphi)$).
$\forall\ h \in \ker(\varphi)$:

$$\varphi(g \cdot h) = \varphi(g) * \varphi(h) = g' * e' = g' \Longrightarrow gh \in \varphi^{-1}(\{g'\}).$$

$\subseteq$: Sei $x \in \varphi^{-1}(\{g'\})$: Dann ist natürlich $\varphi(x) = g'$.

$\varphi(g^{-1}x) = \varphi(g)^{-1} * \varphi(x) = (g')^{-1} * g' = e' \Rightarrow g^{-1}x \in \ker(\varphi) \Rightarrow x = g \cdot (g^{-1}x) \in g \cdot \ker(\varphi)$.

c) folgt aus b).

□

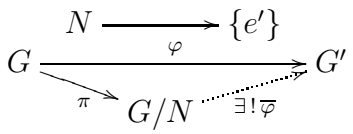
Beispiel 2.15. • $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$:

$$\ker(\det) = \det^{-1}(\{1\}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\} = \mathrm{SL}_n(\mathbb{R}).$$

- V, W $\mathbb{R}$-Vektorräume. Jede $\mathbb{R}$-lineare affine Abbildung $\psi : V \to W$ ist ein Homomorphismus der additiven Gruppen $(V, +)$, $(W, +)$.
  Lineare Algebra: ψ injektive $\Longrightarrow \ker(\psi) = \{0_V\}$. ($0_V$ ist Neutralelement bzgl. $+$ in V).

Übungsbeispiel 32. $(G, \cdot)$, $(G', *)$ zwei Gruppen, $\varphi : G \to G'$ ein Gruppenhomomorphismus, sei $M \subseteq G$, $M' := \varphi(M)$.
Behauptung: es ist $\varphi^{-1}(M') = M \ker(\varphi)$.
Ist die Aussage (bzw. ihr Beweis) auch im Fall $M = \varnothing$ richtig?

Satz 2.16 (Universelle Eigenschaft des Restklassenhomomorphismus)**.** *Sei $(G, \cdot)$ eine Gruppe, $N \triangleleft G$ ein Normalteiler von G, $\pi : G \to G/N$ der Restklassenhomomorphismus.*
Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus (in eine beliebige Gruppe $(G', *)$) mit $\ker(\varphi) \supseteq N$, so existiert genau ein Homomorphismus $\overline{\varphi} : G/N \to G'$ mit $\overline{\varphi} \circ \pi = \varphi$.



Beweis. $\overline{\varphi} \circ \pi = \varphi$ bedeutet folgendes:

$$\forall\ g \in G \text{ ist } \varphi(g) = \overline{\varphi} \circ \pi(g) = \overline{\varphi}(gN)$$

Daher ist die einzige Möglichkeit, $\overline{\varphi}$ mit dieser Eigenschaft zu definieren:

$$\overline{\varphi}(gN) := \varphi(g) \quad \forall gN \in G/N$$

Wegen $gN \subseteq g\ker(\varphi) \overset{\text{Korollar 2.14}}{=} \varphi^{-1}(\varphi(g))$ ist $\overline{\varphi}(gN) = \{\varphi(g)\}$.
Die Definition von $\overline{\varphi}$ ist also unabhängig von der Wahl von g aus der Restklasse gN.

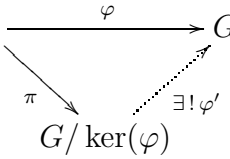
Es bleibt zu zeigen: $\overline{\varphi}$ ist ein Homomorphismus. Seien $gN, hN \in G/H$:

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

und

$$\overline{\varphi}(gN) * \overline{\varphi}(hN) = \varphi(g) * \varphi(h)$$

Die beiden Ausdrücke rechts sind gleich, da φ ein Homomorphismus ist. □

Korollar 2.17. a) *(Homomorphiesatz): Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus und $\pi : G \to G/\ker(\varphi)$ der Restklassenhomomorphismus, so existiert genau ein Gruppenmonomorphismus $\varphi' : G/\ker(\varphi) \to G'$ mit $\varphi' \circ \pi = \varphi$,* 

Insbesondere ist $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

b) *(Klassifikationssatz für zyklische Gruppen) Ist $(G,\cdot)$ zyklisch, so ist*

$$G \cong \begin{cases} (\mathbb{Z},+) & \text{falls } |G| = \infty \\ \mathbb{Z}/n\mathbb{Z} & \text{falls } |G| = n \in \mathbb{N}. \end{cases}$$

Beweis. a) Aus Satz 2.16 mit $N = \ker(\varphi)$ folgt direkt (die Voraussetzung $N \subseteq \ker(\varphi)$ ist erfüllt): es ex. genau ein Gruppenhomomorph. $\varphi' : G/\ker(\varphi) \to G'$ mit $\varphi' \circ \pi = \varphi$. ($\pi$ ist der Restklassenhomom.).

$$\ker(\varphi') = \{\underbrace{g\cdot\ker(\varphi)}_{\in G/\ker(\varphi)} \mid \underbrace{\varphi(g)=e'}_{\Leftrightarrow g\in\ker(\varphi)}\} = \{\quad \underbrace{\ker(\varphi)}_{\text{Neutr.-El. in } G/\ker(\varphi)} \quad\} \overset{\text{Korollar 2.14 c)}}{\Longrightarrow} \varphi' \text{ ist Monom..}$$

Zusatz ("Insbesondere"): ✓

[Vorlesung 10, 7.4. 2014]

b) Sei $G = \langle a\rangle$ zyklisch.

Definiere $\varphi : \mathbb{Z} \longrightarrow G,\ n \longmapsto a^n$, φ ist Gruppenhomomorphismus, epimorph (Satz 2.8a),b))

$$\ker(\varphi) = \{k\in\mathbb{Z} \mid a^k = e = a^0\} = \begin{cases} (\text{Satz } 2.8\, b)) & \{0\} \quad \text{für } |G| = \infty \\ (\text{Satz } 2.8\, c.ii)) & n\mathbb{Z} \quad \text{für } |G| = n \end{cases}$$

$$\Rightarrow G = \operatorname{im}(\varphi) \cong \mathbb{Z}/\ker(\varphi) = \begin{cases} \mathbb{Z}/\{0\} \\ \mathbb{Z}/n\mathbb{Z} \end{cases} \qquad \square$$

Satz 2.18. *Sei G eine Gruppe, $U \le G$ Untergruppe, $N \lhd G$ Normalteiler.*

a) *i) Es ist $UN \le G$ und $U \cap N \lhd U$.*
ii) (1. Isomorphiesatz) Die Abbildung

$$\varphi : U/(U\cap N) \to (UN)/N, \quad a\cdot(U\cap N) \longmapsto aN$$

ist ein Gruppenisomorphismus.

b) *Es sei $H \lhd G$ ein weiterer Normalteiler von G mit $N \subseteq H$.*
i) Dann ist $H/N \lhd G/N$.
ii) (2. Isomorphiesatz) Die Abbildung

$$\psi : G/H \to (G/N)/(H/N)$$

ist ein Gruppenisomorphismus.

Beweis. a) i) Man zeigt $UN \le G$ mit dem Untergruppenkriterium:
– $UN \neq \varnothing$ ✓
– Seien $a,b \in UN$: $a = un$, $b = u'n'$, mit $u,u' \in U$, $n,n' \in N$. Dann ist

$$\begin{aligned} ab^{-1} &= un(u'n')^{-1} = un(n')^{-1}(u')^{-1}. \quad \text{Einschieben von } (u')^{-1}u': \\ &= \underbrace{u\cdot(u')^{-1}}_{\in U}\underbrace{u'\overbrace{n(n')^{-1}}^{\in N}\cdot(u')^{-1}}_{\in N \text{ da } N\lhd G} \in U\cdot N \end{aligned}$$

i)+ii): Definiere

$$\begin{array}{rccccc} \varphi_0: & U & \overset{\iota}{\hookrightarrow} & UN & \overset{\pi}{\longrightarrow} & (UN)/N \\ & u & \mapsto & u & & \\ & & & a & \mapsto & a\cdot N \end{array}$$

ι, π sind Homomorphismen, also ist φ_0 ein Gruppenhomomorphismus.
Wir zeigen: φ_0 ist ein Epimorph., $\ker(\varphi_0) = U \cap N$. Sei $unN \in UN/N$ beliebig gewählt; $unN = uN = \varphi_0(u)$, also ist φ_0 surjektiv.
$\ker(\varphi_0) = \{u \in U \mid \varphi_0(u) = N\} = \{u \in U \mid \underbrace{uN = N}_{\Leftrightarrow u\in N}\} = U \cap N$.
Daher ist also i) $U \cap N \triangleleft U$ (als Kern eines Gruppenhomomorphismus) und ii) $UN/N = \operatorname{im}(\varphi_0) \cong U/\ker\varphi_0 = U/U\cap N$.

b) i) $\pi : G \to G/N$ ist Gruppen-Epimorphismus, $H \triangleleft G$

$$\overset{\text{Satz 2.13d)}}{\Longrightarrow} \quad \underbrace{\pi(H)}_{=H/N} \triangleleft \underbrace{\pi(G)}_{=G/N}$$

ii) Man definiert

$$\begin{array}{rccccc} \psi_0: & G & \overset{\pi}{\longrightarrow} & G/N & \overset{\pi_1}{\longrightarrow} & (G/N)/(H/N) \\ & g & \longmapsto & gN & \longmapsto & \underbrace{gN\cdot(H/N)}_{=\{ghN\mid h\in H\}} \end{array}$$

$$\ker\psi_0 = \underbrace{(\pi_1\circ\pi)^{-1}}_{\pi^{-1}\circ\pi_1^{-1}}(\{\quad \underbrace{H/N}_{\text{Neutralel. in } (G/N)/(H/N)} \quad\}) = \pi^{-1}(\underbrace{\{hN \mid h\in H\}}_{=H/N}) \underset{N\subset H}{=} H$$

Mit Korollar 2.17 a) folgt $\operatorname{im}\psi_0 \cong G/\ker\psi_0$, womit die Behauptung bewiesen ist.

□

Übungsbeispiel 33. Zeigen Sie, dass $\det : \mathrm{GL}_3(\mathbb{R}) \to \mathbb{R}$ ein Gruppenepimorphismus von $(\mathrm{GL}_3(\mathbb{R}), \cdot)$ auf $(\mathbb{R}\setminus\{0\}, \cdot)$ ist.
Wieso ist $H := \det^{-1}(\mathbb{Q}\setminus\{0\}) = \{A \in \mathrm{GL}_3(\mathbb{R}) \mid \det A \in \mathbb{Q}\}$ ein Normalteiler von $\mathrm{GL}_3(\mathbb{R})$? Verwenden Sie den 2. Isomorphiesatz mit $N := \ker(\det)$ und den Homomorphiesatz, um Folgendes zu zeigen:

$$\mathrm{GL}_3(\mathbb{R})/H \cong (\mathbb{R}\setminus\{0\})/(\mathbb{Q}\setminus\{0\})$$

Definition 2.8. Sei $(G, \cdot)$ eine Gruppe.

a) Ein *Automorphismus von* G ist ein Gruppenisomorphismus $\varphi : G \to G$. $\mathrm{Aut}(G)$ bezeichnet die Menge aller Automorphismen von G und

$$\mathrm{Inn}(G) := \{\kappa_a \mid a \in G\}$$

die Menge aller Konjugationen (die *inneren Automorphismen*).

b) $Z(G) := \{z \in G \mid z\cdot g = g\cdot z \ \forall\ g \in G\}$ heisst das *Zentrum der Gruppe* G.

Bemerkung.
- Es ist κ_a bijektiv (Bemerkung nach Def. 2.5), κ_a ist ein Gruppenisomorphismus (Bemerkung nach Definition 2.7). Also: $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$.
- $\{e\} \subseteq Z(G)$.

Satz 2.19. *Sei $(G, \cdot)$ eine Gruppe*

a) *Mit dem Hintereinanderausführen $\circ$ von Abbildungen ist $(\mathrm{Aut}(G), \circ)$ eine Gruppe, die* Automorphismengruppe von G *und $Inn(G) \triangleleft \mathrm{Aut}(G)$.*

b) *$\psi : G \to Inn(G)$, $g \mapsto \kappa_g$ ist ein Gruppenhomomorphismus und $\ker \psi = Z(G)$. Insbesondere: $Z(G)$ ist abelsch und $Z(G) \triangleleft G$.*

Beweis. a) – Seien φ, φ' in $\mathrm{Aut}(G)$. Dann ist $\varphi \circ \varphi'$ ein Homomorphismus, bijektiv, also ein Element von $\mathrm{Aut}(G)$.
- $\mathrm{id}_G \in \mathrm{Aut}(G)$ ist Neutralelement.
- Die Umkehrabbildung φ^{-1} ist Inverses zu φ.
- $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ ✓, es ist $(\kappa_a)^{-1} = \kappa_{a^{-1}}$ und damit hat man: $\kappa_a, \kappa_b \in \mathrm{Inn}(G) \Rightarrow \kappa_a \circ \kappa_b^{-1} = \kappa_a \circ \kappa_{b^{-1}} = \kappa_{ab^{-1}} \in \mathrm{Inn}(G)$, mit dem Untergruppenkriterium ist also $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.
- Für jedes $\varphi \in \mathrm{Aut}(G)$ und $\forall\, x \in G$ ist

$$\varphi \circ \kappa_a \circ \varphi^{-1}(x) = \varphi(a\varphi^{-1}(x)a^{-1}) \overset{\varphi \text{ Homom.}}{=} \varphi(a)\underbrace{\varphi\varphi^{-1}(x)}_{=x}\varphi(a^{-1}) = \kappa_{\varphi(a)}(x),$$

d.h. $\varphi \circ \kappa_a \circ \varphi^{-1} = \kappa_{\varphi(a)} \in \mathrm{Inn}(G)$, also $\triangleleft$ ✓.

b) Ist Übungsaufgabe auf Blatt 5

□

Übungsbeispiel 34. Sei $(G, \cdot)$ eine Gruppe. Zeigen Sie:
Für jeden Automorphismus $\lambda \in \mathrm{Aut}(G)$ gilt: $\lambda(Z(G)) = Z(G)$.

2.5. **Produkte von Gruppen, Struktur endlicher abelscher Gruppen.**

Definition 2.9. Sei $\varnothing \neq I$ eine (Index-)Menge, für jedes $i \in I$ sei $(G_i, *_i)$ eine Gruppe. Dann ist $G := \Pi_{i \in I} G_i$ gemeinsam mit der komponentenweisen Verknüpfung $*$ (vgl. Definition 1.3) wieder eine Gruppe. $(G, *)$ heisst das *äussere direkte Produkt der Familie von Gruppen $(G_i, *_i)_{i \in I}$.*

Bemerkung.
- (vgl. Bemerkung nach Definition 1.3) Für alle $i \in I$ sei $e_i \in G_i$ Neutralelement für $*_i \Rightarrow\ e = (e_i)_{i \in I}$ ist neutral für $*$.
- Beachte: Die $(G_i, *_i)_{i \in I}$ sind gegeben. Die Menge G wird daraus gebildet und zur Gruppe gemacht.

Satz 2.20. *Sei $(G, \cdot)$ eine Gruppe, $r \in \mathbb{N}$, $N_1, N_2, \ldots, N_r \triangleleft G$, sei $N = N_1 \cdots N_r = \{g_1 \cdots g_l \mid g_i \in N_i\}$ das Produkt dieser Normalteiler. Dann gilt*

a) *$N \triangleleft G$ ist ein Normalteiler.*

b) *Die folgenden Aussagen sind äquivalent:*

(i) *Die Abb.* $\varphi : \begin{array}{ccc} N_1 \times \cdots \times N_r & \to & N \\ (g_1, \ldots, g_r) & \mapsto & g_1 \cdots g_r \end{array}$ *ist ein Gruppenisomorph.*

(ii) *Zu jedem* $a \in N$ *existieren eindeutig bestimmte* $g_i \in N_i$ $(1 \leq i \leq r)$ *mit* $a = g_1 \cdots g_r$.

(iii) *Für jedes* $1 \leq i \leq r$ *gilt*

$$N_i \cap (N_1 \cdots N_{i-1} \cdot N_{i+1} \cdots N_r) = \{e\}$$

Beispiel. (Zu b) in Satz 2.20)

- $N_1 := 2\,\mathbb{Z}$ und $N_2 := 3\,\mathbb{Z}$ sind Normalteiler in $\mathbb{Z}$. Es ist $N_1 + N_2 = \mathbb{Z}$ (Operation ist hier additiv). In b.iii): $N_1 \cap (N_2) = 6\,\mathbb{Z} \neq \{0\}$. Und in b.i): die Abbildung $2\,\mathbb{Z} \times 3\,\mathbb{Z} \to \mathbb{Z}$ ist nicht injektiv, $-2 + 3 = 1$ und $10 - 9 = 1$ (damit schlägt auch b.ii) fehl).
- μ_2 μ_3 (die zweiten bzw. die dritten Einheitswurzeln) sind Normalteiler in $\mu_6 = \mu_2 \cdot \mu_3$ (μ_6 sind die 6ten Einheitswurzeln).
  iii) $\mu_2 \cap \mu_3 = \{1\} = \{e\}$ und
  i) $\mu_2 \times \mu_3 \to \mu_6$ ist bijektiv.
  Frage: was ist, wenn man $N_1 := \mu_2$ und $N_2 := \mu_4$ nimmt mit $N := \mu_2 \cdot \mu_4$?

Beweis. a) Für $r = 2$:
Aus Satz 2.18a.i) folgt $N_1 \cdot N_2 \leq G$. Für alle $g \in G$ ist $g(N_1N_2)g^{-1} = gN_1\underbrace{g^{-1}g}_{e}N_2g^{-1} = N_1N_2$, also ist N_1N_2 ein Normalteiler von G.

Nun fährt man fort mit vollständiger Induktion nach r (selber überlegen).

b) $\underline{(i) \Rightarrow (ii)}$: ✓, da φ bijektiv ist.
$\underline{(ii) \Rightarrow (iii)}$: Sei $x \in N_i \cap (N_1 \cdots N_{i-1} \cdot N_{i+1} \cdots N_r)$

$$\overset{ii)}{\Rightarrow} x = e \cdots \underbrace{e}_{\in N_{i-1}} \cdot \overset{\in N_i}{x} \cdot \underbrace{e}_{\in N_{i+1}} \cdots e \overset{!}{=} g_1 \cdots \underbrace{g_{i-1}}_{\in N_{i-1}} \cdot \overset{\in N_i}{e} \cdot \underbrace{g_{i+1}}_{\in N_{i+1}} \cdots g_r$$

$\overset{ii)}{\Longrightarrow}$ alle $g_i = e$ und $x = e$ ✓.
[Vorlesung 11, 10.4. 2014]
$\underline{(iii) \Rightarrow (i)}$: Die Abbildung φ ist definiert.
Behauptung: $\forall\ i, j \in \{1, \ldots, r\}$ mit $i \neq j$ gilt $g_ig_j = g_jg_i$ $\forall\ g_i \in N_i$ und $\forall\ g_j \in N_j$.
Beweis Behauptung:

$$g_ig_j(g_jg_i)^{-1} = \underbrace{\overset{\in N_i}{g_i}}_{\in g_iN_jg_i^{-1} = N_j} \overbrace{g_jg_i^{-1}}^{\in g_jN_ig_j^{-1} = N_i} \underbrace{g_j^{-1}}_{\in N_j} \in N_i \cap N_j \underset{i \neq j}{\subseteq} \underbrace{N_i \cap (N_1 \cdots N_{i-1}N_{i+1} \cdots N_r)}_{=\{e\}}$$

$$\Rightarrow\ e = g_ig_j(g_jg_i)^{-1},\ \text{also } g_ig_j = g_jg_i$$

- φ ist Homom.: Seien $a = (a_1, \ldots, a_r)$, $b = (b_1, \ldots, b_r)$ in $N_1 \times \cdots \times N_r$.

$$\varphi(a)\varphi(b) = a_1 \cdots a_rb_1 \cdots b_r \overset{**}{=} a_1b_1 \cdots a_rb_r = \varphi(a \cdot b)$$

$**$: die b_i können nach obiger Behauptung sukzessive nach links verschoben werden.

- φ ist surjektiv: klar ✓.
- Seien $x = (a_1, \dots, a_r) \in \ker(\varphi)$: $\varphi(x) = a_1 \cdots a_r = e$.
  Dann gilt für beliebiges $1 \le i \le r$:

$$\Rightarrow a_i = a_{i-1}^{-1} \cdots a_1^{-1} a_r^{-1} \cdots a_{i+1}^{-1} \overset{\text{nach obigem}}{=} a_1^{-1} \cdots a_{i-1}^{-1} a_{i+1}^{-1} \cdots a_r^{-1} \in \underbrace{N_i \cap (N_1 \cdots \widehat{N_i} \cdots N_r)}_{=\{e\}}$$

$$\Rightarrow a_j = e \text{ für } j = 1, \dots, r$$

$$\Rightarrow x = (e, e, \dots, e), |\ker(\varphi)| = 1, \quad \text{also ist } \varphi \text{ injektiv.}$$

□

Definition 2.10. Sei $(G, \cdot)$ eine Gruppe, $r \in \mathbb{N}$, $N_1, \dots, N_r \triangleleft G$ und $N = N_1 \cdots N_r = \{g_1 \cdots g_r \mid g_i \in N_i\}$ das Produkt dieser Normalteiler. Sind die äquivalenten Bedingungen von Satz 2.20 b) erfüllt, so heisst N das *(innere) direkte Produkt der Normalteiler* N_i $(1 \le i \le r)$.
Schreibweise: $N = N_1 \cdot \cdots \cdot N_r$ (dir).

Bemerkung. Im Unterschied zu Definition 2.9 wird das Produkt in Definition 2.10 innerhalb der bereits gegebenen Gruppe $(G, \cdot)$ gebildet. Das innere Produkt ist wichtig bei der Strukturuntersuchung einer gegebenen Gruppe G.

Übungsbeispiel 35. Sei $G = \langle a \rangle = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$ zyklische Gruppe der Ordnung 6.
Zeigen Sie: es gilt: $G = \langle a^2 \rangle \cdot \langle a^3 \rangle$ (dir).
(Also wird hier implizit auch behauptet: $\langle a^2 \rangle$ und $\langle a^3 \rangle$ sind Normalteiler von G).
Wieviele Elemente haben die beiden Normalteiler, die G als Produkt darstellen?

Satz 2.21 (Struktursatz für endliche abelsche Gruppen)**.** *Sei G eine endl. ab. Gruppe mit $|G| = n \ge 2$. Dann existieren eindeutig bestimmte Zahlen $r, d_1, \dots, d_r \in \mathbb{N}$ mit*

$$1 < d_1 \mid d_2 \mid \cdots \mid d_r$$

zu denen es (i.a. nicht eind. bestimmte) Elemente $b_i \in G$ gibt mit $\operatorname{ord}(b_i) = d_i$, *s.d.*

$$G = \langle b_1 \rangle \langle b_2 \rangle \cdots \langle b_r \rangle \text{ (dir).} \qquad (d.h.\ n = d_1 \cdots d_r)$$

[Vorlesung : In der Vorlesung wurde nur die Idee des Beweises besprochen.]

Beweis. I. Existenz einer solchen Darstellung
Sei $r \in \mathbb{N}$ minimal derart, dass es $a_1, \dots, a_r \in G$ gibt mit $G = \langle a_1, \dots, a_r \rangle$ gibt.
Wir zeigen: zu diesem r gibt es $d_1, \dots, d_r \in \mathbb{N}$ und $b_1, \dots, b_r \in G$ wie gewünscht.
Benutzen vollständige Induktion nach $r \ge 1$ (da $|G| \ge 2$ ist, ist $r \ge 1$).
Induktionsanfang: $r = 1$. $G = \langle a_1 \rangle$, setze $b_1 := a_1$, $d := \operatorname{ord}(a_1) = n$ ✓.

Induktionsschritt: $(r-1) \rightsquigarrow r$ (≥ 2).
Sei $d_1 \in \mathbb{N}$ minimal mit der folgenden Eigenschaft[3]:

$$(*) \qquad \exists\, a_1, \ldots, a_r \in G \text{ mit } G = \langle a_1, \ldots, a_r \rangle$$
$$\text{und} \quad \exists\, k_2, \ldots, k_r \in \mathbb{Z} \text{ mit } a_1^{d_1} a_2^{k_2} \cdots a_r^{k_r} = e$$

(kann man erreichen)
Beh. 1: Sind $a_1, \ldots, a_r \in G$, $k_2, \ldots, k_r \in \mathbb{Z}$ mit $(*)$, so gilt $d_1 \mid k_i \ \forall\ 2 \leq k \leq r$.
Bew. Beh. 1: Division von k_i durch d_1 mir Rest $(2 \leq i \leq r$ beliebig):
$\exists\, q_i \in \mathbb{Z}$, $t_i \in \mathbb{N}_0$, $0 \leq t_i < d_1$ und $k_i = d_1 q_i + t_i$ $(2 \leq i \leq r)$.
Es gilt[4]: $G = \langle a_1, \ldots, a_r \rangle = \langle a_1 \cdot a_i^{q_i}, a_2, \ldots, a_r \rangle$
$\rightsquigarrow (a_1 a_i^{q_i})^{d_1} \cdot a_2^{k_2} \cdots a_{i-1}^{k_{i-1}} a_i^{t_i} a_{i+1}^{k_{i+1}} \cdots a_r^{k_r} = e$
$a_i^{t_1}$ spielt nun die Rolle von a_1: $\widetilde{a_1}^{t_1} \cdot a_2^{k_2} \cdots a_{i-1}^{k_{i-1}} \tilde{a_i}^{d_i} a_{i+1}^{k_{i+1}} \cdots a_r^{k_r}$ $(\tilde{a_i} = a_1 a_i^{q_i})$.
$\overset{\text{Minimalität von } d_1}{\Longrightarrow} t_i = 0 \Rightarrow d_1 \mid k_i$.
Damit ist Beh. 1 beweisen (denn $2 \leq i \leq r$ war beliebig).
Es seien $a_1, \ldots, a_r \in G$, $k_2, \ldots, k_r \in \mathbb{Z}$ mit $(*)$
$\Rightarrow \forall\ 2 \leq i \leq r$ ist $k_i = d_1 \cdot q_i$ $(q_i \in \mathbb{Z})$.
Setze $b_1 := a_1 a_2^{q_2} \cdots a_r^{q_r}$, dann ist $G = \langle a_1, \ldots, a_r \rangle = \langle b_1, a_2, \ldots, a_r \rangle$ und $b_1^{d_1} = a_1^{d_1} a_2^{k_2} \cdots a_r^{k_r} = e \overset{\text{Minimal. von } d_1}{\Longrightarrow} \operatorname{ord}(b_1) = d_1$.
$(G$ abelsch $\rightsquigarrow \langle b_1 \rangle \triangleleft G) \overset{\langle b_1 \rangle \triangleleft G}{\Longrightarrow} G = \langle b_1 \rangle \cdot \langle a_2, \ldots, a_r \rangle$ Produkt von 2 Normalteilern.
Behauptung: Dieses Produkt ist direkt.

Sei $x \in \langle b_1 \rangle \cap \langle a_2, \ldots, a_r \rangle : x = b_1^{l_1} = a_2^{l_2} \cdots a_r^{l_r}$ mit $l_i \in \mathbb{Z}$, $0 \leq l_1 < d_1$.
$\Longrightarrow b_1^{l_1} a_2^{-l_2} \cdots a_r^{-l_r} = e \overset{\text{Minimal. von } d_1}{\Longrightarrow} l_1 = 0$, also $x = b_1^0 = e$.
$\Longrightarrow G = \langle b_1 \rangle \cdot \langle a_2, \ldots, a_r \rangle$ (dir).
Wende Induktionsvoraussetzung auf $G' := \langle a_2, \ldots, a_r \rangle$ an (nach Konstruktion ist $r-1$ minimale Erzeugerzahl für G').
$\Longrightarrow \exists\ 1 < d_2 \mid d_3 \cdots \mid d_r$, $b_i \in G' \subset G$:
$G' = \langle b_2 \rangle \cdots \langle b_r \rangle$ (dir) und $\operatorname{ord}(b_i) = d_i$.
$\overbrace{b_1^{d_1}}^{\in \langle b_1 \rangle} \overbrace{b_2^{d_2} b_3^0 \cdots b_r^0}^{\in \langle b_2 \rangle} = e \overset{(*), \text{Beh. } 1}{\Longrightarrow} d_1 \mid d_2$, damit folgt die Existenz einer solchen Darstellung.

II. Eindeutigkeit von r, $d_1, \ldots, d_r \in \mathbb{N}$:
Beweis mit vollständiger Induktion nach $n = |G|$:
$n = 2$: $d_1 = 2$, $r = 1$ einzige Möglichkeit.
Induktionsschluss auf n (≥ 3): Sei $G = \langle b_1 \rangle \cdots \langle b_r \rangle$ (dir) $= \langle b_1' \rangle \cdots \langle b_s' \rangle$ (dir).
O.E. ist $s \leq r$. $\operatorname{ord}(b_i) = d_i$, $\operatorname{ord}(b_i') = d_i'$, $n = |G| = d_1 \cdots d_r = d_1' \cdots d_s'$.
Wähle $p \in \mathbb{P}$ mit $p \mid d_1$ $(\Longrightarrow p \mid d_i$ für $i = 2, \ldots, r)$.

[3] Minimalität über alle möglichkeiten r Erzeugenden $a_1, \ldots, a_r$
[4] beide Inklusionen des Gleichheitszeichens rechts für die Erzeugenden zeigen

$G^p := \{g^p \mid g \in G) \leq G$ (da G abelsch ist)
$G^p = \langle b_1\rangle^p \cdots \langle b_r\rangle^p = \langle b_1'\rangle^p \cdots \langle b_r'\rangle^p$.

$$\left.\begin{array}{l} |G^p| = \prod_{i=1}^r \operatorname{ord}(b_i^p) = \prod_{i_1}^r \frac{d_i}{p} = \frac{n}{p^r} \\ |G^p| = \prod_{i=1}^s \operatorname{ord}(b_i'^p) \geq \prod_{i=1}^s \frac{d_i'}{p} = \frac{n}{p^s} \end{array}\right\} \Longrightarrow \frac{n}{p^r} \geq \frac{n}{p^s} \Longrightarrow p^s \geq p^r, s \geq r \overset{s\leq r}{\Longrightarrow} s = r$$

und $\forall\ 1 \leq i \leq r : p \mid d_i'$.
(Dabei ist $\operatorname{ord}(b_i'p) = d_i'$ für $p \nmid d_i'$ und $= \frac{d_i'}{p}$ für $p \mid d_i'$)
Sei $j := \min\{i \mid 1 \leq i \leq r \text{ und } d_i > p\}$ und $j' := \min\{i \mid 1 \leq i \leq r \text{ und } d_i' > p\}$

$$\left.\begin{array}{l} G^p = \langle b_j^p\rangle \cdots \langle b_r^p\rangle = \langle b_{j'}'^p\rangle \cdots \langle b_s'^p\rangle \\ \text{Ordnungen} : \frac{d_j}{p} \mid \cdots \mid \frac{d_r}{p} \quad \frac{d_{j'}'}{p} \mid \cdots \mid \frac{d_s'}{p} \end{array}\right\} \overset{I.V.}{\Longrightarrow} j = j' \text{ und } \forall 1 \leq i < j : d_i = d_i' = p$$

$$\forall j \leq i \leq r : \frac{d_i}{p} = \frac{d_i'}{p} \Rightarrow d_i = d_i'$$

□

Beispiel 2.22. Ist C_n eine zyklische Gruppe der Ordnung n, so ist $C_n = \langle a\rangle \cong (\mathbb{Z}/n\mathbb{Z}, +)$.
Konkret: sei $n = 16$, man finde alle abelschen Gruppen der Ordnung 16 (bis auf Isomorphie): Gesucht sind alle $1 < d_1 \mid d_2 \mid \cdots \mid d_r$ mit $d_1 \cdots d_r = 16$.

$C_2 \cdot C_2 \cdot C_2 \cdot C_2$ (dir)
$C_2 \cdot C_2 \cdot C_4$ (dir)
$C_2 \cdot C_8$ (dir)
$C_4 \cdot C_4$ (dir)
C_{16}

$\rightsquigarrow$ Es existieren 5 paarweise nicht isomorphe abelsche Gruppen der Ordnung 16.

Übungsbeispiel 36. Seien $p_1, p_2, p_3 \in \mathbb{P}$ paarweise verschieden, $n := p_1^3 p_2^2 p_3$. Wieviele verschiedene Möglichkeiten gibt es, für dieses n Werte $r, d_1, \ldots, d_r$ wie in Satz 2.21 zu finden. Gilt immer $r \leq 3$? Warum? Wie kann man diese Aufgabe systematisch angehen? (z.B. ordnen nach r).

3. Grundbegriffe der Ringtheorie

[Vorlesung 12, 12.5. 2014]

3.1. Definitionen, Ideale, Kongruenzen.

Definition 3.1. a) Eine *nichtleere* Menge R mit zwei Verknüpfungen $+$ und $\cdot$, d.h. ein Tripel $(R, +, \cdot)$, heisst *Ring (mit Einselement)*, wenn gilt:
(R1) $(R, +)$ ist eine abelsche Gruppe
(R2) $(R, \cdot)$ ist eine Halbgruppe (mit Neutralelement $1_R \in R$)
(R3) Für alle $x, y, z \in R$ gelten die Distributivgesetze:
$x \cdot (y + z) = x \cdot y + x \cdot z$ und $(y + z) \cdot x = y \cdot x + z \cdot x$.

Mit $R^\times = (R,\cdot)^\times$ bezeichnen wir die Menge der bzgl. $\cdot$ invertierbaren Elemente (die *Einheitengruppe* von R).
Ist $\cdot$ eine kommutative Verknüpfung, so heisst $(R,+,\cdot)$ ein *kommutativer Ring*.

Bemerkung.
- Für einen Ring $(R,+,\cdot)$ schreibt man meist 0 oder 0_R für das Neutralelement bzgl. + ("Null", "Nullelelement"), das neutrale Element bzgl. $\cdot$ wird 1 oder 1_R geschrieben ("Eins", "Einselement").
- Konvention: "Punkt- vor Strichrechnung" gilt: etwa
$$xy^{-1} + xz^n = (x\cdot(y^{-1})) + (x\cdot(z^n)) = x(y^{-1}+z^n)$$
- Erfüllt $(R,+,\cdot)$ die Eigenschaften eines Rings bis auf die Existenz eines Einselements ("Ring ohne Eins"), so kann man zeigen:
$\exists$ Ring R', der R enthält, R' mit Einselement (z.B. Mayberg, Alg. 1, S. 116).
- (R1) und (R2) zusammen sind äquivalent zu folgenden 4 Eigenschaften:
(r1) $(R,+)$ und $(R,\cdot)$ sind assoziative Magmas
(r2) $\exists$ neutrale Elemente bzgl + und $\cdot$ (0 und 1)
(r3) bzgl. + besitzt jedes $x\in R$ ein Inverses, $x+(-x)=(-x)+x=0_R$
(r4) + ist kommutativ
(dabei sind $(R,+)$ und $(R,\cdot)$ wegen (r1) und (r2) Halbgruppen)

Definition (3.1, Forts.). b) Sei $(R,+,\cdot)$ ein Ring. Eine Teilmenge $\varnothing \neq R_0 \subseteq$ heisst *Teilring* oder *Unterring* von R, wenn gilt:
(TR1) $(R_0,+)$ ist Untergruppe von $(R,+)$
(TR2) $(R_0,\cdot)$ ist Teilmagma von $(R,\cdot)$ mit $1_R \in R_0$.
(d.h. R_0 ist mit den auf R_0 eingeschränkten Operationen wieder ein Ring und besitzt dasselbe Einselement wie R).
Ist R_0 ein Unterring von R, so heisst R *Oberring* oder *Erweiterungsring* von R_0.

Beispiele.
- $(\mathbb{C},+,\cdot)$ ist ein kommutativer Ring. Unterringe: $\mathbb{R}\supset\mathbb{Q}\supset\mathbb{Z}$.
- Ist R ein beliebiger Ring, $n\in\mathbb{N}$, so sei
$M_{n,n}(R) := \{n\times n - \text{Matrizen aus Elementen aus } R\}$. Zusammen mit der Addition und Multiplikation von Matrizen ist $M_{n,n}(R)$ ein Ring.
- Sei R ein beliebiger Ring, $\varnothing \neq X$ eine Menge:
zusammen mit den Verknüpfungen von R (wie in Definition 1.5 b)) ist $\mathrm{Abb}(X,R) := \{f : X\to R\}$ ein Ring.

Übungsbeispiel 37. Es sei $(R,+,\cdot)$ ein Ring und seien $a,r\in R$. Geben Sie die folgenden Ringelemente b,c mit Hilfe von Vielfachen- und Potenzschreibweise in einfacherer Form an:
$$b = a\cdot a + a\cdot a + a\cdot a,\quad c = a\cdot a\cdot a + a\cdot a\cdot a$$
Können Sie das Element $b+c$ mit Hilfe des Distributivgesetzes weiter vereinfachen? Wieso sind (im Allgemeinen) die Ringelemente $a\cdot r\cdot a$, $a^2\cdot r$ und $r\cdot a^2$ verschieden? (Können Sie spezielle Beispiele dafür angeben, etwa mit $R = M_{2,2}(R)$?)

Übungsbeispiel 38. Zeigen Sie, dass $\mathrm{Abb}(\mathbb{R},\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$ mit den gemäss Definition 1.5b) von $\mathbb{R}$ übertragenden Verknüpfungen $+$ und $\cdot$ einen kommutativen Ring bildet. Geben Sie sein Einselement an, und beschreiben Sie seine Einheitengruppe.

Satz 3.1 (Rechenregeln für Ringe)**.** *Sei $(R,+,\cdot)$ ein Ring mit Nullelement $0_R \in R$. Dann gilt für beliebige $a,b \in R$:*
a) $a \cdot 0_R = 0_R \cdot a = 0_R$.
b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$.
c) Ist $a \in R^\times$, so ist auch $-a \in R^\times$ und $(-a)^{-1} = -(a^{-1})$.
d) Für alle $m \in \mathbb{Z}$ ist $\quad (ma) \cdot b = a \cdot (mb) = m(a \cdot b)$.
e) Gilt $a \cdot b = b \cdot a$, so gilt $\forall n \in \mathbb{N}_0$:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Beweis. a) $a \cdot 0_R + a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R$.
$\Rightarrow$ $a \cdot 0_R$ und 0_R sind Lösungen der Gleichung

$$a \cdot 0_R + x = a \cdot 0_R \quad \overset{\text{Satz 2.1}}{\Longrightarrow} \quad a \cdot 0_R = 0_R$$

(gespiegelt analog).
b) $a \cdot b + a \cdot (-b) \overset{\text{Distrib.}}{=} a \cdot (b-b) = a \cdot 0_R \overset{a)}{=} 0_R$. Also ist $a \cdot (-b)$ additives Inverses zu ab, d.h. $a \cdot (-b) = -a \cdot b$.
Analog für $(-a) \cdot b$
$(-a) \cdot (-b) \overset{\text{1. Teil für } -b}{=} -((-a) \cdot b) = -(-a(b)) = ab$.
c) $(-a) \cdot (-(a^{-1})) \overset{b)}{=} a \cdot a^{-1} = 1_R$ und $(-(a^{-1}))(-a) = a^{-1} \cdot a = 1_R$.
d) Zeige: $(ma) \cdot b = m(a \cdot b)\ \forall\ m \in \mathbb{Z}$ (die andere Behauptung folgt analog).
$m \in \mathbb{N}_0$: vollst. Induktion nach m
$m = 0$: $(0 \cdot a) \cdot b = 0_R \cdot b = 0_R = 0(a \cdot b)$.
$m \mapsto m+1$ (≥ 1):

$$\begin{aligned}((m+1) \cdot a) \cdot b = (ma + a) \cdot b = (ma)b + ab &\overset{\text{Ind. Vor.}}{=} m(ab) + (ab) \\ &= (m+1)(ab)\end{aligned}$$

Fall $m < 0$: $m = -|m|$
$(ma)b = (|m|(-a)) \cdot b \overset{\text{Fall } m \in \mathbb{N}_0}{=} |m|((-a) \cdot b) \overset{b)}{=} |m|(-ab)) = (-|m|)(ab) = m(ab)$.
e) Vollst. Induktion nach $n \in \mathbb{N}_0$ (cf. Analysis I) $(ab = ba!)$ □

Lemma 3.2. *Für $(R,+,\cdot)$ sind äquivalent:*
a) $|R| = 1$ $\quad$ b) $R = \{0_R\}$ $\quad$ c) $0_R = 1_R$.

Beweis. a) $\Leftrightarrow$ b) $\Rightarrow$ c) sind klar.
c) $\Rightarrow$ b): Für jedes $a \in R$ gilt: $\quad 0_R = a \cdot 0_R = a \cdot 1_R = a$, also gilt b). □

Satz 3.3 (Unterringkriterium)**.** *Sei $(R,+,\cdot)$ ein Ring, sei $\varnothing \neq R_0 \subseteq R$. Dann gilt:*

$$R_0 \text{ ist Unterring von } R \iff \begin{cases} i) & 1_R \in R_0 \\ ii) & \forall a,b \in R_0 \text{ ist } a-b \in R_0 \text{ und } ab \in R_0 \end{cases}$$

Beweis. Nach Definition 3.1 b) ist R_0 ein Unterring von R genau dann, wenn (TR1) und (TR2) gelten.

$$\text{(TR1)} \overset{\text{Satz 2.2}}{\iff} \forall a,b \in R_0 : a-b \in R_0$$
$$\text{(TR2)} \underset{\text{Def. 1.1}}{\iff} \forall a,b \in R_0 : ab \in R_0 \cap (i)$$

□

Beispiel 3.4. Sei $(R,+,\cdot)$ ein Ring. Das *Zentrum von R*, $Z(R) := \{r \in R \mid rx = xr \ \forall x \in R\}$, ist ein Unterring von R:

$$1_R \in Z(R) \qquad (\text{also ist } Z(R) \neq \varnothing)$$
$$r_1, r_2 \in Z(R) \Longrightarrow r_1 - r_2, r_1 \cdot r_2 \in Z(R)$$

[Vorlesung 13, 15.5. 2014]

Definition 3.2. Sei $(R,+,\cdot)$ ein Ring.

a) Eine Teilmenge $\varnothing \neq I \subseteq R$ heisst ein *Ideal von R*, geschrieben $I \lhd R$, falls gilt:

(I1) I ist Untergruppe von $(R,+)$
(I2) $\forall\ a \in I, r \in R$ ist $ar \in I$ und $ra \in I$

Bemerkung.
- $\{0\}$ und R sind Ideale von R (die "trivialen" Ideale).
- Es ist $0 \in I$ für jedes Ideal I von R.
- (I2) heisst: $Ir \subseteq I$ und $rI \subseteq I \ \forall r \in R$.

Definition (3.2, Forts.). $(R,+,\cdot)$ Ring

b) Sei $I \lhd R$ ein Ideal.
$a, b \in R$ heissen *zueinander kongruent modulo I*, $a \equiv b \mod I$, wenn $b - a \in I$ ist.

(d.h. $a + I = b + I$ als Nebenklasse der Gruppe $(R,+)$ nach der Untergruppe I).

Bemerkung.
- Nach Definition ist jedes Ideal I von R eine Untergruppe von $(R,+)$ und da $(R,+)$ eine kommutative Gruppe ist, ist I ein Normalteiler davon. Das erklärt die Notation $\lhd$.
- $a \equiv b \mod I \Leftrightarrow \underset{-b \text{ add. Inv. v. } b}{a-b} \in I \Leftrightarrow b \underset{Hr}{\sim} a$ (für $H := I$), siehe Lemma 2.3.
  Also sind die Äquivalenzklassen genau die Nebenklassen von $(R,+)$ nach der Untergruppe $(I,+)$. Um die Äquivalenzklassen zu beschreiben, betrachtet man die Faktorgruppe $(R/I,+)$ (nach Obigem ist I ja Normalteiler).

Definition (3.2, Forts.). $(R,+,\cdot)$ Ring

c) R heisst *einfach*, wenn $\{0\}$ und R die einzigen Ideale von R sind.

Übungsbeispiel 39. Zeigen Sie: $I := \{f : \mathbb{R} \to \mathbb{R} \mid f(2) = 0\}$ ist ein Ideal von $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$.
Fragen: Sind $g, h \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ kongruent modulo I, falls $f(2) = g(2)$ gilt?
Gilt auch die Umkehrung?

Übungsbeispiel 40. Für $M \subseteq \mathbb{R}$ sei $I_M := \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = 0 \ \forall\ x \in M\}$.
Z.z.: I_M ist ein Ideal von $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$.
Frage: Wie kann man die trivialen Ideale von $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ in der Form I_M (mit M geeignet) darstellen?
Frage: Was bedeutet es für $g, h \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$, zueinander kongruent modulo I_M zu sein?

Satz 3.5. *Sei $(R, +, \cdot)$ ein Ring, $I \lhd R$ ein Ideal.*

a) *Sind $a, a', b, b' \in R$ mit $a \equiv a' \mod I$ und $b \equiv b' \mod I$, so folgt*
$$a + b \equiv a' + b' \mod I \quad \text{und} \quad a \cdot b \equiv a' \cdot b' \mod I$$

b) *Definiert man für $a, b \in R$ $\quad (a + I) \cdot (b + I) := (ab) + I$, so erhält man eine Verknüpfung $\cdot$ auf R/I, die $(R/I, +, \cdot)$ zu einem Ring macht.*
Das Nullelement davon ist I, das Einselement $1 + I$.
R/I heisst der Restklassenring von R modulo I.

Beweis. a)

$$\begin{aligned} a - a',\ b - b' \in I \ &\Rightarrow\ (a - a') + (b - b') = (a + b) - (a' + b') \in I \\ &\quad\ \Rightarrow \text{1. Kongruenz } \checkmark. \\ &\Rightarrow\ ab - a'b' = \overbrace{a}^{\in R} \cdot \overbrace{(b - b')}^{\in I} + \overbrace{(a - a')}^{\in I} \overbrace{b'}^{\in R} \in I \\ &\quad\ \Rightarrow \text{2. Kongruenz } \checkmark \end{aligned}$$

b) Die Definition von $(a+I)\cdot(b+I)$ ist unabhängig von der Wahl der Repräsentanten der Nebenklassen (2. Kongruenz in a)). Man muss also nur noch die Ringaxiome überprüfen, d.h., dass $(R/I, +, \cdot)$ (R1), (R2) und (R3) erfüllt.
(R1): $(R/I, +, \cdot)$ ist abelsche Gruppe (Kapitel 2), mit $0_{R/I} = I\ (= 0_R + I)$
(R2): $\cdot$ ist Operation ✓ Assoziativität soll man selber überlegen. Neutralelement:
$(a + I) \cdot (1 + I) = a \cdot 1 + I = a + I = 1 \cdot a + I = (1 + I) \cdot (a + I)$
(R3) (Distributivgesetze): Seien $a, b, c \in R$.

$$(a + I)((b + I) + (c + I)) = (a + I)((b + c) + I) = a \cdot (b + c) + I$$
$$(a + I) \cdot (b + I) + (a + I) \cdot (c + I) = (ab + I) + (ac + I) = (ab + ac) + I$$

die beiden Ausdrücke ganz rechts sind gleich wegen der Distributivgesetze in R.
Analog überprüft man, dass $((b+I)+(c+I))(a+I) = (b+I)(a+I)+(c+I)(a+I)$ gilt, die zweite Gleichung in (R3). □

Übungsbeispiel 41. Sei $I \lhd \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ das Ideal aus Beispiel 39.
Zeigen Sie: Die Menge aller konstanten Funktionen bilden ein Repräsentantensystem von $\mathrm{Abb}(\mathbb{R}, \mathbb{R})/I$.

Können Sie auch ein Repräsentantensystem für $\mathrm{Abb}(\mathbb{R},\mathbb{R})/I_M$ mit I_M wie in Beispiel 40 angeben?

Beispiel 3.6. Jede Untergruppe $U \leq (\mathbb{Z},+)$ ist von der Form $U = \langle m\rangle = m\,\mathbb{Z}$ ($m \in \mathbb{N}_0$) (Lemma 2.10) und ist ein Normalteiler in $(\mathbb{Z},+)$ (da + kommutativ ist)[5]
Beh.: $\forall\, m \in \mathbb{N}_0$: $\langle m\rangle \lhd (\mathbb{Z},+,\cdot)$
M.a.W.: jede Untergruppe von $(\mathbb{Z},+)$ ist ein Ideal des Ringes $(\mathbb{Z},+,\cdot)$.
Bew.: Untergruppe bzgl. + ✓.

$$\forall r \in \mathbb{Z} : r\cdot\langle m\rangle = \{r\cdot m\cdot j \mid j\in\mathbb{Z}\} \subseteq m\,\mathbb{Z} = \langle m\rangle \;\checkmark$$
$$\langle m\rangle \cdot r = \{m\cdot j\cdot r \mid j\in\mathbb{Z}\} \subseteq m\,\mathbb{Z} = \langle m\rangle \;\checkmark$$

Daher ist für jedes $m \in \mathbb{N}_0$ $(\mathbb{Z}/\langle m\rangle,+,\cdot)$ ein Ring, der sogenannte *Restklassenring* von $\mathbb{Z} \mod \langle m\rangle$.

$m=0:$	$\langle 0\rangle = \{0\},\ \mathbb{Z}/\langle 0\rangle = \{\{k\} \mid k\in\mathbb{Z}\} \xrightarrow{\sim} \mathbb{Z}$	Isom., siehe später
$m=1:$	$\langle 1\rangle = \mathbb{Z},\ \mathbb{Z}/\langle 1\rangle = \{\mathbb{Z}\}$	entspricht dem Nullring
$m\geq 1:$	$\mathbb{Z}/\langle m\rangle$ besteht aus m Elementen (Restkl.), $\mathbb{Z}/\langle m\rangle$ wird von $T := 1+(m)$ als zyklische Gruppe (additiv) erzeugt.	

Insbesonder (Satz 3.5a)) "Rechnen mit Kongruenzen", z.B. in $\mathbb{Z}/\langle 10\rangle$:

$$\underset{\equiv 9\cdot 3\cdot 3\cdot 3}{19\cdot 13^3} \underset{\equiv -5\cdot 1}{-25\cdot 21} \underset{\equiv 1^{17}}{+131^{17}} \equiv \cdots \equiv -1 \equiv 9 \mod 10$$

Definition 3.3. $(R,+,\cdot)$ sei ein Ring.

a) $I_1, I_2 \lhd R$ Ideale. Die *Summe der Ideale* I_1, I_2 ist definiert als

$$I_1 + I_2 := \{a+b \mid a\in I_1, b\in I_2\}$$

das *Produkt der Ideale* I_1, I_2 als

$$I_1\cdot I_2 := \{\sum_{i=1}^{n} a_i b_i \mid n\in\mathbb{N}\, a_i\in I_1, b_i\in I_2\}$$

b) Sei $M \subseteq R$, $\mathcal{M} := \{I \mid M\subseteq I \lhd R\}$ die Menge aller Ideale, die M enthalten. Dann ist

$$(M) := \bigcap_{I\in\mathcal{M}} I$$

das *von M erzeugte Ideal* ((M) ist das kleinste (bzgl. Mengeninklusion) Ideal, das M enthält).

c) $I \lhd R$ heisst *endlich erzeugt*, falls es eine endliche Menge $M \subseteq R$ gibt mit $(M) = I$.

Bemerkung. Zu a): Vorsicht, i.A. ist $I_1 I_2 \subsetneq I_1\cdot I_2$ (Letzteres: das Idealprodukt). $+,\cdot$ rekursiv $\rightsquigarrow$ Summe und Produkte von endlich vielen Idealen (ist assoz. Operation, cf. Satz 3.7b) weiter unten)

[5]Zur Erinnerung: $U = \langle m\rangle$ ist die von $\{m\}$ erzeugte Untergruppe von $(\mathbb{Z},+)$.

Zu b) Es gilt $R \in \mathcal{M}$, also ist $\mathcal{M} \neq \varnothing$. $\rightsquigarrow (M)$ ist tatsächlich ein Ideal (Satz 3.7a) weiter unten).
Zu c) Für $M = \{a_1, \ldots, a_n\}$ schreibt man auch $(a_1, \ldots, a_n)$ anstatt $(\{a_1, \ldots, a_n\})$.

[Vorlesung 14, 19.5. 2014]

Satz 3.7. *Sei $(R, +, \cdot)$ ein Ring*

a) *Ist $J \neq \varnothing$ und ist $I_j \lhd R$ für jedes $j \in J$, so ist auch*

$$\bigcap_{j \in J} I_j \lhd R \quad \text{ein Ideal in } R$$

b) *Sind $I_1, I_2, I_3 \lhd R$ Ideale, so sind $I_1 + I_2$, $I_1 \cdot I_2$ und $I_1 \cap I_2$ Ideale von R und es gilt:*
   (i) $I_1 + I_2 = (I_1 \cup I_2)$
   (ii) $I_1 \cdot I_2 = (\{ab \mid a \in I_1, b \in I_2\})$
   (iii) $I_1 \cdot I_2 \subseteq I_1 \cap I_2$
   (iv) $I_1 \cdot (I_2 + I_3) = (I_1 \cdot I_2) + (I_1 \cdot I_3)$ *und* $(I_1 + I_2) \cdot I_3 = (I_1 \cdot I_3) + (I_2 \cdot I_3)$.

c) *Für $I \lhd R$ sind äquivalent:*
   (i) $I = R$ (ii) $1 \in I$ (iii) $I \cap R^\times \neq \varnothing$

(In der Vorlesung wurden nicht alle Teilschritte beweisen.)

Beweis. a) Für jedes j ist $I_j \leq (R, +) \overset{\text{Satz 2.2}}{\Longrightarrow} \cap_{j \in J} I_j \leq (R, +)$.
Sei $r \in R$, $a \in \cap_{j \in J} I_j$. Dann gilt für alle $j \in J$, dass ra und ar in I_j liegen, also folgt $ra, ar \in \cap_{j \in J} I_j$.
b) Behauptung: $I_1 + I_2 \lhd R$:
• Seien $x, y \in I_1 + I_2$ beliebig, $x = a + b$, $y = a' + b'$ mit $a, a' \in I_1$ und $b, b' \in I_2$.
$x - y = a + b - a' - b' = \underbrace{(a - a')}_{\in I_1} + \underbrace{(b - b')}_{\in I_2} \in I_1 + I_2 \overset{\text{U'Gr-Kriterium}}{\Longrightarrow}$ (I1) ✓.
• Sei $r \in R$ beliebig.
$r(a + b) = \underbrace{ra}_{\in I_1} + \underbrace{rb}_{\in I_2} \in I_1 + I_2$,
dass $(a + b)r$ in $I_1 + I_2$ liegt, geht analog. $\Longrightarrow$ (I2) ✓.
$\Longrightarrow I_1 + I_2$ ist ein Ideal, dass $I_1 \cup I_2$ enthält, also hat man $\supseteq$ von (i).
Für jedes Element $x = a + b \in I_1 + I_2$ gilt: $a + b$ *muss* in jedem Ideal I mit $I \supseteq I_1 \cup I_2$ enthalten sein. $\Longrightarrow I_1 + I_2 \subseteq (I_1 \cup I_2)$ und damit hat man (i).
Beh.: $I_1 \cdot I_2 \lhd R$.
• Sind $x, y \in I_1, I_2$ beliebig, d.h. $x = \sum_{i=1}^n a_i b_i$, $y = \sum_{i=1}^m a_i' b_i'$ mit a_i, a_i' in I_1, $b_i, b_i' \in I_2$, so ist $x - y = a_1 b_1 + \cdots + a_n b_n + (-a_1')b_1' + \cdots + (-a_m')b_m' \in I_1 \cdot I_2$, also (I1) ✓.
• Für alle $r \in R$ gilt:

$$r \cdot x = r \cdot \sum_{i=1}^n a_i b_i = \sum_{i=1}^n \underbrace{(ra_i)}_{\in I_1} b_i \in I_1 \cdot I_2 \text{ und somit (I2). } \checkmark$$

$\Longrightarrow I_1 \cdot I_2$ ist ein Ideal von R, das alle $a \cdot b$ ($a \in I_1$, $b \in I_2$) enthält. Also gilt $\supseteq$ in (ii).

Jedes $x = \sum_{i=1}^{n} a_i b_i \in I_1 \cdot I_2$ muss in jedem Ideal $I \supseteq \{a \cdot b \mid a \in I_1, b \in I_2\}$ enthalten sein. Somit gilt auch $\subseteq$ in (ii).
iii) $I_1 \cap I_2$ ist Ideal (nach a)), $I_1 \cdot I_2$ ist Ideal (nach b)).
Jedes $x \in I_1 \cdot I_2$ schreibt sich als

$$x = \sum_{i=1}^{n} \underbrace{\overbrace{a_i}^{\in I_1}}_{\in R} \underbrace{\overbrace{b_i}^{\in R}}_{\in I_2}$$

Wegen den Klammern oberhalb des Ausdrucks rechts ist $x \in I_1$, wegen den Klammern unterhalb in I_2, also $x \in I_1 \cap I_2$.
iv) $\subseteq$: Sei $x \in I_1 \cdot (I_2 + I_3)$:

$$x = \sum_{i=1}^{n} a_i(b_i + c_i) = \sum a_i b_i + \sum a_i c_i \in (I_1 \cdot I_2) + (I_1 \cdot I_3) \checkmark$$

$\supseteq$: Sei $y \in (I_1 \cdot I_2) + (I_1 \cdot I_3)$:

$$y = \sum_{i=1}^{n} a_i b_i + \sum_{i=1}^{m} a'_i c_i \overset{\text{sei } a_{i+1} := a'_i}{=} \sum_{i=1}^{n+m} a_i \begin{cases} \cdot(b_i + 0) & \text{für } 1 \le i \le n \\ \cdot(0 + c_{i-n}) & \text{für } n+1 \le i \le n+m \end{cases}$$

und das ist ein Element der linken Seite, $\checkmark$.

2. Teil: Übung (analog).
c) Die Implikationen i)$\Rightarrow$ ii) $\Rightarrow$ iii) sind klar.
iii) $\Rightarrow$ i): Sei $u \in I \cap R^\times$: Dann existiert $u^{-1} \in R$ mit $u^{-1} \cdot u = 1$.
Für beliebige $x \in R$ gilt nun:
$\underbrace{(\underbrace{x \cdot u^{-1}}_{\in R}) \cdot \underbrace{u}_{\in I}}_{\in I} = x \cdot 1 = x \in I$, also ist $R = I$. □

Übungsbeispiel 42. Man betrachte $I_1 := \{f : \mathbb{R} \to \mathbb{R} \mid f(1) = 0\} \lhd \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ und $I_2 := I \lhd \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ aus Beispiel 39.
Z.z.: $I_1 + I_2 = \mathrm{Abb}(\mathbb{R}, \mathbb{R})$
((das sollte damit gehen: man nimmt f mit $f(1) = 0$ und Steigung -1, g mit $g(2) = 0$ und Steigung $+1$. Die Summe davon sollte die Einsfunktion sein.))
und $I_1 \cap I_2 = I_1 \cdot I_2 = \{f : \mathbb{R} \to \mathbb{R} \mid f(1) = 0 = f(2)\} = I_{\{1,2\}}$ in der Notation von Beispiel 40.
Frage: Seien M_1, M_2 beliebige Teilmengen von $\mathbb{R}$. Was wären $A, B \subseteq \mathbb{R}$ mit

$$I_{M_1} + I_{M_2} = I_A \text{ und } I_{M_1} \cdot I_{M_2} = I_B$$

(in den Bezeichnungen von Beispiel 40).

Beispiel 3.8. Sei $R = (\mathbb{Z}, +, \cdot)$, seien $m, n \in \mathbb{N}$. $I_1 = (m) = m\cdot\mathbb{Z}$, $I_2 = (n) = n\cdot\mathbb{Z}$. Seien $d = \mathrm{ggT}(m,n)$ und $v = kgV(m,n)$, $d, v \in \mathbb{N}$.
Dann hat man (für $V(m)$:=die Menge der Vielfachen von m in $\mathbb{N}$)

(i) $I_1 \cap \mathbb{N} = V(m)$ und $m = \min(I_1 \cap \mathbb{N})$
(ii) $(m) \subseteq (n) \Longleftrightarrow n \mid m$
(iii) $(m) + (n) = (d)$
(iv) $(m) \cap (n) = (v)$
(v) $(m) \cdot (n) = (mn)$

Insbesondere gilt:
$\mathrm{ggT}(m,n) = 1 \Longleftrightarrow \exists\, x, y \in \mathbb{Z} : mx+ny = 1 \Leftrightarrow (m)+(n) = \mathbb{Z} \Leftrightarrow (m)\cap(n) = (mn)$.
Beweis dieser Eigenschaften: Übung.

3.2. **Ringhomomorphismen, Charakteristik.**

Definition 3.4. $(R, +, \cdot)$ und $(R', +, \cdot)$ seien Ringe.
a) $\varphi : R \to R'$ mit den Eigenschaften
(RHom1) $\forall a, b \in R$ gilt

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{und} \quad \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$$

(RHom2) $\varphi(1_R) = 1_{R'}$
heisst ein *Ringhomomorphismus* (von R nach R')[6].
b) $\varphi : R \to R'$ sei ein Ringhomomorphismus. $\ker\varphi := \varphi^{-1}(\{0_{R'}\})$ heisst der *Kern von* φ, $\mathrm{im}\,\varphi := \varphi(R)$ heisst das *Bild von* φ.
c) Sei φ wie in a). φ heisst *Ring-* $\left\{\begin{array}{l} mono \\ epi \\ iso \end{array}\right\}$ *-morphismus*, wenn φ $\left\{\begin{array}{l} \text{inj.} \\ \text{surj.} \\ \text{bij.} \end{array}\right\}$ ist.

Beim Ringisomorphimus: R und R' heissen dann *zueinander isomorph*, $R \cong R'$. Ein Ring-{homo/iso}-morphismus von R nach R heisst ein *Ring-{endo/auto}-morphismus.*

Bemerkung.
- $\varphi : R \to R'$ Ringhomom. $\Rightarrow \varphi$ ist Gruppenhomomorphismus $\varphi : (R,+) \to (R',+)$. Insbesondere ist $\varphi(0_R) = 0_{R'}$. $\varphi(-a) = -\varphi(a)$ $\forall a \in R$. Wegen $\varphi(1_R) = 1_{R'}$ gilt $\forall a \in R^\times$: $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- φ Ringisomorphismus $\Rightarrow \varphi^{-1} : R' \to R$ ist auch Ringisomorphismus.
- $\varphi : R \to R'$, $\varphi' : R' \to R''$ Ringhomomorphismen. $\Rightarrow \varphi' \circ \varphi : R \to R''$ ist Ringhomomorphismus.

Definition (3.4, Forts.). d) Sei $I \lhd R$ ein Ideal.

$$\pi : (R, +, \cdot) \to (R/I, +, \cdot), \quad a \mapsto a + I$$

heisst der *(kanonische) Restklassenhomomorphismus* von R auf den Restklassenring R/I.

[6](RHom1) sagt, dass φ ein Homomorphismus bzgl. + und $\cdot$ ist, siehe entsprechende Definitionen zu Verknüpfungen, Gruppen.

Übungsbeispiel 43. Sei $\varnothing \neq M \subseteq \mathbb{R}$. Man definiert $\varphi : \mathrm{Abb}(\mathbb{R},\mathbb{R}) \to \mathrm{Abb}(M,\mathbb{R})$ definiert durch die Einschränkung $\varphi(f) := f\mid_M$.
Behauptung: φ ist ein Ringhomomorphismus (wieso ist $\mathrm{Abb}(M,\mathbb{R})$ ein Ring?).
Ist φ ein Ringepimorphismus? Was ist $\ker(\varphi)$? (Bezug zu Übungsbeispiel 40?)

Bemerkung. (zu (d) in Definition 3.4): Nach Satz 3.5 ist π ein Homomorphismus, surjektiv, $\ker(\pi) = I$.
Insbesondere gibt es zu jedem Ideal $I \triangleleft R$ einen Ring $\overline{R}$ und ein Ringepimorphismus $\psi : R \to \overline{R}$ mit $\ker\psi = I$, z.B. gerade $\overline{R} = R/I$, $\psi = \pi$.

Beispiel 3.9. Die "Konjugation mit Ringeinheiten" gibt einen Ringisomorphismus: Sei $(R,+,\cdot)$ ein Ring, $a \in R^\times$, $\kappa_a : R \to R$, $x \mapsto axa^{-1}$.
Was ist die Umkehrabbildung zu κ_a?
In einem konkreten Beispiel: $R = (M_{n\times n},\mathbb{R},+,\cdot)$ und $a \in \mathrm{GL}_n(\mathbb{R}) = R^\times$.

(Der folgende Satz ist analog zu Satz 2.13, jetzt für Ringe.)

Satz 3.10. *$(R,+,\cdot)$ und $(R',+,\cdot)$ seien Ringe, $\varphi : R \to R'$ ein Ringhomomorphismus. Dann gilt*
a) $\varphi(R^\times) \subseteq (R')^\times$ und $\varphi\mid_{R^\times}: R^\times \to (R')^\times$ ist ein (multiplikativer) Gruppenhomomorphismus.
b) Ist $R_0 \leq R$ Unterring $\Rightarrow \varphi(R_0) \leq R'$ ist Unterring von R'
c) Ist $I \triangleleft R$ ein Ideal $\Rightarrow \varphi(I) \triangleleft \varphi(R)$ ist ein Ideal in $\varphi(R)$.
d) Ist $\left.\begin{array}{l} R_0' \leq R' \text{ Unterring} \\ I' \triangleleft R' \text{ Ideal} \end{array}\right\}$ *so gilt* $\left\{\begin{array}{l} \varphi^{-1}(R_0) \leq R \text{ ist Teilring von } R \\ \varphi^{-1}(I') \triangleleft R \text{ ist Ideal von } R \end{array}\right.$
e) $\ker(\varphi) \triangleleft R$.

Beweis. a) $\varphi(1_R) = 1_{R'} \overset{S.1.4b)}{\Longrightarrow} a$ ist inv'bar bzgl. $\cdot$ (d.h. $a \in R^\times$) $\Rightarrow \varphi(a) \in R^\times$.

b) φ ist Gruppenhomomorphismus bzgl. $+ \overset{S.2.13c)}{\Longrightarrow} (\varphi(R_0),+) \leq (R',+)$ ist Untergruppe, also (TR1) ✓.

$$\left.\begin{array}{l} 1 \in R_0 \Rightarrow \varphi(1_R) = 1_R' \in \varphi(R_0) \\ a',b' \in \varphi(R_0) \text{ bel. } \exists\, a,b \in R_0 \text{ mit } \varphi(a) = a', \varphi(b) = b' : \\ \qquad a' \cdot b' = \varphi(a)\cdot\varphi(b) = \varphi(\overbrace{a\cdot b}^{\in R_0}) \in \varphi(R_0) \end{array}\right\} \text{, also (TR2) ✓.}$$

c) Satz 2.13 c) $\Rightarrow (\varphi(I),+) \leq (\varphi(R),+)$ ist U'Gruppe... (I1) ✓
Seien $r' \in \varphi(R)$, $a' \in \varphi(I)$ beliebig, dann existieren $r \in R$, $a \in I$ mit $\varphi(r) = r'$, $\varphi(a) = a'$. Ausserdem ist $I \triangleleft R$, also $ra, ar \in I$. Damit hat man:

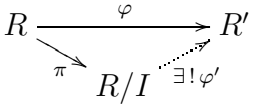
$$a'r' = \varphi(a)\varphi(r) \overset{\text{Homom.}}{=} \varphi(\underbrace{ar}_{\in I}) \in \varphi(I), \text{ analog ist } r'a' \in \varphi(I), \text{ also (I2) ✓.}$$

d) Kann man mit Satz 2.13 e) zeigen.

e) $\{0\} \triangleleft R' \overset{d)}{\Rightarrow} \ker(\varphi) = \varphi^{-1}(\{0\}) \triangleleft R$. □

[Vorlesung 15, 22.5. 2014]

Satz 3.11. *Seien $(R,+,\cdot)$ und $(R',+,\cdot)$ Ringe.*
a) (Universelle Eigenschaft des Restklassenhomomorphismus)
$I \lhd R$, $\pi : R \to R/I$ der Restklassenhomomorphismus. Dann gilt:
Zu jedem Ringhomomorphismus $\varphi : R \to R'$ mit $I \subseteq \ker(\varphi)$ existiert genau ein Ringhomomorphismus $\varphi' : R/I \to R'$ mit $\varphi' \circ \pi = \varphi$.



b)(Homomorphiesatz)
Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Dann existiert genau ein Ringmonomorphismus $\varphi' : R/\ker(\varphi) \to R'$ mit $\varphi' \circ \pi = \varphi$. Insbesondere ist $R/ker(\varphi) \cong \mathrm{im}(\varphi)$
c) Sei $\varphi : R \to R'$ ein Ringepimorphismus, $\Omega := \{I \mid \ker(\varphi) \subseteq I \lhd R\}$ die Menge der Ideale von R, welche $\ker(\varphi)$ enthalten. Sei $\Omega' := \{I' \mid I' \lhd R'\}$ die Menge aller Ideale von R'. Dann gilt:
$\tilde{\varphi} : \Omega \to \Omega'$, $I \mapsto \varphi(I)$ ist eine inklusionserhaltende Bijektion und für $I' \in \Omega'$ ist $\tilde{\varphi}^{-1}(I') = \varphi^{-1}(I') \lhd R$.

[Vorlesung : Beweis von c) nicht in der Vorlesung gemacht]

Beweis. a) $(I,+)$ ist Normalteiler der Gruppe $(R,+) \overset{Satz 2.16}{\Longrightarrow} \exists!$ additiver Gruppenhomomorphismus $\varphi' : R/I \to R'$ mit $\varphi' \circ \pi = \varphi$ (und zwar: $\varphi'(a+I) := \varphi(a)$). Es bleibt zu zeigen: φ' ist auch Ringhomomorphismus.

$$\begin{aligned}
\pi(1_R) &= 1_R + I \in R/I \text{ ist Einselement von } R/I \\
\varphi'(1_R + I) &= \varphi(1_R) = 1_{R'} \\
\varphi'((a+I)\cdot(b+I)) &= \varphi'(a\cdot b + I) = \varphi(ab) \text{ und} \\
\varphi'(a+I)\cdot\varphi(b'+I) &= \varphi(a)\cdot\varphi(b) = \varphi(ab)
\end{aligned}$$

b) Verwende a) mit $I := \ker(\varphi)$. Injektivität: Satz 2.16.

c) • Definition von $\tilde{\varphi}$: $I \in \Omega$, $I \lhd R \overset{S.3.10c)}{\Longrightarrow} \varphi(I) \lhd \varphi(R) \overset{\varphi \text{ epi}}{=} R'$, d.h. $\varphi(I) \in \Omega'$.
• Definieren "$\tilde{\varphi}^{-1}$": $\Omega' \to \Omega$, $I' \mapsto \varphi^{-1}(I')$.

$$\left.\begin{array}{l} I' \lhd R' \overset{S.3.10d}{\Longrightarrow} \varphi^{-1}(I') \lhd R \\ 0 \in I' \Longrightarrow \ker(\varphi) \subseteq \varphi^{-1}(I') \end{array}\right\} \Rightarrow \varphi^{-1}(I') \in \Omega.$$

Brauchen noch: Dies ist bijektiv und Umkehrabbildung hat gewünschte Eigenschaften.
Beh.: (i) $\tilde{\varphi}^{-1}(\tilde{\varphi}) = I$ und (ii) $\tilde{\varphi}(\tilde{\varphi}^{-1}(I')) = I'$ $\forall\ I \in \Omega$, $\forall\ I' \in \Omega'$.
$\supseteq$ in (i): $I \subseteq \varphi^{-1}(\varphi(I)) = \tilde{\varphi}^{-1}(\tilde{\varphi}(I))$ ✓
$\subseteq$ in (i): Sei $a \in \varphi^{-1}(\varphi(I))$, also $\varphi(a) \in \varphi(I)$. Dann existiert $b \in I$: $\varphi(b) = \varphi(a)$.
$\Rightarrow 0 = \varphi(b) - \varphi(a) = \varphi(b-a) \Rightarrow b - a \in \ker(\varphi) \subseteq I$ (und $b \in I$) $\Rightarrow a \in I$ ✓.

Zu (ii): $\varphi(\varphi^{-1}(I')) = I'$ gilt, da φ surjektiv ist. $\Rightarrow \tilde{\varphi}^{-1} \circ \tilde{\varphi} = \mathrm{id}_\Omega$ und $\tilde{\varphi} \circ \tilde{\varphi}^{-1} = \mathrm{id}_{\Omega'}$.
Inklusionserhaltend: $I \subseteq J$, beide in $\Omega \iff \varphi(I) \subseteq \varphi(J)$, beide in Ω'. (Übung) □

Bemerkung.
- Analog zu den Isomorphiesätzen für Gruppen (mit U'Gruppen, Normalteilern) gibt es Isomorphiesätze für Ringe (mit U'Ringen, Idealen).
- Satz 3.11 mit $\varphi = \pi : R \to R/I$ ergibt Bijektion (inkl.erhaltende)

$$\Omega = \{J \lhd R \mid I \subseteq J\} \quad \overset{\tilde{\varphi}, \tilde{\varphi}^{-1}}{\longleftrightarrow} \quad \{J' \mid J' \lhd R/I\} = \Omega'$$

Übungsbeispiel 44. Z.z.: Die Abbildung $\psi : R := \mathrm{Abb}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$, definiert durch $\psi(f) = f(2)$ für $f \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ ist ein Ringepimorphismus. Es sei $I \lhd R$ das Ideal aus Übungsbeispiel 39. Man beweise $R/I \cong \mathbb{R}$ mit Hilfe von Satz 3.11. Was ist der Zusammenhang zu Übungsbeispiel 41? Analog: $R/I_M \cong \mathrm{Abb}(M, \mathbb{R})$ (mit Übungsbeispiel 43).

Nun zur speziellen Rolle von $\mathbb{Z}$ ("initiales Objekt" unter den Ringen).

Bemerkung. Sei $(R, +, \cdot)$ ein Ring.
Gesucht sind alle Ringhomomorphismen $\varphi : \mathbb{Z} \to R$.
$\varphi(1_\mathbb{Z}) \overset{!}{=} 1_R$ und $\mathbb{Z} = \langle 1 \rangle$ wird als additive Gruppe von $1 = 1_\mathbb{Z}$ erzeugt.
$\Rightarrow \forall k \in \mathbb{N}$, $\varphi(k) = \varphi(1 + \cdots + 1) \overset{Homom.}{=} \varphi(1) + \cdots + \varphi(1) = 1_R + \cdots + 1_R = k \cdot 1_R$.
$\Rightarrow \forall k \in \mathbb{Z}$ ist $\varphi(k) = k \cdot 1_R$.

Damit existiert *genau ein* Ringhomomorphismus $\varphi : \mathbb{Z} \to R$ (das ist auch für den Nullring $R = \{0_R\}$ o.k.).
Das Bild davon, $\varphi(\mathbb{Z}) = \{k \cdot 1_R \mid k \in \mathbb{Z}\} \leq R$, ist ein Unterring, der "kleinste" Unterring, denn es gilt:
Jeder Unterring von R muss 0_R, 1_R, also auch $\varphi(\mathbb{Z})$ enthalten.

Die obige Bemerkung führt zu Lemma 3.12

Lemma 3.12. *$(R, +, \cdot)$ sei ein Ring. Es gilt:*

a) *Es existiert genau ein Ringhomomorphismus $\varphi : \mathbb{Z} \to R$ und für diesen ist $\varphi(\mathbb{Z}) = \{k \cdot 1_R \mid k \in \mathbb{Z}\} =: R_0$.*
b) *R_0 ist der kleinste Unterring von R (jeder Unterring von R enthält R_0).*
c) *Es ex. genau ein $n \in \mathbb{N}_0$ mit $R_0 \cong \mathbb{Z}/(n)$.*

Beweis. Beweis von a), b): siehe obige Bemerkung.
c): $R_0 \cong \mathbb{Z}/\ker(\varphi)$. Der Kern $\ker(\varphi)$ ist ein Ideal von $\mathbb{Z}$, also $\ker(\varphi) = (n)$ für ein $n \in \mathbb{N}_0$ (mit Lemma 2.10) □

Konkret: es ist $R_0 \cong \{0_R\}$ falls $n = 1$ und $R_0 \cong \mathbb{Z}$ für $n = 0$.

Definition 3.5. $(R, +, \cdot)$ sei ein Ring. Der in Lemma 3.12 b) definierte kleinste Unterring $R_0 = \{k \cdot 1_R \mid k \in \mathbb{Z}\} \leq R$ heisst der *Primring von R*. Die laut Lemma 3.12 c) eindeutig bestimmte Zahl $n \in \mathbb{N}_0$ mit $R_0 \cong \mathbb{Z}/(n)$ heisst die *Charakteristik des Ringes R* (geschrieben: $\mathrm{char}(R) = n$).

Insbesondere ist $\mathrm{char}(\mathbb{Z}/(n)) = n \ \forall\ n \in \mathbb{N}_0$, ausserdem
$\mathrm{char}(\mathbb{Q})=\mathrm{char}(\mathbb{R}) =\mathrm{char}(\mathbb{C}) = 0 =\mathrm{char}(M_{n\times n}(\mathbb{R}))$.

3.3. **Nullteiler, Ideale in kommutativen Ringen.** Ab nun nehmen wir an, dass alle Ringe kommutativ sind (i.e. für alle $a, b \in R$ ist $ab = ba$).
[Vorlesung 16, 26.5. 2014]

Definition 3.6. Sei $(R, +, \cdot)$ ein komm. Ring.

a) Ein Element $a \in R$ heisst ein *Nullteiler* von R, falls ein $b \in R \setminus \{0\}$ existiert mit $a \cdot b = 0$. Die Menge aller Nullteiler von R wird als $\mathrm{NT}(R)$ geschrieben.
b) R heisst *Integritätsbereich* ("domain"), falls $\mathrm{NT}(R) = \{0\}$ ist. Man sagt dann, R sei *nullteilerfrei* (das Nullelement ist der einzige Nullteiler).
c) R heisst ein *Körper* (*field, corps*), falls $R^\times = R \setminus \{0\}$ gilt, d.h. falls jedes Element $\neq 0$ ein multiplikatives Inverses hat. (R heisst *Divisionsring*, falls R diese Eigenschaft hat, aber nicht notwendig kommutativ ist.)

Bemerkung. Zu a): Für $0 \in R$ gilt: $0 \in \mathrm{NT}(R) \iff \exists\ b \in R \setminus \{0\} : 0 \cdot b = 0$ $\iff R\setminus\{0\} \neq \varnothing \iff R \supsetneq \{0\}$. Ist $R = \{0\}$ der Nullring, so hat man $0\cdot 0 = 0 = 1_R$; $R^\times = \{0\}$, $\mathrm{NT}(R) = \varnothing$!

Zu b) • Der Nullring R ist kein Integritätsbereich, da $\mathrm{NT}(R) = \varnothing$ gilt. Im Integritätsbereich ist notwendig $0_R \neq 1_R$.
• Ist $R_0 \leq R$ Unterring, $a \in R_0$ mit $a \notin \mathrm{NT}(R) \iff a \notin \mathrm{NT}(R_0)$. D.h. ist R ein Integritätsbereich, so ist jeder Unterring $\neq \{0\}$ von R auch ein Integritätsbereich.

Zu c) • Ist R ein Körper, so ist $(R \setminus \{0\}, \cdot)$ eine Gruppe (da $R \setminus \{0\} = R^\times$ ist).
• Der Nullring $R = \{0\}$ ist kein Körper: $R^\times = \{0\} \neq R\setminus\{0\}$. D.h. in jedem Körper ist $0_R \neq 1_R$.

Lemma 3.13. *Sei $(R, +, \cdot)$ ein kommutativer Ring.*
a) Für $a \in R$ sind äquivalent:
i) $a \notin NT(R)$ ii) $\forall\ b, c \in R$ gilt: aus $ab = ac$ folgt $b = c$ (d.h. a ist kürzbar).
b) $R^\times \cap NT(R) = \varnothing$. Insbesondere: Ist R ein Körper, so ist R auch ein Integritätsbereich.
c) Ist R Integritätsbereich (bzw. speziell ein Körper), so gilt $\mathrm{char}(R) \in \mathbb{P} \cup \{0\}$.

Beweis. a)

i)$\Rightarrow$ ii) Sei $ab = ac \Rightarrow 0 = ab - ac = a(b - c) \overset{a\notin NT(R)}{\Longrightarrow} b - c = 0 \ \Rightarrow\ b = c$.
ii) $\Rightarrow$ i) Für jedes $x \in R$ mit $a \cdot x = 0 = a \cdot 0$ gilt wg ii): $x = 0 \Rightarrow a \notin \mathrm{NT}(R)$.

b) Sei $a \in R^\times$. Für alle $x \in R$ mit $ax = 0$ gilt:

$$0 = a^{-1} \cdot 0 = a^{-1}ax = 1x = x \ \Rightarrow a \notin NT(R).$$

Insbesondere gilt im Fall, wo R ein Körper ist:

$$\left.\begin{array}{r} R^\times = R \setminus \{0\} \overset{b)}{\Rightarrow} \mathrm{NT}(R) \subseteq R \setminus R^\times = \{0\} \\ \text{und } R \supsetneq \{0\} \Rightarrow\ 0 \in \mathrm{NT}(R) \end{array}\right\} \Rightarrow NT(R) = \{0\},$$

also ist R ein Integritätsbereich.
c) Sei R ein Intergritätsbereich.
Ann.: $\mathrm{char}(R) \in \mathbb{N}_0 \setminus (\mathbb{P} \cup \{0\}) = \{1\} \cup \{n \in \mathbb{N} \mid n \text{ zusammengesetzte Zahl}\}$[7].
• Fall $\mathrm{char}(R) = 1$: $\Rightarrow 0_R = 1_R$, $R = \{0_R\}$, Widerspruch zu Int.-bereich.
• Fall $\mathrm{char}(R) = n = dd'$ mit $1 < d, d' < n$. Der Primring ist $R_0 = \{k \cdot 1_R \mid k \in \mathbb{Z}\} \cong \mathbb{Z}/(n)$, d.h. $n \cdot 1_R = 0_R$ und $\forall 1 \leq j < n$ gilt $j \cdot 1_R \neq 0_R$

$$(\underbrace{d \cdot 1_R}_{\neq 0_R})(\underbrace{d' \cdot 1_R}_{\neq 0_R}) = n \cdot 1_R = 0_R$$

damit folgt, dass $d \cdot 1_R$ ein Nullteiler ist, der verschieden von 0 ist, also $\mathrm{NT}(R) \supsetneq \{0_R\}$, $\lightning$ zu R Integritätsbereich. □

Satz 3.14 (Struktur der Restklassenringe $\mathbb{Z}/(n)$)**.** *Sei $n \in \mathbb{N}$.*
a) Für $a \in \mathbb{Z}$ sind äquivalent:

$$i)\ a + n\mathbb{Z} \in (\mathbb{Z}/(n))^\times \quad ii)\ a + n\mathbb{Z} \notin NT(\mathbb{Z}/(n)) \quad iii)\ \mathrm{ggT}(a, n) = 1$$

Insbesondere ist $\mathbb{Z}/(n) = (\mathbb{Z}/(n))^\times \dot\cup NT(\mathbb{Z}/(n))$.
b) Es sind äquivalent:

$$i)\ \mathbb{Z}/(n) \text{ ist Körper} \quad ii)\ \mathbb{Z}/(n) \text{ ist Integritätsbereich} \quad iii)\ n \in \mathbb{P}$$

Bemerkung. • Für $n = 0$ ist $\mathbb{Z}/(0) \cong \mathbb{Z}$. In a) sind dann ii) $\Rightarrow$ i) und ii) $\Rightarrow$ iii) falsch. In b) sind ii) $\Rightarrow$ i) und ii) $\Rightarrow$ iii) falsch.

• Für $p \in \mathbb{P}$ nennt man $\mathbb{F}_p := \mathbb{Z}/(p)$ den *Primkörper mit Charakteristik p*. Die Notation $\mathrm{GF}(p)$ wird auch verwendet (Galoiskörper mit p Elementen).

Man kann zeigen, dass es für jede Primzahl p und jedes $k \in \mathbb{N}$ bis auf Isomorphie genau einen endlichen Körper mit p^k Elementen gibt. Man bezeichnet diesen mit $\mathbb{F}_{p^k}$ oder mit $\mathrm{GF}(p^k)$.

Beweis. a) i) $\Rightarrow$ ii): Folgt direkt aus Lemma 3.13b).
ii) $\Rightarrow$ iii): Ann.: $\mathrm{ggT}(a, n) = d > 1$. Dann ist $\frac{n}{d}$ eine ganze Zahl, $1 \leq \frac{n}{d} < n$, also ist $\frac{n}{d} + n\mathbb{Z}$ verschieden von $0 + n\mathbb{Z}$. Ausserdem ist $\frac{a}{d}$ auch eine ganze Zahl. Damit:

$$(a + n\mathbb{Z}) \cdot (\frac{n}{d} + n\mathbb{Z}) = a\frac{n}{d} + n\mathbb{Z} = \frac{a}{d}n + n\mathbb{Z} = n\mathbb{Z}$$

und letzteres ist das Nullelement in $\mathbb{Z}/(n)$. Also folgt: $a + n\mathbb{Z}$ ist ein Nullteiler von $\mathbb{Z}/(n)$, ein Widerspruch zu ii).
iii) $\Rightarrow$ i): Sei $\mathrm{ggT}(a, n) = 1$. Dann folgt aus der elementaren Zahlentheorie, dass wir a', $n' \in \mathbb{Z}$ finden können mit $a \cdot a' + n \cdot n' = 1 = \mathrm{ggT}(a, n)$[8]. Wir nehmen ein solches a', für dieses gilt dann notwendig $a \cdot a' \equiv 1 \mod n$, also:

$$(a + n\mathbb{Z})(a' + n\mathbb{Z}) = 1 + n\mathbb{Z}$$

und damit ist i) erhalten.

[7] n ist zusammengesetzte Zahl, falls $d, d' \in \mathbb{N}$ existieren, $1 < d, d' < n$ mit $n = d \cdot d'$.
[8] Genauer: Sind $a, b \in \mathbb{Z}$, so existieren $a', b' \in \mathbb{Z}$ mit $a \cdot a' + b \cdot b' = \mathrm{ggT}(a, b)$.

b) i) $\overset{L3.13b}{\Longrightarrow}$ ii) $\overset{L3.13c}{\Longrightarrow}$iii)
iii)$\Rightarrow$ i): Sei $n = p \in \mathbb{P}$: $\forall\ 1 \leq a < p$ ist ggT$(a, p) = 1$, also ist nach a) $\mathbb{Z}/(p)^\times = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \ldots, (p-1) + p\mathbb{Z}\}$ und letzteres ist gleich $\mathbb{Z}/(p) \setminus \{p \cdot \mathbb{Z}\}$, also ist $\mathbb{Z}/(p)$ ein Körper. □

Definition 3.7. Sei $(R, +, \cdot)$ ein kommutativer Ring.
a) Für $a \in R$ heisst $(a) = aR = Ra = \{ar \mid r \in R\}$ das *von a erzeugte Hauptideal von R*. Ein Ideal $I \lhd R$ heisst *Hauptideal*, falls ein $a \in R$ existiert mit $I = (a)$. Ist R ein Integritätsbereich und jedes Ideal von R ein Hauptideal, so heisst R ein *Hauptidealbereich* (*principal ideal domain, P.I.D.*).

Bemerkung. Da R kommutativ ist, ist $a \cdot R = \{ar \mid r \in R\}$ tatsächlich ein Ideal (Übung)
aR ist das kleinste Ideal, das a enthält, die Notation "(a)" ist also konsistent mit Definition 3.3 b).
Falls R nicht kommutativ ist, so ist

$$(a) = \{\sum_{i=1}^{n} r_i a s_i \mid n \in \mathbb{N}, r_i, s_i \in R\}$$

Beispiele. • R kommut. Ring: $(0) = \{0\}$, $(1) = R = (u)$ für jedes $u \in R^\times$: die trivialen Ideale sind beide Hauptideale. $\overset{S3.15}{\Longrightarrow}$ Jeder Körper ist ein Hauptidealbereich
• Jedes Ideal von$(\mathbb{Z}, +, \cdot)$ ist ein Hauptideal $\Rightarrow \mathbb{Z}$ ist ein PID.

Definition (3.7, Forts.**).** b) • $P \lhd R$ heisst *maximales Ideal*, wenn $P \neq R$ ist und es kein Ideal $Q \lhd R$ gibt mit $P \subsetneq Q \subsetneq R$.
• $P \lhd R$ heisst *Primideal*, wenn $P \neq R$ ist und für alle $a, b \in R$ gilt: aus $ab \in P$ folgt $a \in P$ oder $b \in P$.

[Vorlesung 17, 12.6. 2014]

Beispiel. Ist $p \in \mathbb{P}$, so ist $(p) \lhd \mathbb{Z}$ ein Primideal (überlegen!)
(p) ist auch ein maximales Ideal (Übung).
$(0) \lhd \mathbb{Z}$ ist Primideal, aber kein maximales Ideal.

Übungsbeispiel 45. Für $M \subseteq \mathbb{R}$ sei $I_M \lhd$ Abb$(\mathbb{R}, \mathbb{R})$ wie in Übungsbeispiel 40. Behauptung: I_M ist Hauptideal. (Benutzen Sie die charakteristische Funktion der Menge $\mathbb{R} \setminus M$)

Satz 3.15. *Für einen komm. Ring $(R, +, \cdot)$ mit $|R| \geq 2$ sind äquivalent:*
a) R ist Körper.
b) $\{0\}$ und R sind die einzigen Ideale von R.
c) Jeder Ringhomomorphismus $\varphi : R \to R'$ in einen (nicht unbedingt kommutativen) Ring R' mit $|R'| \geq 2$ ist ein Monomorphismus.

Beweis. a) $\Rightarrow$ b) Sei $\{0\} \subsetneq I \lhd R$. D.h. es existiert ein $a \in I \cap (R \setminus \{0\}) \overset{R\text{Körper}}{=} R^\times$, d.h. es existiert $a \in I \cap R^\times \Rightarrow I = R$ (mit Satz 3.7 c)).

b) $\Rightarrow$ c) Sei $\varphi : R \to R'$ ein Ringhomomorphismus, $|R|, |R'| \geq 2$. Dann gilt: $\varphi(0_R) = 0_{R'} \neq 1_{R'} = \varphi(1_R)$.
$\Longrightarrow 1_R \notin \varphi^{-1}(\{0_{R'}\}) = \underbrace{\ker(\varphi)}_{=\{0\}\text{wegen b)}} \lhd R$, also ist φ injektiv.

c) $\Rightarrow$ a) Sei $a \in R \setminus \{0\}$ beliebig, sei $I = (a) \lhd R$ das von a erzeugte Hauptideal. Dann ist der kanonische Restklassenhomomorphismus $\pi : R \to R/(a)$ *nicht* injektiv (da $\ker \pi = (a) \supseteq \{0\}$).
$\overset{c)}{\Rightarrow} |R/(a)| = 1$, d.h. $(a) = I = R \ni 1 \Rightarrow \exists\, r \in R : a \cdot r = 1$, d.h. $a \in R^\times$. $\square$

Übungsbeispiel 46. Warum gibt es (mit Satz 3.15) keinen Ringhomomorphismus $\varphi : \mathbb{R} \to \mathbb{Q}$? (Tipp: welche dieser Mengen ist abzählbar?)

Übungsbeispiel 47. Beweisen Sie die folgende Variante von Satz 3.15:
R ein komm. Ring, $|R| \geq 2$, ist Körper $\Longleftrightarrow \{0\}$ ist maximales Ideal von R.

Satz 3.16. *Sei $(R, +, \cdot)$ ein komm. Ring, $I \lhd R$ ein Ideal. Es gilt:*

a) *I ist maximales Ideal von $R \Leftrightarrow R/I$ ist ein Körper.*
b) *I ist Primideal von $R \Leftrightarrow R/I$ ist ein Integritätsbereich.*
c) *$I \lhd R$ maximal $\Rightarrow I \lhd R$ Primideal* [9].
d) *$\{0\} \lhd R$ Primideal $\Leftrightarrow R$ Integritätsbereich.*
e) *R Hauptidealbereich $\Rightarrow$ jedes nicht triviale Primideal $\{0\} \subsetneq P \lhd R$ ist ein maximales Ideal.*

Beweis. a) Es gilt:

$$\begin{array}{lll} I \lhd R \text{ maximales Ideal} & \overset{\text{Def 3.7 b)}}{\Longleftrightarrow} & \nexists\, Q \lhd R :\ I \subsetneq Q \subsetneq R \\ & \Longleftrightarrow & \Omega := \{Q \lhd R \mid I \subset Q\} = \{I, R\} \\ & \overset{\text{Satz 3.11c)}}{\Longleftrightarrow} & \Omega' := \{\text{Ideale von } R/I\} = \{I, R/I\} \\ & \overset{\text{Satz 3.15}}{\Longleftrightarrow} & R/I \text{ ist ein Körper.} \end{array}$$

(Satz 3.11 c) für $\varphi : R \to R/I$).

b) Für $a, b \in R$ beliebig ist

$$\begin{array}{lll} (a+I)(b+I) = 0 + I & \Longleftrightarrow & ab \in I \\ & \overset{\text{falls } I \text{ Primideal}}{\Longrightarrow} & a \in I \text{ oder } b \in I \\ & \Longrightarrow & a + I = I \text{ oder } b + I = I \\ & \Longrightarrow & R/I \text{ ist Integritätsbereich.} \end{array}$$

[9] Die Umkehrung gilt nicht immer!

und

$$\begin{array}{lll}(a+I)(b+I)=0+I & \Longleftrightarrow & ab\in I\\ & \overset{\text{falls } R/I \text{ Integritätsbereich}}{\Longrightarrow} & a+I=I \text{ oder } b+I=I\\ & \Longrightarrow & a\in I \text{ oder } b\in I\\ & \Longrightarrow & I \text{ ist Primideal.}\end{array}$$

c) $I \lhd R$ max. Ideal $\overset{a)}{\Longrightarrow} R/I$ Körper $\overset{\text{Lemma 3.13b)}}{\Longrightarrow} R/I$ Int. bereich $\overset{b)}{\Longrightarrow} I$ Primideal.

d) $\{0\} \lhd R$ Primideal $\overset{b)}{\Longleftrightarrow} R/\{0\} \cong R$ ist ein Integritätsbereich.

e) Sei $\{0\} \subsetneq P \lhd R$ Primideal und $P \subsetneq Q \lhd R$. Da R ein Hauptidealbereich ist existieren $p \neq 0$, $q \neq 0$ in R mit $P = (p) = pR \subsetneq Q = (q) = qR$.

$p \in P \subset Q$: $\exists\ a \in R$ mit $p = q \cdot a \in P \overset{P \text{ Primideal}}{\Longrightarrow} q \in P$ oder $a \in P$.
Im ersten Fall: $(q) \subset P \Longrightarrow\ (q) = (p)\ \lightning$ zu $P \subsetneq Q$.
Im zweiten Fall: $\exists\ b \in R$ mit $a = bp \Longrightarrow p = qa = qbp$. Da $p \neq 0$ ist, ist p kürzbar, d.h. $1 = q \cdot b$, also $q \in R^\times$ und damit ist $(q) = Q = R$.
Also ist $P = (p)$ ein maximales Ideal. □

Übungsbeispiel 48. Es seien $I_1, I_2 \lhd \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ wie in Übungsbeispiel 42 gegeben. Zeigen Sie, dass beide maximale Ideale sind. Sind sie auch Primideale?
Zeigen Sie, dass für eine Teilmenge $M \subseteq \mathbb{R}$ mit $|M| \geq 2$ das Ideal I_M kein Primideal ist und $\mathrm{Abb}(M, \mathbb{R})$ kein Integritätsbereich ist (mehrere Beweismöglichkeiten).

Beispiel 3.17. Sei $R := \mathrm{Abb}(\mathbb{N}, \mathbb{R}) = \{(a_n)_{n\geq 1} \mid a_n \in \mathbb{R}\}$ der Ring aller reellen Zahlenfolgen. Mittels Strukturtransport (Definition 1.5) definiert man $+, \cdot$ auf Folgen von Zahlen wie in Analysis 1.
R ist ein kommutativer Ring. Die Menge C aller konvergenten reellen Zahlenfolgen ist ein Unterring von R (man benutzt das Unterringkriterium: konvergieren $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$, so konvergiert auch $(a_n - b_n)_{n\in\mathbb{N}}$, sowie $(a_n) \cdot (b_n)$, und die konvergente Folge (1) liegt in C).
Der Grenzwert $\lim : C \to \mathbb{R}$, $(a_n)_{n\in\mathbb{N}} \mapsto \lim_{n\to\infty} a_n$ ist ein Ringhomomorphismus (Rechenregeln für Grenzwerte), surjektiv, also ein Ringepimorphismus.
$\ker(\lim) = \{\text{Nullfolgen}\} =: N \lhd C$.

Mit dem Homomorphiesatz gilt: $C/N \cong \mathbb{R}$, und $\mathbb{R}$ ist ein Körper $\overset{S.3.16a)}{\Longrightarrow} N$ ist maximales Ideal von C.

Beh.: N ist *kein* Hauptideal in C.
Ann.: $\exists\ \mathbf{a} := (a_n)_{n\geq 1} \in C$ eine Nullfolge (i.e. $\lim_{n\to\infty} a_n = 0$) mit $N = (\mathbf{a}) = \mathbf{a}C$.
$\mathbf{h} := (\frac{1}{n})_{n\geq 1} \in N \rightsquigarrow \exists\ \mathbf{c} = (c_n)_{n\geq 1} \in C$ mit $\mathbf{h} = \mathbf{a} \cdot \mathbf{c}$
d.h. $\frac{1}{n} = a_n \cdot c_n$, also sind alle $a_n \neq 0$.
$\lim_{n\to\infty}(-1)^n a_n = 0 \Rightarrow \mathbf{a'} := ((-1)^n a_n)_{n\geq 1} \in N$
dann existiert $\mathbf{c'} = (c'_n)_{n\geq 1} \in C$ mit $\mathbf{a'} = \mathbf{a} \cdot \mathbf{c'}$ und $(-1)^n a_n = a_n c'_n$,
also ist $\mathbf{c'} = ((-1)^n)_{n\geq 1} \in C$, $\lightning$.

Beim Satz 3.18 erwähnen wir nur die Aussage und lassen den Beweis aus.

Satz 3.18. *Sei R ein kommutativer Ring mit $|R| \geq 2$.*
Dann besitzt R maximale Ideale.
Ausserdem gilt:
Ist $I \triangleleft R$ ein Ideal mit $I \neq R$, so existiert ein maximales Ideal $M \triangleleft R$ mit $I \subseteq M$.

Idee vom Beweis. Der Beweis benutzt das Lemma von Zorn, um zu zeigen, dass die Menge der echt in R enthaltenen Ideale maximale Elemente besitzt.
Für den Zusatz benutzt man den kanonischen Homomorphismus $\varphi : R \to R/I$, die Tatsache, dass $|R/I| \geq 2$ ist wegen $I \neq R$, sowie Satz 3.11 c). □

Übungsbeispiel 49. Überlegen Sie mit Hilfe von Beispiel 45, dass der Ring $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ "unendliche lange" Ketten von ineinander enthaltenen Hauptidealen besitzt.

Übungsbeispiel 50. Haben Sie in Ihrem bisherigen Studium vom "Zorn'schen Lemma" gehört? Wurde in der "Linearen Algebra" bewiesen, dass jeder Vektorraum (von beliebig grosser Dimension) eine Basis besitzt? Können Sie sich einen entsprechenden Beweis mit dem Zorn'schen Lemma vorstellen, indem man die Menge $\mathcal{M}$ aller Teilmengen von linear unabhängigen Vektoren eines Vektorraums V mit der Mengeninklusion als Ordnungsrelation versieht?

Definition 3.8. a) Sei $m \in \mathbb{N}$. Die Elemente von $(\mathbb{Z}/(m))^\times$ heissen die *primen Restklassen modulo m* (die Restklassen, die zu m relativ prime Zahlen enthalten). $(\mathbb{Z}/(m))^\times$ ist eine multiplikative Gruppe.
b) Die *Euler'sche Phi-Funktion* φ wird wie folgt definiert:

$$\varphi : \mathbb{N} \to \mathbb{N},\ m \mapsto \varphi(m) := |(\mathbb{Z}/(m))^\times|$$

Offenbar ist $\varphi(m) = |\{k \in \mathbb{N} \mid 1 \leq k \leq m \text{ und } \mathrm{ggT}(k, m) = 1\}|$. Insbesondere: $\varphi(p) = p - 1$ für $p \in \mathbb{P}$.

Eigenschaften ausgelassen in der Vorlesung
a) Für $p \in \mathbb{P}$, $n \in \mathbb{N}$ ist $\varphi(p^n)p^{n-1}(p-1) = p^n(1 - \frac{1}{p})$
b) Gilt $\mathrm{ggT}(m, n) = 1$ für $m, n \in \mathbb{N}$, so ist $\varphi(mn) = \varphi(m)\varphi(n)$.
c) Ist $m \in \mathbb{N}$, $m = \prod_{i=1}^r p_i^{e_i}$ die Primfaktorzerlegung von m, so ist

$$\varphi(m) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = m \cdot \prod_{i=1}^{r}(1 - \frac{1}{p_i})$$

(b) und c) sind Korollare vom chin. Restsatz, siehe weiter unten) (mit chin. Restsatz: $\mathrm{ggT}(m, n) = 1$ genau dann, wenn $(m) + (n) = \mathbb{Z}$. $\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ und $(\mathbb{Z}/(mn))^\times \cong (\mathbb{Z}/(m))^\times \times (\mathbb{Z}/(n))^\times$ (Isomorphismus als multiplikative Gruppen).

3.4. **Chinesischer Restsatz.** [Vorlesung 18, 16.6. 2014]

Definition 3.9. Sei R ein kommut. Ring, $I, J \triangleleft R$. Dann heissen I und J *koprim* oder *zueinander teilerfremd*, falls $I + J = R$ ist.

Satz 3.19 und die nachfolgende Bemerkung wurden in der Vorlesung aus Zeitgründen nicht besprochen

Satz 3.19. *Sei R ein kommut. Ring, $n \in \mathbb{N}$, $I_1, \dots, I_n \triangleleft R$ paarweise teilerfremde Ideale. Für $1 \leq j \leq n$ sei $\pi_j : R \to R/I_j$ die kanonische Projektion auf den Restklassenring modulo I_j. Dann ist die Abbildung*

$$\begin{aligned} \pi : R &\to R/I_1 \times \cdots \times R/I_n \\ a &\mapsto (\pi_1(a), \dots, \pi_n(a)) = (a + I_1, \dots, a + I_n) \end{aligned}$$

ein Ringepimorphismus mit $\ker(\pi) = \bigcap_{j=1}^n I_j$*, also insbesondere*

$$R/\cap_{j=1}^n I_j \cong \prod_{j=1}^n (R/I_j)$$

Bemerkung. • Falls $n = 1$ ist, so ist die Aussage des Satzes trivial.
• In Satz 3.19 wird das äussere direkte Produkt der Ringe R/I_j verwendet. Dies ist definiert wie für Verknüpfungsgebilde in Definition 1.3, mit komponentenweise definierten Operationen $+$ und $\cdot$. Das Nullelement ist $(0_{R/I_1}, \dots, 0_{R/I_n}) = (I_1, \dots, I_n)$, das Neutralelement $(1_{R/I_1}, \dots, 1_{R/I_n}) = (1_R + I_1, \dots, 1_R + I_n)$.
• Da die I_j koprim sind, folgt; $\cap_{j=1}^n I_j = \prod_{j=1}^n I_j$ (z.B. in [JS] Satz 3.10, Seite 76).

Beweis. Zuerst mal zeigt man, dass π ein Ringhomomorphismus ist, da die π_j alle Ringhomomorphismen sind. (selber tun)
Beh.: I_j und $\cap_{\substack{k \neq j \\ 1 \leq k \leq n}} I_k$ sind koprim ($1 \leq j \leq n$ beliebig).
Bew.Beh.: Wir wissen: $I_j + I_k = R$ für alle $k \neq j$. D.h. es existieren $x_k \in I_j$ und $a_k \in I_k$ mit $x_k + a_k = 1$ (für $k = 1, \dots, n$, $k \neq j$).

$$\Longrightarrow 1 = \prod_{\substack{k=1 \\ k \neq j}}^n (x_k + a_k) \overset{\text{ausmult, sortieren}}{=} \underbrace{\left(\begin{array}{l} \text{alle Produkte,} \\ \text{die mind. ein} \\ x_k \text{ enthalten} \end{array} \right)}_{\in I_j (\text{da die } x_k \text{ alle in } I_j \text{ liegen})} + \underbrace{a_1 \cdot a_2 \cdots a_{j-1} a_{j+1} \cdots a_n}_{\in I_1 \cdots I_{j-1} \cdot I_{j+1} \cdots I_n \subseteq \cap_{k \neq j} I_k}$$

$\Longrightarrow$ Bew. Beh.✓

Mit dieser Beh. folgt: Für jedes $j \in \{1, \dots, n\}$ existieren $d_j \in I_j$ und $e_j \in \cap_{\substack{1 \leq l \leq n \\ l \neq j}} I_l$ mit $d_j + e_j = 1$.
Betrachten $\pi(e_j)$. Dazu müssen wir die $\pi_k(e_j)$ beschreiben:
Für $k \in \{1, \dots, n\}$ ist

$$\pi_k(e_j) = \begin{cases} 0 + I_k & \text{für } k \neq j \text{ (da } e_j \in I_k \text{ nach Wahl)} \\ \pi_j(1 - d_j) = 1 + I_j & \text{für } j = k. \end{cases}$$

und damit folgt $\pi(e_j) = (0 + I_1, \dots, 0 + I_{j-1}, 1 + I_j, 0 + I_{j+1}, \dots, 0 + I_n)$.

Damit hat man sofort die Surjektivität von π aus der Surjektivität der π_k: Für $y = (y_1, \dots, y_n) \in R/I_1 \times \cdots \times R/I_n$ wählt man $x_k \in R$ mit $y_k = x_k + I_k$ (die π_k

sind surj.). Und dann setzt man $x := \sum x_j e_j$, das erfüllt $\pi(x) = y$, da für jedes $1 \leq k \leq n$ gilt: $\pi_k(x) = y_k$.
Zum Kern von π:

$$\ker(\pi) = \{x \in R \mid \pi(x) = (x+I_1, \ldots, x+I_n) \overset{(*)}{=} (0+I_1, 0+I_2, \ldots, 0+I_n)\} = \cap_{j=1}^n I_j$$

wobei Gleichheit in $(*)$ gilt $\Leftrightarrow (x \in I_1) \cap (x \in I_2) \cap \cdots \cap (x \in I_n)$ ist und das zeigt die letzte Gleichheit.
Mit dem Homomorphiesatz, Satz 3.11, folgt dann

$$R/\ker(\pi) \cong \operatorname{im}\pi, \quad \text{die letzte Beh. im Satz.}$$

□

Korollar 3.20 (Chinesischer Restsatz für Kongruenzen)**.** *Mit den Voraussetzungen von Satz 3.19 gilt:*
Sind $a_1, \ldots, a_n \in R$ beliebig gegeben, so existieren[10] *$x \in R$, die*

$$x \equiv a_j \mod I_j$$

erfüllen für alle $j \in \{1, \ldots, n\}$, und alle diese x bilden genau eine Restklasse von $R/\cap_{j=1}^n I_j$.

Beweis. Alle solchen x liegen in $\pi^{-1}(\{(a_1 + I_1, \ldots, a_n + I_n)\})$. □

Spezialfall zum Korollar: $R = \mathbb{Z}$, $I_1 = (m_1)$, $\ldots$, $I_n = (m_n)$ mit m_i paarweise teilerfremd $\Longleftrightarrow \operatorname{ggT}(m_i, m_j) = 1$ für alle $i \neq j$.
Dann sagt das Korollar: Für alle $a_1, \ldots, a_n \in \mathbb{Z}$ ist das Kongruenzensystem

$$x \equiv a_1 \mod m_1,\ x \equiv a_2 \mod m_2, \ldots,\ x \equiv a_n \mod m_n$$

lösbar. Die Lösungsmenge ist eine Restklasse modulo $\cap_{j=1}^n (m_j) = (M)$ für $M := m_1 \cdots m_n$.

Wie man z.B. auf Wikipedia nachlesen kann, wird der chinesische Restsatz (jedenfalls in der Version für Zahlen und simultanen Kongruenzen) dem chinesischen Mathematiker Sun Zi zugeschrieben, der im 3. Jahrhundert gelebt haben soll.

Zwei illustrierende Beispiele zu dieser Version findet man auf den Seiten 47,48 in den Vorlesungsnotizen von F. Fontein, siehe [Fo].

4. Polynomringe

Sei R ein kommutativer Ring. Notation: Ist $R \leq S$ ein Unterring von S, so sagt man, S sei eine Ringerweiterung von R. Wir betrachten in diesem Kapitel Polynomringe über R, als wichtiges Beispiel von Ringerweiterungen. $R[X]$ sei die Menge aller Polynome einer Variablen X über R.

[10] eines oder mehrere

Es seien $R^{(\mathbb{N}_0)}$ (dies ist eine Teilmenge vom Ring $\mathrm{Abb}(\mathbb{N}_0, R)$ der Abbildungen von $\mathbb{N}_0$ nach R) die Abbildungen $f : \mathbb{N}_0 \to R$, für die gilt: $f(i) = 0$ für fast alle $i \in \mathbb{N}_0$. Wir definieren $R[X] := R^{(\mathbb{N}_0)}$ als Menge.

Zur Ringstruktur von $R^{(\mathbb{N}_0)}$: Wir können eine Abbildung $f : \mathbb{N}_0 \to R$ mit der zugehörigen Folge $(f(i))_{i\in\mathbb{N}_0}$ der Bilder in R identifizieren, damit haben wir:

$$R^{(\mathbb{N}_0)} = \{(a_i)_{i\in\mathbb{N}_0} \mid a_i \in R, a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$$

Darauf definieren wir nun Addition und Multiplikation, um eine Ringstruktur zu erhalten. Seien $(a_i) = (a_i)_{i\in\mathbb{N}_0}$, $(b_i) = (b_i)_{i\in\mathbb{N}_0}$ zwei Elemente von $R^{(\mathbb{N}_0)}$. Die Addition ist dieselbe wie für $\mathrm{Abb}(\mathbb{N}_0, R)$:

$$(a_i) + (b_i) \quad := \quad (a_i + b_i)$$

Die Multiplikation wird jedoch nicht komponentenweise definiert, sondern wie bei der Multiplikation von polynomialen Funktionen:

$$(a_i) \cdot (b_i) := (c_i) \qquad \text{für } c_i := \sum_{\mu+\nu=i} a_\mu b_\nu.$$

Mit diesen Verknüpfungen bildet $R^{(\mathbb{N}_0)}$ einen Ring. Nullelement ist die Nullfolge $(0, 0, \dots)$, das Neutralelement bzgl. der Multiplikation ist $(1, 0, 0, \dots)$.

Damit definiert man $R[X] := R^{(\mathbb{N}_0)}$ und nennt dies den *Ring der Polynome in einer Variablen X über R*. Anschaulicher wird das, wenn man die übliche Schreibweise verwendet, d.h. wenn man $(a_i) \in R[X]$ als

$$\sum_{i\in\mathbb{N}_0} a_i X^i \quad \text{oder} \quad \sum_{i=0}^{n} a_i X^i,$$

wobei n genügend gross ist, dass $a_i = 0$ gilt für $i > n$. Die Variable X muss man als die Folge $(0, 1, 0, 0, \dots)$ auffassen. In der Polynomschreibweise sind dann Addition und Multiplikation wie gewohnt durch folgende Formeln gegeben:

$$\begin{aligned} \sum_i a_i X^i + \sum_i b_i X^i &= \sum_i (a_i + b_i) X^i \\ \sum_i a_i X^i \cdot \sum_i b_i X^i &= \sum_i (\sum_{k+l=i} a_k \cdot b_l) X^i \end{aligned}$$

Wie anfangs Kapitel geht es hier um das Beispiel einer Ringerweiterung. D.h., dass R ein Unterring von $R[X]$ sein sollte. Das erreicht man, indem man R als die konstanten Polynome in $R[X]$ auffasst, also indem man R mit seinem Bild unter der Abbildung $\varphi : R \hookrightarrow R[X]$, $a \mapsto aX^0$, identifiziert. Diese Abbildung ist ein injektiver Ringhomomorphismus (bitte selber überprüfen: φ ist Ringhomomorphismus, φ ist injektiv!).

Definition 4.1. Sei $f = \sum a_i X^i \in R[X]$ ein Polynom über R.
Ist $f \neq 0$ (verschieden vom Nullpolynom), dann ist der *Grad von f* definiert durch

$$\deg f := \max\{i \mid a_i \neq 0\}$$

Bemerkung. a) Dem Nullpolynom $0 \in R[X]$ wird der Grad $-\infty$ zugeordnet.
b) Ist $\deg f = n \geq 0$, $f = \sum a_i X^i$, so heisst a_n der *höchste Koeffizient* oder *Leitkoeffizient* von f. Ist der Leitkoeffizient von f gleich 1, so heisst f *normiert*.

Der Polynomgrad hat die folgenden Eigenschaften:

Lemma 4.1. *Sei $R[X]$ der Polynomring in einer Variablen X über einem Ring R. Für $f, g \in R[X]$ gilt dann:*

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg f, \deg g\} \\ \deg(f \cdot g) &\leq \deg f + \deg g \end{aligned}$$

Ist R ein Integritätsbereich, so gilt Gleichheit: $\deg(f \cdot g) = \deg f + \deg g$.

Beweis. Ist f oder g das Nullpolynom, so sind die Behauptungen sicher richtig. Seien also $m := \deg f \geq 0$ und $n := \deg g \geq 0$, $f = \sum a_i X^i$, $g = \sum b_i X^i$. Dann ist $a_i + b_i = 0$ für $i > \max\{m, n\}$, also ist $\deg(f+g) \leq \max\{m, n\}$.

Für die zweite Behauptung: es ist $\sum_{a_k + b_l = i} a_k b_l = 0$ falls $i > k + l$ ist, also $\deg(f \cdot g) \leq m + n$.

Falls R ein Integritätsbereich ist, so ist das Produkte $a_m \cdot b_n \neq 0$ (da die beiden höchsten Koeffizienten ja nicht verschwinden, i.e. $a_m \neq 0$ und $b_n \neq 0$), also verschwindet der Koeffizienten $\sum_{k+l=m+n} a_k b_l = a_m b_n$ von $f \cdot g$ vom Grad $m + n$ nicht und somit ist $\deg(f \cdot g) = m + n$. □

Bemerkung. Ist R ein Integritätsbereich, so ist auch $R[X]$ ein Integritätsbereich. Um dies zu sehen, benutze man die Formel $\deg(f \cdot g) = \deg f + \deg g$ aus Lemma 4.1.

Wichtig ist das folgende Resultat, das zeigt, dass in Polynomringen ein analoger Satz wie die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ gilt.

Satz 4.2 (Division mit Rest)**.** *Sei R ein Ring und $g = \sum_{i=0}^{d} a_i X^i \in R[X]$ ein Polynom, dessen höchster Koeffizient a_d eine Einheit*[11] *in R ist, $d \geq 0$. Dann gibt es zu jedem Polynom $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$ mit*

$$f = qg + r, \quad \deg r < d, \qquad (*)$$

Beweis. Zuerst: Aus der Voraussetzung, dass der höchste Koeffizient a_d von g eine Einheit ist, folgt $\deg(qg) = \deg q + \deg g$, auch wenn R kein Integritätsbereich ist: Ist q vom Grad $n \geq 0$ mit Leitkoeffizient c_n, so ist $c_n a_d \neq 0$. Das ist der Leitkoeffizient von qg, also gilt $\deg(qg) = n + d$.

Zur Eindeutigkeit der Division mit Rest: Hat f zwei Darstellungen der Art $(*)$, $f = qg + r = q'g + r'$, so folgt:

$$\deg(q - q') + \deg g = \deg(r' - r)$$

nach der obigen Überlegung. Nun haben r und r' Grad $< d$, also ist $\deg(r' - r) < d$, also $\deg(q - q') + \deg g < d$. Da $\deg g = d$ ist, kann diese Ungleichung nur für

[11] Einheiten von R sind invertierbare Elemente bzgl. der Multiplikation.

$q - q' = 0$ (das Nullpolynom) richtig sein. Aus $q = q'$ folgt aber $r = r'$, die Eindeutigkeit der Division mit Rest.

Zur Existenz der Division mit Rest: dies zeigt man mit Induktion über $n = \deg f$. Für $\deg f < d$ setzt man $q = 0$ und $r = f$. Ist $f = \sum_{i=0}^{n} c_i X^i$ mit $n \geq d$ und $c_n \neq 0$, so ist

$$f_1 := f - c_n a_d^{-1} X^{n-d} g$$

ein Polynom mit $\deg f_1 < n$. Nach Induktionsvoraussetzung besitzt f_1 eine Darstellung $f_1 = q_1 g + r_1$ mit Polynomen $q_1, r_1 \in R[X]$, $\deg r_1 < d$. Dann erhält man die gewünschte Zerlegung:

$$f = (q_1 + c_n a_d^{-1} X^{n-d}) g + r_1.$$

□

Bemerkung. Man kann anstatt wie in der Definition von $R[X]$ den Ring $R^{(\mathbb{N}_0)}$ durch $\mathrm{Abb}(\mathbb{N}_0, R)$ ersetzen, die Menge *aller* Abbildungen von $\mathbb{N}_0$ nach R. Dann erhält man anstatt $R[X]$ den Ring $R[[X]]$ der *formalen Potenzreihen* in einer Variablen X über R. Das sind die unendlichen Reihen $\sum_{i=0}^{\infty} a_i X^i$.

Polynomringe in mehreren Veränderlichen Polynomringe in mehreren Veränderlichen können rekursiv definiert werden durch

$$R[X_1, \ldots, X_n] := R[X_1, \ldots, X_{n-1}][X_n],$$

d.h. man betrachtet Polynome in der Variablen X_n mit Koeffizienten aus dem Polynomring $R[X_1, \ldots, X_{n-1}]$. Jedes Element von $R[X_1, \ldots, X_n]$ lässt sich eindeutig schreiben als

$$\sum_{(k_1,\ldots,k_n) \in \mathbb{N}_0^n} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$$

Man kann Polynomringe über beliebig vielen Unbestimmten definieren, siehe z.B. Kapitel 6 von [L] oder Kapitel 2.5 in [Bo].
[Vorlesung 19, 23.6. 2014]

Definition 4.2. Ein Integritätsbereich R heisst ein *euklidischer Ring*, falls eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}_0$ (die *Gradabbildung* oder *euklidische Norm*) existiert mit folgenden Eigenschaften:
Zu beliebigen Elementen $a, b \in R$ mit $b \neq 0$ existieren $q, r \in R$ mit

$$a = q \cdot b + r$$

und, falls $r \neq 0$ ist, $\delta(r) < \delta(b)$.

Beispiele.
- Jeder Körper ist ein euklidischer Ring (Wahl: $q = ab^{-1}$, $r = 0$, δ beliebig).
- $\mathbb{Z}$ ist euklidisch: $\delta : \mathbb{Z} \to \mathbb{N}_0$, $k \mapsto |k|$, "Division mit Rest"

- $R := \mathbb{Z}[i] := \{x + iy \mid x, y \in \mathbb{Z}\} \leq \mathbb{C}$ (wobei $i^2 = -1$), der Ring der Gauss'schen Zahlen (ist ein Unterring von $\mathbb{C}$: selber überprüfen).
  Beh.: Die Abbildung $\delta : R \to \mathbb{N}_0$, $x + iy \mapsto [x + iy|^2 = x^2 + y^2$ ist eine euklidische Norm.
  Seien $a = u + iv$, $b = r + is \neq 0$ zwei Elemente von R. Zur komplexen Zahl $\frac{a}{b}$ gibt es eine Zahl $q := x + iy$, $x, y \in \mathbb{Z}$ mit

$$|x - \mathrm{Re}(\frac{a}{b})| \leq \frac{1}{2}, \quad |y - \mathrm{Im}(\frac{a}{b})| \leq \frac{1}{2}$$

$$\implies \frac{a}{b} = q + z \text{ mit } |z|^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$$
$$\implies a = qb + \underbrace{zb}_{:=r\in\mathbb{Z}[i]} \text{ und, falls } r \neq 0 \text{ ist:}$$

$$|r|^2 = |z|^2|b|^2 \leq \frac{1}{2}|b|^2 < |b|, \text{ also } \delta(r) < \delta(b)$$

- k ein Körper. Dann ist der Polynomring $k[X]$ mit der üblichen Polynomdivision mit Rest (Satz 4.2) ein euklidischer Ring, mit der Gradabbildung δ aus 4.1.

Satz 4.3. *Jeder euklidische Ring ist ein Hauptidealbereich.*

Beweis. R sei euklidischer Ring, $\delta : R \setminus \{0\} \to \mathbb{N}_0$ eine euklidische Norm. Sei $I \triangleleft R$, o.E. sei $I \neq (0)$. Wähle $0 \neq b \in I$ mit $\delta(b) = \min\{\delta(x) \mid x \in I \setminus \{0\}\}$. Für jedes $x \in I$ erhalten wir: $\exists\ q, r \in R$: $x = qb + r$ und $r = 0$ oder $\delta(r) < \delta(b)$. Aus der Gleichung $x = qb + r$ folgt $r = x - qb \in I$, denn $x \in I$, $b \in I$. Nach der Wahl von b kann $\delta(r) < \delta(b)$ nicht auftreten, d.h. es ist $r = 0$ und damit $x = qb$ (mit $x \in I$ beliebig). Also ist $I = b \cdot R = (b)$ ein Hauptideal. □

4.1. **Teilbarkeit in Ringen.** Ab jetzt hält sich die Vorlesung eng an die Skripten [Fr] von C. Frei zur Algebra und an [Ba] zur Algebra I.

Definition 4.3. Sei R ein kommut. Ring, seien $a, b, c, p \in R$.
1) Man sagt, a teilt b, geschrieben $a \mid b$, wenn es ein $d \in R$ gibt mit $ad = b$. Dann heisst a ein *Teiler von* b und b ein *Vielfaches von* a.
2) Ein Element $c \in R$ heisst *irreduzibel*, wenn $c \neq 0$ ist und c keine Einheit ist und aus $c = ab$ folgt, dass a eine Einheit ist oder b eine Einheit ist.
3) $p \in R$ heisst *prim*, wenn $p \neq 0$ ist, p keine Einheit ist und aus $p \mid ab$ folgt: $p \mid a$ oder $p \mid b$.
4) Ein Element $a \in R$ heisst zu $b \in R$ *assoziiert*, falls $a = bu$ ist für eine Einheit $u \in R$.

Bemerkung. 1) Es ist $2 \mid 6 \in \mathbb{Z}$, $2 \nmid 3 \in \mathbb{Z}$, aber $2 \mid 3 \in \mathbb{Q}$.
2) Die Null wird durch jedes $a \in R$ geteilt, denn $a \cdot 0 = 0$. Wegen $1 \cdot a = a$ ist $1 \mid a$ $\forall\ a \in R$. Ausserdem teilt jede Einheit b von R jedes Ringelement a: $b(b^{-1}a) = a$,

also $b \mid a$. Und a ist eine Einheit von $R \iff a \mid 1$.
3) Es gilt:

(*i*) a ist assoziiert zu b genau dann, wenn b assoziiert ist zu a.

(*ii*) Jedes Element $a \neq 0$ von R ist durch all seine Assoziierten teilbar.

Das sieht man so: Zu u existiert ein Inverses, sei das v, v ist auch Einheit. Nun multipliziert man beide Seiten von $a = bu$ mit v und erhält $av = buv = b1_R = b$.

Satz 4.4. *Sei R ein kommutativer Ring, $p \in R$ prim, p kein Nullteiler. Dann ist p irreduzibel.*

Beweis. Sei $p = ab$, also teilt p sicher ab und damit $p \mid a$ oder $p \mid b$. O.E. gelte ersteres. Also gibt es ein $c \in R$ mit $pc = a$. Damit gilt $p = ab = pcb$, also $p(1 - cb) = 0$. Da p kein Nullteiler ist, gilt $1 = cb$ und b ist eine Einheit. □

Als direkte Folge von Satz 4.4 sind in einem Integritätsbereich prime Elemente immer irreduzibel. Es ist jedoch nicht so, dass irreduzible Elemente immer prim sind, wie das folgende Beispiel zeigt.

Beispiel. Sei $\mathrm{Int}\mathbb{Z} := \{f \in \mathbb{Q}[X] \mid f(a) \in \mathbb{Z} \ \forall\, a \in \mathbb{Z}\}$ der Ring der ganzwertigen Polynome in X über $\mathbb{Q}$, es ist $\mathbb{Z}[X] \subsetneq \mathrm{Int}\mathbb{Z} \subsetneq \mathbb{Q}[X]$. In diesem Ring sind 2 und X irreduzibel, sie sind aber beide nicht prim:

- 2 ist irreduzibel: ist $2 = ab \in \mathbb{Q}[X]$, so sind $a, b \in \mathbb{Q}$. Und $\mathbb{Q} \cap \mathrm{Int}\mathbb{Z} = \mathbb{Z}$, also sind $a, b \in \mathbb{Z}$. Damit ist $a \in \{\pm 1\}$ oder $b \in \{\pm 1\}$.
- 2 ist nicht prim: 2 teilt $X(X-1)$, denn $X(X-1) = 2\frac{X(X-1)}{2}$ (und der zweite Faktor ist in $\mathrm{Int}\mathbb{Z}$), aber $2 \nmid X$, $2 \nmid (X-1)$, da $\frac{X}{2} \notin \mathrm{Int}\mathbb{Z}$ und $\frac{X-1}{2} \notin \mathrm{Int}\mathbb{Z}$.
- X ist irreduzibel: Ist $X = ab \in \mathrm{Int}\mathbb{Z} \subsetneq \mathbb{Q}[X]$, dann muss $1 = \deg X = \deg a + \deg b$ sein. Also kann man annehmen, $a = \frac{c_1}{d_1}X$ und $b = \frac{c_2}{d_2}$ mit $c_i, d_i \in \mathbb{Z}$. Weil wir in $\mathrm{Int}\mathbb{Z}$ sind, folgt $b \in \mathbb{Z}$ und $a = cX$ mit $c \in \mathbb{Z}$. Also hat man $X = ab = cbX$, d.h. $cb = 1$, und damit ist $b \in \{\pm 1\}$, eine Einheit (und $c \in \{\pm 1\}$
- X ist nicht prim: X teilt $X(X-1)$ und dies ist gleich $2\frac{X(X-1)}{2}$, aber $X \nmid 2$ (klar) und $X \nmid \frac{X(X-1)}{2}$ (weil $\frac{X-1}{2} \notin \mathrm{Int}\mathbb{Z}$).

Satz 4.5. *Sei R ein Integritätsbereich. Dann gilt:*
(1) $p \in R$ prim $\iff (p) \lhd R$ ist ein Primideal $\neq \{0\}$.
(2) $c \in R$ ist irreduzibel $\iff \{0\} \neq (c) \neq R$ und (c) ist maximal unter den Hauptidealen.

4.2. **Ringe mit eindeutiger Primfaktorzerlegung, UFD-Ringe.**

Definition 4.4. Ein Integritätsbereich R heisst *faktoriell* oder ein *UFD* (unique factorisation domain), falls jedes Element $a \neq 0$ von R, das keine Einheit ist ein Produkt von irreduziblen Elementen

$$a = p_1 p_2 \cdots p_n, \ n \geq 1 \tag{1}$$

ist[12], wobei diese Faktorisierung eindeutig ist bis auf Assoziiertheit. Ist also

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

wobei die p_i und q_j alle irreduzibel sind, so gilt $r = s$ und

$$p_i \text{ ist zu } q_i \text{ assoziiert zu } i = 1, \ldots, r.$$

(falls nötig nummeriert man dazu die q_i zuerst um).

Diese Definition beinhaltet offenbar zwei Bestandteile: Die Existenz von Faktorisierungen und deren Eindeutigkeit.

Lemma 4.6. *Sei R ein Integritätsbereich. Wenn in R jede aufsteigende Kette von Hauptidealen*

$$(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$$

nur endlich viele Ideale enthält[13]*, dann besitzt jedes Element $b \neq 0$ von R, das keine Einheit ist, eine Faktorisierung (1) in $n \geq 1$ irreduzible Elemente.*

Beweis. Hier nur die Beweisidee in der Vorlesung gemacht.
Sei

$$S := \{a \in R \mid a \neq 0, a \text{ keine Einheit und } a \text{ besitzt keine Darstellung wie in (1)}\}.$$

Zu zeigen ist, dass $S = \varnothing$ ist. Angenommen, dies ist nicht der Fall, sei $a \in S$. Wegen $a \in S$ ist a nicht irreduzibel, es ist also $a = bc$ mit $b, c \in R$ und a ist weder assoziiert zu b noch zu c, b und c sind beide keine Einheiten.

Es ist $a \neq 0$, also $bc \neq 0$. Wären b und c Produkte von irreduziblen Elementen, so hätte a eine Darstellung (1). Also ist $b \in S$ oder $c \in S$.

Damit lässt sich nun eine Folge von Hauptidealen $(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$ mit $a_i \in S$ konstruieren: Sei $a_0 = a$, für $i > 0$ sei $a_i \in S$ ein Element mit (i) $a_i \mid a_{i-1}$ und mit (ii) a_i nicht assoziiert zu a_{i-1}. Dies ergibt eine aufsteigende Folge von Hauptidealen

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

im Widerspruch zur Voraussetzung, dass R die ACC für Hauptideale besitzt. Also besitzt jedes $a \neq 0$, a keine Einheit, eine Darstellung (1). □

[Vorlesung 20, 26.6. 2014]

Satz 4.7. *Sei R ein Integritätsbereich. Dann ist R faktoriell genau dann, wenn die folgenden Bedingungen beide erfüllt sind:*
(1) R erfüllt die ACC für Hauptideale
(2) Jedes irreduzible Element von R ist prim.

[12]Dabei erlauben wir ein Produkt mit genau einem Element, d.h. wir erlauben, dass das Element selbst irreduzibel ist.

[13]Man sagt dann, R erfülle die *aufsteigende Kettenbedingung für Hauptideale* oder die *ACC(=Ascending Chain Condition) für Hauptideale.*

Beweis. Die Implikation "faktoriell" $\Longleftarrow$ (1) und (2):
Wegen Lemma 4.6 impliziert (1) die Existenz von Faktorisierungen in R.
Es gelte (2). Wir zeigen, dass die Faktorisierungen dann eindeutig sind. Seien $c_1, \dots, c_n, d_1, \dots, d_m$ irreduzibel mit

$$c_1 \cdots c_n = d_1 \cdots d_m$$

Dabei sei o.E. $n \leq m$. Die c_i und d_j sind alle prim wegen (2). Da c_1 prim ist, muss c_1 eines der d_j Teilen. O.E. sei dies das erste, d.h. o.E. gelte $c_1 \mid d_1$, also $d_1 = c_1 \cdot u_1$ für ein $u_1 \in R$. Da d_1 irreduzibel ist, muss u_1 eine Einheit sein (c_1 ist ja keine Einheit). Durch Kürzen von c_1 erhält man

$$c_2 \cdots c_n = (u_1 d_2) d_3 \cdots d_m$$

Dasselbe kann man nun für c_2 tun und erhält $c_2 = u_2 d_2$ mit u_2 eine Einheit (allenfalls müssen die d_j zuerst umnummeriert werden). Sukzessive erhält man damit: c_i ist assoziiert zu d_i, $i = 1, \dots, n$. Wäre $m > n$, so hätte man $1 = u_1 u_2 \cdots u_n d_{n+1} \cdots d_m$. Daraus folgte, dass für $j > n$ die d_j Einheiten sind. Also muss $n = m$ gelten.

Implikation "faktoriell" $\Longrightarrow$ (1) und (2):
Beh.: Eine aufsteigende Kette $(a_0) \subseteq (a_1) \subseteq \dots$ von Hauptidealen entspricht einer absteigenden Kette $a_0, a_1, \dots$ von Teilern, d.h. $\dots |a_n| a_{n-1}| \dots | a_1 \mid a_0$.
Bew.Beh.:
Es ist (i) $a \mid b \Leftrightarrow (b) \subseteq (a)$
(ii) a ist assoziiert zu $b \Leftrightarrow (b) = (a)$
bzw. es gilt $a \mid b$ *und* a und b nicht assoziiert $\Leftrightarrow (b) \subsetneq (a)$.

Jedes a_i teilt a_0 und a_0 hat nur endlich viele nicht assoziierte Teiler, also gibt es nur endlich viele verschiedene Hauptideale unter den (a_i). Damit erfüllt R die ACC für Hauptideale.

Es bleibt zu zeigen, dass die irreduziblen Elemente alle prim sind: Sei c irreduzibel, sei $c = ab$. Also existiert ein $d \in R$ mit $cd = ab$. Zerlegt man a, b, d in irreduzible Faktoren, so erhält man

$$cd_1 \cdots d_n = a_1 \cdots a_m b_1 \cdots b_k = a_1 \cdots a_m a_{m+1} \cdots a_{k+m}$$

für $n, m, k \geq 1$ und mit $a_{i+k} := b_i$. Da R faktoriell ist, existiert ein i, $1 \leq i \leq k+m$ mit der Eigenschaft, dass c assoziiert ist zu a_i. O.E. sei c assoziiert zu a_i für ein $i \leq m$, dann haben wir $c \mid a_i$ und $a_i \mid a$ (denn aus $r \mid s$ und $s \mid t$ folgt immer $r \mid t$), also $c \mid a$, c ist damit prim. □

Satz 4.8. *Jeder Hauptidealbereich ist faktoriell.*

Ideen zum Beweis. Man zeigt, (1) dass Hauptidealbereiche die ACC für (beliebige) Ideale erfüllen und (2), dass jedes irreduzible Element in einem Hauptidealbereich prim ist Dann folgt die Behauptung mit Satz 4.7. □

Die Sätze 4.3 und 4.8 liefern dann sofort:

Korollar 4.9. *Jeder euklidische Ring ist faktoriell. Insbesondere sind $\mathbb{Z}$ und $K[X]$ (Polynomring in X über einem Körper K) faktoriell.*

Literatur

[Ba] Karin Baur, *Algebra I*, WS 2013/2014.

[Bo] Siegfried Bosch, *Algebra*, Springer, 1993

[Fo] Felix Fontein, *Einführung in die Algebra*, Vorlesung, Herbstsemester 2011, Universität Zürich, `http://www.math.uzh.ch/aa/index.php?file&key1=19131&no_cache=1`

[Fr] Christopher Frei, *Algebra*, Vorlesungsskriptum, TU Graz, WS 2007/2008, `http://blah.math.tu-graz.ac.at/~frisch/lehr/alg/07/FreiAlgskrMarch2008.pdf`

[JS] Jens Carsten Jantzen, Joachim Schwermer, *Algebra*, Springer, 2005.

[L] Günter Lettl, Vorlesung Einführung in die Algebra, Sommersemester 2010, siehe `http://www.uni-graz.at/~lettl/lehre/einfalgebra-s10.html`