§1 Gruppen, Ringe, Körper

1. Definition Sei H eine nichtleere Menge. Eine Abbildung $H \times H \to H$ nennt man eine Verknüpfung auf H.

Bsp $H = \mathbb{Z}$. Dann sind

(a) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a,b) \longmapsto a+b$

(b) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a,b) \longmapsto a \cdot b$

(c) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a,b) \longmapsto a-b$

Verknüpfungen auf $\mathbb{Z}$.

Verknüpfungen werden oft mit den Symbolen $*$, $+$, $\cdot$ oder $\sqcup$ (nichts) bezeichnet, also $a*b$, $a+b$, $a\cdot b$ oder ab.

Ist $*$ eine Verknüpfung auf H, so nennt man $*$ assoziativ, wenn für alle $x,y,z \in H$ gilt

$$(x*y)*z = x*(y*z)$$

<u>Bsp</u> $+$ und $\cdot$ wie in (a) und (b) sind assoziative Verknüpfungen auf $\mathbb{Z}$, dagegen ist $-$ <u>nicht</u> assoziativ, z.B.

$$1-(1-1) = 1$$
$$(1-1)-1 = -1$$

Wenn $*$ eine assoziative Verknüpfung ist, dann nennt man das Paar $(H, *)$ eine <u>Halbgruppe</u>. Also sind $(\mathbb{Z}, +)$ und $(\mathbb{Z}, \cdot)$ Halbgruppen, aber $(\mathbb{Z}, -)$ ist keine Halbgruppe.

Ein Element $e \in H$ heißt <u>Neutralelement</u> der Verknüpfung $*$, wenn für alle $x \in H$ gilt $e * x = x = x * e$.

<u>Bsp</u>: 0 ist Neutralelement in $(\mathbb{Z}, +)$
1 ist Neutralelement in $(\mathbb{Z}, \cdot)$

Eine Halbgruppe mit Neutralelement nennt man auch <u>Monoid</u> oder <u>Halbgruppe mit Eins</u>.

2. Weitere Beispiele von Halbgruppen

- $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{N},+)$ jeweils mit Neutralelement 0
- $(\mathbb{R},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{N},\cdot)$ jeweils mit Neutralelement 1.
- Ist X eine nicht leere Menge, so bildet die Menge $H = \{f : X \to X\}$ aller Abbildungen von X nach X eine Halbgruppe bezüglich der Komposition von Abbildungen als Verknüpfung. Die identische Abbildung id_X ist das Neutralelement.
- Für $a \in \mathbb{Z} - \{0\}$ und $b \in \mathbb{Z}$ sei $T(a,b) : \mathbb{Z} \to \mathbb{Z}$ die Abbildung $T(a,b)(x) = ax + b$. Es gilt

$$T(1,0)(x) = x \quad \text{, also } T(1,0) = id_{\mathbb{Z}}$$

$$T(a,b) \circ T(c,d)(x) = T(a,b)(cx+d)$$
$$= acx + ad + b = T(ac, ad+b)$$

Damit ist $H = \{T(a,b) \mid a \in \mathbb{Z} - \{0\}, b \in \mathbb{Z}\}$ eine Halbgruppe mit Eins. Man nennt H die "$ax+b$" - Halbgruppe.

3. <u>Definition</u> Eine Halbgruppe $(H, *)$ heißt <u>kommutativ</u> oder <u>abelsch</u> (nach N. Abel, norwegischer Mathematiker nach dem der <u>Abel-Preis</u> benannt ist) wenn für alle $x, y \in H$ gilt

$$x * y = y * x$$

<u>Bsp</u> (a) $\cdot$ und $+$ sind kommutativ auf $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$, die entsprechenden Halbgruppen sind abelsch.

(b) Wenn X mindestens 2 verschiedene Elemente hat, so ist $\{f : X \to X\}$ nicht abelsch (Ü A)

(c) Die $ax+b$ - Halbgruppe ist nicht abelsch, z. B.

$$T(2,1) \circ T(1,2) = T(2,5)$$
$$T(1,2) \circ T(2,1) = T(2,3)$$

4. Eine Halbgruppe $(H,*)$ heißt <u>kürzbar</u>, wenn man kürzen darf, wenn also aus

$$a*x=a*y \quad \text{oder} \quad x*a=y*a$$

stets folgt $x=y$

<u>Bsp</u> (a) Addition $+$ liefert kürzbare Halbgruppen auf $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$.

(b) Wenn X mindestens 2 verschiedene Elemente hat, so ist die Halbgruppe $H=\{f:X\to X\}$ <u>nicht</u> kürzbar (ÜA).

(c) Die $ax+b$ – Halbgruppe ist kürzbar. (ÜA)

(d) Sei $H=\mathbb{N}$ mit Verknüpfung

$x*y=\max\{x,y\}$. Diese Verknüpfung ist assoziativ, kommutativ und hat 0 als Neutralelement:

$$\max\{\max\{x,y\},z\}=\max\{x,y,z\}=\max\{x,\max\{y,z\}\}$$

$$\max\{x,y\}=\max\{y,x\}$$

$$\max\{0,x\}=x=\max\{x,0\}$$

Sie ist aber nicht kürzbar:

$$\max\{0,1\} = \max\{1,1\} = 1$$

$$0 * 1 = 1 * 1 \quad \text{aber} \quad 0 \neq 1.$$

Über Halbgruppen kann man so allgemein wenig sagen – es gibt "zu viele" Halbgruppen. Viel wichtiger sind Gruppen.

5. <u>Definition</u> Eine Halbgruppe $(H, *)$ mit Eins heißt <u>Gruppe</u>, wenn es zu jedem $x \in H$ ein $y \in H$ gibt mit

$$x * y = e = y * x$$

Dabei ist e das Neutralelement von H. Mit anderen Worten: es gelten die Regeln

$$x * (y * z) = (x * y) * z \qquad \text{für alle } x, y, z \in H$$

$$x * e = x = e * x \qquad \text{für alle } x \in H$$

Zu jedem $x \in H$ gibt es $y \in H$ mit $x * y = e = y * x$.

Beispiele

(a) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ sind Gruppen

(b) $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$ sind keine Gruppen

denn $0 \cdot y = 1$ hat keine Lösung

(c) $\{f : X \to X\}$ ist keine Gruppe, wenn X mindestens 2 Elemente hat

(d) Die $ax+b$ - Halbgruppe ist keine Gruppe

(e) $\mathrm{Sym}(X)$ (vgl § 0.16) ist eine Gruppe, die symmetrische Gruppe der Menge X

6. Lemma Sei $(G,*)$ eine Gruppe. Dann gilt:

(i) G ist kürzbar

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

Beweis Angenommen, es gilt $a * x = a * y$. Sei b ein Inverses zu a, $b * a = e$. Dann gilt $\underbrace{b * a} * x = \underbrace{b * a} * y \Rightarrow e * x = e * y$

$\Rightarrow x = y$.

Genauso folgt aus $x * a = y * a$, dass $x = y$ gilt. Damit ist (i) bewiesen.

Nun ist (ii) eine direkte Konsequenz: aus $a * b = e = a * c$ folgt mit Kürzen sofort $b = c$, genauso andersherum. $\square$

#

Das nach dem Lemma eindeutig bestimmte Inverse zu x wird dann auch mit x^{-1} bezeichnet. Oder mit $-x$, falls die Verknüpfung mit $+$ bezeichnet wird.

Bisher kennen wir folgende Gruppen:

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ (alle abelsch)

Setzt man $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ und $\mathbb{R}^* = \mathbb{R} - \{0\}$, dann sind auch $(\mathbb{Q}^*, \cdot)$ und $(\mathbb{R}^*, \cdot)$ abelsche Gruppen.

Die symmetrische Gruppe $\mathrm{Sym}(X)$ ist für $\# X \geq 3$ nicht abelsch.

In der Vorlesung und im Mathematik-Studium werden Sie viele weitere Gruppen kennen lernen!

7. Definition Sei R ein (nicht leere) Menge mit zwei Verknüpfungen $+$ und $\circ$. Man nennt $(R,+,\circ)$ einen Ring, wenn gilt:

(i) $(R,+)$ ist eine Gruppe, mit Neutralelement $0 \in R$

(ii) $(R,\circ)$ ist eine Halbgruppe mit Neutralelement $1 \in R$

(iii) es gelten die Distributivgesetze

$$a \circ (x+y) = (a \circ x) + (a \circ y)$$
$$(x+y) \circ a = (x \circ a) + (y \circ a)$$

Konvention: "Punkt geht vor Strich" und dann läßt man die Klammern weg – und den Punkt $\circ$ auch, also

$$a(x+y) = ax + ay$$
$$(x+y)a = xa + ya$$

Beispiele (a) $(\mathbb{Q},+,\circ)$, $(\mathbb{R},+,\circ)$, $(\mathbb{Z},+,\circ)$ sind Ringe

(b) $(\mathbb{N},+,\circ)$ ist kein Ring, denn $(\mathbb{N},+)$ ist keine Gruppe – die Gleichung $x+1=0$ hat keine Lösung $x \in \mathbb{N}$.

8. <u>Satz</u> (Rechenregeln in Ringen)

Sei $(R,+,\cdot)$ ein Ring mit Neutralelemente $0, 1 \in R$. Für $x \in R$ sei $-x$ das Inverse bezüglich $+$, also $x + (-x) = 0 = (-x) + x$.

Dann gelten folgende Rechenregeln.

(i) $x + y = y + x$, die Addition in einem Ring ist kommutativ.

(ii) $0x = 0 = x0$ für alle $x \in R$

(iii) $-(-x) = x$ für alle $x \in R$

(iv) $-(xy) = (-x)y = x(-y)$ für alle $x, y \in R$

insbesondere $(-1)x = -x$ und $(-x)(-y) = xy$

<u>Beweis</u>

(i)
$$(1+x)(1+y) = 1(1+y) + x(1+y) = 1 + y + x + xy$$
$$(1+x)(1+y) = (1+x)1 + (1+x)y = 1 + x + y + xy$$

$\overset{\text{Kürzen}}{\rightsquigarrow}$ $y + x = x + y$

(ii) $0x = (0+0)x = 0x + 0x \overset{\text{Kürzen}}{\rightsquigarrow} 0 = 0x$

genauso $x0 = 0$

(iii)
$$\left.\begin{aligned} -x + (-(-x)) &= 0 \\ -x + x &= 0 \end{aligned}\right\} \overset{\text{Kürzen}}{\rightsquigarrow} -(-x) = x$$

(iv)
$$\left.\begin{aligned} xy + (-x)y &= (x + (-x))y = 0y = 0 \\ xy + (-(xy)) &= 0 \end{aligned}\right\} \Rightarrow (-x)y = -(xy)$$

$\square$

Ein Ring $(R,+,\cdot)$ heißt kommutativ, wenn die Multiplikation $\cdot$ kommutativ ist, wenn also für alle $x,y \in R$ gilt $x \cdot y = y \cdot x$. Alle Ringe, die wir bisher betrachtet haben, waren kommutativ.

Merke: Die Addition $+$ eines Ringes ist immer kommutativ, vgl §1.8(i).

Extremes Beispiel eines Ringes: der Nullring $R = \{0\}$ mit $0 \cdot 0 = 0 + 0 = 0$. In diesem Ring gilt $1 = 0$ (!) und $R^* = R$ (!).

Das ist etwas pathologisch und wird oft ausgeschlossen, indem man explizit verlangt, dass $1 \neq 0$ in R gelten soll.

9. Einheiten und Körper

Sei $(R,+,\cdot)$ ein Ring. Dann heißt ein Element $u \in R$ <u>Einheit</u>, wenn es ein $v \in R$ gibt mit $uv = 1 = vu$. Die Menge aller Einheiten von R bezeichnen wir mit R^*.

<u>Lemma</u> $(R^*,\cdot)$ ist eine Gruppe, die <u>Einheitengruppe</u> von R.

<u>Beweis</u> Ist $u \in R^*$, $uv = vu = 1$ und
$w \in R^*$ $wz = zw = 1$, so

gilt
$$\left.\begin{array}{l}(uw)(zv) = uv = 1\\ (zv)(uw) = zw = 1\end{array}\right\} \Rightarrow uw \in R^*$$

und $v \in R^*$. Weiter gilt $1 \in R^*$, denn $1 \cdot 1 = 1$, also ist R^* eine Gruppe $\square$

<u>Bsp</u>
$$\mathbb{R}^* = \{ r \in \mathbb{R} \mid r \neq 0 \}$$
$$\mathbb{Q}^* = \{ r \in \mathbb{Q} \mid r \neq 0 \}$$
$$\mathbb{Z}^* = \{ \pm 1 \}$$

Def Ein [kommutativer] Ring $(K,+,\cdot)$ mit $1 \neq 0$ heißt **Körper**, wenn gilt $K^* = K - \{0\}$, wenn also jedes Element $x \in K - \{0\}$ eine Einheit ist.

Beispiel
- $\mathbb{R}$, $\mathbb{Q}$ sind Körper
- $\mathbb{Z}$ ist **kein** Körper, denn $\mathbb{Z}^* = \{\pm 1\} \neq \mathbb{Z} - \{0\}$.
- $\mathbb{F}_2 = \{0,1\}$ mit

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

ist ein Körper (aber das Nachrechnen von Hand ist mühsam, wir werden eine bessere Begründung später beweisen).

10. Der Körper $\mathbb{C}$ der komplexen Zahlen

(1. Version – später viel eleganter!)

Setze $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ (reelle Ebene) und definiere $+$ und $\cdot$ wie folgt.

$(a,b)+(c,d)=(a+c,\ b+d)$

Damit ist $(\mathbb{C},+)$ eine Gruppe, wie man leicht sieht: $(a,b)+(0,0)=(a,b)=(0,0)+(a,b)$

$(a,b)+(-a,-b)=(0,0)$

$\big((a,b)+(c,d)\big)+(e,f)=(a+c+e,\ b+d+f)$

$=(a,b)+\big((c,d)+(e,f)\big)$.

Wir setzen jetzt

$$(a,b)\cdot(c,d)=(ac-bd,\ ad+bc)$$

Eine (längere, aber elementare) Rechnung zeigt: es gelten das Assoziativgesetz, die Multiplikation ist kommutativ und das Distributivgesetz gilt auch.

Weiter gilt $(a,b)\cdot(1,0)=(a,b)=(1,0)\cdot(a,b)$,

Folglich ist $(\mathbb{C},+,\cdot)$ ein Ring.

Wie sehen die Einheiten aus?

Probieren: $(a,b)\cdot(a,-b)=(a^2+b^2,\ 0)$

$$(a,b)\cdot\left(\frac{a}{\delta},\frac{-b}{\delta}\right)=\left(\frac{a^2+b^2}{\delta},0\right)$$

für $\delta=a^2+b^2\neq 0$ erhalten wir rechts $(1,0)$

und $\left(\frac{a}{\delta},\frac{-b}{\delta}\right)(a,b)=\left(\frac{a^2+b^2}{\delta},0\right)$

Nun gilt $\delta = a^2+b^2 \neq 0$ genau dann, wenn $(a,b) \neq 0$: $a^2, b^2 \geq 0$, also $a^2+b^2 \geq 0$ und $a^2+b^2 = 0$ genau dann, wenn $a^2 = b^2 = 0$.

Folglich gilt $\mathbb{C}^* = \mathbb{C} - \{(0,0)\}$ und $\mathbb{C}$ ist ein Körper, der Körper der komplexen Zahlen.

Statt $z = (a,b) \in \mathbb{C}$ schreibt man $z = a + ib$. Dabei ist i ein "Symbol", keine reelle Zahl, mit den Rechenregeln

$$i \cdot i = -1$$

$$i \cdot t = t \cdot i \quad \text{für alle } t \in \mathbb{R}$$

Die Verknüpfung $+$ und $\cdot$ lassen sich dann leichter merken:

$$(a+ib)+(c+id) = (a+c) + i(b+d)$$

$$\begin{aligned}(a+ib)\cdot(c+id) &= ac + ibid + ibc + aid \\ &= ac + i^2 bd + i(bc+ad) \\ &= (ac-bd) + i(bc+ad)\end{aligned}$$

In $\mathbb{C}$ hat die Gleichung $x^2 = -1$ also Lösungen, nämlich $x = \pm i$.

Wir konstruieren jetzt eine andere Art von Körpern aus den ganzen Zahlen. Dazu brauchen wir etwas elementare Zahlentheorie

11. Ein kurzer Ausflug in die Elementare Zahlentheorie

Lemma A (Teilen mit Rest)

Sei $m \in \mathbb{N}$, $m \geq 1$. Für jedes $n \in \mathbb{Z}$ gibt es eindeutig bestimmte Zahlen $r, s \in \mathbb{Z}$ mit $n = m \cdot s + r$ und $0 \leq r < m$

Beweis Sei $S = \{ s \in \mathbb{Z} \mid m \cdot s \leq n \}$. In dieser Menge gibt es ein größtes Element $t \in S$ (denn für alle $s \in S$ gilt $s \leq |n|$; wende (M) aus §0.17 auf die Menge $\{ |n| - s \mid s \in S \}$ an).

Es folgt $m \cdot t \leq n$, aber $m(t+1) > n \Rightarrow$
$n = m \cdot t + r$ mit $0 \leq r < m$.

Eindeutigkeit: angenommen, $n = m \cdot s + r = m \cdot s' + r'$ mit $0 \leq r, r' < m$. Wir dürfen annehmen, dass $r' \geq r$ gilt, also $m \cdot (s - s') = r' - r$.

Es gilt $0 \leq r' - r < m$, also $s - s' = 0 \Rightarrow r' - r = 0$

$\square$

Def Sei $a, b \in \mathbb{Z}$. Wir nennen a einen Teiler von b, wenn es $c \in \mathbb{Z}$ gibt mit $a \cdot c = b$ und schreiben dann $a \mid b$. (und $a \nmid b$ wenn a kein Teiler von b ist)

Bsp $-3 \mid 15$ $\quad 4 \mid 0$ $\quad 3 \nmid 5$

Eine Zahl $p \in \mathbb{N}$, $p \geq 2$, heißt Primzahl, wenn ± 1 und $\pm p$ die einzigen Teiler von p sind. Die Menge aller Primzahlen ist $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$

Lemma B Für $n \in \mathbb{N}$, $n \geq 2$ sei $p(n)$ der kleinste Teiler von n mit $p(n) \geq 2$. (existiert nach §0.17 (M)).
Diese Zahl $p(n)$ ist stets eine Primzahl.

Beweis Angenommen, $q \in \mathbb{N}$, $q > 1$ und $q \mid p(n)$.
Wegen $p(n) \mid n$ gilt $q \mid n$, also $p(n) \leq q$.
Wegen $q \mid p(n)$ gilt $q \leq p(n)$, also $q = p(n)$ $\square$

Korollar (Euklid) Die Menge $\mathbb{P}$ der Primzahlen ist unendlich.

<u>Beweis</u> Seien $p_1 < p_2 < \dots < p_s$ Primzahlen. Betrachte $n = p_1 \cdot p_2 \cdot \dots \cdot p_s + 1$. Dann gilt: $p(n) \nmid p_j$ für $j = 1, \dots, s$, denn sonst hätten wir $p(n) \mid 1$. Insbesondere gilt $p(n) \neq p_1, p_2, \dots, p_s$ $\square$

<u>Lemma C</u> Sei $n \in \mathbb{Z}$, $n \geq 2$. Dann gibt es Primzahlen $p_1 \leq p_2 \leq \dots \leq p_s$ mit
$$n = p_1 \cdot p_2 \cdot \dots \cdot p_s .$$

<u>Beweis</u> Induktion nach n. Für $n = 0, 1$ ist nichts zu zeigen und für $n = 2 \in \mathbb{P}$ ist die Aussage wahr. Allgemein setze $q = p(n)$. Dann gilt $n = q \cdot l$ für ein $l \in \mathbb{Z}$ mit $1 \leq l < n$. Nach Voraussetzung ist $l = 1$ oder l ist Produkt von Primzahlen. $\square$

<u>Theorem D</u> ("Hauptsatz der Arithmetik")

Sei $n \in \mathbb{Z}$, $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen
$$p_1 \leq p_2 \leq \dots \leq p_s \text{ mit } n = p_1 \cdot p_2 \cdots p_s .$$

Beweis Zu zeigen ist die Eindeutigkeit solcher einer Primfaktorzerlegung von n.
Angenommen, die Behauptung wäre falsch. Dann gäbe es nach §0.17 (M) ein kleinstes Gegenbeispiel $n \in \mathbb{Z}$, also

$$n = p_1 \cdot p_2 \cdots \cdot p_s \qquad p_1 \leq \cdots \leq p_s$$
$$= q_1 \cdot q_2 \cdots \cdot q_t \qquad \underbrace{q_1 \leq \cdots \leq q_t}_{\text{Primzahl}}$$

und $q_j \neq p_j$ für ein j.
Das Gegenbeispiel kann keine Primzahl sein, also gilt $s, t \geq 2$. Wäre $p_1 = q_1$, so hätten wir mit $p_2 \cdots p_s = q_2 \cdots q_t$ ein kleineres Gegenbeispiel, also gilt $p_1 \neq q_1$.
Wir dürfen annehmen, dass $p_1 > q_1$ gilt.
Betrachte
$$n' = (p_1 - q_1)\, p_2 \cdots p_s$$
$$= n - q_1 p_2 \cdots p_s < n$$
Es folgt $q_1 \mid n'$, also $n' \geq 2$.

Damit hat n' eindeutige Primfaktorzerlegung, mit den Primfaktoren $q_1 < p_2 \le p_3 \le \dots \le p_s$ (und eventuell weiteren Primfaktoren). Es folgt wegen $n' = (p_1 - q_1)\, p_2 \cdots p_s$, dass $q_1 \mid p_1 - q_1$ und damit $q_1 \mid p_1$, aber $p_1 \in \mathbb{P}$ $\lightning$ $\square$

Also gibt es kein Gegenbeispiel.

<u>Korollar</u> Jedes $n \in \mathbb{Z}$, $n \neq 0, \pm 1$ lässt sich eindeutig schreiben als

$$n = \varepsilon\, p_1^{l_1} \cdots p_s^{l_s} \quad \text{mit} \quad \varepsilon = \pm 1,$$

$l_j \geq 1$, $p_1, \dots, p_s \in \mathbb{P}$, $p_1 < p_2 < \dots < p_s$.

<u>Korollar</u> (Euklids Lemma) Sei $a, b \in \mathbb{Z}$, sei $p \in \mathbb{P}$. Wenn gilt $p \mid a \cdot b$, so gilt $p \mid a$ oder $p \mid b$.

<u>Beweis</u> (*) Schreibe $a = \alpha\, p_1 \cdots p_s$ $\quad p_j \in \mathbb{P}, \alpha = \pm 1$

$b = \beta\, q_1 \cdots q_t$ $\quad q_j \in \mathbb{P}, \beta = \pm 1$

$$\left.\begin{aligned} a \cdot b &= \alpha \beta\, p_1 \cdots p_s q_1 \cdots q_t \\ &= p \cdot m \end{aligned}\right\}$$

Eindeutigkeit der Primfaktorzerlegung

$\Rightarrow p \in \{p_1, \dots, p_s, q_1, \dots, q_t\}$

(*) OE $a \neq 0, \pm 1$, $b \neq 0, \pm 1$

12. Kongruenzen Sei $m \in \mathbb{N}$. Wir setzen $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$. Zwei Zahlen $a, a' \in \mathbb{Z}$ heißen kongruent modulo m, wenn gilt $m \mid a - a'$ oder äquivalent, wenn gilt $a - a' \in m\mathbb{Z}$. Die Menge aller Zahlen, die zu einem gegebenen $a \in \mathbb{Z}$ kongruent modulo m ist, ist offensichtlich genau die Menge $\{a + mk \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$. Wenn klar ist, welches $m \in \mathbb{Z}$ gemeint ist, schreibt man auch $\bar{a} = a + m\mathbb{Z}$, die Kongruenzklasse von a modulo m.

Bsp $2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$ gerade Zahlen
$1 + 2\mathbb{Z} = \{\pm 1, \pm 3, \pm 5, \dots\}$ ungerade Zahlen

Lemma A Sei $m \in \mathbb{N}$, sei $a, b \in \mathbb{Z}$. Dann sind äquivalent:

(i) $\bar{a} = \bar{b}$ (d.h. $a + m\mathbb{Z} = b + m\mathbb{Z}$)

(ii) $m \mid a - b$

(iii) $b \in \bar{a}$

(iv) $a \in \bar{b}$

Beweis (i) und (ii) sind nur Umformulierungen.
Wegen $b \in \bar{b}$ gilt offensichtlich (i) $\Rightarrow$ (iii).
Angenommen, $b \in \bar{a}$. Dann gilt $b = a + mk$ für ein $k \in \mathbb{Z}$, also $b + ml = a + m(k+l) \in \bar{a}$ für alle $l \in \mathbb{Z}$, d.h. $\bar{b} \subseteq \bar{a}$. Wegen $a = b - mk$ folgt genauso $\bar{a} \subseteq \bar{b}$, insgesamt also $\bar{a} = \bar{b}$ $\square$

#

Lemma B Sei $m \in \mathbb{N}$, sei $a, a', b, b' \in \mathbb{Z}$.
Wenn gilt $\bar{a} = \bar{a'}$ und $\bar{b} = \bar{b'}$, so gilt

$$\overline{a+b} = \overline{a'+b'} \quad \text{und} \quad \overline{a \cdot b} = \overline{a'b'}.$$

Beweis Schreibe $a' = a + m \cdot k$ und $b' = b + m \cdot l$.
Dann gilt $a' + b' = a + b + m(k+l)$, also $m \mid (a+b) - (a'+b')$
und $a' \cdot b' = ab + aml + bmk + mkl$, also

$$m \mid a \cdot b - a' \cdot b'$$ $\square$

Definition Für $m \in \mathbb{N}$, $m \geq 1$ setzen wir

$$\mathbb{Z}/m = \{ a + m\mathbb{Z} \mid a \in \mathbb{Z} \} = \{ \bar{a} \mid a \in \mathbb{Z} \}$$

Menge der Kongruenzklassen modulo m.

Offensichtlich gilt

$$\mathbb{Z}/m = \{ \bar{0}, \bar{1}, \dots, \overline{m-1} \}$$

also ist $\mathbb{Z}/m$ endlich mit m Elementen.
(warum sind es wirklich m verschiedene Kongruenzklassen? → Teilen mit Rest)
Mit Hilfe von Lemma B definieren wir zwei Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}/m$, durch

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Lemma B sagt, dass diese Verknüpfungen <u>wohl definiert</u> sind.

<u>Satz</u> $(\mathbb{Z}/m, +, \cdot)$ ist ein kommutativer Ring.

<u>Beweis</u> (a) $(\mathbb{Z}/m, +)$ ist Gruppe, denn

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c} = \overline{a+b+c} = \overline{a+b} + \bar{c}$$
$$= (\bar{a} + \bar{b}) + \bar{c}$$

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \overline{0+a} = \bar{0} + \bar{a}$$

$$\bar{a} + \overline{-a} = \overline{a-a} = \bar{0} = \overline{-a+a} = \overline{-a} + \bar{a}$$

(b) $(\mathbb{Z}/m, \cdot)$ ist kommutative Halbgruppe mit Eins

$$\bar{a}(\bar{b} \cdot \bar{c}) = \bar{a} \cdot \overline{bc} = \overline{abc} = \overline{ab} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$
$$\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$$
$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}$$

(c) Distributivgesetz

$$\bar{a}(\bar{b}+\bar{c}) = \bar{a}\,\overline{b+c} = \overline{a(b+c)} = \overline{ab+ac}$$

$$= \bar{a}\bar{b} + \bar{a}\bar{c}$$ und andersrum genauso.

Beachte: Für $m = 1$ erhalten wir $\mathbb{Z}/1 = \{\bar{0}\}$ den trivialen Ring, der Fall ist uninteressant.

13. Satz: Sei $m \in \mathbb{N}$, $m \geq 2$. Dann sind äquivalent: (i) $\mathbb{Z}/m$ ist ein Körper
(ii) m ist eine Primzahl.

Beweis: Angenommen, p ist eine Primzahl. Für $\bar{a} \in \mathbb{Z}/p$ betrachte die Abbildung

$$\lambda_{\bar{a}} : \mathbb{Z}/p \to \mathbb{Z}/p, \quad x \mapsto \bar{a} \cdot x$$

Behauptung: $\lambda_{\bar{a}}$ ist injektiv, wenn $0 < a < p$:

$\bar{a} \cdot \bar{s} = \bar{a} \cdot \bar{t} \Rightarrow \bar{a} \cdot \overline{s-t} = \bar{0}$, d.h. $p \mid a \cdot (s-t)$. Da $0 < a < p$ gilt, folgt $p \mid s-t$ (Euklids Lemma), also $\bar{s} = \bar{t}$.

Da $\mathbb{Z}/p$ endlich ist, ist $\lambda_{\bar{a}}$ bijektiv (§ 0.15). Insbesondere gibt es $b \in \mathbb{Z}$ mit $\bar{a} \cdot \bar{b} = \bar{1}$, d.h. $\bar{a}$ ist Einheit im Ring $\mathbb{Z}/p$.

Nun gilt aber

$\mathbb{Z}/p - \{\bar{0}\} = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

Jetzt nehmen wir an, $m \geq 2$ ist keine Primzahl.

Dann gilt $m = q \cdot l$ mit $2 \leq q, l < m$

Es folgt $\bar{q} \cdot \bar{l} = \bar{0}$ und $\bar{q} \neq \bar{0}$. Wäre $\bar{q} \cdot \bar{a} = \bar{1}$, so hätten wir $\underbrace{\bar{q} \cdot \bar{l}}_{\bar{0}} \cdot \bar{a} = \bar{0} = \bar{l}$,

aber $\bar{l} \neq \bar{0}$ wegen $2 \leq l < m$. Folglich ist $\bar{q} \neq \bar{0}$ keine Einheit in $\mathbb{Z}/m$ und deswegen ist $\mathbb{Z}/m$ kein Körper. $\square$

- Ist $p \in \mathbb{P}$, so schreibt man auch

  $\mathbb{F}_p = \mathbb{Z}/p$, Körper mit p Elementen

  (englisch field = Körper). Unsere Konstruktion liefert also unendlich viele endliche Körper und insbesondere $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$, vgl. §1.9.

- Diese Körper $\mathbb{F}_p$ und die Ringe $\mathbb{Z}/m$ werden in der Kryptographie benutzt, zum Beispiel im RSA-Verfahren.

Über Primzahlen gibt es viele sehr schwierige Fragen. Zum Beispiel:

Goldbach-Vermutung: Jedes $m \in 2\mathbb{Z}$, $m \geq 3$ ist Summe von zwei Primzahlen.

$4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $10 = 7+3$, ... ?

Primzahlzwillinge: Ist $p \in \mathbb{P}$ und $p+2 \in \mathbb{P}$, dann nennt man $p, p+2$ Primzahl-Zwillinge.

$(3,5)$, $(5,7)$, $(11,13)$, ...

Frage: gibt es unendlich viele Primzahl-Zwillinge?

Arithmetische Progressionen: Für $m \geq 1$ nennt man eine Folge $\{a + k \cdot m \mid k = 0, \ldots, s-1\}$ eine arithmetische Progression der Länge s.

2004 bewiesen Green und Tao: zu jedem $s \geq 1$ gibt es $a \in \mathbb{N}$, $m \geq 1$ so, dass

$$\{a + km \mid 0 \leq k < s\} \subseteq \mathbb{P}$$ gilt.

(Das größte explizit bekannte Beispiel ist wohl $s = 26$.)

Wir beenden jetzt die elementare Zahlentheorie und gehen zu Gruppen weiter.

14. Def Sei $(G,\cdot)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt Untergruppe von G, wenn gilt:
(i) $1 \in H$
(ii) ist $x, y \in H$, so ist auch $x \cdot y \in H$
(iii) ist $x \in H$, so ist auch $x^{-1} \in H$.

Offensichtlich ist eine Untergruppe wieder eine Gruppe (Warum?)

Satz Die Untergruppen von $(\mathbb{Z},+)$ sind genau die Mengen $m\mathbb{Z} \subseteq \mathbb{Z}$, für $m \in \mathbb{N}$.

Beweis Ist $x, y \in m\mathbb{Z}$, $x = mk$, $y = ml$, so ist $x+y = m(k+l) \in m\mathbb{Z}$ und $-x = -mk \in m\mathbb{Z}$. Weiter gilt $0 = 0 \cdot m \in m\mathbb{Z} \Rightarrow m\mathbb{Z}$ ist immer eine Untergruppe. #

Sei jetzt $H \subseteq \mathbb{Z}$ eine beliebige Untergruppe. Sei $A = \{h \in H \mid h > 0\}$. Wir unterscheiden:

1. Fall $A = \emptyset$. Da aus $h \in H$ stets folgt $-h \in H$, gilt dann $\{h \in H \mid h < 0\} = \emptyset$, also $H = \{0\} = 0\mathbb{Z}$.

2. Fall $A \neq \emptyset$. Dann hat A ein kleinstes Element $m \in A$. Ist $h \in H$ beliebig, so gibt es r, s mit $h = m \cdot s + r$ und $0 \leq r < m$. (Teilen mit Rest §1.10)

Es gilt für $s>0$: $\underbrace{m+m+\dots+m}_{s \text{ Summanden}} = m \cdot s \in H$

und für $s<0$ $\underbrace{(-m)+(-m)\dots+(-m)}_{-s \text{ Summanden}} = (-m)(-s) \in H$

also $m \cdot s \in H$, also $r = h - m \cdot s \in H$. Aus der Minimalität von m folgt $r=0$, also $h = m \cdot s \in m\mathbb{Z}$, d.h. $H \subseteq m\mathbb{Z}$. Wegen $m \in H$ gilt andererseits $m \cdot s \in H$ für alle $s \in \mathbb{Z}$, also $m\mathbb{Z} \subseteq H$ und damit $H = m\mathbb{Z}$. $\square$

Wir betrachten jetzt Kongruenzen in Gruppen. Für nicht-abelsche Gruppen muss man dabei links und rechts unterscheiden.

15. <u>Definition</u> Sei $(G,\circ)$ eine Gruppe und sei $H \leq G$ eine Untergruppe. Sei $a \in G$. Die Menge $aH = \{ah \mid h \in H\} \subseteq G$ nennt man <u>Linksnebenklasse</u> (von a bezüglich H). Die Menge $Ha = \{ha \mid h \in H\}$ nennt man <u>Rechtsnebenklasse</u>. Man schreibt

$$G/H = \{aH \mid a \in G\}$$
$$H\backslash G = \{Ha \mid a \in G\}$$

Wenn die Verknüpfung mit "+" bezeichnet wird, schreibt man $a+H$ bzw $H+a$.

Beobachte: Die Abbildungen $H \to aH$, $H \to Ha$
$h \mapsto ah$ bzw $h \mapsto ha$ sind bijektiv.
Alle (Links- und Rechts-) Nebenklassen einer gegebenen Untergruppe $H \subseteq G$ sind gleich lang.

Beispiel $H = m\mathbb{Z} \subseteq \mathbb{Z} = G$ für $m \geq 1$.
Da $(\mathbb{Z}, +)$ kommutativ ist, stimmen Rechts- und Linksnebenklassen überein und es gilt $a + m\mathbb{Z} = \bar{a}$ genau wie in §1.11

Die Menge aller Nebenklassen von $m\mathbb{Z}$ ist also genau

$$\mathbb{Z}/_{m\mathbb{Z}} = \{ \bar{a} \mid a \in \mathbb{Z} \} = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1} \}$$
$$= \mathbb{Z}/m$$

Lemma Sei $(G, \cdot)$ eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind äquivalent:

(i) $aH = bH$
(ii) $b^{-1}a \in H$
(iii) $b \in aH$
(iv) $a \in bH$

(vergleiche die Aussage in §1.12 !)

<u>Beweis</u> (i) $\Rightarrow$ (ii) Wegen $a \in aH = bH$ gibt es $h \in H$ mit $a = bh$, also $b^{-1}a = h \in H$.

(ii) $\Rightarrow$ (iii) Ist $b^{-1}a = h \in H$, so ist $b = ah^{-1} \in aH$

(iii) $\Rightarrow$ (iv). Ist $b = ah \in aH$, so ist $a = bh^{-1} \in bH$

(iv) $\Rightarrow$ (i) Ist $a = bh \in bH$, so ist

$$aH = bhH = \{bhh' \mid h' \in H\} = \{b\tilde{h} \mid \tilde{h} \in H\} = bH \qquad \square$$

Das Lemma B in §1.12 funktioniert so allgemein nicht. Ist $h, h' \in H$, so gilt im Allgemein nicht $abH = (ah)(bh')H$; das Problem ist, dass man h im nicht-abelschen Fall nicht einfach an b vorbeiziehen kann. Für abelsche Gruppen geht aber alles gut:

16. <u>Satz</u> Sei $(G, \cdot)$ eine abelsche Gruppe und sei $H \leq G$ eine Untergruppe. Dann können wir auf G/H eine Verknüpfung definieren durch

$$aH \circ bH = abH$$

Bezüglich dieser Verknüpfung ist G/H eine abelsche Gruppe, der <u>Quotient von G modulo H</u>. Das Neutralelement ist $1H = H$, das Inverse von aH ist $a^{-1}H$

<u>Beweis</u> Angenommen, $aH = a'H$ und $bH = b'H$.

Dann gilt $a^{-1}a' \in H$ und $b^{-1}b' \in H$, also

$$a'b'H = a\underbrace{a^{-1}a'}_{h}b\underbrace{b^{-1}b'}_{\tilde h}H = ahb\tilde h H \underset{\substack{\uparrow \\ G \text{ abelsch}}}{=} ab\,h\tilde h H = abH$$

Also ist diese Verknüpfung $(aH, bH) \longmapsto abH$
$$G/_H \times G/_H \longrightarrow G/_H$$
wohldefiniert. Es gilt $aH \cdot H = aH = H \cdot aH$.

$$(aH \cdot bH) \cdot cH = abH \cdot cH = abcH = aH \cdot bcH = aH \cdot (bH \cdot cH)$$

$$aH \cdot a^{-1}H = aa^{-1}H = H$$ $\square$

<u>Beispiel</u> $G = (\mathbb{Z}, +)$ $H = m\mathbb{Z}$ für $m \in \mathbb{N}$

Das ist genau die Konstruktion in § 1.12 und

$$\mathbb{Z}/_{m\mathbb{Z}} = \mathbb{Z}/m$$

17. <u>Definition</u> Seien $(G, \cdot)$ und $(K, \cdot)$ Gruppen. Eine Abbildung $\varphi: G \to K$ heißt <u>Homomorphismus</u> (von Gruppen), wenn für alle $x, y \in G$ gilt

$$\underset{\substack{\uparrow \\ \text{Verknüpfung} \\ \text{in } G}}{\varphi(x \cdot y)} = \varphi(x) \underset{\substack{\uparrow \\ \text{Verknüpfung} \\ \text{in } K.}}{\cdot} \varphi(y)$$

Seien $e_G \in G$ und $e_K \in K$ die jeweiligen Neutralelemente. Die Menge

$$\ker(\varphi) = \{x \in G \mid \varphi(x) = e_K\}$$

heißt <u>Kern</u> des Homomorphismus.

<u>Satz</u> Sei $\varphi: G \to K$ ein Homomorphismus von Gruppen. Dann gilt Folgendes:

(i) $\varphi(e_G) = e_K$

(ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ für alle $x \in G$

(iii) $\varphi(G) \subseteq K$ ist eine Untergruppe

(iv) $\ker(\varphi) \subseteq G$ ist eine Untergruppe

<u>Bew.</u> (i) Sei $x \in G$. Dann gilt

$$\underset{\varphi(x)e_K}{\underset{\|}{\varphi(x)}} = \varphi(xe_G) = \varphi(x)\varphi(e_G)$$

, also wegen Kürzbarkeit $e_K = \varphi(e_G)$

(ii) $$\underset{\varphi(x)\varphi(x^{-1})}{\underset{\|}{\varphi(xx^{-1})}} = \varphi(e_G) = e_K = \varphi(x)\cdot\varphi(x)^{-1}$$

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

(iv) Wir wissen schon: $e_K \in \varphi(G)$. Ist $x, y \in G$, so folgt $\varphi(x)\cdot\varphi(y) = \varphi(xy) \in \varphi(G)$

$$\varphi(x^{-1}) = \varphi(x)^{-1} \in \varphi(G)$$

damit ist $\varphi(G) \subseteq K$ Untergruppe

(*) Einschub

<u>Homomorphismus</u>

homos: griech. <u>gleich</u>

morphe: griech. <u>Form</u>

(iv) Wir wissen schon: $e_G \in \ker(\varphi)$. Ist $x, y \in \ker(\varphi)$, so gilt $\varphi(x) = \varphi(y) = e_K$, also

$\varphi(x)\varphi(y) = e_K \cdot e_K = e_K \Rightarrow x \cdot y \in \ker(\varphi)$

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

also ist $\ker(\varphi)$ Untergruppe. $\square$

<u>Beispiel</u> (a) Sei $m \in \mathbb{Z}$, $(G, \cdot) = (\mathbb{Z}, +)$

$\mu : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto m \cdot x$ ein Homomorphismus, $(\mathbb{Z}, +) \xrightarrow{\mu} (\mathbb{Z}, +)$. Das Bild von μ ist genau $m\mathbb{Z} \subseteq \mathbb{Z}$. Der Kern von μ ist $\{x \in \mathbb{Z} \mid m \cdot x = 0\}$

also $$\ker(\varphi) = \begin{cases} \{0\} & \text{falls } m \neq 0 \\ \mathbb{Z} & \text{falls } m = 0 \end{cases}$$

(b) $(G, \cdot) = (\mathbb{Z}, +)$, $(K, \cdot) = (\mathbb{Z}/m, +)$ für ein $m \in \mathbb{N}$, $m \geq 1$. Sei $\varkappa(x) = \bar{x} = x + m\mathbb{Z}$

$$\varkappa : \mathbb{Z} \to \mathbb{Z}/m$$

Wegen $\overline{x+y} = \bar{x} + \bar{y}$ (vgl § 1.12) ist $\varkappa$ ein Homomorphismus. Es gilt

$$\varkappa(\mathbb{Z}) = \mathbb{Z}/m \qquad (\varkappa \text{ ist surjektiv})$$

und $\ker(\varkappa) = \{x \in \mathbb{Z} \mid \bar{x} = \bar{0}\} = m\mathbb{Z}$

Ein injektiver Homomorphismus nennt man auch Monomorphismus, einen surjektiven Homomorphismus auch Epimorphismus und ein bijektiver Homomorphismus auch ein Isomorphismus.

épi : griech. auf

monos: griech. ein

isos : griech: gleich

Ist $G \xrightarrow{\varphi} K$ ein Isomorphismus, so nennt man die Gruppen G und K isomorph und schreibt $G \cong K$.

18. **Satz** (Charakterisierung von injektiven Homomorphismen)

Sei $\varphi: G \to K$ ein Homomorphismus von Gruppen.
Dann sind äquivalent:

(i) φ ist injektiv

(ii) $\ker(\varphi) = \{e_G\}$, d.h. Kern von φ ist trivial.

Beweis φ injektiv bedeutet: jedes $z \in K$ hat höchstens ein Urbild. Der Kern von φ ist das Urbild von e_K. Also gilt: (i) $\Rightarrow$ (ii).
Jetzt nehmen wir an, dass $\ker(\varphi) = \{e_G\}$ gilt.
Angenommen, $\varphi(x) = \varphi(y)$ gilt für $x, y \in G$. Dann folgt $\varphi(x)\varphi(y)^{-1} = e_K = \varphi(xy^{-1})$, also $xy^{-1} = e_G$, also $x = y$. $\square$

Bemerkung Es gibt kein vergleichbar einfaches Kriterium für die Surjektivität eines Homomorphismus. Falls aber $G \xrightarrow{\varphi} K$ ein Homomorphismus von abelschen Gruppen ist, dann ist

$$\mathrm{cok}(\varphi) = K/\varphi(G)$$

nach §1.14 eine Gruppe. Diese Gruppe

besteht genau dann aus einem Element, wenn gilt $\varphi(G) = K$. Man nennt $\operatorname{cok}(\varphi)$ dann den Kokern von φ, und φ ist surjektiv genau dann, wenn der Kokern trivial (= einelementig) ist.

Wir schließen das 1. Kapitel mit einer einfachen Beobachtung.

19. Satz Sind $(G, \cdot)$ und $(K, \cdot)$ Gruppen, so ist auch das kartesische Produkt $G \times K$ eine Gruppe mit der Verknüpfung

$$(x, y) \cdot (u, v) = (xu, yv)$$

$$(G \times K) \times (G \times K) \to G \times K$$

und Neutralelement $(e_G, e_K) \in G \times K$. Das Inverse von $(x, y) \in G \times K$ ist $(x^{-1}, y^{-1}) \in G \times K$.

$\square$

Beweis: Das ist klar.

Ist $(G_j)_{j \in J}$ eine Familie von Gruppen, dann ist auch $\prod_{j \in J} G_j$ eine Gruppe mit

Verknüpfung $(x_j)_{j \in J} \cdot (y_j)_{j \in J} = (x_j y_j)_{j \in J}$

und Neutralelement $(e_{G_j})_{j \in J}$,

<u>Beispiele</u> (a) $G = K = \mathbb{R}$, dann ist

$\mathbb{R} \times \mathbb{R}$ Gruppe mit Verknüpfung $(x,y) + (u,v) = (x+u, y+v)$

vgl. die Konstruktion von $(\mathbb{C}, +)$ in §1.10.

(b) $J \in \mathbb{N}$, $G_j = \mathbb{R}$ für $j = 0,1,2,\ldots$. Dann

ist $\prod_{j \in \mathbb{N}} \mathbb{R}$ die Menge aller reellen Folgen.

Bezüglich komponentenweiser Addition

$$(x_j)_{j \in \mathbb{N}} + (y_j)_{j \in \mathbb{N}} = (x_j + y_j)_{j \in \mathbb{N}}$$

bilden die Folgen eine Gruppe. Die konvergenten Folgen bilden eine Untergruppe $K \subseteq \prod_{j \in \mathbb{N}} \mathbb{R}$

und die Nullfolgen (= gegen 0 konvergente Folgen) bilden eine Untergruppe $N \subseteq K$.

Das wird bewiesen in Analysis I, Satz 4.9

Dort wird auch gezeigt: die Abbildung

$$K \to \mathbb{R}$$

$$(x_j)_{j \in \mathbb{N}} \mapsto \lim_{j \to \infty} x_j$$

ist ein Homomorphismus.

(c) In der Analysis-Vorlesung haben Sie den Körper der reellen Zahlen wie folgt konstruiert: Sei $G = \prod_{j \in \mathbb{N}} \mathbb{Q}$

(Menge aller Folgen von rationalen Zahlen, mit Addition eine Gruppe)

$C \subseteq G$ Menge aller <u>Cauchy-Folgen</u> in $\mathbb{Q}$

$$C = \{ (x_j)_{j \in \mathbb{N}} \in G \mid \text{zu jedem } \varepsilon > 0 \text{ gibt es } k \in \mathbb{N} \text{ so, dass } |x_i - x_j| \leq \varepsilon \text{ für alle } i,j \geq k \}$$

$$N = \{ (x_j)_{j \in \mathbb{N}} \in G \mid \lim_{j \to \infty} x_j = 0 \}$$

Menge aller Nullfolgen in G. Dann haben Sie gezeigt: es sind $N \subseteq C \subseteq G$ Untergruppen und

$$\mathbb{R} = C/N$$

Cauchyfolgen in $\mathbb{Q}$ modulo Nullfolgen.