§ 3. Homomorphismen, zyklische Gruppen und Chinesischer Restsatz

1. **Def** Seien $(G, *_G)$ und $(K, *_K)$ abelsche Gruppen. Ein **Homomorphismus** von G nach K ist eine Abbildung

$$f: G \to K$$

mit der Eigenschaft

$$f(a *_G b) = f(a) *_K f(b)$$

für alle $a, b \in G$.

Beispiele (a) $G = K$, $f(a) = a$ ist Homomorphismus Identität

(b) Für jedes $d \in \mathbb{Z}$ ist die Abbildung

$f: z \mapsto d \cdot z$ ein Homomorphismus $\mathbb{Z} \to \mathbb{Z}$

(c) Für jedes $d \in \mathbb{N}$ ist die Abbildung

$f: \mathbb{Z} \to \mathbb{Z}/d$, $x \mapsto [x]_d$ ein Homomorphismus, denn

$$f(x+y) = [x+y]_d = [x]_d + [y]_d = f(x) + f(y)$$

(d) Ein aus Analysis: Für $t \in \mathbb{R}$ ist

$$\exp(t) = \sum_{k=0}^{\infty} \frac{1}{k!} t^k .$$ Es gilt $\exp(s+t) = \exp(s) \cdot \exp(t)$

$\exp(0) = 1$

Damit ist $\exp: \mathbb{R} \to \mathbb{R}_{>0}$ ein Homomorphismus zwischen $(\mathbb{R}, +)$ und $(\mathbb{R}_{>0}, \cdot)$

Ein Homomorphismus f heißt <u>Isomorphismus</u>, wenn f bijektiv ist. Dann ist die Umkehrabbildung f^{-1} von f ebenfalls ein Homomorphismus.

<u>Def</u> Sei $f: G \to K$ ein Homomorphismus von abelschen Gruppen $(G, *_G)$ und $(K, *_K)$. Sei $e_K \in K$ das Neutralelement von K. Der <u>Kern</u> von f ist

$$\ker(f) = \{ g \in G \mid f(g) = e_K \}$$

(vgl. Kern einer linearen Abbildung in L.A.)

<u>Lemma</u> Der Kern eines Homomorphismus von abelschen Gruppen $f: G \to K$ ist eine Untergruppe.

Beweis Für das Neutralelement $e_G \in G$ gilt $e_G = e_G *_G e_G$, also folgt $f(e_G) = f(e_G) *_K f(e_G)$
$\Rightarrow f(e_G) = e_K$ (mit Kürzen). Also $e_G \in \ker(f)$, insbesondere ist $\ker(f) \neq \emptyset$.
Ist $x, y \in \ker(f)$, so folgt $f(x *_G y) = f(x) *_K f(y)$
$= e_K$, also $x *_G y \in \ker(f)$, d.h. $\ker(f)$ ist abgeschlossen bzgl der Verknüpfg $*_G$. Ist $x \in \ker(f)$ und x' das Inverse von x, so folgt $f(x *_G x')$
$= f(e_G) = e_K$, also $\underbrace{f(x)}_{=e_K} *_K f(x') = e_K$, d.h.
$f(x') = e_K$. Damit ist $\ker(f)$ Untergrp, vgl. §2.3 □

Bem In den Übungen sieht man:
(a) Ist $f: G \to K$ ein Homomorphismus, so ist das **Bild** $f(G) \leq K$ eine Untergrp.
(b) Ist $f: G \to K$ ein Homomorphismus und ist $x \in G$ mit Inverse x', so ist $f(x')$ das Inverse von $f(x)$.

2. Satz Sei $f: G \to K$ ein Homomorphismus von abelschen Gruppen. Dann sind äquivalent: (i) f ist injektiv
(ii) $\ker(f) = \{e_G\}$

(vgl. LA: eine lineare Abbildung ist genau dann injektiv, wenn ihr Kern nur aus dem Nullvektor besteht.)

Beweis Aus dem vorigen Beweis bzw. der LA wissen wir, dass $f(e_G) = e_K$ gilt.

(i) $\Rightarrow$ (ii) f injektiv $\Rightarrow$ e_G ist das einzige Urbild von e_K, also $\ker(f) = \{e_G\}$

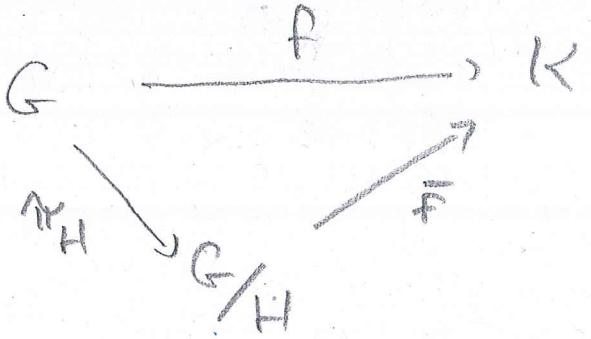
(ii) $\Rightarrow$ (i) Angenommen, $\ker(f) = \{e_G\}$ und $f(x) = f(y)$. Sei x' das Inverse von x. Es folgt $f(x' *_G x) = e_K$

$$= f(x') *_K f(x) = f(x') *_K f(y) = f(x' *_G y)$$

$$\Rightarrow x' *_G x = e_G = x' *_G y \overset{\text{Kürzen}}{\Rightarrow} x = y \qquad \square$$

3. Theorem (Der Homomorphiesatz) Sei $F: G \to K$ ein Homomorphismus von abelschen Gruppen, sei $H = \ker(F) \leq G$. Dann ist die Abbildung $\pi_H: G \to G/H$, $x \mapsto x *_G H$

ein Homomorphism. Es gibt genau ein Homomorphism $\bar{f}: G/H \to K$ mit $\bar{f} \circ \pi_H = f$,



und $\bar{f}$ ist injektiv.

Addendum. Ist f surjektiv, so ist $\bar{f}$ ein Isomorphismus.

Beweis in mehreren (einfachen) Schritten.

(a) π_H ist Homomorphism.

Denn: $x, y \in G$ $\pi_H(x *_G y) = x *_G y *_G H =$

$(x *_G H) * (y *_G H) = \pi_H(x) * \pi_H(y)$.

(b) Eindeutigkeit von $\bar{f}$

Es gilt $\bar{f}(\underbrace{\pi_H(x)}_{\bar{f}(x *_G H)}) = f(x)$

(c) Existenz von $\bar{f}$

Wir definieren $\bar{f}(x *_G H) = f(x)$.

Das ist wohl definiert, denn: $x *_G H = y *_G H$

$\Rightarrow x = y *_G h$ für ein $h \in H$

$\Rightarrow f(x) = f(y *_G h) = f(y) *_K \underbrace{f(h)}_{= e_K} = f(y)$, also

(d) $\bar{f}$ ist Homomorphismus

$$\bar{f}((x *_G H) * (y *_G H)) = \bar{f}(x *_G y *_G H) = f(x *_G y)$$

$$= f(x) *_K f(y) = \bar{f}(x *_G H) *_K \bar{f}(y *_G H).$$

(e) $\bar{f}$ ist injektiv

$$\bar{f}(x *_G H) = f(x) = e_K \iff x \in H \iff x *_G H = H$$

also $\ker(\bar{f}) = \{H\} \leq G/H \rightsquigarrow \bar{f}$ injektiv und §3.2.

(f) Falls f surjektiv ist, so ist $\bar{f}$ bijektiv

Wir wissen schon: $\bar{f}$ ist injektiv. Wenn f surjektiv ist, so ist auch $\bar{f}$ surjektiv, denn $f = \bar{f} \circ \pi_H$. □

4. Konstruktion Wenn $K_1, \dots, K_s$ abelsche Gruppen sind, dann ist das kartesische Produkt $G = K_1 \times K_2 \times \dots \times K_s$ ebenfalls eine abelsche Gruppe, mit Verknüpfung

$$(x_1, \dots, x_s) * (y_1, \dots, y_s) = (x_1 *_{K_1} y_1, \dots, x_s *_{K_s} y_s).$$

5. Der "Chinesische Restsatz" (China v. 300.)

Sei $d_1, \dots, d_s \in \mathbb{N}$. Annahme, für alle $i < j$ gilt $\operatorname{ggT}(d_i, d_j) = 1$ (d.h. die Zahlen $d_1, \dots, d_s$ sind paarweise teilerfremd). Sei $d = d_1 \cdot d_2 \cdots d_s$. Dann gibt es zu beliebigen $a_1, \dots, a_s \in \mathbb{Z}$ genau ein $x \in \mathbb{Z}$ mit $0 \le x < d$ und

$$\begin{aligned} x &\equiv a_1 \pmod{d_1} \\ &\vdots \\ x &\equiv a_s \pmod{d_s} \end{aligned}$$

d.h. die s Kongruenzen sind simultan lösbar, mit einer eindeutigen Lösung in $x \in \{0, \dots, d-1\}$.

Lemma Sei $d_1, \dots, d_s \in \mathbb{N}$ mit $ggT(d_i, d_j) = 1$ für alle $i \neq j$. Dann gilt für $d = d_1 \cdot d_2 \cdots d_s$

$$d_1\mathbb{Z} \cap d_2\mathbb{Z} \cap \dots \cap d_s\mathbb{Z} = d\mathbb{Z}$$

Beweis Es gilt $d\cdot\mathbb{Z} \subseteq d_k\cdot\mathbb{Z}$ für alle $k = 1, \dots, s$, also $d_1\mathbb{Z} \cap \dots \cap d_s\mathbb{Z} \supseteq d\mathbb{Z}$.

Die umgekehrte Inklusion "$\subseteq$" mit Induktion nach s.

Für $s = 0, 1$ ist nichts zu zeigen.

$s = 2$: $d_1\mathbb{Z} \cap d_2\mathbb{Z} \overset{!}{\subseteq} d_1d_2\mathbb{Z}$. Angen., $x \in d_1\mathbb{Z} \cap d_2\mathbb{Z}$, etwa $x = d_1m = d_2n$. Da $ggT(d_1, d_2) = 1$ gibt es $u, v \in \mathbb{Z}$ mit $d_1u + d_2v = 1$. Es folgt

$$x = d_1 \cdot m = d_1 \cdot m(d_1u + d_2v) = d_1 \underbrace{md_2}_{d_2n} u + d_1d_2mv$$

$$= d_1d_2(nu + mv) \in d_1d_2\mathbb{Z} \quad \square$$

$s > 2$ $\underbrace{(d_2\mathbb{Z} \cap \dots \cap d_{s-1}\mathbb{Z})}_{\overset{I.A.}{=} d_1 \cdots d_{s-1}\mathbb{Z}} \cap d_s\mathbb{Z} \overset{s=2}{=} d_1 \cdots d_s\mathbb{Z}$,

denn $ggT(d_1 \cdots d_{s-1}, d_s) = 1$, vgl. §1.10 $\square$

#

6. **Theorem** (Chinesischer Restsatz) Sei $d_1, \dots, d_s \in \mathbb{N}$ mit $ggT(d_i, d_j) = 1$ für alle $i \neq j$. Sei $d = d_1 \cdots d_s$. Dann ist der Homomphism

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}/d_1 \times \mathbb{Z}/d_2 \times \dots \times \mathbb{Z}/d_s$$
$$z \longmapsto ([z]_{d_1}, [z]_{d_2}, \dots, [z]_{d_s})$$

surjektiv mit Kern $\ker(f) = d \cdot \mathbb{Z}$.

Insbesondere erhalten wir einen **Isomorphism**

$$\bar{f}: \mathbb{Z}/d \longrightarrow (\mathbb{Z}/d_1, \dots, \mathbb{Z}/d_s)$$
$$[z]_d \longmapsto ([z]_{d_1}, \dots, [z]_{d_s}).$$

Beis Der Kern von f besteht aus allen $z \in \mathbb{Z}$ mit $z \equiv 0 \pmod{d_1}, \dots, z \equiv 0 \pmod{d_s}$, also $\ker(f) = d_1\mathbb{Z} \cap \dots \cap d_s\mathbb{Z} = d \cdot \mathbb{Z}$

↑ Lemma

Nach dem **Homomplisatz** erhalten wir

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad f \quad} & \mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_s \\ & {\scriptstyle \pi_{d\mathbb{Z}}} \searrow \quad \nearrow {\scriptstyle \bar{f}} & \\ & \mathbb{Z}/d & \end{array}$$

Wir zeigen, dass f surjektiv ist. Sei $1 \le k \le s$, sei $c_k = d_1 \cdots d_{k-1} d_{k+1} \cdots d_s$. Dann gilt $ggT(d_k, c_k) = 1$ nach §1.10, also gibt es $u_k, v_k \in \mathbb{Z}$ mit

$$1 = u_k \cdot d_k + v_k \cdot c_k \Rightarrow \begin{cases} v_k \cdot c_k \equiv 1 \pmod{d_k} \\ v_k \cdot c_k \equiv 0 \pmod{d_j} \text{ für } j \neq k \end{cases}$$

Ist $(a_1, \dots, a_s) \in \mathbb{Z}$, so folgt für $z = a_1 \cdot v_1 \cdot c_1 + a_2 \cdot v_2 \cdot c_2 + \dots + a_s \cdot v_s \cdot c_s$, dass $f(z) = ([a_1]_{d_1}, \dots, [a_s]_{d_s}) \Rightarrow f$ ist surjektiv.

Damit ist $\bar{f}$ bijektiv, also ein Isomorphismus. □

Damit folgt der <u>klassische Chinesische Restsatz</u> §3.5. Wenn $d_1, \dots, d_s$ paarweise teilerfremd sind und $a_1, \dots, a_s \in \mathbb{Z}$ beliebig sind, gibt es genau ein $z \in \mathbb{Z}$ mit $0 \le z < d = d_1 \cdots d_s$ und

$$[z]_{d_1} = [a_1]_{d_1}$$
$$\vdots$$
$$[z]_{d_s} = [a_s]_{d_s}$$

Allerdings sagt der Beweis noch nicht genau, wie wir z finden (aber ungefähr → Ü 4).

7. Def Sei $(G,*)$ eine abelsche Gruppe und sei $x \in G$. Wir definieren für $k \in \mathbb{Z}$

$$x^k = \begin{cases} \underbrace{x * x * \dots * x}_{k\text{-mal}} & \text{wenn } k \geq 1 \\ e & \text{wenn } k = 0 \\ \underbrace{x' * \dots * x'}_{|k|\text{-mal}} & \text{wenn } k < 0 \end{cases}$$

wobei x' das Inverse von x ist. Weiter setzen wir $\langle x \rangle = \{ x^k \mid k \in \mathbb{Z} \} \subseteq G$.

Satz Sei $(G,*)$ eine abelsche Gruppe und sei $x \in G$. Dann gilt:

(i) $\langle x \rangle \subseteq G$ ist eine Untergruppe.

(ii) Ist $H \subseteq G$ eine Untergruppe mit $x \in H$, so ist $\langle x \rangle \subseteq H$.

(iii) Die Abbildung $\mathbb{Z} \to G$, $k \mapsto x^k$ ist ein Homomorphismus mit Bild $\langle x \rangle$.

Man nennt $\langle x \rangle$ die von x erzeugte zyklische Untergruppe von G, vgl. (ii)

Beweis (ii) $H \subseteq G$ Untergruppe mit $x \in H$

$\Rightarrow x' \in H \Rightarrow \langle x \rangle \subseteq H$.

(iii) Mit obiger Definition ist klar:

für $k, l \in \mathbb{Z}$ gilt

$$x^{(k+l)} = x^k * x^l$$

(streng genommen Fallunterscheidung $k \gtrless 0$, $l \gtrless 0$ ...)

also ist $\mathbb{Z} \to G$, $k \mapsto x^k$ ein Homomorphismus.

Das Bild dieser Abbildung ist genau die Menge $\langle x \rangle$.

(i) Das Bild einer abelschen Gruppe unter einem Homomorphismus ist eine Untergruppe ($\to$ üA), also ist $\langle x \rangle$ eine Untergruppe von G. □

Achtung. Wenn wir die Verknüpfung der abelschen Gruppe G mit "$+$" schreiben, dann schreiben wir $k \cdot x$ (statt x^k)! Dann also

$$k \cdot x = \begin{cases} \underbrace{x + \ldots + x}_{k} & k \geq 1 \\ 0 & k = 0 \\ \underbrace{(-x) + \ldots + (-x)}_{|k| \text{-mal}} & k < 0 \end{cases}$$

$$\langle x \rangle = \{ k \cdot x \mid k \in \mathbb{Z} \}$$

$\mathbb{Z} \to G$, $k \mapsto k \cdot x$ usw.

8. Def Sei $(G,*)$ eine abelsche Gruppe, sei $x \in G$.
Wir definieren die Ordnung von x als

$$\operatorname{ord}(x) = \#\langle x \rangle$$

Lemma A Sei $(G,*)$ eine abelsche Gruppe, sei $x \in G$. Dann gilt

(i) $\operatorname{ord}(x) = 1 \iff x = e$

(ii) Wenn $\#G$ endlich ist, so ist $\operatorname{ord}(x)$ auch endlich und $\operatorname{ord}(g) \mid \#G$.

Bew: (i) $\operatorname{ord}(x) = 1 \iff \langle x \rangle = \{e\} \iff x^k = e$ für alle $k \in \mathbb{Z}$
$\iff x = e$

(ii) $\langle x \rangle \leq G$ ist Untergruppe. Wenn G endlich ist, dann ist $\langle x \rangle$ auch endlich und nach dem Satz von Lagrange §2.9 gilt $\operatorname{ord}(x) \mid \#G$ □ #

Lemma B Sei $(G,*)$ eine abelsche Gruppe, sei $x \in G$. Dann sind äquivalent:

(i) $\operatorname{ord}(x) < \infty$

(ii) es gibt $k \in \mathbb{N}$, $k > 0$ mit $x^k = e$

Wenn diese äquivalenten Bedingungen erfüllt sind, dann gilt $\operatorname{ord}(x) = \min\{k \in \mathbb{N} \mid k > 0 \text{ und } x^k = e\}$

Beweis mit Homomorphiesatz. Wir betrachten den Homomorphismus $f: \mathbb{Z} \to G$, $f(k) = x^k$.

(i) $\Rightarrow$ (ii) $\langle x \rangle$ endlich $\Rightarrow$ f nicht injektiv

$\Rightarrow$ $\ker(f) \neq \{0\}$ $\Rightarrow$ $\ker(f) = d \cdot \mathbb{Z} \leq \mathbb{Z}$, $d > 0$
(§3.2) (§2.5)

$\Rightarrow$ $f(d) = x^d = e$ und $d > 0$

(ii) $\Rightarrow$ (i) $k > 0$ und $x^k = e$ $\Rightarrow$ f nicht injektiv

$\Rightarrow$ $\ker(f) \neq \{0\}$ $\Rightarrow$ $\ker(f) = d \cdot \mathbb{Z} \leq \mathbb{Z}$, $d > 0$
(§3.2) (§2.5)

$\Rightarrow$ $\bar{f}: \mathbb{Z}/d \to \langle x \rangle$ Isomorphismus, $\#\mathbb{Z}/d = d < \infty$

Zum Nachsatz: $d = \min\{k \in \mathbb{N} \mid k > 0, [k]_d = [0]\}$
$= \min\{k \in \mathbb{N} \mid k > 0, x^k = e\}$ □

Korollar Sei $(G, *)$ eine endliche abelsche Gruppe, sei $x \in G$. Dann gilt

$$x^{\#G} = e$$

Beweis Sei $d = \mathrm{ord}(x)$, und $m = \#G$. Dann gilt nach Lemma A $d \mid m$, also $m = d \cdot n$ für ein $n \in \mathbb{N}$, also $x^m = (x^d)^n = e^n = e$ □

9. Theorem (Euler) Sei $d \in \mathbb{N}$, $d \geq 1$, sei $x \in \mathbb{Z}$. Wenn gilt $ggT(d,x) = 1$, so gilt für die φ-Funktion

$$x^{\varphi(d)} \equiv 1 \pmod{d}$$

Beis: Da $ggT(d,x) = 1$, folgt $[x]_d \in (\mathbb{Z}/d)^*$, vgl. § 2.15. Weiter ist $\varphi(d) = \#(\mathbb{Z}/d)^*$, nach § 3.8 folgt $[x]_d^{\varphi(d)} = [1]_d$

$$[x^{\varphi(d)}]_d$$

□

(Fermat)

Korollar Sei $p \in \mathbb{P}$ Primzahl und sei $x \in \mathbb{Z}$.

Dann gilt

$$x^p \equiv x \pmod{p}.$$

Falls $p \nmid x$, so gilt $x^{p-1} \equiv 1 \pmod{p}$

Beis: Wenn $p \mid x$, so folgt $x^p \equiv 0 \pmod{p}$ und $x \equiv 0 \pmod{p}$ => fertig.

Wenn $p \nmid x$, so folgt $ggT(p,x) = 1$ (weil p Primzahl) und $\varphi(p) = p-1$, vgl § 2.17. Dann also $x^{p-1} \equiv 1 \pmod{p}$ und folglich auch $x^p \equiv x \pmod{p}$

□

Wir suchen eine (praktische?) Formel für die φ-Funktion. Dazu benötigen wir nochmal etwas Algebra.

10. **Def** Seien $(R,+,\cdot)$ und $(S,+,\cdot)$ kommutative Ringe. Ein Abbildung $f: R \to S$ heißt **Ring-Homomorphismus**, wenn gilt:

(i) Für alle $x,y \in R$ gilt $f(x+y) = f(x)+f(y)$ und $f(x\cdot y) = f(x)\cdot f(y)$

(ii) $f(1) = 1$

Wenn f bijektiv ist, so heißt f **Ring-Isomorphismus**. Dann ist die Umkehrabbildung f^{-1} auch ein Ring-Homomorphismus.

Lemma Sei $f: R \to S$ ein Ringhomomorphismus. Dann gilt:

(i) $\ker(f) = \{x \in R \mid f(x) = 0\}$ ist ein Ideal in R.

(ii) Wenn $x \in R$ eine Einheit ist, so ist auch $f(x) \in S$ eine Einheit.

Insbesondere erhalten wir einen Gruppenhomomorphismus

$$f|_{R^*}: R^* \to S^*.$$

Bsp (i) Sei $x, y \in \ker(f)$, $z \in R$. Dann folgt
$f(x \pm y) = f(x) \pm f(y) = 0 \pm 0 = 0$, also ist $\ker(f)$
eine Untergruppe von $(R, +)$. Weiter gilt
$f(x \cdot z) = f(x) \cdot f(z) = 0 \cdot f(z) = 0$, also
$x \cdot z \in \ker(f) \Rightarrow \ker(f)$ ist Ideal in R.

(ii) Angenommen, es gibt $y \in R$ mit $x \cdot y = 1$.
Es folgt $f(x) \cdot f(y) = 1 \Rightarrow f(x) \in S^*$ □

Beispiel Sei $m \in \mathbb{N}$. Dann ist die Abbildung

$f: \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$, $x \longmapsto [x]_m$ ein
Ringhomomorphismus mit $\ker(f) = m\cdot\mathbb{Z}$.

11. Theorem (Der Homomorphiesatz für Ringe)

Sei $f: R \to S$ ein Ringhomomorphismus und
sei $J = \ker(f) \subseteq R$. Dann ist die Abbildung
$\pi_J: R \to R/J$ ein Homomorphismus und
es gibt genau ein Homomorphismus $\bar{f}: R/J \to S$
mit $f = \bar{f} \circ \pi_J$,

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ & \searrow^{\pi_J} \quad \nearrow_{\bar{f}} & \\ & R/J & \end{array}$$

Dann ist $\bar{f}$ injektiv.

Beis Ein Ring homomorphismus ist insbesondere ein Gruppenhomomorphismus von $(R,+)$ nach $(S,+)$. Der Homomorphiesatz für Gruppen §3.3 zeigt die Existenz, Eindeutigkeit und Injektivität von $\bar{F}$. Bleibt noch zu zeigen: π_J und $\bar{F}$ sind Ringhomomorphismen.

$$\pi_J(x\cdot y) = x\cdot y + J \overset{\text{Def}}{=} (x+J)\cdot(y+J) = \pi_J(x)\cdot\pi_J(y)$$
vgl. §2.12 (V)

$\pi_J(1) = 1+J$ ist Einselement in R/J. (V)

$$\bar{F}((x+J)\cdot(y+J)) = \bar{F}(x\cdot y+J) = f(x\cdot y) = f(x)\cdot f(y)$$

$$= \bar{F}(x+J)\cdot\bar{F}(y+J) \quad (V)$$

$$\bar{F}(1+J) = f(1) = 1 \quad (V)$$

□ #

Beobachtung Sind $R_1,\dots,R_n$ kommutative Ringe, so ist auch $R = R_1\times\dots\times R_n$ ein kommutativer Ring mit Verknüpfungen

$$(x_1,\dots,x_n)+(y_1,\dots,y_n) = (x_1+y_1,\dots,x_n+y_n)$$

$$(x_1,\dots,x_n)\cdot(y_1,\dots,y_n) = (x_1\cdot y_1,\dots,x_n\cdot y_n)$$

und Einselement

$$1_R = (1,1,1,\dots,1)$$

12. Theorem (Chinesischer Restsatz, Vollversion)

Sei $d_1, \dots, d_s \in \mathbb{N}$ mit $ggT(d_i, d_j) = 1$ für alle $i \neq j$. Dann ist der Ringhomomorphismus

$$f: \mathbb{Z} \to \mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_s$$
$$z \mapsto ([z]_{d_1}, \dots, [z]_{d_s})$$

surjektiv, mit $\ker(f) = d \cdot \mathbb{Z}$, wobei $d = d_1 \cdot d_2 \cdots d_s$.

Insbesondere sind die Ringe $\mathbb{Z}/d$ und $\mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_s$ isomorph.

Beweis: Die Abbildung f ist ein Ringhomomorphismus, denn

$$f(x+y) = ([x+y]_{d_1}, \dots, [x+y]_{d_s}) = ([x]_{d_1} + [y]_{d_1}, \dots, [x]_{d_s} + [y]_{d_s})$$
$$= f(x) + f(y)$$

$$f(x \cdot y) = ([x \cdot y]_{d_1}, \dots, [x \cdot y]_{d_s}) = ([x]_{d_1} \cdot [y]_{d_1}, \dots, [x]_{d_s} \cdot [y]_{d_s})$$
$$= f(x) \cdot f(y)$$

$$f(1) = ([1]_{d_1}, \dots, [1]_{d_s}) \qquad (*)$$

Die Behauptung folgt damit aus §3.6. □

13. Beobachtung. Sind $R_1, \dots, R_s$ kommutative Ringe mit Einheitengruppen $R_1^*, \dots, R_s^*$, so gilt für $R = R_1 \times \dots \times R_s$, dass $R^* = R_1^* \times \dots \times R_s^*$. Denn:

$1_R = (x_1, \dots, x_s) \cdot (y_1, \dots, y_s) \Leftrightarrow x_1 \cdot y_1 = 1, \dots, x_s \cdot y_s = 1$ (*)

Satz Sind $d_1, \dots, d_s \in \mathbb{N}$, $d_1, \dots, d_s \geq 1$ mit $\operatorname{ggT}(d_i, d_j) = 1$ für alle $i \neq j$. Dann gilt $\varphi(d_1 \cdots d_s) = \varphi(d_1) \cdot \dots \cdot \varphi(d_s)$.

Beweis Es gilt $\varphi(d) = \#(\mathbb{Z}/d)^*$. Für $d = d_1 \cdots d_s$ folgt aus dem Isomorphismus

$\mathbb{Z}/d \xrightarrow{\overline{F}} \mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_s$, denn

$(\mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_s)^* = (\mathbb{Z}/d_1)^* \times \dots \times (\mathbb{Z}/d_s)^*$

nach der vorigen Beobachtung. □

Beispiel • $60 = 4 \cdot 3 \cdot 5$ p.w. teilerfremd.

$\varphi(4) = 2 \quad \varphi(3) = 2 \quad \varphi(5) = 4$

$\Rightarrow \varphi(60) = \varphi(4) \cdot \varphi(3) \cdot \varphi(5) = 16$

• $4 = 2 \cdot 2$, $\varphi(2) = 1$, aber $\varphi(4) \neq \varphi(2) \cdot \varphi(2)$ ▽

Hier gilt die Formel also nicht – aber es ist auch $\operatorname{ggT}(2,2) = 2 \neq 1$.

Zu einer vollständigen Formel für φ fehlt nun noch folgendes Ergebnis

Lemma Sei $p \in \mathbb{P}$ Primzahl und sei $l \in \mathbb{N}$, $l \geq 1$.

Es gilt $\varphi(p^l) = p^{l-1} \cdot (p-1)$

Beweis Die nicht-Einheiten in $\mathbb{Z}/p^l$ sind nach §2.15 genau die Kongruenzklassen

$[0]_{p^l}, [p]_{p^l}, [2p]_{p^l}, \ldots, [p^l - p]_{p^l}, [p^l]_{p^l} = [0]_{p^l}$

insgesamt also p^{l-1} Kongruenzklassen. Folglich ist $\varphi(p^l) = p^l - p^{l-1} = p^{l-1}(p-1)$. □

14. Satz Sei $n \in \mathbb{N}$, $n \geq 2$. Sei

$n = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$ die Primfaktor-Zerlegung von n, $p_1 < p_2 < \ldots < p_s$ Primzahlen, $l_1, \ldots, l_s \geq 1$ vgl. Hauptsatz der Arithmetik §1.13. Dann gilt

$$\varphi(n) = p_1^{l_1-1}(p_1-1) \cdots p_s^{l_s-1}(p_s-1)$$

oder kurz

$$\varphi(n) = n \cdot \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

Beis Die erste Formel folgt aus §3.13 und die zweite Formel durch Umstellen

$$p_k^{l_k-1}(p_k-1) = p_k^{l}\left(1 - \frac{1}{p_k}\right)$$

□

15. Eine Anwendung: das RSA-Kryptographieverfahren

Allgemeines Prinzip: (Public Key Kryptographie)

M ist eine endliche Menge (z.B. ein Alphabet), $g: M \to M$ ist eine bijektive Abbildung mit Umkehrabbildung $h: M \to M$, d.h. $h(g(x)) = x$ für alle $x \in M$. Die Abbildung g ist öffentlich bekannt, nicht aber h. Der Sender bekommt $x \in M$, in dem er $g(x)$ sendet. Der Empfänger bekommt $y = g(x)$ mit $h(y) = h(g(x)) = x$.

Klar: im Prinzip kennt man h, wenn g bekannt ist. Aber in der Praxis kann die Berechnung von h aus g sehr aufwendig sein, wenn M groß ist.

Das RSA-Verfahren

(Rivest, Shamir, Adleman 1977)

Seien $p_1 < p_2 < \dots < p_s$ Primzahlen, $s \geq 2$.

Sei $m = p_1 \cdot p_2 \cdots p_s$ und $M = \mathbb{Z}/m$,

$l = \varphi(m) = (p_1 - 1)(p_2 - 1) \cdots (p_s - 1)$,

Wähle $a, b \in \mathbb{N}$, $a, b \geq 2$ mit $a \cdot b \equiv 1 \pmod{l}$

Die Zahl a und m sind öffentlich bekannt, dagegen ist b geheim. Man setzt

$$g([x]_m) = [x^a]_m \qquad \text{(öffentlich)}$$

$$h([y]_m) = [y^b]_m \qquad \text{(geheim)}$$

Um b zu bestimmen, muss man $l = \varphi(m)$ kennen. Wenn die Primfaktorzerlegung von m $= p_1 \cdots p_s$ nicht bekannt ist, dann ist die Berechnung von l und b sehr zeitaufwendig.

#

Lemma Unter den Voraussetzungen oben gilt $h(g([x]_m)) = [x]_m$, d.h. das RSA-Verfahren funktioniert.

Beweis Es gilt $a \cdot b = 1 + \ell \cdot k$ für ein $k \in \mathbb{N}$.

Zu zeigen ist $[x]_m^{a \cdot b} = [x]_m^{1+\ell \cdot k} \overset{!}{=} [x]_m$.

Wir betrachten den Isomorphismus von Ringen

$$f: \mathbb{Z}/m \longrightarrow \mathbb{Z}/p_1 \times \dots \times \mathbb{Z}/p_s$$

$$f([x]_m) = ([x]_{p_1}, \dots, [x]_{p_s})$$ aus dem Chinesischen Restsatz § 3.12.

Wegen

$$f([x]_m^{a \cdot b}) = f([x]_m)^{a \cdot b}$$ genügt es zu zeigen: Für jedes $x \in \mathbb{Z}$ gilt

$$[x]_{p_j}^{a \cdot b} = [x]_{p_j} \qquad j = 1, \dots, s$$

Wenn $x \equiv 0 \pmod{p_j}$, so $[x]_{p_j}^{a \cdot b} = [0]_{p_j}^{a \cdot b}$

$a \cdot b \geq 1$

$= [0]_{p_j} = [x]_{p_j}$ q.e.d.

Wenn $x \not\equiv 0 \pmod{p_j}$, so folgt aus Eulers Satz § 3.9 $x^{p_j-1} \equiv 1 \pmod{p_j}$,

also $x^{a \cdot b} = x^{1+(p_1-1)\cdots(p_0-1)\cdot k}$

$\equiv x \cdot 1 \pmod{p_j}$

d.h. $[x]^{a \cdot b}_{p_j} = [x]_{p_j}$ ⇒ auch Behg. $\square$

Bem. Die Sicherheit des RSA-Verfahren beruht nur darauf, dass $\varphi(m)$ sehr schwer (= langsam) berechenbar ist.

Beispiel (nicht realistisch) $s = 2$,

$p_1 = 3$, $p_2 = 5$, $m = 3 \cdot 5 = 15$, $l = 2 \cdot 4 = 8$

$a = 3$, $b = 3$ $\quad 3 \cdot 3 = 9 \equiv 1 \pmod{l}$

Kodierung: $g([x]_{15}) = [x^3]_{15}$

$h([y]_{15}) = [y^3]_{15}$

$h(g(x)) = [x]^{9}_{15} \overset{!}{=} [x]_{15}$ für alle x.

z.B. $x = 7$ $\quad [7]^3_{15} = [49]_{15} \cdot [7]_{15} = [4 \cdot 7]_{15} = [-2]_{15}$

$g([7]_{15}) = [-2]_{15}$ $\quad h([-2]_{15}) = [-2]^3_{15} = [-8]_{15} = [7]_{15}$

$\square$