§3 Kommutative Ringe

1. <u>Erinnerung/Definition</u> Sei $(R,+)$ eine abelsche Gruppe mit Neutralelement $0 \in R$. Sei

$$\begin{aligned} R \times R &\longrightarrow R \\ (a,b) &\longmapsto a \cdot b = ab \end{aligned}$$

eine assoziative Verknüpfung (d.h. $a(bc) = (ab)c$ gilt für alle $a,b,c \in R$). Wir nennen $(R,+,\cdot)$ einen <u>kommutativen Ring</u>, wenn für alle $a,b,x,y \in R$ gilt:

(R1) Die <u>Distributivgesetze</u> gelten

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

(R2) Es gibt ein <u>Einselement</u> $1 \in R$, mit

$$1 \cdot a = a = a \cdot 1$$

(R3) Die Multiplikation ist <u>kommutativ</u>,

$$ab = ba$$

Wenn nur R1 und R2 gefordert wird, spricht man von einem <u>nicht kommutativen Ring</u>.

Wenn nur R1 gefordert wird, spricht man von einem <u>Ring ohne Eins</u> (oder "<u>Rng</u>"). (*)

(*) Stammt aus Jacobsons Algebra-Buch

2. Beispiele (a) Jeder Körper ist ein kommutativer Ring

(b) $\mathbb{Z}$ ist ein kommutativer Ring (mit der "gewöhnlichen" Addition und Multiplikation)

(c) Für $m > 1$ ist $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ ein Ring

(d) Sei V ein K-Vektorraum. Dann ist $\mathrm{End}(V) = \{\varphi : V \to V \mid \varphi \text{ linear}\}$ ein Ring mit

$$\varphi + \psi : v \longmapsto \varphi(v) + \psi(v) \qquad \varphi, \psi \in \mathrm{End}(V)$$
$$\varphi \circ \psi : v \longmapsto \varphi(\psi(v))$$

Wenn $\dim(V) > 1$ gilt, ist $\mathrm{End}(V)$ nicht kommutativ.

(e) $R = \{0\}$ mit $0 \cdot 0 = 0 + 0 = 0$ ist Ring mit $0 = 1$ (!), der Nullring / triviale Ring.

#

3. Rechenregeln in Ringen

(a) Additiv darf man kürzen:

$$a + x = a + y \Rightarrow x = y$$

(addiere $-a$ auf beiden Seiten)

(b) Es gilt stets $0 \cdot a = a \cdot 0 = 0$

(c) Es gilt $a(-b) = -(ab) = (-a)b$
und $(-a)(-b) = ab$
$$(-1)a = -a = a(-1)$$

Beweis (b) $0 \cdot a = (0+0)a \overset{(R1)}{=} 0a + 0a \overset{\text{Kürzen}}{\Rightarrow} 0a = 0$

genauso $a0 = 0$

(c) $a(-b) + ab \overset{R1}{=} a(b-b) = a0 = 0 \Rightarrow a(-b) = -(ab)$

genauso $(-a)b + ab = (-a+a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$

$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$

sowie $(-1)a = -(1a) = -a = a(-1)$ $\square$

Vorsicht! Beim Multiplizieren darf man nicht immer einfach kürzen. Bsp $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $x = \begin{pmatrix} 1 & \\ & 2 \end{pmatrix}$

$a, x, y \in \mathbb{R}^{2\times 2}$ $ax = ay$, aber $x \neq y$ $y = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$

3. Def Sei R ein Ring. Ein Element $a \in R$ heißt Einheit, wenn es $b \in R$ gibt mit

$$ab = 1 = ba$$

Die Menge aller Einheiten ist die Einheitengruppe

$$R^* = \{ a \in R \mid a \text{ Einheit} \}$$

Offensichtlich ist $(R^*, \cdot)$ eine Gruppe, mit 1 als Neutralelement.

Bsp (a) K Körper, $K^* = K - \{0\}$

(b) $\mathbb{Z}^* = \{\pm 1\}$

(c) $\mathrm{End}(V)^* = GL(V) = \{ \varphi : V \to V \mid \varphi \text{ linear + bijektiv} \}$

(d) $R = \{0\}$, $R^* = R$

4. Homomorphismen und Ideale

Seien R und S Ringe. Eine Abbildung $\varphi: R \to S$ heißt Ringhomomorphismus, wenn für alle $x, y \in R$ gilt

(H1) $\varphi(x+y) = \varphi(x) + \varphi(y)$

(H2) $\varphi(xy) = \varphi(x)\varphi(y)$

(H3) $\varphi(1_R) = 1_S$

(H1) sagt, dass φ ein Homomorphismus der additiven Gruppen $(R,+)$ und $(S,+)$ ist.

Der Kern eines Ringhomomorphismus φ ist

$$\ker(\varphi) = \{ x \in R \mid \varphi(x) = 0 \}$$

Ist R ein Ring und $S \subseteq R$ eine Teilmenge mit folgenden Eigenschaften, so heißt S Teilring oder Unterring

(TR1) $0 \in S$ und $x \pm y \in S$ für alle $x, y \in S$

(TR2) $x \cdot y \in S$ für alle $x, y \in S$

(TR3) $1 \in S$

Wenn nur (TR1) und (TR2) verlangt wird, spricht man von einem "Teilrng"

Sei R ein Ring. Ein Teilrng $I \subseteq R$ heißt Ideal, wenn für alle $r \in R$ und $i \in I$ gilt

$$ir \in I \text{ und } ri \in I$$

Man schreibt dann $I \trianglelefteq R$.

Für ein Ideal $I \trianglelefteq R$ gilt offensichtlich

$$I = R \iff 1 \in I$$

(denn: $1 \in I \Rightarrow r = r1 \in I$ für alle $r \in R$.)

Konstruktion Sei R Ring und $I \trianglelefteq R$ Ideal. Dann ist $R/_{I} = \{x+I \mid x \in R\}$ ein Ring mit Multiplikation

$$(x+I)(y+I) = xy+I$$

Beweis: Das ist eine wohldefinierte Verknüpfung,

$$\left.\begin{array}{l} x+I = x'+I \\ y+I = y'+I \end{array}\right\} \Rightarrow \begin{array}{l} x' = x+i \\ y' = y+j \end{array} \text{ für } i,j \in I \left.\right\} \Rightarrow x'y'+I = (x+i)(y+j)+I$$

$$= xy + \underbrace{iy+xj+ij}_{\in I} + I = xy+I.$$ Es gilt weiter

$$(1+I)(x+I) = (x+I) = (x+I)(1+I)$$ □

Satz Sei R ein Ring und $I \subseteq R$. Dann sind äquivalent:
(i) $I \trianglelefteq R$ (ii) Es gibt einen Ring S und einen Homomorphismus $R \xrightarrow{\varphi} S$ mit $\ker(\varphi) = I$.

Beweis (i) ⇒ (ii)

Setze $S = R/_{I}$, $\pi_I : R \to S$
$x \longmapsto x+I$

Nach obiger Konstruktion ist $R/_{I}$ ein Ring.
Es gilt $\ker(\pi_I) = \{x \in R \mid x+I = I\} = I$.

(ii) $\Rightarrow$ (i) Sei $\varphi : R \to S$ ein Ringhomomorphismus mit $I = \ker(\varphi)$. Dann ist $(I,+)$ Untergruppe von $(R,+)$. Für alle $i \in I$, $r \in R$ gilt

$$\left.\begin{array}{l} \varphi(ir) = \varphi(i)\varphi(r) = 0_S \cdot \varphi(r) = 0_S \\ \text{und } \varphi(ri) = \ldots = 0_S \end{array}\right\} \Rightarrow \begin{array}{c} ir \\ ri \end{array} \in I$$

$\square$

5. Homomorphiesatz für Ringe, Isomorphiesätze

<u>Satz</u> (Homomorphiesatz) Sei $R \xrightarrow{\varphi} S$ ein Ringhomomorphismus, sei $I \trianglelefteq R$ Ideal mit $I \subseteq \ker(\varphi)$. Dann gibt es genau einen Ringhomomorphismus $\bar{\varphi} : R/I \to S$ mit $\bar{\varphi} \circ \pi_I = \varphi$

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi_I"'] & & S \\ & R/I \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

<u>Beweis</u> Aus dem Isomorphiesatz für Gruppen § 1.20, angewendet auf den Gruppenhomomorphismus $(R,+) \xrightarrow{\varphi} (S,+)$ erhalten wir die Existenz und Eindeutigkeit des Gruppenhomomorphismus $\bar{\varphi}$. Zu zeigen bleibt, dass $\bar{\varphi}$ ein Ringhomomorphismus ist. Für $x \in R$ gilt

$$\bar{\varphi}(x+I) = \varphi(x) \qquad \text{vgl § 1.20}$$

$$\bar{\varphi}(xy+I) = \varphi(xy) \underset{\substack{\uparrow \\ \varphi \text{ Ringhom}}}{=} \varphi(x)\varphi(y) = \bar{\varphi}(x+I)\,\bar{\varphi}(y+I)$$

sowie $\bar{\varphi}(1_R+I) = \varphi(1_R) = 1_S$

$\square$

Satz (1. Isomorphiesatz für Ringe) Sei R Ring, $S \subseteq R$ Teilring und $I \trianglelefteq R$ Ideal. Dann ist
$$S+I = \{s+i \mid s \in S,\ i \in I\} \subseteq R \text{ Teilring und}$$
$S \cap I \trianglelefteq S$ Ideal. Die Abbildung
$$S/_{S\cap I} \xrightarrow{\varphi} S+I/_{I}$$
$$s + S\cap I \longmapsto s+I$$
ist ein Ringisomorphismus (bijektiver Ringhomomorphismus).

Beweis Klar: $S+I$ und $S\cap I$ sind Untergruppen in $(R,+)$.

Für $s,s' \in S$, $i,i' \in I$ gilt $(s+i)(s'+i') = ss' + \underbrace{is' + si + ii'}_{\in I} \in S+I$

sowie $1 \in S \subseteq S+I \Rightarrow S+I \subseteq R$ ist Teilring.

Für $s \in S$, $i \in I\cap S$ gilt $\left.\begin{array}{l} is \in I\cap S \\ si \in I \cap S \end{array}\right\} \Rightarrow I\cap S \trianglelefteq S$.

Die Abbildung $\varphi: s + S\cap I \longmapsto s+I$ ist nach §1.23 ein Gruppenisomorphismus bezüglich der Addition. Es gilt $\varphi(1 + S\cap I) = 1+I$ sowie für $s,t \in S$
$$\varphi(st + I\cap S) = st+I = (s+I)(t+I) = \varphi(s+I\cap S)\varphi(t+I\cap S)$$
$\square$

Satz (2. Isomorphiesatz für Ringe) Sei R Ring, $I, J \trianglelefteq R$ Ideale mit $I \subseteq J$. Dann ist
$$J/_I = \{j + I \mid j \in J\} \subseteq R/_I \quad \text{ein Ideal und es gibt}$$
einen Isomorphismus von Ringen
$$R/_I \Big/ J/_I \xrightarrow{\cong} R/_J$$

<u>Beweis</u> (Genau wie in §1.23)

(a) betrachte $\varphi : R \to R/J$, $x \mapsto x + J$

$\leadsto$ Homomorphismus $\overline{\varphi} : R/I \to R/J$ (Homomorphiesatz)

$\ker(\overline{\varphi}) = J/I$, also $(R/I)/(J/I) \xrightarrow{\cong} R/J$ $\square$

<u>Bem</u> Ein <u>Ringisomorphismus</u> ist also ein bijektiver Ringhomomorphismus $\varphi : R \to S$.
Die Umkehrabbildung ψ von φ, $\psi : S \to R$ ist dann ebenfalls ein Ringhomomorphismus (Ringisomorphismus).

6. <u>Rechnen mit Idealen</u> Sei R ein Ring mit Idealen $I, J \trianglelefteq R$. Dann sind auch die folgenden Mengen Ideale:

(a) $I + J = \{ i + j \mid i \in I, j \in J \}$

(b) $I \cap J$

(c) $IJ = \{ i_1 j_1 + i_2 j_2 + \dots + i_\ell j_\ell \mid \ell \geq 1, i_1, \dots, i_\ell \in I, j_1, \dots, j_\ell \in J \}$

Es gilt $IJ \subseteq I \cap J \subseteq I, J \subseteq I + J$

<u>Beweis</u> Klar: $I + J$, $I \cap J$ und IJ sind additive Gruppen. Sei $r \in R$, $i \in I$, $j \in J$. Es folgt

$r(i+j) = \underbrace{ri + rj}_{\in I+J}$, $(i+j)r = \underbrace{ir + jr}_{\in I+J}$ $\Rightarrow$ $I + J \trianglelefteq R$

$i \in I \cap J \Rightarrow ri \in I \cap J \Rightarrow I \cap J \trianglelefteq R$

$r(ij) = \underbrace{ri}_{\in I} \cdot j \in J$ genauso $r(ij) \in I$, also

$IJ \trianglelefteq R$ und $IJ \subseteq I \cap J$. $\square$

7. Beispiele (a) K ein Körper.

Ist $I \trianglelefteq K$ Ideal und $I \neq \{0\}$, so folgt $1 \in I$,

denn: $i \in I - \{0\} \Rightarrow i^{-1} i = 1 \in I \Rightarrow I = K$.

Also sind $\{0\}$ und K die einzigen Ideale in K. #

(b) $V \neq \{0\}$ ein K-Vektorraum $R = \mathrm{End}(V)$.

Die einzigen Ideale in R sind $\{0\}$, R

(→ höhere Algebra?)

(c) R kommutativer Ring, $a \in R$. Setze

$(a) = Ra = \{ra \mid r \in R\}$. Dann gilt $(a) \trianglelefteq R$

(später genauer)

(d) $R = \mathbb{Z}$. Wie wir gleich: jedes Ideal $I \trianglelefteq \mathbb{Z}$

ist von der Form $I = m\mathbb{Z} = \{mh \mid h \in \mathbb{Z}\}$ für

ein $m \in \mathbb{N}$. Als Quotient erhält man für $m \geq 1$

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

$\bar{k} = k + m\mathbb{Z}$ (die Bedeutung des Querstrichs hängt also von m ab!!)

$\bar{k} \cdot \bar{l} = \overline{kl}$ und §3.4. Also ist für $m \geq 1$

$\mathbb{Z}/m$ ein kommutativer Ring mit m

Elementen.

8. Satz Sei $I \subseteq \mathbb{Z}$ eine Teilmenge. Dann sind äquivalent

(i) $I = m\mathbb{Z}$ für ein $m \in \mathbb{N}$

(ii) $I \subseteq \mathbb{Z}$ ist Untergruppe bezüglich Addition

(iii) $I \subseteq \mathbb{Z}$ ist Ring bezüglich Addition und Multiplikation

(iv) $I \subseteq \mathbb{Z}$ ist ein Ideal.

Beweis Es gilt (iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii). Ist $r \in \mathbb{Z}$ und $mk \in m\mathbb{Z}$, so folgt $rmk \in m\mathbb{Z}$, also haben wir auch (i) $\Rightarrow$ (iv). Bleibt zu zeigen, dass gilt (ii) $\Rightarrow$ (i). Sei also $I \subseteq \mathbb{Z}$ Untergruppe bzgl $+$.

1. Fall $I = \{0\} \Rightarrow I = 0\mathbb{Z}$ fertig

2. Fall $I \neq \{0\}$, es gibt also ein $x \neq 0$ in I.

Wegen $\pm x \in I$ folgt: es gibt ein $x > 0$ in I. Setze

$m = \min\{x \in I \mid x > 0\}$. Es folgt $m \in I$, also $\langle m \rangle = m\mathbb{Z} \subseteq I$. Beh: $I = m\mathbb{Z}$.

Angenommen, es gibt ein $x \in I - m\mathbb{Z}$. Dann gilt

$x = mk + l$ für ein l, $0 < l < m$ (Teilen mit Rest)

es folgt wegen $mk \in I$, dass $x - mk = l \in I$, ein Widerspruch zur Minimalität von m, denn $0 < l < m$ □

9. Definition Sei R ein Ring. Ein Element $a \in R$ heißt Nullteiler, wenn es ein $b \in R - \{0\}$ gibt mit $ab = 0$ oder $ba = 0$.

Beispiel (a) In $\mathbb{Z}$ ist 0 der einzige Nullteiler.

(b) In $\mathbb{Z}/6$ gilt $\bar{2} \neq \bar{0} \neq \bar{3}$, aber $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$, also sind $\bar{2}$ und $\bar{3}$ Nullteiler in $\mathbb{Z}/6$.

Beobachtung Ist R ein Ring und ist $a \in R$ kein Nullteiler, dann gilt: $ax = ay \Rightarrow x = y$.

Denn: $ax = ay \Rightarrow a(x-y) = 0 \underset{\substack{\uparrow \\ a \text{ kein Nullteiler}}}{\Rightarrow} x - y = 0 \Rightarrow x = y$.

Multiplikation darf man also kürzen, wenn a kein Nullteiler ist.

Ab jetzt betrachten wir kommutative Ringe.

10. Definition Ein kommutativer Ring R heißt Integritätsbereich (engl. integral domain oder domain), wenn gilt

(IB 1) $R \neq \{0\}$

(IB 2) Der einzige Nullteiler in R ist 0.

Beispiele (a) $\mathbb{Z}$ ist Integritätsbereich

(b) jeder Körper ist ein Integritätsbereich

(c) $\mathbb{Z}/6$ ist kein Integritätsbereich.

In Integritätsbereich darf man also multiplikativ kürzen, wenn man die Null auslässt: aus $a \neq 0$ und $ax = ay$ folgt dann $x = y$.

Lemma Jeder endliche Integritätsbereich ist ein Körper.

Beweis Sei R ein endlicher Integritätsbereich. Dann gilt $R \neq \{0\}$ und (IB1). Sei $a \in R - \{0\}$, betrachte die Abbildung $\lambda_a : R \to R$, $x \mapsto ax$. Wegen $a \neq 0$ ist λ_a injektiv: $\lambda_a(x) = \lambda_a(y) \Rightarrow ax = ay \Rightarrow x = y$. Da R endlich ist, ist λ_a bijektiv, also surjektiv. Folglich gibt es ein $b \in R$ mit $\lambda_a(b) = ab = 1$. Es folgt $ab = ba = 1$, also $R^* = R - \{0\}$ $\square$

Beachte $\mathbb{Z}$ ist ein unendlicher Integritätsbereich, aber kein Körper. Allerdings ist $\mathbb{Z}$ ein Teilring im Körper $\mathbb{Q}$. Wir überlegen jetzt, dass jeder Integritätsbereich Teilring eines Körpers ist, vgl. LA II §5.3

11. Der Quotientenkörper eines Integritätsbereichs

Idee: Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ imitieren, Brüche $\frac{a}{b}$ als Äquivalenzklassen.

Sei R ein Integritätsbereich, sei $Q = \{(x,y) \in R \times R \mid y \neq 0\}$.
Wir definieren zwei Verknüpfungen $+, \cdot$ auf Q durch

$$(x,y) + (u,v) = (xv + yu, yv) \qquad \left(\text{"} \frac{x}{y} + \frac{u}{v} = \frac{xv+yu}{yv} \text{"}\right)$$

$$(x,y) \cdot (u,v) = (xu, yv) \qquad \left(\text{"} \frac{x}{y} \cdot \frac{u}{v} = \frac{xu}{yv} \text{"}\right)$$

(dabei haben wir benutzt, dass R ein Integritätsbereich ist).

Es gilt $(x,y) + (0,1) = (x,y) = (0,1) + (x,y)$
$(x,y) \cdot (1,1) = (x,y) = (1,1) \cdot (x,y)$

Beide Verknüpfungen sind auch assoziativ (nachrechnen)

Allerdings ist Q kein Ring, es fehlt die Kürzungsregel für Brüche. Wir definieren eine binäre (zweistellige) Relation $\sim$ auf Q durch $(x,y) \sim (x',y') \Leftrightarrow xy' = x'y$.

Beh: $\sim$ ist eine Äquivalenzrelation auf Q.

Denn: $(x,y) \sim (x,y)$ klar
$(x,y) \sim (x',y') \Rightarrow (x',y') \sim (x,y)$ klar
$(x,y) \sim (u,v) \sim (a,b) \Rightarrow xv = yu$ und $ub = va$
$\Rightarrow xvb = yub = yva \underset{\text{IB},\, v \neq 0}{\Rightarrow} xb = ya$

Wir bezeichnen die Äquivalenzklasse von (a,b) mit $\frac{a}{b}$ und setzen $\mathrm{Quot}(R) = \left\{ \frac{a}{b} \mid (a,b) \in Q \right\}$

Beh $\left.\begin{array}{l}(x,y)\sim(x',y')\\(u,v)\sim(u',v')\end{array}\right\} \Rightarrow (x,y)+(u,v)\sim(x',y')+(u',v')$
und $(x,y)\cdot(u,v)\sim(x',y')(u',v')$

Denn: $(xv+yu, yv)\sim(x'v'+u'y', y'v')$

$\Leftrightarrow \underbrace{xy'}vv'+\underbrace{uv'}yy' = \underbrace{x'y}vv'+\underbrace{u'v}yy'$

und $xy'=x'y$ sowie $uv'=u'v$, Rest genauso.

Folgerung: Wir erhalten wohldefinierte Verknüpfungen

$$\frac{x}{y}+\frac{u}{v}=\frac{xv+yu}{yv} \qquad \frac{x}{y}\cdot\frac{u}{v}=\frac{xu}{yv}$$

Eine Routine-Rechnung zeigt: $(\mathrm{Quot}(R),+,\cdot)$ ist ein Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}\neq\frac{0}{1}$

Ist $a,b\neq 0$ so gilt $\frac{a}{b}\cdot\frac{b}{a}=\frac{1}{1}$, also ist $\mathrm{Quot}(R)$ sogar ein Körper.

Wir definieren $\iota: R\to\mathrm{Quot}(R)$

$$r\longmapsto\frac{r}{1}$$

das ist ein Ringhomomorphismus und injektiv, $\ker(\iota)=\{0\}$.

Für $R=\mathbb{Z}$ erhalten wir genau $\mathrm{Quot}(\mathbb{Z})=\mathbb{Q}$.

Satz Der Quotientenkörper $\mathrm{Quot}(R)$ hat folgende universelle Eigenschaft: Ist K ein Körper und R ein Integritätsbereich und ist $\varphi: R\to K$ ein injektiver Ringhomomorphismus, so gibt es genau einen Ringhomomorphismus $\tilde\varphi:\mathrm{Quot}(R)\to K$ mit $\tilde\varphi\circ\iota=\varphi$

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & K \\ & \mathrm{Quot}(R) \arrow[ur, "\tilde\varphi"'] & \end{tikzcd}$$

Bew. Definiere $\tilde\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$. Das ist wohldefiniert:

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b \Rightarrow \varphi(a)\underbrace{\varphi(b')}_{\neq 0} = \varphi(a')\underbrace{\varphi(b)}_{\neq 0}$$

$$\Rightarrow \frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(a')}{\varphi(b')} \qquad \varphi \text{ injektiv}$$

Es folgt (nachrechnen), dass $\tilde\varphi$ ein Homomorphismus ist,

$$\tilde\varphi\left(\frac{a}{b} + \frac{u}{v}\right) = \tilde\varphi\left(\frac{a}{b}\right) + \tilde\varphi\left(\frac{u}{v}\right) \qquad \tilde\varphi\left(\frac{a}{b}\cdot\frac{u}{v}\right) = \tilde\varphi\left(\frac{a}{b}\right)\tilde\varphi\left(\frac{u}{v}\right)$$

$$\tilde\varphi\left(\frac{1}{1}\right) = 1_K .$$

Zur Eindeutigkeit von $\tilde\varphi$: Angenommen, $\psi: \mathrm{Quot}(R) \to K$ ist ein Homomorphismus mit $\psi \circ \iota = \varphi$. Für $a, b \in R$, $b \neq 0$ folgt $\varphi(a) = \psi\left(\frac{a}{1}\right)$ $\varphi(b) = \psi\left(\frac{b}{1}\right) \neq 0$

$$\Rightarrow \psi\left(\frac{1}{b}\right) = \frac{1}{\varphi(b)} \Rightarrow \psi\left(\frac{a}{b}\right) = \psi\left(\frac{a}{1}\cdot\frac{1}{b}\right) = \frac{\varphi(a)}{\varphi(b)} \qquad \square$$

Wir betrachten jetzt Ideale in Ringen und vor allem in Integritätsbereichen.

12. Satz Sei $\varphi: R \to S$ ein Homomorphismus von (kommutativen oder nicht kommutativen Ringen).
Wenn $I \trianglelefteq R$ ein Ideal ist, so ist $\varphi(I) \trianglelefteq \varphi(R)$ Ideal (und $\varphi(R) \subseteq S$ ist Teilring).
Wenn $J \trianglelefteq S$ ein Ideal ist, so ist $\varphi^{-1}(J) = \{ r \in R \mid \varphi(r) \in J \} \trianglelefteq R$ Ideal.

Beweis $\boxed{\text{ÜA}}$ $\square$

13. **Def** Sei R ein kommutativer Ring und $I \trianglelefteq R$ ein Ideal.

(a) I heißt <u>maximales Ideal</u>, wenn $I \neq R$ und wenn es kein Ideal $J \trianglelefteq R$ gibt mit $I \subsetneq J \subsetneq R$.

(b) I heißt <u>Primideal</u>, wenn gilt: $I \neq R$ und für $a, b \in R$ und $ab \in I$, so folgt $a \in I$ oder $b \in I$.

<u>Satz</u> Sei R ein kommutativer Ring, sei $I \trianglelefteq R$ Ideal.

(i) I ist Primideal genau dann, wenn $R/_I$ ein Integritätsbereich ist

(ii) I ist maximales Ideal genau dann, wenn $R/_I$ ein Körper ist.

Beweis (i) Ist I Primideal, so ist $I \neq R \Rightarrow R/_I \neq \{0\}$
Ist $x = r+I$, $y = s+I$ und $xy = I$, so folgt $rs \in I \Rightarrow r \in I$ oder $s \in I \Rightarrow x = I$ oder $y = I$
$\Rightarrow$ $R/_I$ Integritätsbereich.
Ist $R/_I$ Integritätsbereich, so ist $I \neq R$. Für $r, s \in R$ gilt $\pi_I(rs) = 0 + I \Leftrightarrow rs \in I \Leftrightarrow \pi_I(r) = r+I = I$ oder $\pi_I(s) = s+I = I \Leftrightarrow r \in I$ oder $s \in I$ $\square$

(ii) Sei $I \trianglelefteq R$ maximales Ideal, sei $a+I \in R/I$ mit $a \notin I$. Da $(a)+I = aR+I$ ein Ideal ist und $I \subsetneq (a)+I$ folgt $R = (a)+I$, d.h. es gibt $b \in R$ und $i \in I$ mit $ab+i=1$.
Es folgt $(a+I)(b+I) = ab+i+I = ab+I = 1+I$, also $a+I \in \left(R/I\right)^*$ Einheit $\Rightarrow R/I$ ist Körper.

Ist R/I Körper, so ist $I \neq R$. Angenommen, $J \trianglelefteq R$ ist Ideal mit $I \subsetneq J$. Es folgt aus § 3.12, dass $\pi_I(J) \subseteq R/I$ ein Ideal ist und $\pi_I(J) \neq \{0_{R/I}\}$. Da R/I ein Körper ist, folgt mit § 3.7 (a), dass $\pi_I(J) = R/I$. Wegen $I \subseteq J$ folgt $J = \pi_I^{-1}(\pi_I(J)) = R$ $\square$

<u>Korollar</u> Jedes maximale Ideal ist ein Primideal.

<u>Beweis</u> Jeder Körper ist ein Integritätsbereich $\square$

14. <u>Satz</u> Sei R ein kommutativer Ring, sei $R \neq I \trianglelefteq R$ ein Ideal. Dann existiert ein maximales Ideal $J \trianglelefteq R$ mit $I \subseteq J \subsetneq R$.

<u>Beweis</u> Sei $P = \{ J \trianglelefteq R \mid 1 \notin J \text{ und } I \subseteq J \}$

Dann ist P bezüglich $\subseteq$ partiell geordnet.

Wir kennen Zorns Lemma, vgl Lin. Algebra II §7.

Sei $G \subseteq P$ eine Kette (d.h. für alle $J, K \in G$ gilt $J \subseteq K$ oder $K \subseteq J$). Setze $J = \bigcup G$. Es folgt $1 \notin J$ (weil $1 \notin \bigcup P$)

<u>Beh</u>: J ist Ideal. Denn: $a, b \in J$, $r \in R$

$\Rightarrow$ es gibt $K, L \in G$ mit $\begin{matrix} a \in K \\ b \in L \end{matrix}$ OE $K \subseteq L$

$\Rightarrow a, b \in L \Rightarrow \begin{matrix} a \pm b \in L \\ a \cdot b \in L \end{matrix}$, $ra \in L$. Wegen $L \subseteq J$ folgt $a \cdot b, a \pm b, ra \in J$. Also $J \trianglelefteq R$. Wegen $1 \notin J$ ist $R \neq J$, also (wegen $I \subseteq J$) $J \in P$.

Nach Zorns Lemma gibt es maximale Elemente in P. Nach Konstruktion und §3.4 besteht P genau aus allen Idealen $J \trianglelefteq R$ mit

$$I \subseteq J \subsetneq R$$

$\square$

Korollar Ist R ein kommutativer Ring $R \neq \{0\}$, so existiert ein Körper K und ein surjektiver Ringhomomorphismus $R \xrightarrow{\varphi} K$. $\square$ #

15. **Beispiel** $R = \mathbb{Z}$ wir wissen bereits: alle Ideale sind von der Form $I = m\mathbb{Z}$, $m \in \mathbb{N}$.

- $I = \{0\} = 0\mathbb{Z}$ ist Primideal, denn $\mathbb{Z}/0 \cong \mathbb{Z}$ ist Integritätsbereich. Oder direkt: $a, b \in \mathbb{Z}$, $ab \in \{0\}$ $\Rightarrow a = 0$ oder $b = 0$.
- p Primzahl $\leadsto p\mathbb{Z}$ Primideal, denn: $a, b \in \mathbb{Z}$ $ab = k \cdot p \leadsto p$ teilt a oder p teilt b ✱ $\leadsto$ $a \in p\mathbb{Z}$ oder $b \in p\mathbb{Z}$. Da jeder endliche Integritätsbereich ein Körper ist, vgl. § 3.10, ist $p\mathbb{Z}$ auch ein maximales Ideal in $\mathbb{Z}$.
- $m = k \cdot l$ mit $k, l \geq 2$. Dann gilt $\bar{k} \cdot \bar{l} = \bar{m} = \bar{0}$, aber $\bar{k} \neq \bar{0} \neq \bar{l}$. Da $\mathbb{Z}/m$ kein Integritätsbereich ist, ist $m\mathbb{Z}$ kein Primideal.

Fazit: Die *Primideale* in $\mathbb{Z}$ sind die Ideale
$0\mathbb{Z}$, $p\mathbb{Z}$ p Primzahl
Die *maximalen Ideale* in $\mathbb{Z}$ sind die Ideal
$p\mathbb{Z}$ p Primzahl

✱ Das ist "Euklids Lemma" LA I §1.11

Wenn $m > 1$ und m keine Primzahl ist, dann ist $m\mathbb{Z}$ kein Primideal / maximales Ideal (und $1 \cdot \mathbb{Z} = \mathbb{Z}$ ist kein echtes Ideal!)

16. Erinnerung Zwei Zahlen $k, l \in \mathbb{Z}$ heißen **teilerfremd** oder **koprim**, wenn ± 1 die einzigen gemeinsamen Teiler von k und l sind.

Bsp
- $1, l$ sind für alle $l \in \mathbb{Z}$ koprim
- $10, 11$ sind koprim, $2, 6$ sind **nicht** koprim
- $0, l$ sind für $l \neq \pm 1$ koprim.

Lemma Sei $k, l \in \mathbb{Z}$. Dann sind äquivalent:

(i) k und l sind koprim

(ii) $1 \in k\mathbb{Z} + l\mathbb{Z}$ (äquivalent: $\mathbb{Z} = k\mathbb{Z} + l\mathbb{Z}$, vgl §3.4 und §3.6)

(iii) $\bar{k}$ ist Einheit in $\mathbb{Z}/l\mathbb{Z}$.

Beweis (iii) $\Rightarrow$ (ii) $\bar{k}$ Einheit $\leadsto$ $\bar{k}\,\bar{u} = \bar{1}$ für ein $u \in \mathbb{Z}$ $\leadsto$ $ku = 1 + lv$ für $u, v \in \mathbb{Z}$ $\Rightarrow$ $1 = ku - lv$.

(ii) $\Rightarrow$ (i) Ist t ein Teiler von k und l, so ist t auch Teiler von $ku + lv = 1$, fertig.

(i) $\Rightarrow$ (iii) Angenommen, $\bar{k}$ ist **keine** Einheit in $\mathbb{Z}/l\mathbb{Z}$.

1. Fall: $l = 0$ $\leadsto$ k keine Einheit in $\mathbb{Z}$ $\leadsto$ $k \neq \pm 1$ (denn $\mathbb{Z}^* = \{\pm 1\}$) $\leadsto$ k, l koprim (↯)

2. Fall: $l \neq 0$. Dann gibt es $w \in \mathbb{Z}$ mit $0 < w < |l|$ mit $\overline{kw} = \bar{0}$ ⊛ d.h.

⊛ ÜA 8.3

$o(\bar{k}) \leq w < |l| = \# \mathbb{Z}/l\mathbb{Z}$. Setze $u = o(\bar{k})$, dann gibt es $l' \neq \pm 1$ mit $l'u = l$

denn u teilt $|\ell|$ nach Lagrange.
Es folgt $u\bar{k} = \bar{0}$ $\Rightarrow$ $uk = v\ell = vu\ell'$ $\Rightarrow$ $k = v\ell'$
also ist $\ell' \neq \pm 1$ ein gemeinsamer Teiler von k und ℓ.

17. <u>Produkt von Ringen</u> Sei $(R_i)_{i\in I}$ eine (endliche oder unendliche) Familie von Ringen.
Dann ist auch

$$R = \prod_{i\in I} R_i \quad \text{ein Ring, mit}$$

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I}$$

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i \cdot y_i)_{i\in I}$$

Nullelement $(0_i)_{i\in I}$ Einselement $(1_i)_{i\in I}$.

Solche Produkte haben im allgemeinen viele Nullteiler,
$\mathbb{Z}\times\mathbb{Z}$ hat $(\ell, 0)$ sowie $(0, \ell)$ als Nullteiler.

<u>Koprime Ideale</u> Sei R ein kommutativer Ring. Zwei Ideale $I, J \trianglelefteq R$ heißen koprim, wenn gilt $R = I + J$

(äquivalent: $1 \in I + J$)

18. Der Chinesische Restsatz

Theorem (Chinesischer Restsatz, algebraische Version)
Sei R ein kommutativer Ring und seien $I_1, \dots, I_n \trianglelefteq R$ Ideale. Wenn für alle $1 \leq s < t \leq n$ gilt $R = I_s + I_t$ (d.h. wenn die Ideale $I_1, \dots, I_n$ paarweise koprim sind), dann ist der Ringhomomorphismus

$$R \xrightarrow{\pi} R/I_1 \times \dots \times R/I_n$$
$$r \longmapsto (r + I_1, \dots, r + I_n)$$

surjektiv. Der Kern von π ist $I_1 \cap I_2 \cap \dots \cap I_n$.

Beweis Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Wir nehmen jetzt an, die Aussage gilt für n paarweise koprime Ideale. Seien $I_1, \dots, I_{n+1} \trianglelefteq R$ paarweise koprim. Sei $(x_1, \dots, x_{n+1}) \in R^{n+1}$ gegeben. Wir suchen ein $x \in R$ mit $x + I_s = x_s + I_s$ für $s = 1, \dots, n+1$.

Wähle $y_s \in I_s$ und $z_s \in I_{n+1}$ für $s = 1, \dots, n$ mit $y_s + z_s = 1$ $(I_s + I_{n+1} = R)$. Es folgt

$$1 = (y_1 + z_1) \cdots (y_n + z_n) \in \underbrace{I_1 I_2 \cdots I_n}_{=K \subseteq I_1 \cap \dots \cap I_n} + I_{n+1}$$

also sind $K = I_1 I_2 \cdots I_n \subseteq I_1 \cap \dots \cap I_n$ und I_{n+1} koprim. Wähle $j \in I_{n+1}$ und $k \in K$ mit $j + k = 1$. Wähle jetzt $x' \in R^n$ so, dass gilt

$$x_s + I_s = x' + I_s \quad \text{für } s = 1, \dots, n \quad (\text{Ind. Annahme!})$$

$$1 + I_s = (j+k) + I_s \overset{\uparrow}{=} j + I_s \qquad \text{für } 1 \le s \le n$$

$k \in I_s \supseteq K$

$$1 + I_{n+1} = (j+k) + I_{n+1} = k + I_{n+1}$$

Setze $x = \underbrace{x' \cdot j}_{\in I_{n+1}} + \underbrace{x_{n+1} k}_{\in K}$, es folgt

$$x + I_s = x' \cdot j + I_s = x'(j+k) + I_s = x' + I_s \qquad 1 \le s \le n$$

$$x + I_{n+1} = x_{n+1} \cdot k + I_{n+1} = x_{n+1}(j+k) + I_{n+1} = x_{n+1} + I_{n+1} \qquad \square$$

<u>Korollar A</u> (Chinesischer Restsatz, Sun Zi ~ 5. Jhd?)

Seien $l_1, \dots, l_n$ n verschiedene paarweise koprime ganze Zahlen. Dann gibt es zu jedem n-Tupel

$$(x_1, \dots, x_n) \in \mathbb{Z}^n$$

eine ganze Zahl $y \in \mathbb{Z}$ mit

$$y + l_i \mathbb{Z} = x_i + l_i \mathbb{Z} \qquad i = 1, \dots, n \qquad \square$$

#

Der Kern von π ist $\{x \in R \mid x + I_1 = I_1, \dots, x + I_n = I_n\}$

$= \{x \in R \mid x \in I_1, \dots, x \in I_n\} = I_1 \cap \dots \cap I_n$

<u>Korollar B</u> Sei $l_1, \ldots, l_n$ n paarweise koprime ganze Zahlen. Dann existiert ein Ringisomorphismus

$$\mathbb{Z}/l_1 \cdots l_n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/l_1\mathbb{Z} \times \cdots \times \mathbb{Z}/l_n\mathbb{Z}$$

<u>Beweis</u> Betrachte $\pi : \mathbb{Z} \to \mathbb{Z}/l_1\mathbb{Z} \times \cdots \times \mathbb{Z}/l_n\mathbb{Z}$

Epimorphismus wie im Theorem. Es gilt

$\mathrm{Ker}(\pi) = l_1\mathbb{Z} \cap \cdots \cap l_n\mathbb{Z}$. Für $n=2$ erhalten wir

$l_1\mathbb{Z} \cap l_2\mathbb{Z} = l_1 l_2 \mathbb{Z}$ (denn⊛ $l_1 l_2$ ist das kleinste gemeinsame Vielfache von l_1, l_2) und damit sofort

$l_1\mathbb{Z} \cap \cdots \cap l_n\mathbb{Z} = l_1 \cdots l_n \mathbb{Z}$ per Induktion □

Jetzt Homomorphiesatz §3.5

⊛ vgl. ÜA 8.2

19. <u>Polynomringe</u> Sei R ein kommutativer Ring. Sei

$R^{(\mathbb{N})} = \{(r_i)_{i\in\mathbb{N}} \mid r_i = 0$ für fast alle $i \in \mathbb{N}\}$

("für fast alle" heißt: nur endlich viele Ausnahmen).

Dann ist $R^{(\mathbb{N})}$ eine abelsche Gruppe bzgl komponentenweiser Addition, $(r_i)_{i\in\mathbb{N}} + (s_i)_{i\in\mathbb{N}} := (r_i+s_i)_{i\in\mathbb{N}}$.

Wir definieren eine Multiplikation auf $\mathbb{R}^{(\mathbb{N})}$ wie folgt:

$$(r_i)_{i\in\mathbb{N}} \cdot (s_i)_{i\in\mathbb{N}} = (t_i)_{i\in\mathbb{N}} \qquad t_j = \sum_{i=0}^{j} r_i s_{j-i}$$

Eine einfache Rechnung zeigt: $\mathbb{R}^{(\mathbb{N})}$ wird mit diesen beiden Verknüpfungen ein kommutativer Ring.

Sei T ein nicht in R enthaltenes Element. Ist $(r_i)_{i\in\mathbb{N}} \in R^{(\mathbb{N})}$, so gibt es ein $n \in \mathbb{N}$ mit $r_i = 0$ für alle $i > n$ (weil nur endlich viele $r_i \neq 0$).

Schreibe formal

$$(r_i)_{i\in\mathbb{N}} = r_0 + r_1T + r_2T^2 + \dots + r_nT^n$$

Die Terme r_iT mit $r_i = 0$ läßt man auch weg.

Die beiden Verknüpfungen $+$ und $\cdot$ schreiben sich dann viel intuitiver als

$$(r_0 + r_1T + \dots + r_nT^n) + (s_0 + s_1T + \dots + s_nT^n) =$$

$$(r_0+s_0) + (r_1+s_1)T + (r_2+s_2)T^2 + \dots + (r_n+s_n)T^n$$

wobei $n \gg 1$ so gewählt wird, dass $r_i = 0 = s_i$ für alle $i > n$.

$$(r_0 + \dots + r_n T^n) \cdot (s_0 + s_1 T + \dots + s_n T^n) = \sum_{j=0}^{n} \sum_{i=0}^{j} r_i s_{j-i} T^j$$

Man nennt $R[T] = R^{(\mathbb{N})}$ den Polynomring über R (in der Unbekannten T). Die Elemente von $R[T]$ heißen Polynome in R (in der Unbekannten T).

Bemerkungen
- $T, T^2, \dots T^n$ sind Terme, die man symbolisch hinschreibt. Statt T nennt man die Unbekannte oft auch X und schreibt $R[X]$ usw.
- Der Polynomring $R[T]$ enthält R als Teilring via $R \to R[T]$, $r \mapsto r = r + 0T$. Das Nullelement in $R[T]$ ist 0 (das Nullpolynom), das Einselement ist $1 = 1 + 0T$. Die Polynome der Form r, $r \in R$ nennt man auch konstant oder Skalare.
- Warum haben wir $R[T]$ nicht definiert als Menge der Abbildungen der Form $f(x) = r_0 + x r_1 + x^2 r_2 + \dots + x^n r_n$?

Bsp $R = \mathbb{F}_2 = \{0, 1\}$. Die beiden Abbildungen

$$f(x) = 0$$
$$g(x) = x + x^2$$

stimmen überein. Dagegen sind die Polynome

0 und $T+T^2 \in \mathbb{F}_2[T]$ so wie wir das definiert haben, voneinander verschieden. In der Algebra ist dieser Unterschied wichtig!

Der Grad eines Polynoms $f = r_0 + r_1 T + \dots + r_n T^n \neq 0$ ist $\deg(f) = \max\{k \geq 0 \mid r_k \neq 0\}$. Für das Nullpolynom setzt man $\deg(0) = -\infty$.
Ist $f = r_0 + r_1 T + \dots + r_n T^n$ mit Grad $\deg(f) = n$, so heißt r_n der Leitkoeffizient von f und r_0 heißt der Konstante Term von f.

20. Lemma Seien $f = r_0 + \dots + r_n T^n$, $g = s_0 + \dots + s_m T^m$ Polynome in $R[T]$, R ein kommutativer Ring, mit $\deg(f) = n$ und $\deg(g) = m$, $n, m \geq 0$.
Dann gilt

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$
$$\deg(f \cdot g) \leq \deg(f) + \deg(g)$$

Wenn die Leitkoeffizienten r_n und s_m keine Nullteiler sind, gilt $\deg(fg) = \deg(f) + \deg(g)$.

Beweis Die beiden Formeln folgen direkt aus den Additions- und Multiplikationsregeln für Polynome.
Es gilt $f \cdot g = r_0 s_0 + \dots + r_n s_m T^{n+m}$

Wenn also r_n, s_m keine Nullteiler sind, so folgt, dass $r_n s_m$ der Leitkoeffizient von $f \cdot g$ ist.

<u>Korollar</u> Sei R ein kommutativer Ring. Dann sind äquivalent: (i) R ist Integritätsbereich
(ii) $R[T]$ ist Integritätsbereich.

<u>Beweis</u> (i) $\Rightarrow$ (ii): Ist $f, g \neq 0$, so ist $\deg(f \cdot g) \neq -\infty$ also $f \cdot g \neq 0$.
(ii) $\Rightarrow$ (i): R ist ein Teilring von $R[T]$ $\square$