§ 11 Ring der ganzen Zahlen $\mathbb{Z}$ und Restklassenringe $\mathbb{Z}/m\mathbb{Z}$

(11.1) **Def** (Ring)

Ein **Ring** $R = (R, +, \cdot)$ ist eine Menge R, für welche $+ : R \times R \to R$, $(a,b) \mapsto a+b$ und $\cdot : R \times R \to R$, $(a,b) \mapsto ab$ gegeben sind, so daß die folgenden 'Rechenregeln' erfüllt sind:

(A1)	$+$ assoziativ	vgl (4.1) Def eines Körpers; im Gegensatz zu (4.1) verlangen wir **nicht** (M2), (M3), (M4)
(A2)	$+$ kommutativ	
(A3)	ex Null 0 bzgl $+$	
(A4)	ex Inverses bzgl $+$	
(M1)	$\cdot$ assoziativ	
(D)	Distributivgesetze	

- Gilt zusätzlich (M2) $\cdot$ kommutativ, so heißt R ein **kommutativer Ring**.
- Gilt (M3) ex Einselmt $1 \neq 0$ bzgl $\cdot$, so heißt R ein **Ring mit 1** $(\neq 0)$. Wahlweise läßt man auch Nullringe $R = \{0\}$ mit $1 = 0$ als „Ringe mit 1" zu.
- Erfüllt R (M3) und (M4) ex Inversen bzgl $\cdot$, so heißt R ein **Divisionsring** (oder **Schiefkörper**).

- Gilt in R die Regel

$$\forall a, b \in R: \; ab = 0 \rightarrow (a = 0 \text{ oder } b = 0),$$

so heißt R nullteilerfrei.

- Ein Integritätsbereich ist ein nullteilerfreier kommutativer Ring mit $1 \neq 0$.

Beispiele:

⊛ a) $\mathbb{Z}$ ist ein Integritätsbereich.

b) $\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$

Hamiltonsche Quaternionen:

4-dimensionaler $\mathbb{R}$-VR mit Basis $1, i, j, k$

$+$: VR-Addition

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k)$$
$$= (a+a') + (b+b')i + (c+c')j + (d+d')k$$

$\cdot$:
$$(a+bi+cj+dk)(a'+b'i+c'j+d'k)$$
$$= (aa' - bb' - cc' - dd')$$
$$+ (ab' + ba' + cd' - dc')i$$
$$+ (ac' - bd' + ca' + db')j$$
$$+ (ad' + bc' - cb' + da')k$$

Merkregeln:
$i^2 = j^2 = -1$
$ij = k = -ji$

$\rightsquigarrow \mathbb{H}$ ist ein nicht-kommutativer Divisionsring 15 16

c) $\mathbb{R} \times \mathbb{R}$ mit $+, \cdot$ koordinatenweise definiert ist ein kommutativer Ring mit 1, aber nicht nullteilerfrei.

(11.2) Prinzip der vollständigen Induktion

Wir haben bereits öfter davon Gebrauch gemacht, daß jede nicht-leere Teilmenge $T \subseteq \mathbb{N}$ ein (eindeutiges) kleinstes Element $\min T$ besitzt, und diese Eigenschaft von der geordneten Menge $(\mathbb{N}, \leq)$ zu dem Begriff einer Wohlordnung verallgemeinert; siehe (8.4).

Man leitet daraus die folgende, wichtige Beweismethode ab:

Sei $n_0 \in \mathbb{Z}$, und für $n \in \mathbb{Z}$ mit $n \geq n_0$ seien A_n mathematische Aussagen. Ferner gelte: 1) Die Aussage A_{n_0} ist wahr.

(Induktionsanfang)

2) Für jedes $n \in \mathbb{Z}$ mit $n > n_0$ gilt: Sind $A_{n_0}, A_{n_0+1}, \ldots, A_{n-1}$ allesamt wahr (Induktionsvoraussetzung), so ist auch A_n wahr (Induktionsschluß)

} Induktionsschritt

Dann ist A_n für jedes $n \in \mathbb{Z}$ mit $n \geq n_0$ wahr.

[Übung: Formuliere diese Beweismethode allgemeiner für eine beliebige wohlgeordnete Menge $(N, \leq)$]

(11.3) Def (elementare Teilbarkeitsbegriffe)

Sei R ein kommutativer Ring mit 1.

a) Seien $a, b \in R$. Dann heißt a ein Teiler von b (in R), $a \mid_R b$ „a teilt b in R“, falls es ein $c \in R$ mit $ac = b$ gibt.

Wir sagen, a und b sind (in R) assoziiert, $a \sim_R b$, falls $a \mid_R b$ und $b \mid_R a$.

Gilt $a \mid_R 1$, so nennen wir a eine Einheit (oder invertierbar) in R.

Gibt es ein $c \in R \setminus \{0\}$ mit $ac = 0$, so heißt a ein Nullteiler in R.

[In der Regel schreibt man $\mid$ statt $\mid_R$ etc.]

b) Die Menge aller Einheiten in R wird mit R^* bezeichnet und heißt Einheitengruppe.

[Der Begriff „Gruppe“ wird später genauer behandelt.]

c) Seien $a, b \in R$. Ein Element $d \in R$ heißt ein größter gemeinsamer Teiler von a, b, falls gelten:

(GGT 1) $d \mid a$ und $d \mid b$

(GGT 2) $\forall t \in R: (t \mid a \text{ und } t \mid b) \to t \mid d$

d) Sei R zusätzlich nullteilerfrei und $1 \neq 0$, also R ein Integritätsbereich, und sei $a \in R$.

Dann heißt a unzerlegbar (irreduzibel) in R, falls: $a \notin \{0\} \cup R^*$ und

$\forall b, c \in R: a = bc \to (b \in R^* \text{ oder } c \in R^*)$.

Desweiteren heißt a prim in R, Klopsch

falls: $a \notin \{0\} \cup R^*$ und

$$\forall b,c \in R: a \mid bc \to (a \mid b \text{ oder } a \mid c).$$

Bspl Gegenwärtig ist unser Hauptbeispiel der Ring $\mathbb{Z}$ der ganzen Zahlen. Später lassen sich die Begriffe gewinnbringend auch auf Polynomringe anwenden.

a) Der Teilbarkeitsbegriff auf $\mathbb{N}$ ist uns wohlvertraut und verallgemeinert sich wie definiert auf $\mathbb{Z}$.
Gilt $a \mid b$ in $\mathbb{Z}$, so ist offenbar $|a| \leq |b|$.
Insbesondere folgt aus $a \sim b$ in $\mathbb{Z}$ schon $b = a$ oder $b = -a$. Umgekehrt gilt stets $a \sim a$ und $a \sim -a$.
Die Einheiten in $\mathbb{Z}$ sind also $1, -1$, und es gibt neben 0 keine „echten" Nullteiler.

b) $\mathbb{Z}^* = \{1, -1\}$.

c) Je zwei Elemente $a, b \in \mathbb{Z}$ haben einen größten gem Teiler, der sich z B über den euklidischen Algorithmus berechnen läßt (mehr darum später).
Merke: $\forall t \in \mathbb{Z}: t \mid 0$, insbesondre ist also 0 der eindeutig bestimmte ggT von 0 und 0.

d) Jede Primzahl $p \in \mathbb{P}$ sowie ihr Negatives $-p$ sind unzerlegbar in $\mathbb{Z}$.

Daß p (und $-p$) auch prim ist, überlegen wir uns und führt wesentlich zur eindeutigen Primfaktorzerlegung in $\mathbb{Z}$.

(11.4) Def (Äquivalenzrelation)

Sei $\rho \subseteq A \times A$ eine Relation auf einer Menge A. Dann heißt ρ eine Äquivalenzrelation auf A, falls folgende Bedingungen erfüllt sind

(Ä1) $\forall a \in A: a \rho a$ (ρ reflexiv auf A)

(Ä2) $\forall a, b \in A: a \rho b \leftrightarrow b \rho a$ (ρ symmetrisch)

(Ä3) $\forall a, b, c \in A: (a \rho b \text{ und } b \rho c) \rightarrow a \rho c$ (ρ transitiv)

Ist ρ eine Äquivalenzrelation auf A, so heißt $\{b \in A \mid a \rho b\}$ die zu $a \in A$ gehörige Äquivalenzklasse bzgl ρ. Weiterhin bezeichnet A/ρ die Menge aller Äquivalenzklassen bzgl ρ:

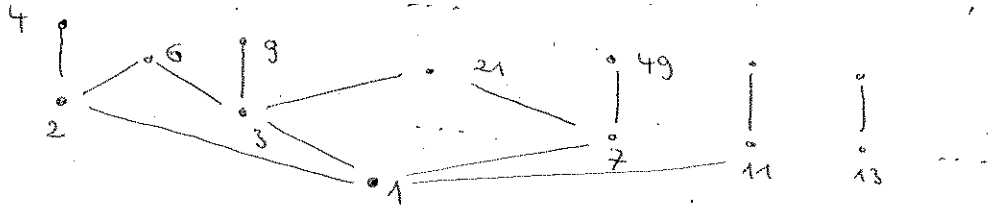
$$A/\rho = \{ \{b \in A \mid a \rho b\} \mid a \in A \}.$$

(11.5) Beispiele und Nicht-Beispiele (Restklassenringe)

a) Die Teilbarkeitsrelation $|$ auf $\mathbb{Z}$ ist reflexiv und transitiv, aber nicht symmetrisch.

Sie ist auch nicht antisymmetrisch (vgl (8.4)). Klassisch

Aber die Einschränkung von | auf $\mathbb{N}$ ist antisymmetrisch und liefert eine interessante Halbordnung (vgl (8.4)):



b) Sei R ein kommutativer Ring mit 1.

Dann ist Assoziiert-sein eine Äquivalenzrelation auf R. Für $R=\mathbb{Z}$ sind die wegen Äquivalenzklassen gerade

$$\{0\}, \{1,-1\}, \{2,-2\}, \ldots$$

und stehen somit in natürlicher Weise in Bijektion zu $\mathbb{N}_0$.

16

c) Sei $m \in \mathbb{N}$. [besonders anhaulich ist der Spezialfall $m=2$!.] 17

Dann ist die wie folgt definierte Relation $\equiv_m$ („kongruent modulo m") eine Äquivalenz auf $\mathbb{Z}$:

$a \equiv_m b$ gdw $m \mid (a-b)$, dh $a-b \in$

$$m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}.$$

Es gibt genau m Äquivalenzklassen bzgl $\equiv_m$, nämlich

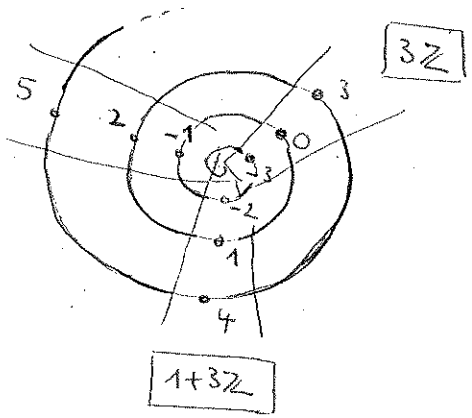
$$(0+)\, m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$$

$$1 + m\mathbb{Z} = \{\ldots, 1-2m, 1-m, 1, 1+m, 1+2m, \ldots\}$$

$$\ldots$$

$$(m-1) + m\mathbb{Z} = \{\ldots (m-1)-2m, (m-1)-m, m-1, \ldots\}$$

Statt $\mathbb{Z}/\equiv_m$ schreibt man gewöhnlich $\mathbb{Z}/m\mathbb{Z}$.



Wir erhalten ein kanonisches Modell für die in (4.5) beschriebenen endlichen Zahlbereiche $R_m(\mathbb{Z})$: Bezeichnet $r_m(a)$ wie in (4.5) den ganzzahligen Rest in $\{0,1,\ldots,m-1\}$ von a bei Division durch m, so gilt nämlich für $r \in \{0,1,\ldots,m-1\}$:

$$a \equiv_m r \iff r_m(a) = r \iff a + m\mathbb{Z} = r + m\mathbb{Z}.$$

Die Operationen $+_m$ und $\cdot_m$ auf $R_m(\mathbb{Z})$ entsprechen der Addition und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$, die mit Hilfe beliebiger Vertreter der Äquivalenzklassen ausgeführt wird:

$$(a+m\mathbb{Z}) + (b+m\mathbb{Z}) = (a+b) + m\mathbb{Z}$$
$$(a+m\mathbb{Z}) \cdot (b+m\mathbb{Z}) = (a\cdot b) + m\mathbb{Z}$$

Man überprüfe dann:

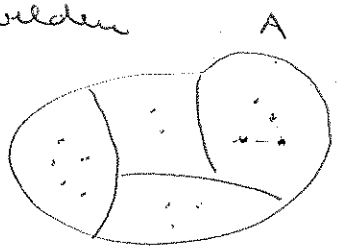
$$a \equiv_m \tilde{a} \text{ und } b \equiv_m \tilde{b} \Rightarrow \begin{cases} a+b \equiv_m \tilde{a}+\tilde{b} \\ a\cdot b \equiv_m \tilde{a}\,\tilde{b} \end{cases} !$$

Die Äquivalenzklassen $a+m\mathbb{Z}$ heißen Restklassen modulo m, der Ring $\mathbb{Z}/m\mathbb{Z}$ heißt Restklassenring modulo m.

(11.6) Hilfssatz

Sei A eine Menge und $\sim$ eine Äquivalenzrel auf A. Dann gilt: Je zwei Äquivklassen bzgl $\sim$ sind entweder gleich oder disjunkt (d.h. haben keine gemeinsamen Elemente).
Folglich ist A die disjunkte Vereinigung aller Äquivklassen bzgl $\sim$.

Bem Man sagt: Die Äquivklassen bilden eine Partition von A.



Bew: Seien $a, b \in A$. Aufgrund der Transitivität von $\sim$ sind die Äquivklassen von a und b gleich gdw $a \sim b$ gilt.
Angenommen, die Äquivklassen von a und b sind nicht disjunkt. Dann ex $c \in A$ mit $a \sim c$ und $b \sim c$. Daraus folgt $a \sim b$, also sind die zwei Äquivalenzklassen gleich.
Da jedes Elmt aus A in wenigstens einer Äquivklasse liegt (nämlich seiner eigenen), ist A die disjunkte Vereinigung aller Äquivklassen. //

(11.7) Lem Sei R ein Integritätsbereich. Dann gilt:

(1) $\forall\, a \in R\setminus\{0\}\ \forall\, b, c \in R: \quad ab = ac \longrightarrow b = c$

(2) Ist $p \in R$ prim, so ist p unzerlegbar (in R).

Bew (1) Seien $a, b, c \in R$ mit $a \neq 0$ und $ab = ac$. Dann folgt $a(b-c) = ab - ac = 0$, wegen R nullteilerfrei also $b - c = 0$, dh $b = c$.

(2) Sei $p \in R$ prim und $p = ab$. Zz: $a \in R^*$ oder $b \in R^*$.

Wegen $p \mid ab$ gilt etwa $p \mid a$, dh $a = pc$ für ein geeignetes $c \in R$. Damit ist $p = ab = pbc$, nach (1) also $1 = bc$ und $b \in R^*$. //

(11.8) Lem (Division mit Rest)

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann ex eind bestimmte $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$.

Bew [vgl Aufg 4.3]: Wir zeigen zunächst die Eindeutigkeit. Gilt $qb + r = q'b + r'$ für $q, r, q', r' \in \mathbb{Z}$ mit $0 \leq r \leq r' < |b|$, so folgt aus $r' - r = qb - q'b \underset{|b|}{\equiv} 0$ und $0 \leq r' - r < |b|$ schon $r' - r = 0$, also $r' = r$, folglich auch $qb = q'b$, also $q' = q$.

Die Existenz beweisen wir per Induktion nach $|a| \in \mathbb{N}_0$. Offenbar dürfen wir dabei $b > 0$ voraussetzen.

IA: $|a| < b$. Setze

$$q = \begin{cases} 0 & a \geq 0 \\ -1 & a < 0 \end{cases} \quad \text{und} \quad r = \begin{cases} a & a \geq 0 \\ b + a & a < 0 \end{cases}.$$

IS: $|a| \geq b$. Setze

$$a' = \begin{cases} a - b & a \geq b \\ a + b & a \leq -b \end{cases}.$$

Es gilt $|a'| < |a|$. Nach IV ist dann

$a' = q'b + r$ für $q', r \in \mathbb{Z}$ mit $0 \leq r < b$.

Also gilt

$$a = \begin{cases} a' + b = (q'+1)b + r \\ a' - b = (q'-1)b + r \end{cases}. \quad //$$

(11.9) Satz und Def (ggT für $\mathbb{Z}$)

Je zwei Elemente in $\mathbb{Z}$ haben einen größten gemeinsamen Teiler, und dieser ist bis auf das Vorzeichen eindeutig. Es gibt daher genau eine Abb $ggT : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}_0$, so daß $ggT(a,b)$ für alle $a, b \in \mathbb{Z}$ ein gr gem Teiler von a, b ist.

[$ggT(a,b)$ heißt dann „der" ggT von a, b]

Bew Seien $a, b \in \mathbb{Z}$. Sind d, d' gr gem Teiler von a, b so gilt $d \mid d'$ und $d' \mid d$, also $d \sim d'$, also $d' \in \{d, -d\}$. Damit ist die Eindeutigkeit bis auf das Vorzeichen gezeigt.

Wir beweisen die Existenz per Induktion nach $\min\{|a|, |b|\}$. Offenbar dürfen wir o.E

voraussetzen, daß $0 \leq b \leq a$ gilt.

IA: $b = \min\{a, b\} + 0$. Offenbar ist dann a ein gr gem Teiler von a, b.

IS: $b = \min\{a, b\} \geq 1$. Division mit Rest liefert

$a = qb + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$.

Merke:

$\forall t \in \mathbb{Z}: (t \mid a \text{ und } t \mid b) \leftrightarrow (t \mid (\underbrace{a - qb}_{=r}) \text{ und } t \mid b)$ ⊛

Wegen $\min\{\underbrace{a - qb}_{=r}, b\} = r < b$ liefert die IV einen gr gem Teiler von $a - qb, b$. Dieser ist aber wegen ⊛ auch ein gr gem Teiler von a, b. // 17

18

(11.10) Bem (euklidischer Algorithmus)

Der vorstehende Beweis liefert ein praktisches Verfahren zur Bestimmung des ggTs.

Bspl: $a = -10725$, $b = 7650$

$$\begin{aligned} ggT(a, b) &= ggT(10725, 7650) \\ &= ggT(3075, 7650) \\ &= ggT(3075, 1500) \\ &= ggT(75, 1500) \\ &= ggT(75, 0) = 75 \end{aligned}$$

(11.11) Hilfssatz (Bézout-Koeffizienten)

Seien $a, b \in \mathbb{Z}$ und $d = ggT(a,b)$.

Dann ex $s, t \in \mathbb{Z}$ mit $sa + tb = d$.

Bew: Für $a = b = 0$ ist $d = 0$, und die Aussage ist offenbar richtig. Sei nun $a \neq 0$ oder $b \neq 0$, und somit $d \neq 0$. Dann ist $\{sa + tb \mid s, t \in \mathbb{Z}\} \cap \mathbb{N} \neq \emptyset$, besitzt also ein Minimum $d' = s_0 a + t_0 b$.

Wir behaupten $d = d'$. Offenbar gilt $d \mid d'$, und es genügt, zz: $d' \mid d$. Wegen $d = ggT(a,b)$ genügt dafür: $d' \mid a$ und $d' \mid b$. Division mit Rest liefert $a = q d' + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < d'$.

Das ergibt $r = a - q d' = (1 - q s_0) a + (-q t_0) b$.

Wegen $r < d'$ ergibt das $r = 0$ und $d' \mid a$.

Ebenso zeigt man $d' \mid b$. //

(11.12) Bem (euklidischer Algorithmus zur Bestimmung von Bézout-Koeffizienten)

Indem man die Rechnungen im euklidischen Algorithmus zurückverfolgt, erhält man ein praktikables Verfahren, Bézout-Koeffizienten zu bestimmen.

Bspl: $a = -10725$, $b = 7650$

$ggT(a,b) = 75$ nach (11.10):

$$10725 = 7650 + 3075$$
$$7650 = 2 \cdot 3075 + 1500$$
$$3075 = 2 \cdot 1500 + 75$$
$$(1500 = 20 \cdot 75 + 0)$$

liefert: $75 = 3075 - 2 \cdot 1500$

$= 3075 - 2(7650 - 2 \cdot 3075)$

$= (-2) \cdot 7650 + 5 \cdot 3075$

$= (-2) \cdot 7650 + 5(10725 - 7650)$

$= (-5)(-10725) + (-7) \cdot 7650 = (-5)a + (-7)b$

(11.13) Lemma von Euklid

Sei $p \in \mathbb{Z}$ unzerlegbar. Dann ist p prim.

Bem: Mit (11.7) folgt also:

$\mathbb{P} \cup -\mathbb{P} = \{a \in \mathbb{Z} \mid a \text{ unzerlegbar}\}$

$= \{a \in \mathbb{Z} \mid a \text{ prim}\}$

Beweis: Seien $a, b \in \mathbb{Z}$ mit $p \mid ab$. ZZ: $p \mid a$ oder $p \mid b$.

Angenommen, $p \nmid a$. Da p unzerlegbar ist, sind die einzigen positiven Teiler von p die trivialen Teiler 1 und $|p|$. Wegen $p \nmid a$ gilt daher $ggT(p, a) = 1$. Nach (11.11) gibt es $s, t \in \mathbb{Z}$ mit $sp + ta = 1$. Also gilt

$b = b \cdot 1 = b(sp + ta) = (bs)p + t(ab)$.

Wegen $p \mid (bs)p$ und $p \mid ab \mid t(ab)$ ergibt das $p \mid b$. //

(11.14) Lemma Sei $n \in \mathbb{N}$. Dann ex endl viele Primzahlen $p_1, \dots, p_r$ mit $n = p_1 \cdots p_r$.

Bew (per Induktion nach n):

IA: $n=1$. Per Konvention ist 1 das leere Produkt ($r=0$).

IS: $n>1$. Ist n unzerlegbar, so ist $n=p_1$ selbst eine Primzahl. Ist n nicht unzerlegbar, so gilt $n=ab$ mit $a,b \notin \mathbb{Z}^* = \{1,-1\}$, o.E. also $1<a,b<n$. Nach IV gilt $a=p_1 \cdots p_s$ und $b=p_{s+1} \cdots p_r$ für $0 \leq s \leq r$ und Primzahlen $p_1, \ldots, p_r$. Das ergibt $n=ab=p_1 \cdots p_r$. //

(11.15) Lem Sei $n \in \mathbb{N}$, und seien $n=p_1 p_2 \cdots p_r$ und $n=q_1 q_2 \cdots q_s$ zwei Primfaktorzerlegungen von n, wobei $r,s \geq 0$, $0<p_1 \leq p_2 \leq \ldots \leq p_r$ und $0<q_1 \leq q_2 \leq \ldots \leq q_s$ sind. Dann gilt $r=s$ und $p_i=q_i$ für $i \in \{1,\ldots,r\}$.

Bew (per Induktion nach n):

IA: $n=1$. Offenbar gibt es nur eine Darstellung ($r=s=0$).

IS: $n>1$. Es gilt $r,s \geq 1$. Nach (11.13) ist p_r prim und $p_r \mid n = q_1 \cdots q_s$. Daher gilt $p_r \mid q_j$ für ein geeignetes $j \in \{1,\ldots,s\}$. Insbesondere gilt $p_r \leq q_j \leq q_s$. Ähnlich folgt $q_s \leq p_r$. Das ergibt $p_r = q_s$. Die IV, angewandt

auf $m = \frac{n}{p_r} = p_1 \cdots p_{r-1}$ und Kürzen

$$m = \frac{n}{q_s} = q_1 \cdots q_{s-1},$$

liefert $r-1 = s-1$ und $p_i = q_i$ für $i \in \{1, \ldots, r-1\}$. //

(11.16) Fundamentalsatz der Arithmetik

Sei $a \in \mathbb{Z} \setminus \{0\}$. Dann besitzt a eine Faktorisierung

$$a = u \cdot p_1 \cdots p_r,$$

wobei $u \in \{1, -1\}$, $r \in \mathbb{N}_0$ und $p_1, \ldots, p_r \in \mathbb{P}$.
Diese Zerlegung ist – bis auf die Reihenfolge der Primfaktoren – eindeutig.

Bew: folgt unmittelbar aus (11.14) und (11.15). //

(11.17) Hilfssatz

Sei $n \in \mathbb{N}_{\geq 2}$ und $a \in \mathbb{Z}$. Dann gelten

(1) $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$, d.h. a ist invertierbar modulo n, d.h. $ggT(a, n) = 1$

(2) $a + n\mathbb{Z}$ ist ein Nullteiler in $\mathbb{Z}/n\mathbb{Z}$ d.h. $ggT(a,n) \neq 1$.

Bem Also gilt $(\mathbb{Z}/n\mathbb{Z})^* = \{ b + n\mathbb{Z} \mid b \in \mathbb{Z} \text{ mit } ggT(b,n) = 1 \}$.

Zu $ggT(b,n) = 1$ sagt man auch „b und n sind teilerfremd".

Ist R ein beliebiger kommutativer Ring mit $1 \neq 0$, so sind R^* und $\{ x \in R \mid x \text{ Nullteiler in } R \}$ disjunkt;

Gilt $xy = 1$ und $xz = 0$, so

folgt stets $z = 1 \cdot z = xyz = (xz)y = 0 \cdot y = 0$.

Bew: Setze $d = ggT(a,m)$. Aufgrund der Vorbemerkung genügt es jeweils „$\Leftarrow$" zu zeigen.

Sei zunächst $d = 1$. Nach (11.11) ex $b, n \in \mathbb{Z}$ mit $ab + mn = 1$. Also gilt $ab \equiv_m 1$, d.h. $(a+m\mathbb{Z})(b+m\mathbb{Z}) = ab + m\mathbb{Z} = 1 + m\mathbb{Z}$, und $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*$.

Sei nun $d \neq 1$, also $d > 1$. Schreibe $a = d\tilde{a}$ und $m = d\tilde{m}$ mit $\tilde{a}, \tilde{m} \in \mathbb{Z}$ und $0 < \tilde{m} < m$. Offenbar gilt dann

$$a\tilde{m} = d\tilde{a}\tilde{m} = \tilde{a}d\tilde{m} = \tilde{a}m \equiv_m 0,$$

also

$$(a+m\mathbb{Z})(\underbrace{\tilde{m} + m\mathbb{Z}}_{\neq 0+m\mathbb{Z}}) = 0 + m\mathbb{Z}.$$

(11.18) Satz Sei $m \in \mathbb{N}$. Dann ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper gdw $m \in \mathbb{P}$. [vgl (4.6)]

Bew $\mathbb{Z}/m\mathbb{Z}$ ist für $m \geq 2$ ein kommutativer Ring mit 1. Nach (11.17) ist jedes Element von $\mathbb{Z}/m\mathbb{Z} \setminus \{0+m\mathbb{Z}\}$ invertierbar gdw m keine echten Teiler besitzt, also $m \in \mathbb{P}$ ist. //