Wie schön (und auch überraschend) die Verhältnisse in einem Hauptidealring sind, zeigt die folgende Feststellung F1. Natürlich wäre alles auf Sand gebaut, wenn wir nicht belegen könnten, daß es interessante Beispiele von Hauptidealringen wirklich gibt. Wir werden aber bald zeigen können, daß z.B. der Ring $\mathbb{Z}$ ein Hauptidealring ist.

F1: Sei R ein Hauptidealring. Dann gilt: Zu jedem System $a_1, \ldots, a_n$ von Elementen aus R existiert ein ggT d von $a_1, \ldots, a_n$ und (jedes solche) d besitzt eine Darstellung der Gestalt

(A) $$d = x_1 a_1 + \ldots + x_n a_n \qquad \text{mit } x_i \in R$$

(Wir sagen, in R gelte der Satz vom größten gemeinsamen Teiler.)

Bew. $J := Ra_1 + \ldots + Ra_n = \{x_1 a_1 + \ldots + x_n a_n \mid x_i \in R\}$ ist ein Ideal in R, also ex. nach Voraussetzung (R ist Hauptidealring) ein $d \in R$ mit

$$J = (d)$$

Nach (7) ist d ein ggT von $a_1, \ldots, a_n$. Wegen $d \in J$ gilt (A). Ist d' ein weiterer ggT von $a_1, \ldots, a_n$, so gilt $d' \triangleq d$, d.h. $(d') = (d) = J$, also hat auch d' eine Darstellung der Art (A). – Mit dem obigen Bew'is gilt übrigens

$$(a_1, \ldots, a_n) = (d)$$

Bem. Sei R ein bel. Integritätsring. Ist d ein gemeinsamer Teiler von $a_1, \ldots, a_n$ aus R und gibt es eine Darstellung der Form (A), so ist d ein ggT von $a_1, \ldots, a_n$.

Bew. $t \mid a_i$ für $1 \le i \le n \xRightarrow{(A)} t \mid d$.

Satz 1: $\mathbb{Z}$ ist ein Hauptidealring.

Zur Vorbereitung des Beweises zunächst Wiederholung einer Grundtatsache aus der Anfängervorlesung:

Def. ('Gaußklammer'): Für $x \in \mathbb{R}$ setze

$$[x] = \operatorname{Max}\{ g \in \mathbb{Z} \mid g \le x \} \overset{!}{\in} \mathbb{Z}$$

(existiert nach Archimedischem Axiom für $\mathbb{R}$)

$[x]$ ist charakterisiert durch folgende zwei Eigenschaften:

① $[x] \in \mathbb{Z}$ ② $[x] \le x < [x]+1$

Die Gaußklammer $x \mapsto [x]$ ist eine subtile Funktion (und grundlagentheoretisch nicht ganz unproblematisch); sie ist ausdrucksstark und "weiß sozusagen alles".

F2 (Division mit Rest in $\mathbb{Z}$): Gegeben $a \neq 0$ und b aus $\mathbb{Z}$. Dann gibt es Darstellung

(D) $\qquad b = qa + r$ mit $0 \le r < |a|$ und $q, r \in \mathbb{Z}$

Bew. o.E. $a > 0$, d.h. $a \in \mathbb{N}$. $\frac{b}{a} \in \mathbb{Q}$.

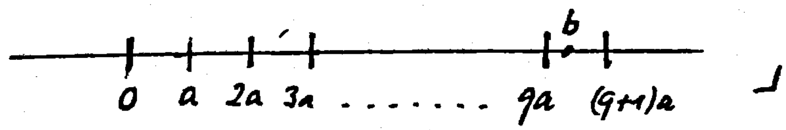
Setze nun

$q := [\frac{b}{a}]$. Dann $q \in \mathbb{Z}$ und $q \le \frac{b}{a} < q+1$, $\overset{a>0}{\Longrightarrow}$

$qa \le b < qa + a$, $\Longrightarrow$

$0 \le \underbrace{b-qa}_{=:r} < a$, $\Longrightarrow$ Beh.

⌜Bild (für $b>0$):



⌟

<u>Bem.:</u> 1) Die Darstellung (D) ist <u>eindeutig</u>.

2) Es gibt Darstellung

(D') $\qquad b = qa + r$ mit $|r| < |a| \quad (q, r \in \mathbb{Z})$,

doch diese nicht mehr eindeutig, z.B. $27 = 4 \cdot 6 + 3 = 5 \cdot 6 - 3$.

3) Es gibt Darstellung

$$b = qa + r \quad \text{mit} \quad -\frac{|a|}{2} < r \le \frac{|a|}{2} \qquad (q, r \in \mathbb{Z}),$$

und diese ist eindeutig!

4) Es gibt Darstellung

$$b = qa + r \quad \text{mit} \quad |r| \le \frac{|a|}{2} \qquad (q, r \in \mathbb{Z}),$$

doch diese ist nicht eindeutig ⌜falls a gerade⌟.

<u>Bew.</u> siehe Bild bzw. ÜA.

<u>Beweis von Satz 1:</u> Sei J ein bel. Ideal von $R = \mathbb{Z}$.

Für $J = \{0\}$ Beh. klar, da $\{0\} = (0)$. Sei also $J \neq \{0\}$.

$\exists\, a \in J$ mit $a \neq 0$. Wähle a so, daß $|a|$ minimal.

<u>Beh.</u> $J = (a)$. $(a) \subseteq J$ klar.

Sei $b \in J$ bel. Nach F2 gibt es $q, r \in \mathbb{Z}$ mit

$$b = qa + r \quad \text{mit} \quad |r| < |a|. \quad , \Rightarrow$$

$$r = b - qa \in J \quad (\text{da } J \text{ Ideal}), \quad \xrightarrow[\text{Wahl von } a]{|r|<|a|} r = 0, \Rightarrow$$

$$b = qa \in (a) \qquad \square$$

Beweisanalyse zu Satz 1 führt auf

<u>Def. 3</u>: Ein Integritätsring R heißt ein <u>euklidischer Ring</u>, falls eine Funktion

$$\nu : R \longrightarrow \mathbb{N}_0 \quad \text{mit} \quad \nu(0) = 0$$

existiert, so daß gilt: Zu $a, b \in R$ mit $a \neq 0$ existieren $q, r \in R$ mit

$$b = qa + r \quad \text{und} \quad \nu(r) < \nu(a).$$

<u>Beispiele:</u> ① $R = \mathbb{Z}$ mit $\nu(a) = |a|$

② $R = K[X]$, K <u>Körper</u> mit $\nu(g) = \operatorname{grad}(g) + 1$ für $g \neq 0$
$\nu(0) = 0$

③ $R = \mathbb{Z}[i]$ mit $\nu(z) = N(z) = z\bar{z} = |z|^2$. <u>Bew.</u> in §5.

<u>F3:</u> Jeder euklidische Ring ist ein Hauptidealring.

<u>Bew.</u> wie oben für $R = \mathbb{Z}$ (mit δ statt $|\,|$) $\square$

Also: $K[X]$ ist Hauptidealring für Körper K.

$\mathbb{Z}[X]$ ist <u>kein</u> Hauptidealring, aber <u>faktoriell</u> (vgl. Algebra I, S. 58ff.)

$\mathbb{Z}[i]$ ist Hauptidealring, also faktoriell! Denn:

<u>F4:</u> Jeder Hauptidealring ist faktoriell.

<u>Bew.</u> z.z. 1) Jedes $a \neq 0$ aus R hat Zerlegung in unzerlegbare Faktoren

2) Jedes unzerlegbare Element von R ist ein Primelement.

Beweis von 1): Aufgabe 12

Beweis von 2): $p \mid ab$, $p \nmid a$. <u>z.z.</u> $p \mid b$.

$$p \nmid a \Rightarrow 1 \text{ ist ein ggT von } a,p \overset{F1}{\Longrightarrow} 1 = xa + yp \text{ mit } x,y \in R,$$

$$\xRightarrow{\text{Multipl. mit } b} b = xab + ypb, \quad \xRightarrow{p \mid ab} p \mid b.$$

q.e.d.

<u>Bem.</u> Für $R = \mathbb{Z}$ erhalten wir so einen zweiten Beweis des Hauptsatzes der elementaren Arithmetik.

Im folgenden sei R ein <u>euklidischer Ring</u> mit eukl. Normfkt. ν.

allgemein gilt:

"elementare Umformung" (U) $\quad (a_1, a_2, \dots, a_n) = (a_1, a_2 - y_2 a_1, \dots, a_n - y_n a_1)$ für bel. $y_i \in R$

Euklidischer Algorithmus:

gegeben $a_1, \dots, a_n \in R$. Wir wollen $d \in R$ bestimmen mit

$$(a_1, \dots, a_n) = (d)$$

Sind alle $a_i = 0$, so $d = 0$. Fertig. Sei o.E.

$$a_1 \neq 0 \quad \text{und} \quad \nu(a_1) \leq \nu(a_i), \text{ falls } a_i \neq 0.$$

$a_i = q_i a_1 + r_i \qquad \nu(r_i) < \nu(a_1) \qquad i \geq 2$

$r_i = a_i - q_i a_1 \qquad (a_1, \dots, a_n) \overset{(U)}{=} (a_1, r_2, \dots, r_n) \qquad \nu(r_i) < \nu(a_1)$

Verfahren fortsetzen: Am Schluß erhalten wir

$$(d, 0, 0, \dots, 0) = (d)$$

Für $R = \mathbb{Z}$ effektives Verfahren.

Fall $n=2$: $\quad a, b \in R, a \neq 0 \qquad$ [o.E. $b \neq 0$, denn $(a,0) = (a)$]

$b = q_0 a + r_1 \qquad \nu(r_1) < \nu(a) \qquad$ Falls $r_1 = 0$, Schluß. Sonst:

$a = q_1 r_1 + r_2 \qquad \nu(r_2) < \nu(r_1)$

$r_1 = q_2 r_2 + r_3 \qquad \nu(r_3) < \nu(r_2)$

$\vdots$

$r_{n-2} = q_{n-1} r_{n-1} + r_n \qquad \nu(r_n) < \nu(r_{n-1})$

$r_{n-1} = q_n r_n \qquad$ muß abbrechen: $r_{n+1} = 0$

Setze $r_0 := a$, $r_{-1} := b$

$$(*) \quad \boxed{\begin{array}{ll} r_{i-1} = q_i r_i + r_{i+1} & \nu(r_{i+1}) < \nu(r_i) \qquad i = 0, 1, \dots, n-1 \\ r_{n-1} = q_n r_n & \end{array}}$$

$n = 0$ möglich