F8: Sei R faktoriell, P wie oben. Es gelten:

(i) $a \mid b \iff w_p(a) \leq w_p(b)$ für alle $p \in P$.

(ii) Für $a_1, \dots, a_n \in R$ setze

[Die rechten Seiten hängen von P ab]

$$d = \prod_{p \in P} p^{\mathrm{Min}(w_p(a_1), \dots, w_p(a_n))} =: (a_1, \dots, a_n)$$

$$m = \prod_{p \in P} p^{\mathrm{Max}(w_p(a_1), \dots, w_p(a_n))} =: [a_1, \dots, a_n]$$

hierbei setze $p^\infty = 0$

Dann: d ist ein (der) ggT von $a_1, \dots, a_n$; m ist ein kgV von $a_1, \dots, a_n$ (das)

(iii) $a, b \in R$. Dann $ab \mathrel{\hat{=}} \underset{m}{[a,b]} \cdot \underset{d}{(a,b)}$, $m \mathrel{\hat{=}} \frac{ab}{d}$ (wenn a, b nicht beide 0)

(iv) $a_1, \dots, a_n$ paarw. teilerfremd $\iff [a_1, \dots, a_n] \mathrel{\hat{=}} a_1 a_2 \cdots a_n$.
(d.h. $(a_i, a_j) = 1$ für $i \neq j$)

(v) $(a_i, b) = 1$ für $1 \leq i \leq n \implies (a_1 a_2 \cdots a_n, b) = 1$.

(vi) $(a_1 f, \dots, a_n f) \mathrel{\hat{=}} (a_1, \dots, a_n) f$, $[a_1 f, \dots, a_n f] \mathrel{\hat{=}} [a_1, \dots, a_n] f$.

(vii) $((a_1, \dots, a_n), a_{n+1}) = (a_1, \dots, a_n, a_{n+1})$, $[[a_1, \dots, a_n], a_{n+1}] = [a_1, \dots, a_n, a_{n+1}]$

Bew. (i) klar, vgl. (*) in F7 (ii) folgt aus (i).

(iii): $w_p(ab) = w_p(a) + w_p(b) = \mathrm{Max}(w_p(a), w_p(b)) + \mathrm{Min}(w_p(a), w_p(b)) = w_p(m) + w_p(d) = w_p(md)$ $\forall p$

$\Rightarrow ab \mathrel{\hat{=}} md$.

(iv) $w_p(a_1 \cdots a_n) = w_p(a_1) + \dots + w_p(a_n) = \mathrm{Max}(w_p(a_1), \dots, w_p(a_n)) \iff$
$(w_p(a_i) > 0 \Rightarrow w_p(a_j) = 0$ für alle $j \neq i) \iff (a_i, a_j) = 1$ für alle $i \neq j$

(v) $(a_1 a_2 \cdots a_n, b) \neq 1 \Rightarrow \exists p$: $p \mid b$ und $p \mid a_1 \cdots a_n$
$\Downarrow$
$p \mid a_i$ für ein i,

$\Rightarrow (a_i, b) \neq 1$ für ein i, W!

(vi) $w_p((a_1f,\dots,a_nf)) = \mathrm{Min}(w_p(a_1f),\dots,w_p(a_nf)) =$

$\mathrm{Min}(w_p(a_1)+w_p(f),\dots,w_p(a_n)+w_p(f)) =$

$\mathrm{Min}(w_p(a_1),\dots,w_p(a_n)) + w_p(f) = w_p((a_1,\dots,a_n)f)$

(analog für [ ])

(vii) klar wegen (ii).

Bem. Verallgemeinerung von (iii): Seien $a_1,\dots,a_n \in R$ gegeben. Wähle $q_1,\dots,q_n$ und c aus R mit

$$a_1q_1 = a_2q_2 = \dots = a_nq_n = c$$

(z.B. $c = a_1a_2\cdots a_n$, $q_i = \prod_{j\neq i} a_j$). Dann gilt

$$c \mathrel{\hat{=}} \underbrace{(a_1,\dots,a_n)}_{=\,d}\underbrace{[q_1,\dots,q_n]}_{=\,m}$$

Bew. $w_p(dm) = w_p(d) + w_p(m) = \mathrm{Min}_i\, w_p(a_i) + \mathrm{Max}_i\, w_p(q_i)$

$q_i = \frac{c}{a_i}$

$= \mathrm{Min}_i\, w_p(a_i) + \mathrm{Max}_i\,(w_p(c) - w_p(a_i)) = \mathrm{Min}_i\, w_p(a_i) + w_p(c) + \mathrm{Max}_i(-w_p(a_i))$

$= \mathrm{Min}_i\, w_p(a_i) + w_p(c) - \mathrm{Min}_i\, w_p(a_i) = w_p(c)$, $\Rightarrow$ Beh.

Fg: Sei $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Ist $X^n = a$ lösbar in $\mathbb{Q}$, so ist $X^n = a$ auch lösbar in $\mathbb{Z}$. Anders ausgedrückt:

Ist $a \in \mathbb{Z}$ keine n-te Potenz in $\mathbb{Z}$, so ist a auch keine n-te Potenz in $\mathbb{Q}$.

Bew. o.E. sei $a \neq 0$. Vor. $\exists b \in \mathbb{Q}$ mit $b^n = a$. Dann $b \neq 0$, und für jedes p gilt $w_p(b^n) = w_p(a)$, $\Rightarrow n\,w_p(b) = w_p(a)$, $\overset{a\in\mathbb{Z}}{\Longrightarrow} n\,w_p(b) \geq 0$, $\overset{n>0}{\Longrightarrow} w_p(b) \geq 0$. Dies gilt für alle p. Also folgt $b \in \mathbb{Z}$ (vgl. Bem. 1 zu Satz 2)

Anwendung: $\sqrt{2}$ ist irrational (d.h. $\sqrt{2} \notin \mathbb{Q}$). Denn 2 ist kein Quadrat in $\mathbb{Z}$ (aus Größengründen), also ist 2 nach F9 auch kein Quadrat in $\mathbb{Q}$, d.h. $\sqrt{2} \notin \mathbb{Q}$.

Korollar: Sei $n \in \mathbb{N}$, $a \in \mathbb{N}$. Dann sind äquivalent:

(i) a ist n-te Potenz in $\mathbb{Z}$.

(ii) $n \mid w_p(a)$ für alle p.

(iii) a ist n-te Potenz in $\mathbb{Q}$

Bew. (ii) $\Rightarrow$ (i): $w_p(a) = n \cdot q$ mit $q = q(p) \in \mathbb{N}_0$ für jedes p, $\Rightarrow$

$$a = \prod_p p^{w_p(a)} = \prod_p p^{n q(p)} = \Big(\underbrace{\prod_p p^{q(p)}}_{\in \mathbb{Z}\ (\text{sgn} \in \mathbb{N})}\Big)^n$$

(i) $\overset{\text{trivial}}{\Longrightarrow}$ (iii) $\overset{F9}{\Longrightarrow}$ (i) $\overset{\text{klar}}{\Longrightarrow}$ (ii).

Anwendungen: $\sqrt[2]{17}$, $\sqrt[2]{1000}$, $\sqrt[2]{25}$, ... sind irrational, d.h. $\notin \mathbb{Q}$.
$2^3 \cdot 5^3$

F10 (Verallgemeinerung von F9): Gegeben sei ein normiertes Polynom $f(X) \in \mathbb{Z}[X]$, – mit ganzzahligen Koeffizienten also und höchstem Koeffizienten 1. Ist dann b eine Nullstelle von f mit $b \in \mathbb{Q}$, so ist notwendigerweise $b \in \mathbb{Z}$ und außerdem ist b ein Teiler des Absolutkoeffizienten a_0 von f.

Beweis: Sei $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$ mit $a_i \in \mathbb{Z}$ und (o.E.) $n \geq 1$, und für $b \in \mathbb{Q}$ gelte

(1) $\qquad b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0$

Ist $b = 0$, so ist $b \in \mathbb{Z}$ und $a_0 = 0$. Sei also $b \neq 0$.

Aus (1) folgt (Division durch b^n):

$$1 + \underbrace{a_{n-1} \cdot \frac{1}{b} + a_{n-2} \frac{1}{b^2} + \dots + a_1 \frac{1}{b^{n-1}} + a_0 \cdot \frac{1}{b^n}}_{=: c \ \ulcorner \in \mathbb{Q} \lrcorner} = 0$$

Angenommen: $b \notin \mathbb{Z}$. Dann $\exists p$ mit $w_p(b) < 0$, d.h. $w_p(\frac{1}{b}) > 0$. Es folgt

$$0 = w_p(-1) = w_p(c) \geq \operatorname{Min}(\underbrace{w_p(a_{n-1} \cdot \tfrac{1}{b})}_{>0}, \dots \underbrace{w_p(a_0 \tfrac{1}{b^n})}_{>0}) > 0.$$

W! Also doch $b \in \mathbb{Z}$.

Und aus (1) folgt jetzt auch $b \mid a_0$.

§2 Der euklidische Algorithmus

R komm. Ring mit $1 \neq 0$.

Für beliebiges $a \in R$ betrachte man die Menge der Vielfachen von a in R, also

$$Ra = \{xa \mid x \in R\} = \{b \in R \mid a \mid b\}$$

Die Teilmenge $J = Ra$ hat folgende Eigenschaften:

(i) $0 \in J$

(ii) $b_1, b_2 \in J \implies b_1 + b_2 \in J$ [*)]

(iii) $c \in R, b \in J \implies cb \in J$

Def. 1: Eine Teilmenge J von R heißt ein Ideal in R, falls (i), (ii), (iii) gelten.

J heißt ein Hauptideal, wenn es ein $a \in R$ gibt mit

$$J = Ra$$

Wir verwenden die Bezeichnung

$$(a) := Ra$$

und nennen (a) das von $a \in R$ erzeugte Hauptideal.

Bem. (1) $(b) \subseteq (a) \iff a \mid b$, [**)]

insbes. (2) $a \mathrel{\hat{=}} b \iff (a) = (b)$

ferner (3) c gemeinsames Vielfaches von $a_1, \dots, a_n \iff (c) \subseteq (a_1) \cap \dots \cap (a_n)$

---

*) Mit (ii), (iii) gilt auch: $b_1, b_2 \in J \implies b_1 - b_2 \in J$ (denn $-b_2 = (-1)b_2$)

**) vollständige Beschreibung der Teilbarkeitsrelation $\mid$ in R durch die Relation $\subseteq$ (in der Menge der Teilmengen von R)

somit

(4) m ist ein kgV von $a_1,\dots,a_n \iff (a_1)\cap\dots\cap(a_n) = (m)$

ferner

(5) d ist gemeinsamer Teiler von $a_1,\dots,a_n \iff (a_i)\subseteq(d)$ für $1\le i\le n$.

und damit auch

(6) d ist gemeinsamer Teiler von $a_1,\dots,a_n \iff Ra_1+Ra_2+\dots+Ra_n\subseteq(d)$

also

(7) d ist ein ggT von $a_1,\dots,a_n \iff (d)$ ist das kleinste Hauptideal mit $Ra_1+\dots+Ra_n\subseteq(d)$. *)

Ein ggT läßt sich also idealtheoretisch nicht so einfach charakterisieren wie oben ein kgV durch (4).

Am schönsten wäre es, wenn $Ra_1+\dots+Ra_n$ ein Hauptideal wäre**):
Dann würde (7) übergehen in

⌜nicht allgemein:⌟ (*) d ist ein ggT von $a_1,\dots,a_n \iff Ra_1+Ra_2+\dots+Ra_n = (d)$

Jedenfalls legt dies folgende Definition nahe:

<u>Def. 2</u>: Ein Integritätsring R heißt ein <u>Hauptidealring</u>, wenn <u>jedes</u> Ideal I von R ein Hauptideal ist.

<u>Bez.</u> Für Elemente $a_1,\dots,a_n$ in einem bel. komm. Ring R mit $1\neq 0$ setze

$$(a_1,\dots,a_n) := Ra_1+\dots+Ra_n \quad ^{***)}$$

Man nennt $(a_1,\dots,a_n)$ <u>das von $a_1,\dots,a_n$ erzeugte Ideal in R</u>.

*) offenbar ist $Ra_1+\dots+Ra_n$ ein <u>Ideal</u> von R. Wie auch $(a_1)\cap\dots\cap(a_n)$.

**) doch das ist i.a. nicht der Fall, siehe aber w.u.

***) das steht in gewisser Kollision mit der Bezeichnung in §1, F8, siehe aber w.u.