<u>F5</u> (<u>Satz von Euklid</u>): Jede Primzahl p ist ein <u>Primelement</u> von $\mathbb{Z}$, d.h. es gilt stets (*).
(Das gleiche gilt für $-p$, also für jedes unzerlegbare Element von $\mathbb{Z}$.)

<u>Bew.</u> s.w.u.

<u>Fundamentalsatz der elementaren Arithmetik</u>: In $\mathbb{Z}$ hat jedes $a \neq 0$ <u>eindeutige</u> Zerlegung in unzerlegbare Faktoren.

<u>Bew.</u> In $\mathbb{Z}$ besitzt jedes $a \neq 0$ eine Zerlegung in unzerlegbare Faktoren (vgl. F3). Die Beh. folgt daher mit F4 aus F5. –

Der springende Punkt ist also die Aussage von F5!

<u>Beweis von F5</u>: Gelte also $p \mid ab$, und o.E. $p \nmid a$.

<u>z.z.</u> $p \mid b$.   o.E. $a, b \in \mathbb{N}$.

Sei $m = \text{kgV}(a,p)$ = kleinstes gemeinsames Vielfaches von a, p.

<u>Beh.</u> $m = ap$

Jedenfalls ist ap ein gemeinsames Vielfaches von a, p. Nach dem <u>Lemma</u> (S.9) folgt daher

$$m \mid ap$$

Es ist $m = ac$ mit $c \in \mathbb{N}$. Also $ac \mid ap$, $\Rightarrow c \mid p \Rightarrow$ $c = 1$ oder $c = p$. Wäre $c = 1$, so $m = a$ und somit $p \mid a$, W!
Also $c = p$, d.h. $m = ap$, wie behauptet.

Nun: $\left.\begin{matrix} p \mid ab \\ a \mid ab \end{matrix}\right\} \overset{\text{Lemma!}}{\Longrightarrow} \underset{\text{kgV}(a,b)}{\overset{\shortparallel}{m}} \mid ab \overset{\text{Beh.}}{\Longrightarrow} ap \mid ab \overset{a \neq 0}{\Longrightarrow} p \mid b$

q.e.d.

(Das Entscheidende war das <u>Lemma</u> auf S.9)

<u>Bem.</u> Eindeutige Zerlegung in unzerlegbare Faktoren hat man z. B. auch für folgende Ringe R (vgl. die Beispiele auf S. 2f.)

$R = \mathbb{Z}[\sqrt{2}]$, $R = \mathbb{Z}[i]$ (Bew. §5)

$R = K[X]$, K Körper (Bew. §2, oder vgl. LA II, S. 142)

$R = \mathbb{Z}[X]$ (vgl. Algebra I, §5: "Satz von Gauß")

$R = K$ Körper (trivial)

$R = \mathbb{C}\langle z\rangle$ (ÜA)

<u>Nicht aber für $R = \mathbb{Z}[\sqrt{-5}]$</u>:

$$3 \cdot 3 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$$

sind wirklich <u>wesentlich verschiedene</u> Zerl'n in <u>unzerlegbare</u> Faktoren (Bew.? vgl. Aufgabe 8!)

Aber Vorsicht: in $\mathbb{Z}[\sqrt{6}]$ hat man

$$2 \cdot 3 = 6 = \sqrt{6}\,\sqrt{6}, \text{ doch } 2, 3, \sqrt{6} \text{ sind } \underline{\text{nicht}} \text{ unzerlegbar}$$

(vgl. Aufgabe 8: $(2+\sqrt{6})(2-\sqrt{6}) = -2$, $(3+\sqrt{6})(3-\sqrt{6}) = 3$, $(2+\sqrt{6})(3-\sqrt{6}) = \sqrt{6}$)

Und in $\mathbb{Z}[\sqrt{6}]$ hat man eindeutige Primfaktorzerlegung! (Bew.? ÜA?)

Nun haben wir also den <u>Fundamentalsatz der elem. Arithmetik</u>.

Jetzt etwas Schulmathematik (aber leichter gemacht als in der Schule):

<u>Def. 7</u>: p Primzahl. Für $a \neq 0$ aus $\mathbb{Z}$ setze

$$w_p(a) = \operatorname{Max}\{k \in \mathbb{N}_0 \mid p^k | a\}^{*)} = \underline{\text{Exponent von } p \text{ in } a}$$

$$\overset{\shortparallel}{e} \qquad p^e | a,\ p^{e+1} \nmid a$$

$w_p(a) \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$

$w_p(0) := \infty$ (sinnvoll, da $p^k | 0$ für <u>alle</u> $k \in \mathbb{N}$)

*) existiert wegen eind. PFZ oder: $p^k | a \Rightarrow p^k \le |a| \Rightarrow k \le \frac{\log|a|}{\log p}$.

F6: Die Funktion $w_p : \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ hat folgende Eigenschaften:

(i) $w_p(a+b) \geq \operatorname{Min}(w_p(a), w_p(b))$

(ii) $w_p(ab) = w_p(a) + w_p(b)$

Zusatz: In (i) gilt $=$, falls $w_p(a) \neq w_p(b)$.

Bew. o.E. $a \neq 0, b \neq 0$.
$$a = p^{w_p(a)} a', \quad p \nmid a'$$
$$b = p^{w_p(b)} b', \quad p \nmid b'$$
o.E. $w_p(a) \leq w_p(b)$

$$a+b = p^{w_p(a)}(\underbrace{a' + b' p^{w_p(b)-w_p(a)}}_{=: c \in \mathbb{Z}}), \implies (i)$$

$w_p(a) < w_p(b)$, $\implies p \nmid c$, $\implies$ Zusatz.

$$ab = p^{w_p(a)+w_p(b)} a'b', \quad p \nmid a'b' \text{ (Euklid!)}$$

$\implies$ (ii).

Satz 2 (Fundamentalsatz der elem. Arithmetik): Für jedes $a \neq 0$ aus $\mathbb{Z}$ gilt $w_p(a) > 0$ nur für endlich viele p. Es ist

(*) $$a = \operatorname{sgn}(a) \cdot \prod_p p^{w_p(a)} \qquad \operatorname{sgn}(a) = \begin{cases} +1 & \text{für } a > 0 \\ -1 & \text{für } a < 0 \end{cases}$$

Bew. o.E. $a \in \mathbb{N}$, d.h. $\operatorname{sgn}(a) = 1$.

$a = q_1 \cdots q_r$ Zerlegung in Primzahlfaktoren q_i

Fasse gleiche zusammen:

(**) $$a = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \qquad (s \leq r)$$

$p \in \mathbb{P}$ bel. $w_p(a) \overset{F6}{=} e_1 w_p(p_1) + \ldots + e_s w_p(p_s) =$
$$\begin{cases} 0 & \text{falls } p \neq p_1, \ldots, p_s \\ e_i & \text{falls } p = p_i \end{cases}$$

Also gilt Satz 2.

<u>Bem'n:</u> <u>1)</u> w_p läßt sich eindeutig zu einer Abbildung $w_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ fortsetzen, so daß (ii) [für alle $a, b \in \mathbb{Q}$]

(i) und (ii) sieh in F6 — gilt. Es gilt dann auch (i). Für $a \neq 0$ aus $\mathbb{Q}$ ist $w_p(a) \neq 0$ nur für endlich viele p, und es gilt

$$a = \operatorname{sgn}(a) \cdot \prod_p p^{w_p(a)}$$

Ferner: $a \in \mathbb{Z} \iff w_p(a) \geq 0$ für alle p

<u>Bew.</u> Definiere $w_p : \mathbb{Q}^\times \longrightarrow \mathbb{Z}$ durch $w_p(\frac{a}{b}) = w_p(a) - w_p(b)$, $b \neq 0$. Wohldefiniert? $\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b \Rightarrow w_p(ab') = w_p(a'b)$ $\overset{F6}{\Longrightarrow} w_p(a) + w_p(b') = w_p(a') + w_p(b) \Rightarrow w_p(a) - w_p(b) = w_p(a') - w_p(b')$.

Rest klar bzw. üA.

<u>2)</u> Nach Satz 2 gilt

$$\underset{\cdot}{\mathbb{N}} \simeq \underset{+}{\mathbb{N}_0^{(\mathbb{P})}} = \{(e_p)_{p \in \mathbb{P}} \mid e_p \in \mathbb{N}_0, e_p = 0 \text{ für fast alle } p\}$$

Isomorphie von Halbgruppen. Nach Bem 1) noch schöner:

$$\mathbb{Q}^\times \simeq \{1, -1\} \times \mathbb{Z}^{(\mathbb{P})} \qquad \text{Isomorphie von } \underline{\text{Gruppen}}$$

<u>Def. 8</u>: Ein Integritätsring R heißt <u>faktoriell</u>, wenn

Nach Satz 2 ist der Ring $\mathbb{Z}$ <u>faktoriell</u>! — jedes $a \neq 0$ aus R eindeutige Zerlegung in unzerlegbare Faktoren hat. (Man spricht dann auch von <u>eindeutiger Primfaktorzerlegung in R</u>.)

($\overset{!}{=}$ unzerlegbare Elte von R, falls R faktoriell)
P heißt <u>Vertretersystem für die Primelemente $\neq 0$</u> von R, wenn

1. Zu jedem Primelt. $q \neq 0$ von R gibt es ein $p \in P$ mit $q \mathrel{\hat{=}} p$.
2. $p, p' \in P$, $p \mathrel{\hat{=}} p' \Rightarrow p = p'$ (d.h. $p \in P$ in 1 ist eind. bestimmt durch q)

Für $R = \mathbb{Z}$ nehme man stets $P = \mathbb{P}$.

Für $R = K[X]$, K Körper nimmt man $P = \{p \in K[X] \mid p \text{ irreduzibel, normiert}\}$

<u>F7:</u> R faktoriell, P wie in Def. 8 (Ein solches P existiert auch, nach dem Auswahlaxiom). Es gibt zu jedem $p \in P$ eine Funktion $w_p : R \longrightarrow \mathbb{N}_0 \cup \{\infty\}$ mit Eigenschaften (i) und (ii) wie in F6, so daß gilt:

a) Für jedes $a \neq 0$ aus R ist $w_p(a) > 0$ nur für endlich viele $p \in P$.

b) Für jedes $a \neq 0$ aus R gilt

$$(*) \quad a = e \prod_{p \in P} p^{w_p(a)} \qquad \text{mit (eind. best.) } e \in R^\times$$

<u>Bew.</u> klar ⌈vgl. den Fall $R = \mathbb{Z}$ oben⌋

<u>Def. 9:</u> Sei R komm. Ring mit $1 \neq 0$. Gegeben $a_1, \ldots, a_n \in R$.

a) Ein $d \in R$ heißt ein ggT von $a_1, \ldots, a_n$, falls:

1. $d \mid a_i$ für alle i 2. $t \mid a_i$ für alle $i \Rightarrow t \mid d$

b) Ein $m \in R$ heißt ein kgV von $a_1, \ldots, a_n$, falls:

1. $a_i \mid m$ für alle i 2. $a_i \mid c$ für alle $i \Rightarrow m \mid c$

<u>Bem.</u> 1) d, d' ggT's von $a_1, \ldots, a_n \Longrightarrow d \mathrel{\hat=} d'$

m, m' kgV's von $a_1, \ldots, a_n \Longrightarrow m \mathrel{\hat=} m'$

(klar)

2) i.a. ist Existenz von ggT's und kgV's nicht gesichert. In <u>faktoriellen Ringen</u> existieren sie aber immer, siehe die folgende Feststellung.

Frage eines Studenten nach einem Integritätsring R und Elementen a,b in R, für die kein ggT bzw. kein kgV existieren.

① Vorbemerkung: Sei R Integritätsring; $a,b \in R\setminus\{0\}$. Es existiere $m = \mathrm{kgV}(a,b)$ in R. Dann ist $d := \frac{ab}{m}$ ein ggT von a,b. Beweis: Zunächst ist wirklich $d \in R$. Wegen $a = \frac{m}{b}\, d$ gilt $d \mid a$, desgl. $d \mid b$. Sei t ein gem. Teiler von a,b. Da $\frac{ab}{t} = a\frac{b}{t} = \frac{a}{t}\cdot b$ gemeins. Vielfaches von a und b ist, muß $m \mid \frac{ab}{t}$ gelten, d.h. $t \mid \frac{ab}{m} = d$.)

② Sei $R = \mathbb{Z}[\sqrt{-5}]$. Dann gilt $\mathrm{ggT}(2, 1+\sqrt{-5}) = 1$, denn $2, 1+\sqrt{-5}$ sind beide unzerlegbar, aber nicht zueinander assoziiert (vgl. Aufg. 7). <u>Annahme:</u> Es existiere $m = \mathrm{kgV}(2, 1+\sqrt{-5})$. Mit ① folgt dann $m = 2(1+\sqrt{-5})$. Nun ist aber $2 \mid 6$ und $1+\sqrt{-5} \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$; nach Def. von m folgt $m \mid 6$, d.h. $2(1+\sqrt{-5}) \mid 6$, also $2 \mid 1-\sqrt{-5}$ W!

③ Sei $R = \mathbb{Z}[\sqrt{-5}]$, $a := (1+\sqrt{-5})^2 = -4+2\sqrt{-5} = 2(-2+\sqrt{-5})$, $b := 6$. Annahme: es existiere $\delta = \mathrm{ggT}(a,b)$. Wegen $2 \mid a$, $2 \mid b$ muß $2 \mid \delta$ gelten. Jedenfalls ist δ ein Teiler von 6, mithin $\delta/2 \mid 3$. Doch 3 ist unzerlegbar in R (vgl. Aufg. 8), also ist $\delta/2 \triangleq 3$ oder $\delta/2 \triangleq 1$. Im ersten Fall ist $\delta \triangleq 6$, also müßte 6 ein Teiler von $a = -4+2\sqrt{-5}$ sein, ein Widerspruch. Bleibt also nur $\delta/2 \triangleq 1$, d.h. $\delta \triangleq 2$ übrig. Doch $1+\sqrt{-5}$ ist gemeinsamer Teiler von a und b, also müßte $1+\sqrt{-5} \mid 2$ gelten, mithin $N(1+\sqrt{-5}) \mid N(2)$, d.h. $6 \mid 4$ (vgl. Aufg. 7). W!.

Im übrigen existiert zu obigen a,b auch kein kgV m in R, sonst müßte $d := \frac{ab}{m}$ nach ① ein ggT von a,b sein.