H4

In $\mathbb{Z}$ is er de interessante eigenschap dat elk getal een (op volgorde na, en op ± 1 na) eenduidige ontbinding heeft in priemgetallen

Priemgetallen hebben zelf dan ook de eigenschap dat ze alleen als product $\pm 1 \cdot \pm p$ kunnen worden geschreven. Er bestaan alleen "flauwe" priemontb.

In termen van hun idealen, $ab \in p\mathbb{Z} \Rightarrow a \in p\mathbb{Z} \vee b \in p\mathbb{Z}$
Dit concept kent een veralgemenisering in de ringentheorie

Def (Priemideaal) een id. $I \subset R$ heet priemideaal als

(P1) $I \neq R$
(P2) $\forall a,b \in R \quad ab \in I \Rightarrow a \in I \vee b \in I$

Vb in $\mathbb{Z}$ is $n\mathbb{Z}$ priem $\Leftrightarrow$ n priemgetal (positief of negatief) of $n = 0 \Rightarrow n\mathbb{Z} = \{0\}$

Voor R commutatief

St. 4.3 $\{0\} \subset R$ is priemideaal $\Leftrightarrow$ R is domein

"$\Leftarrow$" Want in een domein is $\{0\} \neq R$ omdat $1 \neq 0 \Rightarrow$ (P1)
en als $ab = 0 \Rightarrow a = 0$ of $b = 0$, want er zijn geen nuldelers $\Rightarrow$ (P2)
"$\Rightarrow$" als $\{0\}$ een priemideaal is, dan $\{0\} \neq R$, dus $\{0\} \cap R^* = \emptyset$
dus $1 \notin \{0\} \Rightarrow 1 \neq 0$. En $ab \in \{0\}$ dan $a \in \{0\}$ of $b \in \{0\}$
dus er zijn geen nuldelers want er zijn geen $a, b \neq 0$ met $ab = 0$

St 4.5 R commutatieve ring, $I \subset R$ ideaal. Dan
I is priemideaal in R $\Leftrightarrow$ R/I is domein

Bew "$\Leftrightarrow$" (P1) $\Leftrightarrow I \neq R \Leftrightarrow 1 \notin I \Leftrightarrow 1 + I \neq 0 + I$
$\Leftrightarrow$ oftewel $\bar{1} \neq \bar{0}$ in R/I

(P2) $\Leftrightarrow$ $\forall a, b \in R \quad ab \in I \Rightarrow a \in I \vee b \in I$

$\Leftrightarrow$ $\forall \bar{a}, \bar{b} \in R/I \quad \bar{a}\bar{b} = I \Rightarrow \bar{a} = I \vee \bar{b} = I$

$\Leftrightarrow$ $\forall \bar{a}, \bar{b} \in R/I \quad \bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = 0 \vee \bar{b} = 0$

$\Leftrightarrow$ R/I heeft geen nuldelers $\square$

Deze stelling levert een snelle manier op om uit te rekenen of I een priemideaal is

Vbd $\mathbb{Z}[X, Y]$ en ideaal $(5, X^2 + Y + 1)$. we berekenen $\mathbb{Z}[X,Y] / (5, X^2 + Y + 1) \cong (\mathbb{Z}[X][Y] / 5\mathbb{Z}[X][Y]) / (X^2 + Y + 1)$

$\cong (\mathbb{Z}/5\mathbb{Z})[X,Y] / (X^2 + Y + \bar{1})$

neem $\mathrm{ev}_{-\bar{1}-X^2} : (\mathbb{Z}/5\mathbb{Z})[X][Y] \to (\mathbb{Z}/5\mathbb{Z})[X]$, surjectief homom. met kern $(X^2 + Y + \bar{1})$

$\cong (\mathbb{Z}/5\mathbb{Z})[X]$

dit is een domein, dus $(5, X^2 + Y + 1)$ is priem

Def (Maximaal Ideaal) R comm. ring. $I \subset R$ ideaal heet maximaal als

(M1) $I \neq R$

(M2) $\forall J \subset R$ ideaal $I \subset J \subset R \Rightarrow I = J \vee J = R$

een maximaal ideaal is niet meer groter te maken, zonder R te krijgen. Dit betekent niet dat het ook het (unieke) grootste ideaal dat $\neq R$ is, is. (Dat zou je een maximumideaal noemen)

St 4.9 R comm. ring ; $\{0\} \subset R$ maximaal $\Leftrightarrow$ R lichaam

Want $1 \neq 0 \Leftrightarrow 1 \notin \{0\} \Leftrightarrow \{0\} \neq R$ (M1)

$(\forall J \text{ id. } \{0\} \subset J \subset R \Rightarrow J = \{0\} \vee J = R)$ $\cancel{\Leftrightarrow}$

~~$(\forall J \text{ id. } J \neq \{0\} \Rightarrow J = R) \Leftrightarrow (\forall J \text{ id. } \exists x \in J \; x \neq 0 \Rightarrow J \cap R^* \neq 0)$~~

$\Rightarrow x \in R, x \neq 0$ ~~dan~~ zou $\{0\} + (x) = R$, dus

$(\{0\} + (x)) \cap R^* \neq 0$ dus $1 \in \{0\} + (x) \Rightarrow$

$\exists a \quad a(x + 0) = 1 \Rightarrow x$ is eenheid. dus $R^* = R - \{0\}$ $\Rightarrow$ lichaam

Andersom en als R lichaam dan als $J \subset R$ $J \neq \{0\}$

dan $\exists x \in J \; x \neq 0 \Rightarrow x \in R^* \Rightarrow J \cap R^* \neq \emptyset \Rightarrow J = R$ $\square$

st 4.10 R comm. ring $M \subset R$ ideaal;
M maximaal in R $\Leftrightarrow$ R/M lichaam

Bew schrijf $\overline{R} = R/M$. We zagen reeds dat elk ideaal J met $M \subset J$ in R
$J \subset R$ een ideaal $\overline{J} = J/M$ levert in $\overline{R}$
dus als $M \subsetneq J \subsetneq R$, dan is $\overline{J}$ een ideaal
van $\overline{R}$ en omdat $M \neq J$ geldt $J/M \neq \{\overline{0}\} \subset \overline{R}$
want $\exists x \in J$ $x \notin M$ dus er is een $\overline{x} \neq \overline{0}$ in $\overline{J}$
En omdat $J \neq R$ volgt $\overline{J} \neq \overline{R}$ want
omgekeerd zien we in dat $\overline{J} \neq \overline{R}$ $\Rightarrow$ voor J zdd $\overline{J} = J/M$
geldt $J \neq R$, en $\overline{J} \neq \overline{0}$ $\Rightarrow$ voor J zdd $\overline{J} = J/M$ geldt $J \neq M$
dus $M \subsetneq J \subsetneq R$ $\Leftrightarrow \{\overline{0}\} = \overline{M} \subsetneq \overline{J} \subsetneq \overline{R}$

Er ligt dus een ideaal J echt tussen
M en R in desda $\{\overline{0}\}$ geen maximaal ideaal van $\overline{R} = R/M$
is, desda R/M geen lichaam is (wegens st. 4.9)
Dus R/M lichaam $\Leftrightarrow$ $M \subset R$ maximaal ideaal ◇

Gevolg elk maximaal ideaal is ook priemideaal.

Nu volgt een interessant stuk over het
bestaan van maximale idealen in een $1 \neq 0$
commutatieve ring. Het lijkt immers logisch
dat zo'n ideaal moet bestaan: als R een
lichaam is, is het $\{0\}$. En anders moet je $\{0\}$
net zo lang groter maken tot je niet verder kunt,
dwz elk elem. $r \in R$ dat je nog zou "toevoegen"
door $+(r)$ te doen, levert heel R op

Toch is het bovenstaande niet triviaal.
In eindige ringen wel. In aftelbare ringen
ook met wat bewijzen uit het ongerijmde.
Maar voor overaftelbare ringen is er geen manier
om één voor één alle $r \in R$ af te gaan. We
gebruiken dan het Lemma van Zorn

Het lemma van Zorn geeft ons al iets maximaals om mee te tellen, n.l. een maximale keten.

We bewijzen eerst het oftelbare geval als speciaal geval

4.13 elke R comm ring met oftelbaar veel elementen en $1 \neq 0$ bezit een maximaal ideaal

Bew We kunnen R oftellen, dus construeer een rijtje $(r_n)_{n\in\mathbb{N}}$ $r_n \in R\ \forall n \in \mathbb{N}$ waarmee we heel R oftellen, $\bigcup_{n\in\mathbb{N}} \{r_n\} = R$.

Definieer analoog een rijtje idealen in R, door

$$I_0 = (0) \quad \text{en} \quad \underset{n\geq 0}{I_{n+1}} = \begin{cases} I_n + (r_{n+1}) & \text{als } I_n + (r_{n+1}) \neq R \\ I_n & \text{anders} \end{cases}$$

omdat $I_n + (r_{n+1})$ het kleinste ideaal is dat I_n en (r_{n+1}) bevat, $I_0 \subset I_1 \subset I_2 \subset \ldots$

Zij nu $M = \bigcup_{n\in\mathbb{N}} I_n$ aante tonen dat dit een ideaal is, vervolgens dat het maximaal is.

Ideaal: want $0 \in I_0 \subset M$ en

$a, b \in M \Rightarrow a \in I_m,\ b \in I_n$ voor zekere $m, n \in \mathbb{N}$

$\Rightarrow m \leq n$ dan $I_m \subset I_n$ dus $a \in I_n \overset{(I1)}{\Rightarrow} a - b \in I_n \subset M$

en $n \geq m$ hetzelfde. $\Rightarrow (I1)$, M^+ og R^+

en $r \in R$, $a \in M$ dan $a \in I_n$ voor zekere $n \in \mathbb{N} \Rightarrow ra \in I_n$

$\Rightarrow ra \in M \quad \Rightarrow (I2)$

Maximaal: als $\exists J \subset R$ ideaal zdd $M \subsetneq J \subsetneq R$

dan is er dus $r \in J$, $r \notin M$. Zij $r = r_n$ voor een $n \in \mathbb{N}$ (aangezien we alle $r \in R$ kunnen oftellen.) $\Rightarrow$ dan moet dus $I_n + (r_n) = R$ zijn geweest, anders zou $I_{n+1} \ni r_n$.

Maar we weten ook dat $I_n \subset M$, $M \subset J$ en $r_n \in J$, dus $(r_n) \subset J$. Dus $I_n \subset J$ $(r_n) \subset J$

$\Rightarrow I_n + (r_n) \subset J$ maar [illegible] $R \subset J$ contradictie

St 4.14 Hetzelfde geldt voor overaftelbare ringen zoals $C^0([0,1])$. Probleem is dat we geen rij $(r_n)_{n\in\mathbb{N}}$ kunnen vormen zodat $\bigcup_{n\in\mathbb{N}}\{r_n\} = R$.

Oplossing: Lemma van Zorn: een stelling die equivalent blijkt aan het keuze-axioma (AC)

— (Lemma van Zorn) elke verzameling V met partiële ordening $\leq$, zeg "poset" $P = (V, \leq)$ .. heeft een maximale keten (tenminste een)

heeft

Def. een keten C (chain) in een poset P is een $C \subset V$ met $\forall x, y \in C \quad x \leq y \vee y \leq x$
(dus $\leq \cap C$ is een totale ordening)

Def. een keten $C \subset V$ heet maximaal als er geen keten $K \subset V$ is met $C \subsetneq K$

Vbd uiteraard is $\emptyset$ een keten. Als $V = \emptyset$ dan is het moeilijk om iets te bewijzen met het Lemma van Zorn!

Bew 4.14 neem als poset $P = \{ I \subset R \mid I \text{ ideaal van } R, I \not\ni 1 \}$ met als ordening inclusie: $I \leq J \Leftrightarrow I \subset J$

Dan mogen we een maximale keten $\{I_n\}_{n\in X}$ kiezen waarbij X de indexverzameling is. $P \neq \emptyset$ immers $\{0\}$ is een ideaal. Dus $\{I_n\}_{n\in X} \neq \emptyset$

definieer $M = \bigcup_{n\in X} I_n$.

M is een ideaal: als $a, b \in M$ dan $\left.\begin{matrix} a\in I_m \\ a \in I_n \end{matrix}\right\}$ $\left.\begin{matrix} I_m \subset I_n \text{ of} \\ I_n \subset I_m \end{matrix}\right\}$ $\begin{matrix} a-b \in I_m \subset M \\ \text{of } a-b \in I_n \subset M \end{matrix}$
en $\{0\} \in \{I_n\}_{n\in X}$ want $\forall I \subset R$ ideaal geldt $\{0\} \subset I$
dus als $\{0\}$ niet in de maximale keten zit, is deze niet maximaal!

en als $r \in R$, $a \in M$ dan $a \in I_n$ voor een $n \in X$ dus
$ra \in I_n \subset M$ dus M is ideaal.

M is maximaal: ~~want als er een $J \subsetneq R$ ideaal is met $M \subsetneq J$, dan is er dus een $r \in J \subsetneq R$ met $r \notin M$ maar dan $(r) \subset J \neq R \Rightarrow (r) \neq R$, en dus $1 \notin (r)$ $M \subset M+(r)$. Maar dan $\forall I \in \{I_n\}_{n\in X}$ geldt $I \subset \bigcup_{n\in X} I_n = M \subsetneq M+(r)$ dus $\forall I \in \{I_n\}_{n\in X}$ $I \subsetneq M+(r)$ Dus we kunnen $M+(r)$ aan~~

want als $M = R$ dan $1 \in M$ dus $\exists n \in X$ $I_n \ni 1$
contradictie, want $I_n \in P$ en we hadden P gekozen zodat $I \in P \Rightarrow 1 \notin I$.
En als $M \subsetneq J \subsetneq R$ dan $\forall I \in \{I_n\}_{n\in X}$ $I \subset M \subsetneq J$
dus is $\{I_n\}_{n\in X}$ niet maximaal, we kunnen immers J toevoegen. $\Rightarrow$ M maximaal ◆

Gevolg R comm. ring $I \subset R$ ideaal en $I \neq R$
Dan is er een maximaal ideaal $M \subset R$ met $I \subset M$

Bew wegens 4.14 heeft R/I een maximaal ideaal en dit is van de vorm M/I waar $M \subset R$ een ideaal is met $M \supset I$. Vervolgens passen we de derde isomorfiest. toe: $R/M \cong (R/I)/(M/I)$
Omdat M/I maximaal is in R/I, is rechterzijde een lichaam wegens 4.10 $\Rightarrow$ R/M lichaam $\Rightarrow$ M maximaal in R. $\square$

Gevolg R comm. Ring. Dan

$$\bigcup_{\substack{M \subset R \\ \text{max. ideaal}}} M = R - R^*$$

Bew M maximaal, dan $M \subset R - R^*$ wegens (M1) en
$I = R \Leftrightarrow I \cap R^* \neq \emptyset$

dus $\bigcup_M M \subseteq R - R^*$. Andersom, als $r \in R - R^*$ dan is (r) een ideaal in R met $(r) \neq R$. Dus is er een maximaal ideaal $M \subset R$ met $(r) \subset M$. dus $r \in (r) \subset M \subset \bigcup_M M \Rightarrow R - R^* \subset \bigcup_M M$.
"$\subset$" en "$\supset$" bewijzen "$=$". $\square$

Gevolg K lichaam, $n, t \in \mathbb{Z}_{>0}$ en $f_1, \dots f_t \in K[X_1, \dots, X_n]$, t polynomen in n variabelen.

TFAE

(i) er zijn geen $g_1, g_2, \dots g_t \in K[X_1, \dots X_n]$ zodat $g_1 f_1 + \dots + g_t f_t = 1$

(ii) er bestaat een lichaam L, $K \subset L$ zodat er $x_1, \dots x_n \in L$ zijn met (als we $f_j \in L[X_1, \dots X_n]$ evalueren in $x_1, \dots x_n$)

$$f_1(x_1, \dots x_n) = 0 \qquad \vdots$$
$$f_2(x_1, \dots x_n) = 0 \qquad f_t(x_1, \dots x_n) = 0$$

Bew ii ⇒ i: stel dat er toch $g_1, \dots g_t \in K[X_1, \dots X_n]$ zijn met $g_1 f_1 + \dots + g_t f_t = 1$
We werken in een comm. ring (lichaam) dus evaluatie is een homomorfisme. Evalueer de rechterzijde in $(x_1, \dots x_n)$ dan staat er $g_1(x_1, \dots x_n) \cdot 0 + \dots + g_t(x_1, \dots x_n) \cdot 0 = 1$ dus $0 = 1$, tegenspraak want K is een lichaam dus $0 \neq 1$.

i ⇒ ii Stel dat er geen $g_1, \dots g_t$ zijn met $g_1 f_1 + \dots + g_t f_t = 1$
Dan betekent dit dat $I = (f_1, \dots f_n) \subset K[X_1, \dots X_n]$ niet heel de ring $K[X_1, \dots X_n]$. Dus bestaat er een maximaal ideaal in, zeg $M \subset K[X_1, \dots X_n]$, $I \subset M$. Beschouw nu $K[X_1, \dots X_n]/M$, een lichaam wegens 4.10
Beschouw nu de samenstelling van ringhomoms
$$K \hookrightarrow K[X_1, \dots X_n] \longrightarrow L = K[X_1, \dots X_n]/M$$

We weten uit H.2 dat een homomorfisme $H : K \to R \neq \{0\}$ van een lichaam K naar een ring R injectief is.
Dit kwam doordat $H(k) = 0$, $k \neq 0 \Rightarrow k^{-1}$ bestaat en dus
$1 = H(1) = H(k^{-1}k) = H(k^{-1})\,H(k) = H(k^{-1}) \cdot 0 = 0$, $1 = 0$ contradictie.
dus $\ker(H) = \{0\} \Rightarrow$ homom injectief.
Dus $K \hookrightarrow K[X_1, \dots X_n] \to L$ is injectief. We kunnen K dan als deelverz. van L opvatten.

Resteert te bewijzen dat er $x_1, \dots x_n \in L$ zijn met
$f_1(x_1, \dots x_n) = \dots = f_t(x_1, \dots x_n) = 0$
We kiezen $x_i = \overline{X_i} = X_i + M \in L$, de restklasse van het polynoom $X_i \in K[X_1, \dots X_n]$, modulo M.

Dan immers ~~voor~~ $f_j \in L[X_1', \dots X_n']$, dat is dus een polynoom in $X_1', \dots X_n'$ maar met de coëfficienten in $K[X_1, \dots X_n]/M$, geldt dat evaluatie in $X_1' \leftarrow X_1 + M$, $X_2' \leftarrow X_2 + M$ .. $X_n' \leftarrow X_n + M$ oplevert:

VB neem $f \in \mathbb{R}[X]$ $f = X^2 + 1$
dan is er een max. ideaal dat $(f) = (X^2+1)$ bevat.
Dit blijkt (X^2+1) zelf te zijn. Dus neem als lichaam L: $\mathbb{R}[X]/(X^2+1)$
dan kunnen we $f \in L[X']$ zien als $\bar{1} X'^2 + \bar{1}$
met $\bar{1} \in \mathbb{R}[X]/(X^2+1)$

$$(\mathbb{R}[X]/(X^2+1))[X'] \xrightarrow{ev_{\bar{X}}} \mathbb{R}[X]/(X^2+1)$$

en evaluatie in $\bar{X}$ levert op: $f(\bar{X}) = \bar{1}\bar{X}^2 + \bar{1}$
$= \overline{1X^2} + \bar{1}$
$= \overline{X^2+1} = \bar{0}$

Ingewikkeld, de coëfficienten van f als gezien in $L[X_1', \dots X_n']$ zijn dus restklassen van polynomen in $K[X_1, \dots X_n]$ modulo $(f_1, \dots f_n)$

Maar dit betekent ook precies dat $f(\overline{X_1}, \dots \overline{X_n}) = \overline{f} \in (f_1, \dots f_n) \subset M$
en dus is $f(\overline{X_1}, \dots \overline{X_n}) = \bar{0}$ in L $\square$

en dat voorbeeld met $\mathbb{R}[X]$ en (X^2+1) ..
we weten dat $\mathbb{C}$ hier prima aan voldoet, $i^2+1=0$
en $\mathbb{R} \subset \mathbb{C}$. Dit is een andere manier om aan
te tonen $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$ $\square$

Opm Dit kan zelfs een alternatieve formulering voor $\mathbb{C}$ zijn.

H