H1

I. Ringentheorie

Def 1.1 Een ring is een vijftupel $(R, +, \cdot, 0, 1)$ met R verzameling en $+, \cdot : R \times R \to R$ afbeeldingen, $0, 1 \in R$ welke samen voldoen aan

(R1) $(R, +, 0)$ is Abelse groep. Dus we weten
(G1) $\forall a,b,c \in R \quad (a+b)+c = a+(b+c)$
(G2) $\forall a \in R \quad 0+a = a+0 = a$
(G3) $\forall a \in R \quad \exists -a \in R \quad a + -a = -a + a = 0$
(G4) $\forall a,b \in R \quad a+b = b+a$

(R2) $\cdot$ is associatief: $\forall a,b,c \in R \ (ab)c = a(bc)$

(R3) distributieve wetten $\forall a,b,c \in R \quad a(b+c) = (ab)+(ac)$
$\forall a,b,c \in R \quad (a+b)c = (ac)+(bc)$

(R4) $\forall a \in R \quad a \cdot 1 = 1 \cdot a = a$

Als voldaan is aan (R5), heet R commutatieve ring

(R5) $\forall a,b \in R \quad ab = ba$

Als voldaan is aan (R6), heet R scheeflichaam, of delingsring

(R6) $1 \neq 0$ en $\forall a \in R, a \neq 0 \ \exists a^{-1} \in R \quad a^{-1}a = aa^{-1} = 1$

Als aan (R5), (R6) beide voldaan is, heet R lichaam
Vaak noteert men lichamen met L, of K (Körper)

◇

Vb $\mathbb{Z}$ is een ring, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ zijn lichamen. Alle zijn commutatief.

Vb $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0} = n\mathbb{Z})$ was een quotiëntgroep van $\mathbb{Z}$ (Groepentheorie). We kunnen het met geschikte vermenigvuldiging $\cdot$ en eenheid 1 uitbreiden tot ring: neem $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ door

$a + n\mathbb{Z}\ ;\ b + n\mathbb{Z} \mapsto ab + n\mathbb{Z}$, en $1 := \bar{1} = 1 + n\mathbb{Z}$.

$\cdot$ is welgedefinieerd, want als $\bar{a} = \bar{a'}$, $\bar{b} = \bar{b'}$

dan $\bar{a} \cdot \bar{b} = \overline{ab}$, $\bar{a'} \cdot \bar{b'} = \overline{a'b'}$

en $ab - a'b' = ab + a'b - a'b - a'b'$

$\underset{|}{=} (a - a')b + a'(b - b')$

gebruik dat $\mathbb{Z}$ een ring is

en $a - a' \in n\mathbb{Z} \Rightarrow (a-a')b \in n\mathbb{Z}$, $b - b' \in n\mathbb{Z} \Rightarrow a'(b-b')$

$\Rightarrow ab - a'b' \in n\mathbb{Z}$ dus $ab + n\mathbb{Z} = a'b' + n\mathbb{Z}$

$\Rightarrow \bar{a} \cdot \bar{b} = \bar{a'} \cdot \bar{b'}$ dus $\cdot$ welgedefinieerd

(R1) volgt uit (Groepentheorie) en (R2),

(R3), (R4), (R5) volgen nu eenvoudig uit

dat $\mathbb{Z}$ een commutatieve ring is.

(R6) geldt, zoals we later zullen zien

(dus nog niet bewezen!) $\Leftrightarrow$ n is priemgetal. ⚓

<u>Vb</u> voor $n \in \mathbb{Z}_{\geq 0}$ en R een ring definiëren we $M(n, R)$ als de verzameling van uitdrukkingen A waarbij voor elke $(i,j) \in \{1, .. n\}^2$ er een $A_{ij} \in R$, en we definiëren $+, \cdot$ als

$A + B$ door $(A+B)_{ij} = A_{ij} + B_{ij} \in R$

$A \cdot B$ door $(A \cdot B)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} \in R$

twee elementen A, B zijn gelijk als $A_{ij} = B_{ij}$ voor alle i, j

wat $A + B$, $A \cdot B$ weer tot uitdrukkingen in $M(n, R)$, wat $+, \cdot$ welgedefinieerd maakt.

We zien eenvoudig door iteratie over $(i,j) \in \{1, .. n\}^2$ dat (R1) geldt. Nu voor will. $(i,j) \in \{1, .. n\}^2$ ook:

└ met 0 = elem. met $0_{ij} = 0 \in R$

(R2) $[(AB)C]_{ij} = \sum_{k=1}^{n} (AB)_{ik} C_{kj} = \sum_{k=1}^{n} \left(\sum_{l=1}^{n} A_{il} B_{lk} \right) C_{kj}$

$= \sum_{l=1}^{n} A_{il} \sum_{k=1}^{n} B_{lk} C_{kj} = \sum_{l=1}^{n} A_{il} (BC)_{lj} = [A(BC)]_{ij}$

(R3) $[A(B+C)]_{ij} = \sum_{k=1}^{n} A_{ik} (B+C)_{kj} \underset{|}{=} \sum_{k=1}^{n} (A_{ik} B_{kj} + A_{ik} C_{kj})$

wegens (R3) in R

$= \sum_{k=1}^{n} A_{ik} B_{kj} + \sum_{k=1}^{n} A_{ik} C_{kj} = (AB)_{ij} + (AC)_{ij}$

analoog $[(A+B)C]_{ij} = (AC)_{ij} + (BC)_{ij}$

voor $1 \in M(n,R)$ gedefiniëerd door $1_{ij} = \underbrace{\delta_{ij}}_{\text{kronecker delta}} := \begin{cases} 0 & \text{als } i \neq j \\ 1 & \text{als } i = j \end{cases}$

geldt (R4),

n.l. $(A1)_{ij} = \sum_{k=1}^{n} A_{ik} 1_{kj} = 0 + 0 + \cdots + A_{ij} 1 + 0 \cdots = A_{ij}$

$(1A)_{ij} = \sum_{k=1}^{n} 1_{ik} A_{kj} = 1 \cdot A_{ij} = A_{ij}$ (let goed op welke 1,0)

maar i.h.a. voor $n \geq 2$ is $M(n,R)$ niet commutatief

neem bijvoorbeeld $A \in M(n,R)$ met $A_{ij} = \begin{cases} 1 & \text{als } i = 1 \leftarrow \text{index} \\ 0 & \text{als } i \neq 1 \end{cases}$

en $A^t \in M(n,R)$ (suggestieve notatie!)

met $(A^t)_{ij} = A_{ji}$ Dan $(A^t \cdot A)_{11} = \sum_{k=1}^{n} A_{k1} A_{k1} = 1 \cdot 1 + 0 \cdot 0 + \cdots 0 \cdot 0$
$= 1$

terwijl $(A \cdot A^t)_{11} = \sum_{k=1}^{n} A_{1k} A_{1k} = 1 + 1 + \cdots + 1$
$=: n$. Als $n = 1$ hebben we een probleem,

neem dan $A'_{ij} = \begin{cases} 1 & \text{als } i = 1 \quad j \neq 1 \\ 0 & \text{anders} \end{cases}$ dan krijgen we $n - 1$ ..

Notatie omdat we zo gewend zijn aan gehele getallen en $1+1+1+1$ voor $1 \in R$ lang is om op te schrijven, hebben we "scalaire vermenigvuldigingsnotatie" $nr = \overbrace{r + r + \cdots + r}^{n \text{ keer}}$ en ihb $n = 1 + 1 + \cdots + 1$ en $-n = -1 + -1 + \cdots + -1$

Vervolg ook is niet elke $A \neq 0$ "inverteerbaar". (R6)

We hebben het in het voorgaande natuurlijk gehad over de welbekende vierkantsmatrices met elementen uit R

Het blijkt dat $M(n,R)$ commutatief is desda $n = 1$ en R comm. of $n = 0$, of $n \neq 1, 0$ en $R = 0 = \{0\}$. de nulring. $\square$

Vb (Quaternionen) voor $a, b, c, d \in \mathbb{R}$ bekijken we uitdrukkingen $a + bi + cj + dk$, en de verzameling van al deze uitdrukkingen noemen we $\mathbb{H}$. We definiëren optelling als componentsgewijze optelling $(a + bi + cj + dk) + (a' + b'i + c'j + d'k)$
$= (a+a') + (b+b')i + (c+c')j + (d+d')k$ en $\cdot$ aan de hand van distributieve wetten en $i^2 = -1$, $j^2 = -1$, $k^2 = -1$
en $ij = k$ $jk = i$ $ki = j$ en daarmee moet volgen
$ik = i(ij) = -1j = -j$, evenzo $ji = -k$ $kj = -i$
want we willen dat $a \in \mathbb{R}$ en $h \in \mathbb{H}$ commuteren in de zin dat $a = a + 0i + 0j + 0k \in \mathbb{H}$ geldt $ah = ha$.
formeel gezien zouden we $\cdot$ alleen nog maar mogen definiëren op uitdrukkingen strikt van de vorm $a + bi + cj + dk \in \mathbb{H}$.

maar dit vereist vele pagina's schrijfwerk.
We vermelden dat $\mathbb{H}$ een niet-comm. ring is met eenheid $1 = 1+0i+0j+0k$ en $0 = 0+0i+0j+0k$.
Bovendien kunnen we $\mathbb{R}$ als deelverz. zien van $\mathbb{H}$ dmv canonieke injectie $\mathbb{R} \hookrightarrow \mathbb{H} : a \mapsto a+0i+0j+0k$.

Def

voor $h \in \mathbb{H}$, $h = a+bi+cj+dk$, definiëren we de geconjugeerde $\bar{h} = a-bi-cj-dk$
en de norm $N(h) = h\bar{h} = a^2+b^2+c^2+d^2$
$\overset{\parallel}{\bar{h}h}$ dit kunnen we nagaan.

We zien $N(q) \in \mathbb{R}$ voor elke $q \in \mathbb{H}$ en
$N(q) = 0 \Leftrightarrow q = 0$

gevolg

hieruit volgt dat $\mathbb{H}$ delingsring is, want $\mathbb{R}$ is een lichaam
voor $q \neq 0$ is $N(q) \neq 0$ en dus $N(q)^{-1} \in \mathbb{R}$, dan zien we $N(q)^{-1}\bar{q} = q^{-1}$, want

$$q(N(q)^{-1}\bar{q}) = N(q)^{-1} q\bar{q} = N(q)^{-1}N(q) = 1 \in \mathbb{H}$$
$$\text{en } (N(q)^{-1}\bar{q})q = N(q)^{-1}\bar{q}q = N(q)^{-1}N(q) = 1 \in \mathbb{H}$$

$\mathbb{H}$ is dus een scheeflichaam.

Def 1.6

voor R ring is $R' \subset R$ een deelring als geldt:

(D1) $1 \in R'$
(D2) R'^{+} is een o.g van R^{+}
 (H0) $0 \in R'$
 (H1') $\forall a,b \in R' \quad a-b \in R'$
(D3) $\forall a,b \in R' \quad ab \in R'$

Prop

(i) een $R' \subset R$ is een deelring van R $\Leftrightarrow$ R' is met 0 en 1 en + en · zelf een ring

(ii) als R commutatief is, is R' dat ook
(andersom niet: $\mathbb{C} \subset \mathbb{H}$ middels $a+bi \leftrightarrow a+bi+0j+0k$ is commutatief maar $\mathbb{H}$ niet)

Vb (Gehele getallen van Gauss) $\mathbb{Z}[i] = \{a+bi : a,b\in\mathbb{Z}\}$ met gewone optelling en vermenigvuldiging van complexe getallen is een ring, dus deelring van $\mathbb{C}$.

Het is een commutatieve ring maar geen lichaam. Bijvoorbeeld $z = 1+i$ heeft geen inverse, dan immers $(a+bi)z = (a-b)+(a+b)i = 1$ voor $a,b\in\mathbb{Z}$. Deze vergelijking heeft geen opl. in $\mathbb{Z}$ want $a-b=1$, $a+b=0$ geeft $b=a-1$ dus $a+b = 2a-1 = 0$ maar $2a\in 2\mathbb{Z}$ en $1\notin 2\mathbb{Z}$ en $0\in 2\mathbb{Z}$, contradictie.

Overigens is $\mathbb{Q}[i]$ wél een lichaam met inverse gegeven door $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{Q}[i]$. Merk op dat dit veel lijkt op de norm, geconjugeerde-truc in TT!

Vb Iha definiëren we voor $m\in\mathbb{Z}$ en m geen kwadraat

$$\mathbb{Z}[\sqrt{m}] = \{a+b\sqrt{m} : a,b\in\mathbb{Z}\}$$
$$\mathbb{Q}[\sqrt{m}] = \{p+q\sqrt{m} : p,q\in\mathbb{Z}\}$$

waarbij $\sqrt{m}$ niet meer dan "notatie" is want bijvoorbeeld $m=-5$ heeft niet persé een unieke wortel. Definiëren optelling componentsgewijs $a+b\sqrt{m} + c+d\sqrt{m} = (a+b)+(c+d)\sqrt{m}$
vermenigv. door "$\sqrt{m}^2 = m$" $(a+b\sqrt{m})(c+d\sqrt{m}) = (ac+mbd)+(ad+bc)\sqrt{m}$

dan zien we binnenkort (zie "vgl van Pell") onder welke voorwaarden er inversen zijn etc.

Opm We hebben het nog niet over nuldelers gehad. Nu eerst stelling 1.8.

St. 1.8 R ring. voor alle $a, b, b_1, b_2, \dots b_n \in R$:

$(-b)c = -(bc)$

(i) $a(b_1+\dots+b_n) = ab_1+\dots+ab_n$ — maar dit was al bekend? Nee!

(ii) $(b_1+\dots+b_n)a = b_1a+\dots+b_na$

(iii) $a(b-c) = ab-ac$ Analoog $(a-b)c = ac-bc$

Dit impliceert bijvoorbeeld $a(-c) = -(ac)$ en met inductie $a_1a_2\cdots(-a_k)a_{k+1}\cdots a_n = -(a_1a_2\cdots a_n)$

(iv) $a \cdot 0 = 0 \cdot a = 0$ dit "wisten" we nog niet!

Bewijs eerste twee i, ii met volledige inductie naar n en met (R3).

Verder: $a(b-c) + ac \overset{(R3)}{=} a(b-c+c) \overset{(R1)}{=} a(b) = ab$

dus $(ab)-(ac) = a(b-c)$. analoog $(a-b)c = ac-bc$

Tenslotte $0 \cdot a = (0-0)a = 0 \cdot a - 0 \cdot a = 0$

analoog $a \cdot 0 = a(0-0) = a \cdot 0 - a \cdot 0 = 0$. $\square$

Prop t.o.v vermenigvuldiging vormt R geen groep tenzij $R = \{0\}$. Immers is $\{0\}$ zowel additief als multiplicatief een groep, en als $(R, 1, \cdot)$ groep is dan dus $1 \cdot 0 = 1$ wegens (G2) maar we hebben ook $1 \cdot 0 = 0$ wegens St. 1.8 Dus $0 = 1$. zie nu vervolg:

Prop $0 = 1 \Leftrightarrow R = \{0\}$. Immers "$\Leftarrow$" is triviaal, $1 \in \{0\} \Rightarrow 1 = 0$. "$\Rightarrow$" bewijzen we als volgt: stel $a \in R$, dan $a \overset{(R4)}{=} 1a = 0a \overset{1.8}{=} 0$ dus $R \subset \{0\}$, maar $R \neq \emptyset$ dus $R = \{0\}$.

Def R ring. $a \in R$ heet een eenheid of inverteerbaar als er een $b \in R$ is met $ab = ba = 1$

We definiëren $R^* = \{a \in R : a \text{ is een eenheid}\}$

Prop (eig. St 1.12) R^* is een multiplicatieve groep. Want $R^* \subset R$ en $1 \cdot 1 = 1$ dus $1 \in R^*$ dus (R2) $\Rightarrow$ (G1) voor R^* en 1 is eenheid in R^* wegens (R4) $\Rightarrow$ (G2) en om (G3) te bewijzen is het alleen nodig aan te tonen dat als a inverteerbaar is, dan a^{-1} ook. maar $a^{-1}a = aa^{-1} = 1$, dus a^{-1} is inverteerbaar met als inverse a. Dus als $a \in R^*$, dan $a^{-1} \in R^*$ dus elke $a \in R^*$ heeft een inverse in R^* bevat. $\Rightarrow$ G3

Opm Als R commutatief is, is R^* abels. De omkering geldt niet, zie opgave 15 :).

Def (zwakkere definitie eenheid) $a \in R$ heet <u>linkseenheid</u> als er een $b' \in R$ is met $ab' = 1$ en een rechtseenheid als er een $b'' \in R$ is met $b''a = 1$.

Prop Als a zowel l- als r-eenheid is, is a eenheid.
Want dan (aan te tonen $b' = b''$) geldt $b' = 1b' = (b''a)b'$
$= b''(ab') = b''$

Notatie alternatieve notatie $R^* : U(R)$ (unit)

1.10 R ring, dan: R delingsring $\Leftrightarrow$ (R6): $\forall_{\substack{a \in R \\ a \neq 0}} \exists b \in R \; ab = ba = 1$
$\Leftrightarrow \forall a \in R \setminus \{0\}$ a is eenheid $\Leftrightarrow$ $R^* = R - \{0\}$

Vb $M(n,R)$: we definiëren $\det : M(n,R) \to R$ door

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)} \qquad \underline{R \text{ is commutatief}}$$

We kunnen aantonen (zie opgave 14) dat
$A \in M(n,R)^* \Leftrightarrow \det(A) \in R^* \Leftrightarrow A$ <u>links</u>eenheid $\Leftrightarrow A$ <u>r</u>-eenh.

voor $R = \mathbb{R}$ betekent dit bijvoorbeeld A is inverteerbaar
$\Leftrightarrow \det(A) \neq 0$, want $\mathbb{R}$ is lichaam dus delingsring.
dus $\mathbb{R}^* = \mathbb{R} - \{0\}$.

Opm $GL(n,R)$ uit groepentheorie is exact $GL(n,R) = M(n,R)^*$
(Alleen toen wisten we nog niet dat R elke commutatieve ring kan zijn

Vb $\mathbb{Z}[\sqrt{m}]$ met $m \in \mathbb{Z}$ geen kwadraat, definiëren we eerst de <u>norm</u> $N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m})$
$= a^2 - mb^2 \in \mathbb{Z}$

nu beweren we: $\alpha \in \mathbb{Z}[\sqrt{m}]^* \Leftrightarrow N(\alpha) = \pm 1$

Opm met behulp van $\mathbb{Z}^* = \{-1, +1\}$

"$\Leftarrow$": als $N(a + b\sqrt{m}) = -1$ dan $-(a - b\sqrt{m})$ inverse,
als $N(a + b\sqrt{m}) = 1$ dan $a - b\sqrt{m}$ inverse
"$\Rightarrow$" merk op $N(\alpha\beta) = N(\alpha)N(\beta)$, dus als $\alpha \in \mathbb{Z}[\sqrt{m}]^*$ dan is $\alpha^{-1}\alpha = 1$ dus $N(\alpha\alpha^{-1}) = N(1) = 1$ dus
$N(\alpha)N(\alpha^{-1}) = N(\alpha^{-1})N(\alpha) = 1$

dus $N(\alpha) \in \mathbb{Z}^* = \{\pm 1\}$ $\square$

vervolg

Het vinden van $\mathbb{Z}[\sqrt{m}]$ komt overeen met het vinden van opl. voor de vgl. $a^2 - mb^2 = \pm 1$

Voor $m < 0$: $a^2 + |m| \cdot b^2 = 1 \overset{b=0}{\Rightarrow} a = \pm 1$ want $|m| \geq 1$

$a^2 + |m| \cdot b^2 = -1$ geen opl, LHS ≥ 0

speciaal geval als $|m| = 1$: $a = 0$ $b = \pm 1$

dus $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

en $\mathbb{Z}[\sqrt{m}]^* = \{\pm 1\}$ als $m < -1$

Voor $m > 0$: "vergelijking van Pell" $x^2 - my^2 = 1$ heeft oneindig veel oplossingen.
en als je x, y verwisselt heb je juist alle opl. voor $x^2 - my^2 = -1$.

dit geldt voor algemene m ←

Namelijk, als $x + y\sqrt{m}$ eenheid is met inverse $p + q\sqrt{m}$, dan $x^2 + my^2 + 2xy\sqrt{m} = (x + y\sqrt{m})^2$ heeft inverse $p^2 + mq^2 + 2pq\sqrt{m}$. En omdat nu niet de enige opl. ± 1 zijn of misschien $\pm i$, welke "cyclisch" zijn, blijft de rij $\pm \varepsilon$ $\pm \varepsilon^2$ $\pm \varepsilon^3$ .. maar uitbreiden.
We hoeven alleen te laten zien dat er een niet $-\pm 1-$ oplossing is (een "beginnetje")
Dit is soms best moeilijk:

$m = 67 \Rightarrow$ kleinste $x, y \in \mathbb{Z}$ die eenheid $x + y\sqrt{m}$ geven zijn $x = 48842$ $y = 5967$

♡

Nu iets over nuldelers

Def 1.15

Een $a \in R$ heet een linkernuldeler als $a \neq 0$ $\exists_{\substack{b \in R \\ b \neq 0}}$ $ab = 0$. Rechternuldeler: $\exists_{\substack{c \in R \\ c \neq 0}}$ $ca = 0$

Een $\overset{a \neq 0}{a \in R}$ heet een nuldeler als het een linkernuldeler of een rechternuldeler is

Een $\overset{a \neq 0}{a \in R}$ heet nilpotent als voor zekere $n \in \mathbb{Z}_{>0}$ $a^n = 0$ nilpotent $\Rightarrow$ linker- en rechternuldeler.

Def $a \in R$ heet idempotent als $a^2 = a$
Als $a \notin \{0,1\}$ dan idempotent $\Rightarrow$ nuldeler want
$a(a-1) = a^2 - a = 0$ terwijl $a \neq 0$ $a-1 \neq 0$

VB we zien $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ idempotent, dus nuldeler want
$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} = 0$. Tevens is $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ nilpotent voor $n=2$

St. 1.17 Een $a \in R$ kan niet tegelijk nuldeler en eenheid zijn. (1hb een <u>linkernuldeler & r. eenheid</u> of <u>r. nuldeler & l. eenheid</u>)

Bew als $a \in R$ en $a = 0$, dan is a geen nuldeler dus de stelling waar. Als $a \neq 0$, stel a is zowel nuldeler als eenheid
dus $ab = 0$ voor een $b \neq 0$ en $ac = ca = 1$ voor $c \in R$
dan $b = 1b = cab = c \cdot 0 = 0$ contradictie ■

Opm Het blijkt wél mogelijk dat a een links-eenheid en linkernuldeler is, of rechtereenheid en rechternuldeler.

Het bewijs van 1.17 laat alleen zien dat een linkernuldeler niet een rechtseenheid kan zijn, en analoog kan men aantonen dat een rechternuldeler geen linkseenheid kan zijn.

Er zijn dus tegenvoorbeelden. Maar bijvoorbeeld niet in de matrixring $M(n,R)$, als R commutatief is, want daar is A inverteerbaar desda linksinverteerbaar desda rechtsinverteerbaar.

En natuurlijk ook niet in commutatieve ringen want ook daar $a \in R^* \Leftrightarrow$ a linkseenheid $\Leftrightarrow$ a rechtseenh.

Gevolg 1.19 Een delingsring heeft geen nuldelers.
Want als $a \in R$, $a \neq 0$ dan $a \in R^*$ dus a kan geen nuldeler zijn.

Def Een verzwakking van het delingsringaxioma (R6) is dan ook: $1 \neq 0$ en R heeft geen nuldelers. Ringen die hier aan voldoen, samen met

(R5) commutativiteit noemen we <u>domeinen</u> of <u>integriteitsgebieden</u>

Stelling 1.20 $\mathbb{Z}/n\mathbb{Z}$ is een lichaam $\iff$ n is priem $(n \in \mathbb{Z}_{>0})$

Bew. We hebben al gezien $\overset{(R6)}{\text{delingsring}} \iff R^* = R - \{0\}$
Dus voor een commutatieve ring R:
R lichaam $\iff R^* = R - \{0\}$.

Als n niet priem is, kunnen we $n = ab$ schrijven voor $a, b \in \mathbb{Z}, 0 < a, b < n$ dus
$\bar{a} \neq \bar{0} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{b} \neq \bar{0} \in \mathbb{Z}/n\mathbb{Z}$ maar wel
$\bar{a}\bar{b} = \bar{n} = \bar{0}$. Dus als n niet priem, zijn er nuldelers, dus is $\mathbb{Z}/n\mathbb{Z}$ geen lichaam.
Dit bewijst "$\Rightarrow$" via modus tollens.
"$\Leftarrow$": als n priem en $\bar{a} \neq \bar{0}$, is aan te tonen $a \in (\mathbb{Z}/n\mathbb{Z})^*$ bewijs: $(\mathbb{Z}/n\mathbb{Z})^+$ heeft orde n, een priem, dus orde$(\bar{a})^+ = \frac{n}{\text{ggd}(a,n)} = n$ dus $\langle \bar{a} \rangle^+ = (\mathbb{Z}/n\mathbb{Z})^+$
dus omdat $\bar{1} \in (\mathbb{Z}/n\mathbb{Z})^+ = \langle \bar{a} \rangle^+$ is er een $m \in \mathbb{Z}$ met
$m\bar{a} = \underbrace{\bar{a} + \cdots + \bar{a}}_{m} = \bar{1} \in \langle \bar{a} \rangle^+$, dus $\bar{m}\bar{a} = \bar{1} = \bar{a}\bar{m}$
want $\mathbb{Z}/n\mathbb{Z}$ commutatief.

◊

Prop Lichamen en deelringen $K' \subset K$ van lichamen zijn domeinen, want (R5) $\Rightarrow$ commutatief en (R6) $\Rightarrow$ geen nuldelers, ook in deelverz. dus ihb deelringen niet.

Stelling 1.23 In R ring zonder nuldelers (opm: niet noodzakelijk commutatief, dus niet per se domein)

(i) $\forall a, b \in R$: $ab = 0 \iff a = 0 \vee b = 0$
(ii) $\forall a, b, c \in R$: $ab = ac \iff a = 0 \vee b = c$

Bew (i) "$\Rightarrow$" als $ab = 0$ maar $a \neq 0$ $b \neq 0$ dan a nuldeler ↯ "$\Leftarrow$" triviaal 1.8
(ii) $ab = ac \iff a(b-c) = 0 \overset{(i)}{\iff} a = 0 \vee b - c = 0$
$\iff a = 0 \vee b = c$ □

Ringconstructies : enkele methoden

1.24 R_1, R_2 ringen, dan $R = R_1 \times R_2$, definieer
optelling $(a,b) + (a',b') = (a+a', b+b')$
vermenigvuldiging $(a,b)(a',b') = (aa', bb')$
$0_R = (0,0)$ $1_R = (1,1)$ (<u>Productring</u>)

commutatief $R \Leftrightarrow R_1$ en R_2 commutatief
want als R commutatief dan $\forall a,b \in R_1$ geldt
$(ab,1) = (a,1)(b,1) = (b,1)(a,1) = (ba,1)$
$\Rightarrow ab = ba \Rightarrow R_1$ comm.
en $\forall a,b \in R_2$ $(1,ab) = (1,a)(1,b) = (1,b)(1,a) = (1,ba) \Rightarrow ab = ba \Rightarrow R_2$ comm.
andersom, $(a,b)(c,d) = (ac, bd) = (ca, db) = (c,d)(b,a)$

en (a,b) idempotent $\Leftrightarrow a \in R_1$ idempotent en $b \in R_2$ idempotent

R is geen domein want $(a,0)(0,b) = (0,0)$ $\forall a \in R_1$ $b \in R_2$

1.25 (Polynoomringen) R ring. polynoom of veelterm met coëfficiënten in R is uitdrukking van de vorm $\sum_{i=0}^{\infty} a_i X^i$ met bijna alle $a_i = 0$, dwz $\exists n$ $\forall i > n$ $a_i = 0$)

twee polynomen zijn gelijk $\Leftrightarrow a_i = b_i$ $\forall i$

Als $a_i = 0$ voor $i > n$ dan schrijft men het polynoom ook wel als $a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$

verder schrijft men $1 \cdot X^i = X^i$ en $(-a)X^i = -aX^i$

$gr(f) = \max\{n \in \mathbb{N}_0 : a_n \neq 0\} \in \mathbb{N}_0$

Voor het nulpolynoom $f = 0 = \sum_{i=1}^{\infty} 0 \cdot X_i$ is graad kwestie van conventie. Ongedefinieerd of, wat ook goed werkt, $-\infty$.

Def a_j heet j-de coëfficiënt.
Def constante coëfficiënt is a_0. $f = a_0$ heet constant polynoom
Def als $f \neq 0$ en $gr(f) = n$ dan heet a_n de kopcoëfficiënt.
Def als kopcoëfficiënt 1 is, heet f <u>monisch</u>

optelling : $\left(\sum_{i=0}^{\infty} a_i X^i\right) + \left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{i=1}^{\infty}(a_i + b_i) X^i$

verm: bepaald door de regels $(a_i X^i)(b_j X^j) = (a_i b_j) X^{i+j}$ en distributieve wetten, dus:

$$\left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{i=0}^{\infty} b_i X^i\right) = \sum_{i=0}^{\infty}\left(\sum_{j+k=i} a_j b_k\right) X^i$$

notatie: $R[X]$

Bewering: dit is een ring.

(R1): $\left(\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i\right) + \sum_{i=1}^{\infty} c_i X^i =$

$$\sum_{i=1}^{\infty}((a_i + b_i) + c_i) X^i = \sum_{i=0}^{\infty}(a_i + (b_i + c_i)) X^i$$

$$= \sum_{i=1}^{\infty} a_i X^i + \left(\sum_{i=1}^{\infty} b_i X^i + \sum_{i=1}^{\infty} c_i X^i\right)$$

etc...

Opm Als R commutatief is, $R[X]$ ook

Opm R kunnen we opvatten als deelring van $R[X]$ namelijk alle constante polynomen. 1 is ook eenheid van $R[X]$

Opm Als R geen nuldelers heeft, $R[X]$ ~~ook~~ niet
En dan geldt pas:

$$gr(f \cdot g) = gr(f) + gr(g)$$

Als R dus een domein is, $R[X]$ ook
want dan is $R[X]$ ook commutatief en geen nuldelers
en $1 \neq 0$ in R, maar $1 \hookrightarrow 1 \in R[X]$ $0 \hookrightarrow 0 \in R[X]$
dus $1 \neq 0$ in $R[X]$.

De omkering is ook waar omdat R deelring van $R[X]$ is.

Polynomen in meerdere veranderlijken:
voor $n \in \mathbb{N}_1$ definieert men inductief

$$R[X_1, \dots, X_n] = \big(R[X_1, \dots, X_{n-1}]\big)[X_n]$$

waaruit direct volgt dat $R[X_1, \dots, X_n]$ een ring is

Def voor $f = \sum_{\substack{i_1 \geq 0,\, i_2 \geq 0 \dots \\ i_n \geq 0}} a_{i_1 i_2 \dots i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$

Vb $f = a_{100} X_1^1 + a_{203} X_1^2 X_3^3 + a_{000} + a_{022} X_2^2 X_3^2$

noteert men kortheidshalve ook wel als

$f = \sum_i a_i X^i$ met "multi-index" $i = (i_1, i_2, \dots i_n)$

en X^i is afk. voor $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$

Def verschillende soorten graden

$$gr_j(f) = \max\{ m \in \mathbb{N}_0 : \exists i \;\; a_i \neq 0 \wedge i_j = m \}$$

$$totgr(f) = \max\{ m \in \mathbb{N}_0 : \exists i \;\; a_i \neq 0 \wedge \sum_j i_j = m \}$$

Vb $totgr(X_1 + 5\underbrace{X_1^2 X_3^3} + 9 + 45 X_2^2 X_3^2) = 5$

$gr_2(X_1 + 5X_1^2 X_3^3 + 9 + 45 X_2^2 X_3^2) = 2$

1.26 (Quotiëntenlichamen) R moet een domein zijn. lichaam construeren genoteerd $Q(R)$ dat R omvat.

Zij $S = R - \{0\}$. omdat we niet weten of R een delingsring is (dus een lichaam) kunnen we niet stellen $S = R^*$!

Bekijk dan $R \times S$ en definieer de equivalentie relatie $\sim$ door

$$(a,s) \sim (b,t) \Leftrightarrow at = bs$$

- reflexief: $as = as \Rightarrow (a,s) \sim (a,s) \quad \forall (a,s) \in R \times S$
- symmetrisch: $(a,s) \sim (b,t) \Rightarrow at = bs \Rightarrow bs = at \Rightarrow (b,t) \sim (a,s)$
- transitief: stel $(a,s) \sim (b,t)$, $(b,t) \sim (c,r)$ dan

$$at = bs, \quad br = ct$$
$$\Downarrow$$
$$atr = bsr \quad brs = cts \Rightarrow$$

$$atr = bsr = brs = cts \Rightarrow art = cst$$

$\Rightarrow (ar - cs)t = 0$ en $t \neq 0$. R domein, dus

$ar - cs = 0 \Rightarrow ar = cs \Rightarrow (a,s) \sim (c,r)$

Nu definiëren we $Q(R) = (R \times S)/\sim$

Voor de equivalentieklasse $[(q,s)] \in Q(R)$ voeren we de suggestieve notatie $\frac{q}{s}$ in.

$+ : \quad \frac{q}{s} + \frac{p}{r} := \frac{qr + ps}{sr}$, $\cdot, +$ in R

$\cdot : \quad \frac{q}{s} \cdot \frac{p}{r} = \frac{qp}{sr}$, $\cdot$ in R

we moeten wel welgedefinieerdheid aantonen, oftewel als $\frac{p}{r} = \frac{p'}{r'}$ $\frac{q}{s} = \frac{q'}{s'}$ dan $\frac{q}{s} + \frac{p}{r} = \frac{q'}{s'} + \frac{p'}{r'}$ en $\frac{q}{s} \cdot \frac{p}{r} = \frac{q'}{s'} \cdot \frac{p'}{r'}$

Bewijs: stel $pr' = p'r \quad qs' = q's$

t.b. $(qr + ps)s'r' = (q'r' + p's')sr$, $qps'r' = q'p'sr$

Het tweede volgt eenvoudig uit commutativiteit van R:

$qps'r' = qs'pr' = q'sp'r = q'p'sr$

Het eerste: $(qr+ps)s'r' = qrs'r' + pss'r' =$

$qs'rr' + pr'ss' = q'srr' + p'rss' = (q'r' + p's')sr$ QED wederom kunnen we $R \hookrightarrow Q(R)$ beschouwen door $r \longmapsto \frac{r}{1}$ "inbedding"

dit werkt, doordat $\frac{s}{1} = \frac{r}{1} \overset{(*)}{\Leftrightarrow} r \cdot 1 = s \cdot 1 \Leftrightarrow r = s$

dus verschillende elem. liggen verschillend, en

$r,s \hookrightarrow \frac{r}{1} \cdot \frac{s}{1} = \frac{rs}{1} \curvearrowright rs$ en $r,s \hookrightarrow \frac{r}{1} + \frac{s}{1} = \frac{r \cdot 1 + s \cdot 1}{1 \cdot 1} = \frac{r+s}{1} \curvearrowright r+s$

Je zou ook kunnen zeggen dat $\phi : R \longrightarrow Q(R)$ gedefinieerd door $\phi(r) = \frac{r}{1}$ een homom. is dat injectief is $(*)$ en surjectief op $\{\frac{r}{1} \in Q(R) : r \in R\}$

maar we komen pas later over homom's te spreken.

Hiermee is ook beweren: R domein $\Leftrightarrow$ R deelring van een lichaam.

N.L. "$\Leftarrow$" is eerder gedaan en triviaal, maar nu kunnen we ook "$\Rightarrow$" doen door $Q(R)$ als lichaam te zien waar $R \hookrightarrow Q(R)$ ingebed is

$Q(R)$ is namelijk een lichaam! voor $\frac{s}{t} \in Q(R)$ is de inverse gegeven door: als $s = 0$ dan is $\frac{s}{t}$ het nulelement $\frac{0}{1}$, want $\frac{0}{t} = \frac{0}{1}$ immers $(0,t) \sim (0,1)$ $\forall t \in S$

En als $s \neq 0$ dan $s \in S$ dus bestaat ook $\frac{t}{s} \in Q(R)$ en laat nu net $\frac{t}{s} \frac{s}{t} = \frac{ts}{st} = \frac{st}{st} = \frac{1}{1}$, de eenheid, evenzo $\frac{s}{t} \cdot \frac{t}{s} = \frac{1}{1}$ wegens commutativiteit.

We zagen dat $R[X]$ een domein is desda R domein is. Voor K lichaam is $K[X]$ dus zeker een domein.

Def $K(X) = Q(K[X])$. merk op dat $K \hookrightarrow K[X] \hookrightarrow Q(K[X])$ als deelring $K \hookrightarrow K(X)$ kan worden gezien

1.27 (Endomorfismeringen)

Def Zij A een abelse groep, met bewerking $+$
Een endomorfisme was een (Groepentheorie) groepshomomorfisme $f : A \to A$

We weten al uit de groepentheorie dat

$$\mathrm{End}(A) = \{ f : A \to A \mid f(a+b) = f(a) + f(b) \ \forall a,b \in A \}$$

een groep vormt onder functie-optelling

$f+g \in \mathrm{End}(A)$ door $(f+g)(a) = f(a) + g(a)$

immers ligt $f+g$ in $\mathrm{End}(a)$ want
$f+g : A \to A$ en $(f+g)(a+b) = f(a+b) + g(a+b)$
$= f(a) + f(b) + g(a) + g(b)$
hier hebben we nodig dat A abels is $\rightarrow$ $= f(a) + g(a) + f(b) + g(b)$
$= (f+g)(a) + (f+g)(b) \Rightarrow f+g \in \mathrm{End}(A)$

Opm Neutraal element $0 : A \to A$ door $f(a) = 0 \in A$ $\forall a$

Onder samenstelling als $\cdot$ is het zelfs een ring: $f \cdot g : A \to A$
gedefinieerd door
$(f \cdot g)(a) = f(g(a))$

(wederom endomorfisme: $f(g(a+b)) = f(g(a) + g(b))$
$= f(g(a)) + f(g(b))$)

neutraal element: $1 = id_A$.
En $id_A = 0 \Leftrightarrow A = \{0\}$ de triviale groep.

Vb $\mathrm{End}(A)$ hoeft niet commutatief te zijn.
Ihb zien we dat voor $A = \mathbb{R}^2$ elke lineaire afbeelding $T : \mathbb{R}^2 \to \mathbb{R}^2$ een endomorfisme is want $T(v+u) = Tv + Tu$ voor $u, v \in \mathbb{R}^2$
Maar we kunnen de lineaire afb $\mathbb{R}^2 \to \mathbb{R}^2$ identificeren met $M(n, \mathbb{R}) \mid n=2$ en deze is niet commutatief. Dus kan $M(2, \mathbb{R}) \hookrightarrow \mathrm{End}(\mathbb{R}^2)$ dat ook niet zijn.

1.29 (Ringen van functies) V verzameling, R ring.
Zij $T = R^V := \{ f : V \to R \}$
T is een ring met:

$+$: $f, g \in T$ $(f+g)(v) = f(v) + g(v) : V \to R$
$\cdot$: $f, g \in T$ $(f \cdot g)(v) = f(v) \cdot g(v) : V \to R$
0: $0(v) = 0 \in R$ $\forall v \in V$
1: $1(v) = 1 \in R$ $\forall v \in V$

we zien snel in dat voor $\#V \geq 2$ en $R \neq \{0\}$ er steeds nuldelers zijn, n.l. neem $v_1 \in V$ en $f(v_1) = 1 \neq 0$, $f(v) = 0$ als $v \neq v_1$ (die zijn er want $\#V \geq 2$) en $g(v_1) = 0$ en $g(v) = 1$ voor $v \neq v_1$
dan $fg = gf = 0$ maar $f, g \neq 0$

Voor $\#V = n \in \mathbb{N}_1$ zien we dat R^V "dezelfde" ring is als $R \times \cdots \times R$.

Voor $V = I \subset \mathbb{R}$ en $R = \mathbb{R}$ kunnen we bijvoorbeeld deelringen van continue / n-diff'bare functies bekijken, $C^0([0,1])$, $C^1([0,1])$, .. etc.
we zien $f, g \notin C^0([0,1])$. Maar toch zijn er nuldelers, hoor! f, g door

$$g(x) = \begin{cases} 0 & x \leq \frac{1}{2} \\ x - \frac{1}{2} & x \geq \frac{1}{2} \end{cases} \qquad f(x) = \begin{cases} \frac{1}{2} - x & x \leq \frac{1}{2} \\ 0 & x \geq \frac{1}{2} \end{cases} \qquad \text{bijvoorbeeld}$$

1.30 (Groepenring) R ring, G multiplicatief genoteerde groep, dan definieert men

$$R[G] = \Big\{ \text{uitdr. van de vorm } \sum_{g \in G} a_g \cdot g \;\Big|\; a_g \in R \text{ en eindig veel } a_g \neq 0 \Big\}$$

$+$: componentsgewijs

$\cdot$: volgens distributieve wetten en voor "monomen"
$(a_g \cdot g)(b_h \cdot h) = a_g b_h \cdot gh$

We merken terzijde de identificatie van $R[X]$ met $\underset{\text{van}}{\text{deelring}}\, R[\mathbb{Z}^+]$ op, door

$$a_0 + a_1 X + \cdots + a_n X^n \longleftrightarrow a_0 \cdot 0 + a_1 \cdot 1 + \cdots + a_n \cdot n$$

want machten tellen we op, zoals we getallen in $\mathbb{Z}$ optellen.

Alleen niet alle $u \in R[\mathbb{Z}^+]$ worden hiermee geraakt, alleen die u van de vorm $u = \sum_{z \in \mathbb{Z}} u_z \cdot z$ met $u_z = 0$ als $z < 0$

We hebben het dus over een echte deelring van $\mathbb{Z}$.

Opm (opm) voor $\{X^n \mid n \in \mathbb{Z}\} = \langle X \rangle$ een multiplicatief door X voortgebrachte groep met $\text{orde}(X) = \infty$ is deze te identificeren met $\mathbb{Z}^+$, zie (Groepentheorie).