H2

Def R_1, R_2 ringen. Een afbeelding $f: R_1 \to R_2$ heet een ringhomomorfisme als

- $f(1) = 1$
- $\forall a,b \in R_1 \quad f(a+b) = f(a) + f(b)$
- $\forall a,b \in R_1 \quad f(ab) = f(a) \cdot f(b)$

Def een bijectief ringhomom. heet een isomorfisme van ringen. Een isomorfisme $R \to R$ is een (r)automorfisme van R

Prop de inverse van een ringisomorfisme is ook een ring-isomorfisme.

Bew $f(f^{-1}(1)) = 1 = f(1) \overset{inj}{\Rightarrow} f^{-1}(1) = 1$

$f(f^{-1}(a+b)) = a+b = f(f^{-1}(a)) + f(f^{-1}(b)) = f(f^{-1}(a) + f^{-1}(b))$

$f(f^{-1}(ab)) = ab = f(f^{-1}(a)) \cdot f(f^{-1}(b)) = f(f^{-1}(a) \cdot f^{-1}(b))$

$\overset{inj}{\Rightarrow} \quad f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b), \quad f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$ $\diamond$

Def we noemen twee ringen isomorf, $R_1 \cong R_2$ als er een isomorfisme $\phi: R_1 \to R_2$ is

Opm Dit is een equivalentierelatie
(vanwege samenstelling $\phi \circ \psi \Rightarrow$ transitiviteit, ϕ^{-1} isom. $\Rightarrow$ symmetrie en $id_R: R \to R \Rightarrow$ reflexiviteit)

Def we spreken analoog van <u>lichaams-</u> homo / iso / endo / auto - morfisme.

<u>**Vb**</u> (Inclusie-afbeelding) $R' \subset R$ deelring, dan is de inclusie-afbeelding $R' \hookrightarrow R$ door $a \mapsto a$ een homomorfisme.
Het is zelfs heel belangrijk, want hierdoor is de beperking van een homomorfisme $\phi: R \to S$ op een deelring R', $\phi|_{R'}$, ook een homomorfisme n.l. de samenstelling $R' \hookrightarrow R \xrightarrow[\phi]{} S$

<u>**Vb**</u> (Conjugatie) voor $s \in R^*$ is $\gamma_s : R \to R$ door $r \mapsto srs^{-1}$ een <u>automorfisme</u>, n.l. met inverse $\gamma_s^{-1} = \gamma_{s^{-1}}$

Voor $M(n, \mathbb{R})$ is voor een $s \in M(n,\mathbb{R})^*$, γ_s precies een basistransformatie en elke basistransformatie induceert een $s \in M(n,\mathbb{R})^*$ omdat de kolommen van s een basis zijn $\Leftrightarrow$ s volle rang $\Leftrightarrow$ s inverteerbaar.

Opm als R commutatief is, geldt $\gamma_s = id_R$ $\forall s \in R$ ~~En~~ De omkering geldt ~~in~~ de groepentheorie wél, nl. als $\gamma_s(a) = a$ $\forall a,s \in G$ dan $as = sa$ $\forall a,s \in G$ dus G abels. Maar in ringen hebben we niet $s \in R$ maar $s \in R^*$, wat minder of evenveel is als $R - \{0\}$ en voor 0 is het triviaal, maar wat nu voor $s \notin R^*$ en $s \neq 0$? klopt $as = sa$ dan nog wel? Wel als $a \in R^*$ wegens: neem γ_a. Maar wat als ook $a \notin R^*$ en $a \neq 0$? Hier gaat ook de syllabus niet verder op in, dus: ?

Def $\mathrm{Im}(f) = \{y \in R_2 \mid \exists v \in R_1 \ f(v) = y\} = f(R_1)$

Meer algemeen: $f(V) = \{y \in R_2 \mid \exists v \in V \ f(v) = y\}$

$\mathrm{Ker}(f) = \{x \in R_1 \mid f(x) = 0\}$

Opm een ringhomom. geeft een groepshomom op de optelgroepen R_1^+, R_2^+. Per definitie, want $f(a+b) = f(a) + f(b)$.

Prop Dus volgt uit de (groepentheorie) $f: R_1 \to R_2$ injectief $\Leftrightarrow$ kern triviaal $\mathrm{Ker}(f) = \{0\}$

In de groepentheorie waren kernen van groepshomom's precies normaaldelers van G

(Recall normaaldeler $N \triangleleft G \Leftrightarrow N$ o.g van G en $\forall n \in N\ \forall g \in G\ \ gng^{-1} \in N$)

In de ringentheorie zullen we zien dat kernen van ringhomom's precies <u>idealen</u> zijn. Deze definiëren we hieronder:

Def $I \subset R$, R ring, heet een ideaal als

(I1) I^+ een o.g. van R^+ is : (H0') $0 \in I$ en (H1') $a-b \in I$ $\forall a,b \in I$

(I2) $\forall a \in I, r \in R\ \ ar, ra \in I$

Opm dit is de definitie voor een "<u>tweezijdig</u>" ideaal. Eenzijdige idealen komen in twee smaken.

Def <u>linksideaal</u> : vervang (I2) door afzwakking

(I2') $\forall a \in I, r \in R\ \ ra \in I$

Def <u>rechts</u>ideaal: (I2'') $\forall a \in I\ r \in R\ \ ar \in I$

Iha vallen deze definities niet samen. Wel in commutatieve ringen.

Opm Het is enigzins te vergelijken met de nevenklassen aN en Na in de groepentheorie: voor N og G

$$\begin{aligned} \forall a \in G\ aN = Na &\Leftrightarrow \forall a \in G\ \forall n \in N\ \exists m \in N\ \ an = ma \\ &\Leftrightarrow \forall a \in G\ \forall n \in N\ \ ana^{-1} (= m) \in N \\ &\Leftrightarrow N \triangleleft G \end{aligned}$$

Wanneer R commutatief is vallen de begrippen samen. Omdat R^+ abels is, is $I^+ \triangleleft R^+$ in elk geval.

Opm

I is geen deelring van R, tenzij $I = R$
want I deelring $\Rightarrow 1 \in I \Rightarrow$
$\forall r \in R \quad 1r \in I \Rightarrow R \subset I \Rightarrow R = I$
en $I = R \Rightarrow I$ deelring $\Rightarrow 1 \in I$

Dus $1 \in I \Leftrightarrow I = R \Leftrightarrow I$ deelring R $\square$

Generalisatie (St. 2.16)

$$I = R \Leftrightarrow I \cap R^* \neq \emptyset \quad (\Leftrightarrow 1 \in I)$$

want $I \cap R^* \neq \emptyset \Rightarrow \exists a \in I \; \exists b \in R \; ab = 1$
dus voor die a, b: $ab \in I$ (wegens (I2))
dus $1 \in I \Rightarrow I = R$
en $I = R \Rightarrow 1 \in I \Rightarrow I \cap R^* \neq 0$ want $1 \in R^*$

$\square$

Opm

$I \neq R$ is wel gesloten onder $+, \cdot$
Het enige verschil met een deelring $R' \neq R$
is dat $1 \in R'$, $1 \notin I$.

St. 2.8

$f: R_1 \to R_2$ ringhomom. Dan is $Ker(f)$
een ideaal van R_1

Bewijs.

We weten al dat $Ker(f)$ een normale
ondergroep, dus ondergroep van R_1^+ is,
dus (I1) is hiermee bewezen.

Dan (I2): stel $x \in Ker(f)$, $r \in R_1$,
dan $f(xr) = f(x)f(r) = 0 \cdot f(r) = 0$
$f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$
$\Rightarrow xr, rx \in Ker(f) \Rightarrow$ I2. $\square$

Opm

De omkering van deze stelling vereist
dat we eerst over quotiëntringen
gaan praten en dan het canonieke
homom. construeren.

2.11 Voor R commutatieve ring en $a_1, a_2, \dots a_n \in R$
Dan definieert men

$$Ra_i = \{r \cdot a_i \mid r \in R\} = a_i R = \{a_i \cdot r \mid r \in R\}$$

en $Ra_i + Ra_j = \{r_i \cdot a_i + r_j \cdot a_j \mid r_i, r_j \in R\}$

Dus herhaald $Ra_1 + \dots + Ra_n$.
We kunnen nagaan dat dit een ideaal is

(I1): voor $a = r_1 a_1 + \dots + r_n a_n$, $b = q_1 a_1 + \dots + q_n a_n$, $r_i, q_i \in R$
is $a - b = (r_1 - q_1) a_1 + \dots + (r_n - q_n) a_n \in Ra_1 + \dots + Ra_n$
en $0 = 0a_1 + \dots + 0a_n \in Ra_1 + \dots + Ra_n$ dus Og. van R^+

(I2): als $a \in Ra_1 + \dots + Ra_n$, dan $a = r_1 a_1 + \dots + r_n a_n$,
dan voor $r \in R$, $ra = (rr_1) a_1 + \dots + (rr_n) a_n \in Ra_1 + \dots + Ra_n$

als R niet commutatief is, is het slechts een linksideaal. rechts-ideaal is dan $a_1 R + \dots + a_n R$.

Indien R duidelijk is, noteert men ook wel
$(a_1, a_2, \dots a_n)$ voor $Ra_1 + \dots + Ra_n$

Def Een ideaal voortgebracht door één $a \in R$,
$aR = Ra = (a)$, noemt men een hoofdideaal

Def een domein waarvan ieder ideaal een hoofdideaal is, noemt men een hoofdideaaldomein (H5!)

Vb $\mathbb{Z}^+$ heeft als ondergroepen alleen $n\mathbb{Z}$ voor $n \in \mathbb{Z}_{\geq 0}$
en deze zijn ook idealen van het domein $\mathbb{Z}$ ((I2) geldt)
Als $I \subset \mathbb{Z}$ ideaal is, moet I dus wel van de vorm $n\mathbb{Z}$ zijn voor een $n \in \mathbb{Z}_{\geq 0}$. Dus $\mathbb{Z}$ is een hoofdideaaldomein.

Vb $(X^2, X) \subset \mathbb{R}[X]$ is een hoofdideaal, n.l. (X).
want $X^2 \in (X)$ en $X \in X$, dus $(X^2, X) \subset (X)$. en $X \in (X^2, X)$
dus $(X) \subset (X^2, X)$

Opm we gebruiken dat als $a_1, a_2, \ldots a_n \in I$, dan $(a_1, \ldots, a_n) \subset I$, want

Ihb geldt dat $(a_1, \ldots a_n)$ het <u>kleinste</u> ideaal is dat $a_1, \ldots a_n$ bevat
(immers $a_i = 1a_i + 0a_2 + \ldots + 0a_n \in (a_1, \ldots, a_n)$)
maar ook, als $a_1, \ldots a_n \in I$ dan
$(a_1, \ldots a_n) \subset I$, immers voor $r_1, \ldots r_n \in R$
zitten wegens (I2) $r_1 a_1, \ldots, r_n a_n \in I$
en wegens (I1) dan $r_1 a_1 + \ldots + r_n a_n \in I$,
$\forall r_1, \ldots, r_n \in R$

St. 2.13 Evaluatiehom. Voor R <u>commutatieve</u> ring, $\alpha \in R$
is de afbeelding $ev_\alpha : R[X] \to R$
door $ev_\alpha(f) = f(\alpha) =$
(voor $f = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$)
$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n \in R$
een homomorfisme van ringen.
Bovendien $ev_\alpha(R[X]) = R$, $\mathrm{Ker}(ev_\alpha) = (X - \alpha)$

<u>Bewijs</u> We hebben nodig dat R commutatief is!
Neem $f = \sum_{n=0}^{\infty} a_n X^n$ $\quad g = \sum_{n=0}^{\infty} b_n X^n$

$ev_\alpha(1) = 1$

$ev_\alpha(f+g) = ev_\alpha\left(\sum_{n=0}^{\infty}(a_n + b_n) X^n\right)$

$= \sum_{n=0}^{\infty}(a_n + b_n)\alpha^n \overset{(R3)}{=} \sum_{n=0}^{\infty} a_n \alpha^n + \sum_{n=0}^{\infty} b_n \alpha^n$

$= ev_\alpha(f) + ev_\alpha(g)$

Nu gebruiken we commutativiteit voor:

$ev_\alpha(f \cdot g) = ev_\alpha\left(\sum_{n=0}^{\infty}\left(\sum_{j+k=n} a_j b_k\right) X^n\right)$

$= \sum_{n=0}^{\infty}\left(\sum_{j+k=n} a_j b_k\right)\alpha^n$

$= \sum_{n=0}^{\infty}\left(\sum_{j+k=n}(a_j \alpha^j)(b_k \alpha^k)\right)$

$= \left(\sum_{j=0}^{\infty} a_j \alpha^j\right)\left(\sum_{k=0}^{\infty} b_k \alpha^k\right) = ev_\alpha(f)\, ev_\alpha(g)$

Opm als R niet commutatief is, gaat het mis:
Vb over $\mathbb{H}$:

$$(X-j)(X+j) = X^2+1 \quad \text{in } \mathbb{H}[X] \text{ en } i \in \mathbb{H}$$

<u>maar</u> $ev_i((X-j)(X+j)) \neq ev_i(X-j)\, ev_i(X+j)$

$$\| \qquad\qquad\qquad\qquad \|$$

$$i^2+1 = 0 \qquad\qquad (i-j)(i+j) = i^2 - ji + ij - j^2 = 2k \neq 0$$

we hebben commutativiteit nodig
om machten van α "door coëfficiënten te halen"
zoals we in $R[X]$ <u>altijd mogen doen</u> wegens
$(a_i X^i)(b_j X^j) = a_i b_j X^i X^j$, iets wat $R[X]$ "gejouwend" commutatief maakt in X^j t.o.v. R.

(vervolg bewijs) ev_α is surjectief, want voor $r \in R$ is het constante polynoom $r \in R[X]$ geëvalueerd in α: $ev_\alpha(r) = r$

Tenslotte $f \in \mathrm{Ker}(ev_\alpha) \Rightarrow a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$
neem $0 \in R \hookrightarrow R[X]$, dan dus

$$f = \sum_{i=0}^n a_i X^i - 0 = \sum_{i=0}^n a_i X^i - \sum_{i=0}^n a_i \alpha^i = \sum_{i=0}^n a_i (X^i - \alpha^i)$$

en $X^i - \alpha^i = \left(\sum_{j=0}^{i-1} \alpha^j X^{i-1-j}\right)(X-\alpha) \in (X-\alpha)$
dus wegens (I1) n keer toepassen op elk monoom
$a_i(X^i - \alpha^i) \Rightarrow f \in (X-\alpha)$.

$$\Rightarrow \mathrm{Ker} \subset (X-\alpha)$$

nu nog $\mathrm{Ker}(ev_\alpha) \supset (X-\alpha)$. merk op $ev_\alpha(X-\alpha) = \alpha - \alpha = 0$
dus $X - \alpha \in \mathrm{Ker}(ev_\alpha) \Rightarrow (X-\alpha) \subset \mathrm{Ker}(ev_\alpha)$

Hiermee is $\mathrm{Ker}(ev_\alpha) = \alpha$ $\Diamond$

Gevolg (van 2.16: $I \cap R^* \neq \emptyset \Leftrightarrow I = R$) Voor R een delingring geldt dat $\{0\}$ en R de enige idealen zijn. Want $R^* = R - \{0\}$, dus ofwel $I \cap R^* = \emptyset$, dat is desda $I = \{0\}$, ofwel $I \cap R^* \neq \emptyset$ en dan $I = R$.

Gevolg $f: K \to R$ ringhomom, K lichaam (of delingsring), is injectief als $R \neq \{0\}$. Want $f(1) = 1 \neq 0$ dus $1 \notin \mathrm{Ker}(f)$, dus $\mathrm{Ker}(f) = \{0\}$.

2.19 (R/I) omdat I^+ wegens $(I1')$ og is van R^+, en R^+ abels is, is $I^+ \triangleleft R^+$, dus $(R/I)^+$ is een goed gedefinieerde (additieve) quotiëntgroep (Groepentheorie)
we definiëren ook $\cdot : R/I \times R/I \to R/I$,
door $\bar{a}, \bar{b} \mapsto \overline{a \cdot b}$. merk op:

$\bar{a} = a + I = I + a$
$\bar{b} = b + I = I + b$, $\bar{a} = \bar{b} \Leftrightarrow a - b \in I$
$\bar{0} = I$

we moeten wel laten zien dat $\cdot$ welgedefinieerd is, dus dat de keuze vd representanten niet uitmaakt. stel $a \equiv a' \bmod I$, $b \equiv b' \bmod I$, dan volgt wegens $(I2)$ precies $\overline{ab} = \overline{a'b'}$ want

$$ab - a'b' = ab + a'b - a'b - a'b' = \underbrace{(a-a')}_{\in I}\underbrace{b}_{\in R} + \underbrace{a'}_{\in R}\underbrace{(b-b')}_{\in I}$$

dus $(a-a')b \in I$ wegens rechtsideaal
$a'(b-b') \in I$ wegens linksideaal
we hebben dus zowel $(I2')$ als $(I2'')$ $\Leftrightarrow (I2)$ nodig
en met $(I1)$ volgt dat $(a-a')b + a'(b-b') \in I$
dus $ab - a'b' \in I$ dus $\overline{ab} = \overline{a'b'}$

Nu is nog aan te tonen dat $(R2)$ $(R3)$ $(R4)$ gelden. $(R1)$ geldt; we hebben Groepentheorie gehad

$(R2)$: $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{a \cdot b} \cdot \bar{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (bc)}$
$= \bar{a} \cdot \overline{bc} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$

$(R3)$: voor $1 + I = \bar{1}$ geldt $\bar{1} \cdot \bar{a} = \overline{1a} = \bar{a} = \overline{a \cdot 1} = \bar{a} \cdot \bar{1}$

$(R4)$ $\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c})$ $\quad$ $(\bar{a} + \bar{b})\bar{c} = \overline{a+b} \cdot \bar{c}$
$= \overline{a(b+c)}$ $\quad$ $= \overline{(a+b)c}$
wegens (R4) in R $= \overline{ab+ac}$ $\quad$ $= \overline{ac+bc}$
$= \overline{ab} + \overline{ac}$ $\quad$ $= \overline{ac} + \overline{bc}$
$= \bar{a}\bar{b} + \bar{a}\bar{c}$ $\quad$ $= \bar{a}\bar{c} + \bar{b}\bar{c}$

vooral schrijfwerk dus.

Def voor $I \subset R$ ideaal heet $\phi: R \to R/I$ door $\phi(a) = a + I$ de canonieke afbeelding

St. 2.20 ϕ is een surjectief homomorfisme, $Ker(\phi) = I$

Bew voor $a+I \in R/I$ is $\phi(a) = a + I$, dus elke $a+I$ voor elke $a \in R$, dus elke $a + I \in R/I$ (elke nevenklasse in R/I heeft een representant in R, of meer dan een) wordt geraakt door ϕ

bovendien is $\phi(ab) = \overline{ab} = \bar{a}\,\bar{b} = \phi(a) \cdot \phi(b)$
$\phi(1) = \bar{1}$ de eenheid op R/I
$\phi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \phi(a) + \phi(b)$

tenslotte $a \in Ker(\phi) \Leftrightarrow \phi(a) = \bar{0}, \Leftrightarrow \bar{a} = \bar{0} \Leftrightarrow$
$a - 0 \in I \Leftrightarrow a \in I$ $\Rightarrow Ker(\phi) = I$ $\square$

Gevolg voor $I \subset R$ deelverz.: is I een ideaal $\Leftrightarrow$ I is de kern van een homomorfisme

Bew we zagen in 2.8 dat een kern een ideaal is. andersom is het canonieke homomorfisme ϕ uit 2.20 een homomorfisme met $Ker(\phi) = I$ voor I een ideaal $\square$

$\longrightarrow$ NU GAAT HET SNEL : HOMOMORFIESTELLINGEN

Deze wil ik even herhalen uit de groepentheorie. Zij G groep en $N \triangleleft G$ en zij G' een groep neem $f: G \to G'$ homomorfisme van groepen met $N \subset Ker(f)$. Dan is er een unieke groeps-homom g met $g: G/N \to G'$ en $f = g \circ \phi$
Bovendien $Ker(g) = \phi(Ker(f))$

Bew schrijf G multiplicatief (n.l. niet per se abels) met e eenheid. g moet voldoen aan $g(\bar{a}) = f(a)$ $\forall a \in G$ maar kan dit wel, m.a.w. zijn er geen a, b met $\bar{a} = \bar{b}$ maar $f(a) \neq f(b)$? Dus aan te tonen: als $\bar{a} = \bar{b}$ dan $f(a) = f(b)$. Bewijs: $\bar{a} = \bar{b} \Rightarrow$ ~~[illegible]~~ $\Rightarrow a^{-1}b \in N$
$aN = bN$

en $N \subset Ker(f)$ dus $a^{-1}b \in Ker(f)$, dus

$f(a^{-1}b) = e \Rightarrow f(a)^{-1}f(b) = e \Rightarrow f(a) = f(b)$

dus g is welgedefinieerd, en $x \in G$ dan $\phi(x) \in Ker(g) \Rightarrow x \in Ker(f)$ ϕ surj $\Rightarrow$ ing $\Rightarrow \phi\, Ker(f) \subset Ker(g)$

$\bar{x} \in Ker(g) \Leftrightarrow x \in Ker(f)$ dus $x \in Ker(f) \Rightarrow \phi(x) \in Ker(g)$ $\Downarrow$ $Ker(g) = \phi\, Ker(f)$

Uniciteit: stel $g' : G/N \to G'$ met

$f = g \circ \phi$, dus $f(a) = g'(\phi(a)) = g'(\bar{a})$

dan als $\bar{a} \in G/N$, dan $g'(\bar{a}) = f(a) = g(a)$

dus g, g' zijn gelijk $\square$

Stelling 2.22 (Homomorfiest. voor Ringen) Laat $f : R_1 \to R_2$ homom van ringen zijn en $I \subset R_1$ ideaal met $I \subset Ker(f)$. Dan is er een unieke $g : R_1/I \longrightarrow R_2$ met $f = g \circ \phi$. Bovendien $Ker(g) = \phi(Ker(f))$

Bew We weten al dat R/I^{+} de quotiëntgroep is en dat er dus een uniek additief groepshomom. $g : R_1/I^{+} \to R_2^{+}$ is met $Ker(g) = \phi(Ker(f))$ en $g = f \circ \phi$. Alleen nog aan te tonen (aangezien kern van g in de ringentheorie precies de kern van het additieve groeps-homom. is) dat $g(1) = 1$ en $g(ab) = g(a)g(b)$

Dit gaat betrekkelijk eenvoudig:

$g(\bar{1}) = f(1) = 1$

$g(\bar{a} \cdot \bar{b}) = g(\overline{ab}) = f(ab) = f(a)f(b) = g(\bar{a})g(\bar{b})$

($g(\overline{ab}) = g(\phi(ab))$, $f(a)f(b) = g(\phi(a))g(\phi(b))$) $\boxtimes$

Stelling 2.23 (Eerste Isomorfiest. Ringen)

$f : R_1 \to R_2$ ringhomom. Dan is er een isomorfisme van ringen $g : R_1/Ker(f) \xrightarrow{\sim} f(R_1)$ gegeven door $a + Ker(f) \longmapsto f(a)$

Ihb als f surjectief is, is $R_1/Ker(f) \cong R_2$

Bewijs Neem g als in 2.22 met $I \subset Ker(f)$ door $I = ker(f)$. Dan is g injectief want $Ker(g) = \phi(Ker(f)) = Ker(f) = \{\bar{0}\} \subset R_1/Ker(f)$

maar ook is g surjectief want als $r \in f(R_1)$ dan is er een $q \in R_1$ met $f(q) = r$, dus voor $\bar{q} = \phi(q) \in R_1/Ker(f)$ geldt $g(\bar{q}) = r$

g is dus een (uniek) isomorfisme $R_1/Ker(f) \xrightarrow{\sim} f(R_1)$

$\diamond$

Prop (Groepentheorie, herhaling) Als $N \subset N' \subset G$ en $N \triangleleft G$, $N' \triangleleft G$, dan $N \triangleleft N'$ en $N'/N \triangleleft G/N$. Omgekeerd is elke $D \triangleleft G/N$ van de vorm $D = N'/N$ voor $N' \triangleright N$, $N' \triangleleft G$

Bew als $N \triangleleft G$ $N' \triangleleft G$ en $N \subset N'$, dan voor $n \in N$, $g \in N'$ geldt $g \in G$ dus vanwege $N \triangleleft G$ ook $gng^{-1} \in N \Rightarrow N \triangleleft N'$

Opm De omkering "$N \triangleleft N'$ $N' \triangleleft G \Rightarrow N \triangleleft G$" is iha niet per se waar. Voor tegenvoorbeelden: probeer de permutatie-groep.

Zij $nN \in N'/N$, $gN \in G/N$. t.b. dat $gN\, nN (gN)^{-1} \in N'/N$ (merk op dat N o.g. N' want N is zelf een groep)

bovendien $(gN)^{-1} = g^{-1}N$ want $gNg^{-1}N = eN = N$ $g^{-1}N\, gN = eN = N$. Dus: $gN\, nN\, g^{-1}N = gng^{-1}N$

maar $n \in N'$ want $nN \in N'/N$ en $g \in G$. Nu gebruiken we $gng^{-1} \in N'$ want $N' \triangleleft G$. Dus $gng^{-1}N \in N'/N$ QED

Zij nu $D \triangleleft G/N$ Dan voor $nN \in D$ $gN \in G/N$ geldt $gN\, nN (gN)^{-1} = gng^{-1}N \in D$. Zij nu $H = \{n \in G \mid nN \in D\}$ we bewijzen dan dat $H \triangleleft G$, en $D = H/N$

bewijs: zij $n \in H$, $g \in G$. dan $nN \in D$, $gN \in G/N$ dus $gng^{-1}N \in D$ dus $gng^{-1} \in H$ bovendien is H o.g. G want $n, m \in H$ dan $nN, mN \in D$ dus $nm^{-1}N = nN(mN)^{-1} \in D$ dus $nm^{-1} \in D$ en $eN \in D$ want D o.g G/N. dus $e \in H$.

$\Rightarrow H \triangleleft G$. Nu nog aan te tonen $D = H/N$. Bewijs $x \in D \subset G/N$, dus $x = aN$ voor $a \in G$. Maar dan $a \in H$ per definitie, dus $x = aN$, $a \in H \Rightarrow D \subset \{hN \mid h \in H\}$

andersom $\{hN \mid h \in H\} \subset D$ per definitie. dus $D = H/N$ voor $H \triangleleft G$.

$\square$

In de ringentheorie bestaat een zeer analoog resultaat.

Prop I, J idealen in R, $I \subset J$

Dan gelden (I1) en (I2) voor I in J en is J/I dus een welgedefinieerde ~~quotiëntring~~. nee iha geen ring
Bovendien is J/I een ideaal van R/I
en $J/I = \phi(J)$ voor $\phi: R \to R/I$ canonieke homom.

Omgekeerd is elk ideaal K in R/I van de vorm J/I met J ideaal in R

Bew I^+ is een o.g van R^+ dus ook van J^+ want $I^+ \subset J^+$ (Groepentheorie) Als $a \in I$ en $r \in J$, dan wegens $J \subset R \Rightarrow r \in R$ dus wegens (I2) voor I in R volgt $ra, ar \in I$, dus (I2) voor I in J volgt. Dus nu is I een ideaal van J

t.b: $J/I = \{ j + I \mid j \in J \}$ is ideaal in R/I
Bewijs: omdat (I1) en (I2) gelden voor I in J volgt dat J/I gesloten is onder quotiëntoptelling in R/I. merk eerst op $J/I \subset R/I$. dus (I1) geldt voor J/I in R/I want tevens $0 \in J$ dus $0 + I \in J/I$. Nu nog (I2) voor J/I in R/I: dit geldt omdat voor $r + I \in R/I$, $j + I \in J/I$ geldt $(r+I)(j+I) = rj + I$ en $(j+I)(r+I) = jr + I$ en $r \in R, j \in J$ per definitie dus $rj, jr \in J$, dus $jr + I, rj + I \in J/I \Rightarrow$ (I2)
Tenslotte $\phi(J) = \{ j + I \in R/I \mid j \in I \} = J/I$

Omkering: stel

Omkering: voor H ideaal van R/I, definiëer $J = \{ r \in R \mid r + I \in H \}$. Dan is J^+ (normaal) o.g. van R^+ omdat H^+ (normaal) o.g van $(R/I)^+$ is (Groepentheorie) dus geldt (I1) voor J. Bovendien voor $r \in R, j \in J$ geldt $j + I \in H$ en $r + I \in R/I$, dus wegens (I2) voor H in R/I geldt $rj + I, jr + I \in H$, dus $rj, jr \in J$ wat J tot ideaal in R maakt omdat nu (I2) ook geldt. Tenslotte

laten we zien $J/I = H$: immers
$J = \{ j \in R \mid j + I \in H \}$ dus als $j \in J$, dan $j + I \in H$
dus $J/I \subset H$. Andersom als $r + I \in H$ voor een
representant $r \in R$, dan $r \in J$ per definitie J,
dus ook $r + I \in J/I$ per definitie J/I. dus $H \subset J/I$
$\Rightarrow H = J/I$
Tenslotte aan te tonen dat $J/I = \phi(J)$, maar dit
is in het voorgaande juist gedaan $\square$

St. 2.24 (Derde Isomorfiestelling voor Ringen)
voor J, I idealen in R en $I \subset J$,
weten we nu J/I ideaal van R/I.
Bovendien
$$(R/I)/(J/I) \cong R/J$$

We herhalen eerst de analoge st. uit
(Groepentheorie)

(Derde Ismfiest. voor Groepen)
voor N, N' normaaldelers G en $N \subset N'$
was N normaaldeler N' en $N'/N \lhd G/N$, en:
$$(G/N)/(N'/N) \cong G/N'$$

Bew neem homom $f: G/N \to G/N'$ door $f(aN) = aN'$
dit is welgedefinieerd want als $aN = bN$ dan
$b^{-1}a \in N \subset N'$ dus $aN' = bN'$.
$\mathrm{Ker}(f) \ni xN \iff f(xN) = N' \iff xN' = N' \iff x \in N'$ $\Updownarrow$ $xN \in N'/N$
dus $\mathrm{Ker}(f) = N'/N$. Pas de 1e Isomorfiest. Gr.
toe dan verkrijgen we $(G/N)/(N'/N) \cong f(G/N)$
en $f(G/N) = \{ xN' \mid xN \in G/N \} = \{ xN' \mid x \in G \} = G/N'$
dus $(G/N)/(N'/N) \cong G/N'$ $\square$

Nu het bewijs van 2.24 :
Zij opgemerkt dat J^+, I^+ normaal o.g. van R^+ zijn
en dus is $f: R/I \to R/J$ zeker een
homomorfisme van groepen. De kern van f is
nog steeds J/I en f is surjectief. We hoeven alleen
nog aan te tonen $f(1) = 1$ en $f(ab) = f(a) f(b)$

merk op dat per definitie $f(1+I) = 1+J$
dus aan $f(1) = 1$ is voldaan.
Verder $f(\bar{a} \cdot \bar{b}) = f(\overline{ab}) = \widetilde{ab} = \tilde{a} \cdot \tilde{b} = f(\bar{a}) \cdot f(\bar{b})$
waarbij $\bar{a} = a + I$, $\tilde{b} = b + J$. Dus f is surjectief
een ringhomom. en de 1e isomorfiestelling
voor ringen geeft nu $(R/I)/(J/I) \cong R/J$ $\Diamond$

Manieren om idealen samen te stellen:

Def (Som van idealen) voor $I, J \subset R$ idealen
definieert men $I + J = \{ i + j \in R \mid i \in I, j \in J \}$

Prop Dit is weer een ring, want
(I1): $x, y \in I$, dan $x = i + j$, $y = i' + j'$, $i, i' \in I$, $j, j' \in J$
dus $x - y = i + j - (i' + j') = (i - i') + (j - j') \in I + J$
en $0 = 0 + 0$, $0 \in I$ $0 \in J$ $\Rightarrow$ $0 \in I + J$ dus $I + J$
is o.g. van R
(I2) $r \in R$, $x \in I + J$, dan $x = i + j$ voor $i \in I$, $j \in J$
en $rx = ri + rj$, $ri \in I$, $rj \in J$ } wegens (I2) op I, J
$xr = ir + jr$, $ir \in I$, $jr \in J$
dus $rx, xr \in I + J$

Def (Product van idealen) $I, J \subset R$ idealen,
$J \cdot I = \{ x_1 y_1 + \dots + x_n y_n \in R \mid x_1, \dots x_n \in I, y_1, \dots y_n \in J$
en $n \in \mathbb{N}_0 \}$

Prop Dit is een ideaal, want $x_1 y_1 + \dots + x_n y_n \in I \cdot J$
$x_1' y_1' + \dots + x_m' y_m' \in I \cdot J$, dan
$(x_1 y_1 + \dots + x_n y_n) - (x_1' y_1' + \dots + x_m' y_m') = \longrightarrow$
(en $0 = 0 \cdot 0$ met $0 \in I$, $0 \in J$, dus $0 \in I \cdot J$)
$\longrightarrow x_1 y_1 + \dots + x_n y_n + (-x_1') y_1' + \dots + (-x_m') y_m$
met $x_1, \dots x_n, x_1', \dots x_m' \in I$, $y_1, \dots y_n, y_1', \dots y_m' \in J$
dus dit ligt ook weer in $I \cdot J$ want $n + m \in \mathbb{N}_0$
dus $(I \cdot J)^+$ is o.g. van R^+
(I2): als $r \in R$ en $x_1 y_1 + \dots + x_n y_n \in I \cdot J$
dan $r(\dots) = \underset{\in I}{(r x_1)} y_1 + \dots + \underset{\in I}{(r x_n)} y_n \in I \cdot J$ } $\Rightarrow$ (I2)
$(\dots) r = x_1 (y_1 r) + \dots + x_n (y_n r) \in I \cdot J$

het nemen van eindige sommen van producten $x_i y_i$, $x_i \in I, y_i \in J$ is noodzakelijk om $I \cdot J$ een additieve ondergroep te laten zijn.

Prop voor $I, J \subset R$ idealen is $I \cap J$ ideaal van R
want I^+, J^+ zijn o.g. van R^+, dus (Groepentheorie) $(I \cap J)^+$ ook $\Rightarrow$ (I1)
en als $r \in R$, $a \in I \cap J$ dan $ra, ar \in I$ wegens $a \in I$
en $ra, ar \in J$ wegens $a \in J$, dus $ra, ar \in I \cap J$ $\Rightarrow$ I2

Opm net als in groepentheorie is $I \cup J$ een ideaal $\Leftrightarrow$ $I \subset J$ of $J \subset I$. Immers is $I \cup J$ een ideaal, dan is $(I \cup J)^+$ og van R^+ dus $I \subset J$ of $J \subset I$ (groepentheorie). En als $I \subset J$ of $J \subset I$ dan is $I \cup J$ juist J of I (verzamelingenleer) dus $I \cup J$ ideaal.

Def twee idealen $I, J \subset R$ heten copriem of relatief priem als $I + J = R$

Opm $I + J$ heeft $I, J \subset I + J$. Bovendien is het het <u>kleinste</u> ideaal dat I, J bevat, want als $I \subset T$, $J \subset T$ voor T ideaal, $I \ni i$, $j \in J$, dan $i + j \in T$ wegens (I1) dus $I + J \subset T$

Opm $I \cdot J \subset I \cap J$ want $\sum_{i=1}^{n} x_i y_i \in I \cdot J$, dus $\forall i$ $x_i \in I$, $y_i \in J$
dan wegens $x_i \in R$, $y_i \in J$ $\overset{(I2)}{\Rightarrow}$ $\forall i$ $x_i y_i \in J$ $\overset{(I1)}{\Rightarrow}$ $\sum_{i=1}^{n} x_i y_i \in J$
en ook wegens $x_i \in I$, $y_i \in R$ $\Rightarrow$ $\forall i$ $x_i y_i \in I$ $\underset{(I1)}{\Rightarrow}$ $\sum_{i=1}^{n} x_i y_i \in I$
$\Rightarrow x_1 y_1 + \dots + x_n y_n \in I \cap J$

Vb In $\mathbb{Z}$ was elk ideaal van de vorm $n\mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$ en was ook elke $n\mathbb{Z}$ een ideaal (immers een hoofdideaal voortgebracht door $n \in \mathbb{Z}$.)

Voor twee idealen $a\mathbb{Z}$, $b\mathbb{Z}$ geldt dan
$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ met $d = ggd(a, b)$
immers weten we dat $d | a$ $d | b$ dus $d\mathbb{Z} \supset a\mathbb{Z}$, $d\mathbb{Z} \supset b\mathbb{Z}$ dus $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$. Andersom hebben

we het uitgeb. Eucl. Algoritme,
zodat $\exists\, k,l \in \mathbb{Z}$ $\quad ak + bl = d \Rightarrow$
$d \in a\mathbb{Z} + b\mathbb{Z} \Rightarrow (d) = d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$
dat bewijst "=".

IHB $a\mathbb{Z}, b\mathbb{Z}$ copriem desda a, b copriem

ook $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}c$ met $c = \mathrm{kgv}(a,b)$
immers $x \in \mathbb{Z}a \cap \mathbb{Z}b \iff a \mid x \quad b \mid x$
$\iff \mathrm{kgv}(a,b) \mid x$
$\iff x \in \mathbb{Z}c$

tenslotte $\mathbb{Z}a \cdot \mathbb{Z}b = \mathbb{Z}ab$

Bewijs: $ab \in \mathbb{Z}a \cdot \mathbb{Z}b$ want $a \in \mathbb{Z}a$, $b \in \mathbb{Z}b$
$\Rightarrow (ab) \subset \mathbb{Z}a \cdot \mathbb{Z}b$. Andersom, als
$x \in \mathbb{Z}a \cdot \mathbb{Z}b$, dan $x = \sum_{i=1}^{n} (k_i a)(l_i b)$
voor $k_i, l_i \in \mathbb{Z}$ want $x_i \in \mathbb{Z}a \iff x_i = k_i a$ etc.
dus $x = ab \sum_{i=1}^{n} k_i l_i \in ab\mathbb{Z} = \mathbb{Z}ab$
dat bewijst $\mathbb{Z}a \cdot \mathbb{Z}b \subset \mathbb{Z}ab$.

De tweede isomorfiestelling voor groepen
valt ook te "generaliseren" naar ringen
Nu eerst: rekenen met idealen.

2.27 Zij R steeds een <u>commutatieve</u> ring

2.28 (Stapsgewijs Uitdelen)
Door $R/J \cong (R/I)/(J/I)$ toe te passen
kunnen we idealen een voor een uitdelen.

Speciaal geval: neem $I + J$. Dan $I \subset I + J$
$$R/(I+J) \cong (R/I)/((I+J)/I)$$
Maar $(I+J)/I$ is te vereenvoudigen
$= \{(i+j) + I \mid i \in I, j \in J\} = \{j + I \mid j \in J\} = J/I$
want $i \in I$ dus $(i+j) + I = j + I$

Dus $R/(I+J) \cong (R/I)/(J/I)$

Nóg speciaal geval: voor R commutatief zijn er de idealen $Ra_1 + \cdots + Ra_n$, $a_1, \ldots a_n \in R$.
Dan:

$$R/(Ra_1 + Ra_2) \cong (R/Ra_1)/(Ra_2/Ra_1)$$
$$= (R/Ra_1)/\, a_2(R/Ra_1)$$
$$= \bar{R}/(\bar{a}_2)$$

met $\bar{R} = R/Ra_1$ en $\bar{a}_2 = a_2 + Ra_1 \in \bar{R}$
en dus $(\bar{a}_2)$ in R/Ra_1, dus $(\bar{a}_2) = \bar{a}_2\bar{R}$

Kort geschreven: $R/(a,b) = (R/(a))/(\bar{b})$

2.29 Idealen voortgebracht door constante polynomen.
R commutatief,
$I \subset R$ ideaal. Zij $I[X] = \{ f \in R[X] \mid \text{coëff} \in I \}$
We zien dat wegens (I1) voor I, $I[X]$ gesloten is onder optelling want voor $f, g \in I[X]$ met $f = \sum_{i=0}^{\infty} a_i X^i$ $g = \sum_{j=0}^{\infty} b_i X^i$ is

$f+g = \sum_{i=1}^{\infty} (a_i + b_i) X^i$ met $a_i + b_i \in I$ dus
$f+g \in I[x]$ en $0 \in I$ dus $0 \in I[X]$ $\Rightarrow$ (I1) voor $I[X]$

maar ook (I2), want als $r \in R[X]$ en $f \in I[X]$
dan $r \cdot f = \sum_{i=0}^{\infty} \left(\sum_{j+k=i} r_j f_k \right) X^i$, $r_j \in R$ $f_k \in I$ $\forall j,k \overset{(I2)}{\Longrightarrow}$
dus $r_j f_k \in I$ $\forall j,k$
dus ook voor j,k zodat $j+k=i$ $\overset{(I1)}{\Longrightarrow} \sum_{j+k=i} r_j f_k \in I$
$\Rightarrow$ $r \cdot f$ heeft coëfficiënten in I $\Rightarrow$ $rf \in I[X]$
ook voor fr, op analoge wijze maar nu $f_j r_k \in I$
$\Rightarrow$ $I[X]$ ideaal van $R[X]$, en

dit had sneller gekund, want we gaan nu een homom. van ringen ϕ maken met $\operatorname{Ker} \phi = I[X]$
neem $\phi: R[X] \to (R/I)[X]$ door $\phi\left(\sum_{i=0}^{\infty} a_i X^i\right) = \sum_{i=0}^{\infty} \bar{a}_i X^i$
Dit is een homom. want ...
en surjectief want $\sum_{i=0}^{\infty} \bar{a}_i X^i$ wordt geraakt door $\sum_{i=0}^{\infty} a_i X^i$

$$\Rightarrow \quad R[X]/I[X] \cong (R/I)[X]$$

Met een isomorfisme

$$f + I[X] \mapsto \phi(f) \quad \text{dus}$$

$$\overline{a_0 + a_1 X + \cdots + a_n X^n} \longmapsto \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_n X^n$$

$\uparrow$

restklasse mod $I[X]$ van polynoom f.

2.30 Met $\alpha \in R$, R commutatief, is $ev_\alpha : R[X] \to R$ surj. homom. Dus 1e isomorfiest. geeft, met $\operatorname{Ker}(ev_\alpha) = (X - \alpha)$, dat

$$R[X]/(X-\alpha) \cong R$$

Dus idealen van lineaire polynomen "delen heel X weg" en reduceren $R[X]$ dus tot R zelf, de constante polynomen zijn nog wel verschillend modulo $X - \alpha$

2.31 $(a, b) = (a; b + ca)$ voor $a, b, c \in R$

2.36 (Chinese Reststelling voor abstracte ringen)

R commutatieve ring, I, J onderling ondeelbare idealen in R. Dan geldt $I \cap J = I \cdot J$ en er is een ring~~hom~~ is omorfisme ϕ

van $R/(I \cdot J) \cong (R/I) \times (R/J)$

<u>Bew</u> dat $I \cdot J \subset I \cap J$ was bekend en alg. geldig
andersom, $I + J = R$ dus kies een $x \in I, y \in J$ met $x + y = 1$ en kies een $z \in I \cap J$. Dan

$$z = z \cdot 1 = z(x+y) = zx + zy \overset{\text{comm.}}{=} xz + zy$$

$\Rightarrow$ wegens $x \in I$ $z \in J$ $xz \in I \cdot J$ en $y \in J$ $z \in I$ $zy \in I \cdot J$
dus ook $xz + zy \in I \cdot J \Rightarrow z \in I \cdot J$,
wat $I \cap J \subset I \cdot J$ bewijst.

Zij nu $\phi_1 : R \to R/I$ en $\phi_2 : R \to R/J$
de canonieke homomorfismen met kernen I, J

$$\phi : R/(I \cdot J) \longrightarrow R/I \times R/J$$

definieer door $\phi(r) = (\phi_1(r), \phi_2(r))$
homomorfisme, want

$$\phi(1) = (\phi_1(1), \phi_2(1)) = (\bar{1}, \bar{1}) = 1$$

$$\phi(ab) = (\phi_1(ab), \phi_2(ab)) = (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b))$$
$$= (\phi_1(a), \phi_2(a)) \cdot (\phi_1(b), \phi_2(b)) = \phi(a) \cdot \phi(b)$$
$$\phi(a+b) = (\phi_1(a+b), \phi_2(a+b)) = (\phi_1(a) + \phi_1(b) \quad \phi_2(a) + \phi_2(b))$$
$$= (\phi_1(a), \phi_2(a)) + (\phi_1(b), \phi_2(b))$$
$$= \phi(a) + \phi(b)$$

Bewijzen we nu $Ker(\phi) = I \cdot J$:

$$x \in Ker(\phi) \Leftrightarrow \phi(x) = 0 \Leftrightarrow \phi_1(x) = 0 \wedge \phi_2(x) = 0$$
$$\Leftrightarrow x \in Ker(\phi_1) = I \wedge x \in Ker(\phi_2) = J$$
$$\Leftrightarrow x \in I \cap J = I \cdot J \Leftrightarrow x \in I \cdot J$$

dus wegens eerste isomorfiestelling

$$R/I \cdot J \cong R/I \times R/J$$

<u>Mits</u> we kunnen ϕ aantonen dat ϕ <u>surjectief</u> is!

laat $x + y = 1$ voor $x \in I$, $y \in J$. $\Rightarrow \begin{cases} y = 1 - x \\ x = 1 - y \end{cases}$

Dan

$$\begin{aligned}
\phi(1-x) &= (\phi_1(1-x), \phi_2(1-x)) \\
&= (\phi_1(1) - \phi_1(x), \phi_2(y)) \\
&= (\bar{1} - \bar{0}, \tilde{0}) \qquad = (\bar{1}, \tilde{0}) \\
\phi(1-y) &= (\phi_1(x), \phi_2(1) - \phi_2(y)) \\
&= (\bar{0}, \tilde{1} - \tilde{0}) \qquad = (\bar{0}, \tilde{1})
\end{aligned}$$

Dus als $(\bar{a}, \tilde{b}) \in R/I \times R/J$,
dan $a, b \in R$ en wordt
$a(1-x) + b(1-y)$ precies afgebeeld
op $(\bar{a}, \tilde{b})$:

ϕ homom (bewezen)

$$\begin{aligned}
&\phi(a(1-x) + b(1-y)) = \\
&\phi(a)\,\phi(1-x) + \phi(b)\,\phi(1-y) = \\
&(\bar{a}, \tilde{a})(\bar{1}, \tilde{0}) + (\bar{b}, \tilde{b})(\bar{0}, \tilde{1}) = \\
&(\bar{a}, \bar{0}) + (0, \tilde{b}) = (\bar{a}, \hat{b})
\end{aligned}$$

$\Rightarrow$ pas eerste isomorfiestelling toe, we zijn klaar.

Gevolg (De "getallen" - Chinese reststelling)

$n, m \in \mathbb{Z}$ onderling ondeelbaar. $\Rightarrow$ Dan
$n\mathbb{Z}$, $m\mathbb{Z}$ onderling ondeelbaar en

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Gevolg er is het isomorfisme van (multiplicatieve) groepen

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

dus volgt $\varphi(nm) = \varphi(n) \cdot \varphi(m)$

Bew Volgt direct uit het voorgaande met de opmerking $(R_1 \times R_2)^* = R_1^* \times R_2^*$