STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

GROEPENTHEORIE EN LINEAIRE ALGEBRA

Oriënterend colloquium voor leraren in Amsterdam en omgeving

1964 - 1965

GROEPENTHEORIE EN LINEAIRE ALGEBRA

Oriënterend colloquium voor leraren in Amsterdam en omgeving

1964 - 1965

I. ABSTRACTE ALGEBRA

§1. Operaties

Met een zeker recht kan men beweren dat de moderne abstracte algebra samenvalt met de studie van operaties. Met name gaat het daarbij om de binaire operaties, maar ook ééntallige operaties spelen een belangrijke rol; voor meertallige operaties (n-aire operaties met $n \geq 3$) is dit slechts in mindere mate het geval.

Door een ééntallige operatie T, gedefinieerd in een verzameling X, wordt aan ieder object x uit X (we noemen x ook een element van X, en schrijven kortweg: $x \in X$) een nieuw object T(x) uit X toegevoegd. In exacte vorm:

Definitie 1. Een ééntallige operatie in een verzameling X is een afbeelding van X in zichzelf.

Voorbeelden.

a) X is de verzameling der reële getallen; T(x) is het getal $-x$.
b) X is de verzameling van alle natuurlijke getallen; $T(x) = x^2$.
c) X is de verzameling van alle mensen; T(x) is de vader van x, als x een vader heeft; zo niet, dan is T(x) dezelfde persoon als x.

Door een tweetallige of binaire operatie T, gedefinieerd in een verzameling X, wordt aan ieder geordend paar (x,y) van objecten x,y uit X een element van X toegevoegd. Alle geordende paren (x,y) van objecten x,y uit X vormen tezamen weer een verzameling, die men gewoonlijk aangeeft met $X \times X$. De exacte definitie van een binaire operatie kan dan als volgt geformuleerd worden:

Definitie 2. Een binaire operatie in een verzameling X is een afbeelding van X × X in X.

Voorbeelden.

d) X is de verzameling der reële getallen; T(x,y) = x.y.

e) X is de verzameling van de positieve gehele getallen; $T(x,y) = x^y$.

f) X is de verzameling der reële getallen; T(x,y) = y-x.

g) X is de verzameling der rationale getallen; T(x,y) is het kleinste der beide getallen x,y.

h) X is de verzameling der gehele getallen ongelijk nul; T(x,y) is de kleinste positieve gemene veelvoud (k.g.v.) van x en y.

i) X = {0,1,4,5,6,9} ; T(x,y) is het eindcijfer van 5x+6y.

j) X is de verzameling van alle deelverzamelingen van het platte vlak; T(x,y) is de vereniging van x en y: T(x,y) = x ∪ y.

k) X is de verzameling van alle deelnemers aan het oriënterend colloquium "Groepentheorie en lineaire algebra"; T(x,y) = x.

In deze lijst voorbeelden zullen sommige U natuurlijk voorkomen, andere daarentegen gekunsteld aandoen. Daarbij ondervindt U hoogst waarschijnlijk als natuurlijk die binaire operaties die ontleend zijn aan de ... algebra!

Het gebruik van de bekende binaire operaties uit de "gewone" algebra — + , - , , : — wordt gewoonlijk weergegeven door het operatiesymbool tussen de variabelen te plaatsen: x+y, x-y, etc. In aansluiting hieraan zullen we in het vervolg van deze paragraaf een willekeurige binaire operatie T, bij toepassing op variabelen x en y, schrijven tussen x en y; dus: xTy i.p.v. T(x,y). Gemakshalve zullen we daarbij vaak als symbool voor een binaire operatie niet T, maar bijv. * kiezen (en later meestal het teken .).

Verreweg de belangrijkste binaire operaties zijn de associatieve operaties.

Definitie 3. Zij * een binaire operatie in X. De operatie * heet associatief indien, voor willekeurige $x,y,z \in X$:

$$x * (y * z) = (x * y) * z .$$

Voorbeelden.

De operatie . in voorbeeld d) is associatief. Evenzo de operaties in g), h), i), j) en k). Daarentegen zijn de operaties in de voorbeelden e) en f) niet associatief, daar i.h.a.

$$\left(x^y \right)^z \neq x^{\left(y^z\right)}$$

en

$$z - (y - x) \neq (z - y) - x .$$

Een andere belangrijke eigenschap die een binaire operatie al of niet kan bezitten is de commutatieve eigenschap.

Definitie 4. Zij * een binaire operatie in X. De operatie * heet commutatief indien, voor willekeurige $x,y \in X$:

$$x * y = y * x .$$

Voorbeelden.

De operaties in de voorbeelden d), g), h), j) zijn commutatief; de operaties in e), f), i), k) zijn zulks niet.

Definitie 5. Zij * een binaire operatie in X. Een element e van X heet een neutraal element t.o.v. * indien voor iedere $x \in X$ geldt:

$$x * e = e * x = x .$$

Voorbeelden.

In voorbeeld d) is 1 een neutraal element t.o.v. . . Evenzo is in voorbeeld h) het getal 1 een neutraal element t.o.v. kleinste gemene veelvoud. In j) is de lege verzameling $\emptyset$ een neutraal element t.o.v. $\cup$.

Voor de operaties in de voorbeelden e), f), g), i) en k) bestaat geen neutraal element.

Voorbeeld.

1) (deelstelsel van g)). Y is de verzameling van alle rationale getallen $\leq \frac{97}{113}$; $x * y = \min(x,y)$.

In dit geval is er een neutraal element t.o.v. * , nl. $\frac{97}{113}$.

Stelling 1. Zij * een binaire operatie in een verzameling X. Dan bezit X ten hoogste één neutraal element t.o.v. * .

M.a.w.: Als er een neutraal element bestaat t.o.v. * , dan is dit ondubbelzinnig bepaald.

Bewijs van stelling 1. Stel zowel e_1 als e_2 is een neutraal element t.o.v. *. Voor willekeurige $x \in X$ en $y \in X$ geldt dan:

$$e_1 x = x \quad , \qquad y e_2 = y \ .$$

Nemen we i.h.b. $x = e_2$ en $y = e_1$, dan vinden we:

$$e_1 e_2 = e_2 \quad , \quad e_1 e_2 = e_1 \ .$$

Er volgt dat $e_1 = e_2$.

We besluiten deze paragraaf met de invoering van een laatste begrip:

Definitie 6. Zij * een binaire operatie in een verzameling X, en stel X bevat een neutraal element e t.o.v. * . Een element $x \in X$ heet inverteerbaar indien er een $y \in X$ bestaat zodanig dat

$$x * y = y * x = e \ .$$

Voorbeelden.

In voorbeeld d) is een getal x inverteerbaar dan en slechts dan indien $x \neq 0$. In voorbeeld h) bestaat er weliswaar een neutraal element (nl. 1), maar behalve dit neutrale element zelf is geen enkel element inverteerbaar. Ook in j) is het neutrale element (hier $\emptyset$) het enige inverteerbare element.

Stelling 2. Zij * een associatieve binaire operatie in een verzameling X, en stel X bevat een neutraal element e t.o.v. *. Voor iedere $x \in X$ bestaat er ten hoogste één y zodanig dat

$$x * y = y * x = e .$$

Bewijs. Stel $x * y_1 = y_1 * x = e$ en $x * y_2 = y_2 * x = e$.
Dan is $y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2$.

Als * een associatieve binaire operatie is in X, met neutraal element e, en x is inverteerbaar, dan bestaat er dus precies één y zodanig dat $x * y = y * x = e$. Dit element y noemt men de inverse van x.

Voorbeeld.

In voorbeeld d) is de inverse van $x \neq 0$ het getal $\frac{1}{x}$.

§2. Groepen.

Definitie 1. Een groep is een verzameling G, voorzien van een binaire operatie *, met de volgende eigenschappen:

(1) * is associatief; m.a.w. $x * (y * z) = (x * y) * z$, voor alle $x,y,z \in G$.

(2) G bevat een neutraal element t.o.v. * ; m.a.w. er bestaat een $e \in G$ zodanig dat $x * e = e * x = x$ voor alle $x \in G$.

(3) Ieder element van G is inverteerbaar; m.a.w. voor iedere $x \in G$ is er een $y \in G$ zodanig dat $x * y = y * x = e$.

Voorbeelden.

a) G is de verzameling der reële getallen, * is de normale optelling: $x * y = x + y$.

Het neutrale element is 0; de inverse van x is $-x$.

Deze groep zullen we voortaan aangeven met $(R,+)$.

b) G is de verzameling der rationale getallen; * is de normale optelling.

Deze groep zullen we voortaan aangeven met $(Q,+)$.

c) G is de verzameling der gehele getallen; * is de normale optelling.

Deze groep zullen we voortaan aangeven met $(Z,+)$.

d) G is de verzameling der reële getallen $\neq 0$; * is de normale vermenigvuldiging: $x * y = x \cdot y$.

Het neutrale element is 1; de inverse van x is x^{-1}.

Voor deze groep schrijven we in het vervolg $(R',.)$. Op analoge wijze wordt de multiplicatieve groep $(Q',.)$ van alle rationale getallen $\neq 0$ gedefinieerd.

e) G is de verzameling van alle deelverzamelingen van het platte vlak; de operatie * voegt aan twee deelverzamelingen x en y toe hun symmetrisch verschil, d.w.z. $x * y$ is de verzameling van alle punten van het vlak die hetzij tot x, hetzij tot y, maar niet tot beide behoren.

(Het neutrale element is de lege verzameling $\emptyset$; de inverse van x is x zelf).

f) Zij $q \in R$, $q > 0$. In R definiëren we een binaire operatie $+_q$ aldus: als $x \in R$, $y \in R$, dan zij $x +_q y$ het getal t zodanig dat $t \in R_q = [0,q) = \{u: 0 \leq u < q\}$ terwijl voorts $x + y \equiv t \pmod q$ (met $a \equiv b \pmod q$ wordt altijd bedoeld $\frac{a-b}{q} \in Z$). Men kan nagaan dat $(R_q,+_q)$ een groep is.

g) Wanneer men in f) overal de verzameling R vervangt door de verzameling Q der rationale getallen, dan verkrijgt men groepen $(Q_q,+_q)$ die evenals de groepen $(R_q,+_q)$ uit f) oneindig zijn. Vervangt men echter in f) overal R door Z, dan verkrijgt men de bekende restgroepen modulo q (q is nu een natuurlijk getal!). Deze groepen $(Z_q,+_q)$ zijn alle eindig!

h) Zij T de verzameling van alle complexe getallen z met $|z| = 1$ en zij . de gebruikelijke vermenigvuldiging van complexe getallen. Dan is $(T,.)$ een groep.

i) Verschillende deelstelsels van T zijn ook groepen. Zij bijv.

$C_n = \{1, e^{\frac{2\pi i}{n}}, e^{\frac{2 \cdot 2\pi i}{n}}, \ldots, e^{\frac{(n-1)2\pi i}{n}}\}$ (n een natuurlijk getal).

Iedere $(C_n, .)$ is een groep.

j) De groepen $(C_n, .)$ uit voorbeeld h) zijn eindige groepen.

Een eindige groep wordt dikwijls gedefinieerd door de elementen expliciet neer te schrijven en de groepsoperatie door een tabel (vermenigvuldigingstafel) vast te leggen. Zo is de vermenigvuldiging in C_4 e.g. vastgelegd door de volgende tafel (kortheidshalve schrijven we a voor $e^{\frac{\pi i}{2}}$, b voor $e^{\pi i}$ en c voor $e^{\frac{3\pi i}{2}}$):

.	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

De rij en kolom buiten de dubbele strepen laat men daarbij dikwijls weg (ze worden toch binnen de tabel gereproduceerd).

Een andere groep met 4 elementen is de zg. viergroep van Klein $(V, .)$, waar $V = (\varepsilon, \alpha, \beta, \gamma)$ ($\varepsilon, \alpha, \beta, \gamma$ zijn vier onderling verschillende maar overigens willekeurige elementen), terwijl de groepsoperatie gedefinieerd is door de tafel

ε	α	β	γ
α	ε	γ	β
β	γ	ε	α
γ	β	α	ε

k) Een andere eindige groep is de groep $(G,*)$, met $G = \{e,p,q,r,s,t\}$ en vermenigvuldigingstafel

e	p	q	r	s	t
p	e	r	q	t	s
s	r	e	t	q	p
r	s	t	e	p	q
q	t	s	p	e	r
t	q	p	s	r	e

l) Zij G de verzameling der imaginaire getallen (d.w.z. de complexe getallen $z = x + iy$, x en y reëel, met $y \neq 0$), en zij $*$ de aldus gedefinieerde binaire operatie in G:

$$z * w = \mathrm{Re}(z) + w.\mathrm{Im}(z) = x + wy .$$

Dan is $(G,*)$ een groep (met i als neutraal element).

m) Zij G de verzameling van alle permutaties van een zekere verzameling X; als $f \in G$ en $g \in G$, dan zij $f \circ g$ die permutatie van X die aan $x \in X$ toevoegt $f(g(x))$. Dan is $(G,\circ)$ een groep. (Een permutatie van een verzameling X is een één-éénduidige afbeelding van X op zichzelf).

Opmerking. Als X een eindige verzameling is, zeg met n elementen, dan geeft men een permutatie f van X dikwijls weer in de vorm van een matrix met twee rijen en n kolommen; in de eerste rij rangschikt men de elementen van X, en onder ieder element noteert men zijn f-beeld:

$$\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ f(x_1) & f(x_2) & f(x_3) & \dots & f(x_n) \end{pmatrix} .$$

Opgave 1. Ga na dat de groepen, aangegeven in de voorbeelden a) t/m m), inderdaad voldoen aan de eisen van definitie 1. Ga voor elk dezer groepen na wat het neutrale element is, en wat de inverse is van een willekeurig element x.

Het is gebruikelijk de binaire operatie * van een groep (G,*) de groepsvermenigvuldiging te noemen, en deze ook als een vermenigvuldiging te schrijven, i.e. x.y of xy te schrijven i.p v. x * y In dit verband noemt men het neutrale element van de groep meestal het eenheidselement. De inverse van een element x noteerst men dan met x^{-1}.

Een uitzondering op deze gebruiken maakt men bij vele commutatieve groepen.

Definitie 2. Een groep (G,*) heet commutatief of abels als de groepsoperatie * commutatief is.

Opgave 2. Ga na welke van de groepen in a) t/m m) commutatief zijn, en welke niet.

In een commutatieve groep wordt de groepsoperatie * vaak weergegeven met + (ook al is het niet de "normale" optelling van getallen); het neutrale element van G noemt men dan het nulelement van G; voor de inverse van $x \in G$ schrijft men $-x$.
N.B. Voor abelse groepen wordt dikwijls de multiplicatieve notatie gebruikt; voor niet-commutatieve groepen gebruikt men echter nimmer de additieve notatie. M.a.w. het is een conventie slechts dan een groepsoperatie aan te geven met + , wanneer deze groepsoperatie commutatief is.

Opgaven.

3. Zij X = {1,2,3,4}. Bewijs dat de permutaties

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

een groep vormen, en stel de vermenigvuldigingstafel op.

4. Stel de vermenigvuldigingstafel op van de groep van alle permutaties van de verzameling {1,2,3}. Evenzo de additietafel van $(Z_6,+_6)$ (zie voorbeeld g)).

5. Onder het complement van x verstaan we 1-x.
Beschouw nu de volgende instructies:

c = neem het complement van ... ;
r = neem de reciproke van ... ;
t = neem het tegengestelde van ... ;
e = doe niets met ... ;
cert = neem het tegengesteldevan een object; neem de reciproke van het resultaat, pauzeer nu even; neem tenslotte het complement van wat ge reeds verkregen had.

Ieder woord uit de letters c, r, t en e stelt, zodoende, een operator v or. Ond r het produkt van twee woorden w_1 en w_2 , in deze volgorde, verstaan w het woord w_1w_2. Dus tec.cert - teccert.

A) Te bewijzen: tt = rr = cc = e; tr = rt; crc = rcr, teccert = r.

B) Bewijs dat e, r, t en rt een abelse groep vormen. Bewijs dat ieder woord uit de letters e, r en t gelijk is aan een der vier elementen van die groep.

C) Bewijs dat e, r, c, rc, cr en rcr een niet-abelse groep vormen (en dat het "woordenboek op deze drie letters" uitsluitend deze zes operatoren bevat).

D) Bewijs dat e, t, c, tc, ct, tct, ctc, tctc, ctct, ... enz.
een oneindige groep vormen, met als abelse ondergroep de verzameling
e, tc, ct, tctc, ctct, tctctc, ctctct, ...

E) De onder C) gevonden groep wordt "de harmonische groep" genoemd.
Welke zes functies ontstaan wanneer men de operaties van de harmonische groep toepast op de functie $\sin^2 x$? Welke zes dubbelverhoudingen ontstaan, wanneer men een dubbelverhouding (ABCD) tot uitgangs-object neemt?

§3. Eigenschappen van groepen

Zij (G,.) een groep met eenheidselement e. De inverse van een element x zullen wij noteren met x^{-1}.
In (G,.) gelden de volgende eigenschappen:

1) Voor ieder tweetal elementen a en b van G zijn de vergelijkingen
   $a.x = b$ en $y.a = b$ éénduidig oplosbaar

Bewijs. Zij a^{-1} de inverse van a, dan zijn $x = a^{-1}.b$ en $y = b.a^{-1}$ oplossingen van de vergelijkingen.
Dit zijn ook de enige oplossingen, daar uit $a.x = b$ volgt
$a^{-1}.(a.x) = a^{-1}.b \Rightarrow (a^{-1}.a).x = a^{-1}.b \Rightarrow e.x = a^{-1}.b \Rightarrow x = a^{-1}.b.$
Evenzo volgt uit $y.a = b$, $(y.a).a^{-1} = b.a^{-1} \Rightarrow y.(a.a^{-1}) = b.a^{-1}$
$\Rightarrow y.e = b.a^{-1} \Rightarrow y = b.a^{-1}$.

Gevolg 1. Het bovenstaande impliceert dat als $a.x = a.y$ dan is $x = y$,
en uit $x.a = y.a$ volgt ook dat $x = y$.
Gevolg 2. Als a een element is van G met $a.a = a$, dan is $a = e$.

Opgave 1.
Zij G een verzameling met een associatieve binaire operatie . zó dat de vergelijkingen $a.x = b$ en $y.a = b$ oplosbaar zijn voor alle $a,b \in G$.
Dan is (G,.) een groep.

2) Voor ieder tweetal elementen a en b van G geldt
   $(a^{-1})^{-1} = a$
   $(a.b)^{-1} = b^{-1}.a^{-1}$.

Bewijs. Uit $a^{-1}.a = a.a^{-1} = e$ volgt $(a^{-1})^{-1} = a$ (§1. St. 2).
Verder is $(b^{-1}.a^{-1}).(a.b) = b^{-1}.(a^{-1}.a.b) = b^{-1}.b = e$ en
$(a.b).(b^{-1}.a^{-1}) = (a.b.b^{-1}).a^{-1} = a.a^{-1} = e$.
Hieruit volgt dat $(a.b)^{-1} = b^{-1}.a^{-1}$.

3) Zij a een willekeurig element van de groep (G,.) en λ_a de afbeelding van G in G die aan een element $x \in G$ het element a.x toevoegt. Dan is λ_a een 1-1 duidige afbeelding van G op zichzelf.

Bewijs. Stel $\lambda_a(x) = \lambda_a(y)$. Dan is a.x = a.y en dus x = y (gevolg 1, eigenschap 1).
De afbeelding λ_a is dus 1-1 duidig.
We bewijzen nu dat λ_a een afbeelding op G is, d.w.z. ieder element y uit G komt inderdaad als beeld voor.
Immers stel $x = a^{-1}.y$, dan is $\lambda_a(x) = a.a^{-1}.y = y$.

Opmerking 1. Zij (G,) een groep en $a \in G$. Stel $aG = \{ a.x \mid x \in G \}$.
Uit eigenschap 3) volgt dan dat aG = G voor iedere $a \in G$.

Definitie 1. Zij (G,.) een groep met eenheidselement e.
Wij definiëren nu door inductie:

$$\left.\begin{array}{l} a^0 = e \\ a^n = (a^{n-1}).a \\ a^{-n} = (a^{-1})^n . \end{array}\right\} \quad n \text{ natuurlijk getal}$$

Bewijs zelf de volgende stelling.

Stelling 1. Zij $a,b \in G$, dan geldt

$$\left.\begin{array}{l} a^n.a^m = a^{n+m} \\ (a^n)^m = a^{n.m} \\ (a\,b)^n = a^n.b^n \qquad \text{als } a.b = b.a \end{array}\right\} \quad n,m \text{ geheel} .$$

Opmerking 2. Indien men in een groep G de additieve notatie + gebruikt, schrijft men n a inplaats van a^n.
Stelling 1 krijgt dan de volgende vorm.

Stelling 1'. Voor ieder tweetal elementen a en b van (G,+) geldt

$$\left.\begin{aligned} &n\,a + m.a = (n+m)a \\ &m(n\,a) = (m.n)a \\ &n(a+b) = n\,a + n\,b \end{aligned}\right\} \quad n,m \text{ geheel.}$$

Definitie 2. Zij $(G,.)$ een groep met eenheidselement e. Het kleinste natuurlijke getal n met $a^n = e$ heet de orde van a, $a \in G$.
Notatie: $\sigma(a) = n$.
Als er geen natuurlijk getal n is met $a^n = e$, dan heet de orde van a oneindig: $\sigma(a) = \infty$.

Er geldt: $\sigma(e) = 1$, en: als $a \neq e$, dan $\sigma(a) > 1$.

§ 4. Homomorphismen en isomorphismen

Definitie 1. Een homomorphisme van een groep $(G,*)$ in een groep $(H,\odot)$ is een afbeelding φ van G in H met de volgende eigenschap:

$$\varphi(x * y) = \varphi(x) \odot \varphi(y) \tag{1}$$

voor alle $x,y \in G$.

Indien bovendien ieder element van H optreedt als beeld van tenminste één element van G (kortweg: als $\varphi(G) = H$), dan heet φ een homomorphisme van $(G,*)$ op $(H,\odot)$. In dit geval heet de groep $(H,\odot)$ een homomorph beeld van de groep $(G,*)$.

Voorbeelden.
a) De additieve groep $(R,+)$ der reële getallen (vb. 2a) kan homomorph worden afgebeeld op de multiplicatieve groep $(T,.)$ der complexe getallen z met $|z| = 1$ (vb. 2h). Een homomorphisme van $(R,+)$ op $(T,\cdot)$ is bijvoorbeeld de afbeelding φ, gedefinieerd door

$$\varphi(x) = e^{2\pi i x} \qquad (x \in R) \tag{2}$$

b) De groep $(R,+)$ kan homomorph worden afgebeeld in $(R',.)$ (vb. 2d); een homomorphisme van $(R,+)$ in $(R',\cdot)$ is bijv. de afbeelding φ met

$$\varphi(x) = e^x \qquad (x \in R). \tag{3}$$

N.B. φ is een homomorphisme<u>in</u> $(R',\cdot)$, maar niet een homomorphisme <u>op</u> $(R',\cdot)$ (vgl. opgave 3).

c) Zij R'' de verzameling van alle positieve reële getallen. Dan is $(R'',\cdot)$ een groep, en deze groep is een homomorph beeld van de groep $(R,+)$ (de afbeelding φ uit vb. b) is een homomorphisme van $(R,+)$ op $(R'',\cdot)$).

d) Iedere groep $(R_q,+_q)$ $(q>0$; zie vb. 2f) is een homomorph beeld van $(R,+)$; een homomorphisme van $(R,+)$ op $(R_q,+_q)$ wordt gegeven door de afbeelding φ_q, die aan $x \in R$ toevoegt dat getal $y \in R_q$, waarvoor geldt: $x \equiv y \pmod q$.

e) Zij $q > 0$, en zij ψ_q de volgende afbeelding $R_q \to T$:

$$\psi_q(x) = e^{\frac{2\pi i x}{q}} \qquad (x \in R_q). \tag{4}$$

Dan is ψ_q een homomorphisme van $(R_q,+_q)$ op $(T,\cdot)$.

f) Zij n een natuurlijk getal. De groep $(Z_n,+_n)$ (vb. 2g) kan homomorph worden afgebeeld op de groep $(C_n,\cdot)$ (vb. 2i), en omgekeerd.

Verzamelingentheoretisch intermezzo. Stel f is een afbeelding van een verzameling A in een verzameling B, g een afbeelding van B in een verzameling C. De samengestelde afbeelding van A in C die aan $a \in A$ toevoegt $g(f(a)) \in C$, wordt aangegeven met $g \circ f$. Indien f zowel 1-1-duidig is als een afbeelding van A op B, dan is f ondubbelzinnig omkeerbaar; voor de omkeerafbeelding schrijven we f^{-1}.

Stelling 1. Zij φ een homomorphisme van $(G,*)$ in $(H,\odot)$, en ψ een homomorphisme van $(H,\odot)$ in (K,Δ). Dan is $\psi \circ \varphi$ een homomorphisme van $(G,*)$ in (K,Δ).

Bewijs. Voor willekeurige $x,y \in G$ geldt:

$$(\psi \circ \varphi)(x * y) = \psi(\varphi(x * y) = \psi(\varphi(x) \odot \varphi(y)) = \psi(\varphi(x)) \Delta \psi(\varphi(y)) =$$
$$= (\psi \circ \varphi)(x) \Delta (\psi \circ \varphi)(y).$$

Voorbeeld.

g) Het homomorphisme van $(R,+)$ in $(T,\cdot)$, gedefinieerd in voorbeeld a), is de compositie van het homomorphisme $\varphi_1 : R \to R_1$ uit vb. d) en het homomorphisme $\psi_1 : R_1 \to T$ uit vb. e).

Stelling 2. Zij φ een homomorphisme van $(G,*)$ op $(H,\odot)$. Indien φ 1-1-duidig is, dan is φ^{-1} een homomorphisme van $(H,\odot)$ op $(G,*)$.

Bewijs. Stel $u,v \in H$; zij $x = \varphi^{-1}(u)$, $y = \varphi^{-1}(v)$. We moeten aantonen: $\varphi^{-1}(u \odot v) = x * y$. Inderdaad, daar φ een homomorphisme is geldt

$$\varphi(x * y) = \varphi(x) \odot \varphi(y) = u \odot v,$$

waaruit het gestelde volgt.

Definitie. Een 1-1-duidig homomorphisme van een groep $(G,*)$ in (op) een groep $(H,\odot)$ heet een isomorphisme van $(G,*)$ in (resp. op) $(H,\odot)$.

Twee groepen $(G,*)$ en $(H,\odot)$ heten isomorph indien er een isomorphisme van $(G,*)$ op $(H,\odot)$ bestaat.

Stelling 2 kan nu ook zo geformuleerd worden: als φ een isomorphisme is van $(G,*)$ op $(H,\odot)$, dan is φ^{-1} een homomorphisme (ja, zelfs een isomorphisme) van $(H,\odot)$ op $(G,*)$.

Isomorphe groepen beschouwt men binnen de algebra als "essentieel gelijk". Anders geformuleerd: slechts die eigenschappen van een groep $(G,*)$ zijn algebraisch belangrijk, die behouden blijven onder isomorphismen, die $(G,*)$ dus deelt met alle ermee isomorphe groepen.

Voorbeelden.

h) Het homomorphisme φ in voorbeeld b) is een isomorphisme van $(R,+)$ in $(R',\cdot)$. Het homomorphisme φ in voorbeeld c) is een isomorphisme van $(R,+)$ op $(R'',\cdot)$, met als invers isomorphisme φ^{-1} de afbeelding

$$\varphi^{-1}(u) = \log u \qquad (u \in R^{+}). \tag{5}$$

i) Voor ieder natuurlijk getal zijn de groepen $(Z_n,+_n)$ en $(C_n,\cdot)$ isomorph.

j) Zij $q \in R''$. De groepen $(R_q,+_q)$ en $(T,\cdot)$ zijn isomorph; de afbeelding ψ_q uit vb. e) is een isomorphisme van de eerste dezer groepen op de tweede, waarvan het inverse isomorphisme de vorm

$$\psi_q^{-1}(z) = \frac{q}{2\pi} \arg(z) \qquad (z \in T) \tag{6}$$

heeft (met arg(z) bedoelen we het argument van het complexe getal z, en wel met de conventie: $0 \leq \arg(z) < 2\pi$).

Als $f : A \to B$ en $g : B \to C$ beide 1-1-duidige afbeeldingen zijn, dan is ook $g \circ f : A \to C$ 1-1-duidig. Dit feit, tezamen met stelling 1, impliceert:

Stelling 2. Zij φ een isomorphisme van $(G,*)$ in $(H,\odot)$ en ψ een isomorphisme van $(H,\odot)$ in (K,Δ). Dan is $\psi \circ \varphi$ een isomorphisme van $(G,*)$ in (K,Δ).

Voorbeelden.

k) Stel p en q zijn positieve reële getallen. Daar ψ_p en ψ_q (gedefinieerd als in vb.e) isomorphismen van $(R_p,+_p)$ resp. $(R_q,+_q)$ op $(T,.)$ zijn, volgt dat $\psi_q^{-1} \circ \psi_p$ een isomorphisme van $(R_p,+_p)$ op $(R_q,+_q)$ is (voor ψ_q^{-1} zie ook vb. j). Alle groepen $(R_q,+_q)$, $q > 0$, zijn dus onderling isomorph. (De afbeelding $\psi_q^{-1} \circ \psi_p$ heeft een zeer eenvoudige vorm:

$$(\psi_q^{-1} \circ \psi_p)(x) = \frac{q}{p}\,x, \tag{7}$$

voor willekeurige $x \in R_p$).

l) Alle groepen $(Q_r,+_r)$ (r positief rationaal) zijn isomorph (vgl. vb. k).

N.B. Twee verschillende groepen $(Z_n,+_n)$, $(Z_m,+_m)$ (n,m natuurlijke getallen, $n \neq m$) zijn nooit isomorph!

Stelling 3. Stel $(G,*)$ en $(H,\odot)$ zijn groepen; zij e het neutrale element van $(G,*)$, e' het neutrale element van $(H,\odot)$, en zij zowel in $(G,*)$ als in $(H,\odot)$ de inverse van een element x aangegeven met x^{-1}. Indien φ een homomorphisme is van G in H, dan is

$$\varphi(e) = e';$$
$$\varphi(x^{-1}) = (\varphi(x))^{-1}, \text{ voor alle } x \in G.$$

Bewijs. Uit $e * e = e$ volgt $\varphi(e) \odot \varphi(e) = \varphi(e) = \varphi(e) \odot e'$; dus $\varphi(e) = e'$ (vgl. § 3, gevolg 2). Uit $x * x^{-1} = x^{-1} * x = e$ volgt voorts dat $\varphi(x) \odot \varphi(x^{-1}) = \varphi(x^{-1}) \odot \varphi(x) = \varphi(e) = e'$. Dit betekent

dat $\varphi(x^{-1})$ de inverse is van $\varphi(x)$ in $(H,\odot)$ (vgl. § 1 stelling 2).

Definitie 3. Zij $(G,*)$ een groep. Een endomorphisme van $(G,*)$ is een homomorphisme van $(G,*)$ in zichzelf. Een automorphisme van $(G,*)$ is een isomorphisme van $(G,*)$ op zichzelf.

Voorbeelden.

m) Zij q een reëel getal. De afbeelding $\omega_q : R \to R$ die $x \in R$ afbeeldt op $q.x$ is een endomorphisme van $(R,+)$. Als $q \neq 0$ is ω_q zelfs een isomorphisme van $(R,+)$ in zichzelf; ω_q is echter slechts een automorphisme indien $q = 1$.

n) E enzo is de op analoge wijze gedefinieerde afbeelding $\omega_r : Q \to Q$, r rationaal, een n'om rphisme van $(Q,+)$, terwijl voor gehele n de afbeelding ω_n met $\omega_n(x) = nx$ een endomorphisme is van $(Z,+)$.

) Zij $(Im,*)$ de groep uit vb. 21. De afbeelding φ met

(8) $$\varphi(z) = i.Im(z)$$

is een endomorphisme van $(Im,*)$.

Notatie. De verzameling van alle endomorphismen van een groep $(G,*)$ geven we aan met $\mathcal{E}(G,*)$; voor de verzameling van alle automorphismen van $(G,*)$ schrijven we $\mathcal{A}(G,*)$.

Binnen $\mathcal{E}(G,*)$ is de afbeeldings-compositie $\circ$ een associatieve binaire operatie. Deze operatie is i.h.a. niet commutatief (vgl. stelling 5 hieronder). Wel is er een neutraal element t.o.v. $\circ$, nl. de identieke afbeelding ε : $\varepsilon(x) = x$, voor alle $x \in G$. Als G meer dan één element bezit is niet ieder endomorphisme inverteerbaar in de zin van de binaire operatie $\circ$ in $\mathcal{E}(G,*)$; het endomorphisme $\varphi \in \mathcal{E}(G,*)$ is nl. dan en slechts dan inverteerbaar t.o.v. $\circ$, als φ een ondubbelzinnig omkeerbare afbeelding is in de gebruikelijke zin, d.w.z. als φ 1-1-duidig is en bovendien G op zichzelf afbeeldt (GA DIT NA!). Anders gezegd: de inverteerbare elementen in $\mathcal{E}(G,*)$ zijn juist de automorphismen van G.

Stelling 4. Zij $(G,*)$ een groep. Dan is ook $(\mathcal{A}(G,*), \circ)$ een groep.

Bewijs. We merkten reeds op dat $\circ$ associatief is. De identieke afbeelding ε van G is een automorphisme, dus $(\mathcal{A}, \circ)$ heeft een neutraal element. Als φ een automorphisme is van (G,*), dan ook φ^{-1}, dus ook aan het derde postulaat uit de definitie van een groep (§ 2 def.1) is voldaan.

Interessante en belangrijke voorbeelden van automorphismen zijn de zog. inwendige automorphismen. Zij (G,*) een groep. Als $a \in G$, dan schrijven we τ_a voor de volgende afbeelding $G \to G$:

$$\tau_a(x) = a * x * a^{-1} \qquad (x \in G).$$

Bewering: τ_a is een automorphisme van G.
Bewijs. Voor willekeurige $x,y \in G$ geldt (we schrijven weer e voor het neutrale element van G):

$$\tau_a(x*y) = a*x*y*a^{-1} = a*x*e*y*a^{-1} = a*x*(a^{-1}*a)*y*a^{-1} =$$
$$= (a*x*a^{-1}) * (a*y*a^{-1}) = \tau_a(x) * \tau_a(y).$$

Derhalve is τ_a een endomorphisme. En τ_a is omkeerbaar, dus een automorphisme (vgl. opgave 1), want de werking van τ_a wordt ongedaan gemaakt door $\tau_{a^{-1}} : \tau_{a^{-1}} \circ \tau_a = \varepsilon$.

De automorphismen van (G,*) van de vorm $\tau_a, a \in G$, noemt men de inwendige automorphismen van (G,*). De verzameling van alle inwendige automorphismen van (G,*) zullen we aangeven met $\mathcal{J}(G,*)$.

Opmerking. Het kan gebeuren dat $\tau_a = \tau_b$, terwijl $a \neq b$. Ingeval (G,*) commutatief is valt zelfs ieder inwendig automorphisme τ_a samen met de identieke afbeelding ε.

Stelling 5. De toevoeging $\varphi : a \to \tau_a$ is een homomorphisme van (G,*) op $(\mathcal{J}(G,*), \circ)$.
Bewijs. Daar $\varphi(a * b) = \tau_{a*b}$, moeten we aantonen dat $\tau_{a*b} = \tau_a \circ \tau_b$, ofwel dat $\tau_{a*b}(x) = (\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x))$ voor alle $x \in G$. Inderdaad is

$$\tau_{a*b}(x) = (a*b)*x*(a*b)^{-1} = a*b*x*b^{-1}*a^{-1} =$$
$$= a*(b*x*b^{-1})*a^{-1} = a*(\tau_b(x))*a^{-1} = \tau_a(\tau_b(x)).$$

Opgaven.

1. Stel X en Y zijn verzamelingen; f : X → Y zij een afbeelding die een omkeerfunctie g : Y → X heeft (d.w.z. g(f(x)) = x voor alle x ∈ X en f(g(y)) = y voor alle y ∈ Y).
   Bewijs dat f 1-1-duidig is, en dat fX = Y (d.w.z. f is een afbeelding van X op Y).

2. Bewijs dat de permutatiegroep uit § 2 opg.3 isomorph is met de viergroep van Klein (vb. 2j). Evenzo dat de harmonische groep (§2opg.5c) isomorph is met de groep in vb. 2k.

3. Bewijs dat de viergroep van Klein en de groep C_4 niet isomorph zijn. Evenzo dat de harmonische groep en C_6 niet isomorph zijn.

4. Bewijs dat er geen homomorphisme van (R,+) op (R',.) bestaat. Hieruit volgt dat (R,+) en (R',.) niet isomorph zijn.

5. Bewijs dat iedere groep die isomorph is met een abelse groep zelf abels is.

6. Ga na welke van de groepen in de voorbeelden uit § 2 isomorph kunnen worden afgebeeld in de groep $(\mathfrak{M}_m,*)$ uit voorbeeld 21.

7. Bepaal alle endomorphismen van (Z,+). Evenzo alle automorphismen en alle inwendige automorphismen. Volgens stelling 6 is $(\mathfrak{I}(Z,+),\circ)$ een homomorph beeld van (Z,+); is het ook een isomorph beeld?

8. Zij (G,*) de groep uit vb. 2k. Beschrijf de groep $(\mathfrak{A}(G,*),\circ)$.

9. Bewijs dat de binaire operatie $\circ$ in $\mathfrak{E}(G,*)$ niet commutatief is zodra de groep (G,*) niet commutatief is.
   Is het omgekeerde ook waar, m.a.w. volgt uit het abels zijn van (G,*) noodzakelijk dat $\circ$ in $\mathfrak{E}(G,*)$ commutatief is?
   (Aanwijzing: neem voor (G,*) de viergroep van Klein).

10. Is de afbeelding φ, gedefinieerd door (2)(vb.a) het enige isomorphisme van (R,+) op (T,.)?

11. Is de afbeelding $\psi_q^{-1} \circ \psi_p$ (zie formule 7, vb. k) het enige isomorphisme van $(R_p,+_p)$ op $(R_q,+_q)$?
Bestaan er homomorphismen van $(R_p,+_p)$ op $(R_q,+_q)$ die geen isomorphismen zijn?

12. Bestaan er endomorphismen van (R,+) die geen automorphismen zijn?

13. Stel n en m zijn natuurlijke getallen.
A. Als er een homomorphisme van $(Z_n,+_n)$ op $(Z_m,+_m)$ bestaat, dan is m een deler van n.
B. Als er een isomorphisme van $(Z_n,+_n)$ in $(Z_m,+_m)$ bestaat, dan is n een deler van m.

14. Zij (G,*) een groep. Als $a \in G$, dan zij ρ_a de afbeelding $G \to G$ gedefinieerd door

$$\rho_a(x) = x * a \qquad (x \in G)$$

(de rechts-translaties in G)
A. Bewijs dat iedere ρ_a een 1-1-duidige afbeelding van G op zichzelf is, dus een permutatie van G (vgl. vb.2m en § 3).
B. Zij $(\mathfrak{P}(G), \circ)$ de groep van alle permutaties van G. Bewijs dat de afbeelding $\varphi : a \to \lambda_a$ (vgl. § 3) een isomorphisme is van (G,*) in $(\mathfrak{P}(G), \circ)$.
(Hieruit volgt de stelling van CAYLEY: iedere groep is isomorph met een groep van permutaties.)
C. Bewijs dat de afbeelding ψ: $a \to \rho_a$ dan en slechts dan een isomorphisme is van (G,*) in $(\mathfrak{P}(G), \circ)$ indien (G,*) commutatief is.

15. Als X een verzameling is, dan schrijven we $\mathfrak{P}(X)$ voor de verzameling van alle deelverzamelingen van X. Voor het symmetrisch verschil van twee verzamelingen A en B schrijven we $A \Delta B$:

$$x \in A \Delta B \Leftrightarrow \text{òf } x \in A \text{ òf } x \in B \text{ (maar niet beide).}$$

Bewijs dat de groep $(\mathfrak{P}(X), \Delta)$ ingeval X uit twee elementen bestaat isomorph is met de viergroep van Klein.

16. Stel X en Y zijn verzamelingen. Bewijs de volgende stelling: Dan en slechts dan zijn $(\mathfrak{P}(X), \Delta)$ en $(\mathfrak{P}(Y), \Delta)$ isomorph, indien de verzamelingen X en Y gelijkmachtig zijn.

§ 5. Ondergroepen

Definitie 1. Een groep $(H, \odot)$ heet een ondergroep van een groep $(G,*)$ indien voldaan is aan de volgende twee voorwaarden:

1) H is een deelverzameling van G;

2) de identieke afbeelding $\varepsilon : H \to G$ ($\varepsilon(x) = x$, voor alle $x \in H$) is een isomorphisme van $(H, \odot)$ in $(G,*)$.

De tweede voorwaarde betekent dat $x \odot y = x * y$ voor alle $x,y \in H$. Om deze reden geeft men in een ondergroep de groepsoperatie aan met hetzelfde symbool als in de grote groep: men spreekt dus van de ondergroep $(H,*)$ van $(G,*)$.

Verzamelingentheoretisch intermezzo. Als $(H, \odot)$ een ondergroep is van $(G,*)$, dan kan men het verband tussen $\odot$ en $*$ exact weergeven door gebruik te maken van het begrip restrictie van een functie.

Als f een afbeelding is van A in B, en $A_o \subset A$, dan schrijven we $f \mid A_o$ voor de functie die slechts op A_o gedefinieerd is en daar samenvalt met f : $(f(A_o))(a) = f(a)$ voor alle $a \in A_o$; $f(A_o)$ heet de restrictie van f tot A_o. Het verband tussen $\odot$ en $*$ is nu als volgt:

$$(1) \qquad \odot = * \mid H \times H.$$

(N.B. $*$ is immers een afbeelding $G \times G \to G$, en $\odot$ een afbeelding $H \times H \to H$, vgl. § 1 def.2).

In het algemeen kan men, wanneer $*$ een binaire operatie is in een verzameling X, en $Y \subset X$, de functie $* \mid Y \times Y$ beschouwen. Deze afbeelding is dan en slechts dan een binaire operatie in Y indien uit $x,y \in Y$ volgt dat $x * y \in Y$.

Definitie 2. Zij $*$ een binaire operatie in een verzameling X. Een deelverzameling Y van X heet stabiel (voor $*$) indien uit $x \in Y$, $y \in Y$ volgt $x * y \in Y$.

Indien $(G,*)$ een groep is, en $(H,*)$ een ondergroep van G, dan is H stabiel. Maar niet iedere stabiele deelverzameling van G is een ondergroep.

Voorbeelden.

a) $(R'',\cdot)$ is een ondergroep van $(R',\cdot)$ (vgl. vb.3c en vb.2d). De verzameling N der natuurlijke getallen is stabiel in $(R',\cdot)$, maar $(N,\cdot)$ is geen groep en dus ook geen ondergroep van $(R',\cdot)$. In $(R,+)$ is R'' stabiel, maar $(R'',+)$ is geen ondergroep van $(R,+)$.

b) Zij $(G,*)$ een groep, en zij e het neutrale element. Dan is $(\{e\},*)$ een ondergroep van $(G,*)$. Voorts is $(G,*)$ een ondergroep van zichzelf.

c) Als m een natuurlijk getal is, dan zij mZ de verzameling van alle gehele getallen die deelbaar zijn door m: $mZ = \{ mk : k \in Z \}$. Voor iedere m is $(mZ,+)$ een ondergroep van $(Z,+)$.

d) Zij $(Im,*)$ de groep uit vb. 21. Zij H de verzameling van alle zuiver imaginaire getallen yi (y reëel, $y \neq 0$); $(H,*)$ is een ondergroep van $(Im,*)$ die isomorph is met $(R',\cdot)$. Zij verder K de verzameling van alle $z \in Im$ van de vorm $z = x+i$; x reëel; $(K,*)$ is een ondergroep van $(Im,*)$ die isomorph is met $(R,+)$.

e) Stel X en Y zijn verzamelingen en $Y \subset X$. Dan is $(\mathcal{P}(Y), \Delta)$ een ondergroep van $(\mathcal{P}(X), \Delta)$ (voor de notatie zie § 4 opgave 14).

In het vervolg zullen we meestal bij het spreken over een groep $(G,*)$ de vermelding van de operatie $*$ achterwege laten; we spreken dus kortweg over de groep G (behalve op plaatsen waar dit tot verwarring zou kunnen leiden). Verder zullen we i.h.a. de groepsvermenigvuldiging multiplicatief schrijven.

Stelling 1. Zij G een groep, en zij H een niet-lege stabiele deelverzameling van G. Dan en slechts dan is H een ondergroep van G indien met $x \in H$ steeds ook x^{-1} tot H behoort.

Bewijs. Als H een ondergroep is van G geldt zeker: $x \in H \Rightarrow x^{-1} \in H$. Stel nu dat H een niet-lege stabiele deelverzameling is van G die aan deze voorwaarde voldoet. Zij $x \in H$; daar $x^{-1} \in H$ en daar H stabiel is moet $x.x^{-1} \in H$, d.w.z. $e \in H$. Nu volgt onmiddellijk dat H een groep is.

In de practijk geeft de volgende stelling een betere toets:

Stelling 2. Zij G een groep, en zij $\emptyset \neq H \subset G$ zodanig dat $x,y \in H \Rightarrow x.y^{-1} \in H$. Dan is H stabiel, en H is een groep (en dus een ondergroep van G).

Bewijs. Laat $x = y \in H$; er volgt dat $e = x \cdot y^{-1} \in H$. Zij nu x een willekeurig element in H; ook $e \cdot x^{-1} = x^{-1} \in H$. De stelling volgt nu uit stelling 1.

Stelli g 3. Zij φ een homomorphisme van G in H. Dan is φG een ondergroep van H.

Bewijs. Stel $u,v \in \varphi G$, zeg $u = \varphi(x)$, $v = \varphi(y)$, $x,y \in G$. Dan is $uv^{-1} = \varphi(x) \cdot \varphi(y)^{-1} = \varphi(x \cdot y^{-1}) \in \varphi G$. Pas nu stelling 2 toe.

Gevolg. Zij φ een endomorphisme van G, en zij H een ondergroep van G. Dan is ook φH een ondergroep van G.

Bewijs. $\varphi|H$ is een homomorphisme van H in G, en beeldt H af op φH. Volgens stelling 3 is dus φH een ondergroep van G.

Indien meer in het bijzonder φ een inwendig automorphisme τ_a is, dan heten H en $\tau_a H$ geconjugeerde ondergroepen van G.

Voorbeeld.

f) Zij G de groep uit vb. 2k, en zij $H = \{e,p\}$. Dan is H een ondergroep van G. Het inwendige automorphisme τ_s beeldt H af op $\{e,t\}$; $\{e,t\}$ is dus een met H geconjugeerde ondergroep van G. De enige andere met H geconjugeerde ondergroep van G is $\{e,r\}$.

Het kan voorkomen dat alle ondergroepen van een groep (G,*), die geconjugeerd zijn met de ondergroep H, samenvallen met H.

Voorbeelden.

g) Als G commutatief is, valt ieder inwendig automorphisme samen met de identieke afbeelding. Voor iedere ondergroep H van G zijn er dus geen andere geconjugeerde ondergroepen dan H zelf.

h) Zij G de groep uit vb. 2k, en zij $H = \{e,s,q\}$. Dan is H een ondergroep van G, en ieder inwendig automorphisme van G beeldt H in zichzelf af.

Ondergroepen met de juist besproken eigenschap blijken uiterst onderlijk belangrijk te zijn (zie § 5). Zij hebben daarom een eigen naam verworven:

Definitie 3. Een ondergroep H van een groep G heet normaal indien $\tau_a H = H$ voor ieder inwendig automorphisme τ_a van G.

Een normale ondergroep heet ook een normaaldeler (voor de reden zie § 6). De voorwaarde uit definitie 3 kan men ook als volgt formuleren: voor willekeurige $a,x \in G$ geldt: $x \in H \Rightarrow axa^{-1} \in H$. Of ook: $aHa^{-1} = H$ voor alle $a \in G$ (zie ook opgave).

Stelling 4. Zij φ een homomorphisme van G in H, en zij e' het neutrale element in H. Dan is $\varphi^{-1}(e')$ een ondergroep van G.
Bewijs. Stel $x \in \varphi^{-1}(e')$ en $y \in \varphi^{-1}(e')$; d.w.z. $\varphi(x) = \varphi(y) = e'$. Dan is $\varphi(x.y^{-1}) = \varphi(x).\varphi(y)^{-1} = e'.(e')^{-1} = e'$; dus ook $x.y^{-1} \in \varphi^{-1}(e')$. Pas nu stelling 2 toe.

Definitie 4. Zij φ een homomorphisme van G in H. De ondergroep $\varphi^{-1}(e')$ van G heet de kern van φ.
Notatie: $\varphi^{-1}(e') = \text{kern}(\varphi)$.

Stelling 5. Zij gegeven een stelsel ondergroepen H_α van een groep G (α doorloopt een index-verzameling A). Dan is ook $\bigcap_{\alpha \in A} H_\alpha$ een ondergroep van G.
Bewijs. Stel $x \in \bigcap_{\alpha \in A} H_\alpha$ en $y \in \bigcap_{\alpha \in A} H_\alpha$. Voor iedere $\alpha \in A$ behoren dan x en y tot H_α, en dus ook $x.y^{-1}$. Hieruit volgt weer dat $x.y^{-1} \in \bigcap_{\alpha \in A} H_\alpha$. M.b.v. stelling 2 volgt nu de bewering.

Opmerking. Als H_1 en H_2 ondergroepen zijn van G, dan is i.h.a. $H_1 \cup H_2$ niet stabiel en dus zeker geen ondergroep.

Voorbeeld.
i) 2Z en 3Z zijn beide ondergroepen van Z, maar $2Z \cup 3Z$ is niet stabiel.

Stelling 6. Zij G een groep, $A \subset G$ een willekeurige deelverzameling. Dan is er een kleinste ondergroep van G die A omvat. (Deze ondergroep noemt men de ondergroep van G, voortgebracht door A.)

Bewijs. Er zijn ondergroepen die A omvatten, bijv. G zelf. Zij nu H de doorsnede van a le ondergroepen die A omvatten. Volgens stelling 5 is H een groep; ook is $A \subset H$; H i dus de gezocht k einste onde- groep die A omvat.

Een andere karakterisering van de ondergroep, voortgebracht door een verzameling A, wordt gegeven in opgave . Een belangrijk bijzonder g val is de ondergroep voortgebracht door één element.

Ste ing 7. Zij G een groep. De ondergroep H voortgebracht door een element $\in$ G bes aat uit de elementen a^n, $n=0,\pm1,\pm2,\ldots$
Bewijs. Alle genoemde elementen moeten zeker behoren tot iedere onderg oep die a bevat. Anderzijds vormen ze zelf e n r GA DIT NA!)
Deze groep is dan no dzakel'jk de kl inst er r evat.

Opgav n.

1. Zij H een ondergroep van een groep G. Nodig en voldoende opdat H een normaaldel r zij van G is dat $aHa^{-1} \subset H$ voor iedere $a \in G$. Een andere nodige en voldoende voorwaarde is: $aH = Ha$ voor iedere $a \in G$. Bewij dit.

2. Zij G een groep, A een deelverzameling van G. De ondergroep H van G, voortgebracht door A, bestaat uit alle elementen x van G die te schrijven zijn als een eindig product

$$x = c_1 \cdot c_2 \cdot c_3 \cdot \ldots \cdot c_n,$$

waarbij voor iedere i, $1 \leq i \leq n$, hetzij $c_i \in A$ hetzij $c_i^{-1} \in A$.

3. Zij V het (a ithmetische) platte vlak, en zij Λ de verzameling van alle punten $x = (x_1, x_2) \in V$ met geh le coördi aten x_1, x_2 (het e n- heidsrooster in V).

A) Zij C de verzameling van alle congruente afbeeldingen van V in zichzelf; $(C, \circ)$ is een groep.

B) Zij D de verzameling van alle congruente afbeeldingen van V die de oorsprong, (0,0) op zijn plaats laten (alle rotaties van V om (0,0)). Ook $(D, \circ)$ is een groep; D is dus een ondergroep van C.

C) Zij E de verzameling van alle translaties van V, d.w.z. van al die congruente afbeeldingen φ van V in zichzelf waarbij de afstand tussen x en $\varphi(x)$ constant is, voor $x \in V$. Ook E is een ondergroep van C.

D) Zij C_o de verzameling van alle $\varphi \in C$ die Λ in zichzelf afbeelden. Bewijs dat C_o een ondergroep is van C. Dan volgt dat ook $D_o = D \cap C_o$ en $E_o = E \cap C_o$ ondergroepen zijn van C.

E) Bewijs dat iedere $\varphi \in C_o$ te schrijven is als een product

$$\varphi = \varphi_1 \circ \varphi_2 \circ \varphi_3$$

met $\varphi_1 \in E_o$, $\varphi_2 \in D_o$ en $\varphi_3 \in S$, waar S de groep der spiegelingen van V is: $S = \{\varepsilon, \sigma\}$ met $\varepsilon(x) = x$ voor alle x (de identieke afbeelding) en $\sigma x = -x$ voor alle x (de echte spiegeling).

4. Zij Im de groep gedefinieerd in vb. 21), en zij H de verzameling van alle $z \in Im$ met $Im(z) = 1$ (i.e. van alle $z = x+i$, x reëel). Dan is H een ondergroep van Im; H is isomorph met $(R,+)$.

5. Zij Im als in opg.4; zij K de verzameling van alle $z \in Im$ van de vorm $z = x \pm i$, x geheel. Dan is K een ondergroep van Im; K is isomorph met de grootste der twee groepen gedefinieerd in § 2 opgave 5D.

§ 6. Normaaldelers en factorgroepen

Definitie 1. Onder een equivalentierelatie R op een niet-lege verzameling X verstaan wij een deelverzameling R van $X \times X$ met de volgende eigenschappen:

1^o) $(a,a) \in R$ voor alle $a \in X$. (reflexiviteit)

2^o) $(a,b) \in R \Rightarrow (b,a) \in R$. (symmetrie)

3^o) $(a,b) \in R$ en $(b,c) \in R \Rightarrow (a,c) \in R$ (transitiviteit).

Als $(a,b) \in R$, dan zullen we vaak schrijven $a \sim b$ en zeggen "a is equivalent met b.

Heeft men een equivalentierelatie R op X, dan kan men de elementen van X in klassen indelen zó, dat twee elementen dan en slechts dan tot eenzelfde klasse behoren indien zij equivalent zijn.

Een equivalentierelatie op X geeft dus een verdeling van X in disjuncte klassen, waarbij equivalente elementen in dezelfde klasse liggen en niet equivalente elementen in verschillende klassen. Omgekeerd is door iedere verdeling van X in disjuncte klassen een equivalentierelatie op X bepaald. Immers, als wij definieren: $a \sim b$ dan en slechts dan als a en b in dezelfde klasse liggen, dan is "$\sim$" een equivalentierelatie.

Definitie 2. Zij H een ondergroep van een groep G en $x \in G$, dan noemt men de verzameling $x H = \{x h \mid h \in H\}$ een linker nevenklasse van H in G. Evenzo heet $H x = \{h x \mid h \in H\}$ een rechter nevenklasse.

Stelling 1. Zij H een ondergroep van een groep G en stel $x \sim y$ als $x \in y H$ $(x, y \in G)$. Dan is "$\sim$" een equivalentierelatie.

Bewijs

1^o) Daar $x = x e \in x H$ geldt $x \sim x$.

2^o) Als $x \sim y$, dan is $x = y h$, met $h \in H$.
Dus $x h^{-1} = y h h^{-1} = y$ en $y \in x H$, d.w.z. $y \sim x$.

3^o) Als $x \sim y$ en $y \sim z$, dan geldt
$x = y h_1$, $y = z h_2$ met $h_1, h_2 \in H$.
Dus $x = y h_1 = z h_2 h_1 \Rightarrow x \in z H \Rightarrow x \sim z$.

Iedere ondergroep H van G definieert dus een equivalentierelatie op G. Uit stelling 1 volgt dat G uiteenvalt in disjuncte linker nevenklassen x H van H.
Hierbij is x H = y H dan en slechts dan als $x \in y H$ i.e. als $x y^{-1} \in H$.
Daar H = e H is H zelf ook een linker nevenklasse van H.

Voorbeeld: Zij Z de additieve groep van de gehele getallen en m Z de verzameling van alle getallen, deelbaar door m: $m Z = \{ m k \mid k \in Z \}$
m Z is een ondergroep van Z .
Dan zijn de linker nevenklassen van m Z in Z de verzamelingen $n + m Z = \{ n + m k \mid k \in Z \}$. $n = 0,1,\ldots,m-1$.
Er zijn dus precies m verschillende nevenklassen.
Twee elementen x en y van Z liggen in dezelfde nevenklasse als $x = y + m k$, $k \in Z$, dus als $x \equiv y \pmod m$.

Opmerking 1: Als G commutatief is, dan vallen linker en rechter nevenklassen samen: x H = H x.
Als G niet commutatief is, dan is dit in het algemeen niet het geval. Kies b.v. voor G de groep gedefinieerd in § 2 opgave 5 C en voor H de ondergroep $\{ e,r \}$.
Dan is $c H = \{ c, cr \} \neq \{ c, rc \} = H c$.
De ondergroepen N van G met de eigenschap dat linker en rechter nevenklassen samen vallen, zijn juist de normaaldelers van G.
Immers uit § 5 opgave 1 volgt dat een nodige en voldoende voorwaarde opdat N een normaaldeler zij van G is dat x N = N x voor iedere $x \in G$.

Opmerking 2: Zijn a H en b H twee nevenklassen van H in G; dan kan men door middel van de afbeelding $a h \rightarrow b h$ de klasse a H 1-1-duidig afbeelden op b H.
Twee linker nevenklassen van H in G zijn dus gelijkmachtig; in het bijzonder geldt als H een eindige groep is, dat de nevenklassen a H en b H evenveel elementen bezitten.

Stelling 2: De afbeelding $f : g \to g^{-1}$, $g \in G$ is een 1-1-duidige afbeelding van G op G die de linker nevenklassen van H in G overvoert in de rechter nevenklassen.

Bewijs:
Daar $(x^{-1})^{-1} = x$ en $x^{-1} \neq y^{-1}$ als $x \neq y$ volgt dat f een 1-1-duidige afbeelding van G op G is.
Verder is $f(a\ h) = h^{-1}\ a^{-1} \in H\ a^{-1}$ en $h\ a^{-1} = f(a\ h^{-1})$.
De linker nevenklasse a H gaat dus over in de rechter nevenklasse $H\ a^{-1}$.

Definitie 3. Het aantal linker nevenklassen van H in G (eindig of oneindig) heet de index van H in G.
Notatie: $[G : H]$.
Uit stelling 2 volgt dat het aantal linker nevenklassen gelijk is aan het aantal rechter nevenklassen. De index van H in G is dus ook gelijk aan het aantal rechter nevenklassen van H in G.

Definitie 4. Het aantal elementen (eindig of oneindig) van een groep G heet de orde van G.
Notatie: $|G|$

Uit stelling 1 volgt onmiddellijk:
Stelling 3. (Lagrange)
Zij G een eindige groep en H een ondergroep van G.
Dan geldt
$$|G| = [G : H] \cdot |H|.$$
De index en de orde van een ondergroep zijn dus delers van de orde van de groep.

Voorbeeld
Zij S_n de groep van alle permutaties van n elementen $\{a_1, \ldots, a_n\}$.
Dan is $|S_n| = n!$ Stel dat S^*_{n-1} de ondergroep is van S_n, die bestaat uit alle permutaties die a_n invariant laten.
Dan is S^*_{n-1} isomorf met S_{n-1} de groep van alle permutaties van n-1 elementen $\{a_1, \ldots, a_{n-1}\}$. Dus $|S^*_{n-1}| = (n-1)!$

En uit de stelling van Lagrange volgt dat

$$\left[S_n : S^*_{n-1}\right] = \frac{n!}{(n-1)!} = n .$$

Stelling 4: Een ondergroep H van een groep G met index 2 is een normaaldeler van G.

Bewijs:
Als $x \in H$, dan $H x = H = x H$.
Als $x \notin H$ dan volgt uit $\left[G:H\right] = 2$ dat $G = H \cup x H = H \cup H x$.. Dus $x H = H x$.
Voor ieder element $x \in G$ geldt dus $x H = H x \Rightarrow H$ is een normaaldeler van G.

Definitie 5: Een equivalentierelatie gedefinieerd op een groep G heet een congruentie als uit $x \sim y$ en $u \sim v$ volgt $x u \sim y v$.
Notatie: $x \equiv y$.

Stelling 5: Zij N een normaaldeler van G. Dan is de equivalentierelatie op G gedefinieerd door N een congruentie.
Omgekeerd wordt iedere congruentie op G bepaald door een normaaldeler N.

Bewijs:
Zij "$\sim$" de equivalentierelatie op G gedefinieerd door N. Dan volgt uit $x \sim y$ en $u \sim v$ dat $x \in y N$ en $u \in v N$
Dus $x u \in y N v N = y v N N = y v N \Rightarrow x u \sim y v$.
Dus "$\sim$" is een congruentie.
Stel nu omgekeerd dat "$\equiv$" een congruentie is en stel $N = \left\{x \mid x \equiv e, x \in G\right\}$. (N is de congruentie klasse van e).
Dan is N een groep. Immers als $x \equiv e$ en $y \equiv e$, dan zal $x y \equiv e$; dus als $x,y \in N$ dan ook $x y \in N$.
Verder volgt uit $x \equiv e$ en $x^{-1} \equiv x^{-1}$ dat $x x^{-1} \equiv e x^{-1} \Rightarrow x^{-1} \equiv e$, dus als $x \in N$ dan ook $x^{-1} \in N$.
Uit § 5 st. 1 volgt dan dat N een groep is.
N is zelfs een normaaldeler, daar uit $x \in N$ volgt $x \equiv e$;
$g x g^{-1} \equiv g e g^{-1} = e$, dus $g x g^{-1} \in N$ i.e. $g N g^{-1} \subset N$.

De congruentie "$\equiv$" is verder geheel door N bepaald, daar
$x \equiv y \iff x\,y^{-1} \equiv e \iff x\,y^{-1} \in N \iff x \in y\,N$.

Opmerking

Uit stelling 5 volgt dat als "$\equiv$" een congruentie is op G, dan is er een normaaldeler N van G te vinden, zodat de congruentie klassen juist de nevenklassen van N in G zijn.

Stelling 6: Zij φ een homomorfisme van een groep G_1 op een groep G_2. Dan geldt als e_1 en e_2 resp. de neutrale elementen zijn van G_1 en G_2:
1^o) $N = \varphi^{-1}(e_2)$ is een normaaldeler van G_1;
2^o) $\varphi^{-1}(\varphi(a)) = N\,a$ voor alle $a \in G_1$;
3^o) φ is een isomorfie $\iff N = \{e_1\}$.

Bewijs:
1^o) Stel $x \equiv y$ als $\varphi(x) = \varphi(y)$ $x,y \in G_1$.
Dan is $\equiv$ een congruentierelatie op G_1.
Immers als $x \equiv y$ en $u \equiv v$, dan is $\varphi(x) = \varphi(y)$ en $\varphi(u) = \varphi(v)$
Dus $\varphi(x)\varphi(u) = \varphi(y)\varphi(v) \Rightarrow \varphi(xu) = \varphi(yv) \Rightarrow x\,u \equiv y\,v$.
Uit stelling 5 volgt dat de congruentie klasse N van e_1
$N = \{x \mid \varphi(x) = \varphi(e_1)\}$ een normaaldeler is van G_1.
Daar $\varphi(e_1) = e_2$ volgt dat $N = \varphi^{-1}(e_2)$.
2^o) Daar
$\varphi^{-1}(\varphi(a)) = \{x \mid \varphi(x) = \varphi(a)\} = \{x \mid x \equiv a\}$ is $\varphi^{-1}(\varphi(a))$ een nevenklasse van N, die a bevat. Dus $\varphi^{-1}(\varphi(a)) = N\,a$.
3^o) $\Rightarrow$: triviaal
$\Leftarrow$: Als $N = \{e_1\}$, dan volgt uit 2^o dat $\varphi^{-1}(\varphi(a)) = a \Rightarrow \varphi$ is een isomorfie.

Zij nu R een congruentie op een groep G en stel G/R de verzameling van alle congruentie klassen uit G.
Stel $A, B \in G/R$ en $a_1, a_2 \in A$; $b_1, b_2 \in B$.
Dan $a_1 \equiv a_2$ en $b_1 \equiv b_2 \Rightarrow a_1 b_1 \equiv a_2 b_2$.
Hieruit volgt dat de verzameling $A\,B = \{a\,b \mid a \in A,\ b \in B\}$, bevat is in de congruentie klasse C van G die $a_1 b_1$ bevat.
Wij definieren nu in G/R een operatie o op de volgende wijze

A o B = C, waarbij C de congruentie klasse is die A B bevat.
Met deze operatie o is G/R een groep, immers als N de congruentie klasse is die e bevat, dan is

$$A \circ N = A = N \circ A.$$

Verder geldt, als $a \in A$ en $a^{-1} \in A^*$, dat $A \circ A^* = N = A^* \circ A$.
Dus A^* is de inverse van A in G/R.

Zij nu φ de afbeelding van G op G/R gedefinieerd door $\varphi: a \to A$.
met $a \in A$.
Dan is φ een homomorfe afbeelding, daar uit $a \in A$ en $b \in B$ volgt
$ab \in A \circ B$, dus $\varphi(ab) = \varphi(a) \circ \varphi(b)$.
In het bijzonder krijgen wij, als wij voor R de congruentie nemen bepaald door een normaaldeler N van G, de volgende stelling

Stelling 7: Stel N een normaaldeler van G. Dan vormen de nevenklassen van N in G een groep, de factorgroep G/N.
De afbeelding φ_N van G op G/N met $\varphi_N(a) = Na$ is een homomorfe afbeelding met kern N.
φ_N heet het natuurlijke homomorfisme van G op G/N.

Stelling 8. (homomorfie-stelling)
Stel φ een homomorfe afbeelding van een groep G op een groep G_1, met kern N.
Dan is G/N isomorf met G_1.

Bewijs
Volgens stelling 6 is de afbeelding $f : Na \to \varphi(a)$ inderdaad een 1-1 duidige afbeelding van G/N op G_1.
Daar $a N \circ b N = ab N$ geldt

$$f(a N \circ b N) = \varphi(ab) = \varphi(a).\varphi(b) = f(aN).\ f(bN).$$

Dus f is een isomorfie.

Voorbeeld

1) De additieve groep R^+, der reële getallen kan homomorph worden afgebeeld op de multiplicatieve groep T der complexe getallen z met $|z| = 1$ door middel van het homomorfisme φ, gedefinieerd door

$$\varphi(x) = e^{2\pi i x}$$

De kern van φ is de additieve groep Z der gehele getallen, dus

R^+/Z is isomorf met T

2) Stel Z de additieve groep der gehele getallen en m Z de ondergroep van Z bestaande uit alle gehele veelvouden van m.
Dan is z/mZ isomorf met de restklassen-groep Z_m.
De congruentie op Z, gedefinieerd door m Z, valt samen met de congruentie van gehele getallen mod m.
Immers $x \equiv y \pmod m \iff x = y + m k,\ k \in Z \iff x \in y + m Z$.

Opgaven

1) Stel G een eindige groep met $|G| = n$. Bewijs dat voor ieder element $a \in G$ geldt dat $\sigma(a)$ een deler is van n.

2) Stel H_1 en H_2 zijn 2 ondergroepen van een groep G met eindige index. Bewijs dat ook $H_1 \cap H_2$ een eindige index heeft.

3) Stel G een eindige groep met $|G| = p$, p een priemgetal.
Bewijs dat voor iedere $a \neq e$, $a \in G$, geldt dat de ondergroep voortgebracht door a gelijk is aan G.

4) Stel G een groep en $P = \{x \mid x\,g = g\,x \text{ voor alle } g \in G\}$.
P heet het centrum van de groep G.
Bewijs dat P een normaaldeler is van G.

5) Stel G een groep, P het centrum van G en I(G) de groep van alle inwendige automorfismen van G.
Bewijs dan dat G/P isomorf is met I(G).

6) Stel G een groep, A(G) de automorfismengroep van G en I(G) de groep van alle inwendige automorfismen.
Bewijs dat I(G) een normaaldeler is van A(G).

7) Stel S_4 de groep van alle permutaties van 4 elementen $\{1,2,3,4\}$ en V_4 de viergroep van Klein bestaande uit de volgende permutaties

$$V_4 = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1.\end{pmatrix}\right\}$$

Bewijs: S_4/V_4 is isomorf met S_3.

§ 7. Directe producten

Definitie 1. Laat $G_1, G_2, \ldots, G_n$ groepen zijn. Dan definiëren wij $\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$ het (uitwendige) directe product van $G_1, \ldots, G_n$ als de verzameling van alle n-tallen $(a_1, a_2, \ldots, a_n)$, $a_i \in G_i$, met een lineaire operatie $\circ$ gedefinieerd door $(a_1, a_2, \ldots, a_n) \circ (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$.

Stelling 1

1°) $\prod_{i=1}^{n} G_i$ is een groep.

2°) de afbeelding $\varphi_i : a_i \to (e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n)$ is een isomorfe afbeelding van G_i op een normaaldeler N_i van $\prod_{i=1}^{n} G_i$ (e_i is het eenheidselement van G_i).

3°) $N_j \cap \langle \bigcup_{i \neq j} N_i \rangle = (e_1, e_2, \ldots, e_n)$ ($\langle \bigcup_{i \neq j} N_i \rangle$ is de ondergroep van $\prod_{i=1}^{n} G_i$ voortgebracht door $\bigcup_{i \neq j} N_i$)

Bewijs

1°) Het is duidelijk dat de operatie $\circ$ associatief is, Verder geldt

$$(e_1, e_2, \ldots, e_n) \circ (a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n) \circ (e_1, e_2, \ldots, e_n) = (a_1, a_2, \ldots, a_n).$$

$\prod_{i=1}^{n} G_i$ heeft dus een eenheidselement.

Tenslotte is $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$ en $\prod_{i=1}^{n} G_i$ is dus een groep.

2°) Daar $\varphi_i(a_i b_i) = (e_1, \ldots, e_{i-1}, a_i b_i, e_{i+1}, \ldots, e_n) =$

$$= (e_1, \ldots, a_i, \ldots, e_n) \circ (e_1, \ldots, b_i, \ldots e_n)$$

$$= \varphi(a_i) \circ \varphi_i(b_i) \text{ is}$$

φ_i een homomorfisme.

φ_i is 1-1 duidig, dus een isomorfisme en

$\varphi_i(G_i) = N_i = \left\{ (e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i \right\}$. is een

ondergroep van $\prod_{i=1}^{n} G_i$ (zie § 5 stelling 3).

N_i is zelfs een normaaldeler daar

$$(a_1,a_2,\ldots,a_n) \cdot (e_1,\ldots,e_{i-1},b_i,e_{i+1},\ldots,e_n) =$$

$$= (e_1,\ldots,e_{i-1},a_i b_i a_i^{-1},e_{i+1},\ldots,e_n) \cdot (a_1,\ldots,a_n)$$

3°) Het is duidelijk dat

$$\langle \bigcup_{i\neq j} N_i \rangle = \left\{(a_1,a_2,\ldots,a_{j-1},e_j,a_{j+1},\ldots,a_n) \mid a_i \in G_i,\ i \neq j\right\}.$$

en dat $N_j \cap \langle \bigcup_{i\neq j} N_i \rangle = (e_1,\ldots,e_n)$.

Opmerking 1. Als α een willekeurige permutatie is van de verzameling $(1,2,\ldots,n)$ dan is $G_1 \times \ldots \times G_n$ isomorf met $G_{\alpha(1)} \times \ldots \times G_{\alpha(n)}$. Immers de afbeelding α^* $(a_1,\ldots,a_n) \rightarrow (a_{\alpha(1)},\ldots,a_{\alpha(n)})$ is een isomorfisme van

$G_1 \times \ldots \times G_n$ op $G_{\alpha(1)} \times \ldots \times G_{\alpha(n)}$.

Het directe product hangt dus niet af van de volgorde van de groepen $G_1,\ldots,G_n$.

Definitie 2: Een groep G heet (inwendig) direct product van zijn normaaldelers $G_1,\ldots,G_n$ als er een isomorfisme φ van G op $\prod_{i=1}^{n} G_i$ bestaat dat een voortzetting isvan de afbeeldingen φ_i. (m.a.w. $\varphi \mid G_i = \varphi_i$).

Opmerking 2. Uit de bovenstaande definitie en stelling 1 volgt, dat als $\prod_{i=1}^{n} G_i$ het uitwendige directe product is van de groepen $G_1,\ldots,G_n$, dan is $\prod_{i=1}^{n} G_i$ het inwendige directe product van zijn normaaldelers $N_1,\ldots,N_n$ met $N_i = \varphi_i(G_i)$.

Stelling 2

Een groep G is dan en slechts dan (inwendig) direct product van z'n normaaldelers $G_1,\ldots,G_n$ als

1°) ieder element $g \in G$ te schrijven is als $g = a_1 a_2 \ldots a_n$; $a_i \in G_i$

2°) $G_j \cap \langle \bigcup_{i\neq j} G_i \rangle = e$.

Bewijs

$\Rightarrow$: Zij φ de isomorfe afbeelding van G op $\prod_{i=1}^{n} G_i$ met $\varphi \mid G_i = \varphi_i$

Stel $g \in G$ en $\varphi(g) = (a_1,\ldots,a_n)$.

Daar $\varphi(a_1a_2\ldots a_n) = \varphi(a_1) \circ \varphi(a_2) \ldots \varphi(a_n) =$

$= \varphi_1(a_1) \circ \varphi_2(a_2) \circ \ldots \circ \varphi_n(a_n) = (a_1,e,\ldots,e) \circ (e,a_2,\ldots,e) \circ \ldots$

$\circ (e,\ldots e,a_n) = (a_1,a_2,\ldots,a_n)$ en φ 1-1 duidig is, geldt

$\varphi(g) = \varphi(a_1a_2\ldots a_n)$ en dus $g = a_1a_2\ldots a_n$.

Stel nu $\langle \bigcup_{i\neq j} G_i \rangle$ de ondergroep van G voortgebracht door $\bigcup_{i\neq j} G_i$

Dan is $\varphi(\langle \bigcup_{i\neq j} G_i \rangle) = \langle \bigcup_{i\neq j} \varphi(G_i) \rangle = \langle \bigcup_{i\neq j} \varphi_i(G_i) \rangle = \langle \bigcup_{i\neq j} N_i \rangle$

(zie opgave 2 blz 27)

Dus $\varphi(G_j \cap \langle \bigcup_{i\neq j} G_i \rangle) = N_j \cap \langle \bigcup_{i\neq j} N_i \rangle = (e,e,\ldots,e)$.

Daar φ 1-1 duidig is, volgt hieruit dat

$G_j \cap \langle \bigcup_{i\neq j} G_i \rangle = e$.

$\Leftarrow$ Stel nu omgekeerd dat $G,G_1,\ldots,G_n$ voldoen aan de voorwaarden 1) en 2).

We bewijzen nu dat iedere $g \in G$ maar op een manier te schrijven is als $g = a_1a_2\ldots a_n$, met $a_i \in G_i$.

Immers als $a_1a_2\ldots a_n = b_1b_2\ldots b_n$, dan is

$b_1^{-1}a_1 = (b_2\ldots b_n)(a_2\ldots a_n)^{-1}$.

Daar $(b_2\ldots b_n)(a_2\ldots a_n)^{-1} \in \langle \bigcup_{i\neq 1} G_i \rangle$ en $b_1^{-1}a_1 \in G_1$ geldt

$b_1^{-1}a_1 = e \Rightarrow b_1 = a_1$.

Dus $a_2\ldots a_n = b_2\ldots b_n$, en met inductie volgt dan dat $a_i = b_i$, $i=1,\ldots n$.

Evenzo volgt uit 2^{o}) dat $a_ia_j = a_ja_i$ als $i\neq j$.

Immers $(a_ia_j)(a_i^{-1}a_j^{-1}) = (a_ia_ja_i^{-1})a_j^{-1} \in G_j$ daar G_j een normaaldeler is en $(a_ia_j)(a_i^{-1}a_j^{-1}) = a_i(a_ja_i^{-1}a_j^{-1}) \in G_i$, daar G_i een normaaldeler is,

Dus $(a_ia_j)(a_i^{-1}a_j^{-1}) = a_ia_j(a_ja_i)^{-1} = e \Rightarrow a_ia_j = a_ja_i$.

Wij definieren nu de afbeelding φ van G op $\prod_{i=1}^{n} G_i$ door

$\varphi(g) = \varphi(a_1a_2\ldots a_n) = (a_1,a_2,\ldots,a_n)$.

Het is duidelijk dat φ 1-1-duidig is en dat $\varphi|G_i = \varphi_i$.

φ is zelfs een isomorfie, daar

$\varphi(a_1a_2\ldots a_nb_1b_2\ldots b_n) = \varphi(a_1b_1a_2b_2\ldots a_nb_n) = (a_1b_1,a_2b_2,\ldots,a_nb_n)$.

Opmerking 3

Als een groep G geschreven kan worden als het directe product van z'n normaaldelers $G_1,\ldots,G_n$, dan noemen wij deze ondergroepen directe factoren en schrijven $G \cong G_1 \times \ldots \times G_n$.

Uit het bewijs van stelling 2 volgt dat als $G_1,\ldots,G_n$ normaaldelers zijn, dan is $\langle \bigcup_{i=1} G_i \rangle = G_1G_2\ldots G_n = \{a_1a_2\ldots a_n\}$.

Opmerking 4

Uit stelling 2 volgt dat een groep G het directe product is van zijn normaaldelers A en B als

1°) $G = A\,B$ en

2°) $A \cap B = e$.

Tevens is dan ook: $ab = ba$ voor alle $a \in A$ en $b \in B$.

Voorbeeld 1. Zij V het (arithmetische) platte vlak, d.w.z. V is de verzameling van alle geordende paren van reële getallen (a_1,a_2).

V is met de "vektoroptelling" een groep: $(a_1,a_2) + (b_1,b_2) = (a_1+a_2,\ b_1+b_2)$.

V is het directe product van de optelgroep van de reële getallen $(R +)$ met $(R +)$.

Voorbeeld 2. De viergroep van Klein V_4 is isomorf met het directe product van twee cyclische groepen van de orde 2 $V_4 \cong Z_2 \times Z_2$.

Immers stel $V_4 = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$

en $A = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\right\}$, $B = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}$

Dan zijn A en B beide isomorf met Z_2, $A \cap B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}$ en $V_4 = A\,B$.
Uit stelling 2 volgt dus dat $V_4 \cong A \times B \cong Z_2 \times Z_2$.

Voorbeeld 3. Stel Z_{rs} de restklassengroep van de gehele getallen modulo rs, r en s geheel (r,s) = 1. $Z_{rs} = \{0,1,2,\ldots,rs-1\}$.
Stel nu $\langle s \rangle$ de ondergroep van Z_{rs} voortgebracht door s:
$\langle s \rangle = \{0,s,2s,3s,\ldots(r-1)s\}$. $\cong Z_r$ (ga na!).
Evenzo
$\langle r \rangle = \{0,r,2r,\ldots(s-1)r\} \cong Z_s$.
Daar ieder element uit Z_{rs} te schrijven is als $n_1 r+n_2 s$ en $\langle s \rangle \cap \langle r \rangle = 0$, volgt dat

$$Z_{rs} \cong Z_r \times Z_s.$$

Stelling 3. Zij G een groep en G het directe product van z'n normaaldelers A en B, $G \cong A \times B$. Dan is $G/A \cong B$.

Bewijs

Stel $Ag \in G/A$ en $g = a\,b$.
Dan is $a^{-1}g = b \in A\,g$ en $A\,g = A\,b$.
Iedere nevenklasse van A bevat dus een element van B. Daar g maar op een manier te schrijven is als $g = ab$ volgt dat $A\,g = A\,b$ precies een element van B bevat. De afbeelding $\varphi : A\,g = A\,b \rightarrow b$ is een isomorfie van G/A op B.

Opmerking 5: Het directe product van willekeurig veel groepen $\{G_i\}_{i \in T}$ wordt gedefinieerd als de verzameling van alle functies $a = (a_i)_{i \in I}$ op I met $a_i \in G_i$, waarbij slechts eindig veel $a_i \neq e_i$.
De vermenigvuldiging geschiedt componentsgewijs.

Het cartesisch of onbeperkte directe product van de groepen $\{G_i\}_{i \in I}$ wordt gedefinieerd als de verzameling van alle functies $a = (a_i)_{i \in I}$ met $(a_i)_{i \in I}\,(b_i)_{i \in I} = (a_i b_i)_{i \in I}$.
Als I eindig is, dan is het onbeperkte directe product gelijk aan het directe product.

Opgaven

1) Laat A en B ondergroepen zijn van G zodanig dat
   1^{o}) $ab = ba$ voor alle $a \in A$ en $b \in B$.
   2^{o}) $A \cap B = \{e\}$
   3^{o}) $G = \langle A \cup B \rangle$
   Dan is $G \cong A \times B$.

2) Laat $H \cong A \times B$ en $B \cong C \times D$
   Dan is $H \cong A \times C \times D$.

3) Laat G het directe product zijn van z'n normaaldelers A en B.
   H is een ondergroep van G die A omvat.
   Bewijs dat $H \cong A \times (B \cap H)$

4) Laat G het directe product zijn van z'n normaaldelers A en B;
   $G \cong A \times B$
   Stel $a \in A$, $b \in B$ met $\sigma(a) < \infty$ en $\sigma(b) < \infty$.
   Dan is $\sigma(ab)$ = k.g.v. van $\sigma(a)$ en $\sigma(b)$.

Literatuur

1. G. Birkhoff: S. Mac Lane: A survey of modern algebra.
2. W. Burnside: Theory of groups of finite order.
3. R.D. Carmichael: Introduction to the theory of groups of finite order.
4. L. Fuchs: Abelian groups.
5. M. Hall: The theory of groups.
6. A.G. Kurosh: Theory of groups I.
7. W. Ledermann: Introduction to the theory of finite groups.
8. F. Loonstra: Inleiding tot de algebra.
9. G. Papy: Groups.
10. L. Redei: Algebra I.

§ 8. Ringen en Lichamen

Definitie 1. Een ring is een verzameling R, voorzien van twee binaire operaties (+ en .), met de volgende eigenschappen:

(1) (R,+) is een abelse groep,

(2) de operatie . is associatief; d.w.z. (a.b).c = a.(b.c) voor alle a,b,c ∈ R,

(3) de operaties + en . zijn aan elkaar gekoppeld door middel van de twee distributieve wetten:

$$\left.\begin{aligned} a.(b+c) &= a.b + a.c \\ (b+c).a &= b.a + c.a \end{aligned}\right\} \quad \text{voor alle } a,b,c \in R.$$

Opmerkingen bij definitie 1:

ad (1). Het neutrale element van (R,+) geven we aan met 0; voor de inverse van a ∈ (R,+) schrijven we -a.

ad (2). Er zij nadrukkelijk op gewezen dat niet verondersteld is dat R een neutraal element bevat met betrekking tot de operatie . .

ad (3). Dat er twee distributieve wetten gepostuleerd worden hangt samen met het feit dat de operatie . niet commutatief verondersteld is. Is deze operatie wèl commutatief (R heet dan een commutatieve ring) dan kunnen we volstaan met één distributieve wet.

Voorbeelden van ringen. In de voorbeelden a tot en met e wordt onder + resp. . de gebruikelijke optelling resp. vermenigvuldiging voor getallen verstaan.

a. Z, de verzameling der gehele getallen, is een commutatieve ring.

b. De verzameling van alle even getallen is een commutatieve ring.

c. De rationale getallen, evenals de reële en de complexe getallen, vormen een commutatieve ring.

d. $C[i]$, de verzameling van alle complexe getallen z van de gedaante $z = a + bi$, met gehele a en b, is eèn commutatieve ring.

De elementen van C[i] heten gehele getallen van Gauss.

e. Stellen we

$$K(\sqrt{2}) = \{k \mid k=a+b\sqrt{2},\ a \in Q,\ b \in Q\}$$

dan is $K(\sqrt{2})$ een commutatieve ring.
Hierin is Q de verzameling der rationale getallen.

De eigenschappen van de operatie + in een ring R worden hier niet nader besproken omdat deze geheel ressorteren onder het hoofdstuk "abelse groepen" uit de algemene groepentheorie.
Voor de algemene eigenschappen van associatieve operaties, waaronder zowel + als . vallen, zie § 1.

Stelling 1. In een ring R gelden de volgende regels:

(1) $a.0 = 0.a = 0$ voor elke $a \in R$.

(2) $a.(-b) = (-a).b = -(a.b)$ voor alle $a,b \in R$.

(3) $(-a).(-b) = a.b$ voor alle $a,b \in R$.

(4) $\left.\begin{array}{l} a.(b-c) = a.b - a.c \\ (b-c).a = b.a - c.a \end{array}\right\}$ voor alle $a,b,c \in R$.

Bewijs.

(1) $\left.\begin{array}{l} a.(b+0) = a.b + a.0 \\ a.(b+0) = a.b \end{array}\right\} \Rightarrow a.b + a.0 = a.b \Rightarrow a.0 = 0$

Op analoge wijze toont men aan dat $0.a = 0$.

(2) $0 = a.0 = a.(b + (-b)) = a.b + a.(-b) \Rightarrow a.(-b) = -(a.b)$.
Evenzo: $(-a).b = -(a.b)$.

(3) Dit is een direct gevolg van (2).

(4) $a.(b-c) = a.(b + (-c)) = a.b + a.(-c) = a.b + (-(a.c)) = a.b - a.c$.
Evenzo: $(b-c).a = b.a - c.a$.

Opgave 1. Is R een ring en zijn m en n natuurlijke getallen, dan geldt:

$(a_1+a_2+ \ldots +a_m) \,.\, (b_1+b_2+ \ldots +b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i.b_j$ voor alle $a_i, b_j \in R$.
Bewijs dit.

In het vervolg van deze paragraaf zullen we ons, althans wat de algemene theorie betreft, uitsluitend bezighouden met commutatieve ringen.

Definitie 2. Geldt in de (commutatieve) ring R $a.b = 0$ terwijl $a \neq 0$ en $b \neq 0$, dan heten a en b nuldelers van R.

Voorbeeld. De additieve groep C_6 is een ring als we voor de operatie . de vermenigvuldiging modulo 6 nemen.
Nu geldt: $2.3 = 0$ met $2 \neq 0$ en $3 \neq 0$. In de ring C_6 zijn 2 en 3 dus nuldelers.
Zijn dit de enige nuldelers van C_6?

Stelling 2. Als $a \neq 0$ geen nuldeler is van de ring R dan geldt:

$$a.x = a.y \implies x = y \,.$$

Bewijs.
$a.x = a.y \implies a.x - a.y = 0 \implies a.(x-y) = 0$. Hieruit volgt $x - y = 0$ of $x = y$, omdat anders a een nuldeler van R zou zijn.

Voor de definitie van het begrip éénheidselement of neutraal element (met betrekking tot de operatie .) en de daarmee in verband staande begrippen en stellingen, verwijzen wij naar § 1.

Voorbeelden van ringen. (Vervolg van blz. 42).

f. M_2 zij de verzameling van alle 2×2 matrices met bijv. complexe elementen:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \,.$$

Definiëren we:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}$$

dan is M_2 een niet-commutatieve ring met nulelement 0 en eenheidselement e:

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{en} \quad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Dat de operatie . in M_2 niet commutatief is blijkt uit:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} .$$

Een andere bijzonderheid van deze ring is dat ze nuldelers [1] bezit. Zo is bijv.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

terwijl geen der matrices in het linkerlid gelijk is aan het nulelement van M_2.

g. Quaternionen [2]. G zij de verzameling van alle (formele) uitdrukkingen van de vorm

$$a + bi + cj + dk$$

waarbij a,b,c en d reële getallen zijn.

G is een niet-commutatieve ring met eenheidselement, als we afspreken:

---

1) Als de operatie . niet commutatief is dient in het algemeen onderscheid gemaakt te worden tussen linker- en rechternuldelers.

2) Voor een exacte invoering der quaternionen verwijzen wij naar de literatuur genoemd op blz. 40.

(1) $(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) =$

$= (a_1+a_2) + (b_1+b_2)i + (c_1+c_2)j + (d_1+d_2)k$.

(2) Het produkt van twee quaternionen wordt gevonden met behulp van de volgende rekenregels

$i^2 = j^2 = k^2 = -1$,

$ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

h. Als R een gegeven ring is dan kunnen we met behulp van de elementen van R op verschillende manieren nieuwe ringen construeren (zie ook voorbeeld f).

(1) $M[x]$ zij de verzameling van alle uitdrukkingen van de gedaante

$$a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{n=1}^{\infty} a_n x^n$$

waarbij de coëfficiënten a_n elementen van R zijn.
Definiëren we

$$\left(\sum_{n=1}^{\infty} a_n x^n \right) + \left(\sum_{n=1}^{\infty} b_n x^n \right) = \sum_{n=1}^{\infty} (a_n+b_n) x^n$$

$$\left(\sum_{n=1}^{\infty} a_n x^n \right) \cdot \left(\sum_{m=1}^{\infty} b_m x^m \right) = \sum_{k=1}^{\infty} \left(\sum_{n=0}^{k} a_n . b_{k-n} \right) x^k$$

dan is $M[x]$ een ring.
$M[x]$ heet de ring der <u>formele machtreeksen</u> over R.
Is R een commutatieve ring met éénheidselement dan is dat ook het geval met $M[x]$.

(2) $R[x]$ zij de verzameling van alle formele machtreeksen, met slechts eindig veel coëfficiënten ongelijk aan $0 \in R$.
Met de onder (1) gedefiniëerde optelling en vermenigvuldiging voor formele machtreeksen is $R[x]$ een ring. $R[x]$ heet de <u>polynoomring</u> over R.
Bij de notatie van polynomen is het gebruikelijk de termen met coëfficiënt 0 weg te laten.

(3) De verzameling van alle geordende n-tallen

$$(a_1,a_2,\ldots,a_n)\ ,\quad a_i \in R$$

kan tot een ring gemaakt worden door te definiëren

$$(a_1,\ldots,a_n) + (b_1,\ldots,b_n) = (a_1+b_1,\ldots,a_n+b_n)$$

$$(a_1,\ldots,a_n)\ .\ (b_1,\ldots,b_n) = (a_1.b_1,\ldots,a_n.b_n).$$

i. (1) Zij X een gegeven verzameling. Dan is de machtsverzameling $\mathfrak{P}(X)$ van X een ring als we de operaties + en . als volgt definiëren:

$$\left.\begin{array}{l} A + B = (A \cup B) \cap (A' \cup B') \\ A\ .\ B = A \cap B \end{array}\right\} \quad \text{voor alle } A,B \in \mathfrak{P}(X).$$

(Hierbij is A' het complement van A t.o.v. X).

$\mathfrak{P}(X)$ is een commutatieve ring met eenheidselement X en nulelement ϕ.
Behalve X en ϕ zijn alle elementen van $\mathfrak{P}(X)$ nuldelers.

(2) Op soortgelijke wijze kunnen we de verzameling van alle eindige deelverzamelingen van X tot een ring maken.
Wanneer heeft deze ring een éénheidselement?

j. C zij de verzameling van alle continue functies op het interval $[0,1]$.
C is een commutatieve ring met éénheidselement als we voor de operaties + en . resp. de gebruikelijke optelling en vermenigvuldiging van functies nemen.
Bevat C ook nuldelers?

Definitie 3. Is R een ring met éénheidselement e, dan noemen we het element $u \in R$ een eenheid van R als er een $v \in R$ bestaat zodanig dat

$$u.v = v.u = e\ .$$

Volgens § 1 is dit element v (als het bestaat) éénduidig bepaald en het heet dan de inverse van u. We schrijven $v = u^{-1}$.
Het begrip eenheid is dus gelijkwaardig met inverteerbaar element.

Stelling 3. De eenheden van de ring R (met eenheidselement) vormen met betrekking tot de operatie . een groep U. Dit is de groep der eenheden van R.

Bewijs.

a. Als $u_1, u_2 \in U$, dan is ook $u_1.u_2 \in U$, want
$(u_1.u_2).(u_2^{-1}.u_1^{-1}) = e = (u_2^{-1}.u_1^{-1}).(u_1.u_2)$.

b. Het is duidelijk dat de operatie . in U associatief is.

c. U bevat het eenheidselement $e \in R$ want $e.e = e.e = e$.

d. Als $u \in U$, dan is ook $u^{-1} \in U$ volgens de definitie van U.

Definitie 4. Een commutatieve ring R met eenheidselement heet een integriteitsgebied als R geen nuldelers bezit.

Definitie 5. Een (commutatieve) ring K heet een (commutatief) lichaam als
(1) K een eenheidselement bevat,
(2) elke $a \in K$ met $a \neq 0$ inverteerbaar is.

Uit deze definitie en stelling 3 volgt dat $K \setminus \{0\}$ een groep is.

Voorbeelden van lichamen.

a. De rationale getallen, evenals de reële en de complexe getallen, vormen een commutatief lichaam.

b. De quaternionen uit voorbeeld g, blz. 44, vormen een niet-commutatief lichaam.

c. De verzameling van alle complexe getallen van de gedaante $z = a+bi\sqrt{2}$ met rationale a en b is een commutatief lichaam.

d. C_5 (de restklassen modulo 5) is een commutatief lichaam.

Stelling 4. Een lichaam bezit geen nuldelers.

Bewijs. Als $a.b = 0$ met $a \neq 0$, dan is

$$a^{-1}.(a.b) = a^{-1}.0$$

en dus: $b = 0$.

In een lichaam geldt dus de regel dat een product dan en slechts dan gelijk aan 0 is als minstens één der factoren gelijk aan 0 is.

§ 9. Ring-homomorfie, idealen

Definitie 1. Is φ een afbeelding van de ring R in (op) de ring $\overline{R}$ zodanig dat

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a.b) = \varphi(a) \,.\, \varphi(b)$$

voor alle $a,b \in R$ $(\varphi(a),\varphi(b) \in \overline{R})$, dan heet φ een (ring-)homomorfie van R in (op) $\overline{R}$.
Is de afbeelding φ bovendien 1-1-duidig, dan spreken we van een isomorfe afbeelding van R in (op) $\overline{R}$.
Een homomorfe afbeelding van de ring R in (op) zichzelf heet een endomorfie van R.
Een isomorfie van R op R heet een automorfie van R.

Stelling 1. Is φ een homomorfie van de ring R in de ring $\overline{R}$, dan is $\varphi(R) \subset \overline{R}$ een ring.
($\varphi(R)$ is een deelring van $\overline{R}$).

Bewijs. Allereerst tonen we aan dat $\varphi(R)$ gesloten is met betrekking tot de operaties + en . .
Als $\overline{a},\overline{b} \in \varphi(R)$ dan zijn er $a,b \in R$ zodanig dat $\varphi(a) = \overline{a}$ en $\varphi(b) = \overline{b}$.
Nu is $a+b \in R$ en $a.b \in R$, dus $\varphi(a+b) = \varphi(a) + \varphi(b) = \overline{a}+\overline{b} \in \varphi(R)$
en $\varphi(a.b) = \varphi(a).\varphi(b) = \overline{a}.\overline{b} \in \varphi(R)$.
De rest van het bewijs wordt aan de lezer overgelaten.

Opgave. Bewijs de volgende stelling:

Stelling 2. Is φ een homomorfie van de ring R in de ring $\overline{R}$ dan geldt:

(1) is R commutatief dan is ook de ring $\varphi(R)$ commutatief,

(2) $\varphi(0) = \overline{0}$ $\quad (0 \in R,\ \overline{0} \in \overline{R})$,

(3) $\varphi(-a) = -\varphi(a)$ voor alle $a \in R$,

(4) heeft R een eenheidselement e dan heeft ook $\varphi(R)$ een eenheidselement $\overline{e} = \varphi(e)$,

(5) $\varphi(a^{-1}) = (\varphi(a))^{-1}$ als a een eenheid van R is.

Definitie 2. Een niet-lege deelverzameling I van de ring R heet een ideaal van R, als

(1) $a,b \in I \implies a-b \in I$,

(2) $a \in I,\ r \in R \implies a.r \in I$ en $r.a \in I$.

Voorbeeld. In de ring Z is de verzameling van alle 2-vouden een ideaal.

Elke ring R bezit twee z.g. triviale idealen:

(1) de ring R zelf,

(2) het z.g. nulideaal, bestaande uit het element 0 alleen.

Stelling 3. Zij φ een homomorfe afbeelding van de ring R in de ring $\overline{R}$, dan vormen de elementen van R die op $\overline{0} \in \overline{R}$ worden afgebeeld een ideaal van R. Dit ideaal heet de kern van de homomorfie.

Bewijs.

(1) Als $\varphi(a) = \overline{0}$ en $\varphi(b) = \overline{0}$, dan is ook $\varphi(a-b) = \varphi(a) - \varphi(b) = \overline{0}$.

(2) Uit $\varphi(a) = \overline{0}$ volgt $\varphi(a.r) = \varphi(a).\varphi(r) = \overline{0}.\varphi(r) = \overline{0}$ voor elke $r \in R$.

Stelling 4. Een lichaam K bevat uitsluitend triviale idealen.

Bewijs. Zij I een van het nulideaal (0) van K verschillend ideaal; dan bevat I zeker een van 0 verschillend element a. Omdat K een lichaam is, is $a \neq 0$ in K inverteerbaar. I moet met $a \neq 0$ dan ook $a.a^{-1} = e$ bevatten, maar als $e \in I$ dan is ook $k = k.e \in I$ voor elke $k \in K$. Hieruit volgt dat I met (het triviale ideaal) K samenvalt.

§ 10. Quotiëntenlichaam

Stelling 1. Is R een (commutatieve) ring met een van 0 verschillend element, zonder nuldelers, dan is het mogelijk een lichaam Q te construeren dat R als deelring bevat.

Bewijs. Zij B de verzameling van alle geordende paren (a,b) met $a,b \in R$, $b \neq 0$. Twee paren, (a,b) en (c,d) zullen we aequivalent noemen als $a.d = b.c$.
Deze relatie is een aequivalentie-relatie in de zin van § 6, def. 1. Ga dit na!
Met behulp van deze aequivalentie-relatie kunnen we B verdelen in een aantal disjuncte aequivalentieklassen van onderling aequivalente paren (zie § 6).
Voor de aequivalentieklasse die (a,b) bevat schrijven we $\frac{a}{b}$. De verzameling van al deze aequivalentieklassen noemen we Q.
We definiëren in Q:

$$\frac{a}{b} + \frac{c}{d} = \frac{a.d + b.c}{b.d}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a.c}{b.d}$$

(ga na dat deze definities ondubbelzinnig zijn).

Schrijven we verder: $\frac{0}{r} = 0$, $-\frac{a}{b} = \frac{-a}{b}$

dan geldt (ga dit na):

(1) $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$,

(2) $\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a}{b}$,

(3) $\frac{a}{b} + (-\frac{a}{b}) = (-\frac{a}{b}) + \frac{a}{b} = 0$,

(4) $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$

(5) $(\frac{a}{b} . \frac{c}{d}) . \frac{e}{f} = \frac{a}{b} . (\frac{c}{d} . \frac{e}{f})$,

(6) $\frac{a}{b} . (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} . \frac{c}{d} + \frac{a}{b} . \frac{e}{f}$,

(7) $\frac{a}{b} . \frac{c}{d} = \frac{c}{d} . \frac{a}{b}$.

We zien dus dat Q een commutatieve ring is. Omdat R een ring is met een van 0 verschillend element, bevat ook Q een element (= aequivalentieklasse) dat van $\frac{0}{r} = 0$ verschilt. Is $\frac{a}{b}$ zo'n klasse dan is $\frac{b}{a}$ ook zo'n klasse en we definiëren

$$(\frac{a}{b})^{-1} = \frac{b}{a}$$

Nu geldt in Q

(8) $\frac{a}{b} \neq 0 \implies (\frac{a}{b}) . (\frac{a}{b})^{-1} = (\frac{a}{b})^{-1} . (\frac{a}{b}) = 1$,

waarbij $1 = \frac{r}{r}$ $(r \neq 0)$.

Uit het een en ander volgt dat Q een commutatief lichaam is.

We beelden nu R als volgt af in Q:

$$a \longrightarrow \frac{a.r}{r} .$$

Het is gemakkelijk in te zien dat deze afbeelding een <u>isomorfie is van R op een deelring R' van Q</u> bestaande uit alle klassen $\frac{a.r}{r}$.
We mogen dus zeggen (cum grano salis) dat het lichaam Q de ring R omvat.
Q heet het <u>quotiëntenlichaam</u> van R.

Stelling 2. R zij een commutatieve ring met een van 0 verschillend element; K zij een lichaam dat R omvat. Dan bevat K een deellichaam Q' dat isomorf is met het quotiëntenlichaam Q van R.

Bewijs. R bevat geen nuldelers, want $R \subset K$. Aan de voorwaarden van stelling 1 is dus voldaan.
Is $b \neq 0$, $b \in R$ dan ligt b^{-1} in K.
Zij Q' de deelverzameling van K bestaande uit alle producten $a.b^{-1}$ met $a,b \in R$ en $b \neq 0$.
Het (bestaande) quotiëntenlichaam Q van R beelden we als volgt op Q' af:

$$\frac{a}{b} \longrightarrow a.b^{-1} .$$

De lezer bewijze zelf dat dit een isomorfe afbeelding van Q op Q' is. Hiermee is aangetoond dat Q' een met Q isomorf deellichaam van K is.

N.B. Merk op dat het quotiëntenlichaam Q van R het "kleinste" lichaam is dat R als deelring omvat.

Vraagstukken.

1. Bewijs dat elk ideaal van een ring R een deelring van R is.
2. Construeer het bij de ring der even getallen behorende quotiëntenlichaam. Is dit lichaam isomorf met het lichaam der rat. getallen?
3. Geef een voorbeeld waaruit blijkt dat het homomorfe beeld van een integriteitsgebied geen integriteitsgebied behoeft te zijn.
4. R en R' zijn twee gegeven ringen, waarvan R een eenheidselement bevat. Als er een isomorfe afbeelding bestaat van R in R', bezit R' dan noodzakelijk ook een eenheidselement? Licht het antwoord toe met een voorbeeld.
5. Bewijs dat de reeds eerder genoemde quaternionenring een niet-commutatief lichaam is.
6. Geef een voorbeeld van een ideaal in de ring der formele machtreeksen (c.q. polynoom-ring) over een commutatieve ring R.

7. Hoeveel en welke idealen bezitten de ringen C_6, C_5 ?

8. Hoeveel en welke ring-endomorfieën bezit Z?
   Bepaal alle idealen van Z.

9. Is een rechter-nuldeler van M_2 in voorbeeld f ook automatisch een linker-nuldeler?

10. Bepaal van de ringen Z en Q de groep der eenheden.
    Waaruit bestaat de groep der eenheden bij een willekeurig lichaam?

11. Bewijs dat C_n dan en slechts dan een lichaam is als n een priemgetal is.

12. Als R een integriteitsgebied is dan is ook de polynoom-ring R[x] over R een integriteitsgebied.

13. Is de ring R het homomorfe beeld van een lichaam K dan zijn er twee mogelijkheden:
    (1) R bevat slechts één element (het nulelement),
    (2) R is een lichaam dat isomorf is met K.
    Bewijs dit.

II LINEAIRE ALGEBRA

§ 11. Lineaire ruimten

Definitie 1. Zij K een commutatief lichaam. Een lineaire ruimte of vectorruimte over K is een (additieve) abelse groep E, tezamen met een afbeelding σ: $K \times E \to E$ die de onderstaande vier eigenschappen bezit (in plaats van $\sigma(\alpha,x)$ ($\alpha \in K$, $x \in E$) schrijven we $\alpha.x$ of αx):

(1) $\alpha.(x+y) = \alpha.x + \alpha.y$;

(2) $(\alpha+\beta).x = \alpha.x + \beta.x$;

(3) $(\alpha\beta).x = \alpha.(\beta.x)$;

(4) $1.x = x$;

voor alle $\alpha,\beta \in K$ en voor alle $x,y \in E$.

Opmerking 1. De elementen van E noemt men dikwijls vectoren; wij zullen ze in den regel aangeven met symbolen als x,y,z. De elementen van K noemt men in dit verband vaak scalairen; voor hen zullen we de griekse letters $\alpha,\beta,\gamma,\ldots$ reserveren.

Opmerking 2. In het linkerlid van (2) geeft het teken + de optelling in K aan; in het rechterlid staat + echter voor de optelling binnen E. Evenzo moet men in (3) onderscheid maken tussen de vermenigvuldiging binnen het lichaam K en de vermenigvuldiging van een vector met een scalar. Voorts zullen we zowel het nulelement van K als het nulelement van de groep E met 0 aanduiden, hoewel we hier i.h.a. met twee verschillende objecten te doen hebben. Ook het symbool - gebruiken we in twee betekenissen.

Stelling 1 (Elementaire eigenschappen). Zij E een vectorruimte over K. Voor willekeurige $\alpha,\beta \in K$ en $x,y \in E$ geldt:

(a) $\alpha.0 = 0$;

(b) $0.x = 0$;

(c) $\alpha.x = 0 \Rightarrow \alpha = 0$ of $x = 0$;

(d) $(-\alpha)\circ x = -(\alpha\circ x) = \alpha\circ(-x)$;

(e) $\alpha\circ(x-y) = \alpha\circ x - \alpha\circ y$;

(f) $(\alpha-\beta)\circ x = \alpha\circ x - \beta\circ x$.

Bewijs.

(a) $\alpha\circ 0 = \alpha\circ(0+0) = \alpha\circ 0 + \alpha\circ 0 \Longrightarrow 0 = \alpha\circ 0$.

(b) $0\circ x = (0+0)\circ x = 0\circ x + 0\circ x \Longrightarrow 0 = 0\circ x$.

(c) Stel $\alpha\circ x = 0$ maar $\alpha \neq 0$. Dan is $x = 1\circ x = (\alpha^{-1}\alpha)\circ x = \alpha^{-1}\circ(\alpha x) = \alpha^{-1}\circ 0 = 0$.

(d) $\alpha\circ x + (-\alpha)\circ x = (\alpha+(-\alpha))\circ x = 0\circ x = 0 \Longrightarrow (-\alpha)\circ x = -(\alpha\circ x)$.
$\alpha\circ x + \alpha\circ(-x) = \alpha\circ(x-x) = \alpha\circ 0 = 0 \Longrightarrow \alpha\circ(-x) = -(\alpha\circ x)$.

(e) $\alpha\circ(x-y) = \alpha\circ x + \alpha\circ(-y) = \alpha\circ x - \alpha\circ y$.

(f) $(\alpha-\beta)\circ x = \alpha\circ x + (-\beta)\circ x = \alpha\circ x - \beta\circ x$.

Voorbeelden.

(a) Zij R het lichaam der reële getallen, en R^n de verzameling van alle geordende n-tallen reële getallen $x = (x_1, x_2, \ldots, x_n)$ met als optelling

(11.1) $\quad (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$.

Voor $\alpha \in R$ en $x = (x_1, x_2, \ldots, x_n) \in R^n$ zij

(11.2) $\quad \alpha\circ x = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$.

Dan is R^n een lineaire ruimte over R.

(b) Algemener: Zij K een willekeurig commutatief lichaam, K^n de verzameling van alle geordende n-tallen van elementen uit K; optelling in K^n en vermenigvuldiging van een $x \in K^n$ met een $\alpha \in K$ definiëren we als in (a). Dan is K^n een lineaire ruimte over K.

(c) Nog algemener: Zij K een willekeurig commutatief lichaam, T een verzameling, K^T de verzameling van alle functies, gedefinieerd op T en met waarden in K. Als $f, g \in K^T$, dan zij f+g de functie waarvoor

(11.3) $(f+g)(t) = f(t) + g(t) \qquad (t \in T)$;

als $f \in K^T$ en $\alpha \in K$, dan zij $\alpha.f$ de functie met

(11.4) $(\alpha f)(t) = \alpha.f(t) \qquad (t \in T)$.

Op deze wijze wordt K^T tot een vectorruimte over K.

(d) Stel a,b zijn reële getallen met $a < b$; met $C[a,b]$ geven we aan de verzameling van alle continue reëelwaardige functies gedefinieerd op het interval $[a,b]$. Als $f,g \in C[a,b]$ en als $\alpha \in R$, dan definiëren we functies $f+g$ en $\alpha.f$ uit $C[a,b]$ door

(11.5) $(f+g)(t) = f(t) + g(t) \qquad (t \in [a,b])$;

(11.6) $(\alpha f)(t) = \alpha.f(t) \qquad (t \in [a,b])$.

Dan is $C[a,b]$ een lineaire ruimte over R.

(e) Stel a,b zijn reële getallen met $a < b$, en n is een natuurlijk getal. Met $D_n[a,b]$ wordt aangegeven de verzameling van alle reëelwaardige functies gedefinieerd op $[a,b]$, die op dit interval n maal differentieerbaar zijn met continue n-de afgeleide. Ook $D_n[a,b]$ is een lineaire ruimte over R, indien we optelling in D_n en vermenigvuldiging met een reële scalar weer definiëren door (11.5) en (11.6). Voor $C[a,b]$ (vgl. voorbeeld (d)) schrijven we ook wel $D_0[a,b]$.

(f) Stel $g_0,g_1,\ldots,g_n$ zijn reëelwaardige functies gedefinieerd op een reëel interval $[a,b]$. Zij E de verzameling van alle $f \in D_n[a,b]$ die op dat interval voldoen aan de differentiaalvergelijking

$$(11.7)\quad g_n(t).\frac{d^n f(t)}{dt^n} + g_{n-1}(t).\frac{d^{n-1} f(t)}{dt^{n-1}} + \ldots + g_1(t).\frac{df(t)}{dt} = g_0(t).$$

Indien we de optelling in E en de vermenigvuldiging met een reële scalar weer definiëren m.b.v. (11.5) en (11.6), dan is E een vectorruimte over R.

(g) Zij F een lichaam (niet noodzakelijk commutatief). De elementen $\alpha \in F$ met de eigenschap dat zij commuteren met alle elementen van F: $\alpha.\xi = \xi.\alpha$ voor alle $\xi \in F$, vormen een deellichaam van F, het centrum van F.

De additieve groep F^+ van F is een vectorruimte over het centrum van F als we voor het product van een centrumelement α en een willekeurige $x \in F$ steeds nemen hun product in het lichaam F.

In het bijzonder is ieder commutatief lichaam een vectorruimte over zichzelf (dit is ook reeds besloten in voorbeeld (b), voor n = 1 nl.).

(h) Algemener: Zij F een willekeurig lichaam, en zij K een commutatief deellichaam van F. Dan is F een vectorruimte over K.

Zo is R een vectorruimte over het lichaam Q der rationale getallen, en ook over het lichaam $Q[\sqrt{2}]$ van alle getallen van de vorm $a+b\sqrt{2}$ $(a,b \in Q)$.

Evenzo is (de additieve groep van) het lichaam C der complexe getallen een lineaire ruimte over R, en evenzo over Q. Ook het lichaam der quaternionen is een vectorruimte over R, en ook over C en over Q.

(i) Zij X een verzameling, $E = \mathcal{P}(X)$; voor $x,y \in E$ zij $x+y$ het symmetrisch verschil

$$x+y = (x \cup y) \setminus (x \cap y) \quad (= (x \setminus y) \cup (y \setminus x))$$

(vgl. §2, voorbeeld (e) en §4, opgave 15). Zij Z_2 het lichaam $\{0,1\}$, met als lichaamsoperaties: $0+0 = 1+1 = 0$; $0+1 = 1+0 = 1$; $0.0 = 0.1 = 1.0 = 0$; $1.1 = 1$. Dan is E een vectorruimte over K als we definiëren, voor willekeurige $x \in E$:

$$0.x = \emptyset \quad , \qquad 1.x = x \ .$$

Nemen we voor X een eindige verzameling, dan is $\mathcal{P}(X)$ een voorbeeld van een vectorruimte met slechts eindig veel elementen.

(j) Zij p een priemgetal. De restklassen modulo p in Z vormen een lichaam Z_p. Een additieve groep G is een vectorruimte over Z_p, onder de scalar-vermenigvuldiging

$$k.x = x + x + \ldots + x \qquad (k=0,1,2,\ldots,p-1;\ x \in G)$$

dan en slechts dan indien ieder element $x \neq 0$ in G de orde p heeft.

(k) Zij K een commutatief lichaam. De additieve groep van de polynoomring K[x] is een vectorruimte over K (voor $\alpha \in K$ en $P = \gamma_0+\gamma_1 x+\ldots+\gamma_n x^n \in K[x]$ definiëren we

$$\alpha.P = \alpha\gamma_0 + \alpha\gamma_1 x + \ldots + \alpha\gamma_n x^n \ ) \ .$$

§ 12. Lineaire afbeeldingen

Definitie 1. Stel E en F zijn twee vectorruimten over eenzelfde lichaam K. Een afbeelding ϕ: E → F heet lineair indien

(1) ϕ is een homomorphisme van de groep E in de groep F;

(2) $\phi(\alpha.x) = \alpha.\phi(x)$, voor alle $\alpha \in K$ en alle $x \in E$.

Een lineaire afbeelding ϕ van E in F noemt men ook wel een lineair homomorphisme; ook de uitdrukking lineaire operator wordt gebruikt.

Stelling 1. De afbeelding ϕ: E → F is lineair als en slechts als

$$\phi(\alpha x + \beta y) = \alpha\phi(x) + \beta\phi(y)$$

voor alle $\alpha,\beta \in K$ en $x,y \in E$.

Het bewijs van deze eenvoudige stelling zij den lezer overgelaten.

Definitie 2. Stel E en F zijn vectorruimten over een zelfde lichaam K. Een 1-1-duidige lineaire afbeelding van E in (op) F heet een lineair isomorphisme van E in (op) F.

Analoog worden lineaire endomorphismen en lineaire automorphismen gedefinieerd. Als er geen verwarrring mogelijk is laten we de toevoeging "lineair" weg.

Voorbeelden.

(a) Zowel R als C is een vectorruimte over R (§11, voorbeeld (h)). De afbeeldingen Re en Im die aan $x \in C$ respectievelijk het reële en het imaginaire deel toevoegen zijn lineaire afbeeldingen van C in R. De afbeelding die $x \in C$ overvoert in het toegevoegd complexe getal $\overline{x} \in C$ is een lineair automorphisme van C.

(b) De afbeelding $x \to (\mathrm{Re}\ x, \mathrm{Im}\ x)$ is een lineair isomorphisme van C op R^2 (beide beschouwd als vectorruimte over R). De afbeelding $x \to (\mathrm{Im}\ x, \mathrm{Re}\ x)$ is een ander lineair isomorphisme van C op R^2.

(c) Zij K een commutatief lichaam, T een verzameling, $t_0 \in T$. Zij K^T de vectorruimte over K, beschreven in §11, voorbeeld (c); we beschouwen ook K als vectorruimte over zichzelf (vgl. §11, voorbeeld (g)). De afbeelding

$$f \to f(t_0)$$

is een lineaire afbeelding van K^T op K.

(d) Zij $[a,b]$ een reëel interval. De afbeelding die aan $f \in D_1[a,b]$ zijn afgeleide f' toevoegd is een lineaire afbeelding van $D_1[a,b]$ op $C[a,b]$ (vgl. §11, voorbeelden (d) en (e)). Evenzo is, voor $n > 1$, de afbeelding $f \to f'$ een lineaire afbeelding van $D_n[a,b]$ op $D_{n-1}[a,b]$.

(e) De afbeelding

$$f \to \int_a^b f(t)\,dt$$

is een lineaire afbeelding van $C[a,b]$ op R.

(f) Zij

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

een reële $m \times n$ matrix. Met behulp van A kunnen we een lineaire afbeelding T van R^n in R^m definiëren, als volgt:
als $x = (x_1, x_2, \ldots, x_n) \in R^n$, dan zij Tx het element
$y = (y_1, y_2, \ldots, y_m) \in R^m$ met

$$y_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \quad (i=1,2,\ldots,m) .$$

Stelling 2. Stel E_1, E_2, E_3 zijn vectorruimten over een zelfde lichaam K. Indien $\phi_1 : E_1 \to E_2$ en $\phi_2 : E_2 \to E_3$ lineaire afbeeldingen zijn, dan is ook $\phi_2 \circ \phi_1 : E_1 \to E_3$ lineair.

Bewijs.

Volgens §4, stelling 1, is $\phi_2 \circ \phi_1$ een homomorphisme; en

$$\phi_2 \circ \phi_1(\alpha x) = \phi_2(\phi_1(\alpha x)) = \phi_2(\alpha . \phi_1(x)) =$$
$$= \alpha . \phi_2(\phi_1(x)) = \alpha . \phi_2 \circ \phi_1(x)$$

voor alle $\alpha \in K$ en $x \in E_1$.

Op analoge wijze bewijst men, in aansluiting op §4:

Stelling 3. Zij ϕ een 1-1-duidige lineaire afbeelding van E_1 op E_2. Dan is ϕ^{-1} een lineaire afbeelding van E_2 op E_1.

Stelling 4. Zij ϕ_1 een lineair isomorphisme van E_1 in E_2 en ϕ_2 een lineair isomorphisme van E_2 in E_3. Dan is $\phi_2 \circ \phi_1$ een lineair isomorphisme van E_1 in E_3.

Stelling 5. De lineaire automorphismen van een vectorruimte E vormen een groep t.o.v. de afbeeldings-compositie $\circ$.

Deze groep zullen we aangeven met GL(E), of, indien het nodig is ook het lichaam K te vermelden, met GL(E;K).

§ 13. Lineaire deelruimten

Definitie 1. Zij E een lineaire ruimte over K, en $L \subset E$. Men noemt L een lineaire deelruimte van E indien voldaan is aan de beide voorwaarden

(1) L is een ondergroep van E ;

(2) $x \in L,\ \alpha \in K \Rightarrow \alpha.x \in L$.

De lineaire deelruimten spelen in de lineaire algebra dezelfde rol als de ondergroepen in de groepentheorie (meer nog: zij spelen de rol van de normaaldelers; de additieve groep van E is immers commutatief, en in een commutatieve groep is iedere ondergroep normaaldeler).

Voorbeelden.

(a) De reële getallen en de zuiver imaginaire getallen vormen elk een lineaire deelruimte van C (als vectorruimte over R, of over Q). Evenzo alle getallen van de vorm a+bi met b = 2a.

(b) (vgl. §11, voorbeelden (d) en (e)). Over het lichaam der reële getallen is $D_n[a,b]$ steeds een lineaire deelruimte van iedere $D_m[a,b]$ met $0 \leq m \leq n$. Al deze ruimten zijn verder lineaire deelruimten van $R^{[a,b]}$.

(c) De oplossingsruimte E van de differentiaalvergelijking (11.7) (§11, voorbeeld f) is een lineaire deelruimte van $D_n[a,b]$.

(d) De polynomen over K met graad $\leq n$ vormen een lineaire deelruimte van $K[x]$ (vgl. §11, voorbeeld (k)).

Stelling 1. Zij E een lineaire ruimte over K, en zij $L \subset E$. Nodig en voldoende opdat L een lineaire deelruimte van E vormt is dat

$$\alpha x + \beta y \in L$$

voor alle $\alpha, \beta \in K$ en alle $x, y \in L$.

Bewijs.

We bewijzen slechts dat de genoemde voorwaarde voldoende is. Stel $x, y \in L$. Nemen we $\alpha = 1$, $\beta = -1$, dan volgt $x - y \in L$. Dus L is een ondergroep van E (§5, stelling 2). Nemen we α willekeurig en $\beta = 0$, dan volgt: $\alpha x \in L$. Dus L is een lineaire deelruimte.

In aansluiting aan §5 bewijst men verder eenvoudig:

Stelling 2. Stel E, F zijn lineaire ruimten over een lichaam K. Als ϕ: $E \to F$ een lineaire afbeelding is, dan is $\phi(E)$ een lineaire deelruimte van F.

Stelling 3. Stel E, F zijn lineaire ruimten over K, en stel E_0 is een lineaire deelruimte van E. Als ϕ: $E \to F$ lineair is, dan is ook $\phi \mid E_0$ een lineaire afbeelding van E_0 in F.

Gevolg. Onder de aannamen van stelling 3 beeldt ϕ iedere lineaire deelruimte van E af op een lineaire deelruimte van F.

Stelling 4. Zij ϕ een lineaire afbeelding van E in F (over het lichaam K). De kern $\phi^{-1}(0)$ van ϕ is een lineaire deelruimte van E.

Men noemt de kern van een lineaire afbeelding ϕ ook wel de nulruimte van ϕ.

Stelling 5. Zij E een lineaire ruimte over een lichaam K, en zij A een deelverzameling van E. Dan is er een kleinste lineaire deelruimte van E die A omvat.

De kleinste lineaire deelruimte van E die A omvat zullen we aangeven met H(A); we noemen H(A) het lineair omhulsel van A, of ook de lineaire deelruimte, opgespannen door A.
Als $x_1, x_2, \ldots, x_n \in A$ en $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, dan zal de vector $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ moeten behoren tot alle lineaire deelruimten die A omvatten; dus $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \in H(A)$. Omgekeerd vormen al deze lineaire combinaties van elementen uit A kennelijk een lineaire deelruimte van E. Dus:

Stelling 6. Zij E een vectorruimte over K en zij $A \subset E$. Dan bestaat H(A) uit alle lineaire combinaties van eindig veel elementen uit A.

Opmerking. Men zij zich bewust van het feit dat H(A) mede afhangt van het scalairenlichaam K.

Voorbeeld.

(e). In C, beschouwd als lineaire ruimte over zichzelf spant $A = \{i\}$ heel C op: $H(A) = C$. Beschouwen we C daarentegen als lineaire ruimte over R, dan bestaat het lineair omhulsel van $\{i\}$ uit alle zuiver imaginaire getallen.

Opgaven bij §§11, 12, 13.

1. Onder welke voorwaarden voor de verzameling T bestaat er een lineair homomorphisme van K^T op K?

2. Zij K een lichaam, E de lineaire deelruimte van $K[x]$ (beschouwd als vectorruimte over K) die bestaat uit alle polynomen van graad $\leq n$. Bewijs dat E lineair isomorph is met K^n.

3. Bewijs dat R^n dan en slechts dan lineair isomorph is met een lineaire deelruimte van R^m indien $n \leq m$.

4. Als ϕ een lineair homomorphisme is van K^{n+k} op K^n (beide beschouwd als lineaire ruimten over K), dan is de nulruimte van ϕ lineair isomorph met K^k. Bewijs dit.

5. Stel $[a,b]$ en $[c,d]$ zijn twee intervallen op de reële rechte. De lineaire ruimten $C[a,b]$ en $C[c,d]$ over R zijn lineair isomorph. Evenzo $D_n[a,b]$ en $D_n[c,d]$, voor iedere n. Bewijs dit.

6. Als $[c,d]$ een deelinterval is van $[a,b]$, dan is de afbeelding die aan $f \in C[a,b]$ toevoegt zijn restrictie $f|[c,d]$, een lineaire afbeelding van $C[a,b]$ op $C[c,d]$.
Bewijs dit. Wat is de kern van ϕ?

7. Stel E is een lineaire ruimte over K. Als E_1 en E_2 lineaire deelruimten zijn van E, dan is ook $E_1 + E_2 := \{x + y : x \in E_1, y \in E_2\}$ een lineaire deelruimte van E.

8. Stel E en F zijn lineaire deelruimten over K. Met $\mathcal{L}(E,F)$ zullen we aangeven de verzameling van alle lineaire afbeeldingen van E in F. Definieer in $\mathcal{L}(E,F)$ een optelling, en een vermenigvuldiging met de elementen uit K, op zodanige wijze dat $\mathcal{L}(E,F)$ wordt tot een vectorruimte over K.

9. Bewijs de uitspraken in voorbeeld (j) van §11.

10. Zij K een lichaam, $\alpha \in K$. De afbeelding ϕ, die aan $P \in K[x]$, zeg $P = \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \ldots + \gamma_n x^n$, toevoegt

$$\phi(P) = \gamma_0 + \gamma_1 \alpha + \gamma_2 \alpha^2 + \ldots + \gamma_n \alpha^n \in K$$

is een lineaire afbeelding van $K[x]$ op K. Wat is zijn kern?

11. Zij E een vectorruimte over K, en stel A en B zijn deelverzamelingen van E.

(1) als $A \subset B$, dan $H(A) \subset H(B)$;

(2) $H(A \cup B) = H(A) + H(B)$;

(3) $H(H(A)) = H(A)$;

(4) $A \subset H(A)$;

(5) Als $x \in H(A)$, dan is er een eindige deelverzameling A_0 van A waarvoor $x \in H(A_0)$.

§ 14. Lineaire afhankelijkheid en onafhankelijkheid. Basis.

In deze paragraaf is K een gegeven lichaam en E een lineaire ruimte over K.

Definitie 1. Een deelverzameling A van E heet lineair onafhankelijk indien

$$x \notin H(A \setminus \{x\}) \tag{14.1}$$

voor iedere $x \in A$. Indien A niet lineair onafhankelijk is, dan heet A lineair afhankelijk.

Stelling 1. A is dan en slechts dan lineair onafhankelijk indien uit

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0 \tag{14.2}$$

($x_1, x_2, \ldots, x_n$ onderling verschillende vectoren uit A; $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$) altijd volgt: $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

Bewijs.

a) Stel in (14.2) is bijvoorbeeld $\alpha_1 \neq 0$. Dan volgt dat

$$x_1 = \frac{\alpha_2}{-\alpha_1} x_2 + \frac{\alpha_3}{-\alpha_1} x_3 + \ldots + \frac{\alpha_n}{-\alpha_1} x_n \in H(A \setminus \{x_1\})$$

zodat A niet lineair onafhankelijk is.

b) Stel A is lineair afhankelijk; zij bijvoorbeeld $x_1 \in H(A\setminus\{x_1\})$, zeg

$$x_1 = \alpha_2 x_2 + \alpha_3 x_3 + \ldots + \alpha_n x_n,$$

met onderling verschillende $x_2, x_3, \ldots, x_n$ uit A en $\alpha_2, \alpha_3, \ldots, \alpha_n$ K. Dan geldt (14.2) met $\alpha_1 = -1 \neq 0$.

Gevolg 1. A is dan en slechts dan lineair onafhankelijk indien alle eindige deelverzamelingen van A lineair onafhankelijk zijn.

Gevolg 2. Als $0 \in A$ dan is A lineair afhankelijk.

Gevolg 3. Een eindige verzameling $A = \{x_1, x_2, \ldots, x_n\}$ ($x_i \neq x_j$ als $i \neq j$) is dan en slechts dan lineair afhankelijk als er scalairen $\alpha_1, \alpha_2, \ldots, \alpha_n$ bestaan, niet alle 0, waarvoor $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0$.

Stelling 2. Als A lineair onafhankelijk is, en $x_0 \notin H(A)$, dan is ook $A \cup \{x_0\}$ lineair onafhankelijk.

Bewijs.

Zij $A_0 = A \cup \{x_0\}$, en stel A_0 is lineair afhankelijk. Dan is er een $x_1 \in A_0$ met $x_1 \in H(A_0\setminus\{x_1\})$. Daar $x_0 \in H(A)$ is zeker $x_1 \neq x_0$. Zeg dat

$$x_1 = \alpha_0 x_0 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

met $x_2, x_3, \ldots, x_n \in A\setminus\{x_1\}$. Dan is $\alpha_0 \neq 0$, want anders zou reeds $x_1 \in H(A\setminus\{x_2\})$, d.w.z. dan was A niet lineair onafhankelijk. Maar dan volgt dat

$$x_0 = \alpha_0^{-1} x_1 - \alpha_0^{-1}\alpha_2 x_2 + \ldots + \alpha_0^{-1}\alpha_n x_n \in H(A),$$

in tegenspraak met de gegevens.

Stelling 3. Zij A lineair onafhankelijk. Iedere $x \in H(A)$ kan op één en (op volgorde-wijzigingen na) slechts één wijze geschreven worden als lineaire combinatie

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

met onderling verschillende $x_1, x_2, \ldots, x_n \in A$ en $\alpha_1 \neq 0, \alpha_2 \neq 0, \ldots$ $\alpha_n \neq 0$ uit K.

.....

Bewijs.

Ieder element $x \in H(A)$ is een lineaire combinatie van elementen uit A (zelfs als A niet lineair onafhankelijk is); we moeten dus alleen de ondubbelzinnigheid aantonen. Deze is een gevolg van het feit dat

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

en

$$x = \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_n x_n$$

($x_1, x_2, \ldots, x_n$ onderling verschillende vectoren uit A) impliceren dat

$$x - x = 0 = (\alpha_1 - \beta_1)x_1 + (\alpha_2 - \beta_2)x_2 + \ldots + (\alpha_n - \beta_n)x_n$$

waaruit weer volgt dat $\alpha_1 - \beta_1 = \alpha_2 - \beta_2 = \ldots = \alpha_n - \beta_n = 0$, d.w.z. $\alpha_1 = \beta_1; \alpha_2 = \beta_2; \ldots; \alpha_n = \beta_n$.

Definitie 2. Een basis voor E is een lineair onafhankelijke deelverzameling van A die geheel E opspant, d.w.z. waarvoor $H(A) = E$.

Uit stelling 3 volgt onmiddellijk:

Stelling 4. Zij A een basis voor E. Iedere $x \in E$ is op één en (op volgorde-wijzigingen na) slechts één wijze te schrijven in de vorm

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

met onderling verschillende $x_1, x_2, \ldots, x_n \in A$ en met coëfficiënten $\alpha_i \neq 0$.

Voorbeelden.

(a) In R^n vormen de n vectoren $e_1 = (1,0,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0)$, $\ldots$, $e_n = (0,0,\ldots,1)$ een basis.
In R^3 zijn de vectoren $x_1 = (-3,2,17)$, $x_2 = (1,0,-6)$ en $x_3 = (0,2,-1)$ lineair afhankelijk.

(b) In C, beschouwd als vectorruimte over R, is de verzameling $\{2 + 3i, 3 + 2i\}$ lineair onafhankelijk. Iedere $A \subset C$ met meer dan twee elementen is lineair afhankelijk.

(c) Voor iedere $\varepsilon \in (0,1]$ zij f_ε een continue reëelwaardige functie op $[0,1]$ met de eigenschap: $f_\varepsilon(t) \neq 0$ voor $0 \leq t \leq \varepsilon$; $f_\varepsilon(t) = 0$ voor $\varepsilon \leq t \leq 1$. Dan is $A = \{f_\varepsilon : 0 < \varepsilon \leq 1\}$ een oneindige lineair onafhankelijke deelverzameling van $C[0,1]$; A is geen basis.

Van zeer groot belang is de volgende stelling:

Stelling 5. Iedere lineaire ruimte E over een lichaam K heeft een basis.

Het bewijs van stelling 5, in het algemene geval, gebruikt één of andere vorm van het keuze-axioma (de Welordeningsstelling van ZERMELO of het Lemma van ZORN). Wij zullen slechts een bijzonder geval van stelling 5 bewijzen, nl. voor eindig-dimensionale E.

Definitie 3. Een lineaire ruimte E heet eindig-dimensionaal als er een eindige deelverzameling A van E bestaat met $E = H(A)$.

Bewijs van stelling 5 ingeval E eindig-dimensionaal is.
Zij A eindig en $E = H(A)$.
Als $0 \neq x \in A$, dan is de verzameling, die alleen uit x bestaat, lineair onafhankelijk. Als $A \subset H(x_1)$, dan is $H(x_1) = H(A) = E$, dus $H(x_1) = E$, dus $\{x_1\}$ is een basis.

Als zo niet, dan is er een $x_2 \in A \setminus H(x_1)$. Volgens stelling 2 is $\{x_1, x_2\}$ lineair onafhankelijk. Als $A \subset H(x_1, x_2)$, dan is weer $H(x_1, x_2) = E$, dus (x_1, x_2) een basis; zo niet, dan is er een $x_3 \in A \setminus H(x_1, x_2)$, enz. Daar A eindig is moet men na eindig veel stappen komen tot een lineair onafhankelijke verzameling $B = (x_1, x_2, \ldots, x_n) \subset A$ zodanig dat $A \subset H(B)$, zodat $H(B) = H(A) = E$; deze B is een basis voor E.