STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZC 18c

Avondcursus wiskunde 1950-1951;

Moderne algebra, 1;

C.G.Lekkerkerken.

1951

ZW

MATHEMATISCH CENTRUM
2de Boerhaavestr. 49
A M S T E R D A M O.

t/m blz. 15

Avondcursus 1950-1951.

Moderne algebra
door
C.G.Lekkerkerker

§1. Groepen.

Fundamenteel voor ons onderwerp is het begrip groep. Dit is reeds ter sprake gekomen in de cursus analyse (zie §1-3). Daar werd eerst (§1) in het algemeen over verzamelingen gesproken; later (§3) werd van een speciale verzameling elementen, n.l. de verzameling der gehele getallen (dat zijn dus positieve gehele getallen, negatieve gegehele getallen en het getal nul) onder meer aangetoond:

1. de optelling is een bewerking, die aan elk tweetal gehele getallen a en b op ondubbelzinnige wijze een geheel getal c toevoegt; we schrijven a+b=c

2. deze optelling is associatief: a+(b+c)=(a+b)+c

3. er is een element, n.l. het getal 0, met de eigenschap dat voor alle a geldt:

$$0+a=a.$$

4. bij elk getal a bestaat een eenduidig bepaald getal -a, zodat geldt a+(-a)=0.

We zeggen nu dat de gehele getallen één groep vormen t.a.v. de optelling. Beschouwen we de positieve rationale getallen, dan vormen die een groep t.a.v. de vermenigvuldiging. Immers daardoor wordt aan twee positieve rationale getallen ondubbelzinnig een derde positief rationaal getal toegevoegd; de vermenigvuldiging is associatief; er is een positief rationaal getal, n.l. het getal 1, zodat voor elke a geldt 1.a= a en zodat er bij elke a een omgekeerde $\frac{1}{a}$ is, waarvoor $\frac{1}{a}.a=1$ is. Algemeen definieren we:

Een groep is een niet lege verzameling G van elementen a,b,... met de volgende eigenschappen:

1. er is een compositieregel (operatie), die aan elk tweetal elementen a,b ondubbelzinnig een derde element toevoegt, dat meestal het product van a en b genoemd wordt en aangeduid wordt door ab

2. voor drie elementen a,b,c van G geldt: (ab)c=a(bc).

3. er is een eenheidselement e in G met de eigenschap:
ea=a voor alle a in G

4. bij iedere a van G bestaat een element a^{-1}, zodat geldt $a^{-1}a = a$; a^{-1} heet linksinverse van a

In bovengenoemde voorbeelden is de optelling resp. de vermenigvuldiging de compositieregel. We merken op dat bij het product de volgorde der factoren van belang is; ab en ba stellen beide een element van G voor wegens 1, maar hoeven niet gelijk te zijn. Wanneer in een groep steeds ab=ba is, zoals in bovengenoemde voorbeelden, heet de groep commutatief of Abels. In die voorbeelden is 0 resp. 1 het eenheidselement en -a resp. $\frac{1}{a}$ het inverse bij het element a.

Andere voorbeelden van groepen zijn:

1) de verzameling der reele of der rationale getallen met als operatie de optelling

2) de verzameling der complexe getallen $\neq 0$ met als operatie de vermenigvuldiging

3) de verzameling der getallen a+bi, a en b geheel, t.a.v. de optelling.

4) de verzameling der getallen $a+b\sqrt{2}$, waarin a en b rationaalien en niet tegelijk nul zijn, t.a.v. de vermenigvuldiging

5) de verzameling der draaiingen van het platte vlak om de oorsprong

6) de verzamelingen der draaingen van de ruimte om de oorsprong

7) de verzameling van de collineaties van het platte vlak

8) het stelsel van alle translaties van het platte vlak

9) het stelsel van de permutaties van n objecten.

In de gevallen 5) - 9) zijn de elementen der groep geen getallen maar transformaties. We moeten er nog bij zeggen wat hier de groepoperatie is. Wel, het product van twee elementen is natuurlijk de transformatie die verkregen wordt door eerst de ene en daarna de andere transformatie toe te passen. Wat de volgorde hierbij betreft, geldt de volgende afspraak, die op het eerste gezicht vreemd lijkt, maar toch handig blijkt te zijn: onder het product ab van twee elementen a en b, waarbij dus a de eerste en b de tweede factor is, verstaan we in de beschouwde gevallen de transformatie die ontstaat door achter elkaar eerst de tweede en daarna de eerste transformatie toe te passen. Voeren we in het platte vlak achter elkaar twee collineaties π_1 en π_2 uit, dan gaat daarbij een punt x eerst over in $y=\pi_1 x$, vervolgens in $z=\pi_2 y=\pi_2(\pi_1 x)$. En voor dit laatste nu mogen we, als we de collineatie die het product is van van π_1 en π_2 aanduiden door $\pi_2\pi_1$, ook schrijven $\pi_2\pi_1 x$. Hieraan ziet men dat de afspraak verstandig is.

We moeten nu nagaan dat in de gevallen 1)-9) aan de groepeigenschappen voldaan is. We doen dit voor de gevallen 4) em 6). In geval 4) hebben we

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2},$$

en daarbij zijn ac+ 2 bd en ad+ bc twee rationale getallen, niet beide gelijk aan nul, als hetzelfde geldt voor de paren a,b en c,d. De ver -

De vermenigvuldiging is associatief en zelfs commutatief omdat we met (reele)getallen te doen hebben. Als eenheidselement fungeert het getal 1. Tenslotte is gemakkelijk bij een getal $a+ b\sqrt{2}$ een getal $c+ d\sqrt{2} = (a+ b\sqrt{2})^{-1}$ te vinden, zodat geldt $(c+ d\sqrt{2})(a+ b\sqrt{2}) = 1$ en wel:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} = c+ d\sqrt{2};$$

hierbij hoeft de noemer $a^2 - 2b^2$ niet af te schrikken, want die kan niet 0 zijn voor $a, b \neq 0,0$.

Beschouwen we nu 6). Voert men achter elkaar twee draaiingen uit, dan krijgt men weer een draaiing; dus is er bij twee elementen van de verzameling steeds een derde element, dat het product daarvan is. De associativiteit volgt zo: laat bij drie draaiingen D_1, D_2, D_3 het punt x achtereenvolgens overgaan in y, z, u. Dan is

$$D_2D_1x = z \ , \ D_3(D_2D_1x) = D_3z = u$$
$$D_1x = y \ , \ (D_3D_2)(D_1x) = D_3D_2y = u \ ,$$

zodat de draaiingen $D_3(D_2D_1)$ en $(D_3D_2)D_1$ voor een willekeurig punt hetzelfde opleveren en dus identiek zijn. Als eenheidselement fungeert de identieke transformatie, d.i. de transformatie waarbij alle punten op hun plaats blijven. Als inverse van een draaiing D is te nemen de draaiing D^{-1} die juist het omgekeerde doet: voert D een punt x in y over, dan voert D^{-1} y in x over.

In 6) is de vermenigvuldiging niet commutatief. Want als b.v. D_1 en D_2 de rechtse draaiingen om de x-as resp. de y-as zijn over een hoek van 90°, dan wordt de positieve x-as door D_2D_1 in de positieve z-as en door D_1D_2 in de positieve y-as overgevoerd.

Opgave 1. Onderzoek de genoemde, doch niet behandelde voorbeelden.

Opgave 2. Bewijs dat de oneven getallen geen groep t.a.v. de optelling en de getallen $a + b\sqrt[3]{2}$ (a en b rationaal) geen groep t.a.v. de vermenigvuldiging vormen. Opgave 3: Onderzoek de complexe getallen met absolute waarde 1.

§2. Eigenschappen van groepen.

We gaan enige conclusies trekken uit de groepeigenschappen. We hebben het bestaan van een links-inverse en een eenheidselement geeist en er ons niet over uit gelaten, of er meer dan één links-inverse bestaat en of er ook rechts-inversen zijn enz. Nu kunnen we de volgende herleiding geven.

Wegens de associativiteit is $(a^{-1})^{-1}.a^{-1}a = (a^{-1})^{-1}a^{-1}.a$, of $(a^{-1})^{-1}e = ea = a$. Door rechtsvermenigvuldiging met a^{-1} komt er $(a^{-1})^{-1}e.a^{-1} = aa^{-1}$, of $(a^{-1})^{-1}.ea^{-1} = aa^{-1}$, dus $e = aa^{-1}$.

Dit laatste betekent dat a^{-1} tevens rechts-inverse is, of anders gezegd, dat a links-inverse is van a^{-1} en dat dus te nemen is $(a^{-1})^{-1} = a$ Dus geldt ook steeds $ae = a$.

Stel, dat een element a twee links-inversen b_1 en b_2 heeft. Dan geldt $b_1(ab_2) = b_1e = b_1$ en $(b_1a)b_2 = eb_2 = b_2$. Dus is $b_1 = b_2$.

Zijn e_1 en e_2 beiden eenheidselement, dan is $e_1e_2 = e_2$ en $e_1e_2 = e_1$, dus geldt $e_1 = e_2$.

Conclusie: in een groep heeft elk element één inverse, dat zowel links- als rechts-inverse is, en één eenheidselement (kort gezegd één), dat zowel links-één als rechts-één is. We mogen dus spreken van de inverse, de één.

Zijn a en b elementen van een groep G, dan zijn de vergelijkingen $ax = b$, $ya = b$ ondubbelzinnig oplosbaar. Want over de eerste vergelijking b.v. kunnen we zeggen: $x = a^{-1}b$ voldoet blijkbaar; voldoet x, dan krijgen we door beide leden links te vermenigvuldigen met a^{-1}: $x = a^{-1}ax = a^{-1}b$.
We kunnen het zo uitdrukken dat in een groep de deling ondubbelzinnig uitvoerbaar is.

Voor de inverse van een product geldt: $(ab)^{-1} = b^{-1}a^{-1}$. Want er geldt: $(b^{-1}a^{-1}).(ab) = b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$.

We willen nu laten zien dat we op grond van de groepoperatie ook een product van meer dan twee factoren kunnen definieren. We doen dit met een definitie door volledige inductie: zijn gegeven een willekeurig eindig aantal elementen $a_1,\ldots,a_n$ uit de groep, waarbij we op de volgorde der elementen letten, dan voegen we aldus hieraan een element $\prod_{\nu=1}^{n} a_\nu$ toe:

$$\prod_{\nu=1}^{1} a_\nu = a_1 \quad , \quad \prod_{\nu=1}^{k} a_\nu = \prod_{\nu=1}^{k-1} a_\nu \cdot a_k \qquad (k = 2,\ldots,n).$$

Voor $n = 2$ komt er a_1a_2, voor $n = 3$ krijgen we $(a_1a_2)a_3$, enz. We bewijzen met behulp van de associativiteit (groepeigenschap 2):

$$\prod_{\nu=1}^{m} a_\nu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\nu=1}^{m+n} a_\nu,$$

en wel met behulp van volledige inductie naar n. Voor $n = 1$ staat er bovenstaande definitie, met $m = k-1$. En is het bewezen voor een waarde n, dan volgt het gemakkelijk voor de waarde n+1:

$$\prod_{\nu=1}^{m} a_\nu \cdot \prod_{\nu=1}^{n+1} a_{m+\nu} = \prod_{\nu=1}^{m} a_\nu \cdot \Big(\prod_{\nu=1}^{n} a_{m+\nu} \cdot a_{m+n+1} \Big)$$
$$= \Big(\prod_{\nu=1}^{m} a_\nu \cdot \prod_{\nu=1}^{m} a_{m+\nu} \Big) a_{m+n+1}$$
$$= \prod_{\nu=1}^{m+n} a_\nu \cdot a_{m+n+1} = \prod_{\nu=1}^{m+n+1} a_\nu.$$

We merken nog op dat het element $\prod_{\nu=1}^{n} a_{m+\nu}$ vastgelegd is door onze definitie - even $a_{m+\nu}$ voor door b_ν. We geven het ook wel aan door $\prod_{\mu=m+1}^{m+n} a_\nu$. Heeft $\varphi(\nu)$ gehele waarden tussen 1 en n, dan ligt ook vast: $\prod_{\nu=1}^{n} a_{\varphi(\nu)}$.
Zijn verder k_1, k_2, l_1, l_2 natuurlijke getallen met $k_1+k_2 = n$, $l_1+l_2 = k_2$, dan is op grond van het bovenstaande:

$$\prod_{\nu=1}^{n} a_\nu = \prod_{\nu=1}^{k_1} a_\nu \cdot \prod_{\mu=k_1+1}^{k_1+k_2} a_\nu = \prod_{\nu=1}^{k_1} a_\nu \cdot \Big(\prod_{\mu=k_1+1}^{k_1+l_1} a_\nu \cdot \prod_{\mu=k_1+l_1+1}^{k_1+l_1+l_2=n} a_\nu \Big).$$

Dit is voort te zetten, wat we nu maar niet doen. Het ingevoerde symbool $\prod_{\nu=1}^{n}$ blijkt dus alle eigenschappen van een product te bezitten, en we

noemen het dan ook het product van de elementen $a_1,\ldots,a_n$. We mogen hierbij, als gevolg van de associativiteit, de vermenigvuldigingen in een willekeurige volgorde uitvoeren, mits we maar de volgorde der factoren in het oog houden. Zo mogen we b.v. voor n= 5 achtereenvolgens a_3 navermenigvuldigen met a_4, voorvermenigvuldigen met a_2, navermenigvuldigen met a_5, voorvermenigvuldigen met a_1. Schrijven we het product als $a_1a_2\ldots a_n$, dan hoeven we geen haakjes te plaatsen; we mogen b.v. zetten $a_1a_2a_3$.

In het bijzonder mogen de factoren a_ν van een product hetzelfde zijn, zeg a. We noemen het product dan een macht en schrijven:
$\prod_{\nu=1}^{n} a_\nu = \prod_{\nu=1}^{n} a = a^n$.
Uit een eigenschap, hierboven voor producten bewezen, volgt onmiddellijk: $a^m.a^n = a^{m+n}$. Verder kan men door volledige inductie bewijzen: $(a^m)^n = a^{mn}$.
Deze eigenschappen blijven doorgaan als we de definitie van de macht a^n aldus uitbreiden voor n= 0 resp. n=-m (m positief geheel):
$a^0 = e$, $a^n = a^{-m} = (a^{-1})^m$.
We bewijzen hier de relatie $a^m.a^n = a^{m+n}$(m,n geheel). Voor n= 0 luidt de bewering $a^m.a^0 = a^m$, ofwel $a^m e = a^m$; voor n= 0, en evenzo voor m= 0, is de bewering dus juist. Beschouwen we nu het geval n= 1. Voor m= 0, is dan de relatie vervuld, voor $m>0$ berust hij op de definitie, voor m= -1 volgt hij uit $a^{-1}.a = e = a^0 = a^{-1+1}$, en voor m= -p met $p>1$ geldt hij op grond van de herleiding:
$a^m.a = a^{-p}.a = (a^{-1})^p.a = (a^{-1})^{p-1}.a^{-1}.a = (a^{-1})^{p-1}e = (a^{-1})^{p-1} = a^{1-p}$.
Het geval n= -1 is hiertoe terug te brengen:
$a^m.a^{-1} = a^{m-1}.a.a^{-1} = a^{m-1}$.
Voor een willekeurige waarde van n tenslotte bewijzen we de relatie door volledige inductie. B.v. voor n negatief zetten we n= -q; dan is q positief en hebben we:
$$a^m.a^n = a^m.(a^{-1})^q = a^m(a^{-1})^{q-1}a^{-1} = a^m a^{1-q}.a^{-1}$$
$$= a^{m+1-q}.a^{-1} = a^{m-q} = a^{m+n}.$$
Het is vaak handig een product van 0 factoren tot zijn beschikking te hebben. We definieren: $\prod_{\nu=1}^{0} a_\nu = e$.

In een Abelse groep is een product onafhankelijk van de volgorde der factoren. Precies gezegd: is φ een eeneenduidige afbeelding van de verzameling getallen $\{1,2,\ldots,n\}$ op zichzelf, dan geldt:
$\prod_{\nu=1}^{n} a_{\varphi(\nu)} = \prod_{\nu=1}^{n} a_\nu$.
We bewijzen dit weer door volledige inductie. Voor n= 1 is de relatie een trivialiteit; is hij bewezen voor een waarde n, dan bewijzen we hem voor n+1 als volgt. Zij k het natuurlijke getal, waarvoor $\varphi(k) = n+1$ is (dus $1 \leq k \leq n+1$). Dan is
$$\prod_{\nu=1}^{n+1} a_{\varphi(\nu)} = \prod_{\nu=1}^{k-1} a_{\varphi(\nu)} . a_{\varphi(k)} \prod_{\nu=k+1}^{n+1} a_{\varphi(\nu)} = \prod_{\nu=1}^{k-1} a_{\varphi(\nu)} . \prod_{\nu=k+1}^{n+1} a_{\varphi(\nu)} a_{n+1}.$$
Definieert men een functie $\psi(\nu)$ als volgt:
$\psi(\nu) = \varphi(\nu)$ voor $1 \leq \nu < k$
$\psi(\nu) = \varphi(\nu+1)$ voor $n \geq \nu \geq k$,

dan is $\psi(\nu)$ een eeneenduidige afbeelding van de verzameling $\{1,\ldots,n\}$ op zichzelf en hebben we

$$\prod_{\nu=1}^{k-1} a_{\varphi(\nu)} \cdot \prod_{\nu=k+1}^{n+1} a_{\psi(\nu)} = \prod_{\nu=1}^{k-1} a_{\psi(\nu)} \cdot \prod_{\nu=k}^{n} a_{\psi(\nu)} = \prod_{\nu=1}^{n} a_{\psi(\nu)}.$$

Volgens inductieveronderstelling is dit laatste gelijk aan $\prod_{\nu=1}^{n} a_\nu$ en geldt dus:

$$\prod_{\nu=1}^{n+1} a_{\varphi(\nu)} = \prod_{\nu=1}^{n} a_{\psi(\nu)} \cdot a_{n+1} = \prod_{\nu=1}^{n} a_\nu \cdot a_{n+1} = \prod_{\nu=1}^{n+1} a_\nu .$$

In een Abelse groep schrijft men vaak, appellerend aan ons gevoel dat additie een commutatieve bewerking is, een product als een som. Men spreekt van tegengestelde i.p.v. inverse en schrijft

$$a_1 + a_2,\ a_1 + a_2 + a_3,\ \sum_{\nu=1}^{n} a_\nu,\ na,\ 0,\ -a$$

resp. i.p.v.

$$a_1 a_2,\ a_1 a_2 a_3,\ \prod_{\nu=1}^{n} a_\nu,\ a^n,\ e,\ a^{-1}$$

Let wel dat in deze notatie na niet het product van twee groepselementen is. Want enerzijds is n geen element uit de groep, maar een geheel getal; anderzijds betekent na het resultaat na enige malen uitvoeren der groepoperatie. De omtrent producten en machten bewezen eigenschappen luiden in de nieuwe notatie:

$$\sum_{\nu=1}^{k} a_\nu + \sum_{\nu=k+1}^{n} a_\nu = \sum_{\nu=1}^{n} a_\nu , \qquad \sum_{\nu=1}^{n} a_{\varphi(\nu)} = \sum_{\nu=1}^{n} a_\nu ;$$

$$ma + na = (m+n)a , \quad n.ma = nma.$$

We merken nog op, dat elk der hier bewezen eigenschappen voor elk der negen in §1 genoemde voorbeelden (en natuurlijk ook voor elk ander mogelijk voorbeeld) een uitspraak inhoudt. Het voordeel van onze behandelingsmethode is, dat eigenschappen van groepen eens en voorál bewezen worden, zonder dat men bij de bewijzen behoeft te denken aan de concrete betekenis der elementen. Dit is dus, naast het feit van de logische opbouw, het nut van onze abstracte opzet.

Opgaven 1. Bewijs de relatie $(a^m)^n = a^{mn}$.

2. Bewijs voor een Abelse groep: $a^m . b^m = (ab)^m$, m geheel.

3. Bewijs dat de groep van de permutaties van n objecten uit n! elementen bestaat.

§3. Ringen en lichamen.

Eigenschappen.

Sommige der in §1 genoemde voorbeelden bezitten eigenschappen, die niet logisch afhankelijk zijn van de vier, die als groepseigenschappen vooropgesteld werden. Het is van belang, op abstracte wijze verzamelingen te beschouwen, die aan meer eigenschappen voldoen, dan voor groepen geëist werd. In voorbeeld 1) kunnen we zowel optellen als vermenigvuldigen. Daar zijn dus twee compositieregels, met behulp waarvan men aan twee elementen een derde toe kan voegen. We gaan nu ringen en lichamen definieren.

Een ring R is een verzameling elementen , waarin twee compositieregels ondubbelzinnig uitvoerbaar zijn; t.a.v. de ene operatie, die als optelling geschreven wordt, is de verzameling een Abelse groep;

de andere, die als vermenigvuldiging geschreven wordt, is associatief, terwijl als eigenschappen,die beide operaties met elkaar in verband brengen, distributieve wetten gelden:

$$a(b+c)= ab+ac \quad , \quad (a+b)c= ac+bc,$$

als a,b,c willekeurige elemeneten uit R zijn.

Het eenheidselement van de Abelse groep, die bij een ring optreedt, heet het nulelement van de ring.

Een lichaam L is een ring, die ook t.a.v. de vermenigvuldiging een Abelse groep is, afgezien van het nulelement.

Men kan de volgende lijst opstellen van de definierende eigenschappen van ring resp. lichaam; a,b,c,x,y stellen hierbij steeds elementen uit de ring (het lichaam) voor:

Lichaam { Ring { 1. er is een ondubbelzinnig uitvoerbare optelling
2. er is een ondubbelzinnig uitvoerbare vermenigvuldiging
3. $a+(b+c)=(a+b)+c$
4. $a+b= b+a$
5. de vergelijking $a+x= b$ is steeds oplosbaar
6. $a(bc)=(ab)c$
7. $a(b+c)= ab+ac$
8. $(a+b)c= ac+bc$

9. de vergelijking $ax= b$ is steeds oplosbaar } mits a niet het nulelement v.d. ring is
10. de vergelijking $ya= b$ is steeds oplosbaar }
11. $ab=ba$.

Bewijs. Uit 5 volgt dat de vergelijking $a+x= a$ oplosbaar is voor een zeker element a. We noemen de oplossing 0. Voor willekeurige b is ook oplosbaar $a+x= b$; is x een oplossing dan mogen we op grond van 3 en 4 zetten $b+0= a+x+0=a+0+x=a+x= b$. Verder is $b+x= 0$ steeds oplosbaar. De verzameling in kwestie is dus alvast een Abelse groep op grond van 1, 3- 5, met 0 als eenheidselement. De eigenschappen 1-8 leveren dus een ring. Beschouwen we nu de eigenschappen 9 en 10, dan kunnen we aldus redeneren. Laat a een zeker element $\neq 0$ zijn. De vergelijking $ya= a$ heeft een oplossing, zeg e. Laat x voor een willekeurige b een oplossing van $ax= b$ zijn. Dan is $ea= a$, en ook $eb= e(ax)=(ea)x=ax= b$. Verder is $ya= e$ steeds oplosbaar. Dus de verzameling in kwestie is op grond van 9 en 10 ook een groep t.a.v. de vermenigvuldiging, en wel commutatief wegens 11, en daarmee een lichaam.

De aan het begin van §2 voor groepen bewezen eigenschappen leren ons: Het nulelement 0 van een ring is eenduidig bepaald; de vergelijking $a+x= b$ heeft één oplossing; ook de vergelijkingen 9 en 10 hebben voor $a\neq 0$ één oplossing. De oplossing van $a+x= 0$ wordt geschreven $-a$,

en heet het tegengestelde van a. Dan is $a+(-a)=0$ en is de oplossing van $a+x=b$ gelijk aan $b+(-a)$, want er geldt

$$a+b+(-a)=a+(-a)+b=0+b=b+0=b.$$

Deze oplossing wordt ook geschreven als $b-a$. Dan is ook $a-a=0$, voor alle a.

We kunnen nu gemakkelijk verdere eigenschappen van ringen afleiden. Allereerst gelden de distributiviteitswetten

$$a(b-c)=ab-ac \quad , \quad (a-b)c=ac-bc.$$

want er geldt:

$$a(b-c)+ac=a(b-c+c)=a\{b+c+(-c)\}=a(b+0)=ab,$$

zodat $a(b-c)$ de oplossing is van $x+ac=ab$, welke per definitie geschreven wordt als $ab-ac$. Evenzo wordt $(a-b)c$ behandeld.

Vervolgens tonen we aan: $a.0=0.a=0$.

Dit volgt uit $a.0=a.(a-a)=aa-aa=0$; $0.a=(a-a)a=aa-aa=0$.

Verder gelden de herleidingen:

$$(-a)b=a(-b)=-ab \quad ; \quad (-a).(-b)=ab.$$

Want we hebben b.v. $(-a)b+ab=(-a+a)b=0.b=0$. En ook $(-a).(-b)=-(a(-b))=-(-ab)=ab$ (zie ook analyse p.9).

Door volledige inductie naar n kunnen we uit 7 en 8 afleiden:

$$a\sum_{\mu=1}^{n} b=\sum_{\mu=1}^{n} ab_\mu \quad , \quad \sum_{\mu=1}^{n} a_\mu .b=\sum_{\mu=1}^{n} a_\mu b \quad ,$$

of, uitvoeriger genoteerd:

$$a(b_1+b_2+\ldots+b_n)=ab_1+ab_2+\ldots+ab_n,$$
$$(a_1+a_2+\ldots+a_n)b=a_1b+a_2b+\ldots+a_nb.$$

Geldt in een ring steeds $ab=ba$, dan heet de ring <u>commutatief</u>. We hebben al gezien dat het product ab gelijk aan 0 is, als een der factoren 0 is. Een element $a\neq 0$ heet nuldeler, en wel rechts-nuldeler, als er een element $b\neq 0$ is, zodat toch geldt: $ab=0$. Evenzo heet $b\neq 0$ <u>links-nuldeler</u>, als er een element $a\neq 0$ is, zodat $ab=0$ is. We zullen hier voorbeelden van zien. Een commutatieve ring, waarin geen nuldelers voorkomen, wordt <u>integriteitsgebied</u> genoemd.

<u>Stelling</u>. Een lichaam is een integriteitsgebied.

<u>Bewijs.</u> Zij $ab=0$ en b.v. $a\neq 0$. In het lichaam als groep t.a.v. de vermenigvuldiging heeft a een inverse a^{-1}. Door vermenigvuldiging met a^{-1} krijgen we $a^{-1}ab=a^{-1}.0$, ofwel $b=0$. Er kwamen dus geen nuldelers voor.

In een lichaam heet het eenheidselement t.a.v. de vermenigvuldiging eenheidselemenet zonder meer. Een lichaam heeft altijd een nul en een één, d.w.z. een lichaam bevat tenminste twee elementen.

In een ring hoeft geen eenheidselement aanwezig te zijn. Dit zal in §4 uit een voorbeeld blijken. Er kan wel een eenheidselement zijn; er kunnen zelfs meerdere zijn. We moeten hierbij noodzakelijk onderscheid tussen links-één en rechts-één maken. Bestaat er zowel een links-

één, d.i. een één e, met ex= x voor alle x, als een rechts-één e' met xe'= x voor alle x, dan zijn beide gelijk, wegens e= ee'= e'. In dit gevel kunnen er niet meer enen zijn! Maar wel bestaan er ringen met b.v. verschillende links-énen , en zonder rechts-één.

In een lichaam heeft elk element één inverse. In een ring hoeft dit niet zo te zijn. En als in een ring een bepaald element a een inverse heeft, hoeft het niet de enige te zijn, en moet er bovendien onderscheid gemaakt worden tussen links-inverse en rechts-inverse. Wel geldt dat,als er bij het element zowel een links-inverse a^{-1} als een rechts-inverse $a^{*-1}$is, die aan elkaar gelijk zijn, en dat a dan dus ook geen andere inversen heeft:

uit $a^{-1}a= e$, $aa^{*-1}= e$ volgt:

$$a^{-1}= a^{-1}(aa^{*-1})= (a^{-1}a)a^{*-1}= a^{*-1}$$

De aan het eind van §2 besproken eigenschappen kunnen we hier overnemen. We merkem op dat bij de bewijzen daarvan voor m, n positief geheel alleen gebruik gemaakt wordt van de groepeigenschappen 1 en 2. Dus geldt algemeen voor ringen:

$a^m.a^n= a^{m+n}$	$ma+na= (m+n)a$
$(a^m)^n= a^{mn}$	$m.na= mna$
$(ab)^n= a^nb^n$	$n(a+b)= na+nb$,
(m, n positief geheel)	benevens $n.ab= na.b= a.nb$.
	(m, n geheel)

De derde eigenschap links geldt alleen voor commutatieve ringen. Voor lichamen gelden de eigenschappen links voor willekeurige gehele m, n. We merken nog op, dat analoog aan §2 voor n= 0 resp. negatief geheel n a gedefinieerd is als 0 resp. -n a en dat in de uitdrukking n a het symbool n geen element van de ring, maar een geheel getal voorstelt.

Tenslotte merken we op, dat men ook lichamen beschouwt, waarvoor aan eigenschap 11 niet noodzakelijk voldaan is. Men spreekt dan van scheve lichamen.

Opgaven. 1. Een scheef lichaam is een ring.

2. In een scheef lichaam heeft elk element een inverse en is er een eenheidselement.
3. Een scheef lichaam heeft geen nuldelers.
4. In een integriteitsgebied volgt uit ab= ac en $a \neq 0$ de gelijkheid van b en c.
5. Een links-nuldeler bezit geen links-inverse, een rechts-nuldeler geen rechts-inverse
6. Kan een ring Q een inverse hebben?
7. Leid in een commutatieve ring af de formule
   $(a+b)(c+d)= ac+ad+bc+bd$
   en leid daarna door volledige inductie het binomium van Newton af.

§ 4. Voorbeelden van ringen en lichamen.

Ringen worden gevormd door o.a.

10) de gehele getallen } t.a.v. optelling en vermenig-
11) de getallen a+bi met a,b geheel } vuldiging.

Lichamen worden o.a. gevormd door

12) de rationale, de reële, de complexe getallen, of ook de getallen $a+b\sqrt{2}$ met a en b rationaal, alles t.a.v. de optelling en de vermenigvuldiging.

13) Te beschouwen de verzameling der polynomia

$$P_n(x) = a_0+a_1x+\ldots+a_nx^n = \sum_{\nu=0}^{n} a_\nu x^\nu$$

waarin de coefficienten $a_0,a_1,\ldots,a_n$ reële getallen zijn en x een reële veranderlijke is. Optelling of vermenigvuldiging van twee polynomia geeft weer een polynomium:

$(a_0+a_1x+\ldots+a_nx^n)+(b_0b_1x+\ldots+b_mx^m)=$
$=c_0+c_1x+\ldots+c_px^p$ met $p = \text{Max}(n,m)$, $c_0=a_0+b_0$, $c_1=a_1+b_1$, enz;
$(a_0+a_1x+\ldots+a_nx^n)(b_0b_1x+\ldots+b_mx^m)=$
$=a_0b_0+(a_0b_1+a_1b_0)x+\ldots+(a_0b_m+\ldots+a_mb_0)x^m+\ldots = $
$=c_0+c_1x+\ldots+c_{m+n}x^{m+n}$ met $c_0 = a_0b_0$, enz.

Deze polynomia vormen blijkbaar een ring met o als nul, 1 als één.

14) De even getallen, en evenzo de polynomia in b.v. een reële veranderlijke x en met even getallen als coëfficiënten, vormen een ring zonder eenheidselement.

15) In 13) construeerden we een ring van polynomen. We willen nu abstracte polynoomringen beschouwen. We gaan nu i.p.v. de reële getallen uit van een willekeurige ring R. En we beschouwen rijen van elementen van R, zodanig dat slechts een eindig aantal niet gelijk aan nul zijn:

$\pi = (p_0,p_1,\ldots,p_n,o,o,\ldots)$.
$\varrho = (q_0,q_1,\ldots,q_m,o,o,\ldots)$.

Allereerst stellen we vast dat twee rijen alleen dan gelijk heten, als ze elementsgewijs overeenstemmen. We kunnen voor deze rijen optelling definiëren:

$\pi + \varrho = \tau = (t_0,t_1,t_2,\ldots)$ met $t_i=p_i+q_i$,

waarbij $p_i=o$ is voor $i > n$ en $q_i = o$ is voor $i > m$, dus $t_i = o$ is voor $i > m,n$, en vermenigvuldiging met een element uit de ring R:

$\pi a = (p_0a,p_1a,\ldots,p_na,o,o,\ldots)$
resp. $a\pi = (ap_0,ap_1,\ldots,ap_n,o,o,\ldots)$.

Wat we zo krijgen, heeft nog niet veel te maken met een polynoomring; het is geen ring, omdat we nog geen voorschrift hebben om twee rijen van elementen met elkaar te vermenigvuldigen. Wel is het een groep, zoals men gemakkelijk kan nagaan, en wel een Abelse groep waarin de groepoperatie additief geschreven is, en met als eenheidselement de rij (o,o,o,...).

Om een ring te krijgen, gaan we nu, op een manier die uit 13) duidelijk zal zijn, het product van twee rijen van elementen definiëren. En wel zal zijn

$$\pi\rho = \sigma = (s_0, s_1, s_2, \ldots),$$

waarin $s_i = \sum_{k+l=i} p_k q_l$.

Men controleert gemakkelijk de distributieve wetten en de associativiteit van de vermenigvuldiging. Want stellen we

$$\pi = (p_0, p_1, \ldots, p_n, o, o, \ldots)$$
$$\rho = (q_0, q_1, \ldots, q_m, o, o, \ldots)$$
$$\sigma = (s_0, s_1, \ldots, s_r, o, o, \ldots),$$

dan is enerzijds b.v.

$$(\pi + \rho)\sigma = (t_0, t_1, t_2, \ldots)$$

met $t_i = \sum_{k+l=i} (p_k + q_k) s_l$

$$= \sum_{k+l=i} (p_k s_l + q_k s_l) = \sum_{k+l=i} p_k s_l + \sum_{k+l=i} q_k s_l$$

$$= t_i' + t_i'',$$

zodat geldt

$$(\pi + \rho)\sigma = (t_0, t_1, t_2, \ldots) = (t_0' + t_0'', t_1' + t_1'', t_2' + t_2'', \ldots)$$
$$= (t_0', t_1', t_2', \ldots) + (t_0'', t_1'', t_2'', \ldots)$$
$$= \pi\sigma + \rho\sigma,$$

en anderzijds vindt men door uitrekenen:

$$(\pi\rho)\sigma = (u_0, u_1, u_2, \ldots)$$

met $u_i = \sum_{k+l+j=i} (p_k q_l) s_j = \sum_{k+l+j=i} p_k (q_l s_j)$,

dus

$$(\pi\rho)\sigma = \pi(\rho\sigma).$$

We merken op dat in de hierboven optredende rijen steeds slechts een eindig aantal elementen van nul verschillen en dat de optredende sommatievariabelen alleen niet-negatief gehele waarden aannemen. Als R geen commutatieve ring is, is de nieuwe ring ook niet commutatief: $\pi\rho$ hoeft niet gelijk te zijn aan $\rho\pi$ als niet steeds $p_k q_l = q_l p_k$ is. Is de ring R daarentegen commutatief, dan is de nieuwe ring het ook.

Verder wijzen we er op, dat de verzameling van de beschouwde rijen van elementen van R in feite de verzameling is van de uitdrukkingen

$$p_0 + p_1 x + \ldots + p_n x^n;$$

hierbij is x geen getal, ook geen veranderlijke of een stelsel van mogelijke grootheden, zoals men in voorbeeld 13) nog zou kunnen volhouden maar louter een symbool, met behulp waarvan men uitdrukkingen als bovenstaande kan vormen, die zekere axiomatisch vastgelegde wetmatigheden vertonen. We beschouwen alle uitdrukkingen, waarbij de p 's elementen van R

zijn en maken optelling en vermenigvuldiging mogelijk, met,de gewenste uitkomsten, door x op te vatten als een grootheid, die men zo vaak men wil met zichzelf kan vermenigvuldigen, waarbij dus geldt: $x^k x^l = x^{k+l}$ (k,l natuurlijke getallen), terwijl verder mogelijk is de vermenigvuldiging van x met een ringelement, en wel associatief en commutatief; tenslotte wordt distributiviteit geeist. Dus is b.v.

$(p_0+p_1x)\cdot q_1x = p_0\cdot q_1x+p_1x\cdot q_1x$

$=p_0q_1\cdot x+p_1\cdot xq_1\cdot x = p_0q_1x + p_1q_1x.x$

$=p_0q_1\cdot x+p_1q_1\cdot xx = p_0q_1\cdot x+p_1q_1x^2$.

Hoewel het in feite, d.w.z. wat de rekenregels betreft geen verschil maakt, of we afbrekende rijen van elementen of formeel gevormde polynomen beschouwen, zullen we toch als concessie aan ons gevoel de analogie in schrijfwijze met 13) bewaren en ons aan het laatste houden. En we zeggen, dat de nieuwe ring ontstaan is uit R door adjunctie van een onbepaalde x; we geven de nieuwe ring aan door R[x].

16) We borduren nog even voort op de in 15) ter sprake gekomen Abelse groep, en nemen aan dat de ring R een eenheidselement heeft, dat zowel links- als rechts -één is. Als we nu de algemene productdefinitie uit 15) achterwege laten, dan kunnen we van deze Abelse groep, zeg G, toch wel het volgende zeggen. Er bestaat een ring, n.l. R, zodanig dat we een element π van G kunnen links- en rechtsvermenigvuldigen met elementen a,b uit die ring. Hierbij gelden op grond van de eigenschappen van R de volgende kenmerken:

1^o. πa en $a\pi$ zijn elementen van G

2^o. $\pi(a+b)= \pi a+ \pi b$; $(a+b)\pi = a\pi + b\pi$

3^o. $(\pi + \rho)a = \pi a+ \rho a$; $a(\pi + \rho)= a\pi + a\rho$

4^o. $(ab)\pi = a(b\pi)$; $\pi(ab)=(\pi a)b$

5^o. er bestaat een rij elementen $\pi_1, \pi_2, \ldots$ in G, zodanig dat een willekeurig element π uit G op één en slechts één manier geschreven kan worden als een eindige som

$\pi = a_1\pi_1+a_2\pi_2+\ldots+a_n\pi_n$

of $\pi = \pi_1 a_1+ \pi_2 a_2+\ldots+ \pi_n a_n$.

Om het laatste in te zien kiezen men, als 1 de één van R is,

$\pi_1=(1,o,o,\ldots)$, $\pi_2=(o,1,o,\ldots),\ldots,$

$\pi_k=(o,o,o,\ldots,o,1,o,\ldots)$ met op de k^{de} plaats 1 en verder o.

Is nu $\pi =(p_o,p_1,\ldots,p_1o,o,\ldots)$,

dan is blijkbaar

$\pi = p_o\pi_1+p_1\pi_2+\ldots+p_l\pi_{l+1}= \pi_1p_o+ \pi_2p_1+\ldots+ \pi_{l+1}p_l$.

Geld nu ook b.v.

$\pi =p'_o\pi_1+p'_1\pi_2+\ldots+p'_m\pi_{m+1}$,

dan was $\pi=(p_o,p_1,\ldots,p_1,o,o,\ldots)=(p'_o,p'_1,\ldots,p'_m,o,o,\ldots)$.

En dus $p_o=p'_o, p_1=p'_1$, enz, , omdat twee elementrijen alleen dan als gelijk beschouwd worden, als ze elementsgewijs overeenstemmen.

Men noemt algemeen een Abelse groep G, waarbij een ring R met één bestaat, zodat aan 1^0-5^0 voldaan is, een lineaire ruimte over die ring. De eis 5^0 houdt hierbij in, dat een element van de ruimte om zo te zeggen "coördinaatsgewijs" geschreven kan worden. Wegens 2^0 krijgt men de som van twee elementen door de "coördinaten" op te tellen. Vermenigvuldiging met een element van R wordt op grond van 3^0 en 4^0 verkregen, doordat men coördinaatsgewijs vermenigvuldigt:

$$b\,\pi = b(a_1\,\pi_1+a_2\,\pi_2+\ldots+a_n\,\pi_n)$$
$$= b(a_1\,\pi_1)+b(a_2\,\pi_2)+\ldots+b(a_n\,\pi_n)$$
$$= (ba_1)\,\pi_1 + (ba_2)\,\pi_2 +\ldots+ (ba_n)\,\pi_n.$$

Al naar men links- of rechtsvermenigvuldigt, moet men de eerste of de tweede voorstelling in 5^0 gebruiken. Het eenheidselement van de groep G heeft alle coördinaten 0. Verkregen we aanvankelijk onze lineaire ruimte als systeem van alle afbrekende rijen van elementen uit R, bij ons algemeen, aan 't begin van deze alinea gekozen, uitgangspunt verschijnt hij als het systeem van alle eindige sommen $a_1\,\pi_1+a_2\,\pi_2+\ldots+a_n\,\pi_n$, waarbij de π's een vaste rij van elementen uit de ruimte vormen. In beide gevallen zijn blijkbaar coördinaten en rekenregels dezelfde. Evenals in 15) het geval was, zijn er alleen formele verschillen.

17) Een eindigdimensionale lineaire ruimte over de ring R, zeg een n-dimensionale (n een natuurlijk getal) verkrijgt men als men alleen die elementrijen toelaat, waarin slechts de eerste n elementen van 0 kunnen verschillen. De lineaire ruimte in 16) heet oneindigdimensionaal. Dezelfde eigenschappen gelden; alleen moet in 5^0 de rij door een eindige rij, met n elementen, vervangen worden. Vanuit ons standpunt onderwerpt de gewone Analytische Meetkunde het geval, dat n gelijk is aan 3 en voor de grondslag liggende ring R de verzameling der reële getallen genomen wordt, aan een verdergaand onderzoek.

18) In het eindigdimensionale geval is het niet zo gemakkelijk, om zoals in 15) gebeurde, voor twee elementrijen een productdefinitie te geven. De daar gegeven definitie is niet bruikbaar, omdat alles moet afbreken bij iedere n. Toch is er soms wel iets aan te doen en is er een zodanige definitie van product te geven, dat distributiviteit en associativiteit, evenals toen, bewaard blijven. We behandelen hier de invoering van de quaternionen. We kiezen n = 4, R = lichaam van de reële getallen, en noemen π_1, π_2, π_3, π_4 nu e,j,k,l. Leggen we van deze vier elementen de producten onderling vast, en eisen we verder distributiviteit en associativiteit en verwisselbaarheid van elk dier vier elementen met de coördinaten (reële getallen), dan is

$$(a_1e+a_2j+a_3k+a_4l)(b_1e+b_2j+b_3k+b_4l)$$
$$= a_1e.b_1e+\ldots+a_4l.b_4l$$
$$= (a_1b_1)e^2+\ldots+(a_4b_4)l^2,$$

en is dus algemeen het product van twee elementen vastgelegd. En als maar de productvorming van die vier elementen onderling associatief is, dan is vanzelf de productvorming van willekeurige elementen associatief en distributief. We stellen nu:

$ee = e$; $jj=kk=ll=-e$

$ej=je=e$, $ek=ke=k$, $el=le=l$

$jk=l, kl=j, lj=k$

$kj=-l$, $lk=-j$, $jl=-k$

Men kan zelf nagaan, dat de vermenigvuldiging van deze elementen associatief is.

We merken nog op, dat de vermenigvuldiging blijkbaar niet commmutatief is. De quaternionen vormen dus een niet- commutatieve ring.

Men kan de complexe getallen op dezelfde manier invoeren, door n.l. $n = 2$ te nemen, uit te gaan van 1 en i en te stellen $1.i = i.1 = i, i^2 = -1$. De elementen worden nu a+bi. Er is nu commutativiteit. De complexe getallen vormen zelfs een lichaam, zie 12), want we kunnen delen.

Van de quaternionen kunnen we verder aantonen, dat ze zelfs een schoef lichaam vormen. Om dit in te zien, hebben we de volgende herleiding nodig:

$$(a_1e+a_2j+a_3k+a_4l)(a_1e-a_2j-a_3k-a_4l)$$
$$=a_1^2e+a_1a_2j-a_1a_2j+a_2^2e-\ldots-a_4^2e=(a_1^2+a_2^2+a_3^2+a_4^2)e$$

Zijn nu gegeven twee quaternionen

$$q_1=a_1e+a_2j+a_3k+a_4l,\quad q_2=b_1e+b_2j+b_3k+b_4l$$

en stellen we voor 't gemak

$$N=a_1^2+a_2^2+a_3^2+a_4^2$$

dan is

$$q_1\cdot\left(\left(\frac{a_1}{N}e-\frac{a_2}{N}j-\frac{a_3}{N}k-\frac{a_4}{N}l\right).q_2\right)$$
$$=\left(q_1.\left(\frac{a_1}{N}e-\frac{a_2}{N}j-\frac{a_3}{N}k-\frac{a_4}{N}l\right)\right)q_2$$
$$=\frac{N}{N}e.q_2=e(b_1e+b_2j+b_3k+b_4l)=b_1e+b_2j+b_3k+b_4l=q_2$$

en evenzo

$$\left(q_2\left(\frac{a_1}{N}e-\frac{a_2}{N}j-\frac{a_3}{N}k-\frac{a_4}{N}l\right)\right).q_1=q_2.$$

Dus de vergelijkingen $q_1x=q_2$, $yq_1=q_2$ zijn oplosbaar, mits $N\neq 0$ is, d.w.z. mits niet a_1,a_2,a_3,a_4 allen gelijk aan nul zijn, d.w.z. mits $q_1\neq 0$ is. Het is verder duidelijk, dat e het eenheidselement is.

§5. Verder voorbeelden.

19) We grijpen terug op 15). Daar is door adjunctie uit een willekeurige ring R de polynoomring $R[x]$ geconstrueerd. Omdat de ring R willekeurig is, mogen we ook aan de ring $R[x]$ een nieuwe onbepaalde

adjungeren. We kunnen zelfs achtereenvolgens n onbepaalden $x_1, x_2, \ldots, x_n$ adjungeren en krijgen zo een ring $R[x_1][x_2]\ldots[x_n]$, die als elementen bevat alle eindige sommen $\sum a_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ met $a_{k_1 k_2 \ldots k_n}$ in R. In deze som doorlopen $k_1, k_2, \ldots k_n$ onafhankelijk van elkaar ieder een eindig aantal waarden, b.v. $k_1 = 0,1,2,\ldots,k_1$; $k_n = 0,1,2,\ldots,k_n$; is in bepaalde term van de som $k_i = 0$, dan laten we de factor $x_i^{k_i}$ weg. We spreken nog af dat we in een product de onbepaalden onderling mogen verwisselen. We bereiken daarmee dat het er niet toe doet in welke volgorde we de onbepaalden adjungeren. Met het oog daarop geven we de ring ook wel aan door $R[x_1, x_2, \ldots, x_n]$. De eerste symbolick uit 15) voeren we hier niet door, want dat zou te ingewikkeld worden; en we komen daarmee toch in feite op dezelfde ring uit, juist dank zij de verwisselbaarheid der onbepaalden.

20) We gaan nu een heel ander type ring bestuderen. We gaan uit van de ring der gehele getallen, zie 10). We kiezen een natuurlijk getal m. Is nu a een willekeurig geheel getal, dan richten we onze aandacht op de verzameling der gehele getallen b die met a een geheel veelvoud van m verschillen. We voeren hiervoor de notatie in:

$b \equiv a \pmod m$, korter $b \equiv a(m)$,

en lezen dit als:

b is congruent met a modulo (naar de modulus) m.

En het betekent dus, dat we kunnen schrijven

$b-a = vm$, waarin v een geheel getal is.

De eerste bewering is nu, dat de relatie: congruent zijn modulo m een klasseindeling van de gehele getallen teweegbrengt. Zie voor het begrip klasse de cursus analyse, § 4. Er geldt n.l., zoals men inziet door te letten op de zojuist gegeven definitie:

$a \equiv a(m)$

$a \equiv b(m) \rightarrow b \equiv a(m)$

$a \equiv b(m),\ b \equiv c(m) \rightarrow a \equiv c(m)$.

Een klasse is ons geval de verzameling der b, die congruent met a modulo m zijn. Er zijn een zeker aantal klassen, die geen getal gemeen hebben en die tezamen alle gehele getallen bevatten.

De tweede bewering is, dat er precies m van zulke klassen zijn en dat elke klasse één representant bezit onder de rij getallen $0,1,\ldots,m-1$. Deze bewering volgt uit het feit, dat twee getallen uit de genoemde rij geen veelvoud van m verschillen, en dat het getal $b-vm$ tot die rij behoort als we kiezen $v = \left[\frac{b}{m}\right]$.

Vervolgens vatten we onze klassen als elementen van een verzameling op, waarvoor we optelling en vermenigvuldiging gaan definieren. We