

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1951 - 026

Voordracht in de serie Actualiteiten

Dr. W. Peremans

22 december 1951

Meta Mathematische beschouwingen over de algebra



Voordracht door Dr W. Peremans in de serie
Actualiteiten op 22 December 1951.

Metamathematische beschouwingen over de algebra.

Deze voordracht is geïnspireerd door de verschijning van het boek:
A. Robinson, On the metamathematics of algebra (in de serie Studies in
logic and the foundations of mathematics), Amsterdam 1951.

In de abstracte algebra houdt men zich bezig met systemen zoals
groepen, ringen, lichamen, tralies (lattices). Al deze systemen hebben
dit gemeen, dat het verzamelingen zijn, waarin bepaalde operaties (b.v.
optelling, vermenigvuldiging) zijn gedefinieerd, en die aan zekere axi-
oma's voldoen. Men kan al deze algebraïsche systemen dus beschouwen als
speciale gevallen van het volgende.

Een algebraïsch systeem is een verzameling met daarbij behorend
een verzameling operaties. Deze operaties zijn functies van n verander-
lijken (n een natuurlijk getal afhankelijk van de operatie) $O(x_1, \dots, x_n)$,
die aan ieder geordend n -tal elementen van het systeem een element
van het systeem toevoegen. De machtigheid van de verzameling operaties
behoeft niet eindig te zijn. In een bepaalde discussie beschouwen we
klassen van gelijksoortige algebraïsche systemen. Twee algebraïsche sys-
temen heten gelijksoortig als er een eeneenduidige betrekking bestaat
tussen de operaties, dusdanig dat de corresponderende relaties hetzelfde
aantal veranderlijken hebben. Het is dan gebruikelijk de overeenkom-
stige operaties met elkaar te identificeren (ze dezelfde naam te geven).
Zo zijn twee ringen als systemen met optelling en vermenigvuldiging ge-
lijksoortig.

Niet alle in de abstracte algebra gebruikelijke systemen vallen
hieronder. Neem eerst het begrip geordend lichaam. Daarin is een relatie
 $a \leq b$ gedefinieerd, die voor sommige paren wel en voor andere niet geldt.
Hiervan is echter wel een operatie te maken door een binaire operatie
 $O(a, b)$ in te voeren, zodat $O(a, b) = 0$ als $a \leq b$ en $O(a, b) = 1$ als
 $a \not\leq b$ (hierin zijn 0 en 1 de nul en de één van het beschouwde lichaam).
Moeilijker wordt de zaak in een gewaardeerd lichaam. De waarderingfunc-
tie $w(a)$ is geen operatie in de zin zoals hierboven gedefinieerd, daar
de functiewaarde in een ander lichaam dan het beschouwde gewaardeerde
lichaam kan liggen.

We moeten nu nog iets opmerken over de aard van de axioma's. In de

eenvoudigste systemen hebben deze axioma's de vorm van gelijkheden (b.v. de associatieve eigenschap $x(yz) = (xy)z$), waarbij de leden van deze gelijkheden opgebouwd zijn door iteratieve toepassing van de operaties op veranderlijken. Het axioma eist dan, dat bij iedere substitutie van elementen voor de veranderlijken beide leden in hetzelfde element overgaan. Iets ingewikkelder vormen van axioma's krijgt men door op deze gelijkheden nog logische operaties toe te passen, en wel in eerste instantie de operaties uit de propositielogica, dus "en", "of", "niet" en "uit ... volgt". Een stap verder kan men nog gaan door niet alleen propositielogica, maar ook beperkte praedicatenlogica (elementaire logica) toe te passen, waarbij de veranderlijken in de formules nu ook door existentiële quantificatoren kunnen worden gebonden. Een voorbeeld van een dergelijk axioma is het axioma, dat in een multiplicatief systeem het bestaan van een eenheidselement postuleert: er bestaat een x , zodat voor alle y geldt $xy = y$ en $yx = y$.

Ons doel is nu met behulp van methoden en resultaten van de symbolische logica stellingen over dergelijke algebraïsche systemen af te leiden. Hiertoe moeten we evenwel het voorafgaande nog verder in logische taal vertalen. De algebraïsche systemen zijn op te vatten als modellen van de bijbehorende systemen van axioma's. Nu zijn de axioma's nog niet van een vorm als in de logica gebruikelijk, omdat de operaties geen logische relaties zijn. Nu is van een operatie makkelijk een relatie te maken. B.v. kunnen we aan de binaire operatie van de optelling de ternaire relatie $S(a,b,c)$ toevoegen, die juist is als $c = a + b$ en onjuist als $c \neq a + b$. Evenzo voegen we aan de operatie $O(x_1, \dots, x_n)$ toe de relatie $O'(x_1, \dots, x_{n+1})$, die juist is als $x_{n+1} = O(x_1, \dots, x_n)$ en onjuist als $x_{n+1} \neq O(x_1, \dots, x_n)$. Omgekeerd behoeft bij een $(n+1)$ -aire relatie op deze wijze niet een operatie te behoren. Opdat dit voor de relatie $O'(x_1, \dots, x_n, x_{n+1})$ wel het geval is, moet bij iedere keuze van $x_1, \dots, x_n$ één en slechts één x_{n+1} behoren, zodat $O'(x_1, \dots, x_n, x_{n+1})$ juist is. Om dit in logische termen te formuleren, moet ook de gelijkheidsrelatie in het logische systeem opgenomen zijn. We nemen daarom een relatie $E(x,y)$, die voldoet aan de reflexieve, symmetrische en transitieve eigenschappen en die verder de substitutiviteitseigenschap bezit t.o.v. alle andere relaties:

$$(1) (\forall x_1) \dots (\forall x_n)(\forall y_1) \dots (\forall y_n)((R(x_1, \dots, x_n) \wedge E(x_1, y_1) \wedge \dots \wedge E(x_n, y_n)) \rightarrow R(y_1, \dots, y_n)).$$

Dan correspondeert met een relatie $O'(x_1, \dots, x_{n+1})$ een operatie, als geldt:

$$(2) (\forall x_1) \dots (\forall x_n)(\exists x_{n+1}) O'(x_1, \dots, x_n, x_{n+1}),$$

$$(3) (\forall x_1) \dots (\forall x_n)(\forall z)(\forall u)((O'(x_1, \dots, x_n, z) \wedge O'(x_1, \dots, x_n, u)) \rightarrow$$

vende inleiding, waarin we nog slordig hebben omgesprongen met de onderscheiding tussen een deductief logisch systeem (een "taal") en een realisering hiervan in een verzameling met relaties (een "model").

Een taal L wordt gedefinieerd met behulp van een vaste verzameling objectsymbolen (van een willekeurige doch vaste machtigheid), een aftelbare verzameling van symbolen voor objectveranderlijken ("dummy symbols") en een vaste verzameling van relatiesymbolen, waarbij iedere relatie een bepaald geheel getal $n \geq 0$ als orde bezit (de orde is het aantal lege plaatsen in het relatiesymbool). Hiermee wordt op de bekende wijze een praedicatenlogica opgebouwd met welgevormde formules, deductie-axioma's en afleidingsregels. Het feit dat we ons tot de beperkte praedicatenlogica beperken, komt tot uitdrukking in het feit, dat we wel objectveranderlijken maar geen relatieveranderlijken hebben. Een welgevormde formule, waarin alle veranderlijken door quantificatoren gebonden zijn, heet een bewering (statement). Als K een verzameling beweringen is, noemen we de verzameling der beweringen die uit de beweringen van K afleidbaar zijn, $S(K)$.

Laat nu M een verzameling zijn, waarop een verzameling V van relaties is gedefinieerd en laat er een eeneenduidige betrekking C zijn tussen de elementen van M en sommige objectsymbolen van L en tussen de relaties uit V in M en sommige relatiesymbolen in L , waarbij de orde van corresponderende relaties en relatiesymbolen dezelfde is. (Als de machtigheid van de verzameling der objectsymbolen in L niet groot genoeg is om een eeneenduidige betrekking met de elementen van M toe te laten, moeten we de taal eerst uitbreiden; we gaan daarop hier niet in) We kunnen dan met iedere bewering in L , die uitsluitend objectsymbolen en relatiesymbolen bevat, die in de betrekking C optreden (en bovendien nog symbolen voor veranderlijken) op de bekende wijze een bewering over elementen van M laten corresponderen, die juist is of niet. M heet een model van K als met alle beweringen van K juiste beweringen in M corresponderen. M is dan ook een model van die bewering uit $S(K)$, die alleen objectsymbolen en relatiesymbolen bevatten, die in de betrekking C optreden.

Een zeer belangrijk hulpmiddel bij de discussie van algebraïsche systemen met behulp van deze methode is de volledighedsstelling van Gödel, die als volgt te formuleren is.

Als K een consistente verzameling beweringen in een taal L is (d.w.z. $S(K)$ bevat niet alle beweringen van L), dan bestaat er een model van K .

Het omgekeerde van deze stelling is triviaal.

Uit de volledighedsstelling van Gödel volgen de beide volgende stellingen.

Als voor iedere verzameling M met relaties en iedere eeneenduidige correspondentie C , waarvoor de bewering X uit L alleen object- en relatiesymbolen bevat, die in C voorkomen, X in een juiste bewering in M over-

gaat, dan is X een geldige bewering in L (d.w.z. afleidbaar uit de deductie-axioma's).

Als de bewering Y in alle modellen van K in een juiste bewering overgaat, dan is $Y \in S(K)$.

We zullen nu enige voorbeelden van stellingen behandelen, die met metamathematische hulpmiddelen te bewijzen zijn.

Laat in een taal L een oneindige rij beweringen X_n ($n = 1, 2, \dots$) gegeven zijn, dusdanig, dat voor alle n $X_{n+1} \rightarrow X_n$ geldig is en $X_n \rightarrow X_{n+1}$ niet geldig is. Een dergelijke rij heet monotoon stijgend. Laat K de verzameling der X_n zijn. Het is dan onmogelijk, dat er een bewering Y in L bestaat, zodat Y afleidbaar is uit K en alle X_n afleidbaar zijn uit Y (Yaequivalent met K). Als dit n.l. wel het geval was, was Y afleidbaar uit een eindige deelverzameling V van K . Laat m de grootste index zijn, die in V voorkomt. Dan zijn alle beweringen van V uit X_m afleidbaar dus Y uit X_m afleidbaar, maar X_{m+1} is uit Y afleidbaar, dus $X_m \rightarrow X_{m+1}$ is geldig, hetgeen niet het geval is.

We passen dit toe op de theorie der lichamen. Het is makkelijk in te zien, dat het begrip lichaam in een taal te formaliseren is met behulp van de relaties $E(x, y)$, $S(x, y, z)$, $P(x, y, z)$ (d.w.z. $x = y$, $z = x + y$, $z = xy$). De lichaamsaxioma's zijn dan als beweringen in deze taal te formuleren. Ook het feit, dat een lichaam een bepaalde karakteristiek $\neq 0$ heeft, is in één axioma weer te geven. Immers de relatie $S_n(x, y)$, die uitdrukt, dat $y = nx$ is door inductie als volgt te definiëren: $S_0(x, y) = S(x, y, x)$ en $S_{n+1}(x, y) = (\exists z)(S_n(x, z) \wedge S(z, x, y))$. Dat de karakteristiek van een lichaam p is, is nu weer te geven in het axioma $H_p = (x)(y)(S_p(x, y) \rightarrow S(y, y, y))$.

Laat nu A de conjunctie van alle lichaamsaxioma's zijn en p_n ($n = 1, 2, \dots$) een aftelling van de priemgetallen. We vormen nu een rij beweringen X_n als volgt: $X_1 = A$, $X_{n+1} = X_n \wedge \neg H_{p_n}$. Dit betekent, dat X_n een axioma is voor het begrip "lichaam waarvan de karakteristiek niet p_1 , niet p_2 , ..., niet p_{n-1} is". De X_n vormen een monotoon stijgende rij. Dat $X_{n+1} \rightarrow X_n$ geldig is, is duidelijk. dat $X_n \rightarrow X_{n+1}$ niet geldig is, volgt uit het feit dat er voor ieder priemgetal p lichamen van karakteristiek p bestaan. De verzameling K der X_n is een axiomasysteem voor het begrip "lichaam van karakteristiek 0". Daar een eindige verzameling beweringen door conjunctie altijd tot één bewering te maken is, volgt nu uit het voorafgaande.

Het begrip "lichaam van karakteristiek 0" is niet met eindig veel axioma's te karakteriseren.

Het spreekt vanzelf, dat dit alleen geldt voor het begrip taal, dat wij hebben beschouwd. In meer omvattende talen kan een dergelijke karakterisering wel mogelijk zijn.

Laat nu Y een bewering zijn, die geldig is voor alle lichamen van karakteristiek 0. Uit de stelling van Gödel volgt dan, dat Y af-

leidbaar is uit de verzameling K , die hierboven gedefinieerd is en dus ook uit een eindige deelverzameling van K . Als m de grootste index is, die in deze deelverzameling voorkomt, dan is als boven $X_m \rightarrow Y$. Daar X_m geldig is in alle lichamen van karakteristiek $\geq p_m$, geldt ditzelfde ook voor Y . Hiermee is dus gevonden:

Een stelling, die in de hierboven beschreven taal is weer te geven en die geldig is in alle lichamen van karakteristiek 0 is ook geldig in alle lichamen van karakteristiek $p > p_0$, waarin p_0 een constante is afhankelijk van de stelling.

Een voorbeeld van een stelling van deze soort is als volgt te krijgen. De relatie $y = f(x_1, \dots, x_n)$, waarin $f(x_1, \dots, x_n)$ een polynoom in de veranderlijken $x_1, \dots, x_n$ is met gehele coëfficiënten, is gemakkelijk te krijgen door herhaalde toepassing van optelling, aftrekking en vermenigvuldiging op de veranderlijken $x_1, \dots, x_n$. Noem deze relatie $R_f(x_1, \dots, x_n, y)$. Dat de vergelijkingen $f_1(x_1, \dots, x_n) = 0, \dots, f_k(x_1, \dots, x_n) = 0$ een gemeenschappelijke oplossing hebben, is nu aan te geven in de volgende bewering:

$$X = (\exists x_1) \dots (\exists x_n) (\exists y) (R_{f_1}(x_1, \dots, x_n, y) \wedge \dots \wedge R_{f_k}(x_1, \dots, x_n, y) \wedge S(y, y, y)).$$

Stel nu dat de vergelijkingen $f_1 = 0, \dots, f_k = 0$ in geen enkel lichaam van karakteristiek 0 een gemeenschappelijke oplossing hebben, dan is de bewering $Y = \neg X$ dus in alle lichamen van karakteristiek 0 geldig. Uit bovenstaande stelling volgt dan, dat er een p_0 bestaat, dusdanig, dat in geen enkel lichaam met karakteristiek $p > p_0$ het stelsel een oplossing heeft.

Ter vergelijking geven we ook een algebraïsch bewijs van deze stelling. Uit de eliminatietheorie volgt, dat het feit dat $f_1 = 0, \dots, f_k = 0$ geen gemeenschappelijke oplossing in enige uitbreiding van het lichaam der rationale getallen bezitten, impliceert dat er polynomen $g_1, \dots, g_k$ met (gebroken) rationale coëfficiënten bestaan, zodat $f_1 g_1 + \dots + f_k g_k = 1$. Door vermenigvuldiging met een geschikt gekozen geheel getal a krijgen we $f_1 h_1 + \dots + f_k h_k = a$, waarin de coëfficiënten van $h_1, \dots, h_k$ gehele getallen zijn. Laat nu p_0 de grootste priemfactor van a zijn, dan is in ieder lichaam van karakteristiek $p > p_0$ het rechterlid $a \neq 0$. Zou in een dergelijk lichaam $f_1 = 0, \dots, f_k = 0$ een gemeenschappelijke oplossing hebben, dan zou door substitutie van deze oplossing in het linkerlid, dit $= 0$ worden, hetgeen een tegenspraak geeft.

Interessante toepassingen van metamathematische stellingen zijn ook te geven in de theorie van de geordende lichamen. Het begrip "geordend lichaam" is in onze taal makkelijk te formaliseren. Robinson bewijst nu:

Het begrip "Archimedisch geordend lichaam" is niet in onze taal te formaliseren.

Een stelling over geordende lichamen, die in onze taal te formaliseren is en die in alle niet-Archimedisch geordende lichamen geldt, geldt ook in alle Archimedisch geordende lichamen.

Voor het bewijs zij verwezen naar Robinson, hoofdstuk 5.

Uit de laatste stelling volgt direct:

Als een stelling over geordende lichamen, die in onze taal te formaliseren is in een of ander Archimedisch geordend lichaam geldt, dan is er ook een niet-Archimedisch geordend lichaam waarin deze stelling geldt.

Een voorbeeld van een dergelijke stelling luidt: "Ieder polynoom in één veranderlijke bezit tussen twee waarden van het argument waar het verschillend teken aanneemt, een nulpunt". Deze bewering blijkt inderdaad eenvoudig te formaliseren. Het lichaam der reële getallen is een voorbeeld van een Archimedisch geordend lichaam, waarin deze stelling geldt (middelwaardestelling van Weierstrass), dus er bestaat ook een niet-Archimedisch geordend lichaam, waarin deze stelling geldt.

In het bewijs van Steinitz voor het bestaan van algebraïsch afgesloten uitbreidingen van ieder lichaam kan het verzamelingstheoretische gedeelte (transfinitie inductie) ook vervangen worden door metamathematische beschouwingen.

Het is duidelijk wat we zullen verstaan onder de isomorfie van twee modellen. Hierbij dient echter toch nog een opmerking te worden gemaakt. We hebben meermalen de gelijkheid als een relatie $E(x,y)$ ingevoerd, die reflexief, symmetrisch en transitief is. Dit houdt evenwel niet in, dat in een model van een verzameling beweringen met deze relatie ook de relatie der identiteit overeenkomt. Het enige dat we kunnen zeggen, is dat er een equivalentierelatie mee overeenkomt. Op grond van de substitutiviteitseigenschap van de andere relaties kunnen we echter de klassen equivalente elementen samenvatten tot een nieuw model, waarin wel de identiteitsrelatie met $E(x,y)$ correspondeert. Een dergelijk model noemt men normaal.

Als M een model is van een verzameling beweringen K in een taal L dan kunnen we aan K een z.g. compleet diagram D van M toevoegen. D bestaat uit die beweringen $A(a_1, \dots, a_n)$ of $\neg A(a_1, \dots, a_n)$, waarin A een relatiesymbool en a_i objectsymbolen zijn, die in de correspondentie met het model voorkomen, dusdanig, dat de overeenkomstige beweringen in M juist zijn. Het is duidelijk, dat M ook een model van de vereniging K' van K en D is. Ook geldt echter, dat ieder model van K' een deelmodel bevat dat isomorf is met M . Laat nu H een verzameling beweringen zijn, die K omvat. De vraag of de verzameling H' , die de vereniging is van H en K' een model bezit, is volgens de stelling van Gödel equivalent met de vraag of H' consistent is. Maar H' is consistent dan en slechts

dan als iedere eindige deelverzameling van H' consistent is. Was n.l. H' inconsistent, dan was uit H' een bewering van de vorm $X \wedge \neg X$ af te leiden, maar dan was deze bewering ook uit een eindige deelverzameling van H' af te leiden en dus deze eindige deelverzameling inconsistent. Hieruit volgt:

Er bestaat een model van K , dat een uitbreiding van M is en dat ook model van H is dan en slechts dan als voor iedere eindige deelverzameling H'' van H een uitbreiding van M bestaat, die een model is van K en H'' .

Laat nu K bestaan uit de lichaamsaxioma's en M een lichaam zijn. We laten nu H bestaan uit beweringen, dat een willekeurig polynoom met coëfficiënten in M (eigenlijk met coëfficiënten die de objectsymbolen zijn, die overeenkomen met elementen van M) in lineaire factoren te ontbinden is. Dit is te formaliseren in die vorm, dat er elementen $y_1, \dots, y_n$ bestaan, waarvan de elementaire symmetrische functies gelijk zijn aan $-a_1, a_2, -a_3, \dots$, als het polynoom $x^n + a_1x^{n-1} + a_2x^{n-2} + \dots$ is. Nu is uit de algebra bekend, dat bij ieder polynoom $f(x)$ met coëfficiënten in M een uitbreiding van M te vinden is, dusdanig, dat $f(x)$ in lineaire factoren te ontbinden is. Voor een eindig stel polynomen kan hetzelfde worden gevonden door het product van deze polynomen te beschouwen. Bovenstaande stelling levert ons dus ineens, dat er ook een model van een lichaam bestaat waarin alle polynomen met coëfficiënten in M in lineaire factoren te ontbinden zijn. Uit de algebra volgt dan, dat ook de polynomen met coëfficiënten in de uitbreiding in lineaire factoren te ontbinden zijn, d.w.z. dat de uitbreiding algebraïsch afgesloten is.

Men mene niet, dat door deze methode het gebruik van transfinitie inductie (dus van het keuze-axioma) uit het bewijs van Steinitz zou zijn geëlimineerd, want de stelling van Gödel, die we gebruikt hebben, wordt in de vorm waarin hij hier geformuleerd is, ook met transfinitie inductie bewezen.

Deze voorbeelden geven natuurlijk nog een verre van volledig beeld van hetgeen in het boek van Robinson te vinden is. We hebben zelfs maar aan hoogstens één van de twee belangrijkste aspecten van het boek recht doen wedervaren. Behalve toepassing van metamathematische methoden voor het bewijs van stellingen over van ouds bekende mathematische systemen worden ook bekende begrippen uit de algebra gegeneraliseerd voor algemene systemen dan waarvoor ze oorspronkelijk waren gedefinieerd. Voorbeelden van in het boek behandelde begrippen van deze aard zijn het begrip polynoom, het begrip algebraïsch element t.o.v. een grondlichaam en het begrip ideaal. Deze uiteenzettingen zijn echter te ingewikkeld om in kort bestek te kunnen worden behandeld. Om enig idee te geven in welke richting zich dit ontwikkelt nemen we het begrip ideaal.

Voor het begrip ideaal in een ring is voor ons de meest geschikte

karakterisering die als kern van een homomorfie van een ring. Als een ring R homomorf is met een andere ring, dan is de deelverzameling van R bestaande uit verschillen van elementen van R met hetzelfde beeld in R' een ideaal I in R en ieder ideaal is ook op deze wijze te verkrijgen. We kunnen het ideaal dan ook karakteriseren door de identificaties in R uit te voeren, die nodig zijn om van R de restklassenring $R(\text{mod } I)$ te maken. In de taal komt dat hierop neer, dat we aan de verzameling K van beweringen, beweringen van de vorm $E(a, a')$ toevoegen. Op deze wijze is plausibel gemaakt, dat een ideaal metamathematisch kan worden gedefinieerd als een verzameling beweringen, die aan zekere eigenschappen voldoet.

Ten slotte kan nog worden opgemerkt, dat het boek van Robinson uiteraard niet alle methoden van metamathematische aard omvat, die op de algebra van toepassing zijn. Zo blijven vragen van beslisbaarheid geheel buiten beschouwing.
