151 Universele eigenschappen voor algebra 3; 2015/02/08

In het dagelijks leven maken we vaak gebruik van apparaten, zoals bijvoorbeeld auto's en computers, zonder dat we weten hoe die precies in elkaar zitten en hoe ze werken. Dat hoeven we ook niet te weten, want het is voldoende om er wat eigenschappen van te kennen die ons in staat stellen het apparaat te gebruiken. Bijvoorbeeld hebben alle auto's een stuur, een gaspedaal en een rem, en vaak ook een versnellingspook en een koppeling. Als we een computer programmeren dan gaan we ook uit van eigenschappen van de computer, van de programmeertaal en de al aanwezige programmatuur. Deze manier van doen maakt ons leven veel eenvoudiger.

In de wiskunde is het niet anders. Bijvoorbeeld is de verzameling $\mathbb{R}$ van reële getallen met de elementen 0 en 1, de operaties $+$ en $\cdot$, en de ordening $\leq$ axiomatisch volledig gekarakteriseerd. Iedereen mag daarom zijn/haar favoriete implementatie van $\mathbb{R}$ in de verzamelingentheorie gebruiken: elk tweetal realisaties zijn uniek isomorf (binnen het model van ZFC waarin men werkt).

Een volgende stap die in de wiskunde gezet wordt is het karakteriseren van objecten of constructies van objecten door eigenschappen. Deze eigenschappen gelden *universeel* (d.w.z., voor *alle* objecten van een bepaald soort), en heten daarom *universele eigenschappen*. Een cruciaal gevolg van een universele eigenschap is dat het object dat eraan voldoet er op uniek isomorfisme na door bepaald wordt. Deze stap is ook een goede stap in de richting van het gebruik van de *taal van categorieën*, maar daarover hopelijk later meer in dit college. Op dit moment zijn voorbeelden nuttiger. Het is ook nuttig om in bewijzen zoveel mogelijk universele eigenschappen te gebruiken; bewijzen worden daar vaak beter (korter, eenvoudiger) van.

151.1 Quotiënten van verzamelingen

Het eerste voorbeeld dat men tegen zou moeten komen is het quotiënt van een verzameling X naar een equivalentierelatie $\sim$. We spellen het uit. Een afbeelding $q\colon X \to Q$ heet *een quotiënt voor* $\sim$ als q surjectief is en de vezels van q de equivalentieklassen voor $\sim$ zijn. Stel nu dat $q\colon X \to Q$ een quotiënt voor $\sim$ is. Stel dat $f\colon X \to Y$ een afbeelding is die compatibel met $\sim$ is: voor alle x_1 en x_2 in X met $x_1 \sim x_2$ geldt dat $f(x_1) = f(x_2)$. Dan is er een unieke afbeelding $\overline{f}\colon Q \to Y$ met $f = \overline{f} \circ q$. (Lezer: teken vooral het diagram.) Deze eigenschap van q (voor alle dergelijke f bestaat zo'n unieke $\overline{f}$) heet *de universele eigenschap van het quotiënt q voor $\sim$*. Als nu $q_1\colon X \to Q_1$ en $q_2\colon X \to Q_2$ allebei deze universele eigenschap hebben, dan is er een unieke afbeelding $\overline{q_2}\colon Q_1 \to Q_2$ met $q_2 = \overline{q_2} \circ q_1$, en ook een unieke afbeelding $\overline{q_1}\colon Q_2 \to Q_1$ met $q_1 = \overline{q_1} \circ q_2$. Maar dan geldt $\overline{q_1} \circ \overline{q_2} \circ q_1 = \overline{q_1} \circ q_2 = q_1$, en dus (vanwege de universele eigenschap van q_1 toegepast op $\overline{q_1} \circ \overline{q_2}$) dat $\overline{q_1} \circ \overline{q_2} = \mathrm{id}_{Q_1}$. Net zo hebben we $\overline{q_2} \circ \overline{q_1} = \mathrm{id}_{Q_2}$. De conclusie is dus dat $\overline{q_2}$ en $\overline{q_1}$ inversen van elkaar zijn. Zoals beloofd: de universele eigenschap

bepaalt het object op uniek isomorfisme na.

151.2 Breukenlichaam van een domein

Laat D een domein zijn (dus D is een commutatieve ring met 1, waarin geldt dat $1 \neq 0$ en $(ab = 0) \Rightarrow ((a = 0) \vee (b = 0))$). Laat K het *breukenlichaam* van D zijn. De constructie daarvan geeft een injectief homomorfisme van ringen $i\colon D \to K$ dat de volgende universele eigenschap heeft: voor ieder injectief homomorfisme van ringen $f\colon D \to L$ met L een lichaam is er een uniek homomorfisme van ringen $\tilde{f}\colon K \to L$ zodat $f = \tilde{f} \circ i$.

151.3 Quotiënt van een ring naar een ideaal

Laat R een ring zijn, en $I \subset R$ een ideaal. Dan heeft het quotiënt-homomorfisme $q\colon R \to R/I$ de volgende universele eigenschap: voor ieder homomorfisme van ringen $f\colon R \to A$ met $f(I) = \{0\}$ is er een uniek homomorfisme van ringen $\overline{f}\colon R/I \to A$ met $f = \overline{f} \circ q$.

151.4 De ring van polynomen over een ring

Laar R een ring zijn. De *polynoomring in één variabele en met coëfficiënten in* R, $R[X]$, wordt geconstrueerd met een homomorfisme van ringen $c\colon R \to R[X]$ (c voor "constant") en een element X in $R[X]$, die samen de volgende universele eigenschap hebben. Voor ieder paar (f, a) met $f\colon R \to A$ een homomorfisme van ringen, en a in A, is er een uniek homomorfisme van ringen $\tilde{f}\colon R[X] \to A$ met $\tilde{f} \circ c = f$ en $\tilde{f}(X) = a$.

Het is een niet-triviaal feit (een stelling, met een bewijs, niet zo moeilijk) dat zo'n paar (c, X) dat voldoet aan de univerele eigenschap bestaat, en dat dan bovendien $R[X]$ vrij is als R-moduul, met (genummerde) basis $(X^n)_{n\in\mathbb{N}}$. Eigenlijk gebeurt het meer andersom: men neemt dit moduul als startpunt en definieert er een ringstructuur op en bewijst vervolgens dat de universele eigenschap geldt.

Laat nu R een ring en S een verzameling zijn, en $R[S]$ de polynoomring met coëfficiënten in R en met variabelen de elementen van S. Deze ring $R[S]$ wordt door de aannemer opgeleverd met een homomorfisme van ringen $c\colon R \to R[S]$ en een afbeelding $v\colon S \to R[S]$ (v staat voor "variabelen"). Dan heeft het paar (c, v) de universele eigenschap: voor ieder paar (f, a) met $f\colon R \to A$ een homomorfisme van ringen, en $a\colon S \to A$ een afbeelding, is er een uniek homomorfisme van ringen $\tilde{f}\colon R[S] \to A$ met $\tilde{f} \circ c = f$ en $\tilde{f} \circ v = a$.

Ook hier is het bestaan van een paar (c, v) dat voldoet aan de universele eigenschap niet triviaal. Als R-moduul is $R[S]$ vrij, met basis de "monomen" in S, d.w.z., de functies $m\colon S \to \mathbb{N}$

met eindige support (de verzameling van s in S met $m(s) \neq 0$ is eindig). Voor wie deze zaken in meer detail wil lezen: zie de boeken Basic Algebra I en II van Jacobson, of Algebra van Lang, of Bourbaki. Of probeer een algebra-dictaat van Ben Moonen, als die al zover is dat hij dit heeft opgeschreven. Of anders Wikipedia...

151.5 Opgave: vrije modulen

Laat R een ring zijn, en S een verzameling. Geef zelf een definitie van wat een vrij R-moduul met basis S moet zijn, door middel van een universele eigenschap, en laat vervolgens zien dat zo'n object bestaat.

152 Constructie van splijtlichamen en algebraïsche afsluitingen voor algebra 3; 2015/02/08

152.1 Adjunctie van één nulpunt van een irreducibel polynoom

Laat K een lichaam, en f in $K[X]$, irreducibel. Dan is $L := K[X]/(f)$ een lichaam, en het element $\alpha := q(X)$ (met $q\colon K[X] \to L$ het quotiënthomomorfisme) is een nulpunt van f in $L[X]$, en $L = K(\alpha)$.

Merk op: dit is potentieel zeer verwarrend. Laten we de situatie "ontwarren" in plaats van haar te negeren). De verwarring ontstaat uit het feit dat er nu *twee* verschillende ringhomomorfismen van $K[X]$ naar $L[X]$ zijn. Het eerste is $c \circ q$: eerst quotiënt van $K[X]$ naar L, gevolgd door $L \to L[X]$. Het tweede is $\tilde{\phi}\colon g = \sum_n g_n X^n \mapsto \sum_n \phi(g_n) X^n$, waar $\phi = q \circ c\colon K \to L$. De verwarring verdwijnt als sneeuw voor de zon als men de uitspraak preciseert tot: α is een nulpunt van $\tilde{\phi}(f)$. Laten we dit narekenen (alle gelijkheden in de berekening vinden plaats in L):

$$(\tilde{\phi}(f))(\alpha) = \left(\sum_n \phi(f_n) X^n\right)(\alpha) = \sum_n \phi(f_n)\alpha^n = \sum_n \phi(f_n) q(X)^n =$$
$$= \sum_n q(c(f_n)) q(X)^n = \sum_n q(c(f_n) X^n) = q(f) = 0.$$

152.2 Constructie van een splijtlichaam van één polynoom

Laat K een lichaam zijn en f in $K[X]$ monisch en van graad > 0. Laat d de graad van f. Dan $f = X^d + f_{d-1}X^{d-1} + \cdots + f_0$. Laat g een irreducibele factor in $K[X]$ van f zijn. De constructie hierboven geeft ons een uitbreiding $K \to K_1$ en een α_1 in K_1 zodat $f(\alpha_1) = 0$, en $K_1 = K(\alpha_1)$.

Dan hebben we in $K_1[X]$ een factorisatie

$$f = (X - \alpha_1) \cdot f_1,$$

met f_1 in $K_1[X]$ monisch van graad $d-1$. Herhaling geeft uiteindelijk een uitbreiding $K \to K_d$ en elementen $\alpha_1, \ldots, \alpha_d$ in K_d, zodat $K_d = K(\alpha_1, \ldots, \alpha_d)$, en

$$f = \prod_{i=1}^{d} (X - \alpha_i).$$

152.3 Constructie van een splijtlichaam van een verzameling polynomen

Laat K een lichaam zijn, en laat F een deelverzameling van $K[X]$ zijn, bestaand uit monische polynomen. Laat

$$S = \{(f, i) : f \in F, i \in \mathbb{N}, i < \deg(f)\}, \quad R = K[S].$$

We noteren het element (f, i) in R als $r_{f,i}$ (r voor "root"). Laat I het ideaal in R zijn dat voortgebracht wordt door de coëfficiënten in R van de elementen

$$f - \prod_i (X - r_{f,i}), \quad f \text{ in } F, i \text{ in } \mathbb{N} \text{ en } i < \deg(f)$$

van $R[X]$. Laat $q\colon R \to R/I$ het quotiënt-homomorfisme zijn.

Het homomorfisme van ringen $K \to R$ en de afbeelding $S \to R/I$, $(f, i) \mapsto q(r_{f,i})$ hebben samen de volgende universele eigenschap. Voor ieder ringhomomorfisme $\phi\colon K \to A$ en iedere afbeelding $S \to A$, $(f, i) \mapsto r'_{f,i}$ zodat voor alle f in F in $A[X]$ geldt dat $f = \prod_i (X - r'_{f,i})$, is er een uniek homomorfisme van ringen $\psi\colon R/I \to A$ zodat voor voor alle (f, i) in S geldt dat $r'_{f,i} = \psi(r_{f,i})$.

We claimen dat R/I niet de nulring is. We bewijzen het uit het ongerijmde. Neem aan dat $R/I = 0$. Dan is het eenheidselement 1 van R een element van I. Maar dan is 1 een (eindige!) lineaire combinatie $\sum_j h_j g_j$ met h_j in $K[S]$ en g_j in de gegeven verzameling van voortbrengers van I. Dit betekent dat er een eindige deelverzameling F' van F is, zodat de analoog geconstrueerde ring $K[S']/I'$ de nulring is. Laat nu f het product van de elementen van F' zijn, $K \to L$ een splijtlichaam voor f, en $\alpha_1, \ldots, \alpha_{\deg(f)}$ in L zodat $f = (X - \alpha_1) \cdots (X - \alpha_{\deg(f)})$ in $L[X]$. Dan splijt elk element van F' in $L[X]$ ($L[X]$ is een uniek factorisatie domein). Na nummering van de nulpunten van alle elementen van F' krijgen we een uniek ringhomomorfisme $R'/I' \to L$ dat compatibel is met de nummering. Maar dan is R'/I' niet de nulring, want de nulring heeft geen ringhomomorfisme naar een lichaam.

Laat nu $m \subset R/I$ een maximaal ideaal zijn (existentie volgt uit het niet nul zijn van R/I en het lemma van Zorn). Laat $L := (R/I)/m$. Dan is $K \to L$ een lichaamsuitbreiding. Voor alle f in F hebben we $f = \prod_i (X - \overline{r_{f,i}})$ in $L[X]$, en L is voortgebracht door K en de nulpunten in L van de f in F.

152.4 Constructie van een algebraïsche afsluiting van een lichaam

Laat K een lichaam zijn. Laat $K \to L$ een splijtlichaam zijn voor de verzameling van alle monische elementen van $K[X]$.

Claim: $K \to L$ is een algebraïsche afsluiting.

Bewijs. Per definitie is $K \to L$ algebraïsch. Laat $L \to M$ een algebraïsche lichaamsuitbreiding zijn. Dan is $K \to M$ algebraïsch (Stelling 21.9 dictaat). Laat α in M. Dan splijt f_K^α in $L[X]$, dus alle nulpunten van f_K^α in M zitten in L, dus $\alpha \in L$. Conclusie: $L = M$.