ZW 1961-010

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZUIVERE WISKUNDE

Voordracht in de serie "Actualiteiten"

door

Dr. W. Kuyk

28 oktober 1961

Existentiestellingen betreffende abelse polynomen

§ 1. Inleiding.

Laat k een willekeurig lichaam voorstellen en laat $k(X_1,\ldots,X_n)$ een zuiver transcendente lichaamsuitbreiding zijn van k van de graad n. Laat verder G een willekeurige permutatiegroep van $X_1,\ldots,X_n$ voorstellen en k(G) het deellichaam der invarianten onder G in $k(X_1,\ldots,X_n)$. Dan heeft $k(X_1,\ldots,X_n)$ de Galoisgroep G over k(G). We vragen nu of k(G) ook zuiver transcendent is over k. Deze vraag is o.a. van belang in verband met de volgende stelling, waarvan we het bewijs achterwege laten.

Stelling 1. Indien k(G) zuiver transcendent is over k, dan bestaat er een parametervoorstelling

$$(1) \qquad X^n+a_1(\lambda_1,\ldots,\lambda_n)X^{n-1}+\ldots+a_n(\lambda_1,\ldots,\lambda_n)$$

met parameters λ_i en $a_i\ (\lambda_1,\ldots,\lambda_n)\in k(\lambda_1,\ldots,\lambda_n)$, zodanig dat, als de λ_i de elementen van k doorlopen (1) juist alle n-de graadspolynomen levert in k[X] met Galoisgroep isomorf (een deler van) G, met dien verstande, dat er nog een aantal polynomen met deze eigenschap kunnen bestaan die niet in (1) bevat zijn. Deze laatste polynomen zijn in elk concreet geval aan te geven en worden singulier t.o.v. de parametervoorstelling (1) genoemd.

Deze stelling nu is weer van belang i.v.m. het omkeerprobleem van de Galoistheorie, waarbij men vraagt alle of tenminste één polynoom te construeren met Galoisgroep en voorafgegeven groep G en met coëfficiënten uit een gegeven lichaam k.

We bewijzen hier o.a., dat indien G abels is, en indien k de g-de eenheidswortel bevat (g in de orde van G), k(G) zuiver transcendent is over k (voor een volledig overzicht van de resultaten zie men § 5; een gedeeltelijk bewijs van stelling 1 vindt men in [1]).

§ 2. Verband met lagere transcendentiegraad.

Laat $k(X_1^*,\ldots,X_{n-1}^*)$ een zuiver transcendente lichaamsuitbreiding zijn van k en laat X_n^* het element $-X_1^*-\ldots-X_{n-1}^*$ in deze uitbreiding voorstellen. Dan definieert de toevoeging $X_i \longrightarrow X_i$, $k_i \longrightarrow k_i$ $(k_i \in k)$ $(i=1,\ldots,n)$ een homomorfie $\mathcal{H}$ van de polynoomring $k[X_1,\ldots,X_n]$ op $k[X_1^*,\ldots,X_n^*]$. We maken nu de volgende afspraken: Met G^* duiden we die permutatiegroep van $X_1^*,\ldots,X_n^*$ aan die bestaat uit dezelfde permutaties als G, behalve dat ze worden toegepast op de X_i^* i.p.v. de X_i. De doorsnede $k(G) \cap k[X_1,\ldots,X_n]$ geven we aan met $k[G]$, het beeld $\mathcal{H}\,k[G]$ hiervan in $k[X_1^*,\ldots,X_n^*]$ met $k[G^*]$ en het quotiëntenlichaam van $k[G^*]$ met $k(G^*)$.
Een voorbeeld van zulk een homomorfie wordt geleverd door de endomorfie $\mathcal{E}$ van $k[X_1,\ldots,X_n]$, gedefinieerd door de toevoeging $X_i^* = X_i - s_1(X)/n$ $(i=1,\ldots,n)$, met $s_1(X)=X_1+\ldots+X_n$. Dit voorbeeld geldt blijkbaar slechts in het geval dat de karakteristiek p van k het getal n niet deelt.
We zullen $\mathcal{H}$ (en $\mathcal{E}$) ook laten werken op quotiënten P/Q met $P,Q \in k[X_1,\ldots,X_n]$. In dat geval behoeft $\mathcal{H}$ P/Q geen betekenis te bezitten in $k(G^*)$, daar $\mathcal{H}\,Q=0$ kan zijn.

Stelling 2. $k(X_1^*,\ldots,X_n^*)$ is een algebraïsche uitbreiding van $k(G^*)$. Indien de karakteristiek p van k de orde van G en het getal n niet deelt, dan is G^* de Galoisgroep van $k(X_1^*,\ldots,X_n^*)/k(G^*)$.

Bewijs. De elementair-symmetrische polynomen $s_i(X^*)=\mathcal{H}s_i(X)$ $(i=1,\ldots,n)$ liggen in $k(G^*)$ zodat de eerste bewering bijna triviaal is. De Galoisgroep van $k(X_1^*,\ldots,X_n^*)$ over $k(S_1(X^*),\ldots,S_n(X^*))$ is de symmetrische groep S^* van $X_1^*,\ldots,X_n^*$. Adjungeren we nl. aan $k(X_1^*,\ldots,X_n^*)$ een transcendent element t en definiëren we $\overline{X}_i=X_i^*+t/n$ $(i=1,\ldots,n)$, dan is $k(X_1^*,\ldots,X_n^*,t)=k(\overline{X}_1,\ldots,\overline{X}_n)$ en $k(S_1(X^*),\ldots,S_n(X^*),t)=k(S_1(\overline{X}),\ldots,S_n(\overline{X}))$ terwijl de Galoisgroep van $k(X_1^*,\ldots,X_n^*)$ over $k(s_1(X^*),\ldots,s_n(X^*))$ door deze adjunctie niet gereduceerd wordt. De toevoeging $\overline{X}_i \longrightarrow X_i$ definieert een isomorfie van $k(\overline{X}_1,\ldots,\overline{X}_n)$ op $k(X_1,\ldots,X_n)$ resp. van $k(s_1(\overline{X}),\ldots,s_n(\overline{X}))$ op $k(s_1(X),\ldots,s_n(X))$ en de Galoisgroep van $k(X_1,\ldots,X_n)/k(s_1(X),\ldots,s_n(X))$ is de symmetrische groep S.

Zij nu $\overline{k(G^*)}$ het deellichaam der invarianten onder G^* in $k(X_1^*,\ldots,X_n^*)$; dan is G^* de Galoisgroep van $k(X_1^*,\ldots,X_n^*)/\overline{k(G^*)}$ en $k(G^*)\subset\overline{k(G^*)}$. We bewijzen nu dat ook $\overline{k(G^*)}\subset k(G^*)$.
Laat $f(X_1^*,\ldots,X_n^*)\in\overline{k(G^*)}$ terwijl $f(X_1,\ldots,X_n)\notin k(G)$. Laat verder $f_1=f(X_1,\ldots,X_n),\ldots,f_s=f_s(X_1,\ldots,X_2)$ de s (verschillende) geconjugeerden van f t.o.v. k(G) voorstellen, dan ligt het element

$$g = (f_1+\ldots+f_s)/s$$

in k(G), terwijl het beeld van g onder $\mathcal{H}$: $\mathcal{H}g=(\mathcal{H}f_1+\ldots+\mathcal{H}f_s)/s=$ $=f(X_1^*,\ldots,X_n^*)$ in $k(G^*)$ ligt.

De volgende twee stellingen vertellen iets over het verband tussen de zuivere transcendentie van $k(G^*)$ en k(G) over k.

Stelling 3. Laat k(G) zuiver transcendent zijn over k terwijl de karakteristiek p van k n niet deelt. Laat het element $s_1(X)=X_1+\ldots+X_n$ voorkomen onder de elementen van een zuivere basis van k(G)/k. Dan kan men altijd een zuivere basis $U_1,\ldots,U_{n-1},U_n=s_1(X)$ van k(G)/k kiezen zodanig, dat onder de endomorfie $\mathfrak{E}$ de elementen $\mathfrak{E}U_i$ $(i=1,\ldots,n)$ betekenis bezitten in K(G). Indien nu $\mathfrak{E}U_1,\ldots,\mathfrak{E}U_{n-1}$ algebraïsch onafhankelijk zijn over k, dan is $k(G^*)$ zuiver transcendent over k.

Bewijs. Laten we kortheidshalve achterwege (zie [1], p.32).

Stelling 4. Als de karatieristiek p van k het getal n niet deelt, dan volgt uit de zuivere transcendentie van $k(G^*)$ over k de zuivere transcendentie van k(G) over k. (Zie [1], p.33.)

§ 3. Primitieve bases en zuivere bases

Laat ζ een primitieve n-de eenheidswortel voorstellen, dan geven we het lichaam $k(\zeta)$ aan met k', $k(\zeta)(X_1,\ldots,X_n)$ met $k'(X_1,\ldots,X_n)$, etc. Al het in § vermelde gaat dan door als we k door k' vervangen. We hebben nu het volgende lemma.

Lemma. $k'(G) = k(G)(\zeta)$, $k'(G)\cap k(X_1,\ldots,X_n)=k(G)$, $[k'(G): k(G)]=[k':k]$ en deze beweringen blijven gelden als we hierin G door G^* vervangen. Het bewijs volgt voornamelijk uit het feit dat $k(X_1,\ldots,X_n)$ en $k(X_1^*,\ldots,X_n^*)$ lineair disjunct zijn met k' over k.

Definitie 1. We noemen een verzameling van s elementen $\{V_1,\ldots,V_s\}$ in k'(G) een primitieve basis van k'(G) over k', als
(i) $k'(G)=k'(V_1^{(1)},\ldots,V_1^{(\nu_1)},\ldots,\ldots,V_s^{(1)},\ldots,V_s^{(\nu_s)})$, waarin

$V_k^{(j)}$ $(j=1,\ldots,\nu_k)$ de ν_k (verschillende) geconjugeerden van $V_k=V_k^{(1)}$ t.o.v. $k(G)$ voorstellen;

(ii) $\sum_{i=1}^{s} \nu_i = n$.

Definitie 1'. Eenzelfde definitie is te geven van een primitieve basis van $k'(G^*)$ over k'; daarvoor behoeven we in de voorgaande slechts G door G^*, $V_k^{(j)}$ door $V_k^{(j)*}$ en n door $n-1$ te vervangen.

Stelling 5. Als $k'(G^*)$ een primitieve basis over k' bezit en de karakteristiek p van k deelt n niet, dan bezit $k'(G)$ een primitieve basis over k'.

Bewijs. Langs dezelfde weg als het bewijs van stelling 4 en door aan te tonen dat V_k^* in de isomorfie t.o.v. $k'(G)$ dezelfde geconjugeerden bezit als t.o.v. $k'(G^*)$.

Stelling 6. $k(G)$ is zuiver transcendent over k dan en slechts dan als $k'(G)$ een primitieve basis over k' bezit.

Bewijs: (i) De voorwaarde is voldoende. Laat $k_i'=k(G)(V_i)\cap k'$ $(i=1,\ldots,s)$. Dan is $k(G)(V_i)=k(G)k_i'$, zoals een algebraïsche graadbeschouwing leert; we maken geen onderscheid tussen de Galoisgroepen G_i van $k(G)(V_i)/k(G)$ en k_i'/k.
Laat $w_{i1},\ldots,w_{i\nu_i}$ een normale basis van k_i' over k voorstellen, dan is

$$V_i = V_i^{(1)} = \sum_{j=1}^{\nu_i} w_{ij}U_{ij}$$

met U_{ij} in $k(G)$. De andere $V_i^{(l)}$ $(l=1,\ldots,\nu_i)$ worden verkregen door de automorfieën van G_i op de w_{ij} in de bovenstaande vormen toe te passen. Daar de $V_i^{(l)}$ $(l=1,\ldots,\nu_i)$ algebraïsch onafhankelijk zijn over k', zijn de zo verkregen vormen zeker lineair onafhankelijk over k'. De U_{ij} $(j=1,\ldots,\nu_i)$ kunnen dus geschreven worden als lineaire combinaties van $V_i^{(l)}$ over k_i', en $k'(V_i^{(1)},\ldots,V_i^{(\nu_i)})=k'(U_{i1},\ldots,U_{i\nu_i})$ resp. $k'(V_1^{(1)},\ldots,V_1^{(\nu_1)},\ldots,\ldots,V_s^{(1)},\ldots,V_s^{(\nu_s)})=k'(U_{11},\ldots,U_{s\nu_s})$.
Zij $K=k(U_{11},\ldots,U_{s\nu_s})$. Dan $K\subset k'(G)$, $Kk'=k'(G)$ en $k'(G)$ is algebraïsch t.o.v. K met $[k'(G):K]=[k':k]$. D.w.z. (lemma) $K=k(G)$ en $U_{11},\ldots,U_{s\nu_s}$ is een zuivere basis van $k(G)$ over k.

(ii) De voorwaarde is noodzakelijk. Een zuivere basis van $k(G)/k$ is zeker een primitieve basis van $k'(G)/k'$.

Stelling 6'. $k(G^*)$ is zuiver transcendent over k dan en slechts dan als $k'(G^*)$ een primitieve basis over k' bezit.

Bewijs. Precies hetzelfde bewijs als van stelling 5, onder de vervanging gegeven in definitie 1'.

Gevolg: Uit stelling 3 en 5' volgt nu: bezit $k'(G^*)$ een primitieve basis over k' en deelt de karakteristiek p van k het getal n niet, dan is k(G) zuiver transcendent over k.
Merk op dat de beweringen van deze paragraaf behouden blijven indien we voor ζ nemen een willekeurig separabel algebraïsch element over k.

§ 4. Cyclische G.

Laat nu G de cyclische permutatiegroep Z_n voorstellen die voortgebracht wordt door de cykel $(X_1X_2\ldots X_n)$. Masuda [2] bewijst dan:

Stelling 7. $k'(Z_n)$ is zuiver transcendent over k'.
Bewijs. Door aan te tonen dat de elementen $U_i=Y_1Y_i/Y_{i+1}$ $(i=1,\ldots,n)$ met $Y_k = \sum_{j=1}^{n} \zeta^{-jk}X_j$ een zuivere basis van $k'(Z)$ over k' vormen.

Stelling 7'. Indien p niet deelbaar is op n dan is $k'(Z_n^*)$ zuiver transcendent over k'.
Bewijs. We transformeren eerst de basis van stelling 6 op een zodanige manier dat onder $\mathfrak{A}$ de nieuwe basiselementen betekenis bezitten in $k'(X_1^*,\ldots,X_n^*)$. De transformatie

$$U_i^* = U_i \quad (i=1,\ldots,n-2,n)$$
$$U_{n-1}^*=U_{n-1}U_n$$

voldoet, daar nu geen der noemers van U_k^* in nul overgaat.
Passen we nu de in § 1 gedefinieerde endomorfie $\mathfrak{E}$ toe, dan krijgen we:

$$\mathfrak{E}\,Y_k = \sum_{j=1}^{n} \zeta^{-jk}X_k - s_1(X)/n \cdot \sum_{j=1}^{n} \zeta^{-jk} = Y_k$$

indien $k\neq n$ en $\mathfrak{E}\,Y_n=0$. $\mathfrak{E}$ op de basiselementen U_i^* toegepast geeft $\mathfrak{E}\,U_k^* = U_k^*$ $(k=1,\ldots,n-1)$ en $\mathfrak{E}\,U_n^*=0$.
Teneinde te bewijzen dat de over k' algebraïsch onafhankelijke elementen U_k^* $(k=1,\ldots,n-1)$ een zuivere basis van $k'(Z^*)$ over k' vormen, bewijzen we eerst dat $X_1^*,\ldots,X_n^*$ nulwaarden zijn van een polynoom in $k'(U_1^*,\ldots,U_{n-1}^*)[X]$. Laat

$$s_i(X) = \frac{a_i(U_1^*,\ldots,U_n^*)}{b_i(U_1^*,\ldots,U_n^*)}$$

onvereenvoudigbaar zijn in $k'(U_1^*,\ldots,U_n^*)$, dan geldt

$$\varepsilon\, s_i(X)=s_i(X^*)=\frac{\varepsilon a_i}{\varepsilon b_i}=\frac{a_i(U_1^*,\ldots,U_{n-1}^*,0)}{b_i(U_1^*,\ldots,U_{n-1}^*,0)},$$

tenzij $a_i(U_1^*,\ldots,U_{n-1}^*,0) = b_i(U_1^*,\ldots,U_{n-1}^*,0)=0$, en dit kan slechts optreden als de teller en de noemer van $s_i(X)$ de factor $U_n=s_1(X)$ bevatte, hetgeen uitgesloten was. Dat $k'(X_1^*,\ldots,X_n^*)$ de Galoisgroep Z_n^* over $k'(U_1^*,\ldots,U_{n-1}^*)$ bezit bewijst men op dezelfde wijze als in stelling 3 en 4.
Masuda bewijst ook nog ([2]).

Stelling 8. Indien de karakteristiek p van k n niet deelt, dan bezit voor n=2 t/m 7 $k'(Z_n^*)$ een primitieve basis over k'.

We kunnen op eenvoudige manier uit de primitieve basis van stelling 8 voor n=2 t/m 7 primitieve bases voor $k'(Z_n^*)/k'$ afleiden. Hierbij maken we weer gebruik van de invariantie der Y_i (zie terug) bij lineaire verschuiving van de X_k over een bedrag $s_1(X)/n$.
Uit stelling 6' en stelling 8 volgt nu dat voor n=2 t/m 7 $k(Z_n^*)$ en $k(Z_n)$ zuiver transcendent zijn over k.

§ 5. Existentiestellingen.

a. Uit de stellingen 1 en 7 volgt onmiddellijk: Er bestaat, als $p \nmid n$, een parametervoorstelling van het type (1) van alle n-de graadspolynomen over k' met cyclische Galoisgroep Z_n.

b. Uit de stellingen 1 en 8 (gevolg): Er bestaat, als $p \nmid n$, voor n=2 t/m 7 een parametervoorstelling van het type (1) voor alle polynomen met cyclische Galoisgroep Z_n over k.
Om nu over te kunnen gaan op parametervoorstellingen van polynomen met willekeurige abelse groep maken we gebruik van de volgende stelling.

Stelling 9. Laat H een permutatiegroep van m algebraïsch onafhankelijken $Y_1,\ldots,Y_n$ over k voorstellen. Dan definiëren we geheel analoog met k(G) en $k(G^*)$ in § 2, k(H) en $k(H^*)$ in $k(Y_1,\ldots,Y_m)$ resp. $K(Y_1^*,\ldots,Y_m^*)$. Laat verder het directe groepsproduct $F = G \times \mathcal{H}$ van G en H de l=n.m over k algebraïsch onafhankelijke elementen $Z_1,\ldots,Z_l$ permuteren; laat k(F) en $k(F^*)$ weer gedefinieerd zijn geheel analoog aan k(G) en $k(G^*)$ en laat l niet deelbaar zijn door p.
Indien nu $k(H^*)$ en $k(G^*)$ zuiver transcendent zijn over k dan is $k(F^*)$, en dus ook k(F), zuiver transcendent over k. Het bewijs vindt men in [1] . Deze stelling leidt i.v.m. het boven bewezene tot de

volgende conclusies.

c. Uit de stellingen 1, 7' en 9 volgt: Laat A een willekeurige abelse groep voorstellen van de orde g. Indien k de g-de eenheidswortels bevat, en de karakteristiek p van k deelt g niet, dan bestaat er een parametervoorstelling van het type (1) van alle g-de graads (irreducibele) polynomen over k met Galoisgroep A.

d. Uit de stellingen 1, 8 (gevolg) en 9: Indien $p \nmid n$, k willekeurig, en A een abelse groep die een direct product is van cyclische groepen van de orden 2 t/m 7 (deze cyclische factoren eventueel meermalen herhaald), dan bestaat er een parametervoorstelling van het type (1) van alle (irreducibele) polynomen over k met abelse groep A.

Passen we tot slot de irreducibiliteitsstelling van Hilbert [3] toe: Indien G transitief is over $\{X_1,\ldots,X_n\}$ en indien de coëfficiënten $a_i(\lambda_1,\ldots,\lambda_n)$ van (1) in een algebraïsche uitbreiding R van het lichaam der rationale getallen liggen, dan zijn er oneindig veel substituties $\lambda_i \rightarrow g_i$ (g_i geheel) zodanig dat (1) overgaat in een polynoom met precies de Galoisgroep G. De gevallen a,b,c en d geven dan resp.

a'. Er bestaan oneindig veel n-de graadspolynomen met Galoisgroep Z_n over R'.

b'. Er bestaan oneindig veel n-de graadspolynomen met Galoisgroep Z_n (n=2,...,7) over R.

c'. Er bestaan, indien θ een primitieve g-de eenheidswortel (g-de orde van A) oneindig veel polynomen met Galoisgroep A over $R(\theta)$.

d'. Er bestaan oneindig veel polynomen over R met abelse groep A; A uit de klasse aangegeven onder d.

Opmerking. Men kan, met behulp van een eveneens in [1] uitgewerkte methode, parametervoorstellingen van het type (1) construeren, van alle polynomen met zekere Galoisgroep G, voor (in principe weer) oneindig veel (niet abelse) G. De structuur van deze G schijnt moeilijk te karakteriseren.

[1] W. Kuyk, Over het omkeerprobleem van de Galoistheorie, A'dam 1960.

[2] K. Masuda, On a problem of Chevalley, Nagoya Math.Journal vol.8, 1955.

[3] in Journal f.die reine u.angew. Math., Bd 53.