STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1962 - 016

On the inversion of a theorem of E. Noether

W. Kuyk

1962

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

STICHTING ZW 1962-016
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

On the inversion of a theorem of E.Noether

by

W. Kuyk

1. Introduction.

Let $k(X_1,\dots,X_n)$ be a purely transcendental field extension of a field k, and G_n an arbitrary transitive permutation group operating on the $X_1,\dots,X_n$. Let $k(G_n)$ denote the field of all invariants under G in $k(X_1,\dots,X_n)$.
If $k(G_n)$ is also purely transcendental over k, i.e. if there exist elements $U_1,\dots,U_n$ in $k(X_1,\dots,X_n)$,

$$(1)\qquad U_\nu = \frac{p_\nu[X_1,\dots,X_n]}{p_o[X_1,\dots,X_n]} \qquad (\nu=1,\dots,n)$$

with $p_\nu\,[X_1,\dots,X_n] \in k\,[X_1,\dots,X_n] \cap k(G_n)$ $(\nu=0,1,\dots,n)$ such that $k(G_n)=k(U_1,\dots,U_n)$, then the polynomial

$$(X-X_1)\dots(X-X_n)=X^n-s_1\,X^{n-1}+\dots+(-1)^n\,s_n$$

can be written in the form

$$(2)\qquad X^n + a_1(U_1,\dots,U_n)X^{n-1}+\dots+a_n(U_1,\dots,U_n)$$

with $a_\nu(U_1,\dots,U_n) \in k(U_1,\dots,U_n)$ $(\nu=1,\dots,n)$, since the elementary symmetric functions $s_1,\dots,s_n$ of $X_1,\dots,X_n$ certainly belong to $k(G_n)$.

In 1916 E. Noether showed that the polynomial (2) can be regarded as a parametric representation of all polynomials $f[X] \in k[X]$ of degree n with Galois group (considered as a permutation group of the suitably arranged zeros of $f[X]$) a subgroup of G_n [1]. In fact, if $f[X]$ is any such polynomial with zeros $\alpha_1, \ldots, \alpha_n$, say, then substitution of $X_1, \ldots, X_n$ by $\alpha_1, \ldots, \alpha_n$ in (1) transforms $U_1, \ldots, U_n$ into elements $k_1, \ldots, k_n$ in k, provided that $p_o[\alpha_1, \ldots, \alpha_n] \neq 0$; and substitution of $X_1, \ldots, U_n$ by $k_1, \ldots, k_n$ in (2) transforms (2) into $f[X]$[1]. The condition $p_o[\alpha_1, \ldots, \alpha_n] \neq 0$ however, seems to be a rather heavy restriction of the generality of the theorem, for it might be possible that in (2) so many polynomials with Galois group G_n over k are missing that some field K/k with Galois group $G \cong G_n$ might have none generating polynomial that is contained in the parametric representation (2). This is however not true, as is shown in theorem 2 of this report, in the case that k is infinite. This infiniteness condition for k is not an essential restriction, as finite extensions of finite fields have cyclic Galois group, the generating polynomials being easily constructed by means of well known arguments.

On the other hand, if an arbitrary substitution of U_i by elements of k, transforms (2) into a separable polynomial $f[X] \in k[X]$, then the Galois group H_n of $f[X]$ is (as a permutation group of the suitably arranged roots of $f[X]$) a subgroup of G_n. This is a consequence of theorem 2.

2. <u>Theorem 1</u>.

Let K/k be our arbitrary field extension of k with Galois group $G \cong G_n$, let k be infinite. Let, in the notation of the introduction, $k(G_n)$ be purely transcendental over k; let (2) be a parametric representation in the sense of E. Noether etc.,

----

1) An exposition of E. Noether's theorem and a modified proof are given in [2].

entirely like in the introduction. Then there exist infinitely many substitutions $U_i \longrightarrow k_i$ $(k_i \in k)$ that carry (2) into an element $f[X] \in k[X]$ with splitting field K.

<u>Proof</u>: We construct a generating set $\{\rho_1, \ldots, \rho_n\}$ of K/k, with the properties: <u>1</u> $\rho_1, \ldots, \rho_n$ are the roots of an irreducible polynomial in $k[X]$, while the Galois group of K/k permutes $\rho_1, \ldots, \rho_n$ in just the same way as G_n permuted $X_1, \ldots, X_n$.

<u>2</u> $p_o[\rho_1, \ldots, \rho_n] \neq 0$.

Let A: $\{\alpha_1, \ldots, \alpha_m\}$ be a normal basis of K/k and let G_n be the regular permutation group on A representing the Galois group of K/k. Let $t_1, \ldots, t_m$ be m algebraically independent variables that are adjoined to k; denote $k(t_1, \ldots, t_m)$ by $k(t)$ an $K(t_1, \ldots, t_m)$ by $K(t)$. The Galois group of $K(t)|k(t)$ remains G_m. From the expressions $\bar{\alpha}_1 = t_1 \alpha_1 + \ldots + t_m \alpha_m$, $\bar{\alpha}_i = \sigma_i(\alpha_1)$ $(\sigma_i \in G_m;\ i=1, \ldots, m)$.
Then it is readily seen that the set A: $\{\bar{\alpha}_1, \ldots, \bar{\alpha}_m\}$ forms a normal basis of $K(t)|k(t)$. For the determinant $D = g[t_1, \ldots, t_m] \in k[t]$ in the t_i of the transformation $\bar{\alpha}_i = \sigma_i(\bar{\alpha}_1)$ does not vanish, so that $\bar{\alpha}_1, \ldots, \bar{\alpha}_m$ are linearly independent and conjugated over $k(t)$.
The elements $t_1, \ldots, t_n$ can on the other hand be rationally expressed in $\bar{\alpha}_1, \ldots, \bar{\alpha}_m$ over K, because of the fact that the determinant $|\sigma_i \ \sigma_j(\alpha)|$ does not vanish.
Passing from A to $\bar{A}$ we obtain an isomorphic representation $\bar{G}_m$ of G_m, as a permutation group of $\bar{A}$. Let m=n.l. As G can also be represented as a transitive permutation group of n elements (viz. $X_1, \ldots, X_n$), we can divide $\bar{A}$ into n subsets each of l elements: $A = \bar{A}_1 \cup \ldots \cup \bar{A}_n$, such that the permutations in $\bar{G}_m$ permute $\bar{A}_1, \ldots, \bar{A}_n$ in just the same way as G_n permutes $X_1, \ldots, X_m$ (see M.Hall [3], p.57). Define $Z_i = s(\bar{A}_i)$ $(i=1, \ldots, n)$, where $s(M_i)$ denotes the sum of the l elements in M_i. $Z_1, \ldots, Z_n$ are as sums of the elements of disjoint subsets of an algebraically

irreducible set over k, certainly algebraically independent over k. This means $p_o[Z_1,\dots,Z_n] \neq 0$ and moreover $p_o[Z_1,\dots,Z_n] = f[t_1,\dots,t_m] \in k[t]$.
Now, let $t_i \longrightarrow \bar{k}_i$ $(i=1,\dots,m;\ \bar{k}_i \in k)$ be a substitution such that $f[\bar{k}_1,\dots,\bar{k}_m]\, g[\bar{k}_1,\dots,\bar{k}_m] \neq 0$. There exist infinitely many substitution of this kind, as k is infinite.
$t_i \longrightarrow \bar{k}_i$ transforms the set $\bar{A}$ into the set $\bar{\bar{A}}$:
$\{\bar{\bar{\alpha}}_1 = \bar{k}_1\alpha_1 + \dots + \bar{k}_m\alpha_m;\ \bar{\bar{\alpha}}_i = \sigma_i(\bar{\bar{\alpha}}_1)\}$ and $\bar{\bar{A}}$ forms clearly a normal basis of K/k, as the determinant $g(k_1,\dots,k_n) \neq 0$.
Now our proof is complete if we show that the Galois group $\bar{\bar{G}}_m$ of K/k as a permutation group of $\bar{\bar{A}}$ is just the same group as the permutation group $\bar{G}_m$ of $\bar{A}$. For, in that case the substitution $t_i \longrightarrow \bar{k}_i$ carries z_i into elements β_i with the property that $K=k(\beta_1,\dots,\beta_n)$, the Galois group of K/k permuting $\beta_1,\dots,\beta_n$ in just the same way as G_n permutes $X_1,\dots,X_n$, while moreover $p_o[\beta_1,\dots,\beta_n] \neq 0$.
We prove therefore that an automorphism of K/k determines the same permutation of $\bar{\bar{\alpha}}_1,\dots,\bar{\bar{\alpha}}_m$ as of $\bar{\alpha}_1,\dots,\bar{\alpha}_m$. In fact, let π be an automorphism of K/k carrying α_1 into α_k and $\bar{\alpha}_1$ into $\bar{\alpha}_i$; let further $\bar{\alpha}_1 = f(t_1,\dots,t_m,\alpha_1) \in k(\alpha_1)[t]$, then $\bar{\bar{\alpha}}_1 = f(\bar{k}_1,\dots,\bar{k}_m,\alpha_1)$. Applying π to $\bar{\alpha}_1$ and $\bar{\bar{\alpha}}_1$ we find $\pi\bar{\alpha}_1 = \bar{\alpha}_i = f(t_1,\dots,t_m,\alpha_k)$ and $\pi\bar{\bar{\alpha}}_1 = f(\bar{k}_1,\dots,\bar{k}_m,\alpha_k)$, the latter element being clearly equal to $\bar{\bar{\alpha}}_i$.

3. Before proving theorem 2 we slightly generalize the notion of Galois group of a polynomial. Let $f[X]$ be a separable polynomial in $k[X]$. Let k_f be the splitting field of $f[X]$. Let $g_1[X],\dots,g_k[X]$ be the different ineducible factors in $f[X]$, so that $f[X]$ can be written $f[X]=g_1[X]^{m_1}\dots g_k[X]^{m_k}$. We put $g[X]=g_1[X]\dots g_k[X]$. Then, obviously, $k_f=k_g$. The Galois group G of $g[X]$ over k is the group of those automorphisms of k_g leaving k pointwise fixed. Now, since $k_f=k_g$ we define the Galois group of $f[X]$ to be the same group G. Usually G is represented as a permutation group of the different zeros of

$f[X]$. However, it is also possible to represent G without ambiguity as a permutation group of all the zeros of $f[X]$, by assigning to every irreducible factor of $f[X]$ a separate set of zeros and not admitting any permutation that carries a zero of one irreducible factor into a zero of another (necessarily identical) irreducible factor of $f[X]$.
The following theorem is similar to a theorem in van der Waerden, Moderne Algebra I, 1960 (§ 61).

Theorem 2. Let $k(U_1,\dots,U_m)$ be a purely transcendental field extension of a field k; let $m \geqslant 1$. Let

$$P = b_o(U_1,\dots,U_m)X^{n-1}+\dots+b_n(U_1,\dots,U_m)$$

be any separable polynomial irreducible in $k(U_1,\dots,U_m)[X]$ with Galois group G. Let $U_i \longrightarrow k_i$ $(k_i \in k;\ i=1,\dots,m)$ be a substitution carrying P into

$$P^* = b_o^* X^n +\dots+ b_n^* \in k[X].$$

Let P^* have n separable but not necessarily different zeros $\alpha_1,\dots,\alpha_n$. Then the Galois group of P^* (in the above defined sense, as a permutation group of the n suitably arranged roots $\alpha_1,\dots,\alpha_n$) is a subgroup of G.

Proof. Let $X_1,\dots,X_n$ be the zeros of P. By means of the indeterminates $t_1,\dots,t_n$ form the expressions $Z_1=t_1X_1+\dots+t_nX_n$ and $\xi_1=t_1\alpha_1+\dots+t_n\alpha_n$. If π_t denotes a permutation of the set $T: \{t_1,\dots,t_n\}$ then π_x and π_α shall denote the same permutations of $X: \{X_1,\dots,X_n\}$ and $A: \{\alpha_1,\dots,\alpha_n\}$, respectively. Obviously, we have for any π_t

$$\pi_x \pi_t Z_1 = Z_1 \quad \text{and} \quad \pi_\alpha \pi_t \xi_1 = \xi_1 .$$

Hence,

$$\pi_t Z_1 = \pi_x^{-1} Z_1 \quad \text{and} \quad \pi_t \xi_1 = \pi_\alpha^{-1} \xi_1. \tag{3}$$

Therefore, if a certain set of elements $\pi_t Z_1$ or $\pi_t \zeta_1$ is formed by letting π_t run through a group G_t of permutations of T, then the same set is formed by the elements $\pi_x Z_1$ and $\pi_\alpha \zeta_1$, respectively, if π_x and π_α run through the groups G_x and G_α of the same permutations of X and A respectively.
Now let S_t denote the symmetric permutation group of T and let S_x and S_α denote the corresponding groups of the x_i and the α_i. Then, clearly,

$$F = \prod_{\pi_t \in S_t} (Z - \pi_t Z_1) = \prod_{\pi_x \in S_x} (Z - \pi_x Z_1)$$

and

$$F^* = \prod_{\pi_t \in S_t} (Z - \pi_t \zeta_1) = \prod_{\pi_\alpha \in S_\alpha} (Z - \pi_\alpha \zeta_1) .$$

The coefficients of F are symmetric in $X_1,\dots,X_n$ and, therefore, can be expressed in $t_1,\dots,t_n$ and the coefficients $b_o,b_1,\dots,b_n$ of P. They are, in fact, polynomials in t_i and $b_1/b_o,\dots,b_n/b_o$. It is clear that the coefficients of F^* can in exactly the same way be expressed in t_i and $b_1^*/b_o^*,\dots,b_n^*/b_o^*$, since P^* has n zeros, and thus $b_o^* \neq 0$.
Multiplying F by a suitably chosen power of b_o, we obtain a polynomial in $t_i,b_o,\dots,b_n$ and Z, i.e. a polynomial in $t_1,\dots,t_n,U_1,\dots,U_m$ and Z with coefficients in k:

$$\overline{F} = b_o^t \,.F \in k[t_1,\dots,t_n,U_1,\dots,U_m][Z] .$$

The substitution $U_i \longrightarrow k_i$ $(i=1,\dots,m)$ carries every b_j into b_j^* $(j=0,1,\dots,m)$ and hence $\overline{F}$ into

$$\overline{F}^*(Z) = b_o^{*\,t}.\ F^*(Z) \in k[t_1,\dots,t_n][Z] .$$

Let

$$(4) \qquad \overline{F}(Z) = F_1(Z)\dots F_r(Z)$$

be a factorization of $\overline{F}$ into factors that are irreducible in $k(t_1,\dots,t_n,U_1,\dots,U_m)[Z]$. By a well known theorem, we may assume F_i to be polynomials in $k[U_1,\dots,U_m][t_1,\dots,t_n][Z]$ as the Unique Factorization Theorem holds in $k[U_1,\dots,U_m][t_1,\dots,t_n]$. These polynomials are all different[1] and they have each the Galois group $G_x \cong G$ with respect to $k(t_1,\dots,t_n,U_1,\dots,U_m)$ since the conjugates relative to $k(t_1,\dots,t_n,U_1,\dots,U_m)$ of any zero $\pi_t' Z_1$ of F can be obtained by performing all the permutations π_x that belong to G_x on $\pi_t' Z_1$, i.e., in virtue of (3), by performing all the permutations π_t that belong to G_t on $\pi_t' Z_1$, from which it follows that all the elements obtained in this way are different.
Without loss of generality we may suppose Z_1 to be a zero of F_1. The substitution $U_i \longrightarrow k_i$ carries each polynomial F_i $(i=1,\dots,r)$ into a polynomial F_i^* in $k[t_1,\dots,t_n][Z]$, and clearly,

$$\overline{F}^* = F_1^* \dots F_r^* \quad . \tag{5}$$

By reordening the indices of $\alpha_1,\dots,\alpha_n$ we can ensure that ξ_1 is a zero of F_1^*.
Now, let H be the Galois group of $k(A)$ with respect to k. Then, if $\alpha_1,\dots,\alpha_n$ are all different, each element of H corresponds to one and only one permutation of $\alpha_1,\dots,\alpha_n$. However, the same is true, if there are equal zeros among $\alpha_1,\dots,\alpha_n$ (i.e. in virtue of the separability of P^*, if P^* has some identical[2] irreducible factors), provided that we do not admit permutations that carry a zero of one irreducible factor into a zero of another (necessarily identical) irreducible factor.

----

1) Because of the fact that t_i are algebraically independent over $k(X)$ and $X_1,\dots,X_n$ are all different, the polynomial P being irreducible and separable.

2) Identical meaning here: with the same or proportional coefficients.

Since t_i are algebraically independent with respect to $k(A)$, the Galois group H is also the Galois group of $k(T,A)$ over $k(T)$. Now, the conjugates of ξ_1 with respect to $k(T)$ can be obtained by performing all the permutations π_α that belong to $H \cong H$ (with the above mentioned restriction) on ξ_1, and all the elements obtained in this way are different. For, if $\pi'_\alpha\ \xi_1 = t_1\ \alpha_{\mu_1} + \ldots + t_n\ \alpha_{\mu_n} = \pi''_\alpha\ \xi_1 = t_1\ \alpha_{v_1} + \ldots + t_n\ \alpha_{v_n}$, then $\alpha_{\mu_1} = \alpha_{v_1}, \ldots, \alpha_{\mu_n} = \alpha_{v_n}$, and this can only be true for two permutations π'_α and π''_α belonging to H_α, if $\pi'_\alpha = \pi''_\alpha$, on account of the given restriction as to the permutations belonging to H_α. Hence the conjugates of ξ_1 are obtained by performing all the π_α that belong to H_α on ξ_1.

Now, since the zeros of F_1 all have the form $\pi_t\ Z_1$ $(\pi_t \in G_t)$ and since F_1^* is derived from F_1 by the substitution $U_i \longrightarrow k_i$, the zeros of F_1^* all have the form $\pi_t\ \xi_1$ with $\pi_t \in G_t$. As all the conjugates of ξ_1 occur among these zeros of F_1^*, it follows that H_t is a subgroup of G_t, i.e. H is isomorphic to a subgroup of G, q.e.d.

[1] E. Noether: Gleichungen mit vorgeschriebener Gruppe, Math.Ann. Bd.78.

[2] W. Kuyk: Over het omkeerprobleem van de Galoistheorie, 1960, Amsterdam.

[3] M. Hall: The theory of groups, Macmillan, 1959.