STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1962 - 008

Note on a parametric representation of cyclic polynomials

W. Kuyk

1962

ZW 1962-008

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

Note on a parametric representation of cyclic polynomials

by W. Kuyk

1. Let n be a positive integer; let k be an arbitrary field containing the n-th roots of unity; suppose that the characteristic of k does not divide n. Let X $\{X_1,\dots,X_n\}$ be a set of n algebraically independent elements over k and let C_n denote the cyclic permutation group of X generated by the cycle $(X_1\dots X_n)$. Let k_C denote the subfield of k(X) that is pointwise fixed under the permutations in C_n.
It is known that k_C is purely transcendental over k. In fact, Masuda [1] proves that the set U

$$U : \left\{ U_i = Y_1Y_i/Y_{i+1} \;;\quad i=1,\dots,n \right\}$$

with $$Y_i = \sum_{j=1}^{n} \zeta^{-ij}X_j$$

and ζ a primitive n-th root of unity, forms a pure basis of k_C/k.

Now, let Y denote the set $\{Y_1,\dots,Y_n\}$, then we find, using the relations $X_j = n.\sum_{i=1}^{n} \zeta^{ij}Y_i$ $(j=1,\dots,n)$, that k(Y) is identical with k(X), so that Y is an algebraically independent set over k as well.
Form the polynomial

$$(X-X_1)\dots(X-X_n) = X^n + a_1(U_1,\dots,U_n)X^{n-1}+\dots+a_n(U_1,\dots,U_n), \qquad (1)$$

whose coefficients belong to k_C=k(U). This polynomial can be regarded as a parametric representation of polynomials with Galois group C_n over k in the sense of E. Noether [2]. More precisely stated, (1) has the following two properties

a substitution of U_i by arbitrary elements $k_i \in k$, transforms (1) into a polynomial in $k[X]$ with Galois group (a subgroup of) C_n.

b If k is infinite and if K/k is an algebraic field extension with Galois group $C \cong C_n$, then there exist infinitely many n-tuples $(k_1, \ldots, k_n)$ $(k_i \in k)$ such that substitution of U_i by k_i transforms (1) into a generating polynomial of K/k.

Remark. The propositions a and b can be derived from some general theorems that I have not yet published, but can also be found directly by writing the X_i as sums of radicals and applying the Kummer-generation of K/k.

The purpose of this report is firstly to show that (1) is already a polynomial in $k'(U)[X]$, where k' is the prime field in k, and secondly to compute the Galois group of (1) with respect to k'(U).

2. As k denotes an arbitrary field containing the n-th roots of unity, the coefficients of (1) must lie in $k'(\zeta)(U)$; so, without loss of generality we may suppose in the following that k is equal to $k'(\zeta)$.

Theorem 1. The parametric representation (1) is a polynomial in $k'(U)[X]$.

Proof. If $\zeta \in k'$ then there is nothing to prove. We suppose that $[k'(\zeta) : k] > 1$, or that there exist at least one substitution $\zeta \rightarrow \zeta^{\nu}$, $(\nu, n) = 1$, determining an automorphism σ of k/k'. Let H be the Galois group of k/k'. Consider the algebraic field extensions $k'(U) \subset k'(Y) \subset k(X)$. As k'(Y) is purely transcendental over k', and as $k'(Y)(\zeta) = k(X)$, the Galois group of k(X)/k'(Y) is equal to H. From this it follows that $\sigma X_j = X_{\overline{\nu j}}$ $(\overline{\nu j} \equiv \nu j \pmod n)$. Every $\sigma \in H$ determines uniquely a permutation of X (leaving X_n invariant), and we easily see that the product of two automorphisms σ and τ in H determines a permutation of X that is the product of the permutations corresponding to σ and τ. In this way H induces a permutation group H_n of the set X that is isomorphic to H, and the automorphisms of k(X)/k'(Y) can be obtained by permuting the set X according to H_n. So $X_1, \ldots, X_n$ are the zero of a polynomial with coefficients in k'(Y). This means that the elementary symmetric polynomials

$s_i = (-1)^i \ a_i(U_1,\dots,U_n) \quad (i=1,\dots,n)$ in $X_1,\dots,X_n$ lie in $k'(Y)$.

The s_i lie also in $k(U)$, so that $a_i, s_i \in k'(Y) \cap k(U)$. But $k'(U) \cap k(U) = k'(U)$ because of the fact that $k'(Y) \cap k'(U) = k'(U)$ and $\zeta \notin k'(Y)$. It is obvious that $k(X)$ is equal to $k'(Y)(X)$.

Theorem 2. The Galois group G of the polynomial (1) with respect to $k'(U)$, i.e. the Galois group of the field extension $k'(U)(X)/k'(U)$, is the non-abelian permutation group on X, obtained by taking all the products of the permutations in H_n and C_n. C_n is a normal divisor in G, the factor group G/C_n being isomorphic to H.

Proof. As H_n and C_n yield automorphisms of $k(X)/k'(Y)$ and $k(X)/k(U)$ respectively, the products $\sigma\pi$ ($\sigma \in H_n$, $\pi \in C_n$) represent automorphisms of $k(X)/k'(U)$. These $\sigma\pi$ are all different, for

$$\sigma_1 \pi_1 = \sigma_2 \pi_2,$$

with $\sigma_1, \sigma_2 \in H_n$, $\pi_1, \pi_2 \in C_n$, $\sigma_1 \neq \sigma_2$, $\pi_1 \neq \pi_2$, implies $\sigma_2^{-1}\sigma_1 = \pi_2 \pi_1^{-1}$, and this means that H_n and C_n would have an element $\neq e$ in common. This is however impossible, as every $\pi \in C_n$ moves X_n and every $\sigma \in H_n$ leaves X_n invariant.

As $[k(X) : k'(U)] = [k(X) : k(U)] \cdot [k(U) : k'(U)] =$ order of C_n . order of H_n, the set of products $\{\sigma\pi \ ; \sigma \in H_n, \pi \in C_n\}$ forms just all the automorphisms of $k(X)/k'(U)$, and is equal to the group G.

As $k(X)$ is normal with respect to $k'(X)$, C_n is a normal divisor in G, with factor group isomorphic to H.

As H_n is not transitive over X, the group G is non-abelian.

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

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