Galois theory of Salem polynomials

BY CHRISTOS CHRISTOPOULOS AND JAMES MCKEE
Department of Mathematics, Royal Holloway,
University of London, Egham Hill, Egham,
Surrey TW20 0EX

(*Received*)

Abstract

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible reciprocal polynomial of degree $2d$ with roots $r_1, 1/r_1, r_2, 1/r_2, \ldots, r_d, 1/r_d$. The corresponding trace polynomial $g(x)$ of degree d is the polynomial whose roots are $r_1 + 1/r_1, \ldots, r_d + 1/r_d$. If the Galois groups of f and g are G_f and G_g respectively, then $G_g \cong G_f/N$, where N is isomorphic to a subgroup of C_2^d. In a naive sense, the generic case is $G_f \cong C_2^d \rtimes S_d$, with $N \cong C_2^d$ and $G_g \cong S_d$. When $f(x)$ has extra structure this may be reflected in the Galois group, and it is not always true even that $G_f \cong N \rtimes G_g$. For example, for cyclotomic polynomials $f(x) = \Phi_n(x)$ it is known that $G_f \cong N \rtimes G_g$ if and only if n is divisible either by 4 or by some prime congruent to 3 modulo 4.

In this paper we deal with irreducible reciprocal monic polynomials $f(x) \in \mathbb{Z}[x]$ that are 'close' to being cyclotomic, in that there is one pair of real positive reciprocal roots and all other roots lie on the unit circle. With the further restriction that $f(x)$ has degree at least 4, this means that $f(x)$ is the minimal polynomial of a Salem number. We show that in this case one always has $G_f \cong N \rtimes G_g$, and moreover that $N \cong C_2^d$ or C_2^{d-1}, with the latter only possible if d is odd.

1. Introduction

Let

$$f(x) = x^{2d} + f_{2d-1}x^{2d-1} + \cdots + f_0$$

be a monic irreducible reciprocal polynomial of degree $2d$ with integer coefficients. For our purposes, *reciprocal* means that $f(x) = x^{2d}f(1/x)$, so that in particular $f_0 = 1$. The roots of $f(x)$ fall into reciprocal pairs, and we can conveniently label them

$$r_1\,,\ 1/r_1\,,\ r_2\,,\ 1/r_2\,,\ \ldots\,,\ r_d\,,\ 1/r_d\,. \tag{1·1}$$

The corresponding *trace polynomial*,

$$g(x) = x^d + g_{d-1}x^{d-1} + \cdots + g_0$$

has roots

$$s_1 = r_1 + 1/r_1\,,\ s_2 = r_2 + 1/r_2\,,\ \ldots, s_d = r_d + 1/r_d\,. \tag{1·2}$$

Let G_f, G_g be the Galois groups of f, g respectively. Since the splitting field of g is

contained in that of f, the Galois group G_g is a quotient of G_f — there is a natural group homomorphism $\pi : G_f \to G_g$ with kernel N, say. Thus $G_g \cong G_f/N$ and one speaks of G_f as being a group extension of N by G_g. Such an extension is said to *split* if one of the following equivalent statements holds (Theorem 6.5.3 of [**3**] and §I.7 of [**2**]):

- $G_f \cong N \rtimes G_g$;
- there is a group homomorphism $\psi : G_g \to G_f$ such that $\pi\psi = 1$;
- there is a subgroup H of G_f satisfying (i) $H \cong G_g$, (ii) $H \cap N = \{1\}$ (such a subgroup H is called a *complement* of N in G_f);
- there is a set of representatives of the cosets of N that forms a subgroup of G_f.

For some reciprocal polynomials $f(x)$ the extension of N by G_g splits, and for some it does not. For example, if $f(x) = \Phi_n(x)$ is the nth cyclotomic polynomial then in [**6**] it is shown that the extension splits if and only if either $4 \mid n$ or $p \mid n$ for some prime p with $p \equiv 3 \pmod 4$. In this cyclotomic case $N = C_2$ is cyclic of order 2, generated by complex conjugation.

In general, since elements of N send each r_i to either r_i or $1/r_i$, we see that each element of N swaps certain pairs of reciprocal roots, and that N is therefore a subgroup of C_2^d. In particular, N is abelian. The generic case (treated in [**6**]) has $G_g \cong S_d$ (the symmetric group acting on the d roots of g) and $N \cong C_2^d$.

In this paper we shall consider the case where $f(x)$ is a *Salem polynomial*, the minimal polynomial of a Salem number. This means that $f(x) \in \mathbb{Z}[x]$ is irreducible, reciprocal, monic, has degree at least 4, that exactly one pair of reciprocal roots are real and positive, and that all other roots have modulus 1. These polynomials may be thought of as being close to cyclotomic, but we shall see that the Galois theory is (unsurprisingly) strikingly different. In Section 2 we show that either $N \cong C_2^d$ or $N \cong C_2^{d-1}$, and that the latter is only possible if d is odd. Then in Section 3 we complete the proof of our main theorem:

THEOREM 1·1. *Let $f(x)$ be a Salem polynomial of degree $2d$, let $g(x)$ be its trace polynomial, and let G_f, G_g be the Galois groups of $f(x)$, $g(x)$ respectively. Then*

$$G_f \cong N \rtimes G_g$$

where N is the kernel of the natural map $\pi : G_f \to G_g$. Moreover either $N \cong C_2^d$ or $N \cong C_2^{d-1}$, with the latter possible only if d is odd.

To illustrate that both possibilities for N may be needed when d is odd, consider the following two examples with $d = 5$:

(i) $f(x) = x^{10} - 9x^9 - 10x^8 - 10x^7 - 10x^6 - 10x^5 - 10x^4 - 10x^3 - 10x^2 - 9x + 1$,

(ii) $f(x) = x^{10} - 2x^9 - 6x^8 - 10x^7 - 10x^6 - 10x^5 - 10x^4 - 10x^3 - 6x^2 - 2x + 1$.

In both cases the trace polynomial has Galois group S_5; in the former case $N \cong C_2^5$, but in the latter case $N \cong C_2^4$.

In related earlier work, Lalande [**4**] showed that if K is a real number field of degree $2d$ for which the group of units has rank d, and L is the Galois closure of K, then K is generated by a Salem number if and only if the Galois group of L over $\mathbb{Q}$ is a subgroup of $C_2^d \rtimes S_d$.

2. The structure of N when $f(x)$ is a Salem polynomial

Let Γ_f, Γ_g be the splitting fields of f, g respectively. Let $\delta_i = r_i - 1/r_i$ $(1 \leqslant i \leqslant d)$. Plainly $\Gamma_f = \Gamma_g(\delta_1, \ldots, \delta_d)$. Any element of N changes the sign of some δ_i (perhaps

none) and fixes others; elements of G_f send δ_i to $\pm\delta_{\sigma(i)}$ where σ is some permutation of $1, \ldots, d$. With $f(x)$ a Salem polynomial, there is a unique pair of reciprocal real positive roots r_j, $1/r_j$, and the corresponding δ_j is real; for all other i, the number δ_i is purely imaginary (has real part equal to 0) since $1/r_i = \overline{r}_i$.

Reordering $r_1, \ldots, r_d$, we may suppose that

$$\Gamma_f = \Gamma_g(\delta_1, \delta_2, \ldots, \delta_k)$$

with k minimal. For $1 \leqslant i \leqslant k$, let Γ_i be the field $\Gamma_g(\delta_1, \ldots, \delta_i)$, and for convenience we also define $\Gamma_0 = \Gamma_g$. Thus $\Gamma_0 = \Gamma_g$, $\Gamma_k = \Gamma_f$, and $|N| = [\Gamma_f : \Gamma_g] = 2^k$. For $1 \leqslant i \leqslant k$, define σ_i to be the automorphism of Γ_i that changes the sign of δ_i and fixes Γ_{i-1} (such an automorphism exists since $\Gamma_i = \Gamma_{i-1}(\delta_i)$ and $\delta_i^2 = s_i^2 - 4 \in \Gamma_g \subseteq \Gamma_{i-1}$).

We aim to show that $k \geqslant d-1$, under the assumption that $f(x)$ is a Salem polynomial. For this we are helped by the following Lemma, which applies more generally.

LEMMA 2·1. *With notation as above,*

$$\delta_d = \lambda \prod_{i=1}^{k} \delta_i^{e_i} \tag{2·1}$$

for some $\lambda \in \Gamma_g$ and, for each i between 1 and k, some choice of $e_i \in \{0, 1\}$.

Proof. (This is trivial if $k = d$, but there is no need to exclude this case from the following proof.)

We certainly have $\delta_d \in \Gamma_k$, and so can write

$$\delta_d = w\delta_k + w'$$

where w, $w' \in \Gamma_{k-1}$. Applying σ_k gives

$$\sigma_k(\delta_d) = -w\delta_k + w' .$$

Since this must equal $\pm\delta_d$ (for $\delta_d^2 = s_d^2 - 4 \in \Gamma_g$ and σ_k fixes Γ_g) we deduce that either $\delta_d = w\delta_k$ or $\delta_d = w'$.

Relabelling w' as w if needed, we have $\delta_d = w\delta_k^{e_k}$ with $e_k \in \{0, 1\}$ and $w \in \Gamma_{k-1}$. We then write

$$w = w_1\delta_{k-1} + w_1'$$

with w_1, $w_1' \in \Gamma_{k-2}$. Applying σ_{k-1} we deduce as above that one of w_1, w_1' is zero, and relabelling we have $w = w_1\delta_{k-1}^{e_{k-1}}$ with $e_{k-1} \in \{0, 1\}$. Thus

$$\delta_d = w_1\delta_{k-1}^{e_{k-1}}\delta_k^{e_k} .$$

Proceeding similarly we write $w_1 = w_2\delta_2^{e_{k-2}}$, and so on, until we reach (after a finite number of steps) the desired equation (2·1). □

We now use this expression for δ_d to show that $k \geqslant d-1$, and that if $k = d-1$ then each e_i is 1.

LEMMA 2·2. *With notation as above, and with $f(x)$ a Salem polynomial, one must have $k \geqslant d-1$, and if $k = d-1$ then*

$$\delta_d = \lambda \prod_{i=1}^{d-1} \delta_i \tag{2·2}$$

for some $\lambda \in \Gamma_g$. Moreover if $k = d-1$ then d must be odd.

Proof. If $k = d$ then there is nothing to prove.

If $k \leqslant d-1$, then by Lemma 2·1, after some relabelling, we can write

$$\delta_d = \lambda \prod_{i=1}^{m} \delta_i \,, \tag{2·3}$$

where $\lambda \in \Gamma_g$ and $m \leqslant k \leqslant d-1$. We now show that in any equation of the shape (2·3) we must have $m \geqslant d-1$, and hence $k = d-1$. Suppose to the contrary that $m < d-1$. Let j be the unique index between 1 and d for which δ_j is real (all others being purely imaginary). If δ_j does not appear on either side of (2·3), then m must be odd, so that the right hand side of (2·3) is purely imaginary. Then applying an element of G_f that sends r_d to r_j would make the left side of (2·3) become real, but would keep the right side purely imaginary (λ is sent to some element of $\Gamma_g \subseteq \mathbb{R}$), giving a contradiction. Thus δ_j must appear on one side of (2·3), and m must be even. Then applying an element of G_f that sends r_{m+1} to r_j, we again derive a contradiction from (2·3), with one side becoming real and the other side becoming purely imaginary. Thus $m = d-1 = k$. And we must now have d odd, or else one side of (2·3) would be real and the other purely imaginary. □

Notice where we used the hypothesis that $f(x)$ (with degree at least 4) is a Salem polynomial: we needed $\Gamma_g \subseteq \mathbb{R}$, which requires all $r_i + 1/r_i$ to be real; we needed all but one of the $r_i - 1/r_i$ to be purely imaginary, which (together with $r_1 + 1/r_i$ real) forces r_i to be on the unit circle; and we needed one of the $r_i - 1/r_i$ to be real, giving a unique pair of reciprocal real roots r_i, $1/r_i$. We needed $f(x)$ irreducible so that its Galois group acts transitively on the roots. We did not need the real roots to be positive, and of course the Galois group of $f(-x)$ is the same as that of $f(x)$.

We have done most of the work in establishing the structure of N, which we record in a Proposition.

PROPOSITION 2·3. *Let $f(x)$ be a Salem polynomial of degree $2d$ with splitting field Γ_f and Galois group G_f; let $g(x)$ be its trace polynomial with splitting field Γ_g and Galois group G_g. Then $G_g \cong G_f/N$, where either $N \cong C_2^d$ or $N \cong C_2^{d-1}$.*

If $N \cong C_2^d$, then as a group of permutations of the roots of $f(x)$ given by (1·1), N is generated by all transpositions of the form $(r_i\ 1/r_i)$. If $N \cong C_2^{d-1}$, then d is odd and N is generated by all the $(r_i\ 1/r_i)(r_j\ 1/r_j)$. This latter case occurs if and only if the discriminant of $f(x)$ is a square in Γ_g.

Before proving this, let us note that one consequence of Proposition 2·3 is that if d is even then the discriminant of $f(x)$ is not a square in Γ_g. One can see this directly as follows. Let Δ_f, Δ_g be the discriminants of $f(x)$, $g(x)$ respectively. Using the identity

$$\big((r_i + 1/r_i) - (r_j + 1/r_j)\big)^2 = (r_i - r_j)(r_i - 1/r_j)(1/r_i - r_j)(1/r_i - 1/r_j)$$

one checks that

$$\Delta_f = \Delta_g^2 \delta_1^2 \delta_2^2 \cdots \delta_d^2 \,. \tag{2·4}$$

Now for the unique j such that r_j is real we have $\delta_j^2 > 0$, and for all other i (such that $|r_i| = 1$) we have $\delta_i^2 < 0$. If d is even, it follows that $\Delta_f < 0$, so it is not a square in

$\Gamma_g \subseteq \mathbb{R}$. One might ask whether there is anything more that can be said in the event that the discriminant of $f(x)$ is actually a square in $\mathbb{Q}$: for this, see Proposition 4·2 below.

Proof of Proposition 2·3 The first part follows from Lemma 2·2, using $|N| = |G_f|/|G_g| = [\Gamma_f : \Gamma_g] = 2^k$.

For the second part, note that N is certainly a subgroup of the group T generated by all transpositions of the form $(r_i\ 1/r_i)$. Since T has order 2^d we are done in the case $|N| = 2^d$. For the case $N \cong C_2^{d-1}$, note that any permutation in N must be even, for applying an odd permutation in T to (2·3) (with $m = d-1$) would change the sign of one side but not the other (recall that $\delta_i = r_i - 1/r_i$). To see that this case ($N \cong C_2^{d-1}$) occurs if and only if the discriminant of $f(x)$ is a square in Γ_g, notice that the square root of the discriminant of $f(x)$ is fixed by N (and hence lies in Γ_g) precisely when N contains only even permutations (see (2·4)). □

3. **Proof of Theorem 1·1**

We first dispose of the case $N \cong C_2^d$, which is routine but sets the scene for the more delicate case $N \cong C_2^{d-1}$. The group G_f is a subgroup of the symmetric group S_{2d} acting on the roots (1·1). More strongly, G_f is a subgroup of P_{2d}, which we define by

$$P_{2d} = \left\{\sigma \in S_{2d} \mid \text{if } \sigma(r_i) = r_j^e \text{ (with perforce } e = \pm 1) \text{ then } \sigma(1/r_i) = r_j^{-e}\right\} .$$

Let τ be any element of G_g (a subgroup of S_d, permuting the roots (1·2)), and let $\widehat{\tau} \in G_f$ be a preimage of τ under π. If τ cyclically permutes $s_{i_1}, \ldots, s_{i_t}$, then $\widehat{\tau}$ acts on $r_{i_1}, 1/r_{i_1}, \ldots, r_{i_t}, 1/r_{i_t}$ either by a permutation of the shape

$$(r_{i_1}\ r_{i_2}^{e_2}\ \cdots\ r_{i_t}^{e_t})(1/r_{i_1}\ 1/r_{i_2}^{e_2}\ \cdots\ 1/r_{i_t}^{e_t}) \tag{3·1}$$

for some $e_2, \ldots, e_t \in \{1, -1\}$, or alternatively of the shape

$$(r_{i_1}\ r_{i_2}^{e_2}\ \cdots\ r_{i_t}^{e_t}\ 1/r_{i_1}\ 1/r_{i_2}^{e_2}\ \cdots\ 1/r_{i_t}^{e_t}) \tag{3·2}$$

for some $e_2, \ldots, e_t \in \{1, -1\}$. We count 2^t possibilities for permutations of the shape (3·1) or (3·2). Multiplying over all the cycles that make up τ, we see that there are 2^d elements of P_{2d} that induce the permutation τ on the roots of $g(x)$. These include all the elements in the coset $N\widehat{\tau}$. Since we are supposing here that $|N| = 2^d$, *all* of the 2^d possibilities in P_{2d} that induce τ must actually be in G_f. In particular, if

$$\tau = (s_{i_1}\ \cdots\ s_{i_t})\cdots , \tag{3·3}$$

then there is an element $\widetilde{\tau} \in G_f$ given by

$$\widetilde{\tau} = (r_{i_1}\ \cdots\ r_{i_t})(1/r_{i_1}\ \cdots\ 1/r_{i_t})\cdots , \tag{3·4}$$

copying the way that τ acts on the list $s_1, \ldots, s_d$ to each of the lists $r_1, \ldots, r_d$ and $1/r_1, \ldots, 1/r_d$ simultaneously. The set of all the $\widetilde{\tau}$ as τ runs through G_g forms a subgroup $\widetilde{G}_g$ that is a complement of N in G_f (visibly $\widetilde{G}_g \cong G_g$, and $\widetilde{G}_g \cap N = \{1\}$).

For the case $N \cong C_2^{d-1}$ the above argument breaks down: we do not know which 2^{d-1} of the possible 2^d lifts of $\tau \in G_g$ to P_{2d} lie in the coset $N\widehat{\tau}$, and it is not immediate that we can pick lifts that form a subgroup. But in the case $N \cong C_2^{d-1}$ we have that d is odd (Proposition 2·3). If we let T_f be a Sylow 2-subgroup of G_f (necessarily containing N, since N is normal in G_f), and let $T_g = \pi(T_f)$, then T_g will be a Sylow 2-subgroup of G_g. Since T_g has order a power of 2, and the number of roots of $g(x)$ is odd, there must be a

root of $g(x)$ that is fixed by T_g. Relabelling, we may suppose that s_d is fixed by T_g. Then each element of T_f sends r_d to one of r_d or $1/r_d$. Let σ be the transposition $(r_d\ 1/r_d)$, acting on the roots of $f(x)$. By Proposition 2·3, $\sigma \notin N$, and hence $\sigma \notin T_f$.

Take any $\tau \in T_g$. Let $\widehat{\tau}$ be any element of P_{2d} acting on the roots of $f(x)$ that induces the action of τ on the roots of $g(x)$. Then *at most* one of $\widehat{\tau}$ and $\widehat{\tau}\sigma$ is in T_f, for if both were then so would be σ. We deduce that of the 2^d elements of P_{2d} that induce the action of τ on the roots of $g(x)$, *exactly* one of each of the 2^{d-1} compatible permutations of r_1, $1/r_1$, …, r_{d-1}, $1/r_{d-1}$ occurs for some element of T_f, and for each of these the roots r_d, $1/r_d$ are of course either fixed or swapped.

Defining $\widetilde{\tau} \in P_{2d}$ as above, permuting each of the lists r_1, …, r_d and $1/r_1$, …, $1/r_d$ in the same way that τ permutes s_1, …, s_d, we see that G_f contains an element $\widetilde{\tau}\sigma^{e(\tau)}$, where $e(\tau) \in \{0, 1\}$. Note that here $\widetilde{\tau}$ fixes r_d and $1/r_d$. The set of all such lifts forms a subgroup H: we must have $e(\tau_1\tau_2) \equiv e(\tau_1) + e(\tau_2) \pmod 2$ or else we would get the contradictory conclusion that $\sigma \in T_f$. Thus H gives a subgroup of T_f that is isomorphic to T_g, and this H is a complement of N in T_f (the intersection of H and N is $\{1\}$).

Now we appeal to Theorem 7.43 of [**5**] (Gaschütz, 1952): a normal abelian p-subgroup of a finite group G has a complement in G if and only if it has a complement in a Sylow p-subgroup of G. Our group N is a normal abelian 2-subgroup of G_f, with a complement in T_f, so it has a complement in G_f, completing the proof of Theorem 1·1.

4. **Finding an explicit complement of N**

Extending the notation of the previous section, let $\widetilde{G}_g$ be the subgroup of P_{2d} (permuting the roots of f, as before) comprising all the $\widetilde{\tau}$ given by (3·4) for $\tau \in G_g$ given by (3·3). Then $\widetilde{G}_g$ is a subgroup of P_{2d} that is isomorphic to G_g, but viewing G_f as a subgroup of P_{2d} we might not have $\widetilde{G}_g \subseteq G_f$. In any event, we note the following:

LEMMA 4·1. *With notation as above, $G_f \cong N\widetilde{G}_g$.*

Proof. Let $\overline{G}_g$ be a complement of N in G_f (still viewed as a subgroup of P_{2d}), with $\tau \mapsto \overline{\tau}$ being an isomorphism from G_g to $\overline{G}_g$. Since $\overline{\tau}$ and $\widetilde{\tau}$ induce the same action on the roots of g, we must have that if $\overline{\tau}(r_i) = r_j^e$ then $\widetilde{\tau}(r_i) = r_j^{\pm e}$. Hence, from the structure of N (generated by the $(r_i\ 1/r_i)$ or $(r_i\ 1/r_i)(r_j\ 1/r_j)$ in the two possible cases) we see that

$$\widetilde{\tau} n \widetilde{\tau}^{-1} = \overline{\tau} n \overline{\tau}^{-1}$$

for all $n \in N$. Hence

$$n\widetilde{\tau} \mapsto n\overline{\tau}$$

defines an isomorphism between $N\widetilde{G}_g$ and $G_f = N\overline{G}_g$. □

Hence if we have computed G_g explicitly as a subgroup of the group of permutations of its roots (1·2), then we have an explicit construction of a subgroup of P_{2d} that is isomorphic to G_f. In many cases we have more than an isomorphism and in fact $G_f = N\widetilde{G}_g$. The first part of the proof of Theorem 1·1 establishes this whenever $N \cong C_2^d$, and this is part (i) of the next Proposition.

PROPOSITION 4·2. *Let f be a Salem polynomial of degree $2d$, discriminant Δ_f, and with trace polynomial g. Let G_f and G_g be the Galois groups of f and g. We view G_f as a subgroup of P_{2d} (a subgroup of the group of permutations of its roots (1·1)); and G_g*

is a subgroup of the group of permutations of its roots (1·2). For $\tau \in G_g$ given by (3·3), we define $\widetilde{\tau} \in P_{2d}$ via (3·4), and then define $\widetilde{G}_g$ to be the set of all the $\widetilde{\tau}$ for $\tau \in G_g$. Let N be the kernel of the natural map from G_f to G_g. Then

(i) *if $N \cong C_2^d$, then $G_f = N\widetilde{G}_g$;*
(ii) *if $N \cong C_2^{d-1}$ and $\sqrt{\Delta_f} \in \mathbb{Q}$, then $G_f = N\widetilde{G}_g$.*

Proof. The first part was established in the proof of Theorem 1·1, so we are left with the case where $N \cong C_2^{d-1}$ and $\sqrt{\Delta_f} \in \mathbb{Q}$. Then N is generated by the pairs of transpositions $(r_i\ 1/r_i)(r_j\ 1/r_j)$, and G_f comprises only even permutations of the roots of f. Take any $\tau \in G_g$, and let $\widehat{\tau}$ be any lift to G_f. For each cycle

$$(s_{i_1}\ \cdots\ s_{i_t}) \tag{4·1}$$

in the cycle decomposition of τ, the corresponding part of $\widehat{\tau}$ will look like either (3·1) or the odd permutation (3·2). Since $\widehat{\tau}$ is even, there must be an even number of cycles in the decomposition of τ for which the relevant part of $\widehat{\tau}$ has the form (3·2): given any pair of such cycles, say (4·1) and

$$(s_{j_1}\ \cdots\ s_{j_u})\,,$$

applying the element $(r_{i_t}\ 1/r_{i_t})(r_{j_u}\ 1/r_{j_u})$ (which is in N) to the right of $\widehat{\tau}$ breaks both the relevant cycles of $\widehat{\tau}$ into the shape (3·1). After a finite number of such 'breaks', we transform $\widehat{\tau}$ into a product of disjoint pairs of cycles of the shape (3·1), and we may now suppose that $\widehat{\tau}$ is of this form.

Next we apply elements of N to transform $\widehat{\tau}$ into $\widetilde{\tau}$, as given by (3·4). If for one of the pairs of cycles of the shape (3·1) we have $e_2 = -1$, then apply $(r_1\ 1/r_1)(r_2\ 1/r_2)$ on the right to change the sign of e_2; then if $e_3 = -1$, apply $(r_2\ 1/r_2)(r_3\ 1/r_3)$; and so on, working our way through all pairs of cycles. We conclude that $\widetilde{G}_g \subseteq G_f$, and it is easily seen to be a complement of N, completing the proof of the Proposition. □

If $\sqrt{\Delta_f}$ is in Γ_g but not in $\mathbb{Q}$, then the hypotheses of the Proposition fail, and it is possible that the conclusion fails too. For example, with

$$f(x) = x^6 - 5x^5 + 3x^3 - 5x + 1$$

one can check that $\widetilde{G}_g$ is not contained in G_f.

Acknowledgements. Theorem 1·1 appeared in the first author's PhD thesis [**1**]. This paper contains a considerable simplification of his original proof. We are grateful to the referee for a careful reading of the manuscript, and for helpful comments.

REFERENCES

[**1**] C. Christopoulos. On Galois groups of Salem polynomials. PhD. thesis. University of London (2008).
[**2**] C.W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras* (Wiley, 1988).
[**3**] M. Hall, Jr.. *The theory of groups* (Chelsea, 1976).
[**4**] F. Lalande. Corps de nombres engendrés par un nombre de Salem. *Acta Arith.* **88** (1999), 191–200.
[**5**] J.J. Rotman. *An introduction to the theory of groups, Fourth edition.* Graduate Texts in Mathematics **148** (Springer, New York, 1995).
[**6**] P. Viana and P.M. Veloso. Galois Theory of Reciprocal Polynomials. *Amer. Math. Monthly* **109** (2002), No. 5, 466–471.