JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

LEONARDO CANGELMI

Polynomials whose Galois groups are Frobenius groups with prime order complement

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994), p. 391-406

<http://www.numdam.org/item?id=JTNB_1994__6_2_391_0>

Journal de Théorie des Nombres
de Bordeaux **6** *(1994), 391–406*

Polynomials whose Galois groups are Frobenius groups with prime order complement

by LEONARDO CANGELMI

RÉSUMÉ – On donne une caractérisation effective des polynômes irréductibles de degré n à coefficients entiers dont les groupes de Galois sur $\mathbb{Q}$ sont des groupes de Frobenius avec noyau d'ordre n et complément d'ordre premier.

ABSTRACT – We give an effective characterization theorem for integral monic irreducible polynomials f of degree n whose Galois groups over $\mathbb{Q}$ are Frobenius groups with kernel of order n and complement of prime order.

0. Introduction

Recently, there has been some interest in the problem of giving effective characterizations of polynomials of given degree whose Galois groups over $\mathbb{Q}$ are Frobenius groups of some particular kind. Recall that a Frobenius group can always be described as a semi–direct product $N \rtimes H$ and that N and H are respectively called the (Frobenius) kernel and (Frobenius) complement of the group; moreover, the action by conjugation of H over N has to be fixed–point–free, $|H|$ has to divide $|N| - 1$ and the group can always be represented as a transitive permutation group on $|N|$ elements, so that it is of degree $|N|$. Bruen, Jensen and Yui [BJY] proved a characterization theorem for polynomials of prime degree p whose Galois groups are Frobenius groups of degree p (in this case, the Frobenius complements necessarily are cyclic of order dividing $p - 1$). They posed the problem of finding analogous characterizations for polynomials whose Galois groups are Frobenius of prime power degree or Frobenius in general.

In this paper, we give a characterization theorem for polynomials of arbitrary degree n whose Galois groups are Frobenius groups of degree n and with complements of prime order p, where p is forced to divide $n - 1$.

1991 *Mathematics Subject Classification.* Primary 12F10, 12Y05; Secondary 12F12, 12-04.

Key words and phrases. Effective characterization of polynomials with given Galois groups, Frobenius groups with prime order complement.

Manuscrit reçu le 24 Juillet 1993, version définitve le 30 Septembre 1994.

It is worth noticing that in the present case the kernels are as general as it is permitted by the properties of a Frobenius group, that is, they have just to be nilpotent; while the complements are restricted to be cyclic of prime degree. The method we use is derived from one by Williamson [Will], who characterized odd degree polynomials whose Galois groups are generalized dihedral groups. Indeed, these groups are Frobenius with complements of order 2 and abelian kernels; the fundamental observation is that his method does not require the kernel to be abelian, but just the group to be Frobenius. Moreover, we make the characterization completely effective, we discuss the practical problems arising and we justify theoretically its effectiveness referring to "the least prime" in Chebotarev density theorem.

In Section I, we recall the definition of Frobenius group and we show some interesting properties of Frobenius groups with complement of prime order: these can be described as semi–direct products $N \rtimes Z_p$ satisfying some simple conditions.

In Section II, we characterize monic irreducible polynomials, with rational integer coefficients, of degree n, whose Galois groups over $\mathbb{Q}$ are Frobenius groups with kernel of order n and complement of prime order p; that is, groups of the form $N \rtimes Z_p$, with $|N| = n$, which are Frobenius.

In Section III, we point out some effective conditions which are useful in testing whether a polynomial has Galois group as above or not; such conditions involve the computation of several resultant polynomials and their factorization. Then, we apply the characterization theorem to some explicit polynomials, showing that their Galois groups are Frobenius groups with prime order complement.

The author is grateful to Prof. R. Dvornicich (University of Pisa, Italy) for some suggestions and for several fruitful discussions.

Our notations are as follows.

If S is a set, $|S|$ denotes its cardinality.

If g is an element of a group which acts on a set S, $\mathrm{Fix}\, g$ denotes the set of the elements of S fixed by g.

For a group G, $\mathrm{Aut}\,(G)$ denotes the groups of automorphisms of G. If A and B are two groups, $A \rtimes B$ denotes any possible semi–direct product of them.

If n is a positive integer, Z_n, ζ_n and C_n denote respectively the cyclic group of order n, a primitive n–th root of unity and the field $\mathbb{Q}(\zeta_n)$; if n is a prime power, $\mathbb{F}_n$ denotes the field of n elements.

For a polynomial $f \in \mathbb{Z}[X]$, $\mathrm{spl}(f)$, $\mathrm{Gal}(f)$, and D_f denote the splitting field of f, the Galois group of the splitting field and the discriminant of f.

For any number field L, D_L denotes the discriminant of L over $\mathbb{Q}$ and $\mathcal{O}_L$ denotes the ring of integral elements of L.

For any finite extension of number fields $L \supset K$ (also written as L/K) and any $f \in L[X]$, $N_{L/K}(f)$ denotes the norm of f over K. For any finite normal extension of number fields L/K, $\mathrm{Gal}(L/K)$ denotes its Galois group.

If k is a field or a polynomial ring, and $f(X)$ and $g(X)$ are two polynomials in $k[X]$, $\mathrm{Res}_X(f(X), g(X))$ denotes the resultant of f and g with respect to the indeterminate X.

Other notations will be recalled and adopted in the course of the paper.

I. Frobenius groups

I.0. General results

DEFINITION I.0.1. A permutation group G on a set Ω with $|\Omega| = n$ is said to be a group of degree n.

DEFINITION I.0.2. A transitive group G of degree n is said to be a regular group if, and only if, $|\mathrm{Fix}\, g| = 0$, for all $g \in G \backslash \{1\}$.

DEFINITION I.0.3. A transitive group G of degree n is said to be a Frobenius group if, and only if, $|\mathrm{Fix}\, g| \leq 1$, for all $g \in G \backslash \{1\}$, and $|\mathrm{Fix}\, g| = 1$, for some $g \in G \backslash \{1\}$.

It is trivial to see that a transitive group G of degree n is regular if, and only if, $|G| = n$. On the other hand, a transitive group G of degree n is a Frobenius group if, and only if, it has a non trivial subgroup H, of index n, such that $H \cap H^g = \{1\}$, for all $g \in G \backslash H$ (anyone of the stabilizers can be taken as H). This property allows to deduce a very strong theorem about the structure of Frobenius groups.

THEOREM I.0.4 (FROBENIUS). *Let G be a Frobenius group of degree n and H be a subgroup (of index n) such that $H \cap H^g = \{1\}$, for all $g \in G \backslash H$. Then the subset*

$$N = G \setminus \bigcup_{g \in G} (H \backslash \{1\})^g$$

is a normal subgroup (of order n), such that $G = NH$ and $N \cap H = \{1\}$.

Proof. See, e.g., [Rob].

Since the conjugates of H are exactly the stabilizers of the points of Ω, the elements of $N\backslash\{1\}$ are precisely those in G with no fixed points. N is called the (Frobenius) kernel of G, while H is said to be a (Frobenius) complement of G. Note that N turns out to be a regular group of degree n and that G can be written as a semi–direct product, namely $G = N \rtimes H$. Furthermore, G satisfies some other strong necessary conditions, as it is stated in the following proposition.

PROPOSITION I.0.5. *Let $G = N \rtimes H$ be a Frobenius group of degree n, $|N| = n$ and $|H| = h$. Then the following conditions hold:*

a) $C_G(H) = C_H(H)$.
b) *H is core–free (i.e., it does not contain non–trivial normal subgroups of G).*
c) $h \mid n - 1$.
d) (Thompson) *N is nilpotent.*

Proof. See, e.g., [Rob].

I.1. Frobenius groups with prime–order complement

Let N be a group of order n having an automorphism θ of prime order p and let Z_p denote the cyclic group of order p. We can construct the semi–direct product $G = N \rtimes_\theta Z_p$: if $Z_p = \langle\tau\rangle$, then we set $\tau x = \theta(x)\tau$, for all $x \in N$. Then, we may verify whether G is Frobenius by means of several different conditions.

PROPOSITION I.1.1. *Let $G = N \rtimes_\theta Z_p$, $n = |N|$ and $p \nmid n$. Then the following conditions are equivalent:*

a) *G is a Frobenius group of degree n.*
b) $C_G(Z_p) = Z_p$.
c) $\mathrm{Fix}\,\theta = \{1\}$.
d) *For any $x \in N$, there exists exactly one element $y \in N$ such that $x = y^{-1}\theta(y)$.*
e) $x\theta^i(x)\cdots\theta^{(p-1)i}(x) = 1$, *for all $x \in N$ and for all $i = 1, \ldots, p-1$.*
f) *Any element in $G\backslash N$ has order p.*
g) *G has exactly n Sylow p–subgroups.*

Proof.

a)⇒b): see Proposition I.0.5 (a).
b)⇒c): by the very definition of G, we have that $\mathrm{Fix}\,\theta = C_N(\tau) = C_N(Z_p)$; hence, $\mathrm{Fix}\,\theta = \{1\}$, because the only elements commuting with τ are in Z_p.

c)⇒d): if $x^{-1}\theta(x) = y^{-1}\theta(y)$, with x and y in N, then $yx^{-1} = \theta(yx^{-1})$ and therefore $yx^{-1} = 1$.

d)⇒e): let $y = x\theta(x)\cdots\theta^{p-1}(x)$: then $\theta(y) = \theta(x)\cdots\theta^{p-1}(x)x = y^x$. We may write x in the form $z^{-1}\theta(z)$ and hence we get $\theta(zyz^{-1}) = zyz^{-1}$; by the uniqueness of such expression, we get $zyz^{-1} = 1$, hence $y = 1$. This proves the implication in the case $i = 1$. For the general case, note that condition (e) for $i = 1$ implies condition (c); on the other hand, by the primeness of p, we have $\mathrm{Fix}\,\theta = \mathrm{Fix}\,\theta^i$. So θ^i is an automorphism of N with the same properties as θ and therefore the assertion holds for all i.

e)⇒f): any element in $G\backslash N$ can be written in the form $x\tau^i$, for some $x \in N$ and some $i \in \{1,\ldots,p-1\}$: then $(x\tau^i)^p = 1$, since $(x\tau^i)^p = x\theta^i(x)\cdots\theta^{(p-1)i}(x)\tau^{ip}$.

f)⇒g): G contains exactly $|G\backslash N| = n(p-1)$ elements of order p and they give rise to exactly n subgroups of order p.

g)⇒a): Z_p has exactly n conjugates and anyone of them can be written as Z_p^x, for some $x \in N$; if $g \in G\backslash Z_p$, then $Z_p^g = Z_p^x$ for some $x \in N\backslash\{1\}$, hence $Z_p \neq Z_p^g$, and therefore $Z_p \cap Z_p^g = \{1\}$.

Condition (c) of the previous proposition says that the automorphism θ is fixed–point–free.

A Frobenius group with kernel N and complement Z_p will be denoted by $\mathrm{Fr}\,(N,p)$. It is plain that such a group satisfies the following properties, besides the ones claimed in Proposition I.1.1 (cf. Proposition I.0.5):

- $\mathrm{ord}\,(\theta) = p$.
- $p \mid n-1$.
- N is nilpotent.
- $p \mid |\mathrm{Aut}\,(N)|$.

In particular, N is the direct product of its Sylow subgroups: if $q \mid n$ and N_q is the Sylow q–subgroup of N, then $\theta|N_q$ is a fixed–point–free automorphism of N_q of order p. Conversely, given a fixed–point–free automorphism of order p for each of the Sylow subgroups of N, it is determined a fixed–point–free automorphism of order p of N. Therefore, the study of groups as $\mathrm{Fr}\,(N,p)$ is reduced to that of Frobenius groups with Z_p as complement and a q–group as kernel; and this is equivalent to the study of fixed–point–free automorphisms of order p of q–groups, with $q \neq p$.

I.2. Cycle structure of elements of $\mathrm{Fr}\,(N,p)$

In general, given a permutation group G of degree n and assigned a representation of G as a subgroup S of S_n, any element $g \in G$ gives rise to

a partition $\pi(g)$ of n: in fact, g can be written as a permutation of degree n (via the given representation of G), and as such it induces a partition of n given by the lengths of the cycles in the expression of g as product of disjoint cycles. Note that for any permutation of $\{1,\dots,n\}$, the new identification of G with a subgroup of S_n is given by a conjugate of S; hence the partition $\pi(g)$ remains unchanged.

We say that an element g in a group G of degree n is of type π, where π is a given partition of n, if, and only if, $\pi(g) = \pi$, for a given representation of G as a permutation group of degree n. We will write "partitions" in multiplicative form; that is, $n_1^{e_1} \cdot n_2^{e_2} \cdots$ will denote the partition of $\sum e_i n_i$ given by e_1 times n_1, e_2 times n_2, ...

PROPOSITION I.2.1. *Let $G = \mathrm{Fr}\,(N,p)$ and represent G as a permutation group of degree n. Then the partition types induced by G are the following:*

- 1^n, *for the identity of G.*
- $1 \cdot p^{(n-1)/p}$, *for each element in $G\backslash N$.*
- $n_1 \cdots n_r$, *with some $n_j \geq 2$ such that $p \nmid n_j$ and $n_j \mid n$, for each element in $N\backslash\{1\}$.*

Proof. Each element g in $G\backslash N$ has order p and so it is product of disjoint cycles of length p or 1; moreover, since G is Frobenius of degree n, any element can fix at most one point. Hence the only possibility for $\pi(g)$ is to be equal to $1 \cdot p^{(n-1)/p}$. For the elements in $N\backslash\{1\}$, note that they fix no points and that $p \nmid n$.

II. Characterization of polynomials of degree n with $\mathrm{Fr}\,(N,p)$ as Galois groups

II.0. Factorization types of polynomials

Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree n and let π be a partition of n. We say that f is of type π if, and only if, the partition of n given by the degrees of the irreducible factors of f is π. We say that $f \bmod q$ is of type π, where q is a rational prime, if, and only if, the partition of n given by the degrees of the irreducible factors $\bmod q$ of f is π. Again, if E is any number field, we say that f over E is of type π if, and only if, the partition of n given by the degrees of the irreducible factors over E of f is π.

We have the following deep relations between the factorization types of f and the cycle structure of the elements of $\mathrm{Gal}\,(f)$ (this can be faithfully represented as a permutation group of degree n, on the set of roots of f,

and any permutation of the roots reflects on taking a conjugate of the given group representing $\mathrm{Gal}(f)$ in S_n).

LEMMA II.0.1. *Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree n and let π be a partition of n. Let q denote any rational prime such that $q \nmid D_f$ and let $G = \mathrm{Gal}(f)$. Put $L = \mathrm{spl}(f)$.*

a) (Dedekind) *If $f \bmod q$ is of type π, then G contains an element of type π.*
b) (Frobenius) *If G contains elements of type π, then the density of q's such that $f \bmod q$ is of type π is positive.*
c) (Chebotarev) *The density of q's such that $f \bmod q$ is of type π is equal to the proportion of elements in G of type π.*
d) (Lagarias, Odlyzko et al.) *If G contains elements of type π, then there exists q such that $f \bmod q$ is of type π and $q \leq (D_L)^C$, where C is an effectively computable absolute constant; assuming the Generalized Riemann Hypothesis for L, one has $q \leq 70(\log D_L)^2$.*

Proof.

a) See, e.g., [Jac, pp. 302–304].
b) See [Frob].
c) See, e.g., [Lang, pp. 168–170].
d) See [LMO] and [Oes].

II.1. Characterization theorem

Let $L/\mathbb{Q}$ be a normal extension and let K be a subfield of L such that L/K has degree n, $K/\mathbb{Q}$ is a cyclic extension of prime degree p and $p \nmid n$. Put $G = \mathrm{Gal}(L/\mathbb{Q})$ and $N = \mathrm{Gal}(L/K)$; then, since $(p, n) = 1$, $L/\mathbb{Q}$ splits at K and $G = N \rtimes_\theta Z_p$. Moreover, K is the unique subfield of L of degree p over $\mathbb{Q}$, because N is the unique subgroup of G of order n. The product $N \rtimes_\theta Z_p$ is direct if, and only if, $\mathrm{Fix}\,\theta = N$; if this is not the case, then Z_p is not normal and therefore is core–free.

PROPOSITION II.1.0. *Let $L/\mathbb{Q}$ be a normal extension of degree pn, with $\mathrm{Gal}(L/\mathbb{Q}) = N \rtimes_\theta Z_p$ and $p \nmid n$. Then the product is not direct if, and only if, there exists a monic irreducible polynomial f, with integer coefficients and of degree n, such that $L = \mathrm{spl}(f)$.*

Proof. If the product is not direct, Z_p is core–free and the minimal polynomial of an integer primitive element of $L^{Z_p}/\mathbb{Q}$ satisfies the required properties. If the product is direct, L contains a unique field of degree n over $\mathbb{Q}$, hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$, for all roots α and α' of f; so, $\mathrm{spl}(f) = \mathbb{Q}(\alpha) \neq L$.

In general, a normal extension $L/\mathbb{Q}$ whose Galois group is a non–direct product as above might also be given as the splitting field of an irreducible polynomial of degree not equal to n; anyway, the previous proposition says that we can always think of it as the splitting field of a polynomial of degree n.

For the rest of this subsection, $f \in \mathbb{Z}[X]$ will denote a monic irreducible polynomial of degree n and we will put $G = \mathrm{Gal}(f)$ and $L = \mathrm{spl}(f)$.

If $G = \mathrm{Fr}(N,p)$, f is irreducible and normal over L^N, since N is regular; moreover, from Proposition I.2.1 and Lemma II.0.1, we know that there exists a rational prime q such that $f \bmod q$ is of type $1 \cdot p^{(n-1)/p}$. Such conditions turn out to be also sufficient, as we are now going to show in two steps.

PROPOSITION II.1.1. *Let p be a rational prime such that $p \nmid n$. Then the following conditions are equivalent:*

- *$G = N \rtimes_\theta Z_p$, $|N| = n$ and f is irreducible over L^N.*
- *$p \mid [L : \mathbb{Q}]$ and there exists a cyclic extension k of $\mathbb{Q}$ of degree p, such that f is irreducible and normal over k.*

Proof. The first condition trivially implies the other one, by taking $k = L^N$. Conversely, since $\deg f \mid [L : \mathbb{Q}]$ and $(p,n) = 1$, we have $pn \mid [L : \mathbb{Q}]$. Let E be the splitting field of f over k; by the hypothesis, $[E : k] = n$ and therefore $[E : \mathbb{Q}] = pn$. Since $L \subset E$, we get $L = E$; hence, $k \subset L$ and $G = N \rtimes_\theta Z_p$, where $N = \mathrm{Gal}(L/k)$.

PROPOSITION II.1.2. *Let $p \mid n-1$ and let the equivalent conditions of Proposition II.1.1 hold. Put $K = L^N$. If there exists a rational prime q, unramified in L, such that $f \bmod q$ is of type $1 \cdot p^{(n-1)/p}$, then $G = \mathrm{Fr}(N,p)$; moreover, q is inert in K and $q\mathcal{O}_K$ splits completely in L.*

Proof.

Since $[K : \mathbb{Q}] = p$, for any rational prime q, unramified in L, there are just two possibilities: either q is inert in K or it splits completely in K. If the latter is the case, then $q\mathcal{O}_K = \mathcal{Q}_1 \cdots \mathcal{Q}_p$ and $\deg(\mathcal{Q}_i/q) = 1$; hence, reducing $f \bmod \mathcal{Q}_i$ is equivalent to reducing $f \bmod q$. In the case of the hypothesis, we would have that $f \bmod \mathcal{Q}_i$ is of type $1 \cdot p^{(n-1)/p}$ and therefore (see Lemma II.0.1 (a), which applies also to number fields– cf. [vdW, pp. 190–191]) $\mathrm{Gal}(L/K)$ would contain an element, not equal to the identity, which fixes a root of f; but this is impossible, since $N =$

$\mathrm{Gal}(L/K)$ is regular on the roots of f. This shows that q is necessarily inert in K.

So, $\deg(q\mathcal{O}_K/q) = p$ and therefore $\mathcal{O}_K/q\mathcal{O}_K \simeq \mathbb{F}_{q^p}$. Since the factorization of f over $\mathbb{F}_q$ is of type $1 \cdot p^{(n-1)/p}$, the factorization of f over $\mathbb{F}_{q^p}$, and hence over $\mathcal{O}_K/q\mathcal{O}_K$, is of type 1^n. Being f irreducible and normal over K, $L = K(\alpha)$ for any root α of f; then, $q\mathcal{O}_K$ splits completely in L, $q\mathcal{O}_L = \mathcal{Q}_1 \cdots \mathcal{Q}_n$.

Being $\deg(\mathcal{Q}_i/q) = p$ and q unramified in L, the decomposition group of $\mathcal{Q}_i$, $G_{\mathcal{Q}_i}$, is cyclic of order p, i.e. $G_{\mathcal{Q}_i} \simeq Z_p$. Putting $F = \mathbb{Q}(\alpha)$, where α is any fixed root of f, from the factorization of $f \bmod q$ we get $q\mathcal{O}_F = \mathcal{B}_1 \cdots \mathcal{B}_{(n-1)/p}\mathcal{B}$, with $\deg(\mathcal{B}_h/q) = p$ and $\deg(\mathcal{B}/q) = 1$, for $h = 1, \ldots, (n-1)/p$. Comparing the factorizations of $q\mathcal{O}_F$ and of $q\mathcal{O}_L$, we see that there are exactly p primes of L above $\mathcal{B}_h$, while there is exactly one prime above $\mathcal{B}$, say $\mathcal{Q}$. Therefore $F \supset L^{G_\mathcal{Q}}$ and $F \not\supset L^{G_{\mathcal{Q}'}}$, for $\mathcal{Q}' \mid \mathcal{B}_h$. This implies $F = L^{G_\mathcal{Q}}$ and $L^{G_\mathcal{Q}} \neq L^{G_{\mathcal{Q}'}}$, and so $G_\mathcal{Q} \neq G_{\mathcal{Q}'}$. Therefore, G contains n distinct cyclic subgroups of order p, the highest possible number, hence G has n Sylow p–subgroups and it is Frobenius by Proposition I.1.1.

By the same technique used in the proof of the previous proposition, we can show also the following fact, concerning the kind of primes q which give rise to factorizations of $f \bmod q$ of type $1 \cdot p^{(n-1)/p}$.

PROPOSITION II.1.3. *Let $G = \mathrm{Fr}(N, p)$, with $|N| = n$ and $p \mid n-1$. Then, for any rational prime q, unramified in L, $f \bmod q$ is of type $1 \cdot p^{(n-1)/p}$ if, and only if, q is inert in K and $q\mathcal{O}_K$ splits completely in L.*

Proof. Omitted.

We are now in a position to give the announced characterization, just putting together all the above results.

THEOREM II.1.4. *Let p be a rational prime dividing $n-1$. Then $G = \mathrm{Fr}(N, p)$ if, and only if, the following conditions hold:*

1. $p \mid [L : \mathbb{Q}]$.
2. *There exists an extension $k/\mathbb{Q}$, cyclic of degree p, such that f is irreducible and normal over k.*
3. *There exists a rational prime q, unramified in L, such that $f \bmod q$ is of type $1 \cdot p^{(n-1)/p}$.*

We will see in the next section how this characterization can be made effective.

III. Effectiveness of the characterization

III.0. Resultants and factorization of polynomials over number fields

Let $K = k(\beta)$ be a number field, where k is a subfield of K and β is a fixed root of a given a monic irreducible polynomial $g \in k[X]$, of degree m; let $\beta_1, \ldots, \beta_m$ denote the roots of g. Let $f \in K[X]$ be a monic square–free polynomial of degree n and $\alpha_1, \ldots, \alpha_n$ be the roots of f; we may write f as a polynomial in $k[X, \beta]$, $f = f(X, \beta)$. We want to consider the factorization type of f over K; suppose that such a factorization is $f_1 \cdots f_t$. For any polynomial $h(X, \beta) \in K[X]$ and any rational integer s, let $N(s, h, g)$ stand for the norm over k of the shifted polynomial $h(X - s\beta, \beta)$, that is for $N_{k(\beta)/k}(h(X - s\beta, \beta))$. Referring to the factorization algorithm of polynomials over number fields due to Trager [Trag] (see, also, [vdW], pp. 136–137), we can affirm the following:

i) there are only finitely many rational integers s such that $N(s, f, g)$ is not square–free;
ii) for any rational integer s such that $N(s, f, g)$ is square–free, the factorization over k of $N(s, f, g)$ is $N(s, f_1, g) \cdots N(s, f_t, g)$.

Thus, each irreducible factor of f over $k(\beta)$ of degree d maps to an irreducible factor of $N(s, f, g)$ over k of degree nd, and vice versa.

Moreover, we are able to calculate the norms above by means of the function resultant, which is available on any computer algebra system; in fact, the following equalities hold (the last one up to a sign):

$$N(s, f, g) = \prod_{i=1}^{m} f(X - s\beta_i, \beta_i) = \mathrm{Res}_Y(f(X - sY, Y), g(Y)) .$$

In particular, when $f \in k[X]$ is irreducible over k, we may study the factorization type of f over the field $k(\alpha)$, where α is a fixed root of f. In such a case, one of the factors of f is $X - \alpha$ and, since we are obviously interested in the other factors, we define the following polynomial

$$R(s, f) = \frac{N(s, f(X), f)}{N(s, X - \alpha, f)} = \prod_{i \neq j}^{1,n} (X - (\alpha_i + s\alpha_j)),$$

which is a monic polynomial in $k[X]$ of degree $n(n-1)$ and it is a linear resolvent of f when $s \neq 0, 1$. Then, we claim that f is normal over k, i.e. $\mathrm{spl}(f) = k(\alpha)$ for any root α of f, if, and only if, $R(s, f)$ over k is of

type n^{n-1}. In fact, f is normal over k if, and only if, f factors over $k(\alpha)$ as the product of n linear polynomials, which is equivalent to $N(s,f)$ being of type n^n over k, hence to $R(s,f)$ being of type n^{n-1} over k.

III.1. Factorizations of $R(s,f)$

For this subsection and for the next one, assume $f \in \mathbb{Z}[X]$ to be a monic irreducible polynomial of degree n, such that $\mathrm{Gal}(f) = \mathrm{Fr}(N,p)$, *with* $|N| = n$, *and put* $\mathrm{spl}(f) = L$ *and* $K = L^N$.

Fix a root α of f and let α' be any other root of f. How does f factor over $\mathbb{Q}(\alpha)$? Firstly, note that $[L : \mathbb{Q}(\alpha)] = p$ and therefore any irreducible factor of f over $\mathbb{Q}(\alpha)$ may be of degree either 1 or p. Then, since $\mathrm{Gal}(f) = \mathrm{Fr}(N,p)$, we know that there exists a rational prime q, unramified in L, such that $f \bmod q$ is of type $1 \cdot p^{(n-1)/p}$; by Proposition II.1.3, q is inert in K and $q\mathcal{O}_K$ splits completely in L. If $q\mathcal{O}_L = \mathcal{Q}_1 \cdots \mathcal{Q}_n$, then, proceeding as in the proof of Proposition II.1.2, we find that the n Sylow p–subgroups of $G = \mathrm{Gal}(f)$ are the decomposition groups of the primes of L over q, $G_{\mathcal{Q}_i}$, and that the respective decomposition fields are precisely the extensions of $\mathbb{Q}$ by the roots of f, i.e. $L^{G_{\mathcal{Q}_i}} = \mathbb{Q}(\alpha_i)$ $(i = 1, \ldots, n)$. This implies $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\alpha')$ and so $\alpha' \notin \mathbb{Q}(\alpha)$. Hence, the minimal polynomial of α' over $\mathbb{Q}(\alpha)$ has degree equal to p. Thus, we have proved the following fact.

PROPOSITION III.1.1. *Let f be as above and let α be a root of f. Then f over $\mathbb{Q}(\alpha)$ is of type $1 \cdot p^{(n-1)/p}$ and, for any rational integer s such that $R(s,f)$ is square-free, $R(s,f)$ over $\mathbb{Q}$ is of type $(np)^{(n-1)/p}$.*

Since f is irreducible and normal over K, from the last remark in the previous subsection, we have also the following result, involving the factorization of $R(s,f)$ over K.

PROPOSITION III.1.2. *Let f be as above. Then, for any rational integer s such that $R(s,f)$ is square-free, $R(s,f)$ over K is of type n^{n-1}.*

Since we are just interested in the factorization type of $R(s,f)$ over K and not in the actual irreducible factors, we can apply again the method described in the previous subsection, getting the following.

PROPOSITION III.1.3. *Let f as above and $g \in \mathbb{Z}[X]$ be a monic irreducible polynomial such that $K = \mathbb{Q}(\beta)$, where β is a root of g. Then, for any rational integer t such that $N(t,f,g)$ is square-free, $N(t,f,g)$ is irreducible over $\mathbb{Q}$. If s is a rational integer such that $R = R(s,f)$ is square-free, then,*

for any rational integer t such that $N(t, R, g)$ is square-free, $N(t, R, g)$ over $\mathbb{Q}$ is of type $(np)^{n-1}$.

III.2. Determination of K

Recall that K is cyclic of prime degree p over $\mathbb{Q}$. Thus, being abelian over the rationals, by Kronecker–Weber theorem, K is included in a cyclotomic field C_l (where $C_l = \mathbb{Q}(\zeta)$, with ζ a primitive l–th root of unity), for some positive integer l, such that $q \nmid D_K$ implies $q \nmid D_{C_l}$, for any rational prime q. Assuming l to be minimal with respect to this property, its factorization is to be of the kind $p^{2a}q_1 \cdots q_s$, where $a \in \{0, 1\}$ and $q_j \equiv 1 \bmod p$, for $j = 1, \ldots, s$. Moreover, since $D_K \mid D_{C_l}$, we have

$$q \mid D_K \iff q \mid D_{C_l} \iff q \mid l\,, \quad \text{for all primes } q\,.$$

Now observe that f is irreducible and normal over K; hence, $L = K(\alpha)$, for any root α of f. From this, it follows that $D_K \mid D_L \mid D_f$ and therefore, if $q \mid l$, then $q \mid D_f$. Seeing the factorization of l, we deduce that $l \mid pD_f$. Thus, if the factorization of D_f is

$$D_f = \pm p^{e_0} p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_t^{f_t}\,,$$

with $e_0 \geq 0$, $e_i \geq 1$, $f_j \geq 1$, $p_i \not\equiv 1 \bmod p$ and $q_j \equiv 1 \bmod p$, for $i = 1, \ldots, r$ and $j = 1, \ldots, t$, putting

$$m = p^{2e} q_1 \cdots q_t\,, \quad \text{where } e = \begin{cases} 0, & \text{if } e_0 = 0 \\ 1, & \text{if } e_0 \geq 1\,, \end{cases}$$

we have $l \mid m$.

Therefore, $K \subset C_l \subset C_m$ and K can be determined as one of the cyclic subfields of degree p over $\mathbb{Q}$ of C_m. These are finitely many, since they correspond to the subgroups of index p of $\mathrm{Gal}\,(C_m/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$; indeed, their number is precisely $(p^{t+e} - 1)/(p - 1)$.

III.3. Effective version of the characterization theorem

We are now able to give an effective version of Theorem II.1.4. For simplicity, we assume GRH; so, we can use the strongest bound given in Lemma II.0.1. This is not so restrictive, as it is shown by all tested examples, where the least prime q is much smaller than the one given theoretically, even under such assumption.

THEOREM III.3.1. *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and put $G = \mathrm{Gal}(f)$ and $L = \mathrm{spl}(f)$. Let p be a rational prime such that $p \mid n-1$. Assume GRH. If $G = \mathrm{Fr}(N,p)$, with $|N| = n$, then, putting $K = L^N$ and $R = R(s,f)$, for some rational integer s such that $R(s,f)$ is square-free, we have:*

- **i.** *R is of type $(np)^{(n-1)/p}$.*
- **ii.** *K is one of the cyclic subfields of degree p over $\mathbb{Q}$ of C_m, where m is given in Section III.2; moreover, f is irreducible over K and R over K is of type n^{n-1}.*
- **iii.** *There exists a rational prime q, not dividing D_f, such that $q \leq 70(\log D_f)^2$ and $f \bmod q$ is of type $1 \cdot p^{(n-1)/p}$.*

That such conditions are sufficient for $G = \mathrm{Fr}(N,p)$ was already proved in Theorem II.1.4; the point is that now we have an effective way to verify the conditions given in that theorem.

III.4. Examples

Although the given characterization determines if the Galois group of a polynomial of degree n is Frobenius with kernel of order n and complement of prime order p dividing $n-1$, a general method for constructing such polynomials is not known, apart from few cases. Moreover, in some cases a theoretical method may be outlined, but the computations involved exceed the capacity of the computer machines available to the author, so that we are not able to exhibit many polynomials of the required degree and with the required Frobenius Galois group. Therefore, to give some examples of how our method applies, we must refer to polynomials found in the literature, and somehow manipulate them.

Example 1. The simplest example of a polynomial considered by our method is a polynomial of degree 4 whose Galois group is the alternating group of degree 4, $A_4 \simeq \mathrm{Fr}(Z_2 \times Z_2, 3)$. Such polynomials are easy to construct. Take, for example, the following one:

$$f_1(X) = X^4 - 8X^3 + 32X^2 + 40X + 12.$$

We will prove that its Galois group is A_4, verifying the conditions given in Theorem III.3.1 and using also Proposition III.1.3.

- The smallest prime q for which $f_1 \bmod q$ factors as $1 \cdot 3^2$ is 3.
- The resolvent $R = R(-1, f_1)$ is square-free and it is irreducible over $\mathbb{Q}$.
- The discriminant of the polynomial is $2^{12}7^2 13^2$, so the possible cubic field should be included in $C_{7\cdot 13}$. We first try with the cubic field

included in C_7; a primitive element for such cubic field, which we call K, is a root of the polynomial

$$g(X) = X^3 + X^2 - 2X - 1.$$

We compute $N(1, f_1, g)$ which turns out to be square–free and it is irreducible. Then, we compute $N(1, R, g)$ and we verify that it is square–free and of type 12^3.

Hence, we claim that the Galois group of f_1 is A_4 and that the unique cubic field included in its splitting field is the unique cubic field included in C_7, that is K.

Example 2. Bruen, Jensen and Yui [BJY] constructed a family of rational integral polynomials of degree 7 whose Galois groups over $\mathbb{Q}$ are Frobenius groups of order 21, that is groups as $\mathrm{Fr}\,(Z_7, 3)$. From this family, we have taken the following polynomial

$$f_2(X) = X^7 + 14X^6 - 56X^4 + 56X^2 - 16.$$

We apply our characterization theorem to this polynomial.

- We factor $f_2 \bmod q$ for some rational primes q, in order to find a factorization of type $1 \cdot 3^2$ – should we find a factorization type not equal to 1^7, $1 \cdot 3^2$ or 7, we would be sure that $\mathrm{Gal}\,(f_2) \neq \mathrm{Fr}\,(Z_7, 3)$ (see Proposition I.2.1). The prime 3 gives the required factorization.
- We compute the resolvent $R = R(-1, f_2)$, which turns out to be square–free and factors over $\mathbb{Q}$ into 2 irreducible polynomials of degree 21, R_1 and R_2, as we expected.
- The discriminant of f_2 is equal to $2^{24}7^{10}$. Therefore, the unique possible cubic field to consider is K, the cubic field included in C_7. The norm $N(1, f_2, g)$ is square–free and it is irreducible. The norm $N(1, R, g) = N(1, R_1, g)N(1, R_2, g)$ is square–free as well and it is of type 21^6.

Hence, we have verified that the Galois group of f_2 is $\mathrm{Fr}\,(Z_7, 3)$ and we have shown that the cubic field included in its splitting field is K.

Example 3. To find other explicit polynomials, we refer to a proposition by Williamson. If g_1 and g_2 are two monic polynomials in $k[X]$, where k is any number field, let $S(g_1, g_2)$ denote the polynomial whose roots are all the sums of one root of g_1 and one root of g_2; we can easily compute such polynomial by the following formula:

$$S(g_1, g_2)(X) = \mathrm{Res}_Y(g_1(X - Y), g_2(Y)).$$

PROPOSITION III.4.1. *Let g_1 and g_2 be irreducible monic polynomials over a number field k and let E_1 and E_2 be their respective splitting fields over k. If E_1 and E_2 are linearly disjoint over k, then the polynomial $S(g_1, g_2)$ is irreducible over k and its splitting field over k is E_1E_2.*

Proof. See [Will].

We will apply such a result to the polynomials f_1 and f_2, which are irreducible over K. We compute the polynomial $f_3(X) = S(f_1, f_2)(X)$, which is equal to

$$\begin{aligned}
&X^{28} - 280\,X^{26} + 2744\,X^{25} + 25172\,X^{24} - 542752\,X^{23} + 1697024\,X^{22} \\
&+35889152\,X^{21} - 371206640\,X^{20} + 139755392\,X^{19} + 23091117056\,X^{18} \\
&-197585349248\,X^{17} + 697109017920\,X^{16} + 251070245888\,X^{15} \\
&-11245057303040\,X^{14} + 34649341024256\,X^{13} + 30099489030912\,X^{12} \\
&-325478762205184\,X^{11} + 344784352174080\,X^{10} + 1874783504771072\,X^{9} \\
&-898340070691840\,X^{8} - 3735430379200512\,X^{7} + 1366338890506240\,X^{6} \\
&+3119932996354048\,X^{5} - 1502823809994752\,X^{4} - 779881157328896\,X^{3} \\
&+727313536352256\,X^{2} - 192447697354752\,X + 19831601348608.
\end{aligned}$$

Since the splitting fields over K of f_1 and f_2 have relatively prime degrees over K, they are linearly disjoint over K, so that f_3 is irreducible over K and the Galois group of its splitting field over K is $Z_2 \times Z_2 \times Z_7$: being the degree of f_3 equal to 28, we deduce that f_3 is also normal over K. It is also obvious that the degree of the splitting field of f over $\mathbb{Q}$ is a multiple of 3, since such field includes K. So, conditions **1** and **2** of Theorem II.1.4 are satisfied and the only left verification is about the factorization type of f_3 mod q: the smallest prime q which yields the type $1 \cdot 3^9$ is 11.

Hence, $\mathrm{Gal}\,(f_3) = \mathrm{Fr}\,(Z_2 \times Z_2 \times Z_7, 3)$ and the cubic field included in $\mathrm{spl}\,(f_3)$ is K.

Example 4. We proceed as in the previous case. From the mentioned family of polynomials by Bruen, Jensen and Yui, we take another polynomial,

$$f_4(X) = X^7 - 602\,X^5 + 103544\,X^3 - 4452392\,X - 636056,$$

whose splitting field again includes K as above. We construct the polynomial $f_5(X) = S(f_2, f_4)(X)$ and we verify that it is irreducible over $\mathbb{Q}$. This

implies that the splitting field of f_2 and f_4 are different, hence that they are disjoint over K and that the Galois group of f_5 over K is $Z_7 \times Z_7$. As in the previous example, conditions **1** and **2** of Theorem II.1.4 are plainly satisfied. Then, we find that 11 is the smallest prime q such that the factorization type of $f_5 \bmod q$ is $1 \cdot 3^{16}$.

Therefore, $\mathrm{Gal}(f_5) = \mathrm{Fr}(Z_7 \times Z_7, 3)$ and the cubic field included in $\mathrm{spl}(f_5)$ is K. We do not report f_5, because its greatest coefficients are 48–digit numbers.

REFERENCES

[BJY] A. A. Bruen, C. U. Jensen, N. Yui, *Polynomials with Frobenius groups of prime deegre as Galois groups* II, J. Number Theory **24** (1986), 305–359.

[Frob] G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitution seiner Gruppe*, S. B. Akad. Wiss. Berlin (1896), 689–705.

[Jac] N. Jacobson, *Basic algebra I*, 2nd ed., Freeman, New York, 1985.

[Lang] S. Lang, *Algebraic number theory*, GTM 110, Springer–Verlag, New York, 1986.

[LMO] J. C. Lagarias, H. L. Montgomery, A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.

[Oes] J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisé*, Astérisque **61** (1979), 165–167.

[Rob] D. J. S. Robinson, *A course in the theory of groups*, GTM 80, Springer–Verlag, New York, 1982.

[Trag] B. M. Trager, *Algebraic factoring and rational function integration*, ACM Symposium on Symbolic and Algebraic Computation 1976 (Jenks, ed.), ACM Inc., New York, 1976, pp. 219–226.

[vdW] B. L. van der Waerden, *Modern algebra*, 2nd ed., vol. I, Ungar, New York, 1953.

[Will] C. J. Williamson, *Odd degree polynomials with dihedral Galois groups*, J. Number Theory **34** (1990), 153–173.

L. Cangelmi
Dipartimento di Metodi e Modelli Matematici per le Scienze Applicate
Universita di Roma "La Sapienza"
Via A. Scarpa 10
00161 Roma, Italy

e-mail : leonardo@mat.uniroma1.it