A complete parametrization of cyclic field extensions of 2-power degree

Dominique Martinais (*) and Leila Schneps (**)

Abstract

Let q be a power of 2 at least equal to 8 and ζ be a primitive q-th root of unity, and let K be any field of characteristic zero. We define the group of special projective conorms S_K as a quotient of the group of elements of $K(\zeta)$ of norm 1: S_K is obviously trivial if the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is cyclic. We prove that for some fields K, the group S_K is finite, and it is even trivial for certain fields such as $\mathbb{Q}$ or $\mathbb{Q}(X_1,\ldots,X_m)$. We then prove that the group S_K completely parametrizes the cyclic extensions of K of degree q. We exhibit an explicit polynomial defined over $\mathbb{Q}(T_0,\ldots,T_{q/2})$ which parametrizes all cyclic extensions of K of degree q associated to the trivial element of S_K. In particular, this polynomial parametrizes all cyclic extensions of K of degree q whenever the group S_K is trivial.

§1. Introduction

Let q be a power of a prime p and let G be the cyclic group of order q. We consider the problem of proving that it is possible to parametrize all G-Galois extensions of a given field K. It has been known for some time (see [Sa1]) that versal (or generic) polynomials exist for G over every field of characteristic different from p such that the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is cyclic. Such polynomials have been explicitly constructed by G. Smith ([Sm]) for odd p. Therefore, we do not consider the case where the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is cyclic. That is why, for the remainder of the paper, we assume that q is a power of 2 at least equal to 8, and we seek a parametrization of G-Galois extensions in characteristic zero. In this case, it is known (see [Sa1]) that there is no versal polynomial for G over $\mathbb{Q}$: there exists a cyclic Galois extension of $\mathbb{Q}_2$ of degree 8 which cannot be obtained as the splitting field of a polynomial obtained by specialization to values in $\mathbb{Q}_2$ of any cyclic polynomial of degree 8 defined over $\mathbb{Q}(X_1,\ldots,X_m)$ (cf. [L], [Sa1]).

The object of this paper is to explicitly determine a family of polynomials parametrizing all G-Galois extensions of a given field K of characteristic zero. In particular, we prove that for certain fields K such as number fields or fields $k(T)$ where k is a number field, the family consists of a finite number of polynomials, and for certain fields K such as $\mathbb{Q}$ or $\mathbb{Q}(X_1, \ldots, X_m)$, there exists a single polynomial $P \in \mathbb{Q}[T_0, \ldots, T_{q/2}, X]$ which parametrizes all G-Galois extensions of K. We are able to give P explicitly via the following adaptation of Smith's method in the odd case (see [Sm]).

From now on:
— let ζ be a fixed primitive q-th root of unity;
— for all $u \in \mathbb{Z}$, let $\bar{u}$ denote its class modulo q;
— for all $v \in \mathbb{Z}/q\mathbb{Z}$, let $<v>$ denote the integer in $\{0, 1, \ldots, q-1\}$ such that $\overline{<v>} = v$.

The polynomial P is constructed as follows.

Let $T_0, \ldots, T_{q/2}$ be $q/2 + 1$ indeterminates over $\mathbb{Q}$. In an algebraic closure F of $\mathbb{Q}(T_0, \ldots, T_{q/2})$, define B_i for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$ by

$$B_i = \sum_{j=0}^{q/2-1} T_j \, \zeta^{ij}.$$

Let us choose $A \in F$ such that

$$A^2 = T_{q/2},$$

and $C_i \in F$ for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$ such that

$$C_i^q = B_i.$$

Define $E_j \in F$ for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$ by

$$E_j = A \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^*} C_i^{<ji^{-1}>}.$$

Finally, define $R_i \in F$ for all $i \in \mathbb{Z}/q\mathbb{Z}$ by

$$R_i = \sum_{j \in (\mathbb{Z}/q\mathbb{Z})^*} E_i \, \zeta^{ij}.$$

Definition: Let $P \in F[X]$ be the polynomial

$$P = \prod_{i \in \mathbb{Z}/q\mathbb{Z}} (X - R_i).$$

Of course, it will be shown (in §4) that this polynomial is independent of all choices made. We will prove (in §4) that this polynomial is actually defined over $\mathbb{Q}(T_0,\ldots,T_{q/2})$, and in fact that its coefficients are polynomials in $T_0,\ldots,T_{q/2}$.

In §2, we recall Saltman's description of G-Galois extensions of K in terms of elements of $K(\zeta)$ of norm 1. In §3, we introduce the group of special projective conorms S_K associated to any field K and study the fields for which S_K is finite or trivial. Finally, in §4, we show that S_K indexes a family of polynomials parametrizing all G-Galois extensions of K and that a polynomial associated to the trivial element of S_K is the polynomial P given above. Note that a consequence of these results is that the number of polynomials needed to parametrize all G-Galois extensions of K depends only on K and not on q.

To conclude this introduction, we would like to thank D. Saltman for giving us helpful insights into his own work, and J-P. Serre for communicating to us his letter to Platonov. We also thank R. Dentzer, who applied the above algorithm using MAPLE to compute an irreducible polynomial of degree 16 having cyclic Galois group of order 16 over $\mathbb{Q}(T)$. He choose to calculate

$$Q = P(T,1,0,0,0,0,0,\frac{1}{8},X).$$

The result is

$$\begin{aligned}
Q = {} & X^{16} - 8(T^8+1)\,X^{14} + 4(16T^6 - 14T^4 + 6T^2 + 5)(T^8+1)\,X^{12} \\
& - 8(24T^{12} - 28T^{10} + 6T^8 + 36T^6 - 31T^4 + 13T^2 + 2)(T^8+1)\,X^{10} \\
& - 2(128T^{18} - 120T^{16} - 144T^{14} + 560T^{12} - 488T^{10} \\
& \qquad + 144T^8 + 164T^6 - 136T^4 + 56T^2 + 1)(T^8+1)\,X^8 \\
& - 8(16T^{22} + 16T^{20} - 120T^{18} + 208T^{16} - 108T^{14} \\
& \quad - 64T^{12} + 164T^{10} - 128T^8 + 73T^6 - 20T^4 + 3T^2 + 2)T^2(T^8+1)\,X^6 \\
& + 4(64T^{24} - 192T^{22} + 208T^{20} + 80T^{18} - 432T^{16} \\
& \quad + 520T^{14} - 316T^{12} + 112T^{10} + 18T^8 - 66T^6 + 67T^4 - 26T^2 + 5)T^4(T^8+1)\,X^4 \\
& - 8(T^8+1)(32T^{22} - 112T^{20} + 160T^{18} - 72T^{16} \\
& \quad - 84T^{14} + 144T^{12} - 86T^{10} + 28T^8 - 17T^6 + 17T^4 - 7T^2 + 1)T^6\,X^2 \\
& + (T^8+1)(8T^{10} - 16T^8 + 12T^6 - 4T^2 + 1)^2 T^8
\end{aligned}$$

§2. Background on cyclic extensions

Let K be a field of characteristic zero. In this section, we essentially recall Saltman's description of the cyclic extensions of degree q of K (cf. [Sa1] and [Sa2]). This description uses Kummer theory. Before considering cyclic extensions of K, we need a little machinery on the group $\mathrm{Gal}\big(K(\zeta)/K\big)$. Since the group $\mathrm{Gal}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^*$, we can easily state (see [Sa1] and [Sa2] for the proof)

Lemma 2.1: *(i)* [Sa1] *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is cyclic and of order* s, $s > 1$. *Let* τ *be a generator of this group. Then either* $\zeta^\tau = \zeta^{-1}$, *or* $\zeta^\tau = \zeta^m$ *with* $<\overline{m}>= m$ *and* $(m^s - 1)/q$ *odd.*

(ii) [Sa2] *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is not cyclic and of order* $2s$. *Then it has two generators* σ *and* τ *such that* $\zeta^\sigma = \zeta^{-1}$ *and* $\zeta^\tau = \zeta^m$, *with* $<\overline{m}>= m$ *and* $(m^s - 1)/q$ *odd.*

From now on, let L be a cyclic extension of K of degree q. Let η be a generator of $\mathrm{Gal}(L/K)$. As we do not want the two Galois groups $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}\big(K(\zeta)/K\big)$ to intersect non-trivially, we do not consider the field $L(\zeta)$ but the ring $L \otimes_K K(\zeta)$, which we denote by $L \otimes K(\zeta)$. This ring is a direct sum of fields and is a field itself if and only if $L \cap K(\zeta) = K$.

The group of the Galois extension $L \otimes K(\zeta)$ of K as commutative ring (cf. [DM-I]) is the direct product of the group $\mathrm{Gal}(L/K)$ and the group $\mathrm{Gal}\big(K(\zeta)/K\big)$. So it is an abelian group. Let us extend, in the obvious way, η, σ (when it is defined) and τ to $L \otimes K(\zeta)$. We identify L with $L \otimes 1$ and $K(\zeta)$ with $1 \otimes K(\zeta)$ in $L \otimes K(\zeta)$.

Definition: Let $\alpha \in L \otimes K(\zeta)$. We say that α is a generator of $L \otimes K(\zeta)$ if we have $L \otimes K(\zeta) = K(\zeta)(\alpha)$ and $\eta(\alpha) = \zeta\alpha$.

Remark: Such an α always exists, by Kummer theory. If we have one such α, then the complete set of them is given by

$$\{\lambda\alpha \mid \lambda \in K(\zeta)^*\}.$$

Proposition 2.2: [Sa1] *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is cyclic of order* 2, *with a generator* τ *such that* $\zeta^\tau = \zeta^{-1}$. *Then there exist* $y \in K^*$ *and* $b \in K(\zeta)^*$ *such that*

$$\alpha^\tau = y\,\alpha^{-1} \quad \textit{and} \quad \alpha^q = y^{q/2}\,\frac{b^\tau}{b}.$$

Proof: As the group $\mathrm{Gal}\big(L\otimes K(\zeta)/K\big)$ is abelian, τ and η commute. In particular, we have $\alpha^{\eta\tau} = \alpha^{\tau\alpha}$, that is $(\alpha^{\tau})^{\eta} = \zeta^{-1}\alpha^{\tau}$. So there exists $y \in K(\zeta)$ such that $\alpha^{\tau} = y\alpha^{-1}$. Since $\tau^2 = \mathrm{id}_{L\otimes K(\zeta)}$, it is clear that $y^{\tau} = y$. This means $y \in K^*$. Furthermore, $\alpha^q y^{-q/2}(\alpha^q y^{-q/2})^{\tau} = 1$ so b exists by Hilbert's theorem 90.

Proposition 2.3: [Sa1] *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is cyclic of order* s, $s > 1$, *with a generator* τ *such that* $\zeta^{\tau} = \zeta^m$ *with* $<\overline{m}>= m$ *and* $(m^s - 1)/q$ *odd. Then there exists* $b \in K(\zeta)^*$ *such that*

$$\alpha^{\tau} = b^{-1}\alpha^m \quad \textit{and} \quad \alpha^{m^s-1} = \prod_{i=1}^{s}\left(b^{m^{i-1}}\right)^{\tau^{s-1}}.$$

Proof: There exists $b \in K(\zeta)^*$ such that $\alpha^{\tau} = b^{-1}\alpha^m$ exactly as in proposition 1: η and τ commute. By induction, we prove that

$$\alpha^{\tau^s} = \alpha^{m^s}\prod_{i=1}^{s}\left((b^{-1})^{m^{i-1}}\right)^{\tau^{s-i}}.$$

Since s is the order of τ, the proof is complete.

Proposition 2.4: [Sa2] *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is not cyclic. Let* σ, τ, m *and* s *be as in part (ii) of lemma* 2.1. *Then there exists* $b \in K(\zeta)^*$ *and* $z \in K(\zeta)^*$ *such that*

$$\begin{cases} z^{\sigma} = z \\ z^{\tau}/z^m = b\,b^{\sigma} \\ \alpha^{\sigma} = z^{-1}\alpha^{-1} \\ \alpha^{\tau} = b^{-1}\alpha^m \\ \alpha^{m^s-1} = \prod_{i=1}^{s}\big(b^{m^{i-1}}\big)^{\tau^{s-i}}. \end{cases}$$

Proof: We proceed exactly as in proposition 2.2: there exist $b \in K(\zeta)^*$ and $z \in K(\zeta)^*$ such that $\alpha\,\alpha^{\sigma} = z^{-1}$ and $\alpha^{\tau} = b^{-1}\alpha^m$ because σ and η commute and so do τ and η. Since $\sigma^2 = \mathrm{id}_{L\otimes K(\zeta)}$, we have $z^{\sigma} = z$. Since σ and τ commute, we have $z^{\tau}/z^m = b\,b^{\sigma}$. Finally, the last equality holds exactly as in proposition 2.2.

§3. The group of special projective conorms

Let K be a field of characteristic zero. In this section, we let K' denote the field $K(\zeta)$ and K^+ the field $K(\zeta+\zeta^{-1})$. Then if $\mathrm{Gal}(K'/K)$ is not cyclic, it is generated by elements τ and σ where τ acts on ζ via $\zeta^\tau = \zeta^m$ and σ by $\zeta^\sigma = \zeta^{-1}$, as in §2. If $\mathrm{Gal}(K'/K)$ is cyclic it is generated by an element τ such that $\zeta^\tau = \zeta^m$. In this case let σ denote the identity element of $\mathrm{Gal}(K'/K)$.

Definition: The *group of special projective conorms* S_K is the quotient of the group

$$\{c \in K' \mid N_{K'/K}(c) = 1\}$$

by the subgroup consisting of the following elements of norm 1 in K':

$$\{\frac{x^\tau}{x}\frac{w^\sigma}{w} \mid x, w \in K'\}.$$

The group S_K arises naturally in relation to the cyclic Galois extensions of K of degree q. In §4 we will use it to index a family of polynomials parametrizing all such extensions of K. Before doing so, we devote a paragraph to the study of the group S_K, relating it to the Brauer group of K via Saltman's work and studying for which fields S_K is finite or even trivial. It is an immediate consequence of Hilbert's theorem 90 that S_K is trivial whenever $\mathrm{Gal}(K'/K)$ is cyclic. Therefore, for the remainder of this section, we assume that $\mathrm{Gal}(K'/K)$ is not cyclic.

We note that the terminology "special projective conorms" was introduced by Platonov [Pl] in the context of the study of the Tannaka-Artin problem. Platonov defines the group as a subgroup $P(L,R,K) \subset R^*/K^*N_{L/R}(L^*)$, where $K \subset R \subset L$ are field extensions and R/K is cyclic with Galois group generated by τ (in our case, $L = K'$ and $R = K^+$). His definition is as follows: an element $a^* \in R^*/K^*N_{L/R}(L^*)$ is in $P(L,R,K)$ if for any representative $a \in R$ of the class a^*, we have $a^\tau/a \in N_{L/R}(L^*)$. In the following lemma, we show that his definition coincides with ours, that is, that the group $P(K',K^+,K)$ is isomorphic to S_K.

Lemma 3.1: *Let $\phi : S_K \to P(K',K^+,K)$ be defined as follows: $\phi([c]) = [z]$ where for any $c \in K'$ which is a representative of $[c] \in S_K$ and any $z \in K^+$ which is a representative of $[z] \in P(K',K^+,K)$, we have $c\,c^\sigma = z^\tau/z$. Then ϕ is a group isomorphism.*

Proof: We first show that ϕ is well-defined. In fact, ϕ can be deduced from a map $\tilde{\phi} : K'_1 \to (K^+)^*/K^*$ where K'_1 is the set of elements $c \in K'$ with $N_{K'/K}(c) = 1$. For $c \in K'_1$ set $\tilde{c} = c\,c^\sigma$. Then since $N_{K^+/K}(\tilde{c}) = 1$, there exists $z \in K^+$ defined up to K^* such that $\tilde{c} = z^\tau/z$. Let $\tilde{z}$ be the image of z in $(K^+)^*/K^*N(K'^*)$: then we can define $\tilde{\phi}(\tilde{c}) = \tilde{z}$. The kernel of $\tilde{\phi}$ is exactly the set of elements $c \in K_1'$ such that $\tilde{c} = (x\,x^\sigma)^\tau/(x\,x^\tau)$ for some $x \in K'$. But if this is the case, then there exists $w \in K'$ such that $c = (w^\sigma/w)\,(x^\tau/x)$. So $\tilde{\phi}$ induces an injection $\bar{\phi} : S_K \to (K^+)^*/K^*N(K'^*)$. We claim that the image is the group $P(K', K^+, K)$. For suppose some $a^* \in (K^+)^*/K^*N(K'^*)$ is in the image of $\bar{\phi}$. Then there exists $c \in K_1$ and $a \in K^+$ such that a is a representative of the class a^* and $\tilde{c} = a^\tau/a$. So $a^\tau/a \in N_{K'/K^+}\big((K^+)^*\big)$, which means $a^* \in P(K', K^+, K)$.

In response to a letter of Platonov, Serre [Se] proved that S_K is finite when K is a number field. His proof is reproduced in the proof of part (i) of theorem 2.

Before considering number fields and other special cases, we give the theorem relating the group of special projective conorms to the Brauer group of K.

Theorem 3.2: *The group S_K is isomorphic to*

$$\mathrm{Coker}\{\mathrm{Br}\big(K^+/K\big) \oplus \mathrm{Br}\big(K(i)/K\big) \to \mathrm{Br}(K'/K)\}.$$

Proof: Let us associate a $\tilde{z} \in (K^+)^*/N_{K'/K^+}(K'^*)$ to each element A of $\mathrm{Br}(K'/K)$ as follows: let $(K'/K^+, z)$ be the quaternion algebra of elements of A which commute with K^+. Clearly $z \in (K^+)^*$ is defined up to $N_{K'/K^*}(K'^*)$, so we let $\tilde{z}$ be its equivalence class. Let H^* be the subgroup of $(K^+)^*/N_{K'/K}(K'^*)$ consisting of elements which can be obtained in this way. An element $\tilde{z} \in (K^+)^*/N_{K'/K^+}(K'^*)$ is actually in H^* if and only if for every representative $z \in (K^+)^*$ of $\tilde{z}$, the element $z^\tau/z \in N_{K'/K^+}(K')^*$.

By lemma 3.1, the group S_K is isomorphic to the quotient of H^* by K^*. From the map $\mathrm{Br}(K'/K) \to H^*$ just described, we thus obtain a map $\mathrm{Br}(K'/K) \to S_K$, whose kernel is given by the set of elements $A \in \mathrm{Br}(K'/K)$ whose associated quaternion algebra $(K'/K^+, z)$ can be written with some $z \in K^*$. This is clearly the case for any decomposed algebra $A \in \mathrm{Br}(K'/K)$, i.e. any algebra which can be written $A = \big(K^+/K, y\big) \otimes \big(K(i)/K, z\big)$, for $y, z \in K^*$, since the elements commuting with K^+ are given by $(K(i)/K, z) \otimes K^+ = (K'/K^+, z)$. But any algebra A having associated algebra $(K'/K^+, z)$ for $z \in K^*$ must be decomposed, which concludes the proof of the theorem.

We now turn to considering fields K whose associated group S_K is finite or trivial (the list is certainly not complete!).

Theorem 3.3: *Let K be a field such that* $\mathrm{Gal}(K'/K)$ *is not cyclic. Then the group S_K is finite in the following cases* *(i) K is a number field. In this case, S_K is an elementary abelian 2-group.*

(ii) $K = k(T)$ where S_k is finite. In this case, $S_K \simeq S_k$.

Proof: (i) Let $G = \mathrm{Gal}(K'/K) = C_1 \times C_2$ where $C_1 = \mathrm{Gal}(K^+/K)$ and $C_2 = \mathrm{Gal}(K'/K^+)$, and write τ and σ for generators of C_1 and C_2 as usual. Let H be the subgroup of $(K)^*$ generated by the elements x/x^σ and x/x^τ for all $x \in (K')^*$. Then the quotient of the group of elements of norm 1 of K' by the subgroup H is the group S_K. We claim that in fact it is the Tate cohomology group $\hat{H}^{-1}\big(G, (K')^*\big)$. For the group $\hat{H}^{-1}\big(G, (K')^*\big)$ is just the elements of norm 1 modulo the group generated by the set $\{x/x^\rho \mid \rho \in \mathrm{Gal}(K'/K)\}$, which is clearly the same subgroup as H. The following classical lemma (cf. [CF] for example) shows that S_K is finite:

Lemma 3.4: *The Tate cohomology groups $\hat{H}^i\big(G, (K')^*\big)$ are all finite for odd i.*

In order to show that S_K is an elementary abelian 2-group, we show that every element is of order at most 2. Indeed, let c be an element of K' of norm 1, and let $x \in K'$ be such that $cc^\sigma = x^\tau/x$. Then $c^2 = (c/c^\sigma)(x^\tau/x)$, so the image of c^2 in S_K is trivial.

(ii) For this part, we need to use the following two basic facts about the Galois cohomology of function fields (cf. [Ar]). Let k be an infinite field of characteristic different from 2 and let $K = k(T)$.

(1) Let V denote the set of discrete valuations of K which are trivial on k. For each $v \in V$ let us write $k(v)$ for the residue field of K_v, the completion of K at v. Then we have the following exact sequence:

$$0 \to \mathrm{Br}_2(k) \to \mathrm{Br}_2(K) \to \prod_{v \in V} H^1\big(k(v), \mathbb{Z}/2\mathbb{Z}\big).$$

The last arrow is given by $\prod_v \mathrm{Res}_v$ where for each $v \in V$,

$$\mathrm{Br}_2(K) \to \mathrm{Br}_2(K_v) \overset{\mathrm{Res}_v}{\to} H^1\big(k(v), \mathbb{Z}/2\mathbb{Z}\big) \simeq k(v)^*/k(v)^{*2}.$$

(2) Let $\alpha = \sum_i \big(a_i(T), b_i(T)\big)$ be an element of $\mathrm{Br}_2(K)$, and suppose its image under $\prod_v \mathrm{Res}_v$ is trivial. Then by the above exact sequence α is an element of $\mathrm{Br}_2(k)$. For any value $t \in k$ which is not a zero or a pole of any of the $a_i(T)$ or the $b_i(T)$, we have $\alpha = \sum_i \big(a_i(t), b_i(t)\big)$.

We now proceed to the proof of part (ii) of the theorem. Suppose k is a field such that $\mathrm{Gal}(k'/k)$ is not cyclic and S_k is finite. Choose a set of representatives $\{\gamma\}$ for the elements of S_k in k'. We claim that the same set $\{\gamma\}$ forms a set of representatives in K'

for S_K. Let $K = k(T)$, $K' = K(\zeta)$ and $K^+ = K(\zeta + \zeta^{-1})$. Let $c(T) \in K'$ be an element of norm 1, and set $\tilde{c}(T) = c(T)c(T)^\sigma \in K^+$. Then by Hilbert's theorem 90, there exists $\tilde{x}(T) \in K^+$ such that $\tilde{c}(T) = \tilde{x}(T)^\tau / \tilde{x}(T)$. Since $(\tilde{c}(T), -1) = 0$ in $\mathrm{Br}_2(K^+)$, we have $(\tilde{x}(T), -1) = (\tilde{x}(T)^\tau, -1) = \cdots = (\tilde{x}(T)^{\tau^{s-1}}, -1)$ where s is the order of τ. We will show that there exists a choice of $\tilde{x}(T)$ (which is defined up to K^*) with a special property.

Lemma 3.5: *There exists an element $\tilde{x}(T) \in K^+$, defined up to multiplication by an element of k^*, such that $\tilde{c}(T) = \tilde{x}(T)^\tau / \tilde{x}(T)$ and $(\tilde{x}(T), -1)$ is a constant symbol, i.e. $(\tilde{x}(T), -1) \in \mathrm{Br}_2(k^+)$.*

Proof: Let $\tilde{x}_0(T)$ be any element of K^+ satisfying $\tilde{c}(T) = \tilde{x}_0(T)^\tau / \tilde{x}_0(T)$. Let $\tilde{x}(T)$ be the unique polynomial in K^+ obtained by multiplying $\tilde{x}_0(T)$ by an element of K, such that $\tilde{x}(T)$ is not divisible by any polynomial factor defined over k. As remarked above, we we have the set of equalities

$$(\tilde{x}(T), -1) = \big(\tilde{x}(T)^\tau, -1\big) = \cdots = \big(\tilde{x}(T)^{\tau^{s-1}}, -1\big)$$

in the Brauer group $\mathrm{Br}_2(K^+)$. If the symbol $(\tilde{x}(T), -1)$ has any poles they must lie at a common root of the polynomials $\tilde{x}(T), \tilde{x}(T)^\tau, \ldots, \tilde{x}(T)^{\tau^{s-1}}$. But if α is such a common root, then the minimal polynomial of α over K must divide $\tilde{x}(T)$. For let $P_0(T) \in K'$ be the minimal polynomial of α over K'. Then $P_0(T)$ divides $\tilde{x}(T)^{\tau^i}$ for $0 \le i \le s-1$, so $P_0(T)^{\tau^{-i}}$ divides $\tilde{x}(T)$ for $0 \le i \le s-1$. Now, $P_0(T)$ is irreducible so for each i, $P_0(T)^{\tau^i}$ is either equal to $P_0(T)$ or relatively prime to it. Let $P_1(T)$ be the product of the distinct $P_0(T)^{\tau^i}$. Then $P_1(T)$ is the minimal polynomial of α over $K(i)$, and it divides $\tilde{x}(T)$. Moreover $P_1(T)^\sigma$ divides $\tilde{x}(T)^\sigma = \tilde{x}(T)$, and the minimal polynomial of α over K is equal to $P_1(T)$ if $P_1(T)^\sigma = P_1(T)$ and $P_1(T)P_1(T)^\sigma$ otherwise, so this minimal polynomial divides $\tilde{x}(T)$. But this is contrary to the assumption that $\tilde{x}(T)$ has no polynomial factor defined over k. Thus the symbol $(\tilde{x}(T), -1)$ has no poles and is therefore a constant symbol by (1) above.

Let $\tilde{x}(T)$ be as in lemma 3.5. By (2) above, if the symbol $(\tilde{x}(T), -1)$ is a constant symbol then its value is given by $(\tilde{x}(t), -1)$ for some $t \in k$ such that $\tilde{x}(t) \neq 0$. Then $\tilde{x}(t) \in k^+$. Moreover $c(t) \in k'$ and $\tilde{c}(t) \in k^+$. Now $c(t)$ can be written $\gamma(w^\sigma/w)(x^\tau/x)$ for some w and $x \in k'$, where γ is one of the set of representatives for S_k chosen above. Set $\tilde{x}_1 = xx^\sigma$. Let $c_1(T) = \gamma^{-1}c(T)$. Then $c_1(T) \in K'$ is also an element of norm 1 from K' to K. Let $\tilde{c}_1(T) = c_1(T)c_1^\sigma(T) \in K^+$. Then by lemma 3.5, we have an $\tilde{x}_1(T) \in K^+$ such that $\tilde{c}_1(T) = \tilde{x}_1(T)^\tau / \tilde{x}_1(T)$ and $(\tilde{x}_1(T), -1)$ is a constant symbol. Now, since $\tilde{x}_1(t)^\tau / \tilde{x}_1(t) = \tilde{c}_1(t) = \tilde{x}_1^\tau / \tilde{x}_1$, we see that $\tilde{x}_1(t)$ differs from $\tilde{x}_1$ by multiplication by an element of k^*. But lemma 3.5 only gives $\tilde{x}_1(T)$ up to an element of k^*, so we may assume that $\tilde{x}_1(t) = \tilde{x}_1$. Then $(\tilde{x}_1(T), -1) = (\tilde{x}_1, -1) = 0$. This means that $c_1(T)$ can be written $(w(T)^\sigma/w(T))(x(T)^\tau/x(T))$, which concludes the proof of part (ii).

Finally, we have some special cases where although $\mathrm{Gal}(K'/K)$ is not cyclic, the group S_K is trivial.

Theorem 3.6: *The group S_K is trivial for the following fields K:*

(i) $K = \mathbb{Q}$.

(ii) K is any number field having only one place lying over 2 or such that at most one place over 2 has decomposition group equal to $\mathrm{Gal}(K'/K)$.

(iii) K is any local field whose residue field has characteristic different from 2.

(iv) $K = k(T)$ where k is any field such that S_k is trivial.

Proof: The group S_K is trivial if and only if for every element $c \in K'$ such that $N_{K'/K}(c) = 1$, there exist elements x and $w \in K'$ such that $c = (x^\tau/x)(w^\sigma/w)$. In each part we show how to obtain such elements for any given c, using properties of the Brauer group of K.

(i) Let $K = \mathbb{Q}$ and let $c \in K'$ be an element of norm 1. We will exhibit an explicit $x \in K'$ and a $w \in K'$ defined up to $(K^+)^*$ such that $c = w^\sigma x^\tau/(wx)$. We proceed as follows. Let $\tilde{c} = cc^\sigma \in K^+$. Then $\tilde{c}$ is an element of K^+ with $N_{K^+/\mathbb{Q}}(\tilde{c}) = 1$, so by Hilbert's theorem 90, there exists $\tilde{x} \in K^+$, defined up to $\mathbb{Q}^*$, such that $\tilde{c} = \tilde{x}^\tau/\tilde{x}$. Fix a choice of such a $\tilde{x}$. Now, $K' = K^+(i)$ so the symbol $(\tilde{c}, -1) = 0$ in the Brauer group of K^+. Thus $(\tilde{x}^\tau/\tilde{x}, -1) = 0$ and so $(\tilde{x}, -1) = (\tilde{x}^\tau, -1)$ in $\mathrm{Br}_2(K^+)$.

For any prime $\mathbf{p}$ of K^+, let $K^+_{\mathbf{p}}$ denote the completion of K^+ at $\mathbf{p}$. The condition $(\tilde{x}, -1) = (\tilde{x}^\tau, -1)$ ensures that the local symbols $(\tilde{x}, -1)_{\mathbf{p}}$ are either simultaneously trivial or simultaneously non-trivial for all $\mathbf{p}$ lying over a given odd prime p in $\mathbb{Z}$, or lying over ∞. They are trivial for any $\mathbf{p}$ such that $[K^+_{\mathbf{p}} : \mathbb{Q}_p] > 1$, for this degree must be a power of 2 and $p^{2^r} \equiv 1 \bmod 4$ for all odd p when $r > 1$, so there is a square root of -1 in the field $K^+_{\mathbf{p}}$.

Lemma 3.7: *There exists an element $\hat{x} \in \mathbb{Q}^+$ such that $\tilde{c} = \hat{x}^\tau/\hat{x}$ and $(\hat{x}, -1) = 0$ in $Br_2(\mathbb{Q}^+)$.*

Proof: Let $p_1, \ldots, p_n$ be the set of odd primes such that for all primes $\mathbf{p}$ of K^+ lying over one of the p_i, the local symbol $(\tilde{x}, -1)_{\mathbf{p}}$ is non-trivial in $\mathrm{Br}_2(K^+_{\mathbf{p}})$. If $(\tilde{x}, -1)$ is trivial at all the places at ∞ of K^+ set $a = p_1 \cdots p_n$ and if it is non-trivial set $a = -p_1 \cdots p_n$.

Let $\hat{x} = a\tilde{x}$. Clearly $\hat{x}$ satisfies $\tilde{c} = \hat{x}^\tau/\hat{x}$. Moreover, the symbol $(\hat{x}, -1)$ is trivial at ∞ by the choice of a, and it is trivial at every prime $\mathbf{p}$ of K^+ lying over an odd prime p of

$\mathbb{Z}$, by construction (the symbol $(-1, p_i)$ is non-trivial only in $\mathrm{Br}_2(K^+_{\mathbf{p}})$ for primes $\mathbf{p}$ lying over p_i or over 2). But K^+ is a totally ramified extension of $\mathbb{Q}$, so there is only one prime of K^+ lying over 2. So $(\hat{x}, -1)$ must be trivial also at that prime, and thus $(\hat{x}, -1) = 0$ in $\mathrm{Br}_2(K^+)$.

We now finish the proof of (i). Let $\hat{x}$ be as in lemma 3.7. Then since $(\hat{x}, -1) = 0$ in $\mathrm{Br}_2(K^+)$, there exists an element $x \in K' = K^+(i)$ such that $\hat{x} = xx^\sigma$. This gives $\tilde{c} = \big(x^\tau/x\big)\big(x^\tau/x\big)^\sigma$. So c is equal to x^τ/x up to a element of K' whose norm to K^+ is 1: by Hilbert's theorem 90 such an element can be written w^σ/w for some $w \in K'$ and we obtain $c = \big(x^\tau/x\big)\big(w^\sigma/w\big)$.

(ii) The reasoning is identical to (i). Given $c \in K'$ with $N_{K'/K}(c) = 1$, and setting $\tilde{c} = cc^\sigma$, we can give an element $\hat{x} \in K^+$ such that $\tilde{c} = \hat{x}^\tau/\hat{x}$ and such that the local symbol $(\hat{x}, -1)_{\mathbf{p}}$ is trivial in $\mathrm{Br}_2(K^+_{\mathbf{p}})$ for places $\mathbf{p}$ of K^+ lying over all except at most one place (i.e. over all places) of K.

(iii) Let K be a local field with maximal ideal $(\mathbf{p})$. Then K^+ has just one prime $\mathfrak{p}$ lying over $\mathbf{p}$. Let $c \in K'$ satisfy $N_{K'/K}(c) = 1$ and let $\tilde{x} \in K^+$ be such that $\tilde{c} = \tilde{x}^\tau/\tilde{x}$. Then the local symbol $(\tilde{x}, -1)_{\mathfrak{p}}$ must be trivial by the product formula.

(iv) This is an immediate consequence of theorem 2, part (ii).

§4. Construction of cyclic extensions

For every field K of characteristic zero, choose an algebraic closure $\overline{K}$ of K. All extensions of K are considered as subfields of $\overline{K}$. Let $\mathfrak{C}_K$ denote the set of cyclic Galois extensions of K of degree q. For a field L in $\mathfrak{C}_K$, we will use the notation of §2. For every field K of characteristic zero such that the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is not trivial, we choose two integers m and s as in lemma 2.1 and set $k = (m^s - 1)/q$.

We now describe the connection between the set $\mathfrak{C}_K$ and the group S_K which was defined in the previous section.

Lemma 4.1: *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is not cyclic. Then the following map is well-defined :*

$$\begin{array}{rccc} \pi : & \mathfrak{C}_K & \longrightarrow & S_K \\ & L & \longmapsto & [c] \end{array}$$

where $[c]$ *is the class of* $c = b\,z^{(m-1)/2}$ *in* S_K*, and* b *and* z *are as in proposition* 2.4.

Proof: We must first prove that $N_{K(\zeta)/K}(c) = 1$. Since $z^\sigma = z$, we have $c\,c^\sigma = b\,b^\sigma z^{m-1}$. Since $z^\tau/z^m = b\,b^\sigma$, we obtain $c\,c^\sigma = z^\tau/z$ and this completes the first part of the proof.

It remains to prove that the class of c does not depend on the choice of the generator α of $L \otimes K(\zeta)$. So let α be such a generator and let λ be in $K(\zeta)^*$. Let b, z and c (respectively b', z' and c') be associated to α (respectively to $\lambda\alpha$) as in proposition 2.4. Then we have $z = z'\,\lambda\,\lambda^\sigma$ and $b' = b\;(\lambda^m/\lambda^\tau)$. Therefore we have $c = c'\;(\lambda^\tau/\lambda)\;\big((\lambda^{(m-1)/2})^\sigma/\lambda^{(m-1)/2}\big)$. So $[c'] = [c]$.

Remark: If the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is cyclic, then the group S_K is trivial so the map $\pi : \mathfrak{C}_K \to S_K$ is defined in an obvious way.

Let us explain how the group S_K parametrizes the set $\mathfrak{C}_K$.

Theorem 4.2: *Let* θ *be an element in* S_K *such that the set* $\pi^{-1}(\{\theta\})$ *is not empty. Then there exists an integer* n *and a polynomial* $P_\theta \in K(T_0, \ldots, T_n)[X]$ *of degree* q*, where* $T_0, \ldots, T_n$ *are indeterminates over* K*, which parametrizes all extensions* L *in* $\mathcal{C}_K$ *such that* $\pi(L) = \theta$*. This means that for each such* L*, there exist* $t_0, \ldots, t_n$ *in* K *such that the polynomial* $P_\theta(t_0, \ldots, t_n, X) \in K[X]$ *is irreducible and* L *is its splitting field.*

Before proving the theorem, we need a technical lemma.

Lemma 4.3: *Suppose that the group* $\mathrm{Gal}\big(K(\zeta)/K\big)$ *is not cyclic. Let* $\theta \in S_K$ *be such that the set* $\pi^{-1}(\{\theta\})$ *is not empty. Let* t *and* λ *be in* $K(\zeta)^*$ *such that* $N_{K(\zeta)/K}(t) = 1$*,* $[t] = \theta$*,* $\lambda^\sigma = \lambda$ *and* $t\,t^\sigma = \lambda^\tau/\lambda$*.*

Let $L \in \mathfrak{C}_K$ be such that $\pi(L) = \theta$. Then there exist a generator α of $L \otimes K(\zeta)$, $x \in K(\zeta)^*$ and $y \in K^*$ such that

$$b = t\,(\lambda\,y)^{(1-m)/2}\,(x^\sigma/x) \qquad \textit{and} \qquad z = \lambda\,y,$$

where b and z are as in proposition 2.4.

Proof: Let $L \in \mathfrak{C}_K$ be such that $\pi(L) = \theta$. Let α be a generator of $L \otimes K(\zeta)$ and let $c = b\,z^{(m-1)/2}$ which is corresponded to. Since $[c] = [t]$, there exist $u \in K(\zeta)^*$ and $v \in K(\zeta)^*$ such that $c = t\,(u^\sigma/u)\,(v^\tau/v)$. Let c' be associated to the generator $v\alpha$. We then have $c' = t\,\big((u\,v^{(1-m)/2})^\sigma/u\,v^{(1-m)/2}\big)$. Therefore we can choose the generator α such that $c = t\,(x^\sigma/x)$, with $x \in K(\zeta)^*$. In this case, set $y = z/\lambda$. We have $y^\tau/y = (z^\tau/z)\,(\lambda/\lambda^\tau)$, i.e. $y^\tau/y = c\,c^\sigma\,(\lambda/\lambda^\tau) = t\,t^\sigma\,(\lambda/\lambda^\tau) = 1$. We clearly have $y^\sigma = y$ so $y \in K^*$. As $b = c\,z^{(1-m)/2}$, the equality for b holds.

Proof of theorem 4.2: If the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is cyclic, the theorem holds: indeed, it is known that there is a generic Galois extension for the cyclic group of order q over K (see [Sa 1], theorem 2.1).

Therefore, for the remainder of this proof, we assume that the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is not cyclic. Let t and λ be in $K(\zeta)^*$ as in lemma 4.3. Let $X_0, \ldots, X_{2s}$ be $2s+1$ indeterminates over $K(\zeta)$. Since the group $\mathrm{Gal}\big(K(\zeta, X_0, \ldots, X_{2s})/K(X_0, \ldots, X_{2s})\big)$ is isomorphic to $\mathrm{Gal}\big(K(\zeta)/K\big)$, let σ and τ also denote the elements of $\mathrm{Gal}\big(K(\zeta, X_0, \ldots, X_{2s})/K(X_0, \ldots, X_{2s})\big)$ such that $\zeta^\sigma = \zeta^{-1}$ and $\zeta^\tau = \zeta^m$. Set

$$Z = \lambda\,X_{2s} \qquad \text{and} \qquad B = t\,Z^{(1-m)/2}\left(\sum_{i=0}^{2s-1} X_i \zeta^{-i}\right)\left(\sum_{i=0}^{2s-1} X_i \zeta^{i}\right)^{-1}.$$

For all $j \in (\mathbb{Z}/q\mathbb{Z})^*$, define $F_j \in K(\zeta, X_0, \ldots, X_{2s})$ by

$$F_1 = 1\ , \quad F_{-1} = Z^{-kk'} \prod_{x=1}^{s} \big(B^{-k' m^{x-1}}\big)^{\tau^{s-x}},$$

$$F_{\overline{m}^{\,\ell}} = \left(\prod_{x=1}^{\ell} \big(B^{-kk' m^{x-1}}\big)^{\tau^{\ell-x}}\right)\left(\prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}}\right)^{(m^\ell - <\overline{m}^{\,\ell}>)/q}, \ \forall \ell \in \{1, \ldots, s-1\},$$

$$F_{-\overline{m}^{\,\ell}} = \big(Z^{-kk'}\big)^{\tau^\ell}\left(\prod_{x=1}^{\ell} \big(B^{kk' m^{x-1}}\big)^{\tau^{\ell-x}}\right)\left(\prod_{x=1}^{s} \big(B^{-k' m^{x-1}}\big)^{\tau^{s-x}}\right)^{(m^\ell + <-\overline{m}^{\,\ell}>)/q},$$
$$\forall \ell \in \{1, \ldots, s-1\},$$

$$F_j = 0 \quad \text{otherwise.}$$

For all integers p such that $1 \leq p \leq q$ and for all $(j_1, \ldots, j_p) \in \big((\mathbb{Z}/q\mathbb{Z})^*\big)^p$, set

$$a_{j_1,\ldots,j_p} = \sum_{\substack{(i_1,\ldots,i_p)\in(\mathbb{Z}/q\mathbb{Z})^p \\ i_1\neq\cdots\neq i_p}} \zeta^{i_1 j_1+\cdots+i_p j_p}.$$

We prove by induction on p, that $a_{j_1,\ldots,j_p}$ is an integer and $a_{j_1,\ldots,j_p} = 0$ if $j_1 + \cdots + j_p \neq 0$. For all integers p, denote by $\mathfrak{R}_p$ a set of representatives of the natural action of the symmetric group S_p on $\big((\mathbb{Z}/q\mathbb{Z})^*\big)^p$. For all integers p such that $1 \leq p \leq q$, define $A_p \in K(\zeta, X_0, \ldots, X_{2s})$ by

$$A_p = \sum_{\substack{(j_1,\ldots,j_p)\in\mathfrak{R}_p \\ j_1+\cdots+j_p=0}} a_{j_1,\ldots,j_p} F_{j_1} \ldots F_{j_p} \left(\prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}} \right)^{(<j_1>+\cdots+<j_p>)/q}.$$

First of all, it is clear that this sum does not depend on the choice of $\mathfrak{R}_p$. Secondly, let us compute ${A_p}^{\sigma}$ and ${A_p}^{\tau}$. We have $Z^{\sigma} = Z$ and $B\,B^{\sigma} = Z^{\tau}/Z^m$. Therefore, we deduce that

$$F_{j\overline{m}} = {F_j}^{\tau} {F_{\overline{m}}}^{<j>} \left(\prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}} \right)^{(m<j>-<j\overline{m}>)/q}$$

and

$${F_j}^{\sigma} = F_{-j}\, Z^{kk'<j>} \prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}},$$

for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$. Let us set $B_p = F_{j_1} \ldots F_{j_p} \left(\prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}} \right)^{(<j_1>+\cdots+<j_p>)/q}$. All computations done, we find that we have

$${B_p}^{\tau} = F_{j_1\overline{m}} \ldots F_{j_p\overline{m}} \left(\prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}} \right)^{(<j_1\overline{m}>+\cdots+<j_p\overline{m}>)/q}$$

and

$${B_p}^{\sigma} = F_{-j_1} \ldots F_{-j_p} \left(\prod_{x=1}^{s} \big(B^{k' m^{x-1}}\big)^{\tau^{s-x}} \right)^{(<-j_1>+\cdots+<-j_p>)/q}$$

for all $(j_1, \ldots, j_p) \in \big((\mathbb{Z}/q\mathbb{Z})^*\big)^p$ such that $j_1 + \cdots + j_p = 0$. Consequently, we have ${A_p}^{\tau} = A_p$ and ${A_p}^{\sigma} = A_p$, that is $A_p \in K(X_0, \ldots, X_{2s})$.

Let now $P_\theta \in K(X_0, \ldots, X_{2s})[X]$ be the polynomial

$$P_\theta = X^q + \sum_{p=1}^{q} (-1)^p\, A_p\, X^{q-p}.$$

On the other hand, let α be a generator of $L\otimes K(\zeta)$ as in lemma 4.3. For all $j \in (\mathbb{Z}/q\mathbb{Z})^*$, define $e_j \in L\otimes K(\zeta)$ by

$$e_{\overline{m}^\ell} = (\alpha^{kk'})^{\tau^\ell} \quad \text{and} \quad e_{-\overline{m}^\ell} = (\alpha^{kk'})^{\sigma\tau^\ell}, \forall \ell \in \{0, 1, \ldots, s-1\} \quad \text{and} \quad e_j = 0 \quad \text{otherwise.}$$

We clearly have ${e_j}^\sigma = e_{-j}$ and ${e_j}^\tau = e_{j\,\overline{m}}$, for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$. Since $(\alpha^{kk'})^\eta = \zeta\alpha^{kk'}$, it follows that ${e_j}^\eta = \zeta^j e_j$, for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$. As G. Smith did in [Sm], let us introduce $r_i \in L\otimes K(\zeta)$ for all $i \in \mathbb{Z}/q\mathbb{Z}$ by

$$r_i = \sum_{j\in(\mathbb{Z}/q\mathbb{Z})^*} e_j\,\zeta^{ij}.$$

It is clear that ${r_0}^\sigma = r_0$ and ${r_0}^\tau = r_0$. So we have $r_0 \in L$, that is $K(r_0) \subset L$. Since L/K is an abelian extension, $K(r_0)/K$ is a Galois extension. As ${r_0}^{\eta^i} = r_i$ for all $i \in \mathbb{Z}/q\mathbb{Z}$, we have $K(r_0) = K(r_i)_{i\in\mathbb{Z}/q\mathbb{Z}}$. Finally, we notice that $q\,e_1 = \sum_{i\in\mathbb{Z}/q\mathbb{Z}} r_i\,\zeta^{-i}$, so $e_1 \in K(r_0)\otimes K(\zeta)$. Since $L\otimes K(\zeta) = K(\zeta)(e_1)$, this yields $K(r_0) = L$. Thus, the minimal polynomial of r_0 over K is of degree q and is given by

$$Q = \prod_{i\in\mathbb{Z}/q\mathbb{Z}} (X - r_i).$$

We clearly have

$$Q = X^q + \sum_{p=1}^{q} (-1)^p\,\sigma_p\;X^{q-p},$$

with

$$\sigma_p = \sum_{\substack{(j_1,\ldots,j_p)\in\mathfrak{R}_p \\ j_1+\cdots+j_p=0}} a_{j_1,\ldots,j_p}\,e_{j_1}\ldots e_{j_p}, \forall p \in \{1, \ldots, q\}.$$

Now let $x \in K(\zeta)^*$ and $y \in K^*$ be as in lemma 4.3. Let us write $x = \sum_{i=0}^{2s-1} x_i\,\zeta^i$ and prove that $Q = P_\theta(x_0, \ldots, x_{2s-1}, y)$. We clearly have $b = B(x_0, \ldots, x_{2s-1}, y)$ and $z = Z(x_0, \ldots, x_{2s-1}, y)$. Since

$$e_1^q = \prod_{x=1}^{s} \left(b^{k'm^{x-1}}\right)^{\tau^{s-x}},$$

$$\frac{e_{\overline{m}}}{e_1^m} = b^{-kk'},\; e_{-1}e_1 = z^{-kk'}$$

and

$$\frac{e_{j\,\overline{m}}}{e_1^{<j\,\overline{m}>}} = \left(\frac{e_j}{e_1^{<j>}}\right)^\tau \left(\frac{e_m}{e_1^m}\right)^{<j>} e_1^{m<j>-<j\,\overline{m}>}, \forall j \in (\mathbb{Z}/q\mathbb{Z})^*,$$

we prove by induction that

$$\frac{e_j}{e_1^{<j>}} = F_j(x_0, \ldots, x_{2s-1}, y),\ \forall j \in (\mathbb{Z}/q\mathbb{Z})^*.$$

Therefore, we deduce that $Q = P_\theta(x_0, \ldots, x_{2s-1}, y)$. This completes the proof.

Let us now study the case $\theta = 1$. If the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is not cyclic, then we can take $t = 1$ and $\lambda = 1$, t and λ being those of lemma 4.3. So the polynomial P_1 is defined over $\mathbb{Q}(X_0, \ldots, X_{2s})$. Actually, we will exhibit a polynomial defined over $\mathbb{Q}[T_0, \ldots, T_{q/2}]$ wich parametrizes all extensions of $\mathfrak{C}_K$ over $1 \in S_K$, for every field K of characteristic zero. This polynomial is the polynomial $P \in \overline{\mathbb{Q}(T_0, \ldots, T_{q/2})}[X]$ wich was defined in §1 and is a generalization of the generic polynomial of degree a power of an odd prime p of G. Smith [Sm], to $p = 2$.

In the next and last theorem, P denotes the polynomial defined in §1.

Theorem 4.4: *(i) The polynomial P is independent of the choice of C_i, of A and of ζ.*

(ii) We have $P \in \mathbb{Q}[T_0, \ldots, T_{q/2}, X]$.

(iii) Let $(t_0, \ldots, t_{q/2}) \in K^{q/2+1}$ be such that the polynomial $P(t_0, \ldots, t_{q/2}, X) \in K[X]$ is irreducible. Then the Galois group of the splitting field of this polynomial over K is cyclic of order q. Moreover, the mapping $r_i \longmapsto r_{i+1}$, $i \in \mathbb{Z}/q\mathbb{Z}$, defines a generator of this Galois group, where r_i is the specialization of R_i for all $i \in \mathbb{Z}/q\mathbb{Z}$.

(iv) For every cyclic Galois extension L/K of order q such that $\pi(L) = 1$, there exists $(t_0, \ldots, t_{q/2}) \in K^{q/2+1}$ such that the polynomial $P(t_0, \ldots, t_{q/2}, X) \in K[X]$ is irreducible and L is its splitting field over K.

Proof: (i) For all $i \in (\mathbb{Z}/q\mathbb{Z})^*$, let us change the choice of the q-th root of B_i. Set $C'_i = C_i\,\zeta^{\alpha_i}$, $\alpha_i \in \mathbb{Z}/q\mathbb{Z}$ for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$ and define E'_j for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$ and R'_i for all $i \in \mathbb{Z}/q\mathbb{Z}$, as E_j and R_i, by changing C_i to C'_i. Let $\alpha \in \mathbb{Z}/q\mathbb{Z}$ be defined by $\alpha = \sum_{i \in (\mathbb{Z}/q\mathbb{Z})^*} \alpha_i\, i^{-1}$. We then have $E'_j = E_j\,\zeta^{j\alpha}$ for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$ and $R'_i = R_{i+\alpha}$ for all $i \in \mathbb{Z}/q\mathbb{Z}$. This completes the first part of the proof. Now it is clear that if we change A to $-A$, then, R_i is changed to $R_{i+q/2}$ for all $i \in \mathbb{Z}/q\mathbb{Z}$. Finally, if we change ζ to ζ^k, $k \in (\mathbb{Z}/q\mathbb{Z})^*$, then B_i is changed to B_{ik} for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$. Thus, if we change C_i to C_{ik} for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$, the R_i's are not changed. This completes the proof of (i).

Before proceeding to the proof of (ii) and (iii) of theorem 4.4, we give a technical lemma.

Lemma 4.5: *Let F be a field of characteristic zero and let $(t_0, \ldots, t_{q/2}) \in F^{q/2+1}$. For all $i \in (\mathbb{Z}/q\mathbb{Z})^*$ define $b_i \in F(\zeta)$ by*

$$b_i = \sum_{j=0}^{q/2-1} t_j \, \zeta^{ij}.$$

For all $i \in (\mathbb{Z}/q\mathbb{Z})^*$, let us choose $c_i \in \overline{F}$ such that $c_i^q = b_i$ and $a \in \overline{F}$ such that $a^2 = t_{q/2}$. Define in $\overline{F}$

$$\forall j \in (\mathbb{Z}/q\mathbb{Z})^*, \quad e_j = a \prod_{i \in (\mathbb{Z}/q\mathbb{Z})^*} c_i^{<ji^{-1}>}$$

$$\forall i \in \mathbb{Z}/q\mathbb{Z}, \quad r_i = \sum_{j \in (\mathbb{Z}/q\mathbb{Z})^*} e_j \, \zeta^{ij}.$$

Then $Q(r_0, \ldots, r_{q-1}) \in F$ for all $Q \in F[X_1, \ldots, X_q]^G$, where $X_1, \ldots, X_q$ are q indeterminates over F and G is the subgroup of the symmetric group $\mathfrak{S}_p$ generated by the q-cycle $(1\,2\ldots q)$.

Proof: Since F is of characteristic zero, we must prove that

$$\forall (\alpha_1, \ldots, \alpha_q) \in \mathbb{N}^q, \quad \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \prod_{\ell=1}^{q} {r_{i+\ell}}^{\alpha_\ell} \ \in F.$$

Thus, let $(\alpha_1, \ldots, \alpha_q)$ be in $\mathbb{N}^q$. We have

$$\sum_{i \in \mathbb{Z}/q\mathbb{Z}} \prod_{\ell=1}^{q} {r_{i+\ell}}^{\alpha_\ell} = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \sum_{\substack{1 \le \ell \le q \\ 1 \le m \le \alpha_\ell}} \sum_{j_{\ell,m} \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\prod_{\ell,m} e_{j_{\ell,m}} \right) \zeta^{\sum_\ell (i+\ell) \sum_m j_{\ell,m}},$$

that is

$$\sum_{i \in \mathbb{Z}/q\mathbb{Z}} \prod_{\ell=1}^{q} {r_{i+\ell}}^{\alpha_\ell} = \sum_{\substack{1 \le \ell \le q \\ 1 \le m \le \alpha_\ell}} \sum_{j_{\ell,m} \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\prod_{\ell,m} e_{j_{\ell,m}} \right) \zeta^{\sum_\ell \ell \sum_m j_{\ell,m}} \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \zeta^{i \sum_{\ell,m} j_{\ell,m}}$$

$$= q \sum_{\substack{1 \le \ell \le q \\ 1 \le m \le \alpha_\ell}} \sum_{\substack{j_{\ell,m} \in (\mathbb{Z}/q\mathbb{Z})^* \\ \sum_{\ell,m} j_{\ell,m} = 0}} \zeta^{\sum_{\ell,m} \ell j_{\ell,m}} \left(\prod_{\ell,m} e_{j_{\ell,m}} \right).$$

But if $\sum_{\ell,m} j_{\ell,m} = 0$, then

$$\forall j \in (\mathbb{Z}/q\mathbb{Z})^*, \quad \sum_{\ell,m} < j_{\ell,m} j^{-1} > \in q\mathbb{Z} \quad \text{and} \quad \alpha_1 + \ldots + \alpha_\ell \in 2\mathbb{Z},$$

and so we have

$$\prod_{\ell,m} e_{j_{\ell,m}} = t_{q/2}{}^{(\alpha_1+\cdots+\alpha_\ell)/2} \prod_{j\in(\mathbb{Z}/q\mathbb{Z})^*} b_j{}^{\left(\sum <j_{\ell,m}j^{-1}>\right)/q},$$

and consequently

$$\sum_{i\in\mathbb{Z}/q\mathbb{Z}} \prod_{\ell=1}^{q} r_{i+\ell}{}^{\alpha_\ell} \in F(\zeta).$$

As $b_i{}^g = b_{i\ell}$ if $g \in \mathrm{Gal}\big(K(\zeta)/K\big)$ and $\zeta^g = \zeta^\ell$, with $\ell \in (\mathbb{Z}/q\mathbb{Z})^*$, it is clear that $\sum_{i\in\mathbb{Z}/q\mathbb{Z}} \prod_{\ell=1}^{q} r_{i+\ell}{}^{\alpha_\ell}$ is invariant under the group $\mathrm{Gal}\big(K(\zeta)/K\big)$. This completes the proof.

Proof of theorem 4.4: (ii) Write $P = X^q + \sum_{p=1}^{q}(-1)^p\,\Sigma_p\,X^{q-p}$. We can apply lemma 4.5 with $F = \mathbb{Q}(T_0,\ldots,T_{q/2})$, $t_j = T_j$, $b_i = B_i$, $c_i = C_i$, $e_j = E_j$ and $r_i = R_i$. Since coefficients of a polynomial are symmetric polynomials of roots, we then have $\Sigma_p \in F$.

(iii) Let us choose $a \in \overline{K}$ and $(e_j)_{j\in(\mathbb{Z}/q\mathbb{Z})^*} \in \overline{K}^{\,q/2}$ such that

$$a^2 = t_{q/2} \quad \text{and} \quad e_j^q = \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} \left(\sum_{\ell=0}^{q/2-1} t_\ell\,\zeta^{i\ell}\right)^{<ji^{-1}>}, \quad \forall j \in (\mathbb{Z}/q\mathbb{Z})^*.$$

Let $r_i \in \overline{F}$ be defined by $r_i = \sum_{j\in\mathbb{Z}/q\mathbb{Z}} e_j\,\zeta^{ij}$, for all $i \in \mathbb{Z}/q\mathbb{Z}$. According to the relations between coefficients and roots of a polynomial, we have $P(t_0,\ldots,t_{q/2},X) = \prod_{i\in\mathbb{Z}/q\mathbb{Z}}(X - r_i)$ (see the proof of theorem 4.2 for the computation of the coefficients of $\prod_{i\in\mathbb{Z}/q\mathbb{Z}}(X - r_i)$). Let L denote the field $K(r_i)_{i\in\mathbb{Z}/q\mathbb{Z}}$.

Let $X_1,\ldots,X_q$ be q indeterminates over K and let G be the subgroup of $\mathfrak{S}_q$ generated by the q-cycle $(1\,2\ldots q)$. Let us define the rings B and A by $B = K[X_1,\ldots,X_q]$ and $A = B \cap K(X_1,\ldots,X_q)^G$. Let $f : B \to L$ be the ring homomorphism which extends the identity of K and such that $f(X_i) = r_{\overline{i}}$ for all $i \in \{1,2,\ldots,q\}$. This homomorphism is onto, so $\mathfrak{Q} = \mathrm{Ker} f$ is a maximal ideal of B. According to lemma 4.5, we have $f(A) = K$. Since B is integral over A, the natural group homomorphism $D_{\mathfrak{Q}} \to \mathrm{Gal}(L/K)$ is onto, where $D_{\mathfrak{Q}}$ is the decomposition group $D_{\mathfrak{Q}} = \{g \in G, \quad \mathfrak{Q}^g = \mathfrak{Q}\}$. On the other hand, the polynomial $P(t_0,\ldots,t_{q/2},X) \in K[X]$ is irreducible and K is of characteristic zero, so this polynomial is separable. It follows that for all $(i,j) \in (\mathbb{Z}/q\mathbb{Z})^2$, we have $i \neq j \Rightarrow r_i \neq r_j$. So the natural homomorphism $D_{\mathfrak{Q}} \to \mathrm{Gal}(L/K)$ is injective, therefore is an isomorphism. Then, for each element $g \in \mathrm{Gal}(L/K)$, there exists $\alpha \in \mathbb{Z}/q\mathbb{Z}$ such that $r_i{}^g = r_{i+\alpha}$, for all $i \in \mathbb{Z}/q\mathbb{Z}$. This completes the proof, since $P(t_0,\ldots,t_{q/2},X) \in K[X]$ is irreducible, so the group $\mathrm{Gal}(L/K)$ permutes the r_i transitively.

Before the proof of (iv) of theorem 4.4, we need the following useful lemma.

Lemma 4.6: *Let L be a cyclic extension of K of degree q. Let S be a subset of the group $\mathrm{Gal}\big(L\otimes K(\zeta)\big)/L$ such that S generates this group. Let $t_{q/2}\in K^*$ and $(b_i)_{i\in(\mathbb{Z}/q\mathbb{Z})^*}\in \big(K(\zeta)^*\big)^{q/2}$ such that ${b_i}^g=b_{i\ell}$, for all $i\in(\mathbb{Z}/q\mathbb{Z})^*$ and for all $g\in S$ with $\zeta^g=\zeta^\ell$. Suppose that there exists $(e_j)_{j\in(\mathbb{Z}/q\mathbb{Z})^*}\in\big(L\otimes K(\zeta)\big)^{q/2}$ such that*

$$\begin{cases} L\otimes K(\zeta)=K(\zeta)(e_1)\\ {e_1}^\eta=\zeta e_1\\ {e_1}^g=e_\ell,\ \forall g\in S\,,\ \text{with } \zeta^g=\zeta^\ell\\ e_1^q=t_{q/2}^{q/2}\displaystyle\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{<i^{-1}>}\\ \dfrac{e_j}{e_1^{<j>}}=t_{q/2}^{(1-<j>)/2}\displaystyle\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{(<ji^{-1}>-<j><i^{-1}>)/q},\ \forall j\in(\mathbb{Z}/q\mathbb{Z})^*. \end{cases}$$

Then, there exists $(t_0,\ldots,t_{q/2-1})\in K^{q/2}$ such that the polynomial $P(t_0,\ldots,t_{q/2},X)\in K[X]$ is irreducible and L is its splitting field.

Proof: Let $g\in S$ be such that $\zeta^g=\zeta^\ell$ with $\ell\in(\mathbb{Z}/q\mathbb{Z})^*$. Let $j\in(\mathbb{Z}/q\mathbb{Z})^*$; we compute ${e_j}^g$. We have

$$\left(\frac{e_j}{e_1^{<j>}}\right)^g=t_{q/2}^{(1-<j>)/2}\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} {b_i}^{(<ji^{-1}\ell>-<j><i^{-1}\ell>)/q}.$$

On the other hand, we have

$$\frac{e_{j\ell}}{e_\ell^{<j>}}=e_1^{<j\ell>-<j><\ell>}\,t_{q/2}^{(1-<j>+<j><\ell>-<j\ell>)/2}$$
$$\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{(<ji^{-1}\ell>-<j><i^{-1}\ell>+<i^{-1}>(<j><\ell>-<j\ell>))/q}.$$

It follows that

$$\left(\frac{e_j}{e_1^{<j>}}\right)^g\frac{e_\ell^{<j>}}{e_{j\ell}}=\left(e_1^{-q}\,t_{q/2}^{q/2}\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{<i^{-1}>}\right)^{(<j><\ell>-<j\ell>)/q},$$

that is

$$\left(\frac{e_j}{e_1^{<j>}}\right)^g\frac{e_\ell^{<j>}}{e_{j\ell}}=1.$$

Since ${e_1}^g=e_\ell$, we deduce that ${e_j}^g=e_{j\ell}$.

Let us now introduce $r_i\in L\otimes K(\zeta)$, for all $i\in\mathbb{Z}/q\mathbb{Z}$, by

$$r_i=\sum_{j\in(\mathbb{Z}/q\mathbb{Z})^*} e_j\,\zeta^{ij}.$$

So ${r_i}^g = r_i$, for all $i \in \mathbb{Z}/q\mathbb{Z}$. As S generates $\mathrm{Gal}\big(L \otimes K(\zeta)\big)/L$, this means that $r_i \in L$ for all $i \in \mathbb{Z}/q\mathbb{Z}$. Since $e_j e_1^{-<j>} \in K(\zeta)^*$ and ${e_1}^\eta = \zeta e_1$, we have ${e_j}^\eta = \zeta^j e_j$ for all $j \in (\mathbb{Z}/q\mathbb{Z})^*$, so ${r_i}^\eta = r_{i+1}$ for all $i \in \mathbb{Z}/q\mathbb{Z}$. As in the proof of Theorem 4.2, we prove that $K(r_0) = L$ and that the minimal polynomial of r_0 over K is $\prod_{i \in \mathbb{Z}/q\mathbb{Z}}(X - r_i)$. Finally, let $(t_0, \ldots, t_{q/2}) \in \big(K(\zeta)\big)^{q/2}$ be the solution of the Vandermonde system:

$$\sum_{j=0}^{q/2-1} t_j \, \zeta^{ij} = b_i \,, \ \forall i \in (\mathbb{Z}/q\mathbb{Z})^*.$$

Let $g \in S$ be such that $\zeta^g = \zeta^\ell$; since ${b_i}^g = b_{i\ell}$ for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$, it is clear that ${t_j}^g = t_j$ for all $j \in \{0, \ldots, q/2-1\}$. It follows that $(t_0, \ldots, t_{q/2-1}) \in K^{q/2}$. To conclude, we have $\prod_{i \in \mathbb{Z}/q\mathbb{Z}}(X - r_i) = P(t_0, \ldots, t_{q/2}, X)$ according to the relations between coefficients and roots of a polynomial.

Proof of theorem 4.4 (iv): Let L be a cyclic extension of K of degree q such that $\pi(L) = 1$.

First case (the most important one): The group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is not cyclic. We can then choose $S = \{\sigma, \tau\}$ in lemma 4.6. We know that we can choose $t = 1$ and $\lambda = 1$ in lemma 4.3. There so exist $\alpha \in L \otimes K(\zeta)$, $x \in K(\zeta)^*$ and $y \in K^*$ such that

$$\begin{cases} L \otimes K(\zeta) = K(\zeta)(\alpha) \\ \alpha^\eta = \zeta \, \alpha \\ \alpha^\sigma = y^{-1} \alpha^{-1} \\ \alpha^\tau = y^{(m-1)/2} \ \dfrac{x}{x^\sigma} \ \alpha^m \\ \alpha^{kq} = y^{-kq/2} \displaystyle\prod_{i=1}^{s} \left[\left(\frac{x^\sigma}{x} \right)^{m^{i-1}} \right]^{\tau^{s-i}} \qquad . \end{cases}$$

Let k' be an integer such that $kk' \equiv 1 \bmod q$. For all $j \in (\mathbb{Z}/q\mathbb{Z})^*$, define $b_j \in K(\zeta)^*$ by

$$\begin{cases} \forall i \in \{0, 1, \ldots, s-1\}, \begin{cases} b_{\overline{m}^i} = \big(x^{-k'}\big)^{\tau^{i-1}} \\ b_{-\overline{m}^i} = \big(x^{-k'}\big)^{\sigma\tau^{i-1}} \end{cases} \\ b_j = 1 \quad \text{otherwise.} \end{cases}$$

Since σ is of order 2, τ is of order s and σ and τ commute, it is clear that we have ${b_i}^\sigma = b_{-i}$ and ${b_i}^\tau = b_{i\,\overline{m}}$ for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$. Set $t_{q/2} = y^{-kk'}$. We have $t_{q/2} \in K^*$. Define now $(e_j)_{j \in (\mathbb{Z}/q\mathbb{Z})^*} \in \big(L \otimes K(\zeta)\big)^{q/2}$ by

$$\begin{cases} e_1 = \alpha^{kk'} \displaystyle\prod_{i=1}^{s} b_{\overline{m}^{1-i}}^{(<\overline{m}^{i-1}>-m^{i-1})/q} \ b_{-\overline{m}^{1-i}}^{(m^{i-1}+<-\overline{m}^{i-1}>)/q} \\ \forall j \in (\mathbb{Z}/q\mathbb{Z})^*, \quad j \neq 1, \quad \dfrac{e_j}{e_1^{<j>}} = t_{q/2}^{(1-<j>)/2} \displaystyle\prod_{i \in (\mathbb{Z}/q\mathbb{Z})^*} b_i^{(<ji^{-1}>-<j><i^{-1}>)/q}. \end{cases}$$

Let us check that the e_j's satisfy the hypothesis of lemma 4.6. As $e_1\alpha^{-kk'} \in K(\zeta)^*$, we have

$$L\otimes K(\zeta) = K(\zeta)(e_1) \qquad \text{and} \qquad {e_1}^{\eta} = \zeta\, e_1.$$

Since $\alpha^{kk'q} = t_{q/2}^{q/2} \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} \big(b_{\overline{m}^{1-i}}/b_{-\overline{m}^{1-i}}\big)^{m^{i-1}}$, we deduce that

$$e_1^q = t_{q/2}^{q/2} \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{<i^{-1}>}.$$

Since $\alpha^{kk'}\big(\alpha^{kk'}\big)^{\sigma} = t_{q/2}$, we have $e_1\,{e_1}^{\sigma} = t_{q/2}\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i$. Using definition of e_{-1}, it follows that $e_1\,e_{-1} = e_1^q\; t_{q/2}^{1-q/2} \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{1-<i^{-1}>}$, i.e. $e_1\,e_{-1} = t_{q/2}\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i$. Hence we deduce that

$${e_1}^{\sigma} = e_{-1}.$$

Finally, since $\big(\alpha^{kk'}\big)^{\tau}\alpha^{-kk'm} = t_{q/2}^{(1-m)/2}\,\big(b_{-\overline{m}}/b_{\overline{m}}\big)^{k}$,we have

$$\frac{{e_1}^{\tau}}{e_1^m} = t_{q/2}^{(1-m)/2} \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{(<\overline{m}i^{-1}>-m<i^{-1}>)/q}.$$

By the definition of $e_{\overline{m}}$, we have

$${e_1}^{\tau} = e_{\overline{m}}.$$

This completes the proof.

Second case: The group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is cyclic.

a) The group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is trivial.

We can choose $S=\emptyset$ in lemma 4.6. Let $\alpha\in L$ be such that $L=K(\alpha)$ and $\alpha^{\eta}=\zeta\,\alpha$. Let us define $(e_j)_{j\in(\mathbb{Z}/q\mathbb{Z})^*}\in L$ by $e_j=\alpha^{<j>}$ for all $j\in(\mathbb{Z}/q\mathbb{Z})^*$. Then, the e_j's satisfy the hypothesis of lemma 4.6, if we take $t_{q/2}=1$, $b_1=\alpha^q$ and $b_i=1$ for all $i\in(\mathbb{Z}/q\mathbb{Z})^*$, $i\neq 1$.

b) The group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is $\{1,\tau\}$, with $\zeta^{\tau}=\zeta^{-1}$.

Take $S=\{\tau\}$ in lemma 4.6. By proposition 2.2, there exist $\alpha\in L\otimes k(\zeta)$, $y\in K^*$ and $b\in K(\zeta)^*$ such that

$$\begin{cases} L\otimes k(\zeta) = k(\zeta)(\alpha) \\ \alpha^{\eta} = \alpha \\ \alpha^{\tau} = y\,\alpha^{-1} \\ \alpha^{q} = y^{q/2}\,\dfrac{b^{\tau}}{b}\ . \end{cases}$$

Define $(e_j)_{j\in(\mathbb{Z}/q\mathbb{Z})^*}\in\big(L\otimes K(\zeta)\big)^{q/2}$ by $e_j = b\,y^{(1-<j>)/2}\alpha^{<j>}$ for all $j\in(\mathbb{Z}/q\mathbb{Z})^*$. It is easy to check that the e_j are as in lemma 4.6, if we take $t_{q/2}=y$, $b_1=b^{\tau}$, $b_{-1}=b$ and $b_i=1$ for all $i\in(\mathbb{Z}/q\mathbb{Z})^*$ not equal to 1 or -1.

c) Finally, if we are not in the two previous cases, we know (see lemma 2.1) that the group $\mathrm{Gal}\big(K(\zeta)/K\big)$ is generated by τ of order s, with $\zeta^\tau = \zeta^m$ and $k = (m^s - 1)/q$ odd. Let us also take $S = \{\tau\}$ in lemma 4.6. By proposition 2.3, there exist $\alpha \in L\otimes K(\zeta)$ and $b \in K(\zeta)^*$ such that

$$\begin{cases} L\otimes k(\zeta) = k(\zeta)(\alpha) \\ \alpha^\eta = \alpha \\ \alpha^\tau = b^{-1}\,\alpha^m \\ \alpha^{kq} = \displaystyle\prod_{i=1}^{s} \big(b^{m^{i-1}}\big)^{\tau^{s-i}} \quad . \end{cases}$$

Let k' be an integer such that $kk' \equiv 1 \bmod q$. For all $j \in (\mathbb{Z}/q\mathbb{Z})^*$, define $b_j \in K(\zeta)^*$ by

$$\begin{cases} \forall i \in \{0, 1, \ldots, s-1\}\,,\ b_{\overline{m}^i} = (b^{k'})^{\tau^{i-1}} \\ b_j = 1 \quad \text{otherwise.} \end{cases}$$

Since τ is of order s, it is clear that ${b_i}^\tau = b_{i\,\overline{m}}$ for all $i \in (\mathbb{Z}/q\mathbb{Z})^*$. Define now $(e_j)_{j\in(\mathbb{Z}/q\mathbb{Z})^*} \in \big(L\otimes K(\zeta)\big)^{q/2}$ by

$$\begin{cases} e_1 = \alpha^{kk'} \displaystyle\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_{\overline{m}^{1-i}}^{(<\overline{m}^{i-1}>-m^{i-1})/q} \\ \forall j \in (\mathbb{Z}/q\mathbb{Z})^*\,, \quad j \neq 1\,, \quad \dfrac{e_j}{e_1^{<j>}} = \displaystyle\prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{(<ji^{-1}>-<j><i^{-1}>)/q}. \end{cases}$$

Let us check that the e_j's satisfy the hypothesis of lemma 4.6 if we take $t_{q/2} = 1$. Since $e_1\,\alpha^{-kk'} \in K(\zeta)^*$, we have

$$L\otimes K(\zeta) = K(\zeta)(e_1) \quad \text{and} \quad {e_1}^\eta = \zeta\, e_1.$$

Since $\alpha^{kk'q} = \prod_{i=1}^{s} b_{\overline{m}^{1-i}}^{m^{i-1}}$, we have

$$e_1^q = \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{<i^{-1}>}.$$

Let us now compute ${e_1}^\tau$. Since $\alpha^{kk'm}/(\alpha^{kk'})^\tau = b_{\overline{m}}^k$, we have

$$\frac{{e_1}^\tau}{e_1^m} = \prod_{i\in(\mathbb{Z}/q\mathbb{Z})^*} b_i^{(<\overline{m}i^{-1}>-m<i^{-1}>)/q}.$$

So we deduce that

$${e_1}^\tau = e_{\overline{m}}\,.$$

This completes the proof.

We then clearly have

Corollary 4.7: *Let K be a field of characteristic zero. If the group S_K is trivial then, for every cyclic Galois extension L/K of order q, there exists $(t_0, \ldots, t_{q/2}) \in K^{q/2+1}$ such that the polynomial $P(t_0, \ldots, t_{q/2}, X)$ is irreducible and L its splitting field.*

Remark: By theorem 3.6, this is the case if $K = \mathbb{Q}$ or $\mathbb{Q}(X_1, \ldots, X_m)$ where $X_1, \ldots, X_m$ are m indeterminates over $\mathbb{Q}$.

REFERENCES

[Ar] J. Arason, Cohomologishe Invarianten Quadratischer Formen, *J. Algebra* **36** (1975), 448–491.

[CF] J.W.S. Cassels and F. Fröhlich, eds. *Algebraic Number Theory*, Academic Press, 1967.

[DM-I] F. DeMeyer and E. Ingraham, Separable algebras over commutative rings, *in* Lecture Notes in Mathematiques No. 181, Springer-Verlag, Berlin, 1971.

[L] H.W. Lenstra, Rational functions invariant under a finite abelian group, *Invent. Math.* **25** (1974), 299–325.

[Pl] V.P. Platonov, A problem of Tannaka–Artin and groups of special projective conorms, *Soviet Math. Dokl.*, **16** (1975), No. 3, 782–786.

[Sa1] D.J. Saltman, Generic Galois Extensions and Problems in Field Theory, *Adv. in Math.* **43** (1982), 250–283.

[Sa2] D.J. Saltman, Retract Rational Fields and Cyclic Galois extensions, *Isr. J. Math.* **47** (1984), 165–215.

[Se] J-P. Serre, lettre ‘ Platonov.

[Sm] G.W. Smith, Generic Cyclic Polynomials of Odd Degree *Commun. Algebra* **19** (1991), 3367–3391.

(*) UFR de Mathématiques
Université Paris 7

75005 Paris (France)

(**) Laboratoire de Mathématiques
Faculté des Sciences de Besançon
25030 Besançon (France)