TOKYO J. MATH.
VOL. 25, NO. 1, 2002

A Note on the Construction of Metacyclic Extensions

Shin NAKANO and Masahiko SASE

Gakushuin University

(Communicated by T. Kawasaki)

Abstract. Let p be an odd prime and r a divisor of $p-1$. We present a characterization of metacyclic extensions of degree pr containing a given cyclic extension of degree r over a field of characteristic other than p. Furthermore, we give a method of constructing polynomials with Galois groups which are Frobenius groups of degree p.

1. Introduction.

Let p be an odd prime and r a divisor of $p-1$. Let k be a field of characteristic other than p. In this note, we investigate metacyclic extensions over k whose Galois groups are given as a semi-direct product $H \ltimes N$, where H and N are cyclic groups of order r and p, respectively. We will consider a cyclic extension K/k of degree r satisfying some technical conditions, and classify cyclic extensions over K of degree p which are Galois over k, and characterize such metacyclic extensions over k of degree pr in terms of the subextensions of $K(\zeta)/k$, where ζ is a primitive p-th root of unity. The discussion will be done via Kummer extensions over $K(\zeta)$ of degree p, for which Cohen's argument in [2, Chapter 5] is useful to us.

The Galois group G of an irreducible polynomial over k of degree p is regarded as a transitive permutation group of degree p. Furthermore, as observed by E. Galois himself, such G is a Frobenius group of order ps for some divisor s of $p-1$, provided G is solvable. We shall give a method of generating polynomials of degree p whose Galois groups are Frobenius groups.

This note contains partially the result of Imaoka and Kishi [4]. The authors would like to thank Prof. K. Miyake, Dr. Y. Kishi and Mr. M. Imaoka for their valuable discussions.

2. The metacyclic group $M_p(s|r)$.

Throughout this note, we will fix an odd prime p. The field $\mathbf{Z}/p\mathbf{Z}$ of integers modulo p will be denoted $\mathbf{F}_p$. Let r be a divisor of $p-1$.

We begin with the definition of a metacyclic group of order pr, denoted by $M_p(s|r)$, as follows. For the details of the group theoretical properties, see for example [3]. Consider a

Received January 23, 2002

group given by a semi-direct product $H \ltimes N$, where N is a normal subgroup of degree p and H is a cyclic subgroup of degree r. This is a metacyclic group with two generators g and h satisfying

$$g^p = h^r = 1\,, \quad gh = hg^x$$

where x is regarded as an element of $\mathbf{F}_p^\times$. In fact, g, h may be taken to be generators of N and H, respectively. Let s be the order of x. Since $gh^i = h^i g^{x^i}$ for $i \in \mathbf{Z}$, we see that s is a divisor of r, and further, the minimum positive integer i such that h^i commutes with g is given by $i = s$. It should be noted that the structure of the group is independent of the choice of x and determined by only r and s. We denote this group by $M_p(s|r)$. A Galois extension with Galois group $M_p(s|r)$ is called an $M_p(s|r)$-extension.

Let G be a finite group and N a normal subgroup of G. Suppose G/N is cyclic and N is abelian. Let Γ_1 and Γ_2 be abelian subgroups of G containing N. Then it is easy to show that $\Gamma_1\Gamma_2$ is also abelian. So there exists the maximum abelian subgroup of G containing N.

LEMMA 1. *Let G be a finite group and N a normal subgroup of G. Assume that G/N and N are cyclic groups of order r and p, respectively. Let s be the index of the maximum abelian subgroup of G containing N. Then $G = M_p(s|r)$.*

PROOF. Let g be a generator of N and take $h \in G$ such that its class in G/N is a generator of G/N. Replacing h by its p-th power if needed, we have $g^p = h^r = 1$. There is $x \in \mathbf{F}_p^\times$ such that $gh = hg^x$. Since $gh^i = h^i g^{x^i}$ for $i \in \mathbf{Z}$, the order of x is given by

$$\begin{aligned} &\min\{i \mid i > 0,\ x^i = 1\} = \min\{i \mid i > 0, gh^i = h^i g\} \\ &= \min\{(G : \Gamma) \mid G \supset \Gamma \supset N \text{ and } \Gamma \text{ is abelian}\}\,. \end{aligned}$$

The last minimum is equal to s. Hence we obtain $G = M_p(s|r)$. □

One consequence of this lemma is that $M_p(s|r)$ and $M_p(s'|r)$ are never isomorphic if divisors s, s' of r are distinct. Besides this, we itemize some properties of $M_p(s|r)$ as follows:

- $M_p(s|r)$ is abelian, therefore cyclic, if and only if $s = 1$.
- $M_p(s|r)$ is a Frobenius group if and only if $s = r > 1$.
- $M_p(2|2)$ is the dihedral group of order $2p$.

As mentioned in Introduction, if the Galois group of an irreducible polynomial over k of degree p is solvable, then it is a Frobenius group of order ps for some divisor s of $p-1$. In other words, the Galois group of such a polynomial is $M_p(s|s)$. We will consider polynomials of this kind, in the last two sections.

3. Cyclic extensions.

Let ζ be a fixed primitive p-th root of unity. For a field F, $\tilde{F}$ will mean the p-th cyclotomic extension of F, that is, $\tilde{F} = F(\zeta)$. For a Galois extension E/F, we denote its Galois group by $\mathrm{Gal}(E/F)$.

Let K be a field of characteristic other than p. Put $V(\tilde{K}) = \tilde{K}^{\times}/\tilde{K}^{\times p}$ which is considered to be an $\mathbf{F}_p$-vector space. Let

$$\tilde{K}^{\times} \to V(\tilde{K}), \quad \alpha \mapsto \bar{\alpha}$$

be the canonical surjective homomorphism. Kummer theory says that any cyclic extension over $\tilde{K}$ of degree p is given by $\tilde{K}(\sqrt[p]{\alpha})$ for some $\alpha \in \tilde{K}^{\times}$. Thus, we have a bijection between the sets of such cyclic extensions and of one-dimensional subspaces of $V(\tilde{K})$. Let σ be a generator of $\mathrm{Gal}(\tilde{K}/K)$ and put $d = [\tilde{K} : K]$. We define the injective homomorphism $\chi : \mathrm{Gal}(\tilde{K}/K) \to \mathbf{F}_p^{\times}$ by $\zeta^{\sigma} = \zeta^{\chi(\sigma)}$. Let ε be an idempotent of the group algebra $\mathbf{F}_p[\mathrm{Gal}(\tilde{K}/K)]$ defined by

$$\varepsilon = \frac{1}{d}\sum_{i=0}^{d-1} \chi(\sigma^{-i})\sigma^{i}\,.$$

This is an $\mathbf{F}_p$-linear transformation on $V(\tilde{K})$, and its image $V(\tilde{K})^{\varepsilon}$ is the eigenspace of σ with the eigenvalue $\chi(\sigma)$, that is,

$$\bar{\alpha}^{\sigma} = \bar{\alpha}^{\chi(\sigma)} \;\Leftrightarrow\; \bar{\alpha} \in V(\tilde{K})^{\varepsilon}$$

for $\alpha \in \tilde{K}^{\times}$. We define

$$I(\tilde{K}) = \{\alpha \in \tilde{K}^{\times} \mid \bar{\alpha} \in V(\tilde{K})^{\varepsilon}\} \quad \text{and} \quad I^{*}(\tilde{K}) = \{\alpha \in I(\tilde{K}) \mid \alpha \notin \tilde{K}^{\times p}\}\,.$$

The following proposition is known (cf. Cohen [2, Chapter 5]).

PROPOSITION 1. *If L is a cyclic extension of degree p over K, and $\alpha \in \tilde{K}^{\times}$ satisfies $\tilde{L} = \tilde{K}(\sqrt[p]{\alpha})$, then we have $\alpha \in I^{*}(\tilde{K})$. Conversely, for any $\alpha \in I^{*}(\tilde{K})$, $\tilde{K}(\sqrt[p]{\alpha})$ is an abelian extension over K of degree dp which contains a unique cyclic extension L over K of degree p.*

Thus there is a bijection between the sets of cyclic extensions over K of degree p and of one-dimensional subspaces of $V(\tilde{K})^{\varepsilon}$.

4. $M_p(s|r)$-extensions.

In this section, we consider the case that K has a subfield k such that K/k is a cyclic extension of degree r. Let us assume K/k has the following properties:

(A) $K \cap \tilde{k} = k$,

(B) $r > 1$ and r is a divisor of $d = [\tilde{K} : K]$.

We will fix such an extension K/k in the following discussion. Under these assumptions, we will characterize the cyclic extensions over K of degree p which are Galois extensions over k with the Galois group $M_p(s|r)$, that is, $M_p(s|r)$-extensions over k containing K. The degree $[\tilde{k} : k]$ is equal to $d = [\tilde{K} : K]$ by (A). So the four fields k, K, $\tilde{K}$ and $\tilde{k}$ form a "parallelogram". It follows that $\tilde{K}/k$ is abelian and its Galois group is the direct product of those of $\tilde{K}/K$ and $\tilde{K}/\tilde{k}$. Since d divides $p-1$, the assumption (B) implies that the degree $[\tilde{K} : k] = rd$ is prime to p.

We put $V(E) = E^\times/E^{\times p}$ also for a subextension E of $\tilde{K}/k$. Since $E^\times \cap \tilde{K}^{\times p} = E^{\times p}$, we can regard $V(E)$ as a subspace of $V(\tilde{K})$. Moreover $\mathrm{Gal}(\tilde{K}/k)$ acts on $V(E)$ naturally, so $V(E)$ is an $\mathbf{F}_p[\mathrm{Gal}(\tilde{K}/k)]$-module.

LEMMA 2. *Let H be a subgroup of* $\mathrm{Gal}(\tilde{K}/k)$ *and E the subextension of $\tilde{K}/k$ corresponding to H. Then, for $\alpha \in \tilde{K}^\times$ the following properties* (i), (ii) *are equivalent*:

(i) $\bar{\alpha} \in V(E)$.

(ii) $\bar{\alpha}^\xi = \bar{\alpha}$ for every $\xi \in H$.

PROOF. It is easy to see that (i) implies (ii). Conversely, if α satisfies (ii), then $\bar{\alpha}^{[\tilde{K}:E]} = \overline{N_{\tilde{K}/E}(\alpha)} \in V(E)$. Since $[\tilde{K} : E]$ is prime to p, we have $\bar{\alpha} \in V(E)$. □

Let σ and ε be as in the previous section. For a subextension E of $\tilde{K}/k$, we also define

$$I(E) = \{\alpha \in \tilde{K}^\times \mid \bar{\alpha} \in V(E)^\varepsilon\} \quad \text{and} \quad I^*(E) = \{\, \alpha \in I(E) \mid \alpha \notin \tilde{K}^{\times p}\}\,.$$

Note that $V(E) \cap V(\tilde{K})^\varepsilon = V(E)^\varepsilon$ holds, since ε is an idempotent. Let τ be a generator of $\mathrm{Gal}(\tilde{K}/\tilde{k})$. Then the Galois group of $\tilde{K}/k$ is generated by σ and τ. Let s be a divisor of r and put

$$J_s = \{\, j \mid 1 \le j \le s,\, (j, s) = 1\}.$$

For $j \in J_s$, we define an element of $\mathrm{Gal}(\tilde{K}/k)$ as

$$\rho(s, j) = \sigma^{dj/s}\tau$$

and denote by $E(s, j)$ the subextension of $\tilde{K}/k$ corresponding to the cyclic subgroup generated by $\rho(s, j)$.

The main theorem of this note is the following

THEOREM 1. *Let L be a cyclic extension of degree p over K and take $\alpha \in I^*(\tilde{K})$ with $\tilde{L} = \tilde{K}(\sqrt[p]{\alpha})$.*

(1) *If L/k is Galois, then L/k is an $M_p(s|r)$-extension for some divisor s of r.*

(2) *Let s be a divisor of r. Then L/k is an $M_p(s|r)$-extension if and only if $\alpha \in I^*(E(s, j))$ for some $j \in J_s$.*

Since (1) is an immediate consequence of Lemma 1, we shall show (2) only. We need the following two lemmas.

LEMMA 3. *Let F be a subfield of $\tilde{K}$ such that $\tilde{K}/F$ is a Galois extension. Then, for $\alpha \in \tilde{K}^\times$, the following* (i), (ii) *are equivalent*:

(i) *$\tilde{K}(\sqrt[p]{\alpha})/F$ is a Galois extension.*

(ii) *For every $\xi \in$ $\mathrm{Gal}(\tilde{K}/F)$, there exists $x \in \mathbf{F}_p^\times$ such that $\bar{\alpha}^\xi = \bar{\alpha}^x$.*

PROOF. If $\tilde{K}(\sqrt[p]{\alpha})/F$ is a Galois extension, then $\tilde{K}(\sqrt[p]{\alpha^\xi}) = \tilde{K}(\sqrt[p]{\alpha})$ for any $\xi \in \mathrm{Gal}(\tilde{K}/F)$. Therefore, from Kummer theory, we see that there exists $x \in \mathbf{F}_p^\times$ such that $\bar{\alpha}^\xi = \bar{\alpha}^x$. The converse is obvious. □

LEMMA 4. *Suppose $\alpha \in \tilde{K}^\times$ satisfies $\bar{\alpha}^\tau = \bar{\alpha}^x$ for some $x \in \mathbf{F}_p^\times$. If the order of x is equal to s, then $\tilde{K}(\sqrt[p]{\alpha})/\tilde{k}$ is an $M_p(s|r)$-extension.*

PROOF. First we recall that s divides $r = [\tilde{K} : \tilde{k}]$. Let i be a divisor of r and F_i the subextension of $\tilde{K}/\tilde{k}$ corresponding to $\langle \tau^i \rangle$. Suppose $x^i = 1$. Then $\bar{\alpha}^{\tau^i} = \bar{\alpha}^{x^i} = \bar{\alpha}$, thus $\bar{\alpha} \in V(F_i)$ from Lemma 2. So, there exists $\beta \in F_i^\times$ such that $\bar{\beta} = \bar{\alpha}$, and $\tilde{K}(\wp\!\!\!\sqrt{\alpha})$ contains the cyclic extension $F_i(\sqrt[p]{\beta})$ over F_i of degree p. Hence $\tilde{K}(\sqrt[p]{\alpha})/F_i$ is abelian. Furthermore, it is not difficult to verify the converse. So, $\tilde{K}(\sqrt[p]{\alpha})/F_i$ is abelian if and only if $x^i = 1$. Therefore F_s is the smallest subextension of $\tilde{K}/\tilde{k}$ over which $\tilde{K}(\sqrt[p]{\alpha})$ is abelian. Using Lemma 1, we conclude that $\tilde{K}(\sqrt[p]{\alpha})/\tilde{k}$ is an $M_p(s|r)$-extension. □

PROOF OF THEOREM 1 (2). Assume that L is an $M_p(s|r)$-extension of k. Then $\tilde{L}/\tilde{k}$ is also an $M_p(s|r)$-extension. Therefore, it follows from Lemmas 3 and 4 that there exists $x \in \mathbf{F}_p^\times$ of order s with $\bar{\alpha}^\tau = \bar{\alpha}^x$. Since $\chi(\sigma^{d/s})$ is of order s as well, we can choose $j \in J_s$ satisfying $x\chi(\sigma^{d/s})^j = 1$. Then $\bar{\alpha}^{\rho(s,j)} = \bar{\alpha}^{\sigma^{dj/s}\tau} = \bar{\alpha}^{x\chi(\sigma^{dj/s})} = \bar{\alpha}$, and thus $\bar{\alpha} \in V(E(s,j))$ from Lemma 2. So we have $\bar{\alpha} \in V(E(s,j)) \cap V(\tilde{K})^\varepsilon = V(E(s,j))^\varepsilon$. Hence $\alpha \in I^*(E(s,j))$.

Conversely, suppose $\alpha \in I^*(E(s,j))$ for some $j \in J_s$. Then we have $\bar{\alpha}^{\rho(s,j)} = \bar{\alpha}$. On the other hand, we know the relation $\bar{\alpha}^\sigma = \bar{\alpha}^{\chi(\sigma)}$ and the fact that $\mathrm{Gal}(\tilde{K}/k)$ is generated by σ and $\rho(s,j)$. Thus, by Lemma 3, we see that $\tilde{L}/k$ is Galois. So, if L' is a conjugate field of L over k, then L' is contained in $\tilde{L}$ and $[L' : K] = p$, and thus L' must coincide with L. This means that L/k is Galois. The Galois group of L/k is isomorphic to $\mathrm{Gal}(\tilde{L}/\tilde{k})$. Now we have $\bar{\alpha}^\tau = \bar{\alpha}^{\sigma^{-dj/s}\rho(s,j)} = \bar{\alpha}^{\chi(\sigma^{-dj/s})}$. Since j is prime to s, the order of $\chi(\sigma^{-dj/s})$ is equal to s. Therefore, by Lemma 4, $\tilde{L}/\tilde{k}$ is an $M_p(s|r)$-extension, and so is L/k. □

In case $s = 1$, the theorem claims that L/k is abelian extension if and only if $\alpha \in I^*(\tilde{k})$. The case $r = s = 2$ where the Galois groups are dihedral was treated also by Imaoka and Kishi [4].

5. Defining polynomials for $M_p(s|r)$-extensions.

Let notations and assumptions be as in the previous section. We will fix $e \in \mathbf{Z}[G]$ satisfying $y\varepsilon \equiv e \bmod p$ for some $y \in \mathbf{F}_p^\times$. Then we have

$$I(E) = \{\beta^e \gamma^p \mid \beta \in E^\times, \gamma \in \tilde{K}^\times\},$$

for a subextension E of $\tilde{K}/k$.

Now it follows from Proposition 1 that a cyclic extension L over K of degree p is given by $L = K(Tr_{\tilde{L}/L}(\sqrt[p]{\beta^e}))$ with $\beta \in \tilde{K}^\times$ satisfying $\beta^e \notin \tilde{K}^{\times p}$, namely, $\beta^e \in I^*(\tilde{K})$. For such β, denote by $f_\beta(X)$ the monic minimal polynomial of $Tr_{\tilde{L}/L}(\sqrt[p]{\beta^e})$ over K. The next lemma on the coefficients of $f_\beta(X)$ is obtained by thorough calculations in Cohen [2, Chapter 5].

LEMMA 5. *Every coefficient of $f_\beta(X)$ of degree less than p is given in the form of a finite sum*

$$\sum_\nu c_\nu \beta^{z_\nu}, \quad c_\nu \in \mathbf{F}_K,\ z_\nu \in \mathbf{Z}[\mathrm{Gal}(\tilde{K}/K)],$$

where $\mathbf{F}_K$ is the prime field contained in K.

Suppose $\beta \in E(s, j)^{\times}$ satisfies $\beta^e \notin E(s, j)^{\times p}$, where s is a divisor of r and $j \in J_s$. Then $\beta^e \in I^*(E(s, j))$ and, by Theorem 1, the cyclic extension obtained by adjoining a root of $f_\beta(X)$ to K is an $M_p(s|r)$-extension over k. Furthermore, an $M_p(s|r)$-extension of this kind is always constructed in this manner. Now Lemma 5 implies that $f_\beta(X) \in k[X]$, since $K \cap E(s, j) = k$. So we are interested in the minimal splitting field of $f_\beta(X)$ over k. The Galois group of $f_\beta(X)$ needs to be a Frobenius group, that is, $M_p(t|t)$ with a divisor t of $p-1$. In fact, the following result is obtained in the case $s = r$.

THEOREM 2. *Let $j \in J_r$ and $\beta \in E(r, j)^{\times}$ satisfying $\beta^e \notin E(r, j)^{\times p}$. Then $f_\beta(X) \in k[X]$ and its minimal splitting field over k is the $M_p(r|r)$-extension L over k such that $K \subset L \subset \tilde{K}(\sqrt[p]{\beta^e})$.*

PROOF. Let L_β be the minimal splitting field of $f_\beta(X)$ over k, and put $K_\beta = L_\beta \cap K$. Then, since L_β/K_β is a cyclic extension of degree p, it follows that $L = L_\beta K$ is abelian over K_β. However, by Lemma 1, the $M_p(r|r)$-extension L/k never contains a subextension F such that $F \subsetneq K$ and L/F is abelian. Thus K_β must be equal to K. Hence we conclude $L_\beta = L$. □

As for a divisor s of r, we have the following

THEOREM 3. *Let s be a divisor of r and $j \in J_s$. Take $\beta \in E(s, j)^{\times}$ such that $\beta^e \notin E(s, j)^{\times p}$. Then $f_\beta(X) \in k[X]$ and its Galois group over k is isomorphic to $M_p(s|s)$.*

PROOF. Let K_s be the cyclic extension over k of degree s contained in K. Then $\tilde{K}_s$ is the subextension of $\tilde{K}/\tilde{k}$ corresponding to the subgroup $\langle \tau^s \rangle$. Since $\tau^s = \rho(s, j)^s \in \langle \rho(s, j) \rangle$, we have $E(s, j) \subseteq \tilde{K}_s$. So, applying the above discussion to the extension K_s/k instead of K/k, we completes the proof. □

Polynomials with Frobenius groups of degree p as Galois groups are studied from another viewpoint, by Bruen, Jensen and Yui [1].

6. Examples.

We will illustrate the above results with some numerical examples. Take $k = \mathbf{Q}$ and $p = 5$. In this case, $\tilde{\mathbf{Q}} = \mathbf{Q}(\zeta)$ is cyclic over $\mathbf{Q}$ of degree 4. Let $K = \mathbf{Q}(\sqrt{2+\sqrt{2}})$. Then $K/\mathbf{Q}$ is a cyclic extension of degree 4 satisfying the properties $K \cap \tilde{\mathbf{Q}} = \mathbf{Q}$ and $[\tilde{K} : K] = 4$. Put

$$\theta_1 = \sqrt{2+\sqrt{2}}, \quad \theta_2 = \sqrt{2-\sqrt{2}}, \quad \theta_3 = -\sqrt{2-\sqrt{2}}, \quad \theta_4 = -\sqrt{2+\sqrt{2}}.$$

We can take generators σ, τ of $\mathrm{Gal}(\tilde{K}/K)$ and $\mathrm{Gal}(\tilde{K}/\tilde{k})$, respectively, such as $\zeta^\sigma = \zeta^2$ and $\theta_1^\tau = \theta_2$. Then it is easy to check $\theta_2^\tau = \theta_4$ and $\theta_4^\tau = \theta_3$. Now we put $e = 3 + 4\sigma + 2\sigma^2 + \sigma^3$ which satisfies the congruence $2\varepsilon \equiv e \bmod 5$. For $\beta \in \tilde{K}^{\times}$ satisfying $\beta^e \in I^*(\tilde{K})$, the minimal polynomial $f_\beta(X)$ of $Tr_{\tilde{L}/L}(\sqrt[5]{\beta^e})$ is written in the form

$$f_\beta(X) = X^5 - 10N(\beta)X^3 - 5N(\beta)T(\beta^{1+\sigma})X^2 + 5N(\beta)(N(\beta) - T(\beta^{1+2\sigma+\sigma^2}))X - N(\beta)T(\beta^{2+3\sigma+\sigma^2})$$

with $N = N_{\tilde{K}/K}$ and $T = Tr_{\tilde{K}/K}$, which had appeared in Cohen [2, Chapter 5]. Using this, we present several defining polynomials for Frobenius extensions over **Q** via $E(4,1)$, $E(4,3)$ and $E(2,1)$.

(1) $E(4,1) = \mathbf{Q}(\xi)$ with $\xi = \theta_1\zeta + \theta_2\zeta^2 + \theta_4\zeta^4 + \theta_3\zeta^3$. If we choose $\beta_1 = \xi + 1$, then $\beta_1^e \in I^*(E(4,1))$ and

$$f_{\beta_1}(X) = X^5 - 310X^3 - 620X^2 + 10385X + 20956\,.$$

The Galois group of $f_{\beta_1}(X)$ over **Q** is $E_5(4|4)$, that is, the Frobenius group of order 20.

(2) $E(4,3) = \mathbf{Q}(\eta)$ with $\eta = \theta_1\zeta + \theta_2\zeta^3 + \theta_4\zeta^4 + \theta_3\zeta^2$. Taking $\beta_2 = \eta + 1$, we have $\beta_2^e \in I^*(E(4,3))$ and

$$f_{\beta_2}(X) = X^5 - 1110X^3 - 2220X^2 + 259185X + 75036\,,$$

which Galois group over **Q** is also the Frobenius group of order 20.

(3) $E(2,1) = \mathbf{Q}(\omega)$ with $\omega = \sqrt{-5 + 2\sqrt{5}}\sqrt{2}$. Put $\beta_3 = \omega + 1$. Then $\beta_3^e \in I^*(E(2,1))$ and

$$f_{\beta_3}(X) = X^5 - 410X^3 - 820X^2 + 23985X - 13284\,.$$

The Galois group of $f_{\beta_3}(X)$ over **Q** is the dihedral group of order 10.

References

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

[2] H. Cohen, *Advanced topics in computational number theory*, Springer (2000).

[3] B. Huppert, *Endliche Gruppen I*, Springer (1967).

[4] M. Imaoka and Y. Kishi, Spiegelung relation between dihedral extensions and Frobenius extensions, preprint.

Present Address:
Department of Mathematics, Gakushuin University,
Mejiro, Tokyo, 171–8588, Japan.
e-mail: shin@math.gakushuin.ac.jp
sasem@math.gakushuin.ac.jp