Tamely Eisenstein field with prime power discriminant

Komatsu, Toru
Faculty of Mathematics, Kyushu University

出版情報：MHF Preprint Series. 2006-13, 2006-03-16. Faculty of Mathematics, Kyushu University
バージョン：
権利関係：

MHF Preprint Series

Kyushu University
21st Century COE Program
Development of Dynamic Mathematics with High Functionality

Tamely Eisenstein field with prime power discriminant

T. Komatsu

MHF 2006-13

(Received March 16, 2006)

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

Tamely Eisenstein field with prime power discriminant

Toru KOMATSU

§ 1. Introduction

In this paper we study a non-Galois, totally and tamely ramified field with prime power discriminant and present a method for the constructions of such fields with some properties. The existence of such a field is an interesting problem not only for algebraic number theory but also for theory of association scheme (see Theorem 1.1, Hanaki-Uno [**4**]). We also study the Galois groups of the Galois closure extensions of such fields.

Let p be a prime number. For a monic polynomial $f(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{Q}[X]$ of degree d we say that $f(X)$ is a p-Eisenstein polynomial if the coefficients a_i satisfy $p \mid a_i$ for $0 \leq i \leq d-1$ and $p^2 \nmid a_0$. The zeros of a p-Eisenstein polynomial are called p-Eisenstein numbers. For a number field K we say that K is a p-Eisenstein field if K is generated by a p-Eisenstein number over $\mathbb{Q}$. It is known that $K/\mathbb{Q}$ is totally ramified at p if and only if K is a p-Eisenstein field (cf. [**2**]). We define six conditions (1) to (6) on an algebraic number field K with degree $d = [K : \mathbb{Q}]$ by

(1) the field K is not a Galois extension over $\mathbb{Q}$,

(2) the degree d is a divisor of $p-1$,

(3) the discriminant $\mathrm{disc}(K/\mathbb{Q})$ of K is equal to $\pm p^{d-1} \equiv 1 \pmod 4$,

(4) the field K is a p-Eisenstein field,

(5) the extension $K/\mathbb{Q}$ is unramified at all prime numbers other than p,

(6) the field K is totally real or totally imaginary.

We note that for an algebraic number field K with (2), it holds (3) if and only if K satisfies (4) and (5) (see Proposition 2.3). Hanaki and Uno showed the following theorem on the classification of association schemes.

Theorem 1.1 (Hanaki-Uno [**4**])**.** *Let (X, G) be an association scheme of prime order p with $\sharp G = d+1$. If there exist no algebraic number fields which satisfy all of the six conditions* (1) *to* (6)*, then (X, G) is algebraically isomorphic to a cyclotomic scheme.*

The following problem is natural to be considered.

Problem 1.2 (Hanaki [**3**])**.** *Are there any algebraic number fields K satisfying all of the six conditions* (1) *to* (6) *?*

In this paper we obtain an affirmative answer for the Problem 1.2 with explicit construction. We give a method for the constructions of fields satisfying all the six conditions (1) to (6). Let $\zeta = \zeta_p$ be a primitive p-th root of unity in $\overline{\mathbb{Q}}$. Let d be a positive divisor of $p-1$. Let L be the subfield of $\mathbb{Q}(\zeta)$ with $[L : \mathbb{Q}] = d$ and k a subfield of L whose degree $[k : \mathbb{Q}]$ is denoted by n. It holds that $n \mid d \mid p-1$. Let r be the ratio $d/n \in \mathbb{Z}$ which is equal to $[L : k]$. We assume that there exists an unramified cyclic extension M of k with degree r. Let E be the composite field LM of L and M. Then E is a Galois extension of k whose Galois group $G_0 = \mathrm{Gal}(E/k)$ is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^2$. Let G_1 and G_2 be subgroups of G_0 satisfying $E^{G_1} = L$ and $E^{G_2} = M$, respectively. Let G_3 be a subgroup of G_0 such that $G_3 \cap G_1 = G_3 \cap G_2 = 1$ and $G_3 \simeq \mathbb{Z}/r\mathbb{Z}$. We define a number field K to be the subfield E^{G_3} of E fixed by G_3.

Theorem 1.3. *The field K satisfies all of the six conditions* (1) *to* (6) *provided $r \geq 2$. If d divides $(p-1)/2$, then K is totally real with* $\mathrm{disc}(K/\mathbb{Q}) = p^{d-1}$*. When d is not a divisor of $(p-1)/2$, the field K is totally imaginary and* $\mathrm{disc}(K/\mathbb{Q}) = (-1)^{(p-1)/2}p^{d-1} = (-1)^{d/2}p^{d-1}$.

For example we may have $(p, n, r) = (229, 2, 3)$ and $(277, 3, 2)$ (see § 5 for the explicit constructions of K and the definition polynomials of K). The case $r = 1$ implies that $K = L$, which is a cyclic field satisfying the five conditions (2) to (6).

Let K be an algebraic number field with the five conditions (2) to (6). We denote by $\widetilde{K}$ the Galois closure extension of K over $\mathbb{Q}$ and $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. Note that G is isomorphic to a transitive subgroup of the symmetric group $\mathfrak{S}_d$ with degree d.

Proposition 1.4 (Proposition 3.6)**.** *If d is odd, then G is contained in the alternating group $\mathfrak{A}_d$ with degree d. When d is a prime number , the group G is simple.*

For a positive integer $d \in \mathbb{Z}$ with $d \geq 2$ let us denote by $\mathcal{T}_d$ the family of all the transitive subgroup of the symmetric group $\mathfrak{S}_d$ with degree d. For integers $d \in \mathbb{Z}$ with $2 \leq d \leq 7$ we define subfamilies $\mathcal{G}_d$ of $\mathcal{T}_d$ by

$$\mathcal{G}_2 = \{\mathcal{C}_2\}, \quad \mathcal{G}_3 = \{\mathcal{C}_3\}, \quad \mathcal{G}_4 = \{\mathcal{C}_4, \mathfrak{S}_4\}, \quad \mathcal{G}_5 = \{\mathcal{C}_5, \mathfrak{A}_5\},$$
$$\mathcal{G}_6 = \{\mathcal{C}_6, \mathcal{D}_3 \times \mathcal{C}_3, \mathfrak{A}_4 \times \mathcal{C}_2, \mathfrak{S}_5, \mathfrak{S}_6\}, \quad \mathcal{G}_7 = \{\mathcal{C}_7, \mathrm{PSL}_2(\mathbb{F}_7), \mathfrak{A}_7\},$$

respectively. Here $\mathcal{C}_m$, $\mathcal{D}_m$, $\mathfrak{A}_m$ and $\mathfrak{S}_m$ are the cyclic group, the dihedral group, the alternating group and the symmetric group of degree m with order m, $2m$, $m!/2$ and $m!$, respectively. The group $\mathrm{PSL}_2(\mathbb{F}_7)$ is the projective special linear group of 2×2 matrices over the finite field $\mathbb{F}_7$ with 7 elements.

Proposition 1.5 (Proposition 3.7)**.** *The group G is isomorphic to a group in the family $\mathcal{G}_d$ when $2 \leq d \leq 7$.*

In § 2 we study the construction of an algebraic number field with the six conditions (1) to (6). In § 3 we study the Galois group of the Galois closure extension of a field satisfying the five conditions (2) to (6). In § 4 we study a method for finding p-Eisenstein numbers in a p-Eisenstein field. In § 5 we present some numerical examples of fields satisfying the six conditions (1) to (6) with explicit definition polynomials.

Acknowledgement. The author is grateful to Doctor Yasushi Mizusawa for discussing on Problem 1.2. He is supported by the 21st Century COE Program "Development of Dynamic Mathematics with High Functionality".

§ 2. Construction of a non-Galois Eisenstein field

In this section we study the construction of an algebraic number field satisfying the six conditions (1) to (6). We prepare the following fundamental lemmas on the ramifications. Let F be an algebraic number field of finite degree.

Lemma 2.1 (cf. [**2**])**.** *The extension $F/\mathbb{Q}$ is totally ramified at a prime number l if and only if F is a l-Eisenstein field.*

Let l be a prime number. For a prime ideal $\mathfrak{l}$ of F above l we denote by $e_{F,\mathfrak{l}}$ the ramification index of $\mathfrak{l}$ in $F/\mathbb{Q}$ and by $f_{F,\mathfrak{l}}$ the degree of the residue field $\mathcal{O}_F/\mathfrak{l}$ over $\mathbb{F}_l$. Let us define $e_{F,l}$ to be the least common multiple of the indices $e_{F,\mathfrak{l}}$ and $f_{F,l}$ to be the sum of the degrees $f_{F,\mathfrak{l}}$ where $\mathfrak{l}$ runs through all of the prime ideals $\mathfrak{l}$ of F above l.

Lemma 2.2 (cf. [**2**])**.** *If $e_{F,l}$ is not divisible by l, then l-adic valuation of the discriminant* $\mathrm{disc}(F/\mathbb{Q})$ *is equal to $d - f_{F,l}$.*

Lemmas 2.1 and 2.2 imply

Proposition 2.3. *For an algebraic number field F of degree d less than a prime number p, the discriminant* $\mathrm{disc}(F/\mathbb{Q})$ *is equal to $\pm p^{d-1} \equiv 1 \pmod 4$ if and only if $F/\mathbb{Q}$ is a p-Eisenstein field and is unramified at all prime numbers other than p.*

Let the notation be the same as for Theorem 1.3 in the Introduction. Let $\mathfrak{p}$ be a prime ideal E above p. For subfields F of E we denote by $\mathfrak{p}_F$ the prime ideal $\mathfrak{p} \cap F$ of F below $\mathfrak{p}$, respectively.

Lemma 2.4. *The degree $[K : \mathbb{Q}]$ is equal to d. The extension $K/\mathbb{Q}$ is a p-Eisenstein field and is unramified at all prime numbers except for p.*

Proof. The degree $[K : \mathbb{Q}]$ of K is equal to $[E : k][E : K]^{-1}[k : \mathbb{Q}] = r^2 r^{-1} n = d$. The prime ideal $\mathfrak{p}_L$ of L is totally ramified in the extension $L/\mathbb{Q}$ and so is in L/k. On the other hand, $\mathfrak{p}_M$ is unramified in M/k. Thus the inertia field of $\mathfrak{p}$ in E/k is equal to M. Since $G_3 \cap G_2 = 1$, one sees that $\mathfrak{p}$ is unramified in E/K. This means that $\mathfrak{p}$ is totally ramified in K/k and so is $\mathfrak{p}_K$. Here $\mathfrak{p}_k$ is totally ramified in $k/\mathbb{Q}$. Thus $\mathfrak{p}_K$ is totally ramified in $K/\mathbb{Q}$. Lemma 2.1 implies that K is a p-Eisenstein

field. Since L and M are unramified over $\mathbb{Q}$ at all prime numbers except for p, so is the subfield K of the composite field $E = LM$. □

Proposition 2.3 and Lemma 2.4 imply

Corollary 2.5. *The discriminant* $\mathrm{disc}(K/\mathbb{Q})$ *of* K *is equal to* $\pm p^{d-1} \equiv 1 \pmod 4$.

The field K is Galois over k with $\mathrm{Gal}(K/k) \simeq \mathbb{Z}/r\mathbb{Z}$. Let k_0 be a subfield of k so that K/k_0 is Galois.

Lemma 2.6. *The field* k_0 *has a cyclic extension with degree* r *which is unramified at all prime ideals of* k_0 *and which is contained in* E.

Proof. Let r_0 denote the degree of the extension K/k_0. Since $\mathfrak{p}_K$ is totally and tamely ramified in K/k_0, the Galois group $\mathrm{Gal}(K/k_0)$ is cyclic. This means that $\mathrm{Gal}(L/k_0) \simeq \mathrm{Gal}(K/k_0) \simeq \mathbb{Z}/r_0\mathbb{Z}$. It follows from $G_3 \cap G_1 = 1$ that $E = LK$. Thus $E = LK$ is abelian over k_0. This implies that $\mathrm{Gal}(E/k) \simeq (\mathbb{Z}/r\mathbb{Z})^2$ and $\mathrm{Gal}(k/k_0) \simeq \mathbb{Z}/r_1\mathbb{Z}$ where $r_1 = r_0/r$. Let M_0 be the inertia field of $\mathfrak{p}$ in E/k_0. Since E/k_0 is abelian, the prime ideal $\mathfrak{p}_{k_0}$ of k_0 is unramified in M_0/k_0. Here $\mathfrak{p}_{k_0}$ is a unique prime ideal of k_0 above p. This means that M_0 is an abelian extension of k_0 which is unramified at all prime ideals of k_0. The prime ideal $\mathfrak{p}$ is totally ramified in L/k_0 and is unramified in E/L. Thus it holds that $[M_0 : k_0] = [E : L] = r$. By considering the ramification above p, one has $L \cap M_0 = k_0$. It follows from $[L : k_0][M_0 : k_0] = [E : k_0]$ that $E = LM_0$. Thus it satisfies that $\mathrm{Gal}(M_0/k_0) \simeq \mathrm{Gal}(E/L) \simeq \mathbb{Z}/r\mathbb{Z}$. Hence M_0 is a cyclic extension of k_0 with degree r which is unramified at all prime ideals of k_0. By the construction one has $M_0 \subset E$. □

Proposition 2.7. *The field* K *is a non-Galois extension of* $\mathbb{Q}$ *if* $r \geq 2$.

Proof. When $K/\mathbb{Q}$ is Galois, one may have $k_0 = \mathbb{Q}$. Lemma 2.6 means that $\mathbb{Q}$ has a cyclic extension of degree r which is unramified at all prime numbers. It is well-known due to Minkowski's theorem that $\mathbb{Q}$ has no non-trivial extensions which is unramified at all prime numbers. Thus one has $r = 1$. This shows that $K/\mathbb{Q}$ is non-Galois provided $r \geq 2$. □

Proof of Theorem 1.3. Lemma 2.4, Corollary 2.5 and Proposition 2.7 verify that K satisfies the five conditions (1) to (5) when $r \geq 2$. If d divides $(p-1)/2$, then the fields L and M are totally real and so is the subfield K of the composite field $E = LM$. The discriminant $\mathrm{disc}(K/\mathbb{Q})$ is positive since K is totally real. Let us assume that d is not a divisor of $(p-1)/2$. Then L is totally imaginary. When r is odd, the field k is totally imaginary and so is the extension K. For the case that r is even, k is totally real and E is totally imaginary. By the same argument as that for the prime number p in the proof of Lemma 2.4, one can see that K/k is ramified at all infinite places of k, that is, K is totally imaginary. Thus K satisfies the condition (6). The assumption $d \nmid (p-1)/2$ means that $v_2(d) = v_2(p-1)$ and $(-1)^{d/2} = (-1)^{(p-1)/2}$. Hence we have shown Theorem 1.3. □

§ 3. Galois closure extension of an Eisenstein field

In this section we study the Galois group of the Galois closure extension of a field satisfying the five conditions (2) to (6). Let p be a prime number and d a positive divisor of $p-1$. Let K be a field with the five conditions (2) to (6). Let $\widetilde{K}$ denote the Galois closure extension of K over $\mathbb{Q}$, that is, $\widetilde{K}$ is the minimal extension of K which is Galois over $\mathbb{Q}$. Let $\mathfrak{p}$ be the prime ideal of K above p.

Lemma 3.1. *The extension $\widetilde{K}/K$ is unramified at $\mathfrak{p}$.*

Proof. Let z be a p-Eisenstein number such that $K = \mathbb{Q}(z)$. Let $f(X) = \sum_{i=0}^{d} a_i X^i$ be the minimal polynomial of z over $\mathbb{Q}$. Then it holds that $v_p(a_0) = 1$ and $v_p(a_i) \geq 1$ for $1 \leq i \leq d-1$ where v_p is the p-adic valuation of $\mathbb{Q}$. Let us put $f_0(X) = z^{-d} f(zX) \in K[X]$. Then the minimal splitting field $\mathrm{Spl}_K f_0(X)$ of $f_0(X)$ over K is equal to that of $f(X)$ over $\mathbb{Q}$. Let $b_i \in K$ be numbers such that $f_0(X) = \sum_{i=0}^{d} b_i X^i$. This implies that $b_d = 1$, $v_{\mathfrak{p}}(b_0) = 0$ and $v_{\mathfrak{p}}(b_i) \geq 1$ for $1 \leq i \leq d-1$ where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation of K. Let $\beta \in \overline{\mathbb{Q}}$ be a d-th root of $-b_0$, that is, $\beta^d + b_0 = 0$. Now put $N = K(\zeta_d, \beta)$ where ζ_d is a primitive d-th root of unity in $\overline{\mathbb{Q}}$. The extension N/K is unramified at $\mathfrak{p}$ since $v_{\mathfrak{p}}(b_0) = v_{\mathfrak{p}}(d) = 0$. Let $\mathfrak{P}$ be a prime ideal of N above $\mathfrak{p}$. Hensel's lemma shows that $\mathfrak{P}$ splits completely in the extension $\mathrm{Spl}_N f_0(X)/N$, in particular, $\mathfrak{P}$ is unramified in $\mathrm{Spl}_N f_0(X)/N$. Thus $\mathfrak{p}$ is unramified in $\mathrm{Spl}_N f_0(X)/K$ and so is in the subextension $\mathrm{Spl}_K f_0(X)/K$. Here $\mathrm{Spl}_K f_0(X) = \mathrm{Spl}_{\mathbb{Q}} f(X)$ is a

Galois extension of $\mathbb{Q}$ containing K. This means that $K \subseteq \widetilde{K} \subseteq \mathrm{Spl}_{\mathbb{Q}} f(X)$. Hence $\widetilde{K}/K$ is unramified at $\mathfrak{p}$. □

Proposition 3.2. *The extension $\widetilde{K}/K$ is unramified.*

Proof. Lemma 3.1 implies that $\widetilde{K}/K$ is unramified at $\mathfrak{p}$. Since $K/\mathbb{Q}$ is unramified at all prime numbers other than p, so are the conjugate fields of K over $\mathbb{Q}$. Thus the composite field $\widetilde{K}$ of the fields conjugate to K over $\mathbb{Q}$ is unramified at all prime numbers other than p. It follows from the definition that K satisfies the condition (6) if and only if $\widetilde{K}/K$ is unramified at all infinite places of K. Hence $\widetilde{K}/K$ is unramified. □

Let G denote the Galois group of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. Let $\widetilde{\mathfrak{p}}$ be a prime ideal of $\widetilde{K}$ above $\mathfrak{p}$. Let θ be a generator of K over $\mathbb{Q}$, that is, $K = \mathbb{Q}(\theta)$. The minimal polynomial $f(X)$ of θ over $\mathbb{Q}$ has degree d and satisfies that $\mathrm{Spl}_{\mathbb{Q}} f(X) = \widetilde{K}$. Thus G is isomorphic to a transitive subgroup of the symmetric group $\mathfrak{S}_d$ with degree d. Let $\{\theta_j\}_{j=1}^d$ be the zero set of $f(X)$, that is, $f(X) = \prod_{j=1}^d (X - \theta_j)$. In the following we identify G with the image of an injective homomorphism $G \to \mathfrak{S}_d$, $\sigma \mapsto \tau$ where $\sigma \in G$ and $\tau \in \mathfrak{S}_d$ have relations $\sigma(\theta_j) = \theta_{\tau(j)}$ for all $1 \leq j \leq d$.

Lemma 3.3. *The group G has an element of order d.*

Proof. Since K is p-Eisenstein with degree d, the ramification index of $\mathfrak{p}$ in $K/\mathbb{Q}$ is equal to d. Lemma 3.1 implies that $\widetilde{K}/K$ is unramified at $\mathfrak{p}$. Thus the ramification index of p in $\widetilde{K}/\mathbb{Q}$ is equal to d. Note that the ramification of p in $\widetilde{K}/\mathbb{Q}$ is tame for $p \nmid d$. This means that the inertia group of $\widetilde{\mathfrak{p}}$ in $\widetilde{K}/\mathbb{Q}$ is isomorphic to $\mathcal{C}_d$. This shows that G contains $\mathcal{C}_d$ as a subgroup. □

Let us define a positive integer λ to be the minimal prime divisor of d.

Lemma 3.4. *If G_1 is a subgroup of G with index $[G : G_1] < \lambda$, then $G = G_1$.*

Proof. Let K_1 be the fixed field $\widetilde{K}^{G_1}$ of $\widetilde{K}$ by G_1. Let $\mathfrak{p}_1$ be the prime ideal of K_1 below $\widetilde{\mathfrak{p}}$. If $[G : G_1] < \lambda$, then the ramification index of $\mathfrak{p}_1$ in $K_1/\mathbb{Q}$ is a divisor of d less than λ, which is equal to 1. This means that $\mathfrak{p}_1$ is unramified in $K_1/\mathbb{Q}$. Thus $K_1/\mathbb{Q}$ is an extension of degree $[G : G_1]$ which is unramified at all prime numbers. By Minkowski's theorem, we have $[G : G_1] = 1$. □

Lemma 3.5. *Let G_1 be a proper, normal subgroup of G. Then d and the index $[G : G_1]$ have a common prime divisor. If the group G/G_1 is abelian, then G/G_1 is a subgroup of $\mathcal{C}_d$.*

Proof. Since G_1 is a normal subgroup of G, the fixed field $K_1 = \widetilde{K}^{G_1}$ is a Galois extension whose Galois group $\mathrm{Gal}(K_1/\mathbb{Q})$ is isomorphic to the quotient group G/G_1. The ramification index of p in $K_1/\mathbb{Q}$ divides d and $[G : G_1]$. When d and $[G : G_1]$ are relatively prime to each other, the extension $K_1/\mathbb{Q}$ is unramified at p. Thus Minkowski's theorem implies that $K_1 = \mathbb{Q}$ and $G_1 = G$. If G/G_1 is abelian, then so is $K_1/\mathbb{Q}$. By Minkowski's theorem one can see that $\mathrm{Gal}(K_1/\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{C}_d$. □

Proposition 3.6 (Proposition 1.4)**.** *If d is odd, then G is contained in the alternating group $\mathfrak{A}_d$ with degree d. When d is a prime number , the group G is simple.*

Proof. Let $\mathrm{sgn} : \mathfrak{S}_d \to \{\pm 1\}$ be the signature map so that $\mathrm{sgn}(\sigma) = 1$ (resp. -1) if σ is an even (resp. an odd) permutation. Then the map sgn is a group homomorphism and the kernel G_1 of the restricted map $\mathrm{sgn}|_G$ to G is a normal subgroup of G. When $G \not\subseteq \mathfrak{A}_d$, one has that $\mathrm{sgn}(G) = \{\pm 1\}$ and $[G : G_1] = 2$. Lemmas 3.4 and 3.5 imply that $2 \mid d$. Thus we have $G \subseteq \mathfrak{A}_d$ provided d is odd. We assume that d is equal to a prime number l. Let G_1 be a proper, normal subgroup of G and denote by K_1 the fixed field $\widetilde{K}^{G_1}$ of $\widetilde{K}$ by G_1. Note that K_1 is Galois over $\mathbb{Q}$ since G_1 is normal of G. It follows from Lemma 3.5 that l divides the degree $[K_1 : \mathbb{Q}] = [G : G_1]$ of $K_1/\mathbb{Q}$. Here $K \cap K_1$ is equal to $\mathbb{Q}$ or K since $K/\mathbb{Q}$ is of prime degree l. Now suppose that $K \cap K_1 = \mathbb{Q}$. Galois theory implies that the lift KK_1/K of the Galois extension $K_1/\mathbb{Q}$ by K is a Galois extension whose Galois group is isomorphic to $\mathrm{Gal}(K_1/K \cap K_1) = \mathrm{Gal}(K_1/\mathbb{Q})$. This means that $[KK_1 : K]$ and $[K : \mathbb{Q}]$ are both divisible by l. Note that KK_1 is a subfield of $\widetilde{K}$. Then one has that $[\widetilde{K} : \mathbb{Q}] = [\widetilde{K} : KK_1][KK_1 : K][K : \mathbb{Q}] \equiv 0 \pmod{l^2}$. On the other hand, G satisfies $v_l(\sharp G) \leq v_l(\sharp \mathfrak{S}_l) = 1$ for $G \subseteq \mathfrak{S}_l$. It is a contradiction. Thus we have $K \cap K_1 = K$, which means that $K \subseteq K_1$. This implies that $K_1 = \widetilde{K}$ and $G_1 = 1$ due to the minimality of the Galois closure $\widetilde{K}$. Hence the group G is simple. □

For a positive integer $d \in \mathbb{Z}$ with $d \geq 2$ let $\mathcal{T}_d$ be the family of all the transitive subgroup of $\mathfrak{S}_d$. For integers $d \in \mathbb{Z}$ with $2 \leq d \leq 7$ we define subfamilies $\mathcal{G}_d$ of $\mathcal{T}_d$ as in the Introduction, that is,

$$\mathcal{G}_2 = \{\mathcal{C}_2\}, \quad \mathcal{G}_3 = \{\mathcal{C}_3\}, \quad \mathcal{G}_4 = \{\mathcal{C}_4, \mathfrak{S}_4\}, \quad \mathcal{G}_5 = \{\mathcal{C}_5, \mathfrak{A}_5\},$$
$$\mathcal{G}_6 = \{\mathcal{C}_6, \mathcal{D}_3 \times \mathcal{C}_3, \mathfrak{A}_4 \times \mathcal{C}_2, \mathfrak{S}_5, \mathfrak{S}_6\}, \quad \mathcal{G}_7 = \{\mathcal{C}_7, \mathrm{PSL}_2(\mathbb{F}_7), \mathfrak{A}_7\}.$$

Proposition 3.7 (Proposition 1.5)**.** *We have $G \in \mathcal{G}_d$ for $2 \leq d \leq 7$.*

The families $\mathcal{T}_d$ for $2 \leq d \leq 7$ are well-known.

Lemma 3.8 (cf. [**1**] §6.3)**.** *We have*

$$\begin{aligned}
\mathcal{T}_2 &= \{\mathcal{C}_2\},\\
\mathcal{T}_3 &= \{\mathcal{C}_3, \mathfrak{S}_3\},\\
\mathcal{T}_4 &= \{\mathcal{C}_4, (\mathcal{C}_2)^2, \mathcal{D}_4, \mathfrak{A}_4, \mathfrak{S}_4\},\\
\mathcal{T}_5 &= \{\mathcal{C}_5, \mathcal{D}_5, \mathcal{M}_{20}, \mathfrak{A}_5, \mathfrak{S}_5\},\\
\mathcal{T}_6 &= \{\mathcal{C}_6, \mathfrak{S}_3, \mathcal{D}_6, \mathfrak{A}_4, \mathcal{D}_3 \times \mathcal{C}_3, \mathfrak{A}_4 \times \mathcal{C}_2, \mathfrak{S}_4^-, \mathfrak{S}_4^+, (\mathcal{D}_3)^2,\\
&\qquad (\mathcal{C}_3)^2 \rtimes \mathcal{C}_4, \mathfrak{S}_4 \times \mathcal{C}_2, \mathfrak{A}_5, (\mathcal{C}_3)^2 \rtimes \mathcal{D}_4, \mathfrak{S}_5, \mathfrak{A}_6, \mathfrak{S}_6\},\\
\mathcal{T}_7 &= \{\mathcal{C}_7, \mathcal{D}_7, \mathcal{M}_{21}, \mathcal{M}_{42}, \mathrm{PSL}_2(\mathbb{F}_7), \mathfrak{A}_7, \mathfrak{S}_7\},
\end{aligned}$$

where $\mathcal{M}_{dm}$ is the metagroup $\mathcal{C}_d \rtimes \mathcal{C}_m$. Here $\mathfrak{S}_4^+$ and $\mathfrak{S}_4^-$ are groups isomorphic to $\mathfrak{S}_4$ whose images of the signature map are equal to $\{1\}$ and $\{\pm 1\}$, respectively.

Proof of Proposition 3.7. It is easy to see that the groups $\mathfrak{S}_3$, $\mathcal{D}_5$, $\mathcal{M}_{20}$, $\mathfrak{S}_5$ $\mathcal{D}_7$, $\mathcal{M}_{21}$, $\mathcal{M}_{42}$ and $\mathfrak{S}_7$ are not simple. Thus Proposition 3.6 shows the assertions of the cases $d = 3, 5$ and 7. Let us assume $d = 4$. Here $(\mathcal{C}_2)^2$ has no elements of order 4. Lemma 3.3 means that $G \not\simeq (\mathcal{C}_2)^2$. The groups $\mathcal{D}_4$ (resp. $\mathfrak{A}_4$) have normal subgroups $H \simeq \mathcal{C}_2$ (resp. $(\mathcal{C}_2)^2$) such that $\mathcal{D}_4/H \simeq (\mathcal{C}_2)^2$ (resp. $\mathcal{C}_3$). Lemma 3.5 implies that $G \not\simeq \mathcal{D}_4, \mathfrak{A}_4$. This shows the assertion for $d = 4$. Next consider the case $d = 6$. One can see that the groups $\mathfrak{S}_3$, $\mathfrak{A}_4$, $\mathfrak{S}_4^-$, $\mathfrak{S}_4^+$, $\mathfrak{A}_5$, $\mathfrak{A}_6$ have no elements of order 6, respectively. The groups $\mathcal{D}_6$, $(\mathcal{D}_3)^2$, $\mathfrak{S}_4 \times \mathcal{C}_2$ and $(\mathcal{C}_3)^2 \rtimes \mathcal{D}_4$ have normal subgroups whose quotient groups are isomorphic to $(\mathcal{C}_2)^2$, respectively. The group $(\mathcal{C}_3)^2 \rtimes \mathcal{C}_4$ has a normal subgroup whose quotient group is isomorphic to $\mathcal{C}_4$. Lemmas 3.3 and 3.5 prove the assertion for $d = 6$. □

§ 4. Eisenstein number in an Eisenstein field

In this section we study a method for finding p-Eisenstein numbers in a p-Eisenstein field. Let K be a p-Eisenstein field with degree $d \geq 2$ and $\mathfrak{p}$ the prime ideal of K above p. Let $\mathcal{O}_{K,\mathfrak{p}}$ be the completion at $\mathfrak{p}$ of the ring $\mathcal{O}_K$ of integers in K.

Let $\{x_j\}_{j=1}^d$ be a free basis of $\mathcal{O}_{K,\mathfrak{p}}$ over $\mathbb{Z}_p$, that is, $\mathcal{O}_{K,\mathfrak{p}} = \{\sum_{j=1}^d m_j x_j | m_j \in \mathbb{Z}_p\}$. One may assume $v_{\mathfrak{p}}(x_1) = 0$. Since $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$, there exist rational integers $c_j \in \mathbb{Z}$ such that $x_1 c_j \equiv x_j \pmod{\mathfrak{p}}$ for $2 \leq j \leq d$. Now put $z_j = x_j - x_1 c_j \in \mathcal{O}_K$ for $2 \leq j \leq d$, respectively. Note that $z_j \neq 0$ since the basis $\{x_j\}_{j=1}^d$ is free.

Lemma 4.1. *There exists a p-Eisenstein number z in the finite set $\{z_j | j \in \mathbb{Z}, 2 \leq j \leq d\}$ such that $K = \mathbb{Q}(z)$.*

Proof. It follows from $c_j \in \mathbb{Z}$ that $\{x_1\} \cup \{z_j\}_{j=2}^d$ is also a free basis of $\mathcal{O}_{K,\mathfrak{p}}$ over $\mathbb{Z}_p$. Let π be a number in $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(\pi) = 1$ where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation of K. Then there exist numbers $m_j \in \mathbb{Z}_p$ such that $\pi = m_1 x_1 + \sum_{j=2}^d m_j z_j$. Let us denote $\min\{v_{\mathfrak{p}}(z_j) | j \in \mathbb{Z}, 2 \leq j \leq d\}$ by μ. Then one has $\mu \geq 1$ for $z_j \in \mathfrak{p}$. Now suppose $\mu \geq 2$. If $v_{\mathfrak{p}}(m_1) = 0$, then $v_{\mathfrak{p}}(\pi) = 0$, which is a contradiction. When $v_{\mathfrak{p}}(m_1) \geq 1$, one has $v_{\mathfrak{p}}(\pi) \geq \min\{v_{\mathfrak{p}}(m_1), \mu\} \geq 2$ for $v_{\mathfrak{p}}(m_1) = d v_p(m_1) \geq 2$. It is contrary to the fact that $v_{\mathfrak{p}}(\pi) = 1$. Thus we have $\mu = 1$ and $v_{\mathfrak{p}}(z_j) = 1$ for some integer $j \in \mathbb{Z}$ with $2 \leq j \leq d$. For such a number z_j the valuations $v_{\mathfrak{p}}(z_j^i)$ with $0 \leq i \leq d-1$ have distinct images by the natural map $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$, $m \mapsto m \pmod{d}$. This means that the degree of the minimal polynomial of z_j over $\mathbb{Q}$ is not less than d. Thus we have $K = \mathbb{Q}(z_j)$. Let $f(X) = \sum_{i=0}^d a_i X^i \in \mathbb{Q}[X]$ be the minimal polynomial of z_j over $\mathbb{Q}$. If the set $\{0 \leq i \leq d-1 | v_p(a_i) = 0\}$ is not empty, then $v_{\mathfrak{p}}(f(z_j)) = \min\{0 \leq i \leq d-1 | v_p(a_i) = 0\} < \infty$, which contradicts that $f(z_j) = 0$. Thus it satisfies that $v_p(a_i) \geq 1$ for every $0 \leq i \leq d-1$. Then one has that $v_{\mathfrak{p}}(a_0) = v_{\mathfrak{p}}(z_j^d) = d$, which means $v_p(a_0) = 1$. Hence z_j is a p-Eisenstein number. □

§ 5. Some numerical examples

In this section we present some numerical examples of fields satisfying the six conditions (1) to (6) with explicit definition polynomials. Let us denote by $\mathrm{Spl}_F f(X)$ the minimal splitting field of a polynomial $f(X) \in F[X]$ over a field F.

We first consider the case that $p = 229$ and $(n, r) = (2, 3)$. Here one has $d = nr = 6$. The quadratic field k contained in $\mathbb{Q}(\zeta_p)$ is equal to $\mathrm{Spl}_{\mathbb{Q}} g_0(X)$ where $g_0(X) = X^2 - 229$. The cyclic field L of degree $d = 6$ in $\mathbb{Q}(\zeta_p)$ is $\mathrm{Spl}_k g_1(X)$ for $g_1(X) = X^3 - 4X - 1$ (cf. Cohen [**1**], Komatsu [**6**]). It is calculated that

$\mathrm{Cl}(k) \simeq \mathbb{Z}/3\mathbb{Z}$ where $\mathrm{Cl}(k)$ is the ideal class group of k. This means that there exists an unramified cyclic cubic extension M of k. One can see that M is equal to $\mathrm{Spl}_k g_2(X) = \mathrm{Spl}_{\mathbb{Q}} g_2(X)$ where $g_2(X) = X^3 - 687X - 5038$ (cf. Komatsu [**5**]). Now put $E = LM$. Then E is Galois over k with $\mathrm{Gal}(E/k) \simeq (\mathbb{Z}/3\mathbb{Z})^2$. Let α_i and β_j be numbers in $\overline{\mathbb{Q}}$ such that $g_1(X) = \prod_{i=1}^3 (X - \alpha_i)$ and $g_2(X) = \prod_{j=1}^3 (X - \beta_j)$, respectively. Let σ_1 and σ_2 be elements in $\mathrm{Gal}(E/k)$ so that $\sigma_1 : \alpha_i \mapsto \alpha_i$, $\beta_1 \mapsto \beta_2 \mapsto \beta_3 \mapsto \beta_1$ and $\sigma_2 : \alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1$, $\beta_j \mapsto \beta_j$ for $i, j \in \{1, 2, 3\}$, respectively. Then it holds that $L = E^{G_1}$, $M = E^{G_2}$ and $\mathrm{Gal}(E/k) = \langle \sigma_1, \sigma_2 \rangle$ where $G_i = \langle \sigma_i \rangle$ for $i = 1$ and 2. Let us define $\theta = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 \in E$. Then one has $k(\theta) \subseteq E^{G_3}$ for $G_3 = \langle \sigma_1\sigma_2 \rangle$. Note that $G_3 \cap G_1 = G_3 \cap G_2 = 1$ and $G_3 \simeq \mathbb{Z}/3\mathbb{Z}$. One can see that the minimal polynomial $h(X)$ of θ over $\mathbb{Q}$ is equal to $X^6 - 16488X^4 - 136026X^3 + 67963536X^2 + 1121398344X - 30392443755$. This implies that $[\mathbb{Q}(\theta) : \mathbb{Q}] = 6$ and $\mathbb{Q}(\theta) = k(\theta) = E^{G_3}$, which is denoted by K. Theorem 1.3 shows that K satisfies the six conditions (1) to (6). By $6 = d \mid (p-1)/2 = 114$, the field K is totally real. Unfortunately, the number θ is not p-Eisenstein since the constant term a_0 of $h(X)$ satisfies $v_p(a_0) = 2$. Theorem 1.3 implies that $\mathrm{disc}(K/\mathbb{Q}) = 229^5$. On the other hand, it is calculated that $\mathrm{disc}_X h(X) = 2^{12} \cdot 3^{30} \cdot 229^{13} \cdot 24793^2$. Let us put

$$x_1 = 1, x_2 = \theta, x_3 = \theta^2, x_4 = \theta^3/229, x_5 = \theta^4/229, x_6 = \theta^2(\theta^3/229 - 68)/229.$$

Then $\{x_j\}_{j=1}^6 \subseteq \mathcal{O}_K$ is a free basis of $\mathcal{O}_{K,\mathfrak{p}}$ over $\mathbb{Z}_p$ with $v_{\mathfrak{p}}(x_1) = 0$ where $\mathfrak{p}$ is the prime ideal of K above p. The numbers $c_2 = 0, c_3 = 0, c_4 = 68, c_5 = 0$ and $c_6 = 158$ satisfy that $x_1 c_j \equiv x_j \pmod{\mathfrak{p}}$, respectively. By putting $z_j = x_j - x_1 c_j$ one can see that $v_{\mathfrak{p}}(z_2) = 2$, $v_{\mathfrak{p}}(z_3) = 4$, $v_{\mathfrak{p}}(z_4) = 2$, $v_{\mathfrak{p}}(z_5) = 2$ and $v_{\mathfrak{p}}(z_6) = 1$. The minimal polynomial $f(X)$ of z_6 over $\mathbb{Q}$ is equal to

$$\begin{aligned} f(X) =& X^6 - 96180X^5 - 37394605380X^4 + 1703530969560862X^3 \\ &+ 7272426617168122611 6X^2 + 1478517372952988131 49160X \\ &+ 27821740949946705377847421 \\ =& X^6 - 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 229X^5 \\ &- 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 229 \cdot 401 \cdot 617X^4 \\ &+ 2 \cdot 13 \cdot 229 \cdot 286115379503X^3 \\ &+ 2^2 \cdot 3 \cdot 7 \cdot 229 \cdot 367 \cdot 853 \cdot 1213 \cdot 9956087X^2 \\ &+ 2^3 \cdot 3 \cdot 5 \cdot 229 \cdot 5380339785127322167X \\ &+ 229 \cdot 1519169 \cdot 79972878961273721, \end{aligned}$$

which is a p-Eisenstein polynomial. Thus z_6 is a p-Eisenstein number with $K = \mathbb{Q}(z_6)$. The field $\mathrm{Spl}_{\mathbb{Q}} f(X) = E$ is a Galois $(\mathcal{D}_3 \times \mathcal{C}_3)$-extension of $\mathbb{Q}$ with degree 18. By using a calculator Pari-GP one can find a unit $\varepsilon \in K$ whose minimal polynomial $f_1(X)$ over $\mathbb{Q}$ is equal to

$$f_1(X) = X^6 + 564X^5 + 76206X^4 + 70094X^3 - 21032X^2 + 346X + 1.$$

Then it satisfies that

$$\begin{aligned} f_1(X-94) =& X^6 - 56334X^4 + 4639998X^3 + 506979436X^2 \\ & -75182965726X + 2442021793125 \\ =& X^6 - 2 \cdot 3 \cdot 41 \cdot \mathsf{229} X^4 + 2 \cdot 3 \cdot 11 \cdot \mathsf{229} \cdot 307 X^3 \\ & + 2^2 \cdot \mathsf{229} \cdot 553471 X^2 - 2 \cdot 11 \cdot \mathsf{229} \cdot 14923177 X \\ & + 3 \cdot 5^4 \cdot \mathsf{229} \cdot 5687387. \end{aligned}$$

The prime numbers $p \equiv 1 \pmod{12}$ less than 2000 with $3 \mid h(\mathbb{Q}(\sqrt{p}))$ are $p = 229$, 733, 1129 and 1489 (cf. Komatsu [**5**]). In the same way as above one can calculate

Proposition 5.1. *For $p = 229$, 733, 1129 and 1489, the zeros of polynomials*

$$\begin{aligned} & X^6 - 56334X^4 + 4639998X^3 + 506979436X^2 \\ & \qquad -75182965726X + 2442021793125, \\ & X^6 + 1466X^5 + 517498X^4 - 215438962X^3 - 199612437946X^2 \\ & \qquad -49974959030498X - 4171953628526171, \\ & X^6 - 2258X^5 + 1287060X^4 + 402900585X^3 - 513889910560X^2 \\ & \qquad +66733203945617X + 19658366564838499, \\ & X^6 - 2978X^5 - 3195881178465X^4 + 3940122374968794844X^3 \\ & \quad -204859811582615147624850 5X^2 + 5049066523349806461722651425 34X \\ & \qquad -48608237799042834668269234616457255 \end{aligned}$$

are p-Eisenstein numbers, respectively. Such a p-Eisenstein number generates a non-Galois, totally real and sextic field with discriminant p^5.

Next consider the case that $p = 277$ and $(n, r) = (3, 2)$. Then one has $d = nr = 6$. The cyclic cubic field k contained in $\mathbb{Q}(\zeta_p)$ is equal to $\mathrm{Spl}_{\mathbb{Q}} g_0(X)$ where $g_0(X) = X^3 - 831X - 7202$ (cf. Cohen [**1**], Komatsu [**6**]). The cyclic field L of degree $d = 6$ in $\mathbb{Q}(\zeta_p)$ is $\mathrm{Spl}_k g_1(X)$ for $g_1(X) = X^2 - 277$. It is calculated that $\mathrm{Cl}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. This means that there exists an unramified quadratic extension of k. Let $x \in k$ be a solution of $g_0(X) = 0$ and put $\xi = -(x^2 - 10x - 740)/9$. Then the minimal polynomial of ξ over $\mathbb{Q}$ is equal to $\widetilde{g_0}(X) = X^3 - 62X^2 + 81X - 4$. Let us define $g_2(X) = \widetilde{g_0}(X^2)$. Then $M_1 = \mathrm{Spl}_{\mathbb{Q}} g_2(X)$ is an unramified Galois extension of k with $\mathrm{Gal}(M_1/k) \simeq \mathrm{Cl}(k) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Let β be a solution of $g_2(X) = 0$. Then

$M = k(\beta)$ is an unramified quadratic extension of k. Now put $E = LM$. Then E is Galois over k with $\mathrm{Gal}(E/k) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Let α be a solution of $g_1(X) = 0$. We define $\theta = \alpha\beta \in E$. In the same way as for the case $(p, n, r) = (229, 2, 3)$, it is seen that $K = \mathbb{Q}(\theta)$ satisfies the six conditions (1) to (6). The minimal polynomial $h(X)$ of θ over $\mathbb{Q}$ is equal to

$$h(X) = \widetilde{g_0}(X^2/277)277^3 = X^6 - 17174X^4 + 6215049X^2 - 85015732$$

Here $h(X)$ is not a p-Eisenstein polynomial for $v_{277}(85015732) = 3$. In the same way as for $(p, n, r) = (229, 2, 3)$ one can calculate that $z_6 = \theta(26(\theta^2/277)^2 + 218(\theta^2/277) + 148)/277$ is a p-Eisenstein number with $K = \mathbb{Q}(z_6)$. The minimal polynomial of z_6 over $\mathbb{Q}$ is equal to

$$\begin{aligned} f(X) &= X^6 - 2605040960X^4 + 2681576423424X^2 - 12566269001728 \\ &= X^6 - 2^6 \cdot 5 \cdot 277 \cdot 29389X^4 + 2^{16} \cdot 3^3 \cdot 277 \cdot 5471X^2 - 2^{28} \cdot 13^2 \cdot 277. \end{aligned}$$

One can see that $\mathrm{Spl}_{\mathbb{Q}} f(X) = LM_1$ is a Galois $(\mathfrak{A}_4 \times \mathcal{C}_2)$-extension of $\mathbb{Q}$ with degree 24. By using a calculator Pari-GP one can find a unit $\varepsilon \in K$ whose minimal polynomial $f_1(X)$ over $\mathbb{Q}$ is equal to

$$f_1(X) = X^6 - 83X^5 + 1093X^4 + 9510X^3 - 1093X^2 - 83X - 1.$$

Then it satisfies that

$$\begin{aligned} f_1(X + 60) &= X^6 + 277X^5 + 30193X^4 + 1603830X^3 \\ &\quad +40439507X^2 + 334128757X - 1669299781 \\ &= X^6 + 277X^5 + 109 \cdot 277X^4 + 2 \cdot 3 \cdot 5 \cdot 193 \cdot 277X^3 \\ &\quad +277 \cdot 145991X^2 + 31 \cdot 167 \cdot 233 \cdot 277X - 277 \cdot 1699 \cdot 3547. \end{aligned}$$

Proposition 5.2. *Every zero of the polynomial*

$$X^6 + 277X^5 + 30193X^4 + 1603830X^3 \\ +40439507X^2 + 334128757X - 1669299781$$

is a 277*-Eisenstein number which generates a non-Galois, totally real and* 277*-Eisenstein field of degree* 6 *with discriminant* 277^5.

We obtain the following polynomials by considering the unramified extensions of certain algebraic number fields in a similar way as above.

Proposition 5.3. *For* $p = 2713$, 2777, 2857 *and* 3137, *the polynomials*

$$X^4 - 2713X^2 - 2713X + 5426,$$
$$X^4 - 2777X^2 - 8331X - 5554,$$
$$X^4 - 5714X^2 - 22856X + 48569,$$
$$X^4 - 3137X^2 - 47055X - 156850$$

are p*-Eisenstein polynomials whose minimal splitting fields over* $\mathbb{Q}$ *are Galois* $\mathfrak{S}_4$*-extensions, respectively. Every zero of the above* p*-Eisenstein polynomial is a* p*-Eisenstein number which generates a non-Galois, totally real and quartic field with discriminant* p^3.

Let K be an algebraic number field of finite degree and $\widetilde{K}$ the Galois closure extension of K over $\mathbb{Q}$. Let (d, G) be a pair of an integer d and a group G such that $(d, G) = (5, \mathfrak{A}_5)$, $(6, \mathfrak{S}_5)$, $(6, \mathfrak{S}_6)$, $(7, \mathrm{PSL}_2(\mathbb{F}_7))$ or $(7, \mathfrak{A}_7)$.

Problem 5.4. *Do there exist any algebraic number fields* K *of degree* d *with* $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G$ *which satisfy all of the six conditions* (1) *to* (6) *?*

References

[1] H. Cohen, A course in computational algebraic number theory, Grad. Texts in Math., **138** (1993) Springer-Verlag, Berlin.

[2] A. Frohlich, M.J. Taylor, Algebraic number theory, Cambridge Stud. Adv. Math., **27** (1993) Cambridge Univ. Press, Cambridge.

[3] A. Hanaki, *Association schemes of prime order and their splitting fields* (*Japanese*), Sendai Mini Symposium on Number Theory and Combinatorial Theory 2005 (Tohoku Univ.) on Jan. 30-31, 2006. http://www.math.is.tohoku.ac.jp/~taya/sendaiNC/2005/report/hanaki.pdf

[4] A. Hanaki, K. Uno, *Algebraic structure of association schemes of prime order*, to appear in J. Algebraic Combin.

[5] T. Komatsu, *On unramified cyclic cubic extensions of real quadratic fields*, Japan. J. Math. **27** (2001), no. 2, 353–386.

[6] T. Komatsu, *Cyclic cubic field with explicit Artin symbols*, to appear in Tokyo J. Math.

(Toru KOMATSU) Faculty of Mathematics, Kyushu University, 6-10-1 Hakozaki Higashiku, Fukuoka, 812-8581 Japan

E-mail address: trkomatu@math.kyushu-u.ac.jp

List of MHF Preprint Series, Kyushu University

21st Century COE Program
Development of Dynamic Mathematics with High Functionality

MHF2003-1 Mitsuhiro T. NAKAO, Kouji HASHIMOTO & Yoshitaka WATANABE
A numerical method to verify the invertibility of linear elliptic operators with applications to nonlinear problems

MHF2003-2 Masahisa TABATA & Daisuke TAGAMI
Error estimates of finite element methods for nonstationary thermal convection problems with temperature-dependent coefficients

MHF2003-3 Tomohiro ANDO, Sadanori KONISHI & Seiya IMOTO
Adaptive learning machines for nonlinear classification and Bayesian information criteria

MHF2003-4 Kazuhiro YOKOYAMA
On systems of algebraic equations with parametric exponents

MHF2003-5 Masao ISHIKAWA & Masato WAKAYAMA
Applications of Minor Summation Formulas III, Plücker relations, Lattice paths and Pfaffian identities

MHF2003-6 Atsushi SUZUKI & Masahisa TABATA
Finite element matrices in congruent subdomains and their effective use for large-scale computations

MHF2003-7 Setsuo TANIGUCHI
Stochastic oscillatory integrals - asymptotic and exact expressions for quadratic phase functions -

MHF2003-8 Shoki MIYAMOTO & Atsushi YOSHIKAWA
Computable sequences in the Sobolev spaces

MHF2003-9 Toru FUJII & Takashi YANAGAWA
Wavelet based estimate for non-linear and non-stationary auto-regressive model

MHF2003-10 Atsushi YOSHIKAWA
Maple and wave-front tracking — an experiment

MHF2003-11 Masanobu KANEKO
On the local factor of the zeta function of quadratic orders

MHF2003-12 Hidefumi KAWASAKI
Conjugate-set game for a nonlinear programming problem

MHF2004-1 Koji YONEMOTO & Takashi YANAGAWA
Estimating the Lyapunov exponent from chaotic time series with dynamic noise

MHF2004-2 Rui YAMAGUCHI, Eiko TSUCHIYA & Tomoyuki HIGUCHI
State space modeling approach to decompose daily sales of a restaurant into time-dependent multi-factors

MHF2004-3 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Cubic pencils and Painlevé Hamiltonians

MHF2004-4 Atsushi KAWAGUCHI, Koji YONEMOTO & Takashi YANAGAWA
Estimating the correlation dimension from a chaotic system with dynamic noise

MHF2004-5 Atsushi KAWAGUCHI, Kentarou KITAMURA, Koji YONEMOTO, Takashi YANAGAWA & Kiyofumi YUMOTO
Detection of auroral breakups using the correlation dimension

MHF2004-6 Ryo IKOTA, Masayasu MIMURA & Tatsuyuki NAKAKI
A methodology for numerical simulations to a singular limit

MHF2004-7 Ryo IKOTA & Eiji YANAGIDA
Stability of stationary interfaces of binary-tree type

MHF2004-8 Yuko ARAKI, Sadanori KONISHI & Seiya IMOTO
Functional discriminant analysis for gene expression data via radial basis expansion

MHF2004-9 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Hypergeometric solutions to the q - Painlevé equations

MHF2004-10 Raimundas VIDŪNAS
Expressions for values of the gamma function

MHF2004-11 Raimundas VIDŪNAS
Transformations of Gauss hypergeometric functions

MHF2004-12 Koji NAKAGAWA & Masakazu SUZUKI
Mathematical knowledge browser

MHF2004-13 Ken-ichi MARUNO, Wen-Xiu MA & Masayuki OIKAWA
Generalized Casorati determinant and Positon-Negaton-Type solutions of the Toda lattice equation

MHF2004-14 Nalini JOSHI, Kenji KAJIWARA & Marta MAZZOCCO
Generating function associated with the determinant formula for the solutions of the Painlevé II equation

MHF2004-15 Kouji HASHIMOTO, Ryohei ABE, Mitsuhiro T. NAKAO & Yoshitaka WATANABE
Numerical verification methods of solutions for nonlinear singularly perturbed problem

MHF2004-16 Ken-ichi MARUNO & Gino BIONDINI
Resonance and web structure in discrete soliton systems: the two-dimensional Toda lattice and its fully discrete and ultra-discrete versions

MHF2004-17 Ryuei NISHII & Shinto EGUCHI
Supervised image classification in Markov random field models with Jeffreys divergence

MHF2004-18 Kouji HASHIMOTO, Kenta KOBAYASHI & Mitsuhiro T. NAKAO
Numerical verification methods of solutions for the free boundary problem

MHF2004-19 Hiroki MASUDA
Ergodicity and exponential β-mixing bounds for a strong solution of Lévy-driven stochastic differential equations

MHF2004-20 Setsuo TANIGUCHI
The Brownian sheet and the reflectionless potentials

MHF2004-21 Ryuei NISHII & Shinto EGUCHI
Supervised image classification based on AdaBoost with contextual weak classifiers

MHF2004-22 Hideki KOSAKI
On intersections of domains of unbounded positive operators

MHF2004-23 Masahisa TABATA & Shoichi FUJIMA
Robustness of a characteristic finite element scheme of second order in time increment

MHF2004-24 Ken-ichi MARUNO, Adrian ANKIEWICZ & Nail AKHMEDIEV
Dissipative solitons of the discrete complex cubic-quintic Ginzburg-Landau equation

MHF2004-25 Raimundas VIDŪNAS
Degenerate Gauss hypergeometric functions

MHF2004-26 Ryo IKOTA
The boundedness of propagation speeds of disturbances for reaction-diffusion systems

MHF2004-27 Ryusuke KON
Convex dominates concave: an exclusion principle in discrete-time Kolmogorov systems

MHF2004-28 Ryusuke KON
Multiple attractors in host-parasitoid interactions: coexistence and extinction

MHF2004-29 Kentaro IHARA, Masanobu KANEKO & Don ZAGIER
Derivation and double shuffle relations for multiple zeta values

MHF2004-30 Shuichi INOKUCHI & Yoshihiro MIZOGUCHI
Generalized partitioned quantum cellular automata and quantization of classical CA

MHF2005-1 Hideki KOSAKI
Matrix trace inequalities related to uncertainty principle

MHF2005-2 Masahisa TABATA
Discrepancy between theory and real computation on the stability of some finite element schemes

MHF2005-3 Yuko ARAKI & Sadanori KONISHI
Functional regression modeling via regularized basis expansions and model selection

MHF2005-4 Yuko ARAKI & Sadanori KONISHI
Functional discriminant analysis via regularized basis expansions

MHF2005-5 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Point configurations, Cremona transformations and the elliptic difference Painlevé equations

MHF2005-6 Kenji KAJIWARA, Tetsu MASUDA, Masatoshi NOUMI, Yasuhiro OHTA & Yasuhiko YAMADA
Construction of hypergeometric solutions to the q - Painlevé equations

MHF2005-7 Hiroki MASUDA
Simple estimators for non-linear Markovian trend from sampled data:
I. ergodic cases

MHF2005-8 Hiroki MASUDA & Nakahiro YOSHIDA
Edgeworth expansion for a class of Ornstein-Uhlenbeck-based models

MHF2005-9 Masayuki UCHIDA
Approximate martingale estimating functions under small perturbations of dynamical systems

MHF2005-10 Ryo MATSUZAKI & Masayuki UCHIDA
One-step estimators for diffusion processes with small dispersion parameters from discrete observations

MHF2005-11 Junichi MATSUKUBO, Ryo MATSUZAKI & Masayuki UCHIDA
Estimation for a discretely observed small diffusion process with a linear drift

MHF2005-12 Masayuki UCHIDA & Nakahiro YOSHIDA
AIC for ergodic diffusion processes from discrete observations

MHF2005-13 Hiromichi GOTO & Kenji KAJIWARA
Generating function related to the Okamoto polynomials for the Painlevé IV equation

MHF2005-14 Masato KIMURA & Shin-ichi NAGATA
Precise asymptotic behaviour of the first eigenvalue of Sturm-Liouville problems with large drift

MHF2005-15 Daisuke TAGAMI & Masahisa TABATA
Numerical computations of a melting glass convection in the furnace

MHF2005-16 Raimundas VIDŪNAS
Normalized Leonard pairs and Askey-Wilson relations

MHF2005-17 Raimundas VIDŪNAS
Askey-Wilson relations and Leonard pairs

MHF2005-18 Kenji KAJIWARA & Atsushi MUKAIHIRA
Soliton solutions for the non-autonomous discrete-time Toda lattice equation

MHF2005-19 Yuu HARIYA
Construction of Gibbs measures for 1-dimensional continuum fields

MHF2005-20 Yuu HARIYA
Integration by parts formulae for the Wiener measure restricted to subsets in $\mathbb{R}^d$

MHF2005-21 Yuu HARIYA
A time-change approach to Kotani's extension of Yor's formula

MHF2005-22 Tadahisa FUNAKI, Yuu HARIYA & Mark YOR
Wiener integrals for centered powers of Bessel processes, I

MHF2005-23 Masahisa TABATA & Satoshi KAIZU
Finite element schemes for two-fluids flow problems

MHF2005-24 Ken-ichi MARUNO & Yasuhiro OHTA
Determinant form of dark soliton solutions of the discrete nonlinear Schrödinger equation

MHF2005-25 Alexander V. KITAEV & Raimundas VIDŪNAS
Quadratic transformations of the sixth Painlevé equation

MHF2005-26 Toru FUJII & Sadanori KONISHI
Nonlinear regression modeling via regularized wavelets and smoothing parameter selection

MHF2005-27 Shuichi INOKUCHI, Kazumasa HONDA, Hyen Yeal LEE, Tatsuro SATO, Yoshihiro MIZOGUCHI & Yasuo KAWAHARA
On reversible cellular automata with finite cell array

MHF2005-28 Toru KOMATSU
Cyclic cubic field with explicit Artin symbols

MHF2005-29 Mitsuhiro T. NAKAO, Kouji HASHIMOTO & Kaori NAGATOU
A computational approach to constructive a priori and a posteriori error estimates for finite element approximations of bi-harmonic problems

MHF2005-30 Kaori NAGATOU, Kouji HASHIMOTO & Mitsuhiro T. NAKAO
Numerical verification of stationary solutions for Navier-Stokes problems

MHF2005-31 Hidefumi KAWASAKI
A duality theorem for a three-phase partition problem

MHF2005-32 Hidefumi KAWASAKI
A duality theorem based on triangles separating three convex sets

MHF2005-33 Takeaki FUCHIKAMI & Hidefumi KAWASAKI
An explicit formula of the Shapley value for a cooperative game induced from the conjugate point

MHF2005-34 Hideki MURAKAWA
A regularization of a reaction-diffusion system approximation to the two-phase Stefan problem

MHF2006-1 Masahisa TABATA
Numerical simulation of Rayleigh-Taylor problems by an energy-stable finite element scheme

MHF2006-2 Ken-ichi MARUNO & G R W QUISPEL
Construction of integrals of higher-order mappings

MHF2006-3 Setsuo TANIGUCHI
On the Jacobi field approach to stochastic oscillatory integrals with quadratic phase function

MHF2006-4 Kouji HASHIMOTO, Kaori NAGATOU & Mitsuhiro T. NAKAO
A computational approach to constructive a priori error estimate for finite element approximations of bi-harmonic problems in nonconvex polygonal domains

MHF2006-5 Hidefumi KAWASAKI
A duality theory based on triangular cylinders separating three convex sets in R^n

MHF2006-6 Raimundas VIDŪNAS
Uniform convergence of hypergeometric series

MHF2006-7 Yuji KODAMA & Ken-ichi MARUNO
N-Soliton solutions to the DKP equation and Weyl group actions

MHF2006-8 Toru KOMATSU
Potentially generic polynomial

MHF2006-9 Toru KOMATSU
Generic sextic polynomial related to the subfield problem of a cubic polynomial

MHF2006-10 Shu TEZUKA & Anargyros PAPAGEORGIOU
Exact cubature for a class of functions of maximum effective dimension

MHF2006-11 Shu TEZUKA
On high-discrepancy sequences

MHF2006-12 Raimundas VIDŪNAS
Detecting persistent regimes in the North Atlantic Oscillation time series

MHF2006-13 Toru KOMATSU
Tamely Eisenstein field with prime power discriminant