The Gauß Sum and its Applications to Number Theory

Nadia Khan[1,*], Shin-Ichi Katayama[2], Toru Nakahara[3] and Hiroshi Sekiguchi[4]

[1]National University of Computer & Emerging Sciences Lahore campus, Pakistan

[2]University of Tokushima, Japan

[3]Saga University, Japan

[4]Daiichi Tekkou Co., 5 Chome-3 Tokaimachi, Tokai, Aichi Prefecture 476-0015, Japan

Abstract: The purpose of this article is to determine the monogenity of families of certain biquadratic fields K and cyclic bicubic fields L obtained by composition of the quadratic field of conductor 5 and the simplest cubic fields over the field Q of rational numbers applying cubic Gauß sums. The monogenic biquartic fields K are constructed without using the integral bases. It is found that all the bicubic fields L over the simplest cubic fields are non-monogenic except for the conductors 7 and 9. Each of the proof is obtained by the evaluation of the partial differents $\xi-\xi^{\rho}$ of the different $\partial_{F/Q}(\xi)$ with $F=K$ or L of a candidate number ξ, which will or would generate a power integral basis of the fields F. Here ρ denotes a suitable Galois action of the abelian extensions F/Q and $\partial_{F/Q}(\xi)$ is defined by $\prod_{\rho\in G\setminus\{\iota\}}(\xi-\xi^{\rho})$, where G and ι denote respectively the Galois group of F/Q and the identity embedding of F.

Keywords: Monogenity, Biquadratic field, Simplest cubic field, Cyclic sextic field, Discriminant, Integral basis.

INTRODUCTION

Let F be an algebraic number field over the field Q of rational numbes with the extension degree $n=[F:Q]$. Then the ring Z_F of integers in F has an integral basis $\{\omega_j\}_{1\leqq j\leqq n}$ such that Z_F is the Z-module $Z\cdot\omega_1+\cdots+Z\cdot\omega_n$ of rank n. If there exists a suitable number $\xi\in F$ such that $Z_F=\ Z\cdot 1+\cdots+Z\cdot\xi^{n-1}$, then it is said that Z_F has a power integral basis or F is monogenic. It is known as Dedekind-Hasse's problem to determine whether an algebraic number field is monogebnic or not [7, 5]. Let $Ind_F(\xi)$ denote the index $\sqrt{\frac{d_F(\xi)}{d_F}}$ of an integer ξ in F with the discriminant $d_F(\xi)$ of a number ξ and the field discinimant d_F of the field F. This value coincides with $\sqrt{\frac{\text{The volume of the parallelotope spanned by } \{\xi^j\}_{0\leqq j\leqq n-1}\times 4(\text{quadrants})}{\text{The volume of the parallelotope spanned by } \{\omega_j\}_{1\leqq j\leqq n}\times 4(\text{quadrants})}}$ for $n=2$. Then it is enough for the monogenity of F to find a number ξ in F such that the value $Ind_F(\xi)$ is equal to 1. On the other hand, to show the non-monogenity we must prove that $Ind_F(\xi)>1$ for every number ξ in F.

*Address correspondence to this author at the National University of Computer & Emerging Sciences Lahore Campus, Pakistan;
E-mail: p109958@nu.edu.pk

Mathematics Subject Classification (2010) 11R04, 11R11, 11R16.

Let ζ_n be an nth root of unity and k_n be the nth cyclotomic field $Q(\zeta_n)$ with the extension degree $\phi(n)$, where ϕ is the Euler totient function. Let G be the Galois group of k_n/Q and $\widehat{G}$ the character group of G. For a character $\chi\in\widehat{G}$, the Gauß sum τ_χ attached to χ is defined by the sum

$\sum_{x\in G}\chi(x)\zeta_n^x$.

Then τ_χ belongs to the field $k_m\cdot k_n$ with the degree $m\,|\,\phi(n)$ of χ. We find two phenomena.

Theorem 1.1. Let λ_ℓ be a biquadratic character of conductor ℓ. Let K be a biquadratic field $Q(\tau_{\lambda_m},\tau_{\lambda_n})$, where τ_{λ_ℓ} is the quadratic Gauß sum attached to λ_ℓ. Then

(1) K is non-monogenic, if $m\equiv n\equiv 1(\ mod\ 4)$ and $(m,n)=1$.

(2) There exist infinitely many monogenic biquadratic fields K, if $m\equiv 0(\ mod\ 4)$,

$n\equiv 1(\ mod\ 4)$ and $(m,n)=1$ or $m\equiv n\equiv 0(\ mod\ 4)$ and $(m,n)=4$ or 8.

The proof is obtained without using any integral basis of a field $Q(\tau_{\lambda_m},\tau_{\lambda_n})$. This result is a genaralization of the previous work and gives the cardinality to Corollary 1.3 in [24].

Theorem 1.2. There does not exist any monogenic sextic bicubic fields $Q(\tau_{\lambda_5},\eta_{\psi_n})$ with the quadratic Gauß sum τ_{λ_5} and the cubic Gauß period η_{ψ_n} attched to the quadratic character λ_5 and the cubic one ψ_n with the coprime conductors 5 and n, respectively, where the Gauß period η_{ψ_n} is determined by $((-1)^r+\tau_{\psi_n}+\tau_{\psi_n^2})/3$ with the cubic Gauß sum τ_{ψ_n} and the number r of distinct prime factors of n, when n is square free and the fields $Q(\eta_{\psi_n})$ range over the simplest cubic fields of conductor $n=a^2+3a+9$ except for $n=7$ of $a=-1$ and 9 of $a=0$.

In the case of the prime conductor p of quadratic character λ_{p^*} with prime discriminant $p^*=(-1)^{(p-1)/2}p$ and cubic one ψ_p, the monogenity of the sextic field $Q(\tau_{\lambda_{p^*}},\eta_{\psi_p})$ has been determined by the first and the third authors such that there does not exist any cyclic sextic fields $Q(\tau_{\lambda_{p^*}},\eta_{\psi_p})$ except for the prime power conductors $7,3^2$ and 13 [12].

There are related works on the abelian; pure sextic and octic extensions F/Q [11, 23, 17, 15, 16, 6, 14, 3]; [4, 9, 2, 1, 8].

Proof of Theorem 1.1.

The next lemma is fundamental to simplify the proof.

Lemma 2.1. Assume that $Z_K=Z[\xi]$ for a number $\xi=\alpha+\beta\omega$ with $\alpha,\beta\in Q(\tau_{\lambda_m})$, $\omega\in Q(\tau_{\lambda_n})$ and field discriminants m and n. Then

(1) β is a unit in $Q(\tau_{\lambda_m})$.

(2) β and ω are units in $Q(\tau_{\lambda_m})$ and $Q(\tau_{\lambda_n})$, rspectively, if $\alpha=0$.

Proof of Lemma 2.1. Since $K=Q(\tau_{\lambda_m})\cdot Q(\tau_{\lambda_n})$, there exist $\alpha,\beta\in Q(\tau_{\lambda_m})$ and $\omega\in Q(\tau_{\lambda_n})$ such that $\xi=\alpha+\beta\omega$. By $Ind_K(\xi)=1$, it holds that $d_K=d_{Q(\tau_{\lambda_m})}\cdot d_{Q(\tau_{\lambda_n})}\cdot\ d_{Q(\tau_{\lambda_\ell})}=d_K(\xi)\ =\pm N_K(\partial_K(\xi))$ with $\ell=lcm[m,n]$, where the different $\partial_K(\xi)$ of a number ξ with respect to K/Q is defined by $(\xi-\xi^{\sigma})(\xi-\xi^{\tau})(\xi-\xi^{\sigma\tau})$ [25]. The Galois group $G(K/Q)$ coincides with $<\sigma,\tau>$ with $G(Q(\tau_{\lambda_m})/Q)=<\sigma>$ and $G(Q(\tau_{\lambda_n})/Q)=<\tau>$, where $<\sigma_1,\cdots,\sigma_s>$ with σ_j in G means the subgroup generated by $\{\sigma_j\}_{1\leq j\leq s}$ of a group G. Then it holds that

$\sigma:\sqrt{m}\mapsto-\sqrt{m}$, $\sqrt{n}\mapsto\sqrt{n}$ and $\tau:\sqrt{m}\mapsto\sqrt{m}$, $\sqrt{n}\mapsto-\sqrt{n}$.

(1) Thus we have that $\xi-\xi^{\tau}=\beta(\omega-\omega^{\tau})\cong\partial_{Q(\tau_{\lambda_n})}$. Then $\beta\cong 1$. Here for numbers γ,δ and an ideal $\mathfrak{C}$ in an algebraic number field F, $\gamma\cong\delta$ or $\gamma\cong\mathfrak{C}$ means that both sides are equal to $(\gamma)=(\delta)$ or $(\gamma)=\mathfrak{C}$ as ideals, respectively, where $(\gamma_1,\cdots,\gamma_t)$ with $\gamma_j\in F$ denots the ideal $Z_F\cdot\gamma_1+\cdots+Z_F\cdot\gamma_t$ of F.

(2) Let ∂_M denote the field different of an algebraic number field M. Since it is deduced that $\xi-\xi^{\sigma}=(\beta-\beta^{\sigma})\omega\cong\partial_{Q(\tau_{\lambda_m})}$ and $\xi-\xi^{\tau}=\beta(\omega-\omega^{\tau})\cong\partial_{Q(\tau_{\lambda_n})}$, ω and β are units in K.

Proof of Theorem 1.1. (1) Suppose that $Z_K=Z[\xi]$ with $\xi=\alpha+\beta\omega$, $\alpha,\beta\in Q(\tau_{\lambda_m})$ and $\omega\in Q(\tau_{\lambda_n})$. (i) Assume that $\alpha=0$. Put $\beta=\dfrac{s+t\sqrt{m}}{2}$ and $\omega=\dfrac{u+v\sqrt{n}}{2}$. Then by $\xi-\xi^{\sigma}=t\sqrt{m}\omega\cong\sqrt{m}$, $t=\pm1$ holds. By $\xi-\xi^{\tau}=\beta v\sqrt{n}\omega\cong\sqrt{n}$, $v=\pm1$ holds. Thus it is deduced that $N_{K/Q(\tau_{\lambda_m})}(\xi-\xi^{\sigma\tau})\ =N_{K/Q(\tau_{\lambda_m})}(\dfrac{s+t\sqrt{m}}{2}\dfrac{u+v\sqrt{n}}{2}-\dfrac{s-t\sqrt{m}}{2}\dfrac{u-v\sqrt{n}}{2})\ =\dfrac{1}{4}(-(sv)^2n+(tu)^2m)\ =\dfrac{1}{4}(-(\pm4-m)n+(\pm4-n)m)\ \equiv\pm n\pm m\equiv 0(\ mod\ 2)$, which is a contradiction to $\xi-\xi^{\sigma\tau}\cong1$. (ii) Assume that $\alpha\neq0$. Without loss of generality we may put $\xi=\alpha+\omega$ as $\beta^{-1}\xi=\beta^{-1}\alpha+\omega$. Then we have $\xi-\xi^{\sigma\tau}=\alpha+\omega-(\alpha^{\sigma}+\omega)=\pm\sqrt{m}\pm\sqrt{n}$. Thus $N_{K/Q(\tau_{\lambda_m})}(\xi-\xi^{\sigma\tau})=m-n\equiv0(\ mod\ 4)$, which contradicts to $\xi-\xi^{\sigma\tau}\cong1$. Therefore K is non monogenic.

(2) Let $m=4(4t-1)$ and $n=4(4t+3)$ with a square free number $(4t-1)(4t+3)$. Then the biquadratic fields $K=Q(\tau_{\lambda_m},\tau_{\lambda_n})$ coincides with $Q(\alpha,\beta)$ with $\alpha=\sqrt{m}$ and $\beta=\sqrt{n}$. Thus by the Hasse's Conductor-Discriminant Theorem, the field discriminant d_K is equal to $m\cdot n\cdot mn/4^2=2^4\cdot(4t-1)^2\cdot(4t+3)^2$ [25]. Choose a number $\dfrac{\sqrt{4t-1}+\sqrt{4t+3}}{2}\ =\dfrac{\alpha+\beta}{4}$ as ξ. By

$T_{K/Q(\tau_{\lambda_n})}(\xi)=\beta/2$ and $N_{K/Q(\tau_{\lambda_n})}(\xi)=(-\alpha^2+\beta^2)/4=1$, ξ belongs to the ring Z_K because of $K\cap\tilde{Z}_{Q(\tau_{\lambda_n})}=Z_K$, where $\tilde{Z}_F$ means the integral closure of the ring Z_F of algebraic integers in a field F, and for a relative field extension M/F of finite degree of algebraic number fields M and F, $T_{M/F}(\xi)$ and $N_{M/F}(\xi)$ of a number ξ in M denote the relative norm and the relative trace, respectively. By the definition, it follows that $d_{K/Q}(\xi)=(-1)^{4(4-1)/2}N_K(\partial_K(\xi))$ $=N_{K/Q}(\alpha/2\cdot\beta/2\cdot(\alpha+\beta)/4)=d_K$. Thus we obtain $Z_K=Z[1,\xi,\xi^2,\xi^3]$.

On the cardinality of the monogenic fields K the following lemma is available.

Lemma 2.2. There exist infinitely many square-free numbers $16t^2-8t-3$ for $t\in Z$.

Proof of Lemma 2.2 See [18], [21] or use the slightly modified Lemma 8.5 in 1^{st} ed. of [20] with the value of $\zeta(2)$ and prime number theorem [19]. Moreover on the density of

$\#\{D=16t^2-8t-3=(4t-1)^2-4; D:$ squre-free, $D\le x\}$ we have $C\sqrt{x}+O(\sqrt[3]{x}\log x)$, where $C=\frac{1}{4}\prod_{p:odd\ primes}(1-(2/p^2))$ and hence $C>\frac{1}{4}\frac{1}{1-\frac{2}{9}}\frac{2\sqrt{2}}{2\sqrt{2}-1}\quad\frac{3\sqrt{3}}{3\sqrt{3}-1}\frac{1}{\zeta(\frac{3}{2})}>0$ holds by $1-\frac{2}{p^2}>1-\frac{\sqrt{p}}{p^2}$ for any prime number $p\geqq 5$ [10, 13].

Proof of Theorem 1.2.

Let k be a real quadratic field $Q(\tau_{\lambda_5})$ and K the simplest cubic fields which is defined by the cubic equation; $x^3=ax^2+(a+3)x+1$ with $d_K=(a^2+3a+9)^2=d_K(\eta)$ for the field discriminant d_K and the discriminant $d_K(\eta)$ of a solution η of the equation $x^3-ax^2-(a+3)x-1=0$ derived by D. Shanks [22]. The composite field $k\cdot K$ is denoted by L. Then the field L makes a sextic bicubic extension field over the field Q. Assume that $Z_L=Z[\xi]$ for an integer ξ in L. Let σ and τ be generators of the Galois groups $G(K/Q)$ and $G(k/Q)$, respectively. Then we consider the following identity among the partial differents of a number ξ in L;

$$(\xi-\xi^{\sigma})(\xi-\xi^{\sigma})^{\tau}-(\xi-\xi^{\tau})(\xi-\xi^{\tau})^{\sigma}$$
$$-(\xi-\xi^{\sigma\tau})(\xi-\xi^{\sigma\tau})^{\tau}=0.\ (*)$$

Since these three products of the differents are invariant by the action τ, they belong to the the cubic field K. By the assumption of $Ind_L(\xi)=1$, it is deduced that $\partial_L(\xi)=\partial_L=\partial_{L/K}\partial_K=\partial_k\partial_K$ by $\gcd(\partial_K,\partial_k)=1$. Here $\partial_M(\xi)$ and $\partial_{M/L}$ denote the different of a number ξ and the relative field different with respect to L/K, respectively. For an ideal $\mathfrak{C}$ and a number γ of a field M, $\mathfrak{C}=\gamma$ means that both ideals $\mathfrak{C}$ and (γ) are equal to each other in M. On the above identity, we explain the meaning for the case of a prime conductor p of K. By $\partial_L(\xi)=(\xi-\xi^{\sigma})(\xi-\xi^{\sigma^2})$ $(\xi-\xi^{\tau})(\xi-\xi^{\sigma\tau})$ $(\xi-\xi^{\sigma^2\tau})=\partial_L$ it holds that $(\xi-\xi^{\tau})=(\tau_{\lambda_5})$, $(\xi-\xi^{\sigma})=\mathfrak{P}$ and $(\xi-\xi^{\sigma\tau})=(1)$ for the ramified prime ideals $(\tau_{\lambda_5})=(\sqrt{5})$ in k and $\mathfrak{P}$ in K with $(\tau_{\lambda_5})^2=(5)$ and $\mathfrak{P}^3=(p)$. Thus on the difference of the two products in $(*)$ we obtain $N_K((\xi-\xi^{\sigma})(\xi-\xi^{\sigma})^{\tau}-(\xi-\xi^{\tau})(\xi-\xi^{\tau})^{\sigma})$ $=N_K((\xi-\xi^{\sigma\tau})(\xi-\xi^{\sigma\tau})^{\tau})=\pm 1$, and hence $N_K((\xi-\xi^{\tau})(\xi-\xi^{\tau})^{\sigma})=((\sqrt{5})(-\sqrt{5}))^3 \equiv \pm 1(\ mod\ p)$, namely $5^3+1=2\cdot 3^2\cdot 7\equiv 0$ or $5^3-1=2^2\cdot 31\equiv 0(\ mod\ p)$ holds. Since p is a conductor a^2+3a+9 of a simplest cubic field, we obtain the simplest cubic fields K, which should coincide with the maximal real subfield k_7^+ for $a=-1$ of 7th cyclotomic k_7 or k_9^+ for $a=0$ of 9th cyclotomic k_9. Since a sextic field L is a relative cubic extension over the quadratic subfield k, a candidate element ξ of $Z_L=Z[\xi]$ is represented by $\alpha+\beta\omega$ with an integer α, a unit $\beta\in K$ and a unit $\omega=\frac{1+\sqrt{5}}{2}$. In fact, for the case of k_7^+ we can choose $\eta\omega$ as ξ with the Gauß period η attached to a cubic character ψ_7 and for the case of k_9^+ we can find $\eta+\omega$ as ξ with the period η attached to a cubic character ψ_9. For an integral basis $\{\xi_j\}_{1\leqq j\leqq 6}$ of L, we have $\{\eta^i\omega^j\}_{0\leqq i\leqq 2,0\leqq j\leqq 1}$. The sextic field L is generated by $\xi=\eta\omega$, which satisfies $(\xi/\omega)^3+(\xi/\omega)^2-2(\xi/\omega)-1=0$, namely by $\xi^3-2\xi-1\ =(-\xi^2+2\xi+2)\omega$ it holds that $\left(\frac{\xi^3-2\xi-1}{-\xi^2+2\xi+2}\right)^2$ $-\frac{\xi^3-2\xi-1}{-\xi^2+2\xi+2}-1=0$. First we examine the fact for the sextic field L by PARI/GP, which is written in Section 4. Next since the fields K and k are linearly disjoint, that is $K\cap k=Q$ by $\gcd(d_K,d_k)=1$, the ring Z_L of the composite field L coincides with $Z_K \cdot Z_k = Z[1,\eta,\eta^2]\cdot Z[1,\omega] = Z[1,\eta,\eta^2,\omega,\eta\omega,\eta^2\omega]$. Thus for $\xi=\eta\omega$ the representation matrix A of $\{1,\xi,\xi^2,\xi^3,\xi^4,\xi^5\}$ with respect to $\{1,\eta,\eta^2,\omega,\eta\omega,\eta^2\omega\}$ is equal to

$$({}^t(1,\cdot\cdot1,-2,9),{}^t(\cdot\cdot\cdot2,-2,15),{}^t(\cdot\cdot1,-1,6,12),{}^t(\cdot\cdot\cdot2,-3,15),{}^t(\cdot1,\cdot4,-3,-25),{}^t(\cdot\cdot1,-2,9,-20)),$$

which is equivalent to

$$({}^t(1,\cdot,\cdot,\cdot,\cdot,\cdot),{}^t(\cdot,\cdot,\cdot,2,-2,15),{}^t(\cdot,\cdot,1,\cdot,\cdot,\cdot),{}^t(\cdot,\cdot,\cdot,2,-3,15),{}^t(\cdot,1,\cdot,\cdot,\cdot,\cdot),{}^t(\cdot,\cdot,1,-1,3,-8)),$$

and hence whose determinant is equal to -1, namely the matrix A belongs to $SL_6(Z)$, where $\cdot$ means 0 and ${}^tM$ for a matrix M denotes the transposed one. Thus the sectic field $L=k\cdot k_7^+$ is actually monogenic.

In the case of $L=k\cdot k_9^+$, the choice $\xi=\eta\omega$ would be failed, where the Gauß period η is a root of $g(y)=y^3-3y+1$. Then we select $\eta+\omega$ as a candidate ξ of a power integral basis; $Z[\xi]=Z_L$. Since the simplest cubic field is monogenic, $N_K((\xi-\xi^\sigma)(\xi-\xi^{\sigma^2})) = N_K((\eta-\eta^\sigma)(\eta-\eta^{\sigma^2}))=p^2$ holds. Thus it follows that $N_{L/K}(N_K((\eta-\eta^\sigma)(\eta-\eta^{\sigma^2})))=p^4$ and $N_{L/k}(N_k(\xi-\xi^\tau)) = N_{L/k}(N_k(\omega-\omega^\tau)) = 5^3$. On the other hand, by $\partial_L=\partial_K\partial_k$ it is deduced that $d_L=N_L(\partial_K)\ N_L(\partial_k) = d_K^{[L:K]}\cdot d_k^{[L:k]}=(3^4)^2\cdot 5^3=3^8\cdot 5^3=820125$. Here for an ideal $\mathfrak{P}$ in a field M, $N_M(\mathfrak{P})$ means the ideal norm of $\mathfrak{P}$ with respect to M/Q. Then we must confirm that the partial factor $\xi-\xi^{\sigma\tau}$ and hence $\xi-\xi^{\sigma^2\tau} = -(\xi-\xi^{\sigma\tau})^{\sigma^2\tau}$ are not obstacle factors, namely they are units in L. We take the relative norm $N_{L/k}(\xi-\xi^{\sigma\tau})=N_{L/k}(\eta_0-\eta_1+\tau_{\lambda 5}) = (\eta_0-\eta_1+\sqrt{5})(\eta_1-\eta_2+\sqrt{5})(\eta_2-\eta_0+\sqrt{5}) = (\eta_0-\eta_1)(\eta_1-\eta_2)(\eta_2-\eta_0) +\{(\eta_0-\eta_1)(\eta_1-\eta_2)+(\eta_1-\eta_2)(\eta_2-\eta_0)+(\eta_2-\eta_0)(\eta_0-\eta_1)\}\cdot\sqrt{5} +\{(\eta_0-\eta_1)+(\eta_1-\eta_2)+(\eta_2-\eta_0)\}\cdot 5 \ +5\sqrt{5}$. On the first product, we obtain $-C+D$ with $C=\eta_0\eta_2^2+\eta_1\eta_0^2+\eta_2\eta_1^2$ and $D=\eta_0^2\eta_2+\eta_1^2\eta_0+\eta_2^2\eta_1$. By $(\eta_0\eta_1+\eta_1\eta_2+\eta_2\eta_0)(\eta_2+\eta_0+\eta_1)=C+D+3N_K(\eta_0)$. it follows that $C+D=-3N_K(\eta_0)=3$. We obtain $C\cdot D=B_3+3\cdot N_K(\eta_0)^2+S_3N_K(\eta_0)$. Here we use the relations

$B_2B_1=B_3+(D+C)N_K(\eta_0)$ with $B_j=(\eta_0\eta_1)^j+(\eta_1\eta_2)^j+(\eta_2\eta_0)^j$, $j=1,2,3$ and $S_3=\eta_0^3+\eta_1^3+\eta_2^3$. Then we have $B_3=-24$ and $S_3=-3$, and hence $C\cdot D=-18$. Thus the set $\{C,D\}$ of values is equal to $\{-6,3\}$. Then it deduces for the derivative $g'(y)$ of $g(y)$ that $N_{L/K}(\xi-\xi^{\sigma\tau}) = -C+D+\{-g'(\eta_1)-g'(\eta_2)-g'(\eta_0)\}\sqrt{5} +0\cdot 5+5\sqrt{5} = \pm 9-4\sqrt{5}$, and hence $N_k(N_{L/k}(\xi-\xi^{\sigma\tau}))=81-16\cdot 5=1$.

3. EXPERIMENTS AND FUTURE WORKS

To find new phenomena on Number Theory, experiments by PARI/GP are sometimes indispensable. Let L be the cyclic sextic field $Q(\eta,\omega)$ over the simplest cubic field with a root η of the cubic polynomial $x^3=ax^2+(a+3)x+1|_{a=-1}$ and a unit $\omega=\dfrac{1+\sqrt{5}}{2}$ in the real quadratic field with prime discriminant 5. Select a number $\eta+\omega$ as a candidate of integral power basis; $Z_L=Z[\xi]=Z[1,\xi,\cdots,\xi^5]$. PARI/GP gives an affirmative answer as follows.

\\Then PARI/GP gives a power integral basis gp> nfbasis((x^3-2*x-1)^2-(x^3-2*x-1)*(-x^2+2*x+2)-(-x^2+2*x+2)^2) \\the field discriminant d_{L} of the sectic field L gp> nfdisc((x^3-2*x-1)^2-(x^3-2*x-1)*(-x^2+2*x+2)-(-x^2+2*x+2)^2) \\and the prime number decomposition of d_{L} gp> factor(300125) \\namely d_{L}=5^3\cdot 7^4=d_{k}^{[L:k]}\cdot d_{K}^{[L:K]} with d_{k}=5 and d_{K}=7^2.

Since the fields $Q(\tau_{\lambda_5})=Q(\sqrt{5})$ and the simplest cubic field $Q(\eta)$ with $\eta^3=-\eta^2+2\eta+1$ are linearly disjoint, that is, $(\partial_{Q(\tau_{\lambda 5})},\partial_{Q(\eta)})\cong 1$, the set $\{\eta^i\omega^j\}_{0\leqq i\leqq 2,0\leqq j\leqq 1}$ makes an integral basis of L. Let A be the representation matrix of $\{\xi^j\}_{0\leqq j\leqq 5}$ with respect to $\{\eta^i\omega^j\}_{0\leqq i\leqq 2,0\leqq j\leqq 1}$, then it turns out that A belongs to $SL_6(Z)$ in Section 3. Then for $\xi=\eta+\omega$ it is deduced that $Z[\xi]=Z_L$, namely the experiment is correct.

FUTURE WORKS

•$_1$ Generalize Thorem 1.2 for the cyclic sextic fields $L=K\cdot k$ in which any simplest cubic field K and any real or imaginary quadratic field k with $(\partial_K,\partial_k)\cong 1$.

•$_2$ Let p and ζ_p be a prime number and a pth root of unity, respectively and F_p the finite field of p element. Let τ_χ be the Gauß sum $\sum_{x\in F_p}\chi(x)\zeta_n^x$ attached to the non-trivial character χ belonging to the character group $\widehat{F_p^\times}$ with the multiplicative group $F_p^\times = F_p \setminus \{0\}$. Let $J(\chi,\lambda) = \sum_{x,y\in F_p, x+y=1} \chi(x)\lambda(y)$ be the Jacobi sum attached to the non-trivial characters χ and λ. Then the relation

$$J(\chi,\lambda) = \frac{\tau_\chi \tau_\lambda}{\tau_{\chi\lambda}}$$

of Gauß sum and Jacob sum is deduced [12]. Let $\Gamma(x), B(x,y)$ be the Gamma function

$\int_0^\infty e^{-t} t^{x-1} dt \ \ (\Re(x) > 0)$ and Beta function $\int_0^1 t^{x-1}(1-t)^{y-1} dt$ $\Re(x), \Re(y) > 0$, respectively. Then the next reration is well known;

$$B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

Thus find a suitable interpretation between Jacobi sum and Beta function.

ACKNOWLEDGEMENTS

The authors thank to the referee for his/her kind notices to Lemma 2.2 with the references [18] and [21].

REFERENCES

[1] Ahmad S, Nakahara T, Hameed A. On certain pure sextic fields related to a problem of Hasse. International Journal of Algebra and Computation 2016; 26-3: 577-563.

[2] Ahmad S, Nakahara T, Husnine SM. Power integral bases for certain pure sextic fields. International Journal of Number Theory (Singapore) 2014; 10(8): 2257-2265. https://doi.org/10.1142/S1793042114500778

[3] Akizuki S, Ota K. On power bases for ring of integers of relative Galois extensions. Bull London Math Soc 2013; 45: 447-452. https://doi.org/10.1112/blms/bds112

[4] Dedekind R. Über die Zusammenhang zwischen der Theorie der Ideals und der Theorie der höhren Kongruenzen. Abh Akad Wiss Göttingen Math-Phys Kl 1878; 23: 1-23.

[5] Gaál I. Diophantine equations and power integral bases, new computational methods, Birkhäuser Boston, Inc., Boston, 2002. https://doi.org/10.1007/978-1-4612-0085-7

[6] Gras M-N, Tanoé F. Corps biquadratiques monogènes. Manuscripta Math 1995; 86: 63-77. https://doi.org/10.1007/BF02567978

[7] Győry K. Discriminant form and index form equations, Algebraic Number Theory and Diophantine Analysis (F. Halter-Koch and R. F. Tichy. Eds.), Walter de Gruyter, Berlin-New York, 2000; 191-214.

[8] Hameed A, Nakahara T. Integral basis and relative monogenity of pure octic fields. Bull Math Soc Sci Math Roumani 2015; 58-4: 419-433.

[9] Hameed A, Nakahara T, Husnine S, Ahmad S. On existing of canonical number system in certain class of pure algebraic number fields Journal of Prime Research in Mathematics 2011; 7: 19-24.

[10] Katayama S-I. On the Class Numbers of Real Quadratic Fields of Richaud-Degest Type. J Math Tokushima Univ 1997; 31: 1-6.

[11] Khan N, Nakahara T, Katayama S-I, Uehara T. Monogenity of totally real algebraic extension fields over a cyclotomic field. Journal of Number Theory 2016; 158: 348-355. https://doi.org/10.1016/j.jnt.2015.06.018

[12] Khan N, Nakahara T. On the cyclic sextic fields of prime conductor related to a problem of Hasse. To be submitted.

[13] Montgomery L, Weinberger P. Real Quadratic Fields with Large Class Number. Math Ann 1977; 225: 173-176. https://doi.org/10.1007/BF01351721

[14] Motoda Y. Notes on quartic fields. Rep Fac Sci Engrg Saga U Math 2003; 32-1: 1-19. Appendix and Crrigenda to "Notes on Quartic Fields," ibid, 37-1 (2008) 1-8.

[15] Motoda Y, Nakahara T. Power integral basis in algebraic number fields whose galois groups are 2-elementry abelian. Arch Math (Basel) 2004; 83: 309-316. https://doi.org/10.1007/s00013-004-1077-0

[16] Motoda Y, Nakahara T, Shah SIA. On a problem of Hasse for certain imaginary abelian fields. J Number Theory 2002; 96: 326-334. https://doi.org/10.1006/jnth.2002.2805

[17] Motoda Y, Nakahara T, Shah SIA, Uehara T. On a problem of Hasse, RIMS kokyuroku Bessatsu. Kyoto Univ B 2009; 12: 209-221.

[18] Nagell T. Zur Arithmetik der Polynome. Abh Math Sem Hamburg 1922; 1: 180-194. https://doi.org/10.1007/BF02940590

[19] Nakahara T. On cyclic biquadratic fields related to a problem of Hasse. Mh Math 1982; 94: 125-132. https://doi.org/10.1007/BF01301930

[20] Narkiewicz W. Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, 1st ed. 1974, 3rd ed. Berlin-Heidelberg-New York; PWM-Polish Scientific Publishers, Warszawa 2007.

[21] Ricci G. Ricerche arithmetiche sur polinome. Rend Circ Mat Palermo 1933; 57: 433-475. https://doi.org/10.1007/BF03017586

[22] Shanks D. The simplest cubic fields. Mathematics of Computation 1974; 28-128: 1137-1152.

[23] Sultan M, Nakahara T. On certain octic biquartic fields related to a problem of Hasse. Monatshefte für Mathmatik 2014; 174(4): 153-162.

[24] Sultan M, Nakahara T. Monogenity of biquadratic fields related to Dedekind-Hasse's problem. Punjab University Journal of Mathematics 2015; 47(2): 77-82.

[25] Washington LC. Introduction to cyclotomic fields, Graduate texts in mathematics, 2nd ed., Springer-Verlag, New York-Heidelberg-Berlin 1995; 83.

Received on 07-07-2017 Accepted on 12-12-2017 Published on 22-06-2018

https://doi.org/10.6000/1927-5129.2018.14.35