数理解析研究所講究録
第 456 巻 1982 年 152-157

On a problem of Hasse

By

Toru Nakahara

1. Problems

In [8] we considered a problem of Hasse, and especially when the field K is a cyclic biquadratic extension over the rationals Q, we found some examples in each of which integer ring $\mathcal{O}_K$ has a power basis and a characterization for $\mathcal{O}_K$ without any power basis. Recently concerning the former, M. -N. Gras and T. Uehara gave independently a necessary and sufficient condition with five variables for the ring $\mathcal{O}_K$ having a power basis [4], [12].

Problem 1(M. -N. Gras[4]). Do there exist infinitely many cyclic biquadratic fields K over Q whose $\mathcal{O}_K$ have a power basis?

This problem concerns the following Propositions 2, 3.

Problem 2(M. -N. Gras[4]). Do or don't there exist infinitely many cyclic biquadratic fields K over Q which contain the subfield $Q(\sqrt{5})$ and whose $\mathcal{O}_K$ have a power basis?

This concerns itself with Proposition 1.

The next problem occurs with respect to [1], [2], [3], [4], [6], [8], [9], [10], [11] and [12].

Problem 3. Find the parallel phenomena with the Theorems 1, 2, 3 and Propositions 1,2 in a cyclic field with degree six(resp. twelve) over Q.

Problem 4. For $m = 3$(resp. 4) let n be a square-free natural number with $\varphi(n) \equiv 0 \bmod m$. Let K denote a cyclic field with degree $\varphi(n)/m$ over Q. Then characterize such an n-th cyclotomic field k_n whose subfield K contains the ring $\mathcal{O}_K$ with a power basis, where φ means the Euler's function.

In the case of $m = 2$, i. e. when K is the maximal real subfield of k_n, there exist the works of H. Weber [13] for a prime power n and of J. J. Liang [Crellesches J., 286/287(1976),223-226] for a rational integer $n > 1$.

2. Results

Until now we obtained the following [10].

Theorem 1. There exist infinitely many such cyclic biquadratic fields K over Q that the unessential factor m(K) is equal to 4, and that neither $\{1, \alpha, \alpha^2, \beta\}$ nor $\{1, \alpha, \beta, \alpha^3\}$ for any numbers α, β in K makes an integral basis of K.

Example. γ : $X^4 - X^3 - 24X^2 + 4X + 16 = 0$, $K = Q(\gamma) \subset k_{65}$.

Theorem 2. There exist infinitely many such cyclic biquadratic fields K over Q that the unessential factor m(K) is equal to 2 (resp. 3) and that $\{1, \alpha, \beta, \alpha^3\}$ for any numbers α, β in K does not make an integral basis of K.

Example.

γ : $X^4 - X^3 - 24X^2 + 69X - 49 = 0$, $K = Q(\gamma) \subset k_{65}$, $m(K) = 2$.

γ : $X^4 + X^3 + 2X^2 + 4X + 3 = 0$, $K = Q(\gamma) \subset k_{13}$, $m(K) = 3$.

Theorem 3. There exist infinitely many cyclic biquadratic fields K which have the index 1, and still whose rings $\mathcal{O}_K$ have not a power basis.

Example.

η : $X^4 + X^3 + 4X^2 + 20X + 23 = 0$, $K = Q(\eta) \subset k_{29}$, $m(K) = 1$.

Proposition 1. There exists none of such the biquadratic subfield K of a prime cyclotomic field k_p that the ring $\mathcal{O}_K$ has a power basis up to k_5.

Now, for $\ell = m^2 + 4$, $m = (2z + 1)^2 \pm 2$, let $n = \ell m$ be square-free. We put $\chi = \chi_\ell \psi_m$ for a biquadratic character χ_ℓ with conductor ℓ and a quadratic ψ_m with conductor m. The Gauss'period η of $\varphi(n)/4$ terms determined by χ generates a cyclic biquadratic field K over Q. Let Indα be the group index $(\mathcal{O}_K : Z[\alpha])$ for an integer α in K, herein Z denotes the ring of rational integers. We take a number $\xi = (z + 1)\eta + z\,\sigma^2(\eta)$. Then we obtain

$$\mathrm{Ind}\,\xi = \left|(1/\sqrt{\ell^3 m^2})\sqrt{\ell}\, m(\sqrt{\ell}\varepsilon_\ell)\sigma(\sqrt{\ell}\varepsilon_\ell)\right|,$$

where σ and ε_ℓ denote a generator of the Galois group of K/Q with $\chi(\sigma) = i$, $i = \sqrt{-1}$ and a fundamental unit of $Q(\sqrt{\ell})$ respectively. Therefore we have $\mathcal{O}_K = Z[\xi]$.

Proposition 2. There exist cyclic biquadratic fields K whose $\mathcal{O}_K$ have a power basis.

Example. η : $X^4 - X^3 - 11X^2 - 9X + 3 = 0$, $K = Q(\eta) \subset k_{39}$.

Remark. As is well known, the even and the odd biquadratic character with conductor 16 are given by the biquadratic residue symbol[5]

$$\chi_0^{(\nu)}(x) = \left(\frac{-1}{x}\right)_4^{\nu}\left(\frac{1-i}{x}\right)_4 = (-1)^{\nu(x-1)/2}\ i^{(x^2-1)/8}\ , \ (\nu = 0,\ 1).$$

In the case of a character $\chi = \chi_0^{(\nu)}\chi_\ell\psi_m$ with conductor $n = 16\ell m$, $2\nmid m$, we get $\chi((n/2)+1) = -1$. Thus for the Gauss'period $\eta = \sum_{x\in H}\zeta_n^x$ we obtain $\sigma^2(\eta) = \sum_{x\in H}\zeta_n^{((n/2)+1)x} = -\sum_{x\in H}\zeta_n^x = -\eta$, where H and ζ_n denote the kernel of χ and $\exp(2\pi i/n)$ respectively. Therefore contrary to the case of odd conductor, $\{1, \eta, \sigma(\eta), \sigma^2(\eta)\}$ can not make an integral basis of K. We have also the same result in the case of $\chi = \chi_\ell\psi_m$ with conductor $n = \ell m$, $2|m$. This coincides with a special case in a work of Leopoldt[7]. By Hasse [Math. Abhandlungen Bd. 3(1975), 289-379] $\{1, \eta, \sigma(\eta), \sqrt{2\ell}\}$ makes an integral basis of K in the former case and $\{1, \eta, \sigma(\eta), (1+\sqrt{\ell})/2\}$ in the latter. Thus we can calculate the Indα for any integer α in K. Noticing the above, Theorems 2,3 and Proposition 2 hold for the case of a cyclic biquadratic field K with even conductor except for the case of $m(K) = 2$ [10].

On the other hand in [8] we know the next

Proposition 3. There exist infinitely many abelian but non-cyclic biquadratic fields K whose $\mathcal{O}_K$ have a power basis.

The next Lemma is fundamental to prove the part of infiniteness in Theorems 1, 2, 3 and Proposition 3 because the conductor of each field is expressed by a suitable quadratic polynomial.

Lemma([8]). Let $n(t) = at^2 + bt + c$, $a > 0$ be a polynomial with rational integral coefficients. For an even number $a + b$ and an odd number c let the congruence $n(t) \equiv 0 \mod q^2$ have at most two solutions for any prime q. Then the number $n(t)$ is square-free for infinitely many t.

We used the prime number theorem and the value $\pi^2/6$ of $\zeta(2) = \sum_{n=1}^{\infty} 1/n^2$ in a proof of the Lemma.

References

[1] G. Archinard, Extensions cubiques cycliques de Q dont l'anneau des entiers est monogène, L'Enseignement math., 20(1974), 179-203.

[2] K. Girtmair, On root polynomials of cyclic cubic equations, Arch. Math. (Basel), 36(1981), 313-326.

[3] M. -N. Gras, Sur les corps cubiques cycliques dont l'anneau des entiers est monogène, Ann. Sci. Univ. Besançon, Fasc. 6(1973), 1-26.

[4] M. -N. Gras, Z-bases d'entiers 1, θ, θ^2, θ^3 dans les extensions cycliques de degré 4 de Q, Pub. Math. Univ. de Besançon, Theorie des Nombres, 1980-81.

[5] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.

[6] J. G. Huard, Cyclic cubic fields that contain an integer of given index, Lecture Notes in Mathematics, Springer-Verlag, 751(1979), 195-199.

[7] H. W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math., 201(1958), 119-149.

[8] T. Nakahara, On a power basis of the integer ring in an abelian biquadratic field(in Japanese), RIMS Kōkyūroku, 371(1979), 31-46.

[9] T. Nakahara, On abelian biquadratic fields related to a problem of Hasse, Mathematisches Forschungsinstitut Oberwolfach, Tagungsbericht 35/81, 17-18.

[10] T. Nakahara, On cyclic biquadratic fields related to a problem of Hasse, preprint.

[11] J. J. Payan, Sur les classes ambiges et les ordres monogenes d'une extension cyclique de degre primier impair sur Q ou sur un corps quadratique imaginaire, Ark. Mat., 11(1973), 239-244.

[12] T. Uehara, On cyclic quartic fields, preprint.

[13] H. Weber, Lehrbuch der Algebra, Bd. 2(1899), (republished by Chelsea, New York).

Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga 840, Japan