

CLASS NUMBER RELATION BETWEEN CERTAIN SEXTIC NUMBER FIELDS

AKIRA ENDÔ

ABSTRACT. The congruence relation modulo 7 between the class numbers of the real and imaginary sextic subfields of the extension of a quadratic number field obtained by adjoining a seventh root of unity is studied.

1. Introduction. The aim of this note is to study the congruence relation modulo 7 between the class numbers of the real and imaginary sextic subfields of the extension of a quadratic number field obtained by adjoining a seventh root of unity.

Let $m > 1$ be a square free rational integer, $\zeta = e^{2\pi\sqrt{-1}/7}$ a primitive seventh root of unity and Q the field of rational numbers. Let

$$K = Q(\sqrt{m}, \zeta),$$

which is of degree 12 over Q and has the following subfields:

$$K_0 = Q(\zeta), \quad K_1 = Q(\sqrt{m}, \zeta + \zeta^{-1}), \quad K_2 = Q(\sqrt{-7m}, \zeta + \zeta^{-1}),$$

$$F = Q(\zeta + \zeta^{-1}), \quad k = Q(\sqrt{m}, \sqrt{-7}),$$

$$k_0 = Q(\sqrt{-7}), \quad k_1 = Q(\sqrt{m}), \quad k_2 = Q(\sqrt{-7m}).$$

K_0, K_1 and K_2 are cyclic sextic extensions of Q , and K_1 is the maximal real subfield of K . F is a cyclic cubic extension of Q and the maximal real subfield of K_0 and also of K_2 . Denote the class numbers of K and K_i by h and h_i ($i = 1, 2$), respectively. In this note, we obtain a congruence relation modulo 7 between h_1 and h_2 by making use of the continuity of p -adic L -functions.

2. Class number relations. For any subfield Ω of K , U_Ω and W_Ω denote the unit group of Ω and its subgroup of all roots of unity in Ω , respectively. Put $Q_K = (U_K : U_{K_1}W_K)$ and $Q_2 = (U_{K_2} : U_F W_{K_2})$ (cf. [1]). That $Q_2 = 1$ can be proved by the argument similar to that in the proof of Theorem 1 in [4]. Hence one sees that $Q_K = (U_K : U_{K_0}U_{K_1}U_{K_2})$.

Let \mathfrak{X} denote the set of Dirichlet characters attached to K . Let \mathfrak{X}^+ and \mathfrak{X}^- be the set of even and odd characters in \mathfrak{X} , respectively. Furthermore, χ_0 denotes the principal character.

Received by the editors May 7, 1984 and, in revised form, October 10, 1984.
1980 *Mathematics Subject Classification.* Primary 12A35, 12A50.

Key words and phrases. Sextic number field, class number, p -adic L -function.

©1985 American Mathematical Society
0002-9939/85 \$1.00 + \$.25 per page

Note that both of the class numbers of F and K_0 are equal to 1. Since $2h = Q_K h_1 h_2$ [6, Theorem (6.3)], it follows that

$$\frac{7}{w_K} h_2 \prod_{x \in \mathfrak{K}^-} (1 - \chi(7)) \equiv \frac{R_1 h_1}{\sqrt{D_1}} \prod_{x \in \mathfrak{K}^+ - \{x_0\}} \left(1 - \frac{\chi(7)}{7}\right) \pmod{7},$$

where w_K is the number of roots of unity in K , D_1 is the discriminant of K_1 , and R_1 is the 7-adic regulator of K_1 [2, Theorem 1]. D_1 is given by

$$D_1 = \begin{cases} 7^4 m^3, & 7 \nmid m, \quad m \equiv 1 \pmod{4}, \\ 7^4 (4m)^3, & 7 \nmid m, \quad m \equiv 2, 3 \pmod{4}, \\ 7^2 m^3, & 7 \mid m, \quad m \equiv 1 \pmod{4}, \\ 7^2 (4m)^3, & 7 \mid m, \quad m \equiv 2, 3 \pmod{4}. \end{cases}$$

Therefore, if $7 \nmid m$, then $w_K = 14$ and

$$(1) \quad \frac{1}{2} h_2 \equiv \frac{R_1}{7^2 m \sqrt{m}} h_1 \left(1 - \frac{1}{7} \left(\frac{m}{7}\right)\right) \pmod{7};$$

and if $7 \mid m$ and $m = 7m'$, then

$$(2) \quad \frac{7}{w_K} h_2 \left(1 + \left(\frac{m'}{7}\right)\right) \equiv \frac{R_1}{7m\sqrt{m}} h_1 \pmod{7}.$$

In order to calculate R_1 , we must determine a system of fundamental units of K_1 . For any $x \in F$, x' means the image of x under an automorphism of F which maps ζ to ζ^2 . Let $\eta = \zeta + \zeta^{-1}$; then η and η' constitute a system of fundamental units of F . Let $\varepsilon = \frac{1}{2}(a + b\sqrt{m}) > 1$ be the fundamental unit of k_1 . Furthermore, let $\xi = \frac{1}{2}(\alpha + \beta\sqrt{m})$, $\alpha, \beta \in F$, be a unit of K_1 such that ξ and $\xi' = \frac{1}{2}(\alpha' - \beta'\sqrt{m})$ constitute a system of relative fundamental units of K_1 , i.e., $-1, \xi$ and ξ' generate a subgroup of all units in U_{K_1} whose relative norms to F and to k_1 are 1 and ± 1 , respectively (cf. [3]). Note that α is an integer of F and that β or 7β is an integer of F according as $7 \nmid m$ or $7 \mid m$.

If the equation $x^2 = \pm \eta^r \eta'^s \xi$ for $(r, s) = (1, 0), (0, 1)$ or $(1, 1)$ has a solution in K_1 , when the equation $y^2 = \pm \eta^{-s} \eta'^{r-s} \xi'$ also has a solution in K_1 , let $\eta_0 = \sqrt{\pm \eta^r \eta'^s \xi}$ and $\eta'_0 = \sqrt{\pm \eta^{-s} \eta'^{r-s} \xi'}$; otherwise let $\eta_0 = \eta$ and $\eta'_0 = \eta'$. And, if the equation $z^3 = \varepsilon^{\pm 1} \xi \xi'$ has a solution in K_1 , let $\xi_0 = \sqrt[3]{\varepsilon^{\pm 1} \xi \xi'}$; otherwise let $\xi_0 = \xi$. Then $\varepsilon, \eta_0, \eta'_0, \xi_0$ and ξ' constitute a system of fundamental units of K_1 [3]. Accordingly, if e is the index of the subgroup generated by $-1, \varepsilon, \eta, \eta', \xi$ and ξ' in U_{K_1} , then $e = 1, 3, 4$ or 12 . Hence, after easy calculation, one has

$$(3) \quad R_1 = \frac{12}{e} \log \varepsilon R(\eta) R(\xi)$$

with

$$(4) \quad R(\eta) = (\log \eta)^2 + (\log \eta)(\log \eta') + (\log \eta')^2$$

and

$$(5) \quad R(\xi) = (\log \xi)^2 - (\log \xi)(\log \xi') + (\log \xi')^2,$$

where \log is the 7-adic logarithm.

3. Calculating the 7-adic regulator. In this section, we calculate the 7-adic regulator R_1 of K_1 . First, let $\pi = \zeta + \zeta^{-1} - 2$ and $\mathfrak{p} = (\pi)$; then \mathfrak{p} is a unique prime ideal of F lying above (7): $\mathfrak{p}^3 = (7)$. It is easy to verify that

$$(6) \quad \pi^2 + \pi\pi' + \pi'^2 = -7(\pi + \pi' + 2) \equiv -14 \pmod{\mathfrak{p}^4},$$

$$(7) \quad 2\pi^3 + \pi^2\pi' + \pi\pi'^2 + 2\pi'^3 \equiv 3\pi^3 \equiv -21 \pmod{\mathfrak{p}^4}.$$

Since $\eta^6 \equiv 1 + 3\pi + 2\pi^2 \pmod{\mathfrak{p}^3}$, $\log \eta = \frac{1}{6} \log \eta^6 \equiv 4\pi - \pi^2 \pmod{\mathfrak{p}^3}$. Hence, by making use of (6), (7), it follows from (4) that

$$R(\eta) \equiv 2(\pi^2 + \pi\pi' + \pi'^2) - 4(2\pi^3 + \pi^2\pi' + \pi\pi'^2 + 2\pi'^3) \equiv 7 \pmod{\mathfrak{p}^4}.$$

As $R(\eta)$ is a rational 7-adic integer, this congruence holds modulo 7^2 , that is,

$$(8) \quad R(\eta) \equiv 7 \pmod{7^2}.$$

We next consider $\log \varepsilon$. Here and hereafter $N_{\cdot/\cdot}$ means the norm with respect to the assigned field extension. It is easy to see that the following congruences hold:

$$\begin{aligned} \varepsilon^2 &\equiv 1 + 4ab\sqrt{m} \pmod{7} && \text{if } 7|m, \\ \varepsilon^4 &\equiv 1 - (N_{k_1/Q}\varepsilon)ab\sqrt{m} \pmod{7^2} && \text{if } 7|a, \\ \varepsilon^2 &\equiv 1 + 4ab\sqrt{m} \pmod{7^2} && \text{if } 7|b, \\ \varepsilon^6 &\equiv 1 - (a^2 - 1)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = 1, a \equiv \pm 1 \pmod{7}, \\ \varepsilon^8 &\equiv 1 - (a^2 - 2)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = 1, a \equiv \pm 3 \pmod{7}, \\ \varepsilon^{16} &\equiv 1 - 4(a^2 - 8)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = -1, a \equiv \pm 1 \pmod{7}, \\ \varepsilon^6 &\equiv 1 - (a^2 + 3)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = -1, a \equiv \pm 2 \pmod{7}, \\ \varepsilon^{16} &\equiv 1 - 4(a^2 + 12)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = -1, a \equiv \pm 3 \pmod{7}. \end{aligned}$$

It then follows from these that

$$(9) \quad \log \varepsilon = \left\{ \begin{aligned} \frac{1}{2} \log \varepsilon^2 &\equiv 2ab\sqrt{m} \pmod{7} && \text{if } 7|m, \\ \frac{1}{4} \log \varepsilon^4 &\equiv (N_{k_1/Q}\varepsilon)5ab\sqrt{m} \pmod{7^2} && \text{if } 7|a, \\ \frac{1}{2} \log \varepsilon^2 &\equiv 2ab\sqrt{m} \pmod{7^2} && \text{if } 7|b, \\ \frac{1}{6} \log \varepsilon^6 &\equiv (a^2 - 1)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = 1, a \equiv \pm 1 \pmod{7}, \\ \frac{1}{8} \log \varepsilon^8 &\equiv 6(a^2 - 2)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = 1, a \equiv \pm 3 \pmod{7}, \\ \frac{1}{16} \log \varepsilon^{16} &\equiv 5(a^2 - 8)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = -1, a \equiv \pm 1 \pmod{7}, \\ \frac{1}{6} \log \varepsilon^6 &\equiv (a^2 + 3)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = -1, a \equiv \pm 2 \pmod{7}, \\ \frac{1}{16} \log \varepsilon^{16} &\equiv 5(a^2 + 12)ab\sqrt{m} \pmod{7^2} && \text{if } N_{k_1/Q}\varepsilon = -1, a \equiv \pm 3 \pmod{7}. \end{aligned} \right.$$

Lastly we treat $R(\xi)$. The fact that $N_{K_1/k_1}\xi = \pm 1$ implies that if $7 + m$ then $\alpha^3 + 3\alpha\beta^2m \equiv \pm 1 \pmod{p}$ and $3\alpha^2\beta + \beta^3m \equiv 0 \pmod{p}$. On the other hand, $4N_{K_1/F}\xi = \alpha^2 - \beta^2m = 4$. Hence, one has that if $7 + m$, then $\alpha \equiv \pm 1, \pm 2 \pmod{p}$, and if $7|m$, then $\alpha \equiv \pm 2 \pmod{p}$ because $7\beta \equiv 0 \pmod{p^2}$. Then it is easy to see that the following congruences hold:

$$\begin{aligned} \xi^6 &\equiv 1 + 2(\alpha^2 - 1)^2 + 4(\alpha^2 - 1)(\alpha^2 - 3)\alpha\beta\sqrt{m} \pmod{p^3} && \text{if } \alpha \equiv \pm 1 \pmod{p}, \\ \xi^2 &\equiv 1 + 4(\alpha^2 - 4 + \alpha\beta\sqrt{m}) \pmod{p^3} && \text{if } \alpha \equiv \pm 2 \pmod{p}. \end{aligned}$$

It follows from these that

$$\log \xi = \begin{cases} \frac{1}{6} \log \xi^6 \equiv 3(\alpha^2 - 1)(\alpha^2 - 3)\alpha\beta\sqrt{m} \pmod{p^3} & \text{if } 7 + m, \alpha \equiv \pm 1 \pmod{p}, \\ \frac{1}{2} \log \xi^2 \equiv 2\alpha\beta\sqrt{m} \pmod{p^3} & \text{if } 7 + m, \alpha \equiv \pm 2 \pmod{p}, \\ \frac{1}{2} \log \xi^2 \equiv \alpha\beta(2 + 2\beta^2m + \beta^4m^2)\sqrt{m} \\ \quad + \frac{1}{7}\alpha\beta^7m^3(2 - 2\beta^2m - 4\beta^4m^2)\sqrt{m} \pmod{p^3} & \text{if } 7|m. \end{cases}$$

We now assume that $7 + m$ and put $\alpha\beta = c_0 + c_1\pi + c_2\pi^2$ with rational integers c_0, c_1, c_2 . It is easy to verify that if $\alpha \equiv \pm 1 \pmod{p}$, then $c_0^2m \equiv 4 \pmod{7}$ and $(\alpha^2 - 1)(\alpha^2 - 3)\alpha\beta \equiv c_1\pi + (3c_0c_1m + c_2)\pi^2 \pmod{p^3}$, and if $\alpha \equiv \pm 2 \pmod{p}$, then $c_0 \equiv 0 \pmod{7}$. Thus, by making use of (6), (7), it follows from (5) that

$$(10) \quad R(\xi) \equiv \begin{cases} 7c_1(3c_1 + 3c_0c_1^2m + c_2)m \pmod{7^2} & \text{if } \alpha \equiv \pm 1 \pmod{p}, \\ 14c_1(3c_1 + c_2)m \pmod{7^2} & \text{if } \alpha \equiv \pm 2 \pmod{p}. \end{cases}$$

We next assume that $7|m$ and put $7\alpha\beta = d_2\pi^2 + d_3\pi^3 + d_4\pi^4$ with rational integers d_2, d_3, d_4 . In this case, $N_{K_1/k_1}\xi^2 = 1$ implies that $d_3 \equiv d_2 + 2d_2^3m' \pmod{7}$. Then, by easy calculation, it follows from (5) that

$$(11) \quad R(\xi) \equiv 7d_2(d_2^5 - d_2^3m'^2 - 2d_4m') \left(1 + \left(\frac{m'}{7} \right) \right) \pmod{7^2}.$$

4. Theorems. The following theorem is obtained from (1)–(3) and (8)–(11):

THEOREM 1. *With the notation above, if $7 + m$, then*

$$\frac{1}{2}h_2 \equiv -\left(\frac{m}{7}\right) \frac{12}{e} \frac{\log \varepsilon R(\xi)}{7^2m\sqrt{m}} h_1 \pmod{7},$$

where $\log \varepsilon$ and $R(\xi)$ are given by (9) and (10), respectively, and if $7|m$ and $m' = m/7 \equiv 1, 2$ or $4 \pmod{7}$, then

$$\frac{7}{w_K}h_2 \equiv \frac{24}{e}abd_2(d_2^5m'^2 - d_2^3m' - 2d_4)h_1 \pmod{7}.$$

As corollaries of this theorem, the following two theorems hold:

THEOREM 2. *With the notation above, assume that $7 \nmid m$. Then, $7|h_2$ if and only if $7|h_1$ or one of the following conditions is satisfied:*

- (1) $N_{k_1/Q}\epsilon = 1$ and $a \equiv 0, \pm 1, \pm 10 \pmod{7^2}$.
- (2) $N_{k_1/Q}\epsilon = -1$ and $a \equiv 0, \pm 12, \pm 20, \pm 24 \pmod{7^2}$.
- (3) $b \equiv 0 \pmod{7^2}$.
- (4) $c_1 \equiv 0 \pmod{7}$ or $c_1 + c_0c_1^2m \equiv 2c_2 \pmod{7}$.

THEOREM 3. *With the notation above, assume that $7|m$ and $m' \equiv 1, 2$ or $4 \pmod{7}$. Then, $7|h_2$ if and only if $7|h_1$ or one of the following conditions is satisfied:*

- (1) $b \equiv 0 \pmod{7}$.
- (2) $d_2 \equiv 0 \pmod{7}$ or $d_2^5m'^2 - d_2^3m' \equiv 2d_4 \pmod{7}$.

Regarding the conditions in the above two theorems we give the following remark (cf. [5, Theorem 1]):

REMARK. (1) When $7 \nmid m$ and $\alpha \equiv \pm 1 \pmod{p}$, $c_1 \equiv 0 \pmod{7}$ and $c_1 + c_0c_1^2m \equiv 2c_2 \pmod{7}$ are necessary and sufficient conditions for $\xi^{12}\xi'^6 \equiv 1 \pmod{p^4}$ and $\xi^6\xi'^{12} \equiv 1 \pmod{p^4}$, respectively.

(2) When $7 \nmid m$ and $\alpha \equiv \pm 2 \pmod{p}$, $c_1 \equiv 0 \pmod{7}$ and $c_1 \equiv 2c_2 \pmod{7}$ are necessary and sufficient conditions for $\xi^4\xi'^2 \equiv 1 \pmod{p^4}$ and $\xi^2\xi'^4 \equiv 1 \pmod{p^4}$, respectively.

(3) When $7|m$, $d_2 \equiv 0 \pmod{7}$ and $d_2^5m'^2 - d_2^3m' \equiv 2d_4 \pmod{7}$ are necessary and sufficient conditions for $\xi^2\xi'^4 \equiv 1 \pmod{\mathfrak{P}^7}$ and $\xi^4\xi'^2 \equiv 1 \pmod{\mathfrak{P}^7}$, respectively. Herein, \mathfrak{P} is a unique prime ideal of K_1 lying above (7) . Therefore, it can be shown that the assertion of Theorem 3 holds without any restriction on m' .

Finally we give numerical examples for small m (cf. [3]).

The case where $7 \nmid m$.

$m = 2, \epsilon = 1 + \sqrt{2}, \xi = 11 + 4\pi + (12 + 10\pi + 2\pi^2)\sqrt{2}, e = 4, (c_0, c_1, c_2) \equiv (3, 2, 3) \pmod{7}, h_1 = 1, h_2 = 4;$

$m = 3, \epsilon = 2 + \sqrt{3}, \xi = 293 + 210\pi + 36\pi^2 + (154 + 96\pi + 14\pi^2)\sqrt{3}, e = 12, (c_0, c_1, c_2) \equiv (0, 1, 0) \pmod{7}, h_1 = 1, h_2 = 4;$

$m = 5, \epsilon = \frac{1}{2}(1 + \sqrt{5}), \xi = \frac{1}{2}(107 + 77\pi + 10\pi^2 + (49 + 34\pi + 6\pi^2)\sqrt{5}), e = 12, (c_0, c_1, c_2) \equiv (0, 5, 2) \pmod{7}, h_1 = 1, h_2 = 2;$

$m = 6, \epsilon = 5 + 2\sqrt{6}, \xi = 673 + 588\pi + 108\pi^2 + (154 + 48\pi + 2\pi^2)\sqrt{6}, e = 12, (c_0, c_1, c_2) \equiv (0, 3, 1) \pmod{7}, h_1 = 1, h_2 = 28;$

$m = 10, \epsilon = 3 + \sqrt{10}, \xi = 10779 + 7140\pi + 1120\pi^2 + (3472 + 2366\pi + 386\pi^2)\sqrt{10}, e = 12, (c_0, c_1, c_2) \equiv (0, 0, 3) \pmod{7}, h_1 = 2, h_2 = 28.$

The case where $7|m$.

$m = 7, \epsilon = 8 + 3\sqrt{7}, \xi = 15 + 12\pi + 2\pi^2 + \frac{1}{7}(28 + 14\pi + 2\pi^2)\sqrt{7}, e = 12, (d_2, d_3, d_4) \equiv (1, 3, 2) \pmod{7}, h_1 = h_2 = 1;$

$m = 14, \epsilon = 15 + 4\sqrt{14}, \xi = 83 + 64\pi + 12\pi^2 + \frac{1}{7}(126 + 70\pi + 8\pi^2)\sqrt{14}, e = 12, (d_2, d_3, d_4) \equiv (3, 6, 5) \pmod{7}, h_1 = h_2 = 1;$

$m = 77, \epsilon = \frac{1}{2}(9 + \sqrt{77}), \xi = \frac{1}{2}(2231 + 1430\pi + 220\pi^2 + \frac{1}{7}(1897 + 1330\pi + 220\pi^2)\sqrt{77}), e = 12, (d_2, d_3, d_4) \equiv (1, 2, 2) \pmod{7}, h_1 = h_2 = 1;$

$m = 455$, $\varepsilon = 64 + 3\sqrt{455}$, $\xi = 992879 + 688410\pi + 115470\pi^2 + \frac{1}{7}(312774 + 203238\pi + 30804\pi^2)\sqrt{455}$, $e = 3$, $(d_2, d_3, d_4) \equiv (5, 1, 0) \pmod{7}$, $h_1 = 4$, $h_2 = 224$;
 $m = 497$, $\varepsilon = 1201887 + 53912\sqrt{497}$, $\xi = \frac{1}{2}(1762 + 1127\pi + 168\pi^2 + \frac{1}{7}(588 + 413\pi + 70\pi^2)\sqrt{497})$, $e = 3$, $(d_2, d_3, d_4) \equiv (0, 0, 6) \pmod{7}$, $h_1 = 1$, $h_2 = 28$.

ACKNOWLEDGEMENT. The author would like to express his thanks to the referee for valuable suggestions.

REFERENCES

1. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
2. A. Kudo, *On a class number relation of imaginary abelian fields*, J. Math. Soc. Japan **27** (1975), 150–159.
3. S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Math., Vol. 797, Springer-Verlag, Berlin and New York, 1980.
4. C. J. Parry, *Real quadratic fields with class numbers divisible by five*, Math. Comput. **31** (1977), 1019–1029.
5. _____, *On the class number of relative quadratic fields*, Math. Comput. **32** (1978), 1261–1270.
6. C. D. Walter, *Kuroda's class number relation*, Acta Arith. **35** (1979), 41–51.

DEPARTMENT OF MATHEMATICS, KUMAMOTO UNIVERSITY, KUMAMOTO 860, JAPAN