92. On Cubic Galois Extensions of $Q(\sqrt{-3})$

By Hideo WADA
Department of Mathematics, University of Tokyo

(Comm. by Kunihiko KODAIRA, M. J. A., May 12, 1970)

Let k be the field $\mathbf{Q}(\sqrt{-3})$ and let K be the field $k(\sqrt[3]{A})$ for some element A of k. In this paper, we shall determine in Theorem 1 a basis of integers of K and determine in Theorem 2 the genus field of K with respect to k and determine in Theorem 3 whether the class number of K is a multiple of 3 or not

1. A basis of integers.

Let O_k be the ring of integers of $k=\mathbf{Q}(\sqrt{-3})$. Any cubic galois extension K over k can be written as $k(\sqrt[3]{A})$, where $A\in O_k$, $A\neq 1$, is without cubic factors and, without loss of generality, we may assume that $A=fg^2$, f and g being integers of k having no square factors and $f\not\equiv -1$, $g\not\equiv -1 \pmod{\sqrt{-3}}$. Put $A^*=f^2g$, $\theta=\sqrt[3]{A}$, $\theta^*=\theta^2/g=\sqrt[3]{A^*}$ and $O_K=$the ring of integers of K. By the relation $\theta^2=g\theta^*$, every element of K can be expressed in the form $\alpha+\beta\theta+\gamma\theta^*$, $(\alpha,\beta,\gamma\in k)$. Let $\omega=\alpha+\beta\theta+\gamma\theta^*$ be an element of O_K and ω',ω'' be its conjugates over k. It can be easily veryfied that:

(1) $\omega+\omega'+\omega''=3\alpha$,

(2) $\omega\omega'+\omega'\omega''+\omega''\omega=3\alpha^2-3\beta\gamma fg$,

(3) $\omega\omega'\omega''=\alpha^3+\beta^3A+\gamma^3A^*-3\alpha\beta\gamma fg$.

As ω is an integer, 3α and

$$(3\beta)^3A\cdot(3\gamma)^3A^*=(9\beta\gamma fg)^3,$$

$$(3\beta)^3A+(3\gamma)^3A^*=27(\alpha^3+\beta^3A+\gamma^3A^*-3\alpha\beta\gamma fg)-(3\alpha)^3+3\cdot 3\alpha\cdot 9\beta\gamma fg$$

are integers of k. Since A and A^* contain no cubic factors, 3β and 3γ are integers of k. Put $3\alpha=a$, $3\beta=b$ and $3\gamma=c$. Then $\omega=(a+b\theta+c\theta^*)/3$, $(a,b,c\in O_k)$. From (2) and (3), these coefficients must satisfy the congruences:

(4) $a^2-bcfg\equiv 0 \pmod 3$,

(5) $a^3+b^3A+c^3A^*-3abcfg\equiv 0 \pmod{27}$.

We shall next determine a basis of O_K as O_k-module. When $\omega_1=1$, $\omega_2=(a_2+b_2\theta)/3$ and $\omega_3=(a_3+b_3\theta+c_3\theta^*)/3$ are elements of O_K such that:

$$\min\{|b|\,;\,O_K\ni(a+b\theta)/3,\ O_k\ni a,b,\ b\neq 0\}=|b_2|,$$

$$\min\{|c|\,;\,O_K\ni(a+b\theta+c\theta^*)/3,\ O_k\ni a,b,c,\ c\neq 0\}=|c_3|,$$

then $\omega_1,\omega_2,\omega_3$ is a basis of O_K as O_k-module, since O_k is Euclidean.

$(a+b\theta)/3$ is an element of O_K if and only if

$$a^2 \equiv 0 \pmod 3), \quad a^3 + b^3 A \equiv 0 \pmod{27}.$$

From these congruences, a and b are multiples of $\sqrt{-3}$. Put $a=\sqrt{-3}x$, $b=\sqrt{-3}y$. Then we have $x^3+y^3A\equiv 0 \pmod{3\sqrt{-3}}$. From this congruences, we may take $\omega_2=(1-\theta)/\sqrt{-3}$, when $A\equiv 1 \pmod{3\sqrt{-3}}$ and $\omega_2=\theta$, when $A\not\equiv 1 \pmod{3\sqrt{-3}}$.

$\omega=(a+b\theta+c\theta^*)/3$ is an element of O_K if and only if a, b and c satisfy the congruences (4) and (5). If c is not a multiple of 3, but c is a multiple of $\sqrt{-3}$, then from (4) and (5), a and b are also multiples of $\sqrt{-3}$. Put $a=\sqrt{-3}x$, $b=\sqrt{-3}y$ and $c=\sqrt{-3}z$. Then ω is $(x+y\theta+z\theta^*)/\sqrt{-3}$ and we may assume $z=1$. In this case, ω is an integer if and only if

$$x^3+y^3A+A^*-3xyfg\equiv 0 \pmod{3\sqrt{-3}}.$$

From this congruence ω is an integer if and only if $f\equiv g\equiv 1 \pmod{\sqrt{-3}}$ and $f\equiv g \pmod 3$. In this case, $(1+\theta+\theta^*)/\sqrt{-3}$ is an integer.

If c is not a multiple of $\sqrt{-3}$ and $\omega=(a+b\theta+c\theta^*)/3$ is an integer, then $\sqrt{-3}\omega$ is also an integer. From above argument we have $f\equiv g\equiv 1 \pmod{\sqrt{-3}}$, $f\equiv g \pmod 3$ and $(1+\theta+\theta^*)/\sqrt{-3}$ is an integer. So we may assume $c=1$. The congruences (4) and (5) are in this case as follows:

(6) $a^2-bfg\equiv 0 \pmod 3$,

(7) $a^3+b^3A+A^*-3abfg\equiv 0 \pmod{27}$.

Since $A\equiv A^*\equiv 1 \pmod{\sqrt{-3}}$, we have $a\equiv b\equiv 1 \pmod{\sqrt{-3}}$. Put $a=\sqrt{-3}k+1$, $b=\sqrt{-3}l+1$, $f=\sqrt{-3}m+1$ and $g=f+3s$. Then

(8) $a^2-bfg\equiv\sqrt{-3}(m-k-l) \pmod 3$.

From (6) and (8) we may assume $l=m-k$. It can be easily verified that

$$a^3+b^3fg^2+f^2g-3abfg\equiv 9\,(1+\sqrt{-3}m)s^2 \pmod{27}.$$

Therefore (7) can be solved if and only if $f\equiv g \pmod{3\sqrt{-3}}$.

Thus we have proved the following theorem.

Theorem 1. *Let $k=\mathbf{Q}(\sqrt{-3})$, $K=k(\sqrt[3]{A})$ where A is an integer of k, cubefree and $A=fg^2$, $f\not\equiv -1 \pmod{\sqrt{-3}}$, $g\not\equiv -1 \pmod{\sqrt{-3}}$. Put $\theta=\sqrt[3]{A}$, $\theta^*=\theta^2/g$. Then a basis of integers of K as O_k-module where O_k is the ring of integers of k is given as follows:*

$\{1,\theta,\theta^*\}$, *when* $f\not\equiv g \pmod 3$,

$\{1,\theta,(1+\theta+\theta^*)/\sqrt{-3}\}$, *when* $f\equiv g \pmod 3$, $f\not\equiv g \pmod{3\sqrt{-3}}$,

$\{1,(1-\theta)/\sqrt{-3},(f+\theta+\theta^*)/3\}$, *when* $f\equiv g \pmod{3\sqrt{-3}}$.

The ideal $(\sqrt{-3})$ is unramified in K if and only if

$$A\equiv 1 \pmod{3\sqrt{-3}}.$$

2. The genus field.

Among abelian extensions over k, let L be the maximal unramified extension over K. It can be easily proved that the galois group $G(L/k)$ is of $(3, 3, \cdots, 3)$ type (cf. [3]).

As $\varphi(3\sqrt{-3})=18$ and there is the primitive sixth root of unity in O_k, any prime ideal $\mathfrak{p}$ of k which is not $(\sqrt{-3})$, can be expressed as (p), where p is an element of O_k and $p\equiv 1$ or 2 or 4 $(\bmod 3\sqrt{-3})$. Therefore A can be expressed as follows:

$$A=p_1^{e_1}\cdots p_n^{e_n}\cdot q_{n+1}^{e_{n+1}}\cdots q_s^{e_s}\cdot r$$

where $e_i=1$ or 2 $(1\leqq i\leqq s)$

$$p_i\equiv 1 \ (\bmod 3\sqrt{-3}),\quad q_i\equiv 2 \text{ or } 4 \ (\bmod 3\sqrt{-3})$$

$$r=\rho^l(\sqrt{-3})^m,\quad \rho=(1+\sqrt{-3})/2,\quad l, m\in Z.$$

Then we get easily the following theorem.

Theorem 2. *Let L, p_i, q_i and r be as above. Then L is expressed as follows:*

$$L=K(\sqrt[3]{p_1}, \cdots, \sqrt[3]{p_n}, \sqrt[3]{q_{n+1}q_{n+2}^{m_{n+2}}}, \cdots, \sqrt[3]{q_{n+1}q_s^{m_s}})$$

where $m_i=1$ or 2 such that

$$q_{n+1}q_i^{m_i}\equiv \pm 1 \ (\bmod 3\sqrt{-3}).$$

Let t be the number of ramified prime ideals in K/k. Then the degree of $L=K$ is 3^{t-1}, when $n=s$, and 3^{t-2}, when $n<s$.

It is easy to see that the class number of K is not a multiple of 3 if and only if $L=K$. So we have next theorem.

Theorem 3. *The class number of K is not a multiple of 3 if and only if A has one of the following forms (p_i, q_i, r are as above):*

1) $A=p_1$. 2) $A=q_1q_2$, $q_1\equiv 2$, $q_2\equiv 4$ $(\bmod 3\sqrt{-3})$.

3) $A=q_1q_2^2$, $q_1\equiv q_2\equiv 2$ *or* 4 $(\bmod 3\sqrt{-3})$. 4) $A=r$. 5) $A=q_1r$.

Remark. When A is a natural number, K contains the purely cubic field $F=\mathbf{Q}(\sqrt[3]{A})$. Prof. T. Honda determined whether the class number of F is a multiple of 3 or not (cf. [4]). He also proved that the class number of K is not a multiple of 3 if and only if the class number of F is not a multiple of 3 (cf. [4]). If we use this fact and Theorem 3, we can easily get his result.

References

[1] R. Dedekind: Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. J. Reine Angew. Math., **121**, 40–123 (1900).

[2] B. N. Delone and D. K. Faddeev: The Theory of Irrationalities of the Third Degree. Moskva (1940).

[3] H. Hasse: Zur Geschlechtertheorie in quadratischen Zahlkörpern. J. Math. Soc. Japan, **3**, 45–51 (1951).

[4] H. Honda: Pure cubic fields whose class numbers are multiples of 3 (to appear in J. of Number Theory).

[5] J. Martinet et J. J. Payan: Sur les bases d'entiers des extensions galoisiennes et non abeliennes de degré 6 des rationnels. J. Reine Angew. Math., **229**, 29–33 (1968).