

Existence of an unramified cyclic extension
and congruence conditions

Makoto Ishida (石田 真) (石田 真)

(Tokyo Metropolitan University)

Let K be an algebraic number field of odd prime degree ℓ .

Then the following two facts are known.

1) The prime ℓ is totally ramified in K if and only if there exists a primitive element π of K ($K = \mathbb{Q}(\pi)$) having the minimal polynomial $f(X)$ of Eisenstein type with respect to ℓ , i.e.

$$f(X) = X^\ell + a_1 X^{\ell-1} + a_2 X^{\ell-2} + \dots + a_\ell \in \mathbb{Z}[X],$$

$$\text{where } a_1 \equiv a_2 \equiv \dots \equiv a_\ell \equiv 0 \pmod{\ell}$$

$$\text{and } a_\ell \not\equiv 0 \pmod{\ell^2}.$$

Let k^+ be the unique (real) subfield, of degree ℓ , of the ℓ^2 -th cyclotomic field.

2) In the case 1), $L = k^+K$ is an unramified (cyclic) extension over K if and only if we have

$$a_1 + a_\ell \equiv a_2 \equiv \dots \equiv a_{\ell-1} \equiv 0 \pmod{\ell^2}.$$

We exclude the special case $K = k^+$. So, in the following, we may suppose $K \neq k^+$ and $[L : K] = \ell$. Of course, we may also suppose that K is real.

Now our problem in the case 2) is as follows :

Is there an unramified cyclic extension M , of degree ℓ^2 , over K , containing $L = k^+K$? More precisely, are there any higher congruence conditions on the coefficients $a_1, a_2, \dots, a_\ell$ of $f(X)$, which ensure the existence of such an extension M of K ?

I. Under the congruence conditions in 1) and 2), our first conclusion is :

If $a_\ell \not\equiv \ell d^\ell \pmod{\ell^3}$ for any $d \in \mathbb{Z}$, then there is no unramified cyclic extension, of degree ℓ^2 , over K , containing $L = k^+K$.

In fact, let ℓ be the prime ideal in K dividing ℓ and we have $(\pi) = \ell \zeta$ with $(\ell, \zeta) = 1$. The ideal class group C_K of K has the subgroup

$$G_\ell = \left\{ \text{Cl}(\alpha) \mid (\alpha, \ell) = 1 \text{ and } N \alpha^{\ell-1} \equiv 1 \pmod{\ell^2} \right\}$$

of index ℓ , which corresponds to the abelian extension L in the sense of class field theory. Then it is proved

$$a_\ell \not\equiv \ell d^\ell \pmod{\ell^3} \text{ for any } d \in \mathbb{Z}$$

$$\iff \text{Cl}(\ell)^{-1} = \text{Cl}(\zeta) \notin G_\ell$$

$$\iff C_K = \langle \text{Cl}(\ell) \rangle G_\ell.$$

Then the assertion easily follows.

Therefore, in consideration of our problem, we may suppose that we have $a_\ell \equiv \ell d^\ell \pmod{\ell^3}$ with some $d \in \mathbb{Z}$. Then, replacing π by $c\pi$ with $c \in \mathbb{Z}$ such that $cd \equiv 1 \pmod{\ell^2}$, we may assume that we have

$$a_\ell \equiv \ell \pmod{\ell^3}.$$

II. From now on, we treat the cubic case i.e. $\ell = 3$.

Notations :

ζ = a primitive 3rd root of unity,

η = a primitive 9-th root of unity,

$k = Q(\zeta) = Q(\sqrt{-3})$, $K' = kK$, $L' = kL$,

so $L' = kk^+K = K(\eta) = K'(\eta) = K'(\sqrt[3]{\zeta})$,

ℓ' = the prime ideal in K' , dividing 3,

so $(3) = \ell'^6$, $\ell'^2 \parallel \pi$ and $(1-\zeta) = \ell'^3$.

1°. As preliminaries, we have the following two assertions.

(a) Algebraic aspect. By Kummer theory, for any $\alpha \in K'$ ($\alpha \neq 0$), $M' = L'(\sqrt[3]{\eta\alpha}) = K'(\sqrt[3]{\eta\alpha})$ is a cyclic extension, of degree 9, over K' . (Conversely, every cyclic extension, of degree 9, over K' , containing L' , is obtained in this way.) Moreover if we have

$$(*) \quad \alpha \alpha^J = \gamma^3 \quad \text{with } \gamma \in K',$$

(J denotes the complex conjugation)

then M' is an abelian extension, of degree 18, over K and the fixed subfield M by J is a cyclic extension, of degree 9, over K , containing $L = k^+K$.

(b) Arithmetic aspect. As L' is unramified over K' , the unramifiedness of M over K is equivalent to that of M' over L' . Then, by the ramification theory in Kummer extensions, it is also equivalent, under the condition $(\alpha, \ell') = 1$, to the two facts

- (1) the principal ideal (α) is the cube of an ideal in L' .
- (2) $\eta\alpha$ is congruent to the cube of an integer in L' modulo ℓ'^9 for any prime divisors ℓ' of ℓ' in L' .

Of course, we can easily modify these assertions for the case of arbitrary odd prime ℓ .

2°. Now we assume that the following congruence conditions are satisfied :

$$\left\{ \begin{array}{l} a_3 \equiv 3 \pmod{3^3} \quad (\text{as remarked in I}) \\ \text{i.e. } a_3 = 3b \quad (b \in \mathbb{Z}, \quad b \equiv 1 \pmod{3^2}), \\ a_1 \equiv -a_3 = -3b \pmod{3^3}, \\ a_2 \equiv 0 \pmod{3^3}. \end{array} \right.$$

We put $\omega = b(1-\zeta)/\pi$ and $\varepsilon = 1-\omega$, which are integers in K' such that $\ell' \parallel \omega$ and $\ell' \nmid \varepsilon$.

Then, under the above conditions, it is proved that we have

$$(\varepsilon^J)^3 - \varepsilon^3 \zeta \equiv 0 \pmod{\ell'^{15}}.$$

So we have

$$\zeta \equiv \text{the cube of an integer in } K' \pmod{\ell'^{10}},$$

which implies that ℓ' is completely decomposed in $L' =$

$K'(\sqrt[3]{\zeta})$: $\ell' = \mathcal{L}_1' \mathcal{L}_2' \mathcal{L}_3'$, Moreover, for each prime ideal $\mathcal{L}_i'$, we see that

$$(\varepsilon^J - \eta\varepsilon)(\varepsilon^J - \eta\varepsilon\zeta)(\varepsilon^J - \eta\varepsilon\zeta^2) \equiv 0 \pmod{\mathcal{L}_i'^{15}}.$$

Investigating the exponent of $\mathcal{L}_i'$ in each factor of the left-hand side, we have

$$\eta\varepsilon\zeta^j \equiv \varepsilon^J \pmod{\mathcal{L}_i'^9} \quad \text{with some } j = j(i).$$

Hence our second conclusion follows :

We have

$$\eta\varepsilon(\varepsilon^J)^2 \equiv \text{the cube of an integer in } L' \pmod{\mathcal{L}_i'^9} \quad (i=1,2,3)$$

and

$$(\varepsilon(\varepsilon^J)^2)(\varepsilon(\varepsilon^J)^2)^J = (\varepsilon\varepsilon^J)^3.$$

(That is, $\alpha = \varepsilon(\varepsilon^J)^2$ satisfies the conditions (*) in (a) and (2) in (b).)

3°. Consequently, by considering the extension $M' = L'(\sqrt[3]{\eta\varepsilon(\varepsilon^J)^2})$ of K , our third conclusion is :

If the principal ideal $(\varepsilon(\varepsilon^J)^2)$ is the cube of an ideal in L' , then there exists an unramified cyclic extension M , of degree 9, over K , containing $L = k^+K$.

Here we note that, for an integer δ in K' such that

$$\delta \equiv \varepsilon \equiv 1 - \omega \pmod{\ell'^9},$$

we have the similar conclusion for the extension $L'(\sqrt[3]{\eta\delta(\delta^J)^2})$.

4°. As for the assumption in the third conclusion, we can show that ε is a unit in K' if and only if

$$N_{K'/K}(\varepsilon) = \pm 1 \text{ or } \pm \zeta \text{ or } \pm \zeta^2,$$

and so if and only if $(N_{K'/K}(\varepsilon) = \zeta \text{ i.e.})$

$$a_3 = 3b, \quad a_1 = -3b, \quad a_2 = 3(b^2 - 1) \\ (b \equiv 1 \pmod{3^2})$$

(and in this case, our extension M exists).

In this special case, the minimal polynomial of $\pi - b$ is given by $X^3 - 3X + b^3$ and the discriminant is equal to $-27(b^6 - 4)$. We note that the norm $N_{K'/K}(\varepsilon)$ of the unit ε is of course a unit of K and we have $-(N_{K'/K}(\varepsilon))^{-1} = b\pi + 1$.

Hence we have the following assertion :

Let $K = Q(\beta)$ be a cubic number field, where the minimal polynomial of β is

$$X^3 - 3X + b^3 \in \mathbb{Z}[X]$$

$$\text{with } b \equiv 1 \pmod{3^2}.$$

Then $1+b(\beta+b) = 1+b^2+b\beta$ is a unit of K . Moreover, K has an unramified cyclic extension of degree 9 (so the ideal class group of K contains a cyclic subgroup of order 9).

It is also shown that there are infinitely many cubic number fields $K = Q(\beta)$, which are obtained in the above way.

5°. Under the congruence conditions on a_1, a_2, a_3 as in 2°, we investigate the ω -adic expansions of several integers in K' and L' , where $\omega = b(1-\zeta)/\pi$ ($\ell' \nmid \omega$). Let $O_{K'}$ and $O_{L'}$ be the rings of integers in K' and L' respectively. Since we have

(3) = ℓ'^6 in K' and $\ell' = \ell'_1 \ell'_2 \ell'_3$ in L' ,
 we can take $\{0, 1, -1\}$ as a representative system of the residue
 fields $O_{K'}/\ell'$ and $O_{L'}/\ell'_i$.

Then, after cumbersome calculations, we have

$$\begin{cases} -3 \equiv \omega^6 \\ \pi \equiv \omega^2 + \omega^5 - \omega^6 - \omega^7 - \omega^8 - \omega^9 \\ \zeta \equiv 1 - \omega^3 - \omega^6 + \omega^9 \end{cases} \pmod{\ell'^{10}};$$

especially we have

$$\zeta \equiv (1 - \omega - \omega^2)^3 \pmod{\ell'^{10}}$$

(see 2°).

We fix one of ℓ'_i s : e.g. $\ell' = \ell'_1$. Then, by a suitable
 choice of η (a primitive 9-th root of unity), we have

$$\eta \equiv 1 - \omega - \omega^2 - \omega^3 + \omega^7 \pmod{\ell'^9}.$$

As $\omega^J = \omega(1+\zeta) \equiv -\omega - \omega^4 + \omega^7 + \omega^8 \pmod{\ell'^9}$, we see

$$\begin{aligned} \eta(1-\omega) &\equiv 1 + \omega + \omega^4 - \omega^7 - \omega^8 \\ &\equiv 1 - \omega^J \pmod{\ell'^9}. \end{aligned}$$

Consequently, putting $\varepsilon = 1 - \omega$, we have

$$\begin{aligned} \eta\varepsilon &\equiv \varepsilon^J \pmod{\ell'^9} \\ \text{i.e. } \eta\varepsilon(\varepsilon^J)^2 &\equiv (\varepsilon^J)^3 \pmod{\ell'^9}. \end{aligned}$$

For another ℓ'_i ($i=2,3$), we have $\ell'_i = \ell'^\tau$ with some $\tau \in$
 $\text{Gal}(L'/K')$ and, as $\eta^\tau = \eta\zeta^j$,

$$\begin{aligned} \eta\varepsilon(\varepsilon^J)^2 &\equiv (\varepsilon^J)^3 \zeta^{-j} \\ &\equiv (\varepsilon^J (1 - \omega - \omega^2)^{-j})^3 \pmod{\ell'_i{}^9}. \end{aligned}$$

These are the congruences obtained in 2°.

Finally, we add some remarks in local aspect. We are
 interested in seeking all $\alpha \in O_{K'}$, such that

$$\eta\alpha \equiv \alpha^J \beta^3 \pmod{\ell'^9} \quad \text{with } \beta \in O_{K'},$$

because this congruence implies

$$\eta\alpha(\alpha^J)^2 \equiv (\alpha^J\beta)^3 \pmod{\mathcal{L}'^9}$$

$$\text{and } (\alpha(\alpha^J)^2)(\alpha(\alpha^J)^2)^J = (\alpha\alpha^J)^3,$$

that is, $\alpha(\alpha^J)^2$ satisfies the conditions (*) in (a) and (2) in (b).

If $\eta\alpha \equiv \alpha^J\beta^3 \pmod{\mathcal{L}'^9}$, then we have

$$\alpha/\epsilon \equiv (\alpha/\epsilon)^J\beta^3 \pmod{\mathcal{L}'^9}.$$

It is proved that, for any $\gamma \in O_K$, ($\gamma \equiv 1 \pmod{\mathcal{L}'}$), we have

$$\gamma \equiv \gamma^J\beta^3 \quad \text{i.e.} \quad \alpha \equiv \epsilon\gamma \pmod{\mathcal{L}'^9}$$

if and only if

$$\gamma \equiv \lambda\mu^3 \pmod{\mathcal{L}'^9},$$

where $\lambda, \mu \in O_K$, ($\lambda, \mu \equiv 1 \pmod{\mathcal{L}'}$) such that $\lambda \equiv \lambda^J \pmod{\mathcal{L}'^9}$.

Hence, for $\alpha \in O_K$, ($\alpha \equiv 1 \pmod{\mathcal{L}'}$) such that

$$\alpha \equiv \epsilon\gamma \quad \text{i.e.} \quad \equiv \epsilon\lambda\mu^3 \pmod{\mathcal{L}'^9},$$

if the principal ideal $(\alpha(\alpha^J)^2)$ is the cube of an ideal in L' , then the extension $M' = L'(\sqrt[3]{\eta\alpha(\alpha^J)^2})$ has the subfield M , which is an unramified cyclic extension, of degree 9, over K , containing $L = k^+K$.

We note that, as $\epsilon = 1 - \omega$ and $\gamma \equiv 1 \pmod{\mathcal{L}'^2}$, we have

$$\alpha \equiv \epsilon\gamma \equiv 1 - \omega \pmod{\mathcal{L}'^2}.$$

Among 3^7 classes of $O_K/\mathcal{L}'^9$, containing an integer $\equiv 1 - \omega \pmod{\mathcal{L}'^2}$, there are exactly 3^5 classes, containing some $\epsilon\gamma$ as above.