ACTA ARITHMETICA
LI (1988)

Existence of an unramified cyclic extension and congruence conditions

by

MAKOTO ISHIDA (Tokyo)

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 ($K = Q(\pi)$) having the minimal polynomial $f(X)$ of Eisenstein type with respect to l, that is,

$$f(X) = X^l + a_1 X^{l-1} + a_2 X^{l-2} + \ldots + a_l \in \boldsymbol{Z}[X],$$

where

$$a_1 \equiv a_2 \equiv \ldots \equiv a_l \equiv 0 \pmod{l} \quad \text{and} \quad a_l \not\equiv 0 \pmod{l^2}.$$

Let $k^+ = k_l^+$ 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 of K if and only if we have

$$a_1 + a_l \equiv a_2 \equiv \ldots \equiv a_{l-1} \equiv 0 \pmod{l^2}$$

(cf. [2], Chap. 5).

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

Now our problem in the cases 1) and 2) is as follows:

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

In Section 1, we give a necessary condition for the existence of such an extension. In Section 2, we treat the cubic case and prove the key congruences. Then we give several examples of infinitely many (parametrized) cubic number fields, which have such an extension.

1.

1.1. Let $K = Q(\pi)$ be an algebraic number field of odd prime degree l such that

$$\pi^l + a_1 \pi^{l-1} + a_2 \pi^{l-2} + \ldots + a_l = 0,$$

where $a_i \in Z$ satisfy the above congruences in 1) and 2). We suppose that $K \neq k^+$ and K is real. Let $\mathfrak{l}$ be the prime ideal in K dividing l: $(l) = \mathfrak{l}^l$. Then we have $\mathfrak{l} \| \pi$ and so $(\pi) = \mathfrak{l}\mathfrak{c}$ with $(\mathfrak{l}, \mathfrak{c}) = 1$. We know that, for any integer γ in K with $\mathfrak{l} \nmid \gamma$, we have $N_K \gamma^{l-1} \equiv 1 \pmod{l^2}$ (cf. [2], Chap. 5). Hence we can consider the subgroup

$$G_l = \{\mathrm{Cl}(\mathfrak{a}) \mid (\mathfrak{a}, \mathfrak{l}) = 1 \text{ and } N\mathfrak{a}^{l-1} \equiv 1 \pmod{l^2}\}$$

of the ideal class group C_K of K, where $\mathrm{Cl}(\mathfrak{a})$ denotes the ideal class containing an ideal $\mathfrak{a}$. The subgroup G_l corresponds to the abelian extension $L = k^+ K$ of K in the sense of class field theory (Translation theorem) and so we have

$$(C_K : G_l) = [L : K] = l.$$

Since $(\pi) = \mathfrak{l}\mathfrak{c}$ and $\pm a_l = |N_K \pi| = N\mathfrak{l}\, N\mathfrak{c} = lN\mathfrak{c}$, we have $\mathrm{Cl}(\mathfrak{c}) = \mathrm{Cl}(\mathfrak{l})^{-1}$ and

$$\begin{aligned} \mathrm{Cl}(\mathfrak{c}) \in G_l &\Leftrightarrow N\mathfrak{c}^{l-1} \equiv 1 \pmod{l^2} \\ &\Leftrightarrow (a_l/l)^{l-1} \equiv 1 \pmod{l^2} \\ &\Leftrightarrow a_l/l \equiv d^l \pmod{l^2} \quad \text{with some } d \in Z \\ &\Leftrightarrow a_l \equiv l d^l \pmod{l^3}. \end{aligned}$$

Consequently, if $a_l \not\equiv l d^l \pmod{l^3}$ for any $d \in Z$, we have

$$\mathrm{Cl}(\mathfrak{l}) = \mathrm{Cl}(\mathfrak{c})^{-1} \notin G_l.$$

Then, as $(C_K : G_l) = l$, we have

$$C_K = \langle \mathrm{Cl}(\mathfrak{l}) \rangle \cdot G_l.$$

Furthermore, in this case, suppose that there exists an unramified cyclic extension M of K such that $[M : K] = l^2$ and $M \supset L \supset K$. Then M corresponds to a subgroup H_l of C_K such that

$$C_K \supset G_l \supset H_l \quad \text{and} \quad C_K/H_l \text{ is cyclic of order } l^2.$$

As $(G_l : H_l) = l$, i.e. $G_l^l \subset H_l$ and $\mathrm{Cl}(\mathfrak{l})^l = \mathrm{Cl}((l)) = 1$, we have $C_K^l \subset H_l$. This contradicts the fact that C_K/H_l is cyclic of order l^2.

Therefore our first assertion is:

(I) *If $a_l \not\equiv l d^l \pmod{l^3}$ for any $d \in Z$, then there is no unramified cyclic extension of K of degree l^2 containing $L = k^+ K$.*

Accordingly, in consideration of our problem, we may suppose that we have $a_l \equiv l d^l \pmod{l^3}$ with some $d \in Z$. Then there is $c \in Z$ such that $cd \equiv 1 \pmod{l^2}$ and $\pi' = c\pi$ satisfies

$$\pi'^l + a_1' \pi'^{l-1} + \ldots + a_l' = 0,$$

where $a_i' = c^i a_i$. We see easily that $a_1', a_2', \ldots, a_l' \in Z$ satisfy the above congruences in 1) and 2) and $a_l' = c^l a_l \equiv (cd)^l l \equiv l \pmod{l^3}$. Hence we may assume that

$$a_l \equiv l \pmod{l^3},$$

i.e. $a_l = lb$ with $b \in Z$, $b \equiv 1 \pmod{l^2}$.

1.2. Remark. By similar reasoning, we have the following assertion:

Let p be a prime. Let $K = Q(\varrho)$ be an algebraic number field of degree l such that

$$\varrho^l + b_1 \varrho^{l-1} + b_2 \varrho^{l-2} + \ldots + b_l = 0,$$

where $b_i \in Z$, $b_1 \equiv b_2 \equiv \ldots \equiv b_l \equiv 0 \pmod{p}$ and $b_l \not\equiv 0 \pmod{p^2}$. Then we have $(p) = \mathfrak{p}^l$ with a prime ideal $\mathfrak{p}$ in K. Suppose

$$p \equiv 1 \pmod{l}$$

and let k_p^+ be the unique subfield, of degree l, of the pth cyclotomic field. We suppose $K \neq k_p^+$ and then it is shown that $k_p^+ K$ is an unramified cyclic extension of K of degree l (cf. [2], Chap. 3).

So, in this case, there also occurs a similar problem as in Introduction.

Consider the subgroup

$$G_p = \{\mathrm{Cl}(\mathfrak{a}) \mid (\mathfrak{a}, \mathfrak{p}) = 1 \text{ and } N\mathfrak{a}^{(p-1)/l} \equiv 1 \pmod{p}\}$$

of C_K which corresponds to the abelian extension $k_p^+ K$. Then if $b_l \not\equiv p d^l \pmod{p^2}$ for any $d \in Z$, we can also prove that we have $C_K = \langle \mathrm{Cl}(\mathfrak{p}) \rangle \cdot G_p$.

Consequently, we see that if $b_l \not\equiv p d^l \pmod{p^2}$ for any $d \in Z$, then there is no unramified cyclic extension of K of degree l^2, containing $k_p^+ K$.

2. From now on, we treat the cubic case, i.e. $l = 3$ and let $K = Q(\pi)$ and a_1, a_2, a_3 be the same as in Section 1 ($l = 3$). We use the following notation:

ζ = a primitive 3rd root of unity,

η = a primitive 9th root of unity (such that $\eta^3 = \zeta$),

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

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

$\mathfrak{l}'$ = the prime ideal in K', dividing 3, so

$$(3) = \mathfrak{l}'^6, \quad \mathfrak{l}'^2 \| \pi \quad \text{and} \quad (1-\zeta) = \mathfrak{l}'^3.$$

We have $[L':K']=3$ and let $\mathrm{Gal}(L'/K')=\langle\tau\rangle$, where $\eta^\tau=\eta\zeta$. Moreover, let J be the complex conjugation. We note that, as K is real, J is an automorphism of K' and L' over K.

2.1. As preliminaries, we state two (well-known) results.

(a) *Algebraic aspect.* For an arbitrary element $\alpha\in K'$ $(\alpha\neq 0)$, put $\theta=\sqrt[3]{\eta\alpha}$ (a fixed 3rd root of $\eta\alpha$). First we note that θ is not in L', i.e. $\eta\alpha$ is not a cube in L'. In fact, we have

$$\eta\alpha=\beta^3\ (\beta\in L')\ \Rightarrow\ \zeta\alpha^3=(N_{L'/K'}\beta)^3$$
$$\Rightarrow\ \zeta \text{ is a cube in } K'\ \Rightarrow\ L'=K' \text{ (contradiction).}$$

Then, by Kummer theory, $M'=L'(\sqrt[3]{\eta\alpha})=K'(\sqrt[3]{\eta\alpha})$ is a cyclic extension of K' such that $[M':K']=3^2$ and $M'\supset L'$. (Conversely, every cyclic extension of K' of degree 3^2, containing L' is obtained in this way.)

Proof. We have $[M':K']=[M':L'][L':K']=9$. Also M' is a minimal splitting field of $(X^3-\eta\alpha)(X^3-\eta\alpha\zeta)(X^3-\eta\alpha\zeta^2)=X^9-\zeta\alpha^3\in K'[X]$. Hence M' is an abelian extension of K'. Let $\sigma\in\mathrm{Gal}(L'/K')$ such that $\sigma|L'=\tau$. Then $(\theta^\sigma)^3=(\eta\alpha)^\tau=\eta\zeta\alpha=\theta^3\zeta$ and so

$$\theta^\sigma=\theta\eta\zeta^i \quad \text{with some } i\in\boldsymbol{Z},$$

which shows $\theta^{\sigma^2}=\theta\eta^2\zeta^{2i+1}$, $\theta^{\sigma^3}=\theta\eta^3\neq\theta$ and so $\mathrm{ord}\,\sigma>3$. Hence we have $\mathrm{Gal}(L'/K')=\langle\sigma\rangle$.

Moreover if we have

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

then M' is an abelian extension of K of degree 18.

Proof. As $\alpha\alpha^J\in K'\cap\boldsymbol{R}=K$, we may take γ in K. Then $(\theta^J)^3=\eta^J\alpha^J=\eta^{-1}\alpha^J$ and so $(\theta\theta^J)^3=\alpha\alpha^J=\gamma^3$, i.e. $\theta\theta^J/\gamma=1$ as a real 3rd root of 1, which shows

$$\theta^J=\gamma\theta^{-1}.$$

Hence J and σ generate the (whole) automorphism group (of order 18) of M' over K and so M' is a Galois extension of K. Furthermore

$$\theta^{J\sigma}=(\gamma\theta^{-1})^\sigma=\gamma\theta^{-1}\eta^{-1}\zeta^{-i}$$

and

$$\theta^{\sigma J}=(\theta\eta\zeta^i)^J=\gamma\theta^{-1}\eta^{-1}\zeta^{-i};$$

so we see $\sigma J=J\sigma$ on $M'=K'(\theta)$.

Then the fixed subfield M, by $\langle J\rangle$, of M' is a cyclic extension of K such that $[M:K]=3^2$ and $M\supset L=k^+K$. As a remark, M is a minimal splitting field of

$$(X^9-\zeta\alpha^3)(X^9-(\zeta\alpha^3)^J)\in K[X].$$

(b) *Arithmetic aspect.* Similarly as in (a), let $M'=L'(\sqrt[3]{\eta\alpha})$ with $\alpha\in K'$ $(\alpha\neq 0)$. We suppose that α satisfies $(*)$ and let M be the fixed subfield, by $\langle J\rangle$, of M'.

As L' is unramified over K' and $([M:K],[K':K])=1$, the unramifiedness of M over K is equivalent to that of M' over L'. Then, by the ramification theory in Kummer extensions of prime degree (cf. [1], Ia, § 11), it is also equivalent, under the condition $(\alpha,\mathfrak{l}')=1$, to the two facts:

(1) the principal ideal $(\eta\alpha)=(\alpha)$ is the cube of an ideal in L',

(2) $\eta\alpha$ is congruent to the cube of an integer in L' modulo $\mathfrak{L}'^9$ for any prime divisors $\mathfrak{L}'$ of $\mathfrak{l}'$ in L'. (Note $\mathfrak{L}'\|\mathfrak{l}'$ and so $\mathfrak{L}'^3\|(1-\zeta)$.)

Of course, we can easily modify these results (a) and (b) for the case of arbitrary odd prime degree.

2.2. Now we assume that the coefficients of the minimal polynomial of π $(K=\boldsymbol{Q}(\pi))$ satisfy the following congruence conditions modulo 3^3:

$$a_3\equiv 3 \pmod{3^3},$$

i.e.

$$a_3=3b \quad (b\in\boldsymbol{Z},\ b\equiv 1 \pmod{3^2}) \quad \text{(as remarked in Section 1);}$$

$$a_1+a_3\equiv 0 \pmod{3^3},$$

i.e.

$$a_1\equiv -a_3=-3b\equiv -3 \pmod{3^3};$$
$$a_2\equiv 0 \pmod{3^3}$$

(see the congruences 2) in Introduction). Then, as $3b^3\equiv 3b=a_3 \pmod{3^3}$, we have

$$\pi^3-3b\pi^2+3b^3\equiv\pi^3+a_1\pi^2+a_2\pi+a_3=0 \pmod{3^3=\mathfrak{l}'^{18}}.$$

We put

$$\omega=b(1-\zeta)/\pi \quad \text{and} \quad \varepsilon=1-\omega.$$

As $-\pi(\pi^2+a_1\pi+a_2)=a_3=3b$ and $\mathfrak{l}'^2\|\pi$, $\mathfrak{l}'^3\|1-\zeta$, we see that ω and ε are integers in K' and $\mathfrak{l}'\|\omega$, $\mathfrak{l}'\nmid\varepsilon$.

We consider the number

$$(\varepsilon^J)^3-\varepsilon^3\zeta=\{(\pi-b(1-\zeta^2))^3-(\pi-b(1-\zeta))^3\zeta\}/\pi^3$$

in K'. The numerator is equal to

$$(1-\zeta)\pi^3-3b\{(1-\zeta^2)-(1-\zeta)\zeta\}\pi^2$$
$$+3b^2\{(1-\zeta^2)^2-(1-\zeta)^2\zeta\}\pi-b^3\{(1-\zeta^2)^3-(1-\zeta)^3\zeta\}$$
$$=(1-\zeta)\{\pi^3-3b\pi^2+3b^3\},$$

which is congruent to 0 modulo $\mathfrak{l}'^3\cdot\mathfrak{l}'^{18}=\mathfrak{l}'^{21}$ as remarked above. Hence we have

$$(\varepsilon^J)^3-\varepsilon^3\zeta\equiv 0 \pmod{\mathfrak{l}'^{21-6}=\mathfrak{l}'^{15}}.$$

As a consequence, we see

$$\zeta\equiv(\varepsilon^J/\varepsilon)^3 \pmod{\mathfrak{l}'^{10}},$$

which implies that $\mathfrak{l}'$ is completely decomposed in $L=K'(\sqrt[3]{\zeta})$: $\mathfrak{l}'=\mathfrak{L}'_1\,\mathfrak{L}'_2\,\mathfrak{L}'_3$ in L (cf. [1], Ia, § 11).

We fix one of $\mathfrak{L}'_i$ $(i=1,2,3)$: e.g. $\mathfrak{L}'=\mathfrak{L}'_1$. Then we have

$$(\varepsilon^J)^3-\varepsilon^3\zeta=(\varepsilon^J)^3-(\varepsilon\eta)^3$$
$$=(\varepsilon^J-\varepsilon\eta)(\varepsilon^J-\varepsilon\eta\zeta)(\varepsilon^J-\varepsilon\eta\zeta^2)\equiv 0 \pmod{\mathfrak{L}'^{15}}.$$

Here we remark that, for $0\leqslant i<j\leqslant 2$,

$$(\varepsilon^J-\varepsilon\eta\zeta^i)-(\varepsilon^J-\varepsilon\eta\zeta^j)=\varepsilon\eta(\zeta^i-\zeta^j)$$

is exactly divisible by $\mathfrak{L}'^3$. Let $\mathfrak{L}'^{e_i}\|\varepsilon^J-\varepsilon\eta\zeta^i$ $(i=0,1,2)$ and suppose that (say) $e_0\geqslant e_1, e_2$. Then we have

$$e_0+e_1+e_2\geqslant 15 \quad\text{and so}\quad e_0\geqslant 5,\ e_1=e_2=3;$$

consequently we have

$$e_0\geqslant 15-6=9.$$

Hence we see that we have

$$\eta\varepsilon\zeta^i\equiv\varepsilon^J \pmod{\mathfrak{L}'^9} \quad\text{for some } i\ (=0,1 \text{ or } 2),$$

i.e.

$$\eta\varepsilon(\varepsilon^J)^2\equiv(\varepsilon^J)^3\zeta^{-i} \pmod{\mathfrak{L}'^9}.$$

The other prime divisors $\mathfrak{L}'_2$, $\mathfrak{L}'_3$ of $\mathfrak{l}'$ in L' can be written as $\mathfrak{L}'^{\tau}$ or $\mathfrak{L}'^{\tau^2}$. As $\eta^{\tau^j}=\eta\zeta^j$ and $\varepsilon,\ \varepsilon^J\in K'$, we have

$$\eta\varepsilon(\varepsilon^J)^2\equiv(\varepsilon^J)^3\zeta^{-i-j} \pmod{(\mathfrak{L}'^{\tau^j})^9}.$$

Therefore, as $\zeta\equiv(\varepsilon^J/\varepsilon)^3 \pmod{\mathfrak{l}'^9}$, we have

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

Moreover we have

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

That is, $\alpha=\varepsilon(\varepsilon^J)^2$ satisfies the conditions $(*)$ in (a) and (2) in (b) of 2.1.

Hence, by considering the extension $M'=L'\left(\sqrt[3]{\eta\varepsilon(\varepsilon^J)^2}\right)$ of K, our second assertion is:

(II) *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 K of degree 3^2, containing $L=k^+K$.*

Moreover we have easily a modified assertion:

(II′) *For an integer δ in K' such that*

$$\delta\equiv\varepsilon=1-\omega \pmod{\mathfrak{l}'^9},$$

if the principal ideal $(\delta(\delta^J)^2)$ is the cube of an ideal in L', then there exists an unramified cyclic extension M of K of degree 3^2, containing L.

2.3. As for the second (or the modified) assertion (II) (or (II′)) in 2.2, we have the following results:

(A) First, ε is a unit in K' if and only if $N_{K'/k}(\varepsilon)=\pm 1,\ \pm\zeta$ or $\pm\zeta^2$. We have

$$N_{K'/k}(\varepsilon)=\zeta$$
$$\Leftrightarrow b^3(1-\zeta)^3+a_1b^2(1-\zeta)^2+a_2b(1-\zeta)+3b=3b\zeta \quad (a_3=3b)$$
$$\Leftrightarrow b^3(1-\zeta)^2+a_1b^2(1-\zeta)+a_2b+3b=0$$
$$\Leftrightarrow b^3=-2b^3-a_1b^2=b^3+a_1b^2+a_2b+3b$$
$$\Leftrightarrow a_1=-3b,\ a_2=3(b^2-1).$$

(We can easily see that the other cases, i.e. $N_{K'/k}(\varepsilon)=\pm 1,\ -\zeta$ or $\pm\zeta^2$ do not occur.)

Consequently, we see that if

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

(note: $a_1+a_3\equiv 0,\ a_2\equiv 0 \pmod{3^3}$), then the conclusion of the second assertion (II) holds; that is, our extension M exists.

Here we remark that, in this case, the minimal polynomial of $\pi-b$ is given by

$$(X+b)^3-3b(X+b)^2+3(b^2-1)(X+b)+3b=X^3-3X+b^3.$$

We see easily that $-(N_{K'/K}(\varepsilon))^{-1}=b\pi+1$ is a unit in K (also see the relation: $\pi^3/3=(b\pi+1)(\pi-b)$). Hence we can restate the above result as follows: Let $K=\boldsymbol{Q}(\beta)$ be a cubic number field, where the minimal polyno-

mial of β is

$$X^3-3X+b^3\in Z[X] \quad \text{with } b\equiv 1 \pmod{3^2}.$$

We note that the discriminant of this polynomial is equal to $-27(b^6-4)$ and so K is not totally real, provided $b\neq 1$. Then K has an unramified cyclic extension M such that $[M:K]=3^2$ and $M\supset L=k^+K$. And $1+b(\beta+b)=1+b\beta+b^2$ is a unit of K.

Moreover, as a remark, we can show that there exist infinitely many such cubic number fields. In fact, let S be a finite set of primes. For any $p\notin S$ with $p\equiv 2 \pmod 3$ ($p\neq 2$), we can find $c\in Z$ such that $p\| c^3-2$. Then, for $b\in Z$ with $b\equiv 1 \pmod{3^2}$ and $b\equiv c \pmod{p^2}$, the discriminant $-27(b^6-4)=-27(b^3-2)(b^3+2)$ of X^3-3X+b^3 is exactly divisible by p; that is, p is totally ramified in $K=Q(\beta)$, where $\beta^3-3\beta+b^3=0$.

(B) Next, let

$$\delta=\varepsilon+(b-1)=b(\pi-(1-\zeta))/\pi,$$

which is an integer in K', prime to $\mathfrak{l}'$; as $b\equiv 1 \pmod{3^2=\mathfrak{l}'^{12}}$, we have

$$\delta\equiv\varepsilon \pmod{\mathfrak{l}'^9}.$$

Suppose that a prime ideal $\mathfrak{p}'$ in K' divides $\pi-(1-\zeta)$. Then

$$\begin{aligned}0&=\pi^3+a_1\pi^2+a_2\pi+3b \quad (a_3=3b)\\ &\equiv(1-\zeta)^3+a_1(1-\zeta)^2+a_2(1-\zeta)+3b\\ &=(a_2+3b-3)-(3a_1+a_2+6)\zeta \pmod{\mathfrak{p}'}.\end{aligned}$$

Hence if

$$a_2+3b-3=0,\quad 3a_1+a_2+6=-3,\quad \text{i.e.}\quad a_2=-3(b-1),\quad a_1=b-4,$$

then we see that $\mathfrak{p}'$ divides 3, which implies $\mathfrak{p}'=\mathfrak{l}'$ and so the principal ideal $(\pi-(1-\zeta))$ is a power of $\mathfrak{l}'$. As δ is an integer, prime to $\mathfrak{l}'$, we have $(\delta)=(b)\mathfrak{l}'^2/(\pi)$. Here clearly $(b)^J=(b)$, $(\pi)^J=(\pi)$ and, as the unique prime divisor of 3 in K', $\mathfrak{l}'^J=\mathfrak{l}'$. Hence we have

$$(\delta^J)=(\delta)^J=(\delta) \quad \text{and so} \quad (\delta(\delta^J)^2)=(\delta)^3.$$

Moreover if we assume $b\equiv 1 \pmod{3^3}$, then

$$a_1+a_3=4(b-1)\equiv 0 \pmod{3^3}.$$

Consequently, we see that if

$$a_1=b-4,\quad a_2=-3(b-1),\quad a_3=3b \quad (b\equiv 1 \pmod{3^3})$$

(note: $a_1+a_3\equiv 0$, $a_2\equiv 0 \pmod{3^3}$), then the conclusion of the second modified assertion (II') holds; that is, our extension M exists.

Summarizing the results (A) and (B), our third assertion is:

(III) *Let $K=Q(\pi)$ be a cubic number field, where the minimal polynomial of π is*

$$X^3-3bX^2+3(b^2-1)X+3b\in Z[X] \quad (b\equiv 1 \pmod{3^2})$$

or

$$X^3+(b-4)X^2-3(b-1)X+3b\in Z[X] \quad (b\equiv 1 \pmod{3^3}),$$

then K has an unramified cyclic extension, of degree 3^2, containing $L=k^+K$ (where $k^+=Q(\eta+\eta^{-1})=Q(\cos 40^\circ)$). And so the ideal class group of K contains a cyclic subgroup of order 3^2.

2.4. Under the congruence conditions on a_1, a_2, a_3 as in 2.2 we investigate the ω-adic expansions of several integers in K' and in L', where $\omega=b(1-\zeta)/\pi$ ($\mathfrak{l}'\|(\omega)$). We omit cumbersome calculations and only state several obtained results. Let $O_{K'}$ and $O_{L'}$ be the rings of integers in K' and L' respectively.

Since $\mathfrak{l}'$ is totally ramified in K', we can take $\{0, 1, -1\}$ as a representative system of the residue field $O_{K'}/\mathfrak{l}'$.

Then we have

$$\begin{aligned}-3&\equiv\omega^6,\\ \pi&\equiv\omega^2+\omega^5-\omega^6-\omega^7-\omega^8-\omega^9 \pmod{\mathfrak{l}'^{10}},\\ \zeta&\equiv 1-\omega^3-\omega^6+\omega^9.\end{aligned}$$

Accordingly we have

$$\zeta\equiv(1-\zeta-\zeta^2)^3 \pmod{\mathfrak{l}'^{10}},$$

which implies that $\mathfrak{l}'$ is completely decomposed in L': $\mathfrak{l}'=\mathfrak{L}'_1\mathfrak{L}'_2\mathfrak{L}'_3$ (see 2.2).

So we can also take $\{0, 1, -1\}$ as a representative system of the residue fields $O_{L'}/\mathfrak{L}'_i$ ($i=1, 2, 3$). We fix one of $\mathfrak{L}'_i$: e.g. $\mathfrak{L}'=\mathfrak{L}'_1$. Then, by a suitable choice of η (a primitive 9th root of unity), we have

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

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

$$\eta(1-\omega)\equiv 1+\omega+\omega^4-\omega^7-\omega^8\equiv 1-\omega^J \pmod{\mathfrak{L}'^9}.$$

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

$$\eta\varepsilon\equiv\varepsilon^J \pmod{\mathfrak{L}'^9}, \quad \text{i.e.} \quad \eta\varepsilon(\varepsilon^J)^2\equiv(\varepsilon^J)^3 \pmod{\mathfrak{L}'^9}.$$

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

$$\eta\varepsilon(\varepsilon^J)^2\equiv(\varepsilon^J)^3\zeta^{-J}\equiv(\varepsilon^J(1-\omega-\omega^2)^{-J})^3 \pmod{\mathfrak{L}'^9_i}.$$

These are the congruences obtained in 2.2.

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

$$\eta\xi \equiv \xi^J \beta^3 \pmod{\mathfrak{L}'^9} \quad \text{with } \beta \in O_{K'}$$

because this congruence implies

$$\eta\xi(\xi^J)^2 \equiv (\xi^J\beta)^3 \pmod{\mathfrak{L}'^9} \quad \text{and} \quad \big(\xi(\xi^J)^2\big)\big(\xi(\xi^J)^2\big)^V = (\xi\xi^J)^3;$$

that is, $\alpha = \xi(\xi^J)^2$ satisfies the conditions (*) in (a) and (2) in (b) of 2.1.

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

$$\xi/\varepsilon \equiv (\xi/\varepsilon)^J \beta^3 \pmod{\mathfrak{l}'^9}.$$

It is proved that, for any $\gamma \in O_{K'}$ ($\gamma \equiv 1 \pmod{\mathfrak{l}'}$), we have

$$\gamma \equiv \gamma^J\beta^3, \quad \text{i.e.} \quad \xi \equiv \varepsilon\gamma \pmod{\mathfrak{l}'^9}$$

if and only if

$$\gamma \equiv \lambda\mu^3 \pmod{\mathfrak{l}'^9},$$

where $\lambda, \mu \in O_{K'}$ ($\lambda, \mu \equiv 1 \pmod{\mathfrak{l}'}$) such that $\lambda \equiv \lambda^J \pmod{\mathfrak{l}'^9}$. Moreover we see that we have

$$\lambda\mu^3 \equiv 1 + B\omega^2 + C\omega^3 + D\omega^4 + (B+BC)\omega^5 + F\omega^6 + (CD - C - D)\omega^7 + H\omega^8 \pmod{\mathfrak{l}'^9}$$

$$(B, C, D, F, H \in \{0, 1, -1\}).$$

Consequently, for $\xi \in O_{K'}$ ($\xi \equiv 1 \pmod{\mathfrak{l}'}$) such that

$$\xi \equiv \varepsilon\gamma, \quad \text{i.e.} \quad \equiv \varepsilon\lambda\mu^3 \pmod{\mathfrak{l}'^9},$$

if the principal ideal $(\xi(\xi^J)^2)$ is the cube of an ideal in L, then the extension $M' = L\big(\sqrt[3]{\eta\xi(\xi^J)^2}\big)$ has a subfield M, which is an unramified cyclic extension of K such that $[M:K] = 3^2$ and $M \supset L$.

We note that, as $\varepsilon = 1-\omega$ and $\gamma \equiv 1 \pmod{\mathfrak{l}'^2}$, we have

$$\xi \equiv \varepsilon\gamma \equiv 1-\omega \pmod{\mathfrak{l}'^2}.$$

So, considering the above ω-adic expansions of $\lambda\mu^3 \pmod{\mathfrak{l}'^9}$, we see that, among 3^7 classes of $O_{K'}/\mathfrak{l}'^9$ containing an integer $\equiv 1-\omega \pmod{\mathfrak{l}'^2}$, there are exactly 3^5 classes containing some $\varepsilon\gamma$ as above.

References

[1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica-Verlag, Würzburg-Wien 1970.

[2] M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Math. 555, Springer-Verlag, Berlin–Heidelberg–New York 1976.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
2-1-1, Fukasawa, Setagaya
Tokyo 158, Japan

Received on 4. 11. 1986 (1686)

ACTA ARITHMETICA
LI (1988)

Stabilität bei symmetrischen h-Basen

von

CHRISTOPH KIRFEL (Bergen, Norwegen)

1. Einleitung. Da symmetrische Basen eine große Rolle im Frobenius- und im Reichweitenproblem spielen, wollen wir zunächst Frobeniuszahl und Reichweite einer Basis natürlicher Zahlen definieren.

Sei $B_k = \{b_1, b_2, \ldots, b_k\} \subseteq N$, $(b_1, b_2, \ldots, b_k) = 1$, so ist die *Frobeniuszahl* $g(B_k)$ die größte nicht mit B_k darstellbare ganze Zahl. Dabei wollen wir in unseren Darstellungen nur nicht-negative ganzzahlige Koeffizienten zulassen:

$$g(B_k) = \max\{n \in \mathbf{Z} \mid n \text{ nicht darstellbar als } \sum_{j=1}^{k} x_j b_j,\ x_j \in N_0,\ b_j \in B_k\}.$$

Dabei verstehen wir unter N_0 die Menge der natürlichen Zahlen einschließlich der Null.

Sei nun $A_k = \{a_1, a_2, \ldots, a_k\} \subseteq N$ mit $a_1 = 1 < a_2 < \ldots < a_k$. Dann sind alle natürlichen Zahlen mit A_k darstellbar, und wir können nach der Anzahl der Summanden in einer Darstellung fragen. Mit hA_k wollen wir die Menge derjenigen Zahlen bezeichnen, die mit höchstens h Summanden aus A_k darstellbar sind:

$$hA_k = \{n \in N_0 \mid n = \sum_{j=1}^{k} x_j a_j,\ x_j \in N_0,\ a_j \in A_k,\ \sum_{j=1}^{k} x_j \leqslant h\}.$$

A_k nennen wir dann eine *h-Basis* oder einfach eine *Basis*.

Wir betrachten nun die kleinste Zahl N, die nicht mit höchstens h Summanden aus A_k dargestellt werden kann. Wir nennen $N-1$ die *h-Reichweite* $n_h(A_k)$ von A_k:

$$n_h(A_k) = \min\{n \in N \mid n \notin hA_k\} - 1.$$

Wir setzen $n_0(A_k) = 0$.

Mit h_0 möchten wir die kleinste Summandenanzahl, bei der die Reichweite erstmals das größte Element a_k überschreitet, bezeichnen:

$$h_0 = h_0(A_k) = h_0^{(k)} = \min\{h \in N_0 \mid n_h(A_k) \geqslant a_k\}.$$