TOKYO J. MATH.
VOL. 6, NO. 2, 1983

On the Construction of Certain Number Fields

Shin NAKANO

Gakushuin University
(Communicated by T. Mitsui)

Introduction

By a number field, we mean in this paper any finite extension of the field Q of rational numbers. For any natural number n, ζ_n means a primitive n-th root of unity. Let l be an odd prime fixed throughout this paper.

It was proved by Yahagi [8] that there exist infinitely many number fields whose l-class groups are isomorphic to any given finite abelian l-group. Some weaker results had been obtained by Gerth [1] and Iimura [5]. The degrees of those number fields given in [1], [5] and [8] are all divisible by l, and the methods in these papers do not seem to yield any number fields with degree relatively prime to l, even if we require these fields to satisfy only a weaker condition to have the class number divisible by l.

On the other hand, Satgé [7] constructed infinitely many quadratic extensions of $Q(\zeta_l+\zeta_l^{-1})$, whose class numbers are divisible by l. This is a generalization of the result in Honda [4] where the case $l=3$ is treated.

In this paper, we shall give one of the ways of constructing extensions K of a given number field k (satisfying a few conditions given below), such that $[K:k]|l-1$ and the class numbers of K are divisible by l. We shall show that there exist infinitely many such extensions K. In particular, we can apply this to the case k is any proper subfield of $Q(\zeta_l)$, and get a similar result to Satgé's. We can show namely that there exist infinitely many extensions of k with degree $l-1$ over Q, which are independent of $Q(\zeta_l)$ over k and whose class numbers are divisible by l.

Our method is based on the following simple idea. Let K be an arbitrary number field. According to the class field theory, the class number of K is divisible by l if and only if there exists an unramified

Received August 1, 1982

cyclic extension L/K of degree l. Furthermore, the existence of such an extension L/K is equivalent to the existence of an unramified Kummer extension $L'/K(\zeta_l)$ of degree l such that L'/K is abelian. So, the condition that the class number of K be divisible by l can be discribed in terms of the ramification theory of Kummer extension (Proposition 1). Now, we shall give a certain polynomial $f(X) \in k[X]$ (see below § 1) so that the field K defined by $f(X)=0$ satisfies the condition given in Proposition 1. Finally, we shall show, using local conditions, that infinitely many K's exist.

NOTATIONS. $\boldsymbol{Z}$ denotes as usual the ring of rational integers. For an arbitrary field K, $K^\times$ denotes its multiplicative group. If K is a number field, then $\mathfrak{o}_K$ denotes the ring of integers of K. Moreover for a prime ideal $\mathfrak{P}$ of K and $\alpha \in K^\times$, $\nu_{\mathfrak{P}}(\alpha)$ denotes the order of α at $\mathfrak{P}$.

§ 1. Preliminary propositions.

Let k be a number field such that $\zeta_l \notin k$. Put $k'=k(\zeta_l)$ and $m=[k': k]$. Then k'/k is cyclic of degree m and $m|l-1$. Assume that there exists a prime ideal $\mathfrak{l}$ of k which is totally ramified in k'. Note that $\mathfrak{l}|l$. Let G be the Galois group of k'/k, s be a generator of G and g be a positive integer such that $\zeta_l^s=\zeta_l^g$. We fix s and g. Then G is isomorphic to a subgroup of $(\boldsymbol{Z}/l\boldsymbol{Z})^\times$ under the map

$$G \ni s^i \longmapsto g^i \bmod l \in (\boldsymbol{Z}/l\boldsymbol{Z})^\times \ , \quad (0 \leqq i \leqq m-1) \ .$$

We denote by ω the element $\sum_{i=0}^{m-1} g^i s^{-i}$ of the group ring $\boldsymbol{Z}[G]$. Set

$$F(X, Y)=\prod_{t \in G}(X-\zeta_l^t Y) \ . \tag{$*$}$$

Then $F(X, Y) \in \mathfrak{o}_k[X, Y]$ and $F(X, 1)$ is the minimal polynomial of ζ_l over k. Take $h(X) \in \mathfrak{o}_k[X]$ which is constant or monic, $y \in \mathfrak{o}_k$ such that $h(0)$ and ly are relatively prime, and a unit ε of $\mathfrak{o}_k$. For these, we define a polynomial of $\mathfrak{o}_k[X]$

$$f(X)=F(X, ly)-\varepsilon h(X)^l \ .$$

Let θ be a root of $f(X)$. Put $K=k(\theta)$ and $K'=K(\zeta_l)$. The above notations ω, $h(X)$, y, ε, $f(X)$, θ, K and K' will be fixed throughout this paragraph. Denote by $f'(X)$ the derivative of $f(X)$. Then we get $f(X) \equiv X^m-\varepsilon h(X)^l$ (mod $\mathfrak{l}$) and $f'(X) \equiv mX^{m-1}$ (mod $\mathfrak{l}$). As $\mathfrak{l} \nmid m$ and $h(0)$ and ly are relatively prime, $f(X)$ mod $\mathfrak{l}$ is a separable polynomial of $(\mathfrak{o}_k/\mathfrak{l})[X]$. This implies that $\mathfrak{l}$ is unramified in K. As $\mathfrak{l}$ is totally ramified in k', we have $K \cap k'=k$.

Therefore the Galois group of K'/K can be identified with G, as we shall do in the following. The group ring $Z[G]$ acts on $K'^{\times}$.

LEMMA 1. *Let L'/K' be a cyclic extension of degree l. Then L' is abelian over K if and only if $L'=K'(\sqrt[l]{\alpha})$ for some $\alpha \in (K'^{\times})^{\omega}$.*

PROOF. See Long [5] § 1.

The following lemma is well-known in the theory of Kummer extension (e.g. Hecke [3] § 39).

LEMMA 2. *L'/K' is an unramified cyclic extension of degree l if and only if $L'=K'(\sqrt[l]{\alpha})$ for some $\alpha \in \mathfrak{o}_{K'}$, $\alpha \neq 0$, satisfying the following conditions:*

(1) $\alpha \notin K'^{l}$.

(2) $\nu_{\mathfrak{P}'}(\alpha) \equiv 0 \pmod{l}$ *for any prime ideal $\mathfrak{P}'$ of K'.*

(3) *α and l are relatively prime and the congruence $X^l \equiv \alpha \pmod{(1-\zeta_l)^l}$ is solvable in $\mathfrak{o}_{K'}$.*

The above two lemmas yield, in virtue of the class field theory as mentioned in the introduction, the following

PROPOSITION 1. *The class number of K is divisible by l if and only if there exists $\alpha \in \mathfrak{o}_{K'}$, $\alpha \neq 0$, satisfying the conditions* (1), (2) *and* (3) *of Lemma 2 and that $\alpha\gamma^l \in (K'^{\times})^{\omega}$ for some $\gamma \in K'^{\times}$.*

Now, set $\beta=\theta-ly\zeta_l$ and $\alpha=\beta^{\omega}$. These are the elements of $\mathfrak{o}_{K'}$.

LEMMA 3. (i) *$N_{K'/K}\beta=\varepsilon h(\theta)^l$, where $N_{K'/K}$ is the norm map from K' to K.* (ii) *No prime factor $\mathfrak{P}'$ of β of K' divides β^t for any $t \in G$, $t \neq 1$.* (iii) *All prime ideals $\mathfrak{P}$ of K dividing $h(\theta)$ are decomposed completely in K'.*

PROOF. By the definition of $F(X, Y)$, we have $N_{K'/K}\beta=F(\theta, ly)=\varepsilon h(\theta)^l$. To see (ii), assume $\beta \equiv \beta^{s^i} \equiv 0 \pmod{\mathfrak{P}'}$ for some $\mathfrak{P}'$ and $s^i \neq 1$. Then $ly\zeta_l(1-\zeta_l^{g^i-1}) \equiv 0 \pmod{\mathfrak{P}'}$. Since $g^i \not\equiv 1 \pmod{l}$, we have $1-\zeta_l^{g^i-1} | l$. Hence $ly \equiv 0 \pmod{\mathfrak{P}'}$ and $\theta \equiv 0 \pmod{\mathfrak{P}'}$. On the other hand, we have $h(\theta) \equiv 0 \pmod{\mathfrak{P}'}$, from (i). So we have $ly \equiv h(0) \equiv 0 \pmod{\mathfrak{P}'}$. This is a contradiction. (iii) is shown easily from (i) and (ii). So our lemma is proved.

PROPOSITION 2. *If $\alpha \notin K'^{l}$ then the class number of K is divisible by l.*

PROOF. By Proposition 1, it is sufficient to show that $\alpha=\beta^{\omega}$

satisfies the conditions (2) and (3) of Lemma 2. Let $\mathfrak{P}'$ be a prime ideal of K' and $\mathfrak{P}$ the prime ideal of K defined by $\mathfrak{P}=\mathfrak{P}'\cap\mathfrak{o}_K$. By Lemma 3, we have $\nu_{\mathfrak{P}'}(\beta)=0$ or $\nu_{\mathfrak{P}'}(\beta)=\nu_{\mathfrak{P}}(N_{K'/K}\beta)=\nu_{\mathfrak{P}}(\varepsilon h(\theta)^l)\equiv 0 \pmod l$. Therefore, we have $\nu_{\mathfrak{P}'}(\alpha)=\sum_{i=0}^{m-1} g^i\nu_{\mathfrak{P}'^{\sigma^i}}(\beta)=0 \pmod l$, for any prime ideal $\mathfrak{P}'$ of K'. So, (2) is satisfied. Next, $\beta\equiv\theta-ly \pmod{(1-\zeta_l)^l}$, as $(l)=(1-\zeta_l)^{l-1}$. Hence $\alpha=\beta^\omega\equiv\prod_{i=0}^{m-1}(\theta-ly)^{g^i} \pmod{(1-\zeta_l)^l}$. From the choice of $h(X)$ and y, we see easily that θ and l are relatively prime, and so are also α and l. We have $\sum_{i=0}^{m-1} g^i\equiv 0 \pmod l$, since $m\neq 1$. This shows that α satisfies (3), and the proof is completed.

Next, take a prime ideal $\mathfrak{p}$ of k such that $N\mathfrak{p}\equiv 1 \pmod l$ (where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$). Then we can find $u\in\mathfrak{o}_k$ satisfying the congruence $F(u, 1)\equiv 0 \pmod{\mathfrak{p}}$. For such u, set

$$\lambda_u=(lu)^{l-m}\prod_{i=1}^{m-1}(1-u^{\bar{g}^i-1})^{g^i-1}\,, \qquad (\sharp)$$

where $\bar{g}$ is a positive integer such that $\bar{g}g\equiv 1 \pmod l$. $\lambda_u \bmod \mathfrak{p}$ is uniquely determined in $(\mathfrak{o}_k/\mathfrak{p})^\times$ independing of the choice of $\bar{g}$ since $u^l\equiv 1$, $u\not\equiv 1 \pmod{\mathfrak{p}}$.

PROPOSITION 3. *If* (i) $f(X)$ *is irreducible,* (ii) $h(lyu)\equiv 0 \pmod{\mathfrak{p}}$ *and* (iii) $\varepsilon y^{l-m}\lambda_u$ *is not an l-th power* $\bmod\ \mathfrak{p}$, *then the class number of K is divisible by l.*

PROOF. By the choice of u, we have $F(lyu, ly)\equiv 0 \pmod{\mathfrak{p}}$. We first claim that there exists $x\in\mathfrak{o}_k$ such that $\mathfrak{p}\,\|\,F(x, ly)$ and $x\equiv lyu \pmod{\mathfrak{p}}$. It is sufficient to show this in case $F(lyu, ly)\equiv 0 \pmod{\mathfrak{p}^2}$. Set $\Phi(X)=F(X, ly)$ and take $\Psi(X)\in\mathfrak{o}_k[X]$ such that $\Phi(X)\Psi(X)=X^l-(ly)^l$. Then we have $\Phi'(lyu)\Psi(lyu)\equiv l(lyu)^{l-1} \pmod{\mathfrak{p}}$. Since ly and $h(0)$ are relatively prime, and consequently $y\not\equiv 0 \pmod{\mathfrak{p}}$, we get $\Phi'(lyu)\not\equiv 0 \pmod{\mathfrak{p}}$. Set $x=lyu+\pi$, where $\pi\in\mathfrak{p}-\mathfrak{p}^2$. Then, using Taylor's formula,

$$\Phi(x)\equiv\Phi(lyu)+\Phi'(lyu)\pi\equiv\Phi'(lyu)\pi\not\equiv 0 \pmod{\mathfrak{p}^2}\,,$$

and so we have $\mathfrak{p}\,\|\,F(x, ly)$ and $x\equiv lyu \pmod{\mathfrak{p}}$. Now, from (ii), $\mathfrak{p}\,|\,f(x)$. On the other hand, we have $N_{K/k}(\theta-x)=\pm f(x)$, since $f(X)$ is irreducible. Hence $\mathfrak{p}\,\|\,N_{K/k}(\theta-x)$. So there exists a prime ideal $\mathfrak{P}$ of K such that $N_{K/k}\mathfrak{P}=\mathfrak{p}$ and $\theta\equiv x \pmod{\mathfrak{P}}$. Then we have $N_{K'/K}\beta\equiv 0 \pmod{\mathfrak{P}}$, since $N_{K'/K}\beta=\varepsilon h(\theta)^l$, and there exists a prime ideal $\mathfrak{P}'$ of K' which divides β and $\mathfrak{P}$. As $\mathfrak{P}$ is decomposed completely in K', we have $N_{K'/k}\mathfrak{P}'=\mathfrak{p}$.

Next, we see $\theta\equiv ly\zeta_l \pmod{\mathfrak{P}'}$ since $\beta\equiv 0 \pmod{\mathfrak{P}'}$. On the other hand, $\theta\equiv x\equiv lyu \pmod{\mathfrak{P}}$. Therefore $u\equiv\zeta_l \pmod{\mathfrak{P}'}$ and we get

$$\beta^{s-i}=\theta-ly\zeta_l^{g^i}\equiv lyu(1-u^{g^i-1}) \pmod{\mathfrak{P}'}\ , \quad (1\leqq i\leqq m-1)\ .$$

Set $\alpha'=\alpha/h(\theta)^l$. Then $\alpha'\in\mathfrak{o}_{K'}$ and

$$\alpha'=\varepsilon\prod_{i=1}^{m-1}\beta^{s-i(g^i-1)}\equiv\varepsilon\prod_{i=1}^{m-1}\{(lyu)^{g^i-1}(1-u^{g^i-1})^{g^i-1}\} \pmod{\mathfrak{P}'}\ .$$

As we have $\sum_{i=1}^{m-1}(g^i-1)\equiv -m \pmod{l}$, we get

$$\alpha'\equiv v^l\varepsilon(lyu)^{l-m}\prod_{i=1}^{m-1}(1-u^{g^i-1})^{g^i-1}\equiv v^l\varepsilon y^{l-m}\lambda_u \pmod{\mathfrak{P}'}\ ,$$

for some $v\in\mathfrak{o}_k$ such that $\mathfrak{p}\nmid v$. Therefore, the assumption (iii) shows that α' is not an l-th power mod $\mathfrak{P}'$, since $N_{K'/k}\mathfrak{P}'=\mathfrak{p}$. Thus $\alpha'\notin K'^l$ and $\alpha\notin K'^l$. Our proposition follows from this and Proposition 2.

REMARK. It is easy to see that for $\mathfrak{p}$, u and ε there exists $y\in\mathfrak{o}_k$ satisfying (iii) of Proposition 3.

§2. Main theorem.

THEOREM. *Let k be a number field such that $\zeta_l\notin k$ and assume that there exists a prime ideal of k which is totally ramified in $k(\zeta_l)$. Set $m=[k(\zeta_l): k]$. Then there exist infinitely many number fields K with the following properties*:

(a) *$K=k(\theta)$, θ being any root of the polynomial $f(X)=F(X, ly)-z^l$, where $F(X, Y)$ is the polynomial of $\mathfrak{o}_k[X, Y]$ as defined by (*) and y, z are suitably chosen elements of $\mathfrak{o}_k$.*

(b) *The class number of K is divisible by l.*

(c) *$K\cap k(\zeta_l)=k$.*

(d) *$[K: k]=m$.*

Furthermore, in case $\zeta_m\notin k$, we may add the following condition on K:

(e) *K/k is non-Galois.*

PROOF. We apply Proposition 3 with $\varepsilon=1$ and $h(X)=$constant. Recall that $k(\zeta_l)/k$ is cyclic and $F(X, 1)$ is the minimal polynomial of ζ_l over k. So, there exists a prime ideal $\mathfrak{p}_1$ of k such that $F(X, 1) \bmod \mathfrak{p}_1$ is irreducible in $(\mathfrak{o}_k/\mathfrak{p}_1)[X]$. Next, take a prime ideal $\mathfrak{p}_2$ of k and $u\in\mathfrak{o}_k$ satisfying the congruences $N\mathfrak{p}_2\equiv 1 \pmod{l}$ and $F(u, 1)\equiv 0 \pmod{\mathfrak{p}_2}$. Obviously $\mathfrak{p}_1\neq\mathfrak{p}_2$ because $\mathfrak{p}_1$ is inert while $\mathfrak{p}_2$ is decomposed completely in $k(\zeta_l)$. Let λ_u be defined by (#). Take $y, z\in\mathfrak{o}_k$ such that

(i) $ly\equiv 1 \pmod{\mathfrak{p}_1}$,

(ii) $y^{l-m}\lambda_u$ is not an l-th power mod $\mathfrak{p}_2$,

(iii) $z\equiv 0 \pmod{\mathfrak{p}_1}$,

(iv) $z \equiv 0 \pmod{\mathfrak{p}_2}$,

(v) ly and z are relatively prime.

It is clear that such y, z exist. Let θ be any root of $f(X)=F(X, ly)-z^l$ and $K=k(\theta)$. Then (c) is shown in §1. From (i) and (iii), we have $f(X) \equiv F(X, 1) \pmod{\mathfrak{p}_1}$. So $f(X)$ is irreducible in $\mathfrak{o}_k[X]$ by the choice of $\mathfrak{p}_1$. Then, by Proposition 3, (b) and (d) are satisfied.

Next, we consider the case $\zeta_m \notin k$. We can find a prime ideal $\mathfrak{p}_3$ of k which is not decomposed completely in $k(\zeta_m)$. We may assume that $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are distinct and $\mathfrak{p}_3 \nmid m$. Then it is easy to see that y, z can be chosen so that the following additional conditions are satisfied:

(vi) $ly \equiv 0 \pmod{\mathfrak{p}_3}$,

(vii) $z \equiv 1 \pmod{\mathfrak{p}_3}$.

In this case, we have $f(X) \equiv X^m - 1 \pmod{\mathfrak{p}_3}$. Therefore $\mathfrak{p}_3$ has a prime divisor in K with relative degree 1. Assume that K/k is Galois. Then $f(X) \bmod \mathfrak{p}_3$ factors into a product of distinct linear factors in $(\mathfrak{o}_k/\mathfrak{p}_3)[X]$. This shows that $\mathfrak{p}_3$ is decomposed completely in $k(\zeta_m)$, since the minimal polynomial of ζ_m over k is the irreducible factor of X^m-1. This contradicts the choice of $\mathfrak{p}_3$, and (e) is satisfied.

To see that there are infinitely many choices of $K=k(\theta)$, it is sufficient to show that, for any finite set S of such K's, there exists another field with properties (a)-(d) (and also (e) in case $\zeta_m \notin k$) which is not contained in S. Let $S=\{K_1, \cdots, K_n\}$. For each i $(1 \leqq i \leqq n)$, we can find a prime ideal $\mathfrak{Q}_i \nmid l$ of K_i which is not decomposed completely in $K_i(\zeta_l)$. Put $\mathfrak{q}_i = \mathfrak{Q}_i \cap \mathfrak{o}_k$ and $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Choose prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ (and $\mathfrak{p}_3$, if $\zeta_m \notin k$) as above which do not divide $\mathfrak{a}$. Then we can find y, z satisfying in addition to (i)-(v) (and (vi), (vii), if $\zeta_m \notin k$) also the condition:

(viii) $z \equiv 0 \pmod{\mathfrak{a}}$.

Now, the field K defined as above for such y, z satisfies the properties (a)-(d) (and also (e) in case $\zeta_m \notin k$), and every prime ideal of K lying above $\mathfrak{q}_i$ is decomposed completely in $K(\zeta_l)$ by Lemma 3 $(1 \leqq i \leqq n)$. Hence $K \notin S$ and our theorem is proved.

COROLLARY 1. *For any proper subfield M of $\boldsymbol{Q}(\zeta_l)$, there exist infinitely many number fields K satisfying the following conditions:*

(a) *The class number of K is divisible by l.*

(b) $K \cap \boldsymbol{Q}(\zeta_l) = M$.

(c) $[K : \boldsymbol{Q}] = l-1$.

If $[\boldsymbol{Q}(\zeta_l) : M] > 2$ i.e., $M \neq \boldsymbol{Q}(\zeta_l + \zeta_l^{-1})$, we may add the following condition on K.

(d) *K/M is non-Galois (therefore $K/\boldsymbol{Q}$ is also non-Galois).*

COROLLARY 2. *For a given divisor $m \neq 1$ of $l-1$, there exist infinitely many extensions of $\boldsymbol{Q}(\zeta_l)$ of degree m whose class numbers are divisible by l.*

References

[1] F. GERTH III, Number fields with prescribed l-class group, Proc. Amer. Math. Soc., **49** (1975), 284–288.

[2] G. GRAS, Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l, Ann. Inst. Fourier, vol. **23**, no. 3 (1973), 1–48.

[3] E. HECKE, Vorlesungen über die Theorie der Algebraischen Zahlen, Chelsea, New York, 1970.

[4] T. HONDA, On real quadratic fields whose class numbers are multiple of 3, J. Reine Angew. Math., **233** (1968), 101–102.

[5] K. IIMURA, On the l-class group of an algebraic number field, J. Reine Angew. Math., **322** (1981), 136–144.

[6] R. LONG, Steinitz classes of cyclic extensions of prime degree, J. Reine Angew. Math., **250** (1971), 87–98.

[7] P. SATGÉ, Corps résolubles et divisibilité de nombres de classes d'idéaux, Enseignement Math., **25** (1979), 165–188.

[8] O. YAHAGI, Construction of number fields with prescribed l-class groups, Tokyo J. Math., **1** (1978), 275–283.

[9] Y. YAMAMOTO, On unramified Galois extensions of quadratic number fields, Osaka J. Math., **7** (1970), 57–76.

Present Address:
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
GAKUSHUIN UNIVERSITY
MEJIRO, TOSHIMA-KU
TOKYO 171