52. A Note on Capitulation Problem for Number Fields. II

By Kenkichi IWASAWA
Princeton University

(Communicated by Shokichi IYANAGA, M. J. A., June 13, 1989)

In the present note, we shall again consider a capitulation problem for number fields which we discussed in our earlier paper [2]. Using some properties of Z_p-extensions of number fields, we shall prove the following:

Proposition. *For each prime number $p\geqslant 2$, there exist infinitely many finite algebraic number fields k such that the p-class group of k capitulates in a proper subfield of Hilbert's p-class field over k.*

We note that in the special case $p=2$, the proposition was proved in [2] by elementary argument.

1. Let M be any number field, finite or infinite over the rational field $\boldsymbol{Q}$. Throughout the following, we fix a prime number $p\geqslant 2$ and denote by $A(M)$ the p-primary component of the ideal class group of M; if M is finite over $\boldsymbol{Q}$, this is the p-class group of M, denoted by $C_{M,p}$ in [2].

Lemma 1. *Let k' be an unramified cyclic extension of degree p over a finite algebraic number field k. Then $A(k)$ capitulates in k' if and only if the following* a), b) *hold*:

a) *there exists a prime ideal of k which is undecomposed and principal in k',*

b) *if the class of an ideal $\mathfrak{a}'$ of k' belongs to $A(k')$, the norm $N_{k'/k}(\mathfrak{a}')$ is a principal ideal in k'.*

Proof. Let K and K' denote Hilbert's p-class fields over k and k' respectively: $k\subseteq k'\subseteq K\subseteq K'$. Let t: $\mathrm{Gal}(K/k)\rightarrow\mathrm{Gal}(K'/k')$ be the transfer map. Fix an element σ of $\mathrm{Gal}(K'/k)$ such that the restriction $\sigma|k'$ is a generator of $\mathrm{Gal}(k'/k)$. Then, for any τ in $\mathrm{Gal}(K'/k')$, we have

$$t(\tau|K)=\prod_{i=0}^{p-1}\sigma^i\tau\sigma^{-i}.$$

By Artin [1], $A(k)$ capitulates in k' if and only if $\mathrm{Im}(t)=1$. Hence the lemma follows from the fact that a) is equivalent with $t(\sigma|K)=1$ and b) with $t(\tau|K)=1$ for all τ in $\mathrm{Gal}(K'/k')$.

2. Let $\boldsymbol{Q}_\infty$ denote the unique Z_p-extension over $\boldsymbol{Q}$: $\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q})\simeq Z_p$, and let

$$\boldsymbol{Q}=\boldsymbol{Q}_0\subset\boldsymbol{Q}_1\subset\cdots\subset\boldsymbol{Q}_n\subset\cdots\subset\boldsymbol{Q}_\infty$$

be the sequence of intermediate fields for $\boldsymbol{Q}_\infty/\boldsymbol{Q}$. For each $n\geqslant 0$, let $\mathfrak{p}_n$ be the unique prime ideal of $\boldsymbol{Q}_n$, dividing the rational prime p; $\mathfrak{p}_n$ is a principal ideal in $\boldsymbol{Q}_n$ and $\mathfrak{p}_{n+1}^p=\mathfrak{p}_n$ for $n\geqslant 0$.

Let F be a real cyclic extension of degree p over $\boldsymbol{Q}$ such that

i) (p) is a prime ideal in F,

ii) the class number of F is divisible by p,

iii) $A(F_\infty)=0$ for $F_\infty=F\boldsymbol{Q}_\infty$.

Let $F_n=F\boldsymbol{Q}_n$ for $n\geqslant 0$. Then it follows from i) that $\mathfrak{p}_n$ is a prime ideal in F_n, $n\geqslant 0$, that $F\cap\boldsymbol{Q}_\infty=\boldsymbol{Q}$, and that

$$F=F_0\subset F_1\subset\cdots\subset F_n\subset\cdots\subset F_\infty$$

is the sequence of intermediate fields for the $\boldsymbol{Z}_p$-extension F_∞/F. For each $n\geqslant 0$, let K_n denote Hilbert's p-class field over F_n. Since the prime ideal (p) of F is fully ramified in F_n, we see that for $0\leqslant m\leqslant n$, $F_n\cap K_m=F_m$ and $[K_m:F_m]$ divides $[K_n:F_n]$. Hence it follows from ii) and iii) that

iv) for any $n\geqslant 0$, the class number of F_n is divisible by p,

v) for sufficiently large $n\geqslant 0$, $F_{n+1}K_n=K_{n+1}$ so that $\mathrm{Gal}(F_{n+1}/F_n)$ acts trivially on $\mathrm{Gal}(K_{n+1}/F_{n+1})$ and, hence, on $A(F_{n+1})$.

Lemma 2. *Let n be an integer such that $\mathrm{Gal}(F_{n+1}/F_n)$ acts trivially on $A(F_{n+1})$. Let $k'=F_{n+1}$ and let k be a field such that*

$$\boldsymbol{Q}_n\subseteq k\subseteq k',\quad [k':k]=p,\quad k'\neq\boldsymbol{Q}_{n+1},\ F_n.$$

Then k' is a proper subfield of Hilbert's p-class field over k and $A(k)$ capitulates in k'.

Proof. We first note that since $F_{n+1}/\boldsymbol{Q}_n$ is an abelian extension of type (p,p), there exist $p-1$ fields k as mentioned above. It is also easy to see that k'/k is an unramified cyclic extension of degree p and that there exists a prime ideal $\mathfrak{p}$ of k such that $\mathfrak{p}_n=\mathfrak{p}^p$ in k and $\mathfrak{p}=\mathfrak{p}_{n+1}$ in k', the latter equality being a consequence of i). Thus the condition a) of Lemma 1 is satisfied for k'/k. Let $\mathfrak{a}'$ be as stated in the condition b) of the same lemma. Since $\mathrm{Gal}(F_{n+1}/F_n)$ acts trivially on $A(k')$ $(=A(F_{n+1}))$, $N_{k'/k}(\mathfrak{a}')$ and $N_{k'/\boldsymbol{Q}_{n+1}}(\mathfrak{a}')$ lie in the same ideal class as ideals of k'. However, as is well known, the class number of $\boldsymbol{Q}_{n+1}$ is prime to p. Therefore $N_{k'/\boldsymbol{Q}_{n+1}}(\mathfrak{a}')$ is principal in $\boldsymbol{Q}_{n+1}$ and, consequently, $N_{k'/k}(\mathfrak{a}')$ is a principal ideal in k'. Thus the condition b) in Lemma 1 is also satisfied, and $A(k)$ capitulates in k' by that lemma. That k' is a proper subfield of Hilbert's p-class field over k follows from iv) above.

3. To find number fields F with properties i), ii), iii) in § 2, we need two more lemmas.

Lemma 3. *Let L be a number field, finite over $\boldsymbol{Q}$, and let L'/L be a cyclic extension of degree p, unramified at infinity. Let $L_\infty=L\boldsymbol{Q}_\infty$, $L'_\infty=L'\boldsymbol{Q}_\infty$. Suppose that*

1) *L_∞ has a unique p-place,*

2) *every prime ideal of L, prime to p and ramified in L', is undecomposed in L_∞,*

3) *$A(L)=0$, $A(L')=0$.*

Then $A(L'_\infty)=0$.

We omit the proof here, noting only that the essential step is to show that $H^2(L'_\infty/L_\infty, E)=0$ for the group E of units in L'_∞.

From now on, we assume that p is an odd prime: $p>2$. For each prime number q with $q\equiv 1 \bmod p$, there is a unique subfield C_q of the cyclotomic field of q-th roots of unity such that $C_q/\boldsymbol{Q}$ is a cyclic extension of degree p; q is then the unique rational prime ramified in C_q and, consequently, $A(C_q)=0$.

Lemma 4. *There exist infinitely many pairs of prime numbers* (q_1, q_2) *with the following properties:*

1) $q_1 \equiv q_2 \equiv 1 \bmod p$ *and both* q_1 *and* q_2 *are undecomposed in* $\boldsymbol{Q}_\infty$,

2) *for* $M_1=C_{q_1}$, $M_2=C_{q_2}$,

i) p *is undecomposed in* M_1, *but* q_2 *is decomposed in* M_1,

ii) q_1 *is undecomposed in* M_2.

Proof. Let P and P' denote the cyclotomic fields of p-th and p^2-th roots of unity, respectively. Then P' and $P(\sqrt[p]{p})$ are cyclic extensions of degree p over P and there exists a prime ideal $\mathfrak{q}_1$ of P with absolute degree 1 such that $\mathfrak{q}_1$ is undecomposed in both P' and $P(\sqrt[p]{p})$. Let $q_1=N_{P/\boldsymbol{Q}}(\mathfrak{q}_1)$. Then $q_1 \equiv 1 \bmod p$, p is undecomposed in $M_1=C_{q_1}$, and q_1 is undecomposed in $\boldsymbol{Q}_1$ and, hence, in $\boldsymbol{Q}_\infty$. Now, P', PM_1, and $P(\sqrt[p]{q_1})$ are independent cyclic extensions of degree p over P. Hence there is a prime ideal $\mathfrak{q}_2$ of P with absolute degree 1 such that $\mathfrak{q}_2$ is undecomposed in P' and $P(\sqrt[p]{q_1})$, but is decomposed in PM_1. Let $q_2=N_{P/\boldsymbol{Q}}(\mathfrak{q}_2)$. Then $q_2 \equiv 1 \bmod p$, q_2 is undecomposed in $\boldsymbol{Q}_\infty$, but is decomposed in M_1, and q_1 is undecomposed in $M_2=C_{q_2}$. Since there are infinitely many choices for $\mathfrak{q}_1$, $\mathfrak{q}_2$ above, there exist infinitely many pairs (q_1, q_2).

4. Let p still be an odd prime: $p>2$, and let (q_1, q_2) and M_1, M_2 be as stated in Lemma 4. Let $L=M_1$, $L'=M_1M_2$. Clearly L' is a totally real cyclic extension of degree p over L. For the extension L'/L, the conditions 1), 2) of Lemma 3 follow easily from Lemma 4, 1) and 2)-i). Since $L=M_1=C_{q_1}$, $A(L)=0$. By Lemma 4, 2)-ii), (q_1) is a prime ideal of M_2 and it is the unique prime ideal of M_2, ramified in $L'=M_1M_2$. Hence $A(M_2)=0$ implies $A(L')=0$. Thus 1), 2), 3) of Lemma 3 are satisfied for L'/L and it follows from that lemma that $A(L'_\infty)=0$.

Now, $L'/\boldsymbol{Q}$ is an abelian extension of type (p, p), unramified outside (q_1, q_2), and by Lemma 4, 2)-i), the decomposition field of p for the extension $L'/\boldsymbol{Q}$ is a cyclic extension of degree p over $\boldsymbol{Q}$. Since $p>2$, there exists a cyclic extension $F/\boldsymbol{Q}$ of degree p such that $\boldsymbol{Q} \subseteq F \subseteq L'$ and that F is different from M_1, M_2, and the decomposition field of p for $L'/\boldsymbol{Q}$. Clearly (p) is then undecomposed in F. Since $F \neq M_1, M_2$, L'/F is an unramified extension of degree p and the class number of F is divisible by p. Furthermore $A(L'_\infty)=0$ implies $A(F_\infty)=0$ for $F_\infty=F\boldsymbol{Q}_\infty \subseteq L'\boldsymbol{Q}_\infty=L'_\infty$. Thus F is a number field satisfying i), ii), iii) of § 2. Since there exist infinitely many pairs (q_1, q_2) by Lemma 4, there also exist infinitely many number fields F such as defined above, and it follows from v) and Lemma 2 in § 2 that for each F, there exist infinitely many finite algebraic number fields k such that the p-class group $A(k)$ of k capitulates in a proper subfield of Hilbert's p-class field over k. This completes the proof of the proposition in the introduction for $p>2$. Since the case $p=2$ was already treated in [2], the proposition is now proved for any prime number $p \geqslant 2$.

Remark. Greenberg's conjecture for $\boldsymbol{Z}_p$-extensions ($p \geqslant 2$) states that if F is a totally real finite algebraic number field, then $A(F_\infty)=0$ for $F_\infty = F\boldsymbol{Q}_\infty$. It is clear from the above argument that if this conjecture is assumed, we can easily find many examples of number fields F satisfying i), ii), iii) in § 2, and hence also many examples of finite algebraic number fields k, having the property mentioned in the proposition. In fact, we can find a number field k such that $A(k)$ is an abelian group of type $(p, \cdots, p)$ with arbitrarily large rank and that $A(k)$ capitulates in an unramified cyclic extension of degree p over k.

References

[1] E. Artin: Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz. Hamb. Abh., **8**, 46–51 (1930).

[2] K. Iwasawa: A note on capitulation problem for number fields. Proc. Japan Acad., **65A**, 59–61 (1989).