64. *On Capitulation of Ideals of an Algebraic Number Field*

By Katsuya MIYAKE
Department of Mathematics, College of General Education, University of Nagoya

(Communicated by Shokichi IYANAGA, M. J. A., June 12, 1984)

1. Introduction and the main result. Let k be a fixed algebraic number field of finite degree, and K be an unramified abelian extension of k. We denote the absolute ideal class groups of k and K by $C\ell(k)$ and by $C\ell(K)$, respectively. Let $\lambda_{K/k}$: $C\ell(k)\to C\ell(K)$ be the homomorphism defined naturally by lifting ideals of k to the ones of K, and put $P_k(K)=\mathrm{Ker}(\lambda_{K/k})$. Then this is the subgroup of $C\ell(k)$ consisting of those classes the ideals of which become principal in K. Let $S_k(K)$ be the unramified abelian extension of k corresponding to $P_k(K)$ by class field theory. Among the family of unramified abelian extensions of k, the members of the form $S_k(K)$ are very special. Our concern in this note is to characterize these members.

Since K and $S_k(K)$ are abelian over k, they are expressed as the compositions of the maximal p-subextensions $K^{(p)}$ and $S_k^{(p)}(K)$, respectively, for a prime p running over the prime divisors of $|C\ell(k)|$. Since we can show $S_k^{(p)}(K)=S_k^{(p)}(K^{(p)})$ (Proposition 1), we may restrict ourselves to p-extensions of k for a fixed prime p.

Let $\mathcal{K}^{(p)}=\mathcal{K}^{(p)}(k)$ be the family of all unramified abelian p-extensions of k. For $K\in\mathcal{K}^{(p)}$, the maximal unramified abelian p-extension of K is denoted by $\tilde{K}$. Then $\tilde{K}$ is the genus field of the relative abelian extension $\tilde{k}/K$ in the sense of Furuta [2]. Put $\tilde{\mathcal{K}}^{(p)}=\tilde{\mathcal{K}}^{(p)}(k)=\{\tilde{K}\,|\,K\in\mathcal{K}^{(p)}\}$. For our purpose, it is natural to classify the members of $\mathcal{K}^{(p)}$ using $\tilde{\mathcal{K}}^{(p)}$. The subfamily of $\mathcal{K}^{(p)}$ determined by $L\in\tilde{\mathcal{K}}^{(p)}$ as $\mathcal{G}_L^{(p)}=\mathcal{G}_L^{(p)}(k)=\{K\in\mathcal{K}^{(p)}\,|\,\tilde{K}=L\}$ will be called a p-genus of capitulation over k, or simply, a p-cap.-genus. A p-cap. -genus $\mathcal{G}_L^{(p)}$ will be called regular if the p-group $\mathrm{Gal}(L/k)$ is regular. (See Hall [3, § 4] or Huppert [4, Ch. III, § 10].)

The main result of this note is

Theorem 1. *Suppose that the p-cap.-genus $\mathcal{G}_L^{(p)}(k)$ with $L\in\tilde{\mathcal{K}}^{(p)}(k)$ is regular. Then for $K\in\mathcal{G}_L^{(p)}(k)$, $S_k^{(p)}(K)$ is determined by L and the degree $[K:k]$; more precisely, we have*

$$\mathrm{Gal}(L/S_k^{(p)}(K))=\{\sigma\in\mathrm{Gal}(L/k)\,|\,\sigma^{[K:k]}=1\}.$$

An immediate consequence of the theorem is

Theorem 2. *Let K_1 and K_2 be unramified abelian p-extensions of*

k. If K_1 and K_2 belong to the same regular p-genus of capitulation, then $S_k^{(p)}(K_1)$ contains $S_k^{(p)}(K_2)$ if and only if $[K_1:k]\leqq[K_2:k]$.

Remark 1. A p-group G is regular if one of the following conditions (1)~(5) is satisfied:

(1) The class of G is less than p;

(2) The order of G is less than or equal to p^p;

(3) The commutator subgroup $[G, G]$ of G is cyclic, and $p>2$;

(4) The exponent G is equal to p;

(5) The index of the subgroup $\langle\sigma^p \mid \sigma\in G\rangle$ of G is less than or equal to p^{p-1}.

(See Huppert [4, Ch. III, 10.2 and 10.13].)

In the final section, two types of examples are shown. An irregular case for $p=3$ is actually contained. (See Remark 2.)

2. The p-part of $S_k(K)$. Let p be the fixed prime number dividing $|C\ell(k)|$. For an unramified abelian extension K of k, let $K^{(p)}$, $S_k^{(p)}(K)$ and $S_k^{(p)}(K^{(p)})$ be the maximal p-subextensions of K, $S_k(K)$ and $S_k(K^{(p)})$, respectively, over k. We prove

Proposition 1. $S_k^{(p)}(K)=S_k^{(p)}(K^{(p)})$.

Proof. Let $C\ell^{(p)}(k)$ be the p-Sylow group of $C\ell(k)$, and $C\ell^{(p)\prime}(k)$ be the product of all Sylow groups of $C\ell(k)$ other than $C\ell^{(p)}(k)$. Then $C\ell(k)$ is a direct product of $C\ell^{(p)}(k)$ and $C\ell^{(p)\prime}(k)$. Therefore

$$\mathrm{Gal}\,(S_k^{(p)}(K)/k)\cong C\ell(k)/P_k(K)\cdot C\ell^{(p)\prime}(k)\cong C\ell^{(p)}(k)/P_k(K)\cap C\ell^{(p)}(k).$$

Let c be an element of $C\ell^{(p)}(k)$. Then we have $\lambda_{K/k}(c)=\lambda_{K/K^{(p)}}(\lambda_{K^{(p)}/k}(c))$ and $N_{K/K^{(p)}}(\lambda_{K/k}(c))=\lambda_{K^{(p)}/k}(c)^{[K:K^{(p)}]}$, where $N_{K/K^{(p)}}: C\ell(K)\to C\ell(K^{(p)})$ is the norm homomorphism. Since the degree $[K:K^{(p)}]$ is relatively prime to the order of $\lambda_{K^{(p)}/k}(c)$ which is a power of p, we easily see that

$$\lambda_{K/k}(c)=1\Longleftrightarrow\lambda_{K^{(p)}/k}(c)=1.$$

This shows that $P_k(K)\cap C\ell^{(p)}(k)=P_k(K^{(p)})\cap C\ell^{(p)}(k)$. Therefore we have $|\mathrm{Gal}\,(S_k^{(p)}(K)/k)|=|\mathrm{Gal}\,(S_k^{(p)}(K^{(p)})/k)|$ and $[S_k^{(p)}(K):k]=[S_k^{(p)}(K^{(p)}):k]$. It is clear by the definition that $S_k(K)\subset S_k(K^{(p)})$ since $K\supset K^{(p)}$. Therefore we have $S_k^{(p)}(K)\subset S_k^{(p)}(K^{(p)})$. Hence we conclude that $S_k^{(p)}(K)=S_k^{(p)}(K^{(p)})$ by comparing their degrees over k. Q.E.D.

3. The proof of Theorem 1. Let the notation and the assumptions be as in the theorem. Put $G=\mathrm{Gal}\,(L/k)$ and $A=\mathrm{Gal}\,(L/K)$. Then A is a normal abelian subgroup of G, and contains the commutator subgroup $[G, G]$ of G. We have $[G, G]=\mathrm{Gal}\,(L/\tilde{k})$ because $\tilde{k}$ is the maximal abelian extension of k in L. Let $C\ell^{(p)}(k)$ be the p-Sylow group of $C\ell(k)$ and $C\ell^{(p)\prime}(k)$ be as in the preceding section. Since $\tilde{k}$ is the maximal unramified abelian p-extension of k, it is the class field of k corresponding to the subgroup $C\ell^{(p)\prime}(k)$ of $C\ell(k)$. Therefore $C\ell(k)/C\ell^{(p)\prime}(k)$ is canonically isomorphic to $\mathrm{Gal}\,(\tilde{k}/k)=G/[G, G]$. Define $C\ell^{(p)}(K)$ and $C\ell^{(p)\prime}(K)$ similarly for K in place of

k. Because $L=\tilde{K}$, we have $C\ell^{(p)\prime}(K)=N_{L/K}(C\ell(L))$ where $N_{L/K}$ is the norm homomorphism, and also, a canonical isomorphism of $C\ell(K)/C\ell^{(p)\prime}(K)$ onto $A=\mathrm{Gal}(L/K)$. Let $\lambda: C\ell(k)/C\ell^{(p)\prime}(k)\to C\ell(K)/C\ell^{(p)\prime}(K)$ be the homomorphism induced from $\lambda_{K/k}$, and $V_{G\to A}: G\to A$ be the transfer of G to A. The latter induces a homomorphism $V: G/[G,G]\to A$ since A is abelian. By Artin [1], we have the following commutative diagram:

$$\begin{array}{ccc} C\ell(K)/C\ell^{(p)\prime}(K) & \xrightarrow{\sim} & A=\mathrm{Gal}(L/K) \\ \lambda\uparrow & & \uparrow V \\ C\ell(k)/C\ell^{(p)\prime}(k) & \xrightarrow{\sim} & G/[G,G]=\mathrm{Gal}(\tilde{k}/k). \end{array}$$

Now, $C\ell(k)$ is a direct product of $C\ell^{(p)}(k)$ and $C\ell^{(p)\prime}(k)$. Since the p-group $\lambda_{K/k}(C\ell^{(p)}(k))$ has only 1 in common with $C\ell^{(p)\prime}(K)$, we have $\mathrm{Ker}(\lambda)=P_k(K)\cdot C\ell^{(p)\prime}(k)/C\ell^{(p)\prime}(k)$. As for the kernel of V, we can use Theorem 4 of [5, I-1], because G is a regular p-group by the assumption, and obtain $V_{G\to A}(\sigma)=\sigma^{[G:A]}=\sigma^{[K:k]}$ for every $\sigma\in G$. Therefore we have $\mathrm{Ker}(V)=\{\sigma\in G\mid \sigma^{[K:k]}=1\}/[G,G]$. Hence the class field $S_k^{(p)}(K)$ of k corresponding to the subgroup $P_k(K)\cdot C\ell^{(p)\prime}(k)$ of $C\ell(k)$ is the subfield of L corresponding to the subgroup $\mathrm{Ker}(V_{G\to A})=\{\sigma\in \mathrm{Gal}(L/k)\mid \sigma^{[K:k]}=1\}$ of $G=\mathrm{Gal}(L/k)$. The proof is completed.

4. Examples. Let $\tilde{\tilde{k}}$ be the maximal unramified abelian p-extension of $\tilde{k}$, and put $G=\mathrm{Gal}(\tilde{\tilde{k}}/k)$. For a subgroup H of G, we denote the subfield of $\tilde{\tilde{k}}$ corresponding to H by H^*. Hence we have $H=\mathrm{Gal}(\tilde{\tilde{k}}/H^*)$, and $[G,G]^*=\tilde{k}$ for example. We consider the two cases where G is isomorphic to either one of the following G_1 and G_2 for $p\geqq 5$:

(1) $G_1=\langle a,b,c\rangle$: $a^{p^2}=b^{p^2}=c^p=1,\quad a^{-1}b^{-1}ab=c,\quad a^{-1}c^{-1}ac=b^p,$ $b^{-1}c^{-1}bc=1$;

(2) $G_2=\langle a,b,c\rangle$: $a^{p^2}=b^{p^2}=c^p=1,\quad a^{-1}b^{-1}ab=a^p,\quad a^{-1}c^{-1}ac=b^p,$ $b^{-1}c^{-1}bc=1$.

Both groups are of order p^5, and their commutator subgroups are abelian and of type (p,p). $G_1/[G_1,G_1]$ is of type (p^2,p), but $G_2/[G_2,G_2]$ is of type (p,p,p).

(1) *Subgroups of G_1 containing $[G_1,G_1]$*: $H_0=G_1$.
$H_{1,0}=\langle a^p,b,c\rangle$, $H_{1,m}=\langle ab^m,b^p,c\rangle$ $(m=1,2,\cdots,p)$.
$H_{2,0}=\langle a^p,b^p,c\rangle$, $H_{2,m}=\langle ba^{pm},c\rangle$ $(m=1,2,\cdots,p)$.
$H_3=[G_1,G_1]=\langle c,b^p\rangle$.
Commutators: $H_0'=\langle b^p,c\rangle$, $H_{1,m}'=\langle b^p\rangle$ $(m=1,2,\cdots,p)$, and $H'=[H,H]=1$ for every other H on the list.

(2) *Subgroups of G_2 containing $[G_2,G_2]$*: $H_0=G_1$.
$H_{1,0}=\langle a^p,b,c\rangle$, $H_{1,1,m}=\langle ab^m,c,b^p\rangle$ $(m=1,2,\cdots,p)$.
$H_{1,0,m,n}=\langle ac^m,bc^n\rangle$ $(m,n=1,2,\cdots,p)$.
$H_{2,\ell,m,n}=\langle a^\ell b^m c^n,a^p,b^p\rangle$ where $(\ell,m,n)=(0,0,1),\quad(0,1,n)$

with $n=1, 2, \cdots, p$, or $(1, m, n)$ with $m, n=1, 2, \cdots, p$.
$H_3=[G_2, G_2]=\langle a^p, b^p\rangle$.
Commutators: $H'_0=\langle a^p, b^p\rangle$, $H'_{1,1,m}=\langle b^p\rangle$, $H'_{1,0,m,n}=\langle a^p b^{pn}\rangle$ $(m, n=1, 2, \cdots, p)$, and $H'=1$ for every other H on the list.

Case 1. $G=G_1$. In this case, only three among $(p+3)$ intermediate fields of $\tilde{\tilde{k}}/\tilde{k}$ appear in $\mathcal{K}^{(p)}$.

$\mathcal{K}^{(p)}=\{[G_1, G_1]^*=\tilde{k}, \langle b^p\rangle^* \ (=L, \text{say}), 1^*=\tilde{\tilde{k}}\}$.
$\mathcal{G}^{(p)}_{\tilde{\tilde{k}}}=\{k\}$. $\mathcal{G}^{(p)}_L=\{H^*_{1,m} \ (m=1, 2, \cdots, p)\}$.
$\mathcal{G}^{(p)}_{\tilde{k}}=\{H^*_{1,0}, H^*_{2,m} \ (m=0, 1, 2, \cdots, p), H^*_3=\tilde{k}\}$.

For $K\in\mathcal{G}^{(p)}_L$, we have $[K:k]=p$, and $S^{(p)}_k(K)=H^*_{1,0}$. As for $\mathcal{G}^{(p)}_{\tilde{k}}$ there are two $S^{(p)}_k(K)$'s: $S^{(p)}_k(\tilde{k})=S^{(p)}_k(H^*_{2,m})=k\subsetneq S^{(p)}_k(H^*_{1,0})=H^*_{2,0}$.

Case 2. $G=G_2$. In this case, all of the intermediate fields of $\tilde{\tilde{k}}/\tilde{k}$ appear in $\mathcal{K}^{(p)}$, i.e. $\mathcal{K}^{(p)}=\{L \mid \tilde{k}\subset L\subset\tilde{\tilde{k}}\}$.

$\mathcal{G}^{(p)}_{\tilde{k}}=\{k\}$. For $L=\langle b^p\rangle^*$, $\mathcal{G}^{(p)}_L=\{H^*_{1,1,m} \ (m=1, 2\cdots, p)\}$, and $S^{(p)}_k(K)=H^*_{1,0}$ for $\forall K\in\mathcal{G}^{(p)}_L$. For $L=\langle a^p b^{pn}\rangle^*$ $(1\leqq n\leqq p)$, $\mathcal{G}^{(p)}_L=\{H^*_{1,0,m,n}(m=1, 2, \cdots, p)\}$, and $S^{(p)}_k(K)=H^*_{1,1,n}$ for $\forall K\in\mathcal{G}^{(p)}_L$. $\mathcal{G}^{(p)}_{\tilde{k}}=\{H^*_{1,0}$, all of $H^*_{2,\ell,m,n}, H^*_3=\tilde{k}\}$, and $S^{(p)}_k(\tilde{k})=S^{(p)}_k(H^*_{2,\ell,m,n})=k\subsetneq S^{(p)}_k(H^*_{1,0})=H^*_{2,0,0,1}$.

Remark 2. If $p=3$, G_2 is regular, and the above results of Case 2 hold. But G_1 is not regular, and Theorem 4 of [5, I-1] is not applicable to $A=H_{1,0}$. In fact, we have $V_{G\to A}(b)=b^p c^{-\binom{p}{2}}(b^p)^{\binom{p}{3}}=(b^p)^{1+\binom{p}{3}}$ which is not equal to b^p if $p=3$. But we have $\mathrm{Ker}(V_{G\to A})=H_{2,0}$, too, and all of the above results of Case 1 for $p=3$.

Remark 3. A direct product of regular p-groups is no longer regular in general (c.f. Huppert [4, Ch. III, 10.3c)]). But it is not hard to see that the transfer homomorphism of a direct product G of regular p-groups to a normal abelian subgroup A is always equal to the $[G:A]$-th power map. Therefore Theorems 1 and 2 hold for a much wider class of p-cap.-genera than for the class of regular ones.

References

[1] E. Artin: Idealklassen in Oberkörpern und allgemeine Reziprozitätsgesetze. Abh. Math. Sem. Hamburg, **7**, 46–51 (1930).
[2] Y. Furuta: The genus field and genus number in algebraic number fields. Nagoya Math. J., **29**, 281–285 (1967).
[3] P. Hall: A contribution to the theory of groups of prime-power order. Proc. London Math. Soc. (2), **36**, 29–95 (1933).
[4] B. Huppert: Endliche Gruppen I. Springer-Verlag, Berlin·Heidelberg, New York (1967).
[5] K. Miyake: The application of the Principal Ideal Theorem to p-groups. Preprint series, 1984, No. 3, Dept. of Math., College of General Education, Nagoya Univ. (1984).