20. Notes on the Ideal Class Groups of the p-Class Fields of Some Algebraic Number Fields

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

(Communicated by Shokichi IYANAGA, M. J. A., April 13, 1992)

1. In our recent work [7], we studied the structure of the ideal class group of the p-class fields of quadratic number fields. As we indicated there, our methods may be applicable to wider varieties of number fields than that of quadratic fields. Here we treat some cases of Abelian cubic fields and of relative quadratic extensions where we find a little more complicated structures than in quadratic number fields.

2. We fix an odd prime p. Let k be an algebraic number field of finite degree, $\tilde{k}$ the Hilbert p-class field of k and $\tilde{\tilde{k}}$ that of $\tilde{k}$, i.e. the second p-class field of k. We denote the p-primary parts of the ideal class groups of k and of $\tilde{k}$ by $\mathrm{Cl}^{(p)}(k)$ and by $\mathrm{Cl}^{(p)}(\tilde{k})$, respectively. We suppose that the p-rank of $\mathrm{Cl}^{(p)}(k)$ is larger than 1 because $\mathrm{Cl}^{(p)}(\tilde{k})$ would be trivial if otherwise.

For simplicity, we put $C:=\mathrm{Cl}^{(p)}(k)$ and $G:=\mathrm{Gal}(\tilde{\tilde{k}}/k)$ throughout this paper. Denote the alternative product of C by itself by $C\wedge C$, and the lower central series of G by

$$G_1=G\supset G_2=[G_1,G]\supset G_3=[G_2,G]\supset\cdots.$$

Then $C\wedge C$ may be identified with the Schur multiplier of C (cf. e.g. Karpilovsky [3], 2.6.7 Theorem). The quotient group G/G_3 is a central extension of $G/G_2=\mathrm{Gal}(\tilde{k}/k)$ by the kernel G_2/G_3 which lies in both of the commutator subgroup and the center of G/G_3. Since G/G_2 is isomorphic to C by the Artin map of class field theory, there is a canonical surjective homomorphism of $C\wedge C$ onto G_2/G_3 (cf. e.g. [4], Theorem 4).

Let φ be an automorphism of $G=\mathrm{Gal}(\tilde{\tilde{k}}/k)$ and $\langle\varphi\rangle$ the cyclic group generated by it. Then $\langle\varphi\rangle$ acts not only on the abelian groups $G_2=[G,G]$ and G/G_2 but also on C through the Artin map. Define an action of $\langle\varphi\rangle$ on $C\wedge C$ by $(a\wedge b)^{\varphi}:=a^{\varphi}\wedge b^{\varphi}$ for $a,b\in C$.

Proposition 1. *For an algebraic number field k of finite degree, there exists a surjective $\langle\varphi\rangle$-homomorphism of $C\wedge C$ onto G_2/G_3.*

Proof. For $\alpha,\beta\in G$, the commutator $[\alpha,\beta]$ mod G_3 depends only upon the cosets $\alpha\cdot G_2$ and $\beta\cdot G_2$; therefore, by assigning $[\alpha,\beta]$ mod G_3 to the pair of $\alpha\cdot G_2$ and $\beta\cdot G_2$, we have a well defined surjective homomorphism from the alternative product $(G/G_2)\wedge(G/G_2)$ onto G_2/G_3; since $[\alpha,\beta]^{\varphi}=[\alpha^{\varphi},\beta^{\varphi}]$, the proposition is clear.

We shall need the following fact (cf. e.g. [5], §2, Proposition 4).

Proposition 2. *Let H be a subgroup of G which contains G_2, and $V_{G\to H}: G \to H/[H,H]$ the transfer of G to H. If H is stable under φ, then the induced homomorphism from $V_{G\to H}$,*

$$\bar{V}_{G\to H}: G/G_2 \to H/[H,H],$$

is compatible with the actions of φ on G/G_2 and on $H/[H,H]$.

Now suppose that the order of φ is a divisor of $p-1$. The group ring $\boldsymbol{Q}_p[\langle\varphi\rangle]$ over the field of p-adic rational numbers $\boldsymbol{Q}_p$ is decomposed into a direct product of $\boldsymbol{Q}_p$-simple algebras each of which corresponds to a primitive idenpotent of $\boldsymbol{Q}_p[\langle\varphi\rangle]$. By assumption, each of them corresponds to an absolutely irreducible representation (a linear character) of $\langle\varphi\rangle$ because $\boldsymbol{Q}_p$ contains all the $(p-1)$-th roots of 1. Moreover, all of the primitive idenpotents belong to the group ring $\boldsymbol{Z}_p[\langle\varphi\rangle]$ over the ring of p-adic rational integers because the order $|\langle\varphi\rangle|$ is relatively prime to p. Therefore, a finite $\boldsymbol{Z}_p[\langle\varphi\rangle]$-module is decomposed into a direct product of eigen-modules of φ.

In this paper, we only study the cases of either $|\langle\varphi\rangle|=2$ or 3 mainly because of simplicity.

3. Abelian cubic fields. In this section, we assume that $p\equiv 1 \bmod 3$, and suppose that k is an abelian cubic extension of $\boldsymbol{Q}$.

3.1. Let ρ be one of non-trivial automorphisms of k. Since $\tilde{\tilde{k}}$ is normal over $\boldsymbol{Q}$, the 3-Sylow group of $\mathrm{Gal}(\tilde{\tilde{k}}/\boldsymbol{Q})$ is of order 3 and generated by a lift of ρ. We fix such a lift and denote it again by ρ. It defines an inner automorphism φ and naturally induces automorphisms of G of order 3 and of G/G_2. The action of φ on the last does not depend upon the choice of the lift of ρ. It is well known that the action of φ on C induced by the Artin map for k coincides with the natural one of ρ on C. By assumption, $\boldsymbol{Z}_p$ contains a primitive third root ζ of 1. Hence C is decomposed into a direct product of eigen-submodules of $\langle\varphi\rangle$:

$$C=C(1)\times C(\zeta)\times C(\zeta^2),$$
$$C(\zeta^n):=\{c\in C\,|\,c^{\varphi}=c^{\zeta^n}\},\qquad n=0,1,2.$$

Proposition 3. *The notation being as above, we have $C(1)=\{1\}$, and hence $C=C(\zeta)\times C(\zeta^2)$.*

Proof. For $c\in C$, we see $c^3=c^{1+\varphi+\varphi^2}=1$ because $\mathrm{Cl}^{(p)}(\boldsymbol{Q})=1$. Hence we have $c=1$ because p is relatively prime to 3. Q.E.D.

We may assume that $C(\zeta)\neq 1$ by replacing ζ with ζ^2 if necessary.

The alternative product $C\wedge C$ is decomposed into a direct product,

$$C\wedge C=C(\zeta)\wedge C(\zeta^2)\times C(\zeta^2)\wedge C(\zeta^2)\times C(\zeta)\wedge C(\zeta);$$

these three factors are the eigen-submodules corresponding respectively to the eigen-values, 1, ζ, ζ^2, of φ.

Suppose that the abelian group $C(\zeta)$ is of type

$$(\delta(1),\cdots,\delta(s)),\quad \delta(i)=p^{d_i},\quad i=1,\cdots,s,\quad 1\leq d_1\leq\cdots\leq d_s,$$

and that the invariants of $C(\zeta^2)$ are

$$(\varepsilon(1),\cdots,\varepsilon(t)),\quad \varepsilon(j)=p^{e_j},\quad j=1,\cdots,t,\quad 1\leq e_1\leq\cdots\leq e_t.$$

Fix bases, $\bar{a}_i$, $(\bar{a}_i^{\delta(i)}=1)$, $i=1,\cdots,s$, of $C(\zeta)$, and $\bar{b}_j$, $(\bar{b}_j^{\varepsilon(j)}=1)$, $j=1,\cdots,t$, of

$C(\zeta^2)$. We may suppose $s \geq t$. Let D be a metabelian p-group defined by

$$\begin{gathered} D=\langle a_i, b_j, c_{i,j} \mid i=1, \cdots, s, j=1, \cdots, t\rangle, \\ a_i^{\delta(i)}=b_j^{\varepsilon(j)}=c_{i,j}^{\min\{\delta(i), \varepsilon(j)\}}=1, \qquad [a_i, b_j]=c_{i,j}, \\ [a_i, a_m]=[b_j, b_n]=[a_i, c_{m,n}]=[b_j, c_{m,n}]=1, \\ (i, m=1, \cdots, s\,;\; j, n=1, \cdots, t). \end{gathered}$$

Then $D/[D,D]$ is isomorphic to C, and $[D,D]$ to $C(\zeta)\wedge C(\zeta^2)$; hence D may be considered a non-splitting central extension of C with the kernel $C(\zeta)\wedge C(\zeta^2)$. It is easy to see that the actions of φ determine an automorphism of D of order 3 by

$$a_i^{\varphi}=a_i^{\zeta}, \quad b_j^{\varphi}=b_j^{\zeta^2}, \quad c_{i,j}^{\varphi}=c_{i,j}, \quad (i=1, \cdots, s\,; j=1, \cdots, t),$$

because these elements, a_i^{ζ}, $b_j^{\zeta^2}$, $c_{i,j}$, of D form a set of generators which satisfy the same relations as a_i, b_j and $c_{i,j}$ do. There will be no confusion if we denote this automorphism again by φ. Let E be the semi-direct product of D and $\langle\varphi\rangle$; since $[D,D]$ is in the center of it, E is a central extension of $E/[D,D]$. It is apparent from Proposition 3 that $E/[D,D]$ is isomorphic to $\mathrm{Gal}(\tilde{k}/\boldsymbol{Q})$. Hence by the same way as we did for Theorem 1 in [7], we can prove the following theorem by utilizing Theorem 1 of Nomura [8].

Theorem 1. *Let k be an Abelian cubic field, and the notation and the assumptions be as above. Then there exists an unramified central extension K of $\tilde{k}/k$ whose group* $\mathrm{Gal}(K/k)$ *is isomorphic to D. Hence there is a natural surjection from G/G_3 onto D. In particular, we have*

$$|\mathrm{Cl}^{(p)}(\tilde{k})| \geq |C(\zeta)\wedge C(\zeta^2)|\cdot|G_3| = |G_3|\cdot \prod_{i,j} \min\{\delta(i), \varepsilon(j)\},$$

and
$$p\text{-rank}\,(\mathrm{Cl}^{(p)}(\tilde{k})) \geq p\text{-rank}\,(C(\zeta))\cdot p\text{-rank}\,(C(\zeta^2)).$$

3.2. Now we suppose that $t=p\text{-rank}\,(C(\zeta^2))$ is either 0 or 1; then we are able to show a simple and good estimate of $|G_3|$.

Theorem 2. *Let k be an Abelian cubic field and the notation be as above. Suppose that* p-rank$(C) \geq 2$, $C=\mathrm{Cl}^{(p)}(k)$, *and that* p-rank$(C(\zeta^2))$ *is either* 0 *or* 1. *Let K_i/k be the maximal unramified cyclic extension which corresponds to the subgroup*

$$\langle \bar{a}_1, \cdots, \bar{a}_{i-1}, \bar{a}_{i+1}, \cdots, \bar{a}_s\rangle \times C(\zeta^2)$$

of C, and $j_{K_i/k}: C \to \mathrm{Cl}^{(p)}(K_i)$ be the capitulation homomorphism, for $i=1, \cdots, s$. Then we have

(1) $$|G_3| \geq \prod_{i=1}^{s} [C(\zeta): C(\zeta)^{[K_i:k]}]/|C(\zeta)\cap \mathrm{Ker}\, j_{K_i/k}|;$$

(2) $$p\text{-rank}\,(\mathrm{Cl}^{(p)}(\tilde{k})) \geq p\text{-rank}\,(C(\zeta)\wedge C(\zeta^2)) + p\text{-rank}\,(G_3^{\psi});$$

(3) $$p\text{-rank}\,(G_3^{\psi}) \geq \sum_{i=1}^{s} p\text{-rank}\,(j_{K_i/k}(C(\zeta)_i)),$$

where $\psi=1+\zeta^2\varphi+\zeta\varphi^2$ and $C(\zeta)_i=\langle \bar{a}_1, \cdots, \bar{a}_i, \bar{a}_{i+1}^{\delta(i+1)/\delta(i)}, \cdots, \bar{a}_s^{\delta(s)/\delta(i)}\rangle$.

We can give a proof to the theorem by modifying the proofs of Theorem 3 and of Proposition 5 of [7]. Here we give an outline of it.

Since $C(\zeta^2)\wedge C(\zeta^2)=\{1\}$ in our present case, we have

$$C\wedge C = C(\zeta)\wedge C(\zeta^2)\times C(\zeta)\wedge C(\zeta);$$

hence in particular, we see

3.2.1. *The eigen-submodule of G_2/G_3 for the eigen-value ζ of φ is trivial.*

We choose a set of generators of G,

$$G=\langle\alpha_i,\beta\,|\,i=1,\cdots,s\rangle,\quad \alpha_i^{\delta(i)},\quad \beta^{\varepsilon(1)}\in G_2=[G,G],\quad (i=1,\cdots,s),$$

such that two sets of cosets $\{\alpha_i\cdot G_2\,|\,i=1,\cdots,s\}$ and $\{\beta\cdot G_2\}$ form bases of the submodules of G/G_2 corresponding to $C(\zeta)=\langle\bar{a}_i\,|\,i=1,\cdots,s\rangle$ and $C(\zeta^2)=\langle\bar{b}_1\rangle$, respectively, by the Artin map. We understand $\beta=1$ and $\varepsilon(1)=1$ if p-rank$(C(\zeta^2))=0$. Put $H_i:=\mathrm{Gal}(\tilde{\tilde{k}}/k_i)$; apparently we have

$$H_i=\langle\alpha_m,\beta\,|\,1\leq m\leq s,\ m\neq i\rangle\cdot G_2,\qquad i=1,\cdots,s.$$

The quotient group G/H_i is a cyclic group of order $\delta(i)$ and generated by the coset of α_i. For simplicity, we denote the transfer of G to H_i by $V_i:=V_{G\to H_i}$, and the intersection of all of the commutator subgroups $[H_i,H_i]$, $i=1,\cdots,s$, by H_∞, i.e.

$$H_\infty:=\bigcap_{i=1}^{s}[H_i,H_i]=\mathrm{Gal}(\tilde{\tilde{k}}/\tilde{K}_1\cdots\tilde{K}_s),$$

where $\tilde{K}_i$ is the Hilbert p-class field of K_i. Let $\bar{V}_i$: $G/G_2\to H_i/[H_i,H_i]$ be the homomorphism naturally induced from V_i; this corresponds to the capitulation homomorphism $j_{K_i/k}$ by the Artin maps of k and of K_i (cf. e.g. [5]). Since H_i is stable under φ, we see by Proposition 2

3.2.2. *$\bar{V}_i$ is a $\langle\varphi\rangle$-homomorphism.*

Put $H:=\langle\alpha_i\,|\,1\leq i\leq s\rangle\cdot G_2$ and

$$M_i:=\langle\alpha_1,\cdots,\alpha_i,\alpha_{i+1}^{\delta(i+1)/\delta(i)},\cdots,\alpha_s^{\delta(s)/\delta(i)}\rangle\cdot G_2,$$

for $i=1,\cdots,s$; the quotient groups H/G_2 and M_i/G_2 are isomorphic to $C(\zeta)$ and to $C(\zeta)_i$, respectively, by the Artin map.

We see (1) and (2) of the next proposition by a similar way to what we did for Proposition 3 in [7]; the last assertion follows from 3.2.1 and 3.2.2 at once.

Proposition 4. *Let the notation be as above. Then for each $i=1,\cdots,s$, we have*

(1) $V_i(H)\cap G_2/[H_i,H_i]=V_i(M_i)$ *and* $H\cap\mathrm{Ker}\,V_i\subset M_i$;

(2) $[H:M_i]=[V_i(H):V_i(M_i)]=|C(\zeta)^{\delta(i)}|$;

(3) $V_i(M_i)\subset G_3\cdot[H_i,H_i]/[H_i,H_i]$.

We modify the notation in Blackburn [1]: for $x, y\in G$, define

$$\gamma_1(x,y):=[x,y],\quad \gamma_n(x,y):=[\gamma_{n-1}(x,y),y],\quad n=2,3,4,\cdots,$$

inductively. Define s subgroups X_i, $i=1,\cdots,s$, of the abelian group G_3 by

$$X_i:=\langle\gamma_n(\alpha_m,\alpha_i),\ \gamma_n(\beta,\alpha_i)\,|\,1\leq m\leq s,\ m\neq i,\ n=2,3,4,\cdots\rangle.$$

By the same way as we did for Lemma 1 and Proposition 2 in [7], we obtain following lemma and proposition:

Lemma 1. (1) *$G_3\cdot[H_i,H_i]=X_i\cdot[H_i,H_i]$ for $i=1,\cdots,s$;*

(2) *If $i\neq m$, then $X_i\subset[H_m,H_m]$ and $X_i\cap X_m\subset H_\infty$;*

(3) *$X_i\cap[H_i,H_i]=X_i\cap H_\infty$ and $X_i\cdot[H_i,H_i]/[H_i,H_i]\cong X_i/X_i\cap H_\infty$ for $i=1,\cdots,s$.*

Proposition 5. *Let the notation be as above and denote the natural projection of G onto G/H_∞ by π. Then s subgroups $\pi(X_i)$, $i=1,\cdots,s$, form* *a direct product in the abelian group* $\pi(G_3)=G_3\cdot H_\infty/H_\infty$.

It is now easy to show our Theorem 2 by Propositions 4 and 5 together with Lemma 1 in a similar way to that in [7]. Here we do not go into the details any farther.

Remark. In case of p-rank$(C(\zeta^2))=0$, i.e. $C(\zeta^2)=\{1\}$, we do not obtain any information on G_2/G_3 by our Theorem 1. If we know by any means, however, that $j_{K_i/k}(C(\zeta)_i)$ is not trivial for any i, then we conclude by Theorem 2 that G_3 is not trivial, and hence that G_2/G_3 is not either.

Remark. Theorem 2 also holds for a cyclic cubic extension k of an algebraic number field k_0 of finite degree if the class number $|\mathrm{Cl}(k_0)|$ is relatively prime to p (cf. Section 4).

4. Relative quadratic extensions. In this section, let p be an odd prime, and k be a quadratic extension of an algebraic number field k_0 of finite degree. We assume that the class number $|\mathrm{Cl}(k_0)|$ of k_0 is not divisible by p.

When k_0 is neither $\boldsymbol{Q}$ nor an imaginary quadratic field, we cannot directly utilize the results of Nomura [8] anymore. We are able, however, to analize G_3 by capitulation homomorphisms as we did in the preceding section. We need the assumption on the class number of k_0 to set our base on the following fact (cf. [5], Proposition 2).

Proposition 6. *Let the notation and the assumptions be as above, and denote the non-trivial automorphism of* k/k_0 *by* ρ. *Then for every element* c *of* $C=\mathrm{Cl}^{(p)}(k)$, *we have* $c^\rho=c^{-1}$.

Since $\tilde{\tilde{k}}$ is a Galois extension of k_0, the 2-Sylow group of $\mathrm{Gal}(\tilde{\tilde{k}}/k_0)$ is of order 2. Fix an element of $\mathrm{Gal}(\tilde{\tilde{k}}/k_0)$ of order 2, and denote it again by ρ for simplicity. Through the inner automorphism of $\mathrm{Gal}(\tilde{\tilde{k}}/k_0)$ by ρ, we have an automorphism φ of $G=\mathrm{Gal}(\tilde{\tilde{k}}/k)$ of order 2. By Proposition 6 we see that the whole of G/G_2 is an eigen-module of φ for the eigen-value -1; hence we also see that G_2/G_3 is that for 1 because it is a surjective image of $C\wedge C$.

Suppose that $r:=p$-rank(C) is at least equal to 2 and that the invariants of C is

$$(\varepsilon(1),\cdots,\varepsilon(r)),\quad \varepsilon(i)=p^{e_i},\quad i=1,\cdots,r,\quad 1\leq e_1\leq\cdots\leq e_r.$$

Fix a basis, $\bar{a}_i,\cdots,\bar{a}_r$, of C which corresponds to these.

It is now easy to extract and assemble necessary parts of the proof of the following theorem from those of Theorem 3 and Proposition 5 of [7]; hence here it is omitted.

Theorem 3. *Let* k *be a quadratic extension of an algebraic number field* k_0 *of finite degree, and the notation and the assumptions be as above. Let* K_i/k *be the maximal unramified cyclic extension which corresponds to the subgroup*

$$\langle\bar{a}_1,\cdots,\bar{a}_{i-1},\bar{a}_{i+1},\cdots,\bar{a}_r\rangle$$

of C, *and* $j_{K_i/k}: C\to\mathrm{Cl}^{(p)}(K_i)$ *be the capitulation homomorphism, for* $i=1,\cdots,r$. *Then we have*

$$(1)\qquad |G_3| \geq \prod_{i=1}^{r} [C : C^{[K_i:k]}]/|\mathrm{Ker}\, j_{K_i/k}|;$$

$$(2)\qquad p\text{-rank}\,(G_3^{1-\varphi}) \geq \sum_{i=1}^{r} p\text{-rank}\,(j_{K_i/k}(C_i)),$$

where $C_i = \langle \bar{a}_1, \cdots, \bar{a}_i, \bar{a}_{i+1}^{\varepsilon(i+1)/\varepsilon(i)}, \cdots, \bar{a}_r^{\varepsilon(r)/\varepsilon(i)} \rangle$.

Remark. In their paper [2], Heider and Schmithals give us five real quadratic fields k whose 3-ideal class groups are of type (3, 3) together with a list of capitulation kernels, $\mathrm{Ker}\, j_{K/k}$, for all maximal unramified cyclic extensions, K/k. The discriminants d_k of them are 32009, 42817, 62501, 72329, and 94636. In case of $d_k = 62501$, all of the kernels coincide with the whole C. In each of the others, however, there exists one K/k with $\mathrm{Ker}\, j_{K/k} \neq C$. It is possible to choose a basis of C so that this K appears as one of K_i of Theorem 3. We see, therefore, p-rank$(G_3^{1-\varphi}) \geq 1$, and hence, $[G_2 : G_3] = 3$ and $|\mathrm{Cl}^{(p)}(\tilde{k})| \geq 9$ because $|C \wedge C| = 3$. As for the structure of G/G_3, nevertheless, we have a precise result of Theorem 1 of [7] for these quadratic number fields including the case of $d_k = 62501$.

References

[1] N. Blackburn: On Prime-power groups with two generators. Proc. Cambridge Phil. Soc., **54**, 327–337 (1958).

[2] F.-P. Heider und B. Schmithals: Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen. J. reine angew. Math., **336**, 1–25 (1982).

[3] G. Karpilovsky: The Schur Multiplier. Claredon Press, Oxford (1987).

[4] K. Miyake: Central extensions and Schur's multiplicators of Galois groups. Nagoya Math. J., **90**, 137–144 (1983).

[5] ——: Algebraic investigations of Hilbert's theorem 94, the principal ideal theorem and the capitulation problem. Expo. Math., **7**, 289–346 (1989).

[6] ——: Some p-groups with two generators which satisfy certain conditions arising from arithmetic in imaginary quadratic fields (Preprint Series 1991, no. 13, Coll. Gen. Educ., Nagoya Univ., p. 41) (to appear in Tôhoku Math. J.).

[7] ——: On the ideal class groups of the p-class fields of quadratic number fields. Proc. Japan Acad., **68**A, 62–67 (1992) (Preprint Series 1992, no. 2, Coll. Gen. Educ., Nagoya Univ.).

[8] A. Nomura: On the existence of unramified p-extensions. Osaka J. Math., **28**, 55–62 (1991).