36. A Note on the Artin Map. II*)

By Takashi ONO
Department of Mathematics, The Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., June 12, 1990)

This is a continuation of my preceding paper [2] which will be referred to as (I) in this paper.[1] In (I), we defined, for a finite Galois extension K/k of number fields, a monoid homomorphism (a generalized Artin map)

$$\alpha_{K/k} : I(K/k) \longrightarrow C[G]_0, \ G=G(K/k),$$

where $I(K/k)$ denotes the monoid of nonzero integral ideals $\mathfrak{a}$ of k whose prime factors are all unramified in K and $C[G]_0$ denotes the center of the group ring $C[G]$. We, then, obtained a condition for the finiteness of the image of $\alpha_{K/k}$ in terms of characters (I. Theorem). In this paper, we shall study the kernel of $\alpha_{K/k}$ in a similar way. It will turn out that the structure of the kernel becomes simpler if the group G becomes away from being *abelian*.

§1. **Center of G.** Let G be a finite group. We shall denote by $\mathrm{Irr}(G)$ the set of all irreducible C-characters of G. For each $\chi \in \mathrm{Irr}(G)$, we put

$$\chi^*(x)=\frac{\chi(x)}{\chi(1)}, \quad x \in G.$$

As is well-known, we have $|\chi^*(x)| \leqq 1$ for all x, χ.[2] In this context, it is to be noted that

(1.1) $\qquad |\chi^*(x)|=1 \quad$ for all $x, \chi \Leftrightarrow G$ is abelian.

In this paper, we are interested in the following property (Z) of G which is weaker than (1.1):

(Z) There is an $x \neq 1$ in G such that $|\chi^*(x)|=1$ for all $\chi \in \mathrm{Irr}(G)$.

(1.2) **Proposition.** *G satisfies $(Z) \Leftrightarrow$ the center of G is nontrivial.*

Proof. For an $x \in G$, let $Z(x)$ be the centralizer of x. Our assertion follows from the following chains of equivalences: x is in the center of $G \Leftrightarrow G=Z(x) \Leftrightarrow [G]=[Z(x)]$[3] $\Leftrightarrow \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2=[G]=[Z(x)]=\sum_{\chi \in \mathrm{Irr}(G)} |\chi(x)|^2 \Leftrightarrow |\chi(x)|=\chi(1)$ for all $\chi \Leftrightarrow |\chi^*(x)|=1$ for all χ. Q.E.D.

(1.3) **Remark.** Any nilpotent group $G(\neq 1)$ satisfies (Z). On the other hand, let $G=H \cdot \langle \tau \rangle$, a semidirect product of an abelian normal subgroup H of odd ($\geqq 3$) order and a cyclic subgroup $\langle \tau \rangle$ such that $\tau\sigma\tau^{-1}=\sigma^{-1}$, $\sigma \in H$, $\tau^2=1$. Then G does not satisfy (Z) as its center is trivial. Such a group G appears as the Galois group of K/Q where K is the Hilbert class field of a

*) To the memory of Michio Kuga.

1) For example, we mean by (I.2) the item (2) in (I).

2) As for elementary facts on characters, see first three chapters (pp. 1–46) of I. M. Isaacs, Character Theory of Finite Groups, Academic Press, New York-London, 1976.

3) We denote by $[S]$ the cardinality of a set S.

quadratic field k of prime discriminant; Artin reciprocity implies that $H\approx H_k$, the ideal class group of k. For details of this $K/\boldsymbol{Q}$, see § 3.

§ 2. **Kernel of $\alpha_{K/k}$.** Let K/k be a finite Galois extension of number fields with the Galois group $G=G(K/k)$, $\mathfrak{p}$ a prime ideal of k unramified in K and $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in K. Denote by $[(K/k)/\mathfrak{P}]$ the Frobenius automorphism of $\mathfrak{P}$. We denote by $\alpha_{K/k}(\mathfrak{p})$ the element in the center $\boldsymbol{C}[G]_0$ of the group ring $\boldsymbol{C}[G]$:

(2.1) $$\alpha_{K/k}(\mathfrak{p})=\frac{1}{n}\sum_{\sigma\in G}\left[\frac{K/k}{\mathfrak{P}^\sigma}\right],\qquad n=[K:k].$$ [4]

By linearity, we obtain a monoid homomorphism:

(2.2) $$\alpha_{K/k}: I(K/k)\longrightarrow \boldsymbol{C}[G]_0,$$

where $I(K/k)$ means the monoid of nonzero integral ideals $\mathfrak{a}$ such that $(\mathfrak{a}, \Delta_{K/k})=1$, here $\Delta_{K/k}$ being the relative discriminant of K/k. For $\mathfrak{a}$, $\mathfrak{b}$ in $I(K/k)$, we shall define an equivalence by

(2.3) $$\mathfrak{a}\underset{K/k}{\sim}\mathfrak{b}\overset{\text{def}}{\Longleftrightarrow}\alpha_{K/k}(\mathfrak{a})=\alpha_{K/k}(\mathfrak{b}).$$ [5]

Let σ_i, $1\leqq i\leqq r$, $\sigma_1=1$, be the representatives of conjugate classes of G, $\mathfrak{P}_i$ be a prime ideal in K such that $\sigma_i=[(K/k)/\mathfrak{P}_i]$ and $\mathfrak{p}_i$ be the prime ideal in k below $\mathfrak{P}_i$. If

(2.4) $$\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})},\quad \mathfrak{a}\in I(K/k),$$

is a factorization of $\mathfrak{a}$ in k, we put

(2.5) $$e_i(\mathfrak{a})=\sum_{\mathfrak{p}\sim\mathfrak{p}_i}\nu_{\mathfrak{p}}(\mathfrak{a}),\quad 1\leqq i\leqq r.$$

Since $\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}\sim\prod_{i=1}^r\mathfrak{p}_i^{e_i(\mathfrak{a})}$, we have

(2.6) $$\alpha_{K/k}(\mathfrak{a})=\prod_{i=1}^r\alpha_{K/k}(\mathfrak{p}_i)^{e_i(\mathfrak{a})}.$$

Since $\boldsymbol{C}[G]$ is semisimple, there is an isomorphism

$$\boldsymbol{C}[G]\approx\boldsymbol{C}_{n_1}\oplus\cdots\oplus\boldsymbol{C}_{n_r},$$

where $\boldsymbol{C}_m$ denotes the ring of all square matrices of order m over $\boldsymbol{C}$. This isomorphism induces an isomorphism

(2.7) $$\omega:\boldsymbol{C}[G]_0\rightleftarrows\boldsymbol{C}^r.$$

Let ω_ν be the projection of ω on the νth factor and χ_ν be the νth irreducible character of $\boldsymbol{C}[G]$, $1\leqq\nu\leqq r$.[6] Then we have

(2.8) $$\chi_\nu(z)=n_\nu\omega_\nu(z),\quad n_\nu=\chi_\nu(1),\quad z\in\boldsymbol{C}[G]_0.$$

From (2.1), (2.8), it follows that

(2.9) $$\omega_\nu(\alpha_{K/k}(\mathfrak{p}_i))=\chi_\nu^*(\sigma_i),\quad 1\leqq\nu,\ i\leqq r.$$

Then, from (2.6), (2.9), we have

(2.10) $$\omega_\nu(\alpha_{K/k}(\mathfrak{a}))=\prod_{i=1}^r\chi_\nu^*(\sigma_i)^{e_i(\mathfrak{a})},\quad 1\leqq\nu\leqq r.$$

Since ω in (2.7) is an isomorphism, we have

(2.11) $$\alpha_{K/k}(\mathfrak{a})=1\Longleftrightarrow\prod_{i=1}^r\chi_\nu^*(\sigma_i)^{e_i(\mathfrak{a})}=1,\quad 1\leqq\nu\leqq r.$$

As $\chi_1^*(\sigma_i)=\chi_\nu^*(\sigma_1)=1$ for all i, ν, we obtain from (2.11) the following

4) As for other mode of definition, see (I.1), (I.2).

5) In the sequel, we simply use $\sim$ in place of $\underset{K/k}{\sim}$.

6) We may assume that χ_1 is the trivial character.

equivalence which is useful to determine the kernel of $\alpha_{K/k}$:

(2.12) $$\alpha_{K/k}(\mathfrak{a})=1 \Longleftrightarrow \prod_{i=2}^{r} \chi_\nu^*(\sigma_i)^{e_i(\mathfrak{a})}=1, \quad 2\leqq\nu\leqq r.$$

In general, let F be a free commutative monoid with a set of free generators p's, M a monoid and f a monoid homomorphism: $F\to M$. We shall call f *separable* if the following condition holds:

(2.13) $$f(a)=1 \Longleftrightarrow f(p)=1 \qquad \text{for all } p\,|\,a.^{7)}$$

(2.14) **Theorem.** *Let K/k be a Galois extension of number fields. If the Galois group $G=G(K/k)$ has no center, then the generalized Artin map $\alpha_{K/k}$ is separable.*

Proof. Suppose that $\alpha_{K/k}(\mathfrak{a})=1$, $\mathfrak{a}\in I(K/k)$. Then, by (2.12), we have

(2.15) $$\prod_{i=2}^{r} |\chi_\nu^*(\sigma_i)|^{e_i(\mathfrak{a})}=1, \quad 2\leqq\nu\leqq r.$$

Since G has no center, G does not satisfy the condition (Z) by (1.2) and so, for each i, $2\leqq i\leqq r$, there is a ν, $2\leqq\nu\leqq r$, such that

(2.16) $$|\chi_\nu^*(\sigma_i)|<1.$$

Substituting (2.16) in (2.15), we find that all $e_i(\mathfrak{a})=0$, $2\leqq i\leqq r$; in other words, any prime factor $\mathfrak{p}$ of $\mathfrak{a}$ is $\sim\mathfrak{p}_1$ and so $\alpha_{K/k}(\mathfrak{p})=1$ which proves ($\Rightarrow$) of (2.13). Conversely, ($\Leftarrow$) of (2.13) is trivial. Q.E.D.

(2.17) **Remark.** Since, for a prime ideal $\mathfrak{p}\in I(K/k)$, we have

(2.18) $$\alpha_{K/k}(\mathfrak{p})=1 \Leftrightarrow \mathfrak{p} \text{ splits completely in } K \Leftrightarrow \mathfrak{p}=N_{K/k}\mathfrak{P},$$

we find, when $G=G(K/k)$ has no center, that $\operatorname{Ker}\alpha_{K/k}$ is the submonoid of $I(K/k)$ generated by primes which split completely for K/k and that, for $\mathfrak{a}\in I(K/k)$,

(2.19) $$\alpha_{K/k}(\mathfrak{a})=1 \Longrightarrow \mathfrak{a}=N_{K/k}\mathfrak{A} \qquad \text{for some ideal } \mathfrak{A} \text{ in } K.$$

Here, note that the converse of (2.19) is not true. In fact, choose a prime $\mathfrak{p}\in I(K/k)$ which does not split completely for K/k and put $\mathfrak{a}=\mathfrak{p}^f=N_{K/k}\mathfrak{P}$, $f>1$. If we had $\alpha_{K/k}(\mathfrak{a})=1$, then $\alpha_{K/k}(\mathfrak{p})=1$ as $\alpha_{K/k}$ is separable by (2.14) and so $\mathfrak{p}=N_{K/k}\mathfrak{P}$ which contradicts to $f>1$.

(2.20) **Remark.** Contrary to (2.19), assume that K/k is abelian. Then we know that, for $\mathfrak{a}\in I(K/k)$,

(2.21) $$\mathfrak{a}=N_{K/k}\mathfrak{A} \text{ for some ideal } \mathfrak{A} \text{ in } K \Longrightarrow \alpha_{K/k}(\mathfrak{a})=1.$$

Again, the converse of (2.21) is not true, except the trivial case where $K=k$. In fact, let $\mathfrak{P}$ be a prime ideal in K which is unramified for K/k such that $N_{K/k}\mathfrak{P}=\mathfrak{p}^f$ with $f>1$. Since K/k is abelian, there is a prime ideal $\mathfrak{q}$ in k such that $\alpha_{K/k}(\mathfrak{p}\mathfrak{q})=1$. As $\alpha_{K/k}(\mathfrak{q})=\alpha_{K/k}(\mathfrak{p})^{-1}$ in $G=G(K/k)$, the Frobenius elements $\alpha_{K/k}(\mathfrak{p})$ and $\alpha_{K/k}(\mathfrak{q})$ share the same order f in G; in other words, we have $N_{K/k}\mathfrak{Q}=\mathfrak{q}^f$, $f>1$. If we put $\mathfrak{a}=\mathfrak{p}\mathfrak{q}$, then we have $\alpha_{K/k}(\mathfrak{a})=1$ but obviously $\mathfrak{a}$ can not be a norm of an ideal in K because $f>1$.

§ 3. Quadratic fields with prime discriminant.

Let $l\neq 2$ be a prime and $k=\boldsymbol{Q}(\sqrt{l^*})$, $l^*=(-1)^{(l-1)/2}l$. As the discriminant $\Delta_k=l^*\equiv 1 \bmod 4$, k is referred to as a quadratic field of prime discriminant. The ring $\mathfrak{o}_k$ of integers is given as $\mathfrak{o}_k=\boldsymbol{Z}+\boldsymbol{Z}\omega$, $\omega=(1+\sqrt{l^*})/2$, and the norm form q_k is

7) $p\,|\,a$ means that p appears in the canonical expression of a.

defined by

(3.1) $$q_k(z)=N_{k/Q}(x+y\omega)=x^2+xy+((1-l^*)/4)y^2,\ z=(x,y).$$

Let $h=h_k$ be the class number of k and ε be the fundamental unit of k when $\Delta_k>0$. By the genus theory, we know that h is odd and $N_{k/Q}\varepsilon=-1$.[8] Let K be the Hilbert class field of k. One verifies easily that $K/\boldsymbol{Q}$ is a Galois extension. The subgroup H of $G=G(K/\boldsymbol{Q})$ corresponding to k, i.e., $H=G(K/k)$, is normal in G and the Artin reciprocity map $\alpha_{K/k}$ identifies the ideal class group H_k with H. Let τ be any element of G of order 2. As h is odd, we have $\tau\notin H$ and $G=H\cdot\langle\tau\rangle$, a semidirect product with H normal. We claim that

(3.2) $$\tau\sigma\tau^{-1}=\sigma^{-1},\qquad \sigma\in H.$$

In fact, since $\mathfrak{p}\mathfrak{p}^\tau=N_{k/Q}\mathfrak{p}\sim 1$,[9] we have $\tau\alpha_{K/k}(\mathfrak{p})\tau^{-1}=\alpha_{K/k}(\mathfrak{p}^\tau)=\alpha_{K/k}(\mathfrak{p})^{-1}$ and (3.2) follows from Čebotarev theorem. From (3.2) we see also that G has no center if $h\geqq 3$.

$$\begin{array}{ccc} K & & \mathfrak{P} \\ {\scriptstyle h}\big| & & \\ k & & \mathfrak{p} \\ {\scriptstyle 2}\big| & & \\ \boldsymbol{Q} & & p\neq l \end{array}$$

Case 1. $h\geqq 3$. We identify the monoid $I(K/\boldsymbol{Q})$ with the monoid of positive integers a, $l\nmid a$. For $p\in I(K/\boldsymbol{Q})$, i.e., for $p\neq l$, we have

(3.3) $$\alpha_{K/Q}(p)=1 \Longleftrightarrow p=q_k(z) \text{ for some } z=(x,y)\in \boldsymbol{Z}^2.$$

In fact, this follows from the following chain of equivalences:

$\alpha_{K/Q}(p)=1 \Longleftrightarrow p$ splits completely for $K/\boldsymbol{Q} \Longleftrightarrow p$ splits completely for $k/\boldsymbol{Q}$ and $\mathfrak{p}$, $\mathfrak{p}|p$, splits completely for $K/k \Longleftrightarrow p=N_{k/Q}\mathfrak{p}$ and $\alpha_{K/k}(\mathfrak{p})=1$ $\Longleftrightarrow p=N_{k/Q}\mathfrak{p}$ and $\mathfrak{p}=(\pi)$, $N_{k/Q}\pi>0$, $\pi=x+y\omega\in\mathfrak{o}_k \Longleftrightarrow p=q_k(z)$, $z=(x,y)\in\boldsymbol{Z}^2$.

Since $G(K/\boldsymbol{Q})$ has no center, by (2.14) the Artin map is separable and hence we have, for $a\in I(K/\boldsymbol{Q})$, i.e., for $a>0$ with $l\nmid a$,

(3.4) $$\alpha_{K/Q}(a)=1 \Longleftrightarrow q_k \text{ represents } p \text{ for all } p\,|\,a.$$[10]

Case 2. $h=1$. We have $K=k$ and $G=\langle\tau\rangle$. If we identify G with the group $\{\pm 1\}$ (canonically), the Artin map $\alpha_{K/Q}$ is nothing but the Kronecker character $\chi_k(a)=(a/l)$, $l\nmid a$. Since $h=1$, we have, for $p\neq l$, 2,

(3.5) $$\left(\frac{p}{l}\right)=\left(\frac{l^*}{p}\right)=1 \Longleftrightarrow q_k\longrightarrow p,$$

and

(3.6) $$\chi_k(2)=1 \Longleftrightarrow l^*\equiv 1 \bmod 8 \Longleftrightarrow q_k\longrightarrow 2.$$

If we decompose a as $a=2^{e_2}\prod p^{e_p}\prod q^{e_q}$, with $(p/l)=1$, $(q/l)=-1$, then we have

8) As for elementary facts on quadratic fields, see, for example, T. Ono, An Introduction to Algebraic Number Theory, New York, 1990.

9) $\mathfrak{a}\sim 1$ means that $\mathfrak{a}$ is a principal ideal.

10) We say that q_k represents $n\in\boldsymbol{Z}$ (written: $q_k\to n$) if $n=q_k(z)$ for some $z\in\boldsymbol{Z}^2$. Needless to say that $\alpha_{K/Q}(a)=1\Rightarrow q_k\to a$, by (3.4).

$$(3.7) \qquad \alpha_{K/Q}(a)=\begin{cases}(-1)^{\Sigma e_q}, & l^*\equiv 1 \bmod 8,\\ (-1)^{e_2+\Sigma e_q}, & l^*\equiv 5 \bmod 8.\end{cases}$$

The observation above shows that the generalized Artin map has something to do with the arithmetic of good old days.

References

[1] Cox, D.: Primes of the Form x^2+ny^2. John Wiley and Sons, New York (1989).[11]
[2] Ono, T.: A note on the Artin map. Proc. Japan Acad., **65A**, 304–306 (1989).