Y. Furuta
Nagoya Math. J.
Vol. 66 (1977), 167-182

NOTE ON CLASS NUMBER FACTORS AND PRIME DECOMPOSITIONS

YOSHIOMI FURUTA

Introduction

Let K be a Galois extension of an algebraic number field k of finite degree with Galois group g, $\mathfrak{D}$ be a congruent ideal class group of K, and M be the class field over K corresponding to $\mathfrak{D}$. Assume that M is normal over k. Then g acts on $\mathfrak{D}$ as a group of automorphisms. Donote by I_g the augmentation ideal of the group ring $\boldsymbol{Z}_g$ over the ring of integers $\boldsymbol{Z}$. Then we have a sequence $\mathfrak{D} \supset I_g\mathfrak{D} \supset I_g^2\mathfrak{D} \supset \cdots$ and a sequence of the corresponding class fields $K = K_{M/k}^{(0)} \subset K_{M/k}^{(1)} \subset K_{M/k}^{(2)} \subset \cdots$. We call $K_{M/k}^{(i)}$ the *i-th central class field of K in M with respect to k.* We put simply $K^{(i)} = K_{M/k}^{(i)}$, when it is not in danger of confusion.

In the previous paper [10], we have shown that the Galois group $G(K^{(i+1)}/K^{(i)})$ is isomorphic to a factor group of $G(K^{(1)}/K)$ or of slightly modified group of $G(K^{(1)}/K)$ when K is non-cyclic over k.

In the present paper we apply the above result firstly to the case where K is cyclic over k and we have more explicit structure of $G(K^{(i+1)}/K^{(i)})$. In fact we have a formula of the extension degree of $K^{(i+1)}/K^{(i)}$ in § 2, which generalize the genus formula in [8] when K is cyclic over k. Furthermore in § 3 we express the structure of $G(K^{(i+1)}/K^{(i)})$ by using "Auflösung" characters of H. W. Leopoldt [19], when the ground field k is the rational number field $\boldsymbol{Q}$.

Secondly we study on prime decompositions in $K^{(i+1)}/K^{(i)}$ and in § 5 we have explicit criteria of prime decompositions for some non-abelian extensions. As a special case we have a new expression of the reciprocity of the biquadratic residue symbol. § 2 and § 3 are unnecessary to the argument of § 4 and § 5.

Received June 30, 1976.

https://doi.org/10.1017/S0027763000017797 Published online by Cambridge University Press

§ 1. Preliminaries

1.1. Notation being as in Introduction, suppose that K is a cyclic extension of k, whose Galois group is g generated by σ. Then for $i = 0, 1, 2, \cdots$, we have easily[1)]

$$(1) \qquad G(K^{(i+1)}/K^{(i)}) \cong \mathfrak{D}^{(\sigma-1)^i}/\mathfrak{D}^{(\sigma-1)^{i+1}} \cong \mathfrak{D}/(\mathfrak{R}^{(i)}\mathfrak{D}^{\sigma-1}) ,$$

where $\mathfrak{R}^{(i)} = \mathfrak{R}^{(i)}(\mathfrak{D})$ is the group of elements $\mathfrak{c}$ of $\mathfrak{D}$ such that $\mathfrak{c}^{(\sigma-1)^i} = 1$. Since K is cyclic over k, the field $K^{(1)}$ coincides with the genus field $K^* = K^*_{M/k}$ of K in M, which is by definition the maximal extension of K contained in M and obtained by composing an abelian extension over k. We have[2)]

$$(2) \qquad \mathfrak{D}/\mathfrak{D}^{\sigma-1} \cong G(K^{(1)}/K) = G(K^*/K) \cong H(K/k)/(k^{\times}N_{K/k}H(M/K)) ,$$

where $H(M/K)$ and $H(K/k)$ are the idele group of K and k corresponding to M and K respectively, and $k^{\times}$ is the principal idele group of k.

Denote by $\mathfrak{H}(K/k)$ and $\mathfrak{H}^*(K/k)$ the congruent ideal group of k corresponding to $H(K/k)$ and $k^{\times}N_{K/k}H(M/k)$ respectively. Then we have

$$(3) \qquad G(K^*/K) \cong \mathfrak{H}(K/k)/\mathfrak{H}^*(K/k) .$$

Denote by $\mathfrak{H}(M/K)$ the congruent ideal group of K corresponding to M and by $\mathfrak{F} = \mathfrak{F}(M/K)$ the conductor of $\mathfrak{H}(M/K)$. Let $\mathfrak{R}_0^{(i)}$ be the group of ideals $\mathfrak{a}$ of k such that $\mathfrak{a} = N_{K/k}\mathfrak{A}$ for some ideal $\mathfrak{A} \in \mathfrak{R}^{(i)}$. Then (1), (2) and (3) imply

$$(4) \qquad G(K^{(i+1)}/K^{(i)}) \cong \mathfrak{H}(K/k)/\mathfrak{R}_0^{(i)}\mathfrak{H}^*(K/k) .$$

1.2. The structure of $\mathfrak{H}^*(K/k)$ is known for many cases explicitly.[3)] In the following we shall show a recursive method to get $\mathfrak{R}^{(i)}$ or $\mathfrak{R}_0^{(i)}$. In order to determine $\mathfrak{R}^{(i)}$, it is enough to get a finite number of integral ideals by which all classes of $\mathfrak{R}^{(i)}$ are represented mod $\mathfrak{H}(M/K)$. We call a system of these ideals a *full set of representatives of* $\mathfrak{R}^{(i)}$. We call the set of norms of these ideals to k a *full set of representatives of* $\mathfrak{R}_0^{(i)}$.

Suppose that for $\nu = 1, \cdots, t_i$, ideals $\mathfrak{A}_\nu$ consist a full set of representatives of $\mathfrak{R}^{(i)}$. When $N_{K/k}\mathfrak{A}_\nu \in N_{K/k}\mathfrak{H}(M/K)$, we can choose an integral ideal $\mathfrak{B}_\nu$ of K such that

1) See Y. Furuta [10, §1].
2) Cf. Y. Furuta [10, §2].
3) See for instance H. W. Leopoldt [19], A. Fröhlich [5] and Y. Furuta [8].

(5) $$\mathfrak{B}_\nu^{\sigma-1} \equiv \mathfrak{A}_\nu \bmod. \mathfrak{H}(M/K) .$$

Then it follows from the definition of $K^{(i)}$ that $\mathfrak{R}_\nu$ for $\nu = 1, \cdots, t_i$ and B_ν chosen as above make a full set of representatives of $\mathfrak{R}^{(i+1)}$.

Remark. Since the above $\mathfrak{A}_\nu$ and $\mathfrak{B}_\nu$ are representatives mod. $\mathfrak{H}(M/K)$, we can restrict them to be prime ideals of K of absolute degree 1. When that is the case, we call the set of $\mathfrak{A}_\nu$ and $\mathfrak{B}_\nu$ resp. $\mathfrak{a}_\nu = N_{K/k}\mathfrak{A}_\nu$ and $\mathfrak{b}_\nu = N_{K/k}\mathfrak{B}_\nu$ a full set of prime representatives of degree 1 of $\mathfrak{R}^{(i)}$ resp. of $\mathfrak{R}_0^{(i)}$.

1.3. In the case where k is the rational number field $\boldsymbol{Q}$, K is a quadratic field and M is a ray class field over K mod. $\mathfrak{F}$ for some divisor $\mathfrak{F}$ of K, we have further the following way[4] of the determination of $\mathfrak{R}_0^{(i+1)}$ from $\mathfrak{R}_0^{(i)}$. We assume, by the above remark, that the representatives of $\mathfrak{R}^{(i)}$ are prime ideals of K of degree 1. Let $\mathfrak{p}$ be such a representative and assume $p = N_{K/Q}\mathfrak{p} \in N_{K/Q}S_K(\mathfrak{F})$, $S_K(\mathfrak{F})$ being the ray mod. $\mathfrak{F}$ in K. Then there exists a prime ideal $\mathfrak{q}$ of K of degree 1 such that $\mathfrak{q}^{\sigma-1} \equiv \mathfrak{p} \bmod. S_K(\mathfrak{F})$. Hence for some $(\alpha) \in S_K(\mathfrak{F})$ we have

$$\alpha = \mathfrak{p}\mathfrak{q}^{1-\sigma} = \mathfrak{p}\mathfrak{q}^2/N_{K/Q}\mathfrak{q} = \beta/q ,$$

where σ is the non-trivial automorphism of K over $\boldsymbol{Q}$, $q = N_{K/Q}\mathfrak{q}$, the rational prime, and β is an integer of K such that $q \equiv \beta \bmod. \mathfrak{F}$. Since $N_{K/Q}\alpha = N_{K/Q}\mathfrak{p} = p$, we have

(6) $$pq^2 = N_{K/Q}\beta .$$

Conversely let $p \in \mathfrak{R}_0^{(i)}$, i.e., $p = N_{K/Q}\mathfrak{p}$ and $\mathfrak{p} \in \mathfrak{R}^{(i)}$. Let q be a rational prime which satisfies (6) for some integer β of K such that $q \equiv \beta \bmod. \mathfrak{F}$, β has no rational integral divisor, and q be decomposed completely in K. Then (6) implies $\beta = \mathfrak{p}\mathfrak{q}^2$, $N_{K/Q}\mathfrak{q} = q$, hence $\mathfrak{p}\mathfrak{q}^{1-\sigma} = \beta/q \in S_K(\mathfrak{F})$, which means $q \in \mathfrak{R}_0^{(i+1)}$.

Now let D be the discriminant of K. Then the above q is a primitive solution z of the Diophantine equation

(7) $$x^2 - Dy^2 - 4pz^2 = 0 .$$

Therefore a full set of prime representatives of degree 1 of $\mathfrak{R}_0^{(i+1)}$ is obtained from the full set of prime representatives p of degree 1 of $\mathfrak{R}_0^{(i)}$ by adding rational primes q of degree 1 such that q is a primitive

4) Cf. H. Hasse [14] and G. Gras [12, §IV, B].

solution of (7) by $z = q$ and $\frac{1}{2}(x + y\sqrt{D}) \equiv q$ mod. $\mathfrak{F}$.

§ 2. Nilpotent factors of the ideal class group of cyclic extensions

2.1. We can study the structure of the ideal class group of cyclic extensions of any degree by using (1). This is a generalization of H. Hasse [14] and G. Gras [12] by means of dual way[5] in some sense.

For the sake of simplicity we treate of the case where M is the absolute class field of K, in wide sense or in narrow sense, which we denote by $K^{\#}$.

For an algebraic number field K, we denote by J_K the idele group, by $K^{\times}$ the principal idele group and by U_K the unit idele group of K whose real infinite components are of all non-zero real numbers or positive real numbers according as we treate on the absolute class field in wide sense or in narrow sense. Denote by $K_{\mathfrak{P}}^{\times}$ the multiplicative group of non-zero elements of the completion $K_{\mathfrak{P}}$ of K at $\mathfrak{P}$, and by $U_{\mathfrak{P}}$ the unit group of $K_{\mathfrak{P}}$, which are embedded in J_K in usual way.

Now let K/k be a cyclic extension and let $M = K^{\#}$. Let $R^{(i)}$ be a full set of representatives of $\mathfrak{K}^{(i)}$ and assume[6] that $R^{(i)}$ is consisted by prime ideals of degree 1 over k. Let $R_0^{(i)}$ be the set of all $N_{K/k}\mathfrak{P}$ where $\mathfrak{P} \in R^{(i)}$. Denote further by K_i^* the class field over K corresponding to $\mathfrak{K}^{(i)}\mathfrak{D}^{\sigma-1}$. Then K_i^* is the maximal extension over K which is contained in K^* and in which all primes of $R^{(i)}$ are completely decomposed. We put

$$H^{(i)} = \prod_{\mathfrak{p} \in R_0^{(i)}} (H \cap H^* k_{\mathfrak{p}}^{\times}), \tag{8}$$

where $H = H(K/k)$ is the subgroup of J_k corresponding to K as in § 1.1, and $H^* = k^{\times} N_{K/k} U_K$. Then (1) implies

$$G(K^{(i+1)}/K^{(i)}) \cong G(K_i^*/K) \cong H/H^{(i)} . \tag{9}$$

Moreover by [8, Proposition 2], we have $H^* = k^{\times} \prod_{\mathfrak{p}} (H \cap U_{\mathfrak{p}})$ where $\mathfrak{p}$ runs over all primes of k. Hence by simple calculations, (8) implies

$$\begin{aligned} H^{(i)} &= k^{\times} \cdot \prod_{\mathfrak{p} \notin R_0^{(i)}} (H \cap U_{\mathfrak{p}}) \cdot \prod_{\mathfrak{p} \in R_0^{(i)}} (H \cap k_{\mathfrak{p}}^{\times}) \\ &= k^{\times} \prod_{\mathfrak{p} \notin R_0^{(i)}} (H \cap U_{\mathfrak{p}}) \cdot \prod_{\mathfrak{p} \in R_0^{(i)}} k_{\mathfrak{p}}^{\times} . \end{aligned} \tag{10}$$

5) The investigation in this way has been treated in some cases by E. Inaba [15], A. Fröhlich [3] and H. Koch [17].

6) See *Remark* of §1.2.

Now (9) and (10) imply the following

PROPOSITION 2.1. *Let K be a cyclic extension of k, and $K^{(i)}$ be the i-th central class field of K with respect to k in the absolute class field $K^{\#}$ of K. Let $R_0^{(i)}$ be a full set of representatives of $\mathfrak{R}_0^{(i)}$ which consists of primes of k of degree 1 in K. Then we have*

$$G(K^{(i+1)}/K^{(i)}) \cong H\Big/\Big(k^{\times}\cdot\prod_{\mathfrak{p}}(H\cap U_{\mathfrak{p}})\cdot\prod_{\mathfrak{p}\in R_0^{(i)}}k_{\mathfrak{p}}^{\times}\Big),$$

where $H = H(K/k)$, the idele group of k corresponding to K.

2.2. Notation being as above, denote further by $z_{K/k}^{(i)}$ the extension degree $(K^{(i)}:K^{(i-1)})$ for $i \geqq 1$, where $K^{(0)} = K$. We call $z_{K/k}^{(i)}$ the *i-th central class number of K with respect to k.* Now by an analogous calculation as the genus formula in [8, Theorem[7]] we have a formula for $z_{K/k}^{(i)}$ as follows. By (9) we have

$$z_{K/k}^{(i)} = (K^{(i)}:K^{(i-1)}) = (K_{i-1}^{*}:K) = (K_{i-1}^{*}:k)/(K:k)\,.$$

For a wile denote by $\mathfrak{p}$ resp. $\mathfrak{q}$ primes of k contained resp. not contained in $R_0^{(i-1)}$. Then

$$(K_{i-1}^{*}:k) = (J_k:H^{(i-1)}) = \Big(J_k:k^{\times}\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}\Big)\cdot\Big(k^{\times}\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}:H^{(i-1)}\Big)\,.$$

Denote by $\mathfrak{P}$ resp. $\mathfrak{Q}$ one of prime divisors of $\mathfrak{p}$ resp. $\mathfrak{q}$ in K fixed once for all. Denote for a wile by N the norm for local fields. Then since $\mathfrak{p}$ is decomposed completely in K by the assumption, we have

$$k^{\times}\prod_{\mathfrak{q}}NU_{\mathfrak{Q}}\prod_{\mathfrak{p}}NK_{\mathfrak{P}}^{\times}\cap\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times} = \Big(k^{\times}\cap\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}\Big)\cdot\prod_{\mathfrak{q}}NU_{\mathfrak{Q}}\prod_{\mathfrak{p}}NK_{\mathfrak{P}}^{\times}\,.$$

Moreover since $NK_{\mathfrak{P}}^{\times} = k_{\mathfrak{p}}^{\times}$, we have

$$\begin{aligned}\Big(k^{\times}\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}:H^{(i-1)}\Big) &= \Big(k^{\times}\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}:k^{\times}\prod_{\mathfrak{q}}NU_{\mathfrak{Q}}\prod_{\mathfrak{p}}NK_{\mathfrak{P}}^{\times}\Big)\\ &= \Big(\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}:k^{\times}\prod_{\mathfrak{q}}NU_{\mathfrak{Q}}\prod_{\mathfrak{p}}NK_{\mathfrak{P}}^{\times}\cap\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}\Big)\\ &= \frac{\prod_{\mathfrak{q}}(U_{\mathfrak{q}}:NU_{\mathfrak{Q}})}{((k^{\times}\cap\prod_{\mathfrak{q}}U_{\mathfrak{q}}\prod_{\mathfrak{p}}k_{\mathfrak{p}}^{\times}):(k^{\times}\cap\prod_{\mathfrak{q}}NU_{\mathfrak{Q}}\prod_{\mathfrak{p}}NK_{\mathfrak{P}}^{\times}))}\,.\end{aligned}$$

Now we have the following

7) Cf. also L. Goldstein [11, §2].

https://doi.org/10.1017/S0027763000017797 Published online by Cambridge University Press

PROPOSITION 2.2. *Let K be a cyclic extension of k. For a prime $\mathfrak{q}$ of k, denote by $e_{\mathfrak{q}}$ the ramification index of $\mathfrak{q}$ in K. Let $R_0^{(i)}$ be a full set of representatives of $\mathfrak{R}_0^{(i)}$ which consists of primes of degree* 1 *in K. Denote by $E(R_0^{(i)})$ the group of all $R_0^{(i)}$-units*[8] *of k, and by $\tilde{E}(R_0^{(i)})$ the group of all elements of $E(R_0^{(i)})$ which are everywhere locally norm from K. Denote further by $h(R_0^{(i)})$ the extension degree of the maximal extension over k which is contained in the absolute class field of k and in which all primes of $R_0^{(i)}$ are decomposed completely. Then we have*

$$z_{K/k}^{(i+1)} = \frac{h(R_0^{(i)}) \prod_{\mathfrak{q} \in R_0^{(i)}} e_{\mathfrak{q}}}{(K:k)(E(R_0^{(i)}):\tilde{E}(R_0^{(i)}))} .$$

Remark. For $i=0$, the above formula coinsides with the genus formula in [8] or in L. Goldstein [11], when K is cyclic over k.

§3. Nilpotent factors of the ideal class group of cyclic extensions over Q

3.1. When K is an abelian extension over the rational number field $\boldsymbol{Q}$ and M is the absolute class field of K in narrow sense, the genus field $K^* = K^*_{M/k}$ corresponds to the "Auflösung" character group by H. W. Leopoldt [19]. Thus by (1) and (2), we can study the structure of $G(K^{(i+1)}/K^{(i)})$ by means of the above character group.

For an abelian extension $K/\boldsymbol{Q}$, let X be the corresponding character group, namely the character group of the congruent ideal class group corresponding to K, which is also the character group of $G(K/\boldsymbol{Q})$ via Artin's reciprocity. For a character χ in X denote by K_χ the abelian field corresponding to χ. The p-component χ_p of χ for a rational prime p is defined by

$$\chi_p(a) = \chi\left(\frac{|a|, K_\chi}{p}\right),$$

when $a \in \boldsymbol{Q}$ and is prime to the conductor of χ. Then χ_p is a character of some congruent ideal class group. The "Auflösung" X^* of X is the group generated by all χ_p where $\chi \in X$ and p runs over all rational primes. H. W. Leopoldt [19] has proved.

(11) $$G(K^*/K) \cong X^*/X .$$

8) This means elements of k whose prime divisors are at most primes contained in $R_0^{(i)}$; and which are totally positive when $K^{\#}$ is the absolute class field in narrow sense.

https://doi.org/10.1017/S0027763000017797 Published online by Cambridge University Press

3.2. Put $H^* = \boldsymbol{Q}^\times \cdot N_{K/\boldsymbol{Q}} U_K$. Then it follows from [8, Proposition 1] that

$$G(K^*/K) \cong H/H^* , \tag{12}$$

where $H = H(K/Q)$. For the sake of convenience we shall imply[9] Leopoldt's formula (11) from (12). Since we treate here the absolute class field in narrow sense, we have to take the group of all positive real numbers as the infinite component U_{p_∞} of $U_{\boldsymbol{Q}}$. Then $J_{\boldsymbol{Q}} = \boldsymbol{Q}^\times U_{\boldsymbol{Q}}$ and an element $\mathfrak{a}$ of $J_{\boldsymbol{Q}}$ is expressed uniquely as $\mathfrak{a} = a\mathfrak{u}$, where $a \in \boldsymbol{Q}^\times$ and $\mathfrak{u} = (u_p) \in U_{\boldsymbol{Q}}$. Let H_χ be the subgroup of $J_{\boldsymbol{Q}}$ corresponding to K_χ, and denote by S_0 the set of all finite primes of $\boldsymbol{Q}$. Then we have

$$\begin{aligned} H^* &= \boldsymbol{Q}^\times \prod_{p \in S_0} (H \cap U_p) \cdot U_{p_\infty} = \boldsymbol{Q}^\times \cdot \prod_{p \in S_0} \Big(\Big(\bigcap_{\chi \in X} H_\chi\Big) \cap U_p\Big) \cdot U_{p_\infty} \\ &= \bigcap_{\substack{\chi \in X \\ p \in S_0}} \boldsymbol{Q}^\times \prod_{\substack{q \neq p \\ q \in S_0}} U_q \cdot (H_\chi \cap U_p) \cdot U_{p_\infty} . \end{aligned} \tag{13}$$

For $\chi \in X$ and $p \in S_0$ we define $\varphi_{\chi,p}$ by

$$\varphi_{\chi,p}(\mathfrak{a}) = \varphi_{\chi,p}(a\mathfrak{u}) = \left(\frac{u_p, K_\chi}{p}\right) ,$$

where $\mathfrak{a} = a\mathfrak{u} \in J_{\boldsymbol{Q}}$, $a \in \boldsymbol{Q}^\times$, $\mathfrak{u} = (u_p) \in U_{\boldsymbol{Q}}$. Then $\varphi_{\chi,p}$ is a differential of $J_{\boldsymbol{Q}}$ in the sense of the class field theory. The kernel of $\varphi_{\chi,p}$ is equal to $\boldsymbol{Q}^\times \prod_{q \neq p,\, q \in S_0} U_q \cdot (H_\chi \cap U_p) \cdot U_{p_\infty}$, and it follows from (13) that the character group of $J_{\boldsymbol{Q}}/H^*$ is generated by $\varphi_{\chi,p}$ where $\chi \in X$ and $p \in S_0$. Let $\psi_{\chi,p}$ be the congruent ideal character corresponding to $\varphi_{\chi,p}$. Then since the conductor of $\varphi_{\chi,p}$ is equal to the product of a power of p and p_∞, we see

$$\psi_{\chi,p}(a) = \chi\left(\frac{a, K_\chi}{p}\right)^{-1} = \chi_p^{-1}(a) ,$$

for $a \in \boldsymbol{Q}$ which is positive and prime to the conductor of χ. Hence X^* corresponds to K^* and (11) is implied.

3.3. Assume that K is cyclic extension over $k = \boldsymbol{Q}$. Notation $\mathfrak{R}^{(i)}$, $R^{(i)}$, $R_0^{(i)}$ and K_i^* be as in §2.1. For the character group X of $K/\boldsymbol{Q}$ put

$$X_i^* = \{\chi \in X^* \mid \chi(p) = 1 \quad \text{for all } p \in R_0^{(i)}\} . \tag{14}$$

Then by the definition of K_i^*, the character group corresponding K_i^* is equal to $X_i^* X$. Now we have

9) Cf. [8, Remark].

https://doi.org/10.1017/S0027763000017797 Published online by Cambridge University Press

PROPOSITION 3.1. *Let K be a cyclic extension over $\boldsymbol{Q}$, X be the character group for $K/\boldsymbol{Q}$, and $K^{(i)}$ be the i-th central class field of K with respect to $\boldsymbol{Q}$ in the absolute class field of K in narrow sense. Then X_i^* being as* (14), *we have*

$$G(K^{(i+1)}/K^{(i)}) \cong X_i^* X/X \cong X_i^*/(X_i^* \cap X) .$$

3.4. In the case where $K = \boldsymbol{Q}(\sqrt{d})$, a quadratic field, we can determine X_i^* as follows more explicitly by using the result of § 1.3.

Since $\mathfrak{R}^{(1)}$ consists of ambigous classes and any ambigous class of $\boldsymbol{Q}(\sqrt{d})$ is represented by a ramified prime ideal[10], $R_0^{(1)}$ consists of prime divisors of the discriminant D of $\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q}$.

Let $D = q_1^* \cdots q_n^*$ be the decomposition of D to prime discriminants, namely $q^* = (-1)^{(q-1)/2} q$ for a prime $q \neq 2$ and $q^* = -4$ or ± 8 for $q = 2$. Put

$$\chi_{q^*}(a) = \left(\frac{q^*}{a}\right) . \tag{15}$$

Then[11] X^* is generated by $\chi_{q_1^*}, \cdots, \chi_{q_r^*}$. Let p be a prime number such that[12] $\chi_{q_i^*}(p) = 1$ for $i = 1, \cdots, r$. Assume further that the Diophantine equation

$$x^2 - Dy^2 - 4p = 0 \tag{16}$$

has no solution. Then by § 1.3 the Diophantine equation

$$x^2 - Dy^2 - 4pz^2 = 0 \tag{17}$$

has a primitive solution x, y, z, where z can be taken as a prime number. We call it a *primitive prime solution* of (17). Then a full set of representatives $R_0^{(i+1)}$ is determined from $R_0^{(i)}$ recursively as follows. Let $S_0^{(i)}$ be a subset of $R_0^{(i)}$ which consists of rational primes $p \in R_0^{(i)}$ such that $\chi_{q_i^*}(p) = 1$ for $i = 1, \cdots, r$, and (16) has no solution. For every such p choose a primitive prime solution $p' = z$ of (17). Then as $R_0^{(i+1)}$ we can take the union of primes p' and $R_0^{(i)}$.

Then we can determine X_i^* by (14), and $z_{K/k}^{(i)}$ by Proposition 2.2 explicitly.

10) See for instance G. Gras [12, Corollaire 4.2].
11) See also H. Hasse [13].
12) We set always $\chi_{q^*}(q) = 1$.

§ 4. *EL*-genus central extensions

4.1. Let K be a Galois extension of an algebraic number field k of finite degree. We call an extension K' of K a *central extension of* K *with respect to* k, when K' is normal over k and the Galois group of K' over K is contained in the center of the Galois group of K' over k. We call K' an *EL-genus extension of* K *with respect to* k, when each local completion of K' is equal to the composite of the corresponding local completion of K and an abelian extension of the corresponding local completion of k. For an extension M of K, we denote by $\hat{K}_{M/k}$ the maximal extension of K which is contained in M and is a central EL-genus extension of K with respect to k. We denote further by $K^*_{M/k}$ the genus field of K in M with respect to k. The structure of the Galois group $G(K^*_{M/k}/K)$ and $G(\hat{K}_{M/k}/K^*_{M/k})$ have been studied in [10]. For the sake of simplicity and of later use, we treate here only the case where M is a ray class field of K mod. $\mathfrak{F}$, $\mathfrak{F}$ being any divisor of K.

For a finite or infinite prime $\mathfrak{P}$ of K we denote by $K_{\mathfrak{P}}$ the local completion of K, by J_K the idele group of K, and by $K^\times$ the multiplicative group of non-zero elements of K. We embed $K_{\mathfrak{P}}$ and $K^\times$ in J_K in usual manner. Denote further by $U_{\mathfrak{P}}(r)$ the group of units u of $K_{\mathfrak{P}}$ such that $u \equiv 1$ mod. $\mathfrak{P}^r$, where r is a non-negative integer. When $\mathfrak{P}$ is an infinite prime, we take $r = 0$ or 1 and by $u \equiv 1$ mod. $\mathfrak{P}$ mean that u is a positive unit or any unit according as $\mathfrak{P}$ is real or imaginary. For a divisor $\mathfrak{F} = \prod_{\mathfrak{P}} \mathfrak{P}^{r_{\mathfrak{P}}}$ of K, set $U_K(\mathfrak{F}) = \prod_{\mathfrak{P}} U_{\mathfrak{P}}(r_{\mathfrak{P}})$.

Now let M be a ray class field of K mod. $\mathfrak{F}$. Then since $K^\times N_{M/K} J_M = K^\times U_K(\mathfrak{F})$, the following propositions imply immediately from Proposition 1, 2 and 3 of [10].

PROPOSITION 4.1. $G(K^*_{M/k}/K) \cong k^\times N_{K/k} J_K / k^\times N_{K/k} U_K(\mathfrak{F})$.

PROPOSITION 4.2.

$$G(\hat{K}_{M/k}/K^*_{M/k}) \cong (k^\times \cap N_{K/k} J_K)/N_{K/k} K^\times (E_k \cap N_{K/k} U_K(\mathfrak{F})) ,$$

where E_k is the group of units of k.

PROPOSITION 4.3. *Notation K, k and M being as above, let L be a subfield of M which contains $K^*_{M/k}$. Then*

$$G(\hat{L}_{M/k}/L) \cong \frac{k^\times \cap N_{L/k} J_L}{N_{K/k}(K^\times \cap N_{L/K} J_L) \cdot (E_k \cap N_{K/k} U_K(\mathfrak{F}))} .$$

Moreover by [10, § 3] we have

PROPOSITION 4.4. *Notation being as Proposition* 4.3, *assume further* $E_k \cap N_{K/k}U_K(\mathfrak{F}) = 1$. *Let* K *and* L *be normal over* k *with Galois groups* g *and* G *respectively, and let* H *be the Galois group of* L *over* K. *Then*

$$G(\hat{L}_{M/k}/L) \cong H^{-3}(G, Z)\Big/\Big(\mathrm{cor}_{H,G}\, H^{-3}(H, Z) + \sum_{\nu} \mathrm{cor}_{G_\nu,G}\, H^{-3}(G_\nu, Z)\Big)\,,$$

$$G(\hat{K}_{M/k}/K^*_{M/k}) \cong H^{-3}(g, Z)\Big/\Big(\sum_{\nu} \mathrm{cor}_{g_\nu,g}\, H^{-3}(g_\nu, Z)\Big)\,,$$

where G_ν *and* g_ν *are decomposition groups in* L/k *resp.* K/k *of an arbitrarily fixed prime divisor in* L *resp. in* K *of a prime* $\mathfrak{p}_\nu$ *of* k.

§ 5. Prime decomposition criteria

5.1. As an application of the previous sections § 1 and § 4, we shall have some criteria of the prime decomposition in certain non-abelian extensions over $\boldsymbol{Q}$. This kind of criteria have been treated formerly by L. Rédei [20], S. Kuroda [18], A. Fröhlich [4] and [6] and Y. Furuta [7], and recently by E. Brown [1], K. Burde [2] and P. Kaplan [16].

PROPOSITION 5.1. *Let* K *be a cyclic extension of an algebraic number field* k *with Galois group* g, *which is generated by* σ. *Let* M *be an abelian extension of* K *which is normal over* k. *Let* L *be an intermediate field between* M *and* K, *and abelian over* k *with Galois group* G. *Then* $K^{(i+1)}_{M/k} \supset L^{(i)}_{M/k} \supset K^{(i)}_{M/k}$. *Let further* $\mathfrak{D} = \mathfrak{D}(M/K)$ *be the ideal class group of* K *corresponding to the class field* M *over* K, *and denote by* $C(\mathfrak{A})$ *the class of* $\mathfrak{D}$ *represented by an ideal* $\mathfrak{A}$ *of* K. *Then the notation* $\mathfrak{H}(L/K)$ *and* $\mathfrak{R}^{(i)} = \mathfrak{R}^{(i)}(\mathfrak{D})$ *being as in* (1) *and* (3), *we have*

$$G(L^{(i)}_{M/k}/K^{(i)}_{M/k}) \cong \mathfrak{D}/C(\mathfrak{H}(L/K))\mathfrak{R}^{(i)} \cong G(K_i/K)\,,$$

where K_i *is the largest extension of* K *in* L *such that every prime* $\mathfrak{p}$ *of* K *is completely decomposed in* K_i *when* $\mathfrak{p}$ *is contained in a class of* $\mathfrak{R}^{(i)}$.

Moreover let $\mathfrak{A}$ *be an ideal of* K *which is the norm of an ideal* $\mathfrak{A}^{(i)}$ *of* $K^{(i)}_{M/k}$ *and prime to the conductor* $\mathfrak{F}(M/K)$, *and* $\mathfrak{B}$ *be an ideal of* K *such that* $\mathfrak{B}^{(\sigma-1)^i} \equiv \mathfrak{A} \bmod. \mathfrak{H}(M/K)$. *Let* σ *and* τ *be elements of* $G(L^{(i)}_{M/k}/K^{(i)}_{M/k})$ *and* $G(K_i/K)$ *which correspond to* $\mathfrak{A}^{(i)}$ *and* $\mathfrak{B}$ *respectively by Artin's reciprocity map. Then* σ *and* τ *correspond each other by the above isomorphism.*

Proof. It follows from the translation theorem of class field theory that the subgroup of $\mathfrak{D}$ corresponding to $L^{(i)}_{M/k}$ over K is equal to $C(N_{L/K}I^i_G(\mathfrak{J}_L)) = C(N_{L/K}(\mathfrak{J}_L)^{(\sigma-1)^i}) = C(\mathfrak{H}(L/K)^{(\sigma-1)^i})$, where $\mathfrak{J}_L$ is the group of ideals of L which is prime to the conductor $\mathfrak{F}(M/L)$. Clearly $C(\mathfrak{H}(L/K)^{(\sigma-1)^i}) \subset \mathfrak{D}^{(\sigma-1)^i}$. Hence $L^{(i)}_{M/k} \supset K^{(i)}_{M/k}$ and we have $G(L^{(i)}_{M/k}/K^{(i)}_{M/k}) \cong \mathfrak{D}^{(\sigma-1)^i}/C(\mathfrak{H}(L/K)^{(\sigma-1)^i})$. Moreover since $L \subset K^*_{M/k} = K^{(1)}_{M/k}$, $C(\mathfrak{H}(L/K)) \supset \mathfrak{D}^{\sigma-1}$. Hence $C(\mathfrak{H}(L/K)^{(\sigma-1)^i}) \supset \mathfrak{D}^{(\sigma-1)^{i+1}}$ and $L^{(i)}_{M/k} \subset K^{(i+1)}_{M/k}$. Now the isomorphism of (1) in § 1 implies immediately the proposition.

5.2. By considering the special case where K is a quadratic field, L is a biquadratic field and $i = 1$, we have some criteria for the prime decomposition in non-abelian normal fields of degree 8.

PROPOSITION 5.2. *Let $\boldsymbol{Q}(\sqrt{d_1})$ and $\boldsymbol{Q}(\sqrt{d_2})$ be two quadratic fields, L be their composite, and $K = \boldsymbol{Q}(\sqrt{d})$ be the intermediate field of L over $\boldsymbol{Q}$ distinct from $\boldsymbol{Q}(\sqrt{d_1})$ and $\boldsymbol{Q}(\sqrt{d_2})$. Let Λ be a quadratic extension of L which is normal and non-abelian over $\boldsymbol{Q}$. Let further M be a normal extension over $\boldsymbol{Q}$, abelian over K and contains Λ. Denote M_0 the largest subfield of M which is abelian over $\boldsymbol{Q}$. Then notation being as in § 1, every prime of K which represents a class of $\mathfrak{R}^{(1)}(D(M/K))$ is decomposed completely in L. Moreover let $\mathfrak{p}$ be a prime ideal of L which is degree 1 over $\boldsymbol{Q}$ and is decomposed completely in M_0. Then we have*

$$(\Lambda/L, \mathfrak{p}) = (L/\boldsymbol{Q}, q) ,$$

where q is any rational prime such that $4pq^2 = x^2 - y^2D$, $\frac{1}{2}(x + y\sqrt{D}) \equiv q \bmod \mathfrak{F}(M/K)$ for $p = N_{L/Q}\mathfrak{p}$, some integers x, y and the discriminant D of $K/\boldsymbol{Q}$.

Proof. We have $L^{(1)}_{M/Q} \supset K^{(1)}_{M/Q} = K^*_{M/Q} = L^*_{M/Q} = M_0$, and Proposition 5.1 implies

$$G(L^{(1)}_{M/Q}/K^{(1)}_{M/Q}) \cong \mathfrak{D}/C(\mathfrak{H}(L/K))\mathfrak{R}^{(1)} , \tag{18}$$

which is isomorphic to a subgroup of $G(L/K)$. Moreover $L^{(1)}_{M/Q}$ is quadratic over $K^{(1)}_{M/Q}$ if and only if every prime of K which represents a class of of $\mathfrak{R}^{(1)}$ is decomposed completely in L. On the other hand since Λ is quadratic over L, Λ is central over L with respect to $\boldsymbol{Q}$. Moreover since Λ is non-abelian over $\boldsymbol{Q}$, we have $L^{(1)}_{M/Q} = \Lambda M_0 \supsetneqq M_0 = K^{(1)}_{M/Q}$. Thus our first assertion of the proposition is proved.

Let $\mathfrak{p} = N_{M_0/L}\mathfrak{P}$ for a prime $\mathfrak{P}$ of M_0. Then Proposition 5.1 implies

https://doi.org/10.1017/S0027763000017797 Published online by Cambridge University Press

$$(\Lambda/L, \mathfrak{p}) = (\Lambda M_0/M_0, \mathfrak{P}) = (L/K, \mathfrak{q}) ,$$

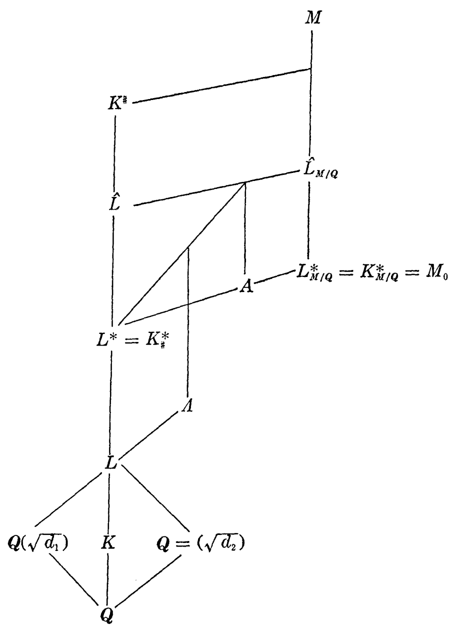
where $\mathfrak{q}^{\sigma-1} \equiv N_{M_0/K}\mathfrak{P}$ mod. $H(M/K)$, σ being the generator of $G(K/\boldsymbol{Q})$. Now the last assertion of the proposition follows from § 1.3.

PROPOSITION 5.3. *Let K, L and Λ be as in Proposition 5.2. and assume that Λ is an EL-genus extension of L with respect to $\boldsymbol{Q}$. Then every prime of K which is ramified over $\boldsymbol{Q}$ is decomposed completely in L. Moreover let $K^{\#}$ be the absolute class field of K in narrow sense and $K^{*}_{\#}$ be the genus field of K in $K^{\#}$ with respect to $\boldsymbol{Q}$. Let $\mathfrak{p}$ be a prime of L which is of degree 1 over $\boldsymbol{Q}$ and decomposed completely[13] in $K^{*}_{\#}$. Then there exists an abelian extension A of $\boldsymbol{Q}$ such that*

$$(\Lambda/L, \mathfrak{p}) = (L/\boldsymbol{Q}, q)(A/\boldsymbol{Q}, p) ,$$

where $p = N_{L/\boldsymbol{Q}}\mathfrak{p}$ and $4pq^2 = x^2 - y^2D$ by the discriminant D of $K/\boldsymbol{Q}$ and rational integers x and y such that $(q, x, y) = 1$.

Proof. It is well known that L is contained in $K^{\#}$. We apply Proposition 5.2 to the case where M contains $K^{\#}$. Let g be the Galois group of L over $\boldsymbol{Q}$, and denote by $\hat{L}$ resp. L^{*} the EL-genus central extension resp. the genus field in $K^{\#}$ with respect to $\boldsymbol{Q}$. Then since



13) This is characterized by using "Auflösung" character.

$$E_Q \cap N_{L/Q}U_L(\mathfrak{F}(M/L)) \subseteqq E_Q \cap N_{L/Q}U_L(\mathfrak{F}(K^\#/L)) = 1 ,$$

Proposition 4.4 implies

$$G(\hat{L}_{M/Q}/L^*_{M/Q}) \cong G(\hat{L}/L^*) \cong H^{-3}(g, Z)/\sum_\nu \operatorname{cor}_{g_\nu, g} H^{-3}(g_\nu, Z) , \tag{19}$$

where g_ν runs over the decomposition groups of primes in L ramified over $\boldsymbol{Q}$. Since Λ is contained in $\hat{L}_{M/Q}$ and Λ is non-abelian over $\boldsymbol{Q}$, $\hat{L}_{M/Q}$ is quadratic over $L^*_{M/Q} = K^*_{M/Q}$. Hence (19) implies $g_\nu \subsetneqq g$ for every ν, which implies the first assertion of the proposition. Now we have $\hat{L}_{M/Q} = \Lambda L^*_{M/Q} = \hat{L}L^*_{M/Q}$. Hence there exists a quadratic extension A of $K^*_\#$ such that A is contained in $L^*_{M/Q}$ and $\hat{L}\Lambda = \hat{L}A$. Let $\mathfrak{p}$ be a norm of a prime $\mathfrak{P}$ of $K^*_\# = L^*$ to L. Then

$$(\Lambda/L, \mathfrak{p}) = (\Lambda L^*/L^*, \mathfrak{P}) = (\hat{L}/L^*, \mathfrak{P})(A/L^*, \mathfrak{P}) .$$

Apply Proposition 5.1 to the case where $k = \boldsymbol{Q}$, $M = K^\#$ and $i = 1$. Then since $L^{(1)}_{M/k} = \hat{L}$ and $K^{(1)}_{M/k} = K^*_\# = L^*$, we have $(\hat{L}/L^*, \mathfrak{P}) = (L/K, \mathfrak{q})$, where $\mathfrak{q}^{\sigma-1} = \mathfrak{p}_1\alpha$, $\mathfrak{p}_1 = N_{L^*/K}\mathfrak{P}$ and α is a totally positive element of K. Moreover it follows from § 1.3 that $(L/K, \mathfrak{q}) = (L/\boldsymbol{Q}, q)$. Clearly $(\Lambda/L^*, \mathfrak{P}) = (A/\boldsymbol{Q}, p)$. Thus the proposition is proved.

5.3. We can have a reciprocity law of the restricted biquadratic residue symbol, by applying Proposition 5.2 and 5.3 to the special case $d_2 = -1$.

Let q be a rational prime such that $q \equiv 1 \bmod. 4$, and put $K = \boldsymbol{Q}(\sqrt{-q})$. Let L be the composite of K and $\boldsymbol{Q}(\sqrt{-1})$ and let B be the subfield of degree 4 of the ray class field over $\boldsymbol{Q}$ mod. q. Let further Λ be the subfield of $L(\sqrt[4]{q})B$ over L of degree 2 distinct from LB and $L(\sqrt[4]{q})$. Then it follows from [7, Theorem 2] that if p is a rational prime such that $(q/p) = 1$, then

$$\left(\frac{q}{p}\right)_4 \left(\frac{p}{q}\right)_4 = (\Lambda/L, \mathfrak{p}) , \tag{20}$$

where $(-)_4$ is the forth power residue symbol in $\boldsymbol{Q}$ and $\mathfrak{p}$ is a prime divisor of p in L.

Now let us apply Proposition 5.3 to the right hand side of (20).

PROPOSITION 5.4. *Let p and q be rational primes such that p, $q \equiv 1$*

mod. 4 *and* $(q/p)=1$. *Then we have*[14)]

$$\left(\frac{q}{p}\right)_4\left(\frac{p}{q}\right)_4=\left(\frac{p_1}{q}\right)=\left(\frac{-1}{p_1}\right),$$

where p_1 *is any rational prime which is a primitive solution*[15)] v *of the Diophantine equation* $pv^2=x^2+y^2q$ *or* $pv^2=x^2+4y^2q$ *according as* $q\equiv 1$ *or* $\not\equiv 1$ mod. 8.

Proof. Let notation $L^*, \hat{L}, K^*_\#, M$ and M_0 be as in Proposition 5.3 and its proof. Then $L=L^*=K^*_\#$. Moreover $\hat{L}\supsetneqq L^*$ if and only if the class number of K is divisible by 4, which is equivalent[16)] to $q\equiv 1$ mod. 8.

(i) Assume $q\equiv 1$ mod. 8. Then $\hat{L}\supsetneqq L^*$, which implies $\hat{L}_{M/Q}\supsetneqq L^*_{M/Q}$ by (19) and $\Lambda M_0=\hat{L}_{M/Q}$. Since prime divisors of 2 in $\boldsymbol{Q}(\sqrt[4]{q})$ are unramified over $\boldsymbol{Q}(\sqrt{q})$, we choose M to be the ray class field over K mod. q. Then LB is the unique quadratic extension of $L^*=L$ in M_0. Since $\hat{L}\supsetneqq L=L^*$, it follows from the definition of Λ that Λ is equal to $\hat{L}$ and the field A in Proposition 5.3 is equal to L. Now Proposition 5.3 and (20) imply the present proposition in the case $q\equiv 1$ mod. 8.

(ii) Assume $q\not\equiv 1$ mod. 8. Then $\hat{L}=L^*=L$ as seen above. Moreover we can see[17)] that prime divisors of 2 in $\boldsymbol{Q}(\sqrt[4]{q})$ are ramified over $\boldsymbol{Q}(\sqrt{q})$. This implies that the only prime divisors of 2 are ramified in Λ over L. Thus we choose M to be the ray class field over K mod 2. We note that Λ is not an EL-genus extension of K with respect to $\boldsymbol{Q}$, for otherwise the above equality $\hat{L}=L^*$ contradicts to (19). Now the proposition is followed from Proposition 5.2 and (20).

5.4. The following table is a numerical example for Proposition 5.4 when p and q are smaller than 53 and p_1 is smaller than 19.

The numbers n for $(q/p)_4$ means $n^4\equiv q$ mod. p, and the symbol Δ means $(q/p)_4=-1$.

14) This reciprocity has other expression from that of E. Brown [1], K. Burde [2] or P. Kaplan [16]. The latters follow from S. Kuroda [18]. See also A. Fröhlich [16].

15) There exists such p_1 except the case $p=x^2+y^2q$ by some integers x and y. Cf. §1.3.

16) See for instance H. Hasse [14].

17) See for instance Hasse's Bericht Ia, §11, Satz 9 and II, §9, XI.

p	q	$4q$	$v=p_1$	x	y	$(q/p)_4$	$(p/q)_4$	(p_1/q)
5	29	116	5 13	3 27	1 1	△	△	1 1
5	41		3 7 11 19	2 9 21 42	1 2 2 1	1	△	−1 −1 −1 −1
13	17		3 7 11	7 5 31	2 6 6	△	3	−1 −1 −1
13	53	212	13 17	17 43	3 3	1	11	1 1
17	13	52	2 7 11 19	4 1 43 77	1 4 2 2	3	△	−1 −1 −1 −1
17	53	212	13 17	45 39	2 4	△	△	1 1
29	5	20	1	3	1			
29	53	212	3 19	7 9	1 7	4	△	−1 −1
37	41		3 7 11 19	13 38 34 109	2 3 9 6	△	8	−1 −1 −1 −1
37	53	212	3 19	11 107	1 3	2	△	−1 −1
41	5	20	2 3 7	12 17 27	1 2 8	△	1	−1 −1 −1
41	37	148	2 19	4 73	1 8	8	△	−1 −1
53	17		1	6	1			
53	29	116	3	19	1	△	4	−1
53	37	148	2 19	8 109	1 7	△	2	−1 −1

https://doi.org/10.1017/S0027763000017797 Published online by Cambridge University Press

References

[1] E. Brown, Biquadratic reciprocity laws, Proc. Amer. Math. Soc., **37** (1973), 374–376.

[2] K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. reine und angew. Math., **235** (1969), 175–184.

[3] A. Fröhlich, On the absolute class-group of abelian fields, (I), (II), J. London Math. Soc., **29** (1954), 211–217; **30** (1955), 72–80.

[4] A. Fröhlich, The restricted biquadratic residue symbol, Proc. London Math. Soc., **9** (1959), 189–207.

[5] A. Fröhlich, The genus field and genus group in finite number fields I, II, Mathematika, **6** (1959), 40–46, 142–146.

[6] A. Fröhlich, A prime decomposition symbol for certain non Abelian number fields, Acta Sci. Math., **21** (1960), 229–246.

[7] Y. Furuta, A reciprocity law of the power residue symbol, J. Math. Soc. Japan, **10** (1958), 46–54.

[8] Y. Furuta, The genus field and genus number in algebraic number fields, Nagoya Math. J., **29** (1967), 281–285.

[9] Y. Furuta, On class field towers and the rank of ideal class group, Nagoya Math. J., **48** (1972), 147–157.

[10] Y. Furuta, On nilpotent factors of congruent ideal class groups of Galois extensions, Nagoya Math. J., **62** (1976), 13–28.

[11] L. J. Goldstein, On prime discriminants, Nagoya Math. J., **45** (1972), 119–127.

[12] G. Gras, Sur le ℓ-classes d'ideaux dans les extensions cycliques relatives de degré premier ℓ, Ann. Inst. Fourier, Grenoble, **23, 3** (1973) ,1–48; **23, 4** (1973), 1–44.

[13] H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkörper, J. Math. Soc. Japan, **3** (1951), 45–51.

[14] H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, Math. Nachr., **46** (1970), 61–70.

[15] E. Inaba, Über die Struktur der ℓ-klassengruppe zyklischer Zahlkörper von Primzahlgrad ℓ, J. Fac. Sci. Univ. Tokyo, **4** (1940), 61–115.

[16] P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques réels dont le 2-sous-groupe des classes est cyclique, C. R. Acad. Sci. Paris, **275** (1972), 887–890.

[17] H. Koch, Über die 2-Komponente der Klassengruppe quadratischer Zahlkörper mit zwei Diskriminantenteilern, Math. Nachr., **54** (1972), 309–333.

[18] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern, J. Math. Soc. Japan, **3** (1951), 148–156.

[19] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr., **9** (1953), 351–362.

[20] L. Rédei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. reine und angew. Math., **171** (1934), 131–148.

Kanazawa University