ON META-ABELIAN FIELDS OF A CERTAIN TYPE

YOSHIOMI FURUTA

Let k be an algebraic number field of finite degree, and l a rational prime (including 2); k and l being fixed throughout this paper. For any power l^n of l, denote by ζ_n an arbitrarily fixed primitive l^n -th root of unity, and put $k_n = k(\zeta_n)$. Let r be the maximal rational integer such that $\zeta_r \in k$ i.e. $k_r = k$ and $k_{r+1} \neq k$.

S. Kuroda [7] shows that the decomposition law of rational primes in some absolute non-abelian normal extension is determined by the rational 2^2 -th power residue symbol of Dirichlet, to which A. Fröhlich [1] gives a more general apprehension. L. Rédei defined in [8] a new symbol, which he called "bedingtes Artinsches Symbol" (restricted Artin symbol), and he established in [9] a theory concerning Pell's equations by means of this symbol.

In the present paper, we define in §1 the "restricted l^n -th power residue symbol", which is related to the restricted Artin symbol in the same manner as the ordinary power residue symbol to the ordinary Artin symbol. The restricted l^n -th power residue symbol is a generalization of Dirichlet's symbol mentioned above. So we investigate some meta-abelian extensions over k, for which the decomposition law of prime ideals of k is given by means of the restricted l^n -th power residue symbol. More precisely, let A/k be an abelian extension over k and \Re/A a kummerian extension of A obtained by adjoining to A the l^{n_i} -th roots ω_i of numbers a_i in k (i = 1, ..., t). We call a normal subfied M of \Re a k-meta-abelian l-field over k, or simply k-meta-aeblian, if M contains all the l^{n_i} -th roots of unity. Then the decomposition law of prime ideals of k in a k-meta-abelian l-field is determined. This result is a generalization of that of Kuroda [7] concerning P-meta-abelian 2-field over P, P being the rational number field.

Received, July 10, 1958.

YOSHIOMI FURUTA

The writer would like to express his gratituede to Prof. S. Kuroda and Dr. T. Kubota for their valuable advices.

§1. Preliminaries

For a prime ideal \mathfrak{p} of k prime to $l_{n}^{(1)}$ a number a of k prime to \mathfrak{p} , and a rational integer n, the restricted l^{n} -th power residue symbol $\left[\frac{a}{\mathfrak{p}}\right]_{n}$ is defined recursively as follows:

For $n \\ eq 0$ we set $\left[\frac{a}{p}\right]_n = 1$.²⁾ For $n \ge 1$ and r > 0 the symbol $\left[\frac{a}{p}\right]_n$ is defined fined only when $\left[\frac{a}{p}\right]_{n-r} = 1$, and, if this condition is fulfilled, we put $\left[\frac{a}{p}\right]_n = \zeta_r^x$ where $a^{(Np^{\rho}-1)/l^n} \equiv \zeta_r^x \pmod{p}$, p being the smallest natural number with $l^n | Np^{\rho} - 1$ (we denote here by N, as well hereafter, the absolute norm). For $n \ge 1$ and r = 0 the symbol $\left[\frac{a}{p}\right]_n$ is defined only when $a^{(Np^{\rho}-1)/l^n} \equiv 1 \pmod{p}$, and in this case we put $\left[\frac{a}{p}\right]_n = 1$. Since all the l^r -th roots of unity are incongruent each other mod. p owing to $\zeta_r \in k$, the symbol $\left[\frac{a}{p}\right]_n$ is uniquely defined. For an ideal m of k prime both to a and l with the prime ideal decomposition $m = p_1^{l_1} \dots p_t^{l_t}$, we set $\left[\frac{a}{m}\right]_n = \left[\frac{a}{p_1}\right]_n^{l_1} \dots \left[\frac{a}{p_t}\right]_n^{l_t}$, when each $\left[\frac{a}{p_t}\right]_n (i = 1, \dots, t)$ is defined.

Now, from the definition follows immediately

LEMMA 1. We have $\left(\frac{a}{p}\right)_{t^{t}} = \left[\frac{a}{p}\right]_{t}$ for $1 \leq t \leq r$, where the left-hand-side is the ordinary l^{t} -th power residue symbol mod. \mathfrak{p} in k.

LEMMA 2. Let Ω be a normal extension over k; \mathfrak{p} a prime ideal in k, not ramified in Ω ; and \mathfrak{P} a prime divisor of \mathfrak{p} in Ω . Let further f' and f'' be the degrees³ of \mathfrak{p} with respect to Ω_n/k , and to k_n/k , respectively. If a number a in k satisfies $\left[\frac{a}{\mathfrak{p}}\right]_{n-r} = 1$ in Ω , then putting $\kappa = f'/f''$, we have

(1)
$$\left[\frac{a}{\mathfrak{P}}\right]_n = \left[\frac{a}{\mathfrak{P}}\right]_n^k,$$

¹⁾ Throughout this paper we always assume that p is prime to l.

²⁾ The symbol $\left[\frac{a}{p}\right]_n$ is defined for $n \leq 0$ only for the sake of simplifying the definion.

³⁾ By the degree of a prime ideal \mathfrak{p} of k with respect to a normal extension Ω/k we mean, as usual, the number f such that $N_{\Omega/k}\mathfrak{P}=\mathfrak{p}^{f}$, \mathfrak{P} being a prime divisor of \mathfrak{p} in Ω .

where the left- and right-hand-sides are the restricted l^n -th power residue symbol in Ω , and in k, respectively.

Proof. For $n \\le 0$, (1) is clear. For $n \ge 1$ we have $\left[\frac{a}{\Re}\right]_n = \zeta_x^r$, where x is determined by $a^{(N\mathfrak{p}_{l_1}-1)/n} \equiv \zeta_r^x \pmod{\Re}$, f_1 being the degree of \mathfrak{P} with respect to $\mathfrak{Q}_n/\mathfrak{Q}$. Since both sides of the congruence are numbers of k, $a^{(N\mathfrak{p}_{l_1}-1)/l^n} \equiv \zeta_r^x \pmod{\Re}$, $(M\mathfrak{P}^{f_1}-1)/l^n = (N\mathfrak{P}^{f''}-1)/l^n = ((N\mathfrak{P}^{f''})^\kappa - 1)/l^n = ((1 + sl^n)^\kappa - 1)/l^n \equiv s\kappa = \kappa (N\mathfrak{P}^{f''}-1)/l^n \pmod{R^n}$. Since $a^{sl^n} = a^{N\mathfrak{P}^{f''}-1} \equiv 1 \pmod{\mathfrak{p}}$, by definition, $a^{(N\mathfrak{P}_{l_1}-1)/l^n} \equiv a^{\kappa(N\mathfrak{P}^{f''}-1)/l^n} \equiv \left[\frac{a}{n}\right]_n^\kappa \pmod{\mathfrak{p}}$, which proves (1).

Now, if χ is a character of the Galois group of an abelian extension A/k, we call simply χ a *character of* A/k, and set $\chi(\mathfrak{m}) = \chi(\left(\frac{A/k}{\mathfrak{m}}\right))$, where $\left(\frac{A/k}{\mathfrak{m}}\right)$ is the Artin symbol.

Let $\mathfrak{N}, \mathfrak{B}$ and \mathfrak{C} be subgroups of an abelian group \mathfrak{B} ; and \mathfrak{N} a subgroup of $\mathfrak{B}\mathfrak{C}$. We call \mathfrak{N} an *l^r*-subgroup of $\mathfrak{B}\mathfrak{C}$, if for any $a \in \mathfrak{N}$ there exist $b \in \mathfrak{B}$ and $c \in \mathfrak{C}$ such that a = bc and $b^{i^r} \in \mathfrak{N}$.

Now let A and B be two abelian extensions over k; \mathfrak{A} and \mathfrak{B} their Galois groups; and φ and Ψ their character groups, respectively. Then the Galois group \mathfrak{B} of AB/k is isomorphic to a subgroup of the direct product of \mathfrak{A} and \mathfrak{B} , and the isomorphism is given by $\sigma \to (\sigma_A, \sigma_B)$, where $\sigma \in \mathfrak{B}$, $\sigma_A = \operatorname{rest}_{AB \to A} \sigma$ and $\sigma_B = \operatorname{rest}_{AB \to B} \sigma$. By setting

(2)
$$\varphi\psi(\sigma) = \varphi(\sigma_A)\psi(\sigma_B)$$
 for $\varphi \in \Phi, \ \psi \in \Psi$,

we can imbed \emptyset and Ψ in the character group X of \mathfrak{G} . If we define the homomorphism ι of $\emptyset \times \Psi$ (direct⁴) onto X by

(3)
$$\iota(\varphi \times \psi) = \varphi \psi \quad \text{for } \varphi \times \psi \in \mathbf{0} \times \Psi$$

the character group X of \mathfrak{G} is induced from $\mathscr{O} \times \mathscr{V}$ by the homomorphism ι . Furthermore the character group of $\mathfrak{AB}/\mathfrak{B}$ is induced from \mathscr{O} by the isomorphism $\lambda = \lambda_{k \to B}$ of $\mathfrak{O}/\mathfrak{O} \cap \mathscr{V} \cong \mathfrak{OV}/\mathscr{V}$, i.e.

(4)
$$(\lambda_{k \to B} \varphi) (\overline{\alpha}) = \varphi(\alpha_A)$$

where $\alpha_A = \operatorname{rest}_{AB \to A} \overline{\alpha}$ for $\overline{\alpha} \in \mathfrak{G}(AB/B)$.

⁴⁾ Throughout this paper the notation \times means the direct product.

YOSHIOMI FURUTA

LEMMA 3. Notations being as above, if X_1 is an l^r -subgroup of $\Phi \times \Psi$, then $X_1^* = \mathfrak{c}(X_1)$ is an l^r -subgroup of $\Phi \Psi$. If X_1^* is an l^r -subgroup of $\Phi \Psi$, then there exists an l^r -subgroup X_1 of $\Phi \times \Psi$ such that $\mathfrak{c}(X_1) = X_1^*$.

Proof. (i) Let X_1 be an l^r -subgroup of $\emptyset \times \Psi$. Let further $\chi^* = \varphi \psi \in X_1^*$, $\varphi \in \emptyset$, $\psi \in \Psi : \chi^* = \iota(\chi)$, $\chi = \varphi_1 \times \psi_1 \in X_1$, $\varphi_1 \in \emptyset$, $\psi_1 \in \Psi$; and $\iota(\varphi_1) = \varphi \varphi_0$. Then $\iota(\psi_1) = \psi \varphi_0^{-1}$ and by the assumption $\varphi_1^{l^r} \in X_1$. Hence $\chi^* = \varphi \psi = (\varphi \varphi_0) (\psi \varphi_0^{-1})$, $\varphi \varphi_0 \in \emptyset$, $\psi \varphi_0^{-1} \in \Psi$ and $(\varphi \varphi_0)^{l^r} \in X_1^*$. Therefore $X_1^* = \iota(X_1)$ is an l^r -subgroup of $\emptyset \Psi$.

(ii) Conversely, let X_1^* be an l^r -subgroup of $\mathscr{O}\mathscr{V}$. If we denote by X_1 the group consisting of all $\varphi \times \psi \in \mathscr{O} \times \mathscr{V}$ such that $\varphi \psi \in X_1^*$ and $\varphi^{l^r} \in X_1^*$, then obiousely $\iota(X_1) = X_1^*$, and X_1 is an l^r -subgroup of $\mathscr{O} \times \mathscr{V}$.

§2. Fundamental lemma

Let $K = k_n (\omega_1, \ldots, \omega_t)$, where ω_i is an l^{n_i} -th root of $a_i \in k$ $(i = 1, \ldots, t)$ and $n = \max(n_1, \ldots, n_t)$; A an abelian extension over k containing k_n ; \mathcal{O} and Ψ the character groups of A/k_n and of K/k_n respectively; and $X = \mathcal{O}\Psi$ the character group of AK/k_n in the sense of (3). If we define ψ_i by

(5)
$$\psi_i(\alpha) = \omega_i^{\alpha} / \omega_i$$
 for every $\alpha \in \mathfrak{G}(K/k_n)$,

the character group Ψ of K/k_n is generated by all such ψ_i $(i = 1, \ldots, t)$.

Let U_{σ} be a representative of $\sigma \in \mathfrak{G}(k_n/k)$ in $\mathfrak{G}(AK/k)$. Put $U_{\sigma}^{-1}\alpha U_{\sigma} = \alpha^{\sigma}$ for $\alpha \in \mathfrak{G}(AK/k_n)$, and $\chi^{\sigma}(\alpha) = \chi(\alpha^{\sigma})$ for $\chi \in X$. If $\chi = \varphi \psi$, $\varphi \in \Phi$, $\psi \in \Psi$, then we have

(6)
$$\chi^{\sigma}(\alpha) = \varphi \psi^{\sigma}(\alpha)$$

since $\chi^{\sigma}(\alpha) = \varphi \psi(\alpha^{\sigma}) = \varphi(\alpha_{A}^{\sigma}) \psi(\alpha_{K}^{\sigma}) = \varphi(\alpha_{A}) \psi^{\sigma}(\alpha_{K})$. On the other hand we may write $\omega_{i}^{U\sigma} = \omega_{i} b_{i,\sigma}$ for some $b_{i,\sigma} \in k_{n}$, because $(\omega_{i}^{U\sigma}/\omega_{i})^{l^{n}} = a_{i}^{U\sigma}/a_{i} = 1$. By comparing $\omega_{i}^{U\sigma\alpha^{\sigma}}$ and $\omega_{i}^{\alpha U\sigma}$, we see $\psi_{i}(\alpha^{\sigma}) = \psi_{i}(\alpha)^{U\sigma}$, hence $\psi^{\sigma}(\alpha) = \psi(\alpha)^{U\sigma}$ for any $\psi \in \Psi$. Let l^{μ} be the order of ψ , and c an integer determined by $\zeta_{\mu}^{\sigma} = \zeta_{\mu}^{c}$. Then we have

(7)
$$\psi^{\sigma}(\alpha) = \psi^{c}(\alpha).$$

Put $m = \mu - r$, and assume $m \ge 0$. Then $(\zeta_{\mu}^{lm})^{\sigma} = \zeta_{\mu}^{lm}$ for any $\sigma \in \mathfrak{G}(k_n/k)$. Hence we have

(8)
$$c-1 \equiv 0 \pmod{l^r}$$
 for any $\sigma \in \mathfrak{S}(k_n/k)$.

It is clear that (8) holds for $m \leq 0$. Now, again assume m > 0. Then since $\zeta_{\mu}^{lx} \notin k$ for any positive integer x < m, there exists $\sigma \in \mathfrak{G}(k_n/k)$ such that $(\zeta_{\mu}^{lx})^{\sigma} \neq \zeta_{\mu}^{lx}$ for any positive integer x < m. Hence if $\mu > r$,

(9)
$$c-1 \equiv 0 \pmod{l^{r+1}}$$
 for some $\sigma \in \mathfrak{S}(k_n/k)$.

Now we prove the following fundamental

LEMMA 4. Notations A, K, Φ, Ψ and X being as above, let M be a subfield of AK over k_n , and X_0 the subgroup of the character group $X = \Phi \Psi$ of AK/k_n corresponding to M. If M is a k-meta-abelian l-field over k, then X_0 is an l^r subgroup of $\Phi \Psi$, and conversely.

Proof. By the assumption, $AK \supset M \supset k_n$, therefore in order that M is a k-meta-abelian *l*-field over k, it is necessary and sufficient that M is normal over k. Put $\mathfrak{H} = \mathfrak{G}(AK/M)$.

(i) Suppose that M is normal over k, i.e. $\mathfrak{D}^{\sigma} = \mathfrak{D}$ for any $\sigma \in \mathfrak{S}(k_n/k)$. Then, by (6), $\varphi \varphi \in X_0$ implies $\varphi \varphi^{\sigma} \in X_0$, hence $\varphi^{\sigma} \varphi^{-1} \in X_0$. Let l^{μ} be the order of φ . If $\mu > r$, then by (7), (8) and (9), $\varphi^{\sigma} \varphi^{-1} = \varphi^{c-1} = (\varphi^{l^{r}})^{y}$ for some $\sigma \in \mathfrak{S}(k_n/k)$, where (y, l) = 1. Hence $\varphi^{l^{r}} \in X_0$. If $\mu \leq r$, trivially $\varphi^{l^{r}} \in X_0$. Therefore X_0 is an l^{r} -subgroup of $\mathfrak{O} \Psi$.

(ii) Conversely, suppose that X_0 is an l^r -subgroup of $\mathscr{P}\mathcal{P}$. Let $\mathscr{I} \in X_0$, then there exist $\varphi \in \mathscr{P}$ and $\psi \in \mathscr{P}$ such that $\mathscr{I} = \varphi \psi$ and $\psi^{l^r} \in X_0$. On the other hand by (6) $\mathscr{I}^\circ = \varphi \psi^\circ$ for any $\sigma \in \mathfrak{S}(k_n/k)$, and, by (7) and (8), $\psi^\circ = \psi^c$, where $c - 1 \equiv 0$ (mod. l°). Hence $\mathscr{I}^\circ = \varphi \psi^\circ \in X_0$. Therefore $\mathfrak{F}^\circ = \mathfrak{F}$ for any $\sigma \in \mathfrak{S}(k_n/k)$. Thus the lemma is proved.

§ 3. Theorems

Denote by $\{a\}$ the cyclic group generated by $a \in k$, and set $\{a\}_n = \{a\}/k_n^{ln} \cap \{a\}$. Let ψ be a generating character of $k_n(\omega)/k_n$, ω being an l^n -th root of a. If we denote by $\{\psi\}$ the character group of $k_n(\omega)/k_n$, we see $\{a\}_n \cong \{\psi\}$. Thus, denoting by $[a]_n$ a generating class of $\{a\}_n$, we can identify $[a]_n$ with ψ .

Let $K = k_n$ ($\omega_1, \ldots, \omega_t$), where ω_i is an l^{n_i} -th root of $a_i \in k$ ($i = 1, \ldots, t$) and $n = \max(n_1, \ldots, n_t)$; $\Psi = \langle a_1 \rangle_{n_1} \times \ldots \times \langle a_t \rangle_{n_t}$; A an abelian extension over k with the character group \emptyset . Put $X = \emptyset \times \Psi$. Then the character group X^* of AK/k_n and the group X correspond each other by means of (2) and (3), restricting \emptyset to Ak_n/k_n . Therefore by lemma 3 and lemma 4 we have

THEOREM 1. Every k-meta-abelian l-field M over k corresponds to an l^r -subgroup X_0 of $\Phi^* \times \Psi$, where Φ^* is the restriction to Ak_n/k_n of the character group Φ of an abelian extension A/k and $\Psi = \{a_1\}_{n_1} \times \ldots \{a_t\}_{n_t}$ for $a_i \in k$ and for natural numbers n_i $(i = 1, \ldots, t)$; and conversely.

Notations being as in theorem 1, let \mathfrak{p} be a prime ideal of k not ramified in M/k; \mathfrak{P} a prime divisor of \mathfrak{p} in k_n . If f_0 is the degree of \mathfrak{p} with respect to k_n/k , then by the translation theorem of the class field theory we have for any integer x

(10)
$$\varphi^*(\mathfrak{P}^x) = (\lambda_{k \to k_n} \varphi) \quad (\mathfrak{P}^x) = \varphi(N_{k_n/k} \mathfrak{P}^x) = \varphi(\mathfrak{P}^{f_0 x}),$$

 $\lambda_{k \to k_n}$ being as (4). For $\psi = \psi_1^{x_1} \times \ldots \times \psi_t^{x_t} \in \Psi$, $\psi_i = [a_i]_{n_i}$ $(i = 1, \ldots, t)$, put $n = \max(n_1, \ldots, n_t)$ and $a = \prod_{i=1}^t a_i^{x_i l^{n-n_i}}$. Put further $K = k_n(\omega_1, \ldots, \omega_t)$, ω_i being an l^{n_i} -th root of a_i $(i = 1, \ldots, t)$, and $\psi^* = \iota(\psi)$, ι being the homomorphism of Ψ onto the character group of K/k_n by means of (3). Then $\psi^*(\mathfrak{P}^x) = \left(\frac{a}{\mathfrak{P}}\right)_{l^n}^x$. Moreover by lemma 1 $\psi^*(\mathfrak{P}^x) = \left[\frac{a}{\mathfrak{P}}\right]_n^x$ in k_n . If $\psi^{*i^r}(\mathfrak{P}^x) = 1$, then by lemma 1 $\psi^{*i^r}(\mathfrak{P}^x) = \left[\frac{a}{\mathfrak{P}}\right]_{n-r}^x = 1$, hence by lemma 2

(11)
$$\psi^*(\mathfrak{P}^x) = \left[\frac{a}{\mathfrak{P}}\right]_n^x = \left[\frac{a}{\mathfrak{P}}\right]_n^x,$$

where the last is the symbol in k. Now we define $\psi(\mathfrak{p}^x)$ by

(12)
$$\psi(\mathfrak{p}^{x}) = \left[\frac{a}{\mathfrak{p}}\right]_{n}^{x}$$

and, for $\chi = \varphi \times \psi \in \mathbf{0} \times \Psi$, $\chi(\mathfrak{p}^x)$ by

(13)
$$\chi(p^{x}) = \varphi^{f_{0}x}(\mathfrak{p})\psi^{x}(\mathfrak{p}).$$

THEOREM 2. Let M be a k-meta-abelian l-field over k corresponding by theorem 1 to an l^r -subgroup X_0 of $\Phi \times \Psi$. Then the degree of a prime ideal \mathfrak{p} of k, not ramified in M/k, is equal to $f = f_0 f_1$ where f_0 and f_1 are the smallest integers such that $l^n | N\mathfrak{p}^{f_0} - 1$ and $\chi(\mathfrak{p}^{f_1}) = 1$ for all $\chi \in X_0$, respectively.

Proof. \mathfrak{P} being a prime divisor of \mathfrak{p} in k_n , the degree of \mathfrak{p} with respect to M/k is equal to the product of the degrees of \mathfrak{p} with respect to k_n/k and of \mathfrak{P} to M/k_n . Since the former is equal to f_0 , we have only to show that the

degree of \mathfrak{P} with respect to M/k_n , i.e. the smallest number x such that $\chi^*(\mathfrak{P}^r) = 1$ for all $\chi^* \in X_0^* = \iota(X_0)$ is equal to f_1 . By theorem 1 and lemma 3, $\chi^* \in X_0^*$ implies $\chi^* = \varphi^* \psi^*$ and $\psi^{*l^r} \in X_0^*$ for some $\varphi \in \Phi$ and for some $\psi \in \Psi$. On the other hand, by (10), (11), (12), and (13) we see that $\chi^*(\mathfrak{P}^r) = 1$ under the condition $\psi^{*l^r}(\mathfrak{P}^r) = 1$ if and only if $\chi(\mathfrak{P}^r) = 1$. Furthermore, by (11) and (12) $\psi^{*l^r}(\mathfrak{P}^r) = 1$ if and only if $\psi^{l^r}(\mathfrak{P}^r) = 1$. Whence the theorem follows immediately.

References

- A. Fröhlich, Non abelian laws of prime decomposition, Proc. Int. Congress Math. 1954, Amsterdam. pp. 20-21.
- [2] A. Fröhlich, On fields of class two, Proc. London Math. Soc. (3), 4 (1954), pp. 235-256.
- [3] Y. Furuta, A reciprocity law of the power residue symbol, J. Math. Soc. Japan, 10 (1958), pp. 46-54.
- [4] W. H. Mills, The *m*-th power residue symbol, Amer. J. Math., 73 (1951), pp. 59-64.
- [5] W. H. Mills, Reciprocity in algebraic number fields, *ibid.*, pp. 65-77.
- [6] H. Hasse, Invariante Kennzeichnung relativ-abelscher Zahlkörper mit vorgegebener Galois Gruppe über einem Teilkörper des Grundkörpers, Abh. Deutsch. Akad. Wiss. Berlin, 8 (1947).
- [7] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoischen Körpern, J. Math. Soc. Japan, 3 (1951), pp. 148-156.
- [8] L. Rédei, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, Acta Math. Acad. Sci. Hungaricae, 4 (1954), pp. 1-29.
- [9] L. Rédei, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, *ibid.*, pp. 31-85.

Mathematical Institute Nagoya University