Akagawa, Y.
Osaka J. Math.
23 (1986), 151-179

A TRIPLING ON THE ALGEBRAIC NUMBER FIELD

Dedicated to Professor Nagayoshi Iwahori on his 60th birthday

YASUMASA AKAGAWA

(Received February 3, 1983)
(Revised March 7, 1985)

Throughout this paper we fix an (even or odd) prime number l, $n=l^\nu$ a power of l, and an algebraic number field k which contains $\exp(2\pi i/n)$ and has a finite degree over the rational number field $\boldsymbol{Q}$. For elements $x, y\in k^\times$ and a prime spot $\mathfrak{p}$ in k (abbrev. k-prime), Hilbert's n-th power residue symbol $\left(\frac{x, y|k}{\mathfrak{p}}\right)_n$ is defined by $\sqrt[n]{y}^\sigma=\left(\frac{x, y|k}{\mathfrak{p}}\right)_n\cdot\sqrt[n]{y}$ using norm residue symbol $\sigma=\left(\frac{x, k(\sqrt[n]{y})/k}{\mathfrak{p}}\right)$, which takes the value in the group of the n-th roots of 1 in k, W. We denote the completion of k at $\mathfrak{p}$ by $k_\mathfrak{p}$ and the group of the n-th roots of 1 in $k_\mathfrak{p}$ by $W_\mathfrak{p}$. After the canonical inclusions of fields $k\subset k_\mathfrak{p}$ and of Galois groups $G(k_\mathfrak{p}(\sqrt[n]{y})/k_\mathfrak{p})\subset G(k(\sqrt[n]{y})/k)$, the (global) Hilbert's power residue symbol is extended to the local symbol $(x, y|k_\mathfrak{p})_n$ taking the value in $W_\mathfrak{p}$. We put

$$(x, y)_n=\prod_{\text{all } k\text{-prime } \mathfrak{p}}(x, y|k_\mathfrak{p})_n$$

which is a pairing on $k^\times$ taking the value in the group $\prod_\mathfrak{p} W_\mathfrak{p}$. Then this pairing symbol admits fundamental properties like the multiplicativity about each component, the conjugacy theorem about isomorphism $\tau: k\to k^\tau$, and the transgression theorem about the lifting of k to some extension k'/k. Moreover it has the norm theorem saying that x is in the norm group $N_{K/k}K^\times$; $K=k(\sqrt[n]{y})$, if and only if $(x, y)_n=1$ and further it has the reciprocity law saying that $(x, y)_n=(y, x)_n^{-1}$.

In this paper we define a tripling symbol $(x, y, z)_n\in W$ on $k^\times$. Not that it is defined for all the elements of $k^\times\times k^\times\times k^\times$, but it is done only for the ones having a property named *strictly orthogonal*. The definition of strict orthogonality is rather complicated but we shall illustrate here some sufficient conditions for it. In case $l\neq 2$, $\{x, y, z\}$ are strictly orthogonal if they are all n-th powers in $k_\mathfrak{l}^\times$ at any $\mathfrak{l}|(l)$ under inclusion $k\subset k_\mathfrak{l}$ and any two of them are orthogonal about the symbol $(\ ,\ )_n$. In case $l=2$ we need some additional conditions; saying when $\exp(2\pi i/4n)\in k$, $\{x, y, z\}$ are strictly orthogonal if further any two of them are orthogonal about $(\ ,\ )_{2n}$. Our results of this paper are the

following properties of the symbols: It is multiplicative about each component, admits the conjugacy, and has the transgression relation (Theorem 1). It has the norm theorem saying that $z \in N_{L/k}L^\times$, $L=k(\sqrt[n]{x}, \sqrt[n]{y})$ if and only if $(x, y, z)_n = 1$, under the assumption that $\{x, y, z\}$ are in the above illustrated situation (Theorem 2a). (This theorem is described for general strictly orthogonal triples by some modifications, Theorems 2, 2a.) Further this symbol has the reciprocity law $(x, y, z)^{-1}=(y, x, z)=(z, y, x)$ namely it is alternative about the permutation of entries, under some few conditions only when $l=3$ (which can be erased if $\exp(2\pi i/3n) \in k$) (Theorem 3).

When $n=2$ and $k=\boldsymbol{Q}$, Furuta defined a symbol $[d_1, d_2, a]=\pm 1$ for some $d_1, d_2, a \in \boldsymbol{Q}^\times$ and obtained some properties of it similar to ours. But the reciprocity law $[d_1, d_2, a]=[d_1, a, d_2]$ is not completed in it though the possibility for it is suggested by tables of values of the symbol. Our symbol is an extension of Furuta's (Section 3, vi)), completing the reciprocity law.

When x and y are strictly orthogonal and the principal ideals (x) and (y) are different k-primes except n-th power, the existence of some central extension M/k containing $L=k(\sqrt[n]{x}, \sqrt[n]{y})$ which is unramified on L is determined by the checking of $(x, y, z)_n=1$, z running over the elements of $k^\times$ such that the principal ideal (z) is an n-th power ideal, so in a finite set essentially (the end of Section 1). For example, let $n=3$ and $k=\boldsymbol{Q}(\sqrt{-3})$. Let $x, y \in k^\times$ generate prime pirncipal ideals (x) and (y) different from each other, $L=k(\sqrt[3]{x}, \sqrt[3]{y})/k$ be unramified at $\mathfrak{l}|(3)$, and $(x, y)_3=1$. Then the class number of L is divisible by 3 if and only if $(x, y, \zeta_3)_3=1$, $\zeta_3=\exp(2\pi i/3)$. Such condition for L is the same that $k(\sqrt[3]{xy})$ (and $k(\sqrt[3]{xy^2})$) has an unramified cyclic extension of degree 3 not derived from the genus field. Fix this x and let y run under the above conditions. Then, if we apply the reciprocity law for the above vanishing of the symbol, the relative density of the set of prime ideals (y) such that L has the class number divisible by 3 in the set of all the (y) is calculated to be 1/3 (the end of Section 2). The last statement will be extended by some accordant modification to any n and $k=\boldsymbol{Q}(\exp(2\pi i/n))$.

About the class number of $k(\sqrt[5]{x}, \sqrt[5]{y})$; $x, y \in k=\boldsymbol{Q}(\exp(2\pi i/5))$, a simple example is given (Section 3 viii)).

1. Definition of (x, y, z)

We denote the ring of rational integers by $\boldsymbol{Z}$ and $Z(n)=\boldsymbol{Z}/n\boldsymbol{Z}$. When a finite set A in a group is given, $\langle A \rangle$ means the subgroup generated by A. For a natural number m and $F^\times$ the multiplicative group of a field F, we put $(F^\times)^m=\{x^m \mid x \in F^\times\}$. When an m-ple element $\{x_1, \cdots, x_m\}$ in $F^\times$ can hold

$$x_1^{n_1} \cdots x_m^{n_m} \equiv 1 \bmod (F^\times)^l \qquad \text{only if} \quad n_1 \equiv \cdots \equiv n_m \equiv 0 \bmod l,$$

we say that $\{x_1, \cdots, x_m\}$ is l-independent. The algebraic closure of a field F will

be denoted by $\bar{F}$. Put $n'=n$ or $2n$ according as $l\neq 2$ or $l=2$ respectively. Let ζ_m imply a primitive m-th root of 1 in general and ζ a fixed one among ζ_n's. When $A\subset\bar{k}^\times$ is given, we use the notation $k\{A\}=k(\sqrt[n]{A})=k(\sqrt[n]{x}\,|\,x\in A)$, $k\{A\}'=k(\sqrt[n']{A})$ regardless the condition $\zeta_{n'}\in k$ (but uniquely determined if $-1\in\langle A\rangle\cdot(k)^n$, as $\zeta_{n'}\in k\{A\}\subset k\{A\}'$) and samely for local case.

Let $G^*=\prod^*\langle\sigma_i^*\rangle=\langle\sigma_1^*,\cdots,\sigma_r^*\rangle$ be the free group of a finite rank $r\geqq 1$. Let $\{N_\lambda^*\,|\,\lambda\in\Lambda\}$ be the set of all the normal subgroups of G^*, with (finite) l-power indices. By $N_{\lambda'}^*\subset N_\lambda^*\rightleftarrows\lambda'\geqq\lambda$, the index set Λ is directed. Together with the canonical homomorphism $\phi_{\lambda,\lambda'}$: $G^*/N_{\lambda'}^*\to G^*/N_\lambda^*$ given for every pair $\lambda'\geqq\lambda$, $\{G^*/N_\lambda^*;\ \phi_{\lambda,\lambda'}\}$ forms a projective system. The projective limit

$$\mathfrak{G}=\varprojlim_\lambda G^*/N_\lambda^*$$

is called the free pro-l group of rank r. The open subgroups of $\mathfrak{G}$ are given by $\mathfrak{N}_\lambda=\mathrm{Ker}\,(\mathfrak{G}\to G^*/N_\lambda^*)$ by definition and $\mathfrak{G}$ is compact and totally disconnected. Since N_λ^*'s are again finitely generated free groups of rank $(r-1)[G^*:N_\lambda^*]+1$ by the well-known Schreier's Theorem, any open subgroup of $\mathfrak{G}$ is again free pro-l group itself and has l-power index in $\mathfrak{G}$. The subset $\{s_1,\cdots,s_r\}$, $s_i=\lim(\sigma_i^* \bmod N_\lambda^*)$, in $\mathfrak{G}$ forms a (topologico-algebraic) generator system of $\mathfrak{G}$. When a finite l-group G and r elements $\sigma_1,\cdots,\sigma_r$ in G are given, there exists uniquely a homomorphism η: $G^*\to G$ such that $\eta(\sigma_i^*)=\sigma_i$, accordingly uniquely a homomorphism $\bar{\eta}$: $\mathfrak{G}\to G$ such that $\bar{\eta}(s_i)=\sigma_i$; $i=1,\cdots,r$. Thus we know specially that there is a surjective homomorphism from $\mathfrak{G}$ on $G=\underbrace{Z(l)\times\cdots\times Z(l)}_{r}$ its kernel being the Frattini subgroup of $\mathfrak{G}$ by itself and the images of s_i's forming a $Z(l)$-basis of G, which means that $\{s_1,\cdots,s_r\}$ is a minimal generator system of $\mathfrak{G}$. Further we know that $\mathfrak{G}$ has the universal mapping property about finite l-groups, that is, when a row-exact diagram

$$\begin{array}{ccccc} & & \mathfrak{G} & & \\ & & \downarrow{\scriptstyle\bar{\eta}} & & \\ P & \xrightarrow{\theta} & G & \longrightarrow & 1 \end{array}$$

of another finite l-group P and homomorphism arrows, it can be completed to a commutative diagram

$$\begin{array}{ccccc} & & \mathfrak{G} & & \\ & \swarrow^{\psi} & \downarrow{\scriptstyle\bar{\eta}} & & \\ P & \xleftarrow{\theta} & G & \longrightarrow & 1\,. \end{array}$$

Because, we may take any $\tau_i\in\theta^{-1}(\sigma_i)$ for each σ_i and define ψ so that $\psi(s_i)=\tau_i$. Taking $\varprojlim$, $\mathfrak{G}$ has also the universal mapping property about pro-l groups.

The free pro-l group of rank 1 is the one isomorph to the additive group of the l-adic integers $\boldsymbol{Z}_l$. The unit group will be joined to pro-l groups, giving rank 0.

For each k-prime $\mathfrak{l}$ over (l), we shall fix a local Galois extension $\Omega^{\mathfrak{l}}/k_{\mathfrak{l}}$ whose Galois group $G(\Omega^{\mathfrak{l}}/k_{\mathfrak{l}})$ is a free pro-l group (of any rank $\geqq 0$), e.g., $\Omega^{\mathfrak{l}}=k_{\mathfrak{l}}$, $\Omega^{\mathfrak{l}}=$ the maximal unramified l-extension, $\Omega^{\mathfrak{l}}=$the cyclotomic $\boldsymbol{Z}_l$-extension. When $l\neq 2$ and $\boldsymbol{Q}_l\subset F$ is any local subfield of $k_{\mathfrak{l}}$ not containing ζ_l, the maximal l-extension Ω/F has the free pro-l Galois group of rank $[F:\boldsymbol{Q}_l]+1$ [7]. So, if we put $\Omega^{\mathfrak{l}}=\Omega k_{\mathfrak{l}}\subset\overline{k_{\mathfrak{l}}}$, $G(\Omega^{\mathfrak{l}}/k_{\mathfrak{l}})$ is a free pro-l group of rank $([F:\boldsymbol{Q}_l]+1-1)[\Omega\cap k_{\mathfrak{l}}:F]+1=[\Omega\cap k_{\mathfrak{l}}:\boldsymbol{Q}_{\mathfrak{l}}]+1$. When r' is a natural number not greater than this number and $k_{\mathfrak{l}}\subset\Omega'\subset\Omega^{\mathfrak{l}}$ is an intermediate Galois extension having Galois group $G(\Omega'/k_{\mathfrak{l}})$ generated by at most r' elements, using the universal mapping property we can find a pro-l extension of $k_{\mathfrak{l}}$ in $\Omega^{\mathfrak{l}}$ containing Ω' and its Galois group being a free pro-l group having rank r'. So, for example when $l\neq 2$, $k_{\mathfrak{l}}$ has always a free pro-l extension of rank 2 cantaining the maximal unramified l-extension and the cyclotomic $\boldsymbol{Z}_l$-extension simultaneousely.

Let F/k be a finite Galois l-extension. From the Kummer theory, $(F^\times)^n\cap k^\times/(k^\times)^n$ is isomorph to $\mathrm{Hom}(G(F/k),\langle\zeta_n\rangle)$ in virtue of the pairing

$$(\sigma, b)\mapsto \sqrt[n]{b}^{\sigma-1};\quad \sigma\in G(F/k),\quad b\in(F^\times)^n\cap k^\times$$

choosing an arbitrary $\sqrt[n]{b}$. When τ is an automorphism of F such that $k^\tau=k$ and $\zeta^\tau=\zeta'\in\langle\zeta_n\rangle$, this isomorphism is also τ-isomorphism because $\sqrt[n]{b}^\tau$ is one of $\sqrt[n]{b^\tau}$'s and

$$(\sqrt[n]{b}^{\tau\sigma\tau^{-1}-1})^\tau=(\sqrt[n]{b^\tau})^{\sigma-1}.$$

(We note that $G(F/k)$ is made a τ-group by $\sigma\mapsto\tau^{-1}\sigma\tau$ and, when A is a τ-group, $\mathrm{Hom}(A,\langle\zeta_n\rangle)$ is also a τ-group defining the action of τ by $\hat{a}^\tau(a)=(\hat{a}(a^{\tau^{-1}}))^\tau$; $\hat{a}\in\mathrm{Hom}(A,\langle\zeta_n\rangle)$, $a\in A$).

Lemma 1. *When $\zeta\in k^\times$ and $G(\Omega^{\mathfrak{l}}/k_{\mathfrak{l}})$ is a free pro-l group,*

(1) $(\xi,\zeta_m|F)_n=1$; $\xi\in F^\times\cap(\Omega^{\mathfrak{l}\times})^n$, $\zeta_m\in F^\times$, $m=l^\mu\geqq n$

(2) $(\xi,\eta|F)_n=1$; $\xi,\eta\in F^\times\cap(\Omega^{\mathfrak{l}\times})^n$

about local Hilbert power residue symbols, for any finite extension $F/k_{\mathfrak{l}}$ in $\Omega^{\mathfrak{l}}$, and

(3) $F^\times\cap(\Omega^{\mathfrak{l}\times})^n=(F^\times)^n\cdot N_{F'/F}(F'^\times\cap(\Omega^{\mathfrak{l}\times})^n)$

for any succession of finite extensions $F'\supset F\supset k_{\mathfrak{l}}$ in $\Omega^{\mathfrak{l}}$.

Proof. (1) is evident because $F\{\xi\}/F$ can be contained in a larger cyclic extension in $\Omega^{\mathfrak{l}}$ of any given l-power degree. Since a subgroup of finite index in a free pro-l group is again a free pro-l group, we may prove (2) and (3) only in the case where $F=k_{\mathfrak{l}}$ and rank $G(\Omega^{\mathfrak{l}}/k_{\mathfrak{l}})\geqq 1$. Since $(\xi,\xi|F)_n=1$ from (1)

even if $l=2$ and $F^\times/(F^\times)^n$ has the type $(n, \cdots, n)$, we may prove (2) when $\eta^{n/l} \notin (F^\times)^n \cdot \langle \xi \rangle$. Put $H=\langle \sigma \rangle = G(F\{\xi\}/F)$ and let $G=H \cdot Z(n)[H]$ be the semi-direct product of H and the group ring $Z(n)[H]$. We fix an isomorphism $G(F\{\eta\}/F) \cong Z(n)[H]/(1-\sigma)Z(n)[H]$ which is extended canonically to $G(F\{\xi, \eta\}/F) = G(F\{\xi\}/F) \times G(F\{\eta\}/F) \cong G/(1-\sigma)Z(n)[H]$. Using the universal mapping property it can be extended further to $\theta: G(\Omega^1/F) \to G$ which becomes surjective by itself because $(1-\sigma)Z(n)[H]$ is the commutator subgroup of G, so in the Frattini subgroup of G. Let E/F be belonged to Ker θ in the sense of Galois theory. Since $G(E/F\{\xi\}) \cong Z(n)[H]$ as H-groups, we have

$$\mathrm{H}^0(H, \mathrm{Hom}(G(E/F\{\xi\}), \langle \zeta \rangle)) \cong \mathrm{H}^{-1}(H, G(E/F\{\xi\})) = 1 \qquad \text{(see [9])}.$$

So, from the Kummer theory $\mathrm{Hom}(G(E/F\{\xi\}), \langle \zeta \rangle) = F\{\xi\}^\times \cap (E^\times)^n/(F\{\xi\}^\times)^n$, we can find $v \in F\{\xi\}^\times \cap (E^\times)^n$ such that

$$N_{F\{\xi\}/F} v \equiv \eta \bmod (F\{\xi\}^\times)^n .$$

Since $(F\{\xi\}^\times)^n \cap F^\times = (F^\times)^n \cdot \langle \xi \rangle$ we have (2). We denote the left and the right hand sides of (3) by X and Y respectively. For (3) only to show $X \subset Y$ is required. Let us use the induction about $[F': F]$, so we may assume $[F': F]=l$ and $F'=F(\sqrt[l]{\xi})$; $\xi \in X$. Take $\xi' \in F'^\times \cap (\Omega^{1\times})^n$ such that $F'\{\xi'\}/F$ is a cyclic extension of degree ln containing $F\{\xi\}$. Then $\xi \in (F^\times)^n \cdot \langle N_{F'/F}\xi' \rangle \subset Y$ because $(\sqrt[n]{\xi'})^{1+\sigma+\cdots+\sigma^{l-1}}$ is one of $\sqrt[n]{N_{F'/F}\xi'}$, $\langle \sigma \rangle = G(F'/F)$, and $((\sqrt[n]{\xi'})^{1+\sigma+\cdots+\sigma^{l-1}})^{\sigma-1} = \sqrt[n]{\xi'^{\sigma^l-1}} = \zeta_n$. Further we have seen just above that if $\eta \in X$ and $\eta^{n/l} \notin (F^\times)^n \cdot \langle \xi \rangle$ then also $\eta \in (F^\times)^n \cdot \langle \xi \rangle \cdot N_{F\{\xi\}/F} v \subset Y$. Since X is spanned by a ξ and all such η's, (3) follows. q.e.d.

The product of the real archimedean k-primes will be denoted by ∞, $=1$ if $l \neq 2$. For a fractional divisor $\mathfrak{a}$ in k, we denote the set of its k-prime factors by $S_k(\mathfrak{a})$. For a finite set $A \subset k^\times$, we define a finite set of prime k-divisors $S_{km}(A)$ (or $S_m(A)$) by

$$S_m(A) = \{\mathfrak{p} \mid \mathfrak{p} \in S((l)\infty) \quad \text{or} \quad k(\zeta_m, \sqrt[m]{A})/k \quad \text{is ramified at } \mathfrak{p}\}.$$

We should note that $S(x) = S((x)) \cup S((l)\infty)$ for the principal ideal (x) and $S(l) = S(1) = S((l)) \cup S(\infty)$.

Abbrev. $S_n(A) = S(A)$ and $S_{n'}(A) = S'(A)$. When $x, y \in k^\times$ satisfy

$$(4) \qquad \left(\frac{x, y \mid k}{\mathfrak{p}}\right)_n (= (x, y \mid k_\mathfrak{p})_n) = 1 \qquad \text{at a } \mathfrak{p}$$

we say that x and y are orthogonal at $\mathfrak{p}$ and when x and y are orthogonal at any $\mathfrak{p} \in S(x, y)$ therefore at every $\mathfrak{p}$, both are said orthogonal. From Lemma 1, (4) is satisfied at $\mathfrak{l} \mid (l)$ if

$x, y \in (\Omega^{\mathfrak{I}\times})^n$ after the canonical inclusion $k \subset k_{\mathfrak{I}}$.

In this case, multiplying suitable elements in $(k^\times)^n$ to x and y if necessary, we can make

(5) $\quad x \in N_{k_{\mathfrak{I}}(y)/k_{\mathfrak{I}}}(k_{\mathfrak{I}}\{y\}^\times \cap (\Omega^{\mathfrak{I}\times})^n)$, $\quad y \in N_{k_{\mathfrak{I}}(x)/k_{\mathfrak{I}}}(k_{\mathfrak{I}}\{x\}^\times \cap (\Omega^{\mathfrak{I}\times})^n)$

because of (3), without influence on the orthogonality of x and y. When $l \neq 2$, we shall say x and y are *strictly orthogonal* if both are orthgoonal and satisfy (5) at any $\mathfrak{I}|(l)$. Next we intend to give the same definition when $l=2$. Note that x and y are orthogonal at a $\mathfrak{p} \notin S(l)$ such that $(\zeta, x|k_{\mathfrak{p}})_2=1$ and $(\zeta, y|k_{\mathfrak{p}})_2=1$ or more sufficiently such that $\zeta_{n'} \in k_{\mathfrak{p}}$ if and only if

(6) $\quad [k_{\mathfrak{p}}\{-x, y\} : k_{\mathfrak{p}}] \leqq n$ or (accordingly and) $\quad [k_{\mathfrak{p}}\{x, -y\} : k_{\mathfrak{p}}] \leqq n$.

Because, we can put easily $\langle -x, y\rangle \cdot (k_{\mathfrak{p}}^\times)^n = \langle \xi^{l^i}, \eta^{l^j}\rangle \cdot (k_{\mathfrak{p}}^\times)^n$ using $i, j \in \{0, 1, \cdots, \nu\}$ and $\xi, \eta \in k_{\mathfrak{p}}^\times$ such that $(\xi, \eta|k_{\mathfrak{p}})_n=\zeta$ and $k_{\mathfrak{p}}^\times = \langle \xi, \eta\rangle \cdot (k_{\mathfrak{p}}^\times)^n$. Then $(x, y|k_{\mathfrak{p}})_n$ $(=(-x, y|k_{\mathfrak{p}})_n$ at such $\mathfrak{p})=1$ if and only if the power residue symbol is trivial on $\langle -x, y\rangle \cdot (k_{\mathfrak{p}}^\times)^n$ therefore if and only if $i+j \geqq \nu$. On the other hand, $[k_{\mathfrak{p}}\{-x, y\} : k_{\mathfrak{p}}] = l^{2\nu-i-j}$ so we obtain the former inequality of (6). Replacing $\{-x, y\}$ by $\{x, -y\}$ we obtain the latter. When x and y are orthogonal and satisfy (5) at any $\mathfrak{I}|(2)$ and further

(7) $\quad \zeta_{n'} \in k_{\mathfrak{p}}$ if $\mathfrak{p} \in S_4(x, y) - S(2)$

(8) $\quad [k_{\mathfrak{p}}\{-x, y\}' : k_{\mathfrak{p}}] \leqq n'$ and $[k_{\mathfrak{p}}\{x, -y\}' : k_{\mathfrak{p}}] \leqq n'$ if $\mathfrak{p} \in S'(x, y) - S(2)$,

then x and y are said *strictly orthogonal.* When a negation of (8), say $[k_{\mathfrak{p}}\{-x, y\}' : k_{\mathfrak{p}}] > n'$ is happened at a $\mathfrak{p} \notin S(2)$, $k_{\mathfrak{p}}\{-x, y\}'/k_{\mathfrak{p}}$ must contain the unramified extension of degree 4 at $\mathfrak{p} \notin S_2(x, y)$ and of degree 2 at $\mathfrak{p} \in S_2(x, y) - S(2)$ so we have easily $\zeta_{4n} \in k_{\mathfrak{p}}\{-x, y\}'$. This means (8) does not depend on the choice of $\sqrt[n']{\mp x}$ nor $\sqrt[n']{\pm y}$ (though $k_{\mathfrak{p}}\{\mp x, \pm y\}'/k$ is not necessarily unique) and it is held outside $S'(x, y)$ by itself. A set $A=\{x_1, \cdots, x_m\}$ in $k^\times$ are said (strictly) orthogonal if so are any pairs $\{x_i, x_j\}$ taken in A, $i \neq j$. When $l \neq 2$, for an orthogonal set $A=\{x_1, \cdots, x_m\} \subset k^\times$ there is an orthgonal set $B=\{y_1, \cdots, y_m\} \subset k^\times$ such that $x_i \equiv y_i \bmod (k^\times)^n$ and $B \subset N_{k_{\mathfrak{I}}(B)/k_{\mathfrak{I}}}(k_{\mathfrak{I}}\{B\}^\times \cap (\Omega^{\mathfrak{I}\times})^n)$ (so B is strictly orthgonal) if and only if $A \subset (\Omega^{\mathfrak{I}\times})^n$ from Lemma 1. In case $l \neq 2$ we say such A is strictly orthgoonal mod $(k^\times)^n$.

Lemma 2. *Let $l=2$. Let $A=\{x, y, z\}$ be a strictly orthogonal triple in $k^\times$. Then*

(9) $\quad \zeta_{4n} \in k_{\mathfrak{p}}$ *at any* $\mathfrak{p} \in S_2(A) - S(2)$.

Proof. Fix such a $\mathfrak{p}$. From (7) we know $\zeta_{n'} \in k_{\mathfrak{p}}$. We may assume $\mathfrak{p} \in S_2(x)$ so $k_{\mathfrak{p}}(\sqrt{x})/k_{\mathfrak{p}}$ is ramified. Then both $k_{\mathfrak{p}}\{x\}'/k_{\mathfrak{p}}$ and $k_{\mathfrak{p}}\{-x\}'/k_{\mathfrak{p}}$ are

purely ramified cyclic extensions of degree n'. Here assume that $k_\mathfrak{p}(\sqrt{y})/k_\mathfrak{p}$ is, accordingly $k_\mathfrak{p}(\sqrt{-y})/k_\mathfrak{p}$ is also, unramified. Then by (8), $k_\mathfrak{p}(\sqrt{y})=k_\mathfrak{p}=k_\mathfrak{p}(\sqrt{-y})$ therefore $k_\mathfrak{p}\{-y\}'\subsetneqq k_\mathfrak{p}\{x\}'$ and $k_\mathfrak{p}\{y\}'\subsetneqq k_\mathfrak{p}\{-x\}'$ accordingly

$$k_\mathfrak{p}\{x\}=k_\mathfrak{p}\{-x\}\supset k_\mathfrak{p}\{y,\ -y\}'\supset k_\mathfrak{p}\{-1\}'$$

meaning (9). After all we may assume that the three extensions $k_\mathfrak{p}(\sqrt{x})$, $k_\mathfrak{p}(\sqrt{y})$, $k_\mathfrak{p}(\sqrt{z})$ over $k_\mathfrak{p}$ are all ramified. Then by (8)

$$(k_\mathfrak{p}^\times)^{n'}\cdot\langle x\rangle=(k_\mathfrak{p}^\times)^{n'}\cdot\langle -y\rangle=(k_\mathfrak{p}^\times)^{n'}\cdot\langle z\rangle=(k_\mathfrak{p}^\times)^{n'}\cdot\langle -x\rangle$$

which means again (9). q.e.d.

Under the condition (9) we have easily

$$(x_j,\ \zeta_n\,|\,k_\mathfrak{p})_2=(x_j,\ -1\,|\,k_\mathfrak{p})_n=1;\quad x_j\in A\,,\ \mathfrak{p}\notin S(2)\,.$$

So, the next comming condition (11) given for the subextension $k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p}$ in an abelian extension $k_\mathfrak{p}(\zeta_{n'})\{x_j\}'/k_\mathfrak{p}$ is independent on the choice of $\sqrt[n']{x_j}$ so well-defined.

Corollary 1. *Let $A=\{x_1,\cdots,x_m\}$ be an m-ple in $k^\times$. If* (7) *and* (9) *are satisfied for A, i.e., if $\zeta_{n'}\in k_\mathfrak{p}$; $\mathfrak{p}\in S_4(A)-S(2)$ and $\zeta_{4n}\in k_\mathfrak{p}$; $\mathfrak{p}\in S_2(A)-S(2)$ only when $l=2$, then the following conditions* (10) *and* (11) *and the previous condition* (8) *are all equivalent each other:*

(10) $\quad[k_\mathfrak{p}\{x_i,\ x_j\}'\colon k_\mathfrak{p}]\leqq n';\quad x_i,\ x_j\in A\ (i\neq j);\ \mathfrak{p}\in S'(A)-S(l)$

(11) $\quad(x_i,\ k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p})=\mathrm{id.};\ x_i,\ x_j\in A\ (i\neq j);\ \mathfrak{p}\in S'(A)-S(l)\,.$

So, if $m\geqq 3$, among the conditions (5), (7), (8) *of strict orthogonality, the last one* (8) *can be replaced by* (10) *or by* (11).

Proof. We may assume $l=2$ and prove the equivalence of (8), (10), and (11) under the assumptions (7) and (9) at a fixed $\mathfrak{p}\in S'(A)-S(2)$. When $\mathfrak{p}\in S_2(A)$, $[k_\mathfrak{p}\{\pm x_i,\ \pm x_j\}'\colon k_\mathfrak{p}]$ does not depend on the choice of $\pm$signs from (9), so (8) and (10) are equivalent. When $\mathfrak{p}\in S'(A)-S_2(A)$, $k_\mathfrak{p}\{\pm x_i,\ \pm x_j\}'/k_\mathfrak{p}$ has ramification index $\leqq n$, independent on the choice of $\pm$signs, and samely for the independence of relative degree provided it is $\geqq 4$. For the negations of (8) and of (10) the very last condition that the relative degree $\geqq 4$ is necessary in common so we have the equivalence of (8) and (10). Next, when $\mathfrak{p}\in S_4(A)$, $\zeta_{n'}\in k_\mathfrak{p}$ and $(\zeta_{n'},\ x_i\,|\,k_\mathfrak{p})_2=1$ for any $x_i\in A$ from (7) and (9) so applying (6) described about n' instead of n, we have the equivalence of (8) and (11). When $\mathfrak{p}\in S'(A)-S_4(A)$, we treat at first the case where both $x_i,\ x_j\in(k_\mathfrak{p}^\times)^2$. We may assume $k_\mathfrak{p}\{x_i,\ x_j\}'\supsetneqq k_\mathfrak{p}\{\sqrt{x_i},\ x_j\}$ therefore it is a sharp quadratic extension; because if they are the same, the cyclic extension $k_\mathfrak{p}\{x_i,\ x_j\}'/k_\mathfrak{p}\{x_i\}'$ must be trivial, in other words $x_j\in\langle x_i\rangle\cdot(k_\mathfrak{p}^\times)^{n'}$ so both (10) and (11) can stand always by themselves. Under

this assumption, (10) becomes

$$[k_\mathfrak{p}\{\sqrt{x_j}, x_i\} : k_\mathfrak{p}] \leqq n .$$

Since $k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p}$ is a cyclic extension, (11) is also rewritten as

$$(\sqrt{x_i}, x_j | k_\mathfrak{p})_n = 1 .$$

From $(\zeta, \sqrt{x_i}|k_\mathfrak{p})_2=(\zeta, x_j|k_\mathfrak{p})_2=1$ we can apply (6) again for $\sqrt{x_i}$ and x_j and obtain the equivalence of (10) and (11). The last remained case is $\mathfrak{p}\in S'(A)-S_4(A)$ and at least one of x_i and x_j, say x_j, is not in $(k_\mathfrak{p}^\times)^2$. Then $n \neq 2$ and $[k_\mathfrak{p}\{x_j\}' : k_\mathfrak{p}]=n'$ so (10) is equivalent to $x_i \in \langle x_j\rangle \cdot (k_\mathfrak{p}^\times)^{n'}$. At the same time, $[\mathrm{Ker}(\ , k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p}) : (k_\mathfrak{p}^\times)^{n'}]=[k_\mathfrak{p}^\times : (k_\mathfrak{p}^\times)^{n'}]/|\mathrm{Im}(\ , k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p})|=[k_\mathfrak{p}^\times : (k_\mathfrak{p}^\times)^{n'}]/n'=n'$ or n according as $\zeta_{n'}\in k_\mathfrak{p}$ or not, so it is equal to $[\langle x_j\rangle \cdot (k_\mathfrak{p}^\times)^{n'} : (k_\mathfrak{p}^\times)^{n'}]$. On the other hand, $(x_j, k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p})=\mathrm{id.}$ is evident, so $\mathrm{Ker}(\ , k_\mathfrak{p}\{x_j\}'/k_\mathfrak{p})=\langle x_j\rangle \cdot (k_\mathfrak{p}^\times)^n$. Thus (10) and (11) are equivalent also in this case. q.e.d.

From this Corollary, we have easily

Corollary 2. *Let $A=\{x_1, \cdots, x_m\}$ be a strictly orthogonal m-ple in $k^\times$, $m\geqq 3$ and $A\subset N_{k_\mathfrak{l}\{A\}/k_\mathfrak{l}}(k_\mathfrak{l}\{A\}^\times \cap (\Omega^{\mathrm{I}\times})^n)$ at every $\mathfrak{l}|(l)$. Then, any subset of $\langle A\rangle \subset k^\times$ is again strictly orthogonal.*

Let us denote the idèle group, the principal idèle group, and the idèle class group of k by J_k, P_k, and C_k respectively. When a finite set $S=\{\mathfrak{p}\}$ of prime k-divisors are given, the restricted product $\prod'_{\mathfrak{p}\in S}k_\mathfrak{p}^\times$ is a closed subgroup of J_k. We shall state here Hasse Normensatz in a little sharper form.

Theorem H. *Let K/k be a cyclic extension, S be finite, and J' be an open $G(K/k)$-subgroup of J_K containing $\prod'_{\mathfrak{p}\in S}K_\mathfrak{p}^\times : K_\mathfrak{p}=\sum_{\mathfrak{B}|\mathfrak{p}} K_\mathfrak{B}$. Put $P'=J'\cap P_K$ and $C'=J'/P'$. Then P' and C' are also $G(K/k)$-groups, $C'\cong C_K$, and there is an exact sequence*

$$1 \to P' \to J' \to C' \to 1 .$$

The cohomology homomorphism

$$\mathrm{H}^0(G(K/k), P') \to \mathrm{H}^0(G(K/k), J')$$

induced from the former is injective. In other words,

$$P' \cap N_{K/k}J' = N_{K/k}P' .$$

The proof is given as a direct consequence of the isomorphism $C'\cong C_K$ obtained by the approximation theorem, accordingly of $\mathrm{H}^{-1}(G(K/k), C')=\mathrm{H}^{-1}(G(K/k), C_K)=1$.

When $\{x, y\}$ is l-independent, we denote the Galois automorphism in

$G(k\{x,y\}/k)$ such that $\sqrt[n]{x}\mapsto\zeta\cdot\sqrt[n]{x}$, $\sqrt[n]{y}\mapsto\sqrt[n]{y}$ by σ_x.

Proposition 1. *Let $\{x,y\}$ be strictly orthogonal and l-independent. We fix any finite set S of prime k-divisors containing $S'(x,y)$. Put $k\{y\}=K$ and $\sigma=\sigma_y$ in $G(k\{x,y\}/k)$. Then we can find $a\in K^\times$ such that, putting $M=k\{x,y,a\}$,*

(12) $a^{1-\sigma}\equiv x \bmod (K^\times)^n$

(13) $G(M/k\{y\})\cong G(M/k\{x\})\cong Z(n)\times Z(n)$

(14) *if $\mathfrak{P}|\mathfrak{p}\in S(\infty)$ is real in $k\{x,y\}$, it remains so in M/k*

(15) *$M\subset\Omega^{\mathfrak{l}}$ at every $\mathfrak{l}\in S((l))$ under any inclusion $M\subset\overline{k_1}$ over $k\{x,y\}\subset\Omega^{\mathfrak{l}}$ given by* (5)

(16) *$M(\zeta_{n'})\{x,y\}'/k(\zeta_{n'})\{x,y\}'$ is fully decomposed at $\mathfrak{p}\in S-S(l)$ in general but inertial specially if $n=2$, $\zeta_4\notin k_{\mathfrak{p}}$, and $k_{\mathfrak{p}}\{x\}=k_{\mathfrak{p}}\{y\}=k_{\mathfrak{p}}(\zeta_4)$.*

Proof. Let us take, if any, $\mathfrak{p}\in S-S(l)$ and $\mathfrak{P}|\mathfrak{p}$ in K. Put $[K_{\mathfrak{P}}:k_{\mathfrak{p}}]=d$ $(=d_{\mathfrak{p}})$ so the decomposition group $G_{\mathfrak{p}}(K/k)=\langle\sigma|_K{}^{n/d}\rangle$.

We shall treat the case $l\neq 2$ at first. From (6), $\sqrt[d]{x}\in K_{\mathfrak{P}}^\times$ and it is easily seen that

(17) $x=N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\sqrt[d]{x}$.

Here we want to apply Theorem H on

$$J_{Kx}^S=\left\{\prod x_{\mathfrak{P}}\in J_K \;\middle|\; \begin{array}{ll} x_{\mathfrak{P}}\in(\Omega^{\mathfrak{l}\times})^n & ;\ \mathfrak{P}|\mathfrak{l}\in S(l) \\ x_{\mathfrak{P}}\in(K_{\mathfrak{P}}^\times)_u\cdot\langle\zeta_d,\sqrt[d]{x}\rangle & ;\ \mathfrak{P}|\mathfrak{p}\in S-S(l)\end{array}\right\}.$$

Actually $J_{Kx}^S\supset\prod'_{\mathfrak{p}\in S}K_{\mathfrak{p}}^\times$, J_{Kx}^S is $G(K/k)$-invariant and open, and from (5) and (17),

$$x\in N_{K/k}J_{Kx}^S\,.$$

So, we can find $u\in P_{Kx}^S=J_{Kx}^S\cap P_K$ such that

$$x=N_{K/k}u$$

namely $u\in K^\times$ such that

(18) $u\in(\Omega^{\mathfrak{l}\times})^n$ at $\mathfrak{P}|\mathfrak{l}\in S(l)$

(19) $u\in(K_{\mathfrak{P}}^\times)^n\langle\zeta_d,\sqrt[d]{x}\rangle$; $\mathfrak{P}|\mathfrak{p}\in S-S(l)$.

Let us put

$$a=u^\delta\in K^\times;\ \delta=1+2\sigma+\cdots+n\sigma^{n-1}\in\boldsymbol{Z}[G(K/k)]\,.$$

Then

$$a^{1-\sigma}\equiv u^{1+\sigma+\cdots+\sigma^{n-1}}=x \bmod (K^\times)^n$$

and a ssatifies (12). Let us extend $\sigma\in G(k\{x,y\}/k)$ to an element of $G(K\{u^{\sigma^i}|i=0,1,\cdots,n-1\}/k)$ in arbitrary way. Since $\zeta\in K$ we have $\sqrt[n]{u}^{\sigma^n-1}=\sqrt[n]{x}^{\sigma-1}=1$,

so

$$\sigma^n = \mathrm{id.} \qquad \text{as an element of } G(M/k)$$

which implies (13) immediately. The condition (15) follows from (18). When $\mathfrak{P}|\mathfrak{p}\in S-S(l)$, using $d=d_{\mathfrak{p}}$ we reform δ like as

$$\delta = \sum_{i=1}^{n/d} \sigma^{i-1}(i\cdot\Sigma + \frac{n}{d}\cdot\Sigma');\ \Sigma = \sum_{j=0}^{d-1} \sigma^{j\cdot n/d},\quad \Sigma' = \sum_{j=0}^{d-1} j\sigma^{j\cdot n/d}.$$

We can put $u^{\sigma^{n/d}} \equiv u\zeta_c \bmod (K_{\mathfrak{P}}^{\times})^n$; $c\,|\,d$ using (19). Then

(20) $u^{\Sigma} \equiv u^d \cdot \zeta_c^{d(d-1)/2} = u^d \equiv 1 \bmod (K_{\mathfrak{P}}^{\times})^n \cdot \langle x\rangle$.

When specially $l\neq 3$, we have also

(21) $u^{\Sigma'} \equiv u^{d(d-1)/2} \cdot \zeta_c^{d(d-1)(2d-1)/6} \equiv 1 \bmod (K_{\mathfrak{P}}^{\times})^n \cdot \langle x^{(d-1)/2}\rangle$.

Thus

(22) $a \equiv 1 \bmod (K_{\mathfrak{P}}^{\times})^n \cdot \langle x\rangle$; $\mathfrak{P}|\mathfrak{p}\in S-S(l)$

which implies (16) when $l\neq 2$ nor 3. When $l=3$ the last will become

(22)'' $a \equiv (u^{(n/d)\cdot\Sigma'})^{1+\sigma+\cdots+\sigma^{n/d-1}} \equiv \zeta_3^{n(\mathfrak{p})} \bmod (K_{\mathfrak{P}}^{\times})^n \cdot \langle x\rangle$; $\mathfrak{P}|\mathfrak{p}\in S-S(l)$

using an $n(\mathfrak{p})=0$, 1, or 2. Take any element $h\in k^{\times}$ such that

$$h \equiv \zeta_3^{-n(\mathfrak{p})} \bmod (k_{\mathfrak{p}}^{\times})^n;\ \mathfrak{p}\in S-S(3),\quad \equiv 1 \bmod (k_{\mathfrak{l}}^{\times})^n;\ \mathfrak{l}\,|\,(3)$$

and multiply a by this h. Then, ah, instead of a, will satisfy (12)$\sim$(16).

Let next $l=2$. Only when $n=2$, there may exist a $\mathfrak{p}\in S-S(2)$ such that $\zeta_4\notin k_{\mathfrak{p}}$, but such a $\mathfrak{p}$ is unramified in K/k because of (7). We fix a local unit element $\varepsilon_{\mathfrak{p}}\in K_{\mathfrak{P}}$; $\mathfrak{p}\in S-S(2)$, such that $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\varepsilon_{\mathfrak{p}} = -1$ if $d>1$, $\zeta_4\notin k_{\mathfrak{p}}$, and $\sqrt{-x}\in k_{\mathfrak{p}}$ i.e. in the special case of (16) and $\varepsilon_{\mathfrak{p}}=1$ otherwise. We know $\sqrt{\zeta_d}\in K_{\mathfrak{P}}$ at each $\mathfrak{P}|\mathfrak{p}\in S-S(2)$ because it is evident from the first if $d<n$, from (7) if K/k is totally ramified, and in the remained cass $k(\sqrt{y})/k$ is intertial at this $\mathfrak{p}$. By (8) $\sqrt[d]{-x}$ is in $K_{\mathfrak{P}}$ therefore so is $\sqrt[d]{x}$, and (17) can be replaced by

(17)' $x = N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\ \varepsilon_{\mathfrak{p}}\cdot\sqrt[d]{\pm x}$

where $\pm x$ indicates $-x$ only when $d>1$ and $\sqrt{-x}\notin k_{\mathfrak{p}}$ and does $+x$ in the other case. Because, at first when $\pm x=-x$, $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\sqrt[d]{-x} = -x\cdot\zeta_d^{d(d-1)/2} = x$. When next $\pm x=x$ and $\zeta_4\in k_{\mathfrak{p}}$, $d=1$ or $k_{\mathfrak{p}}(\sqrt{x})=k_{\mathfrak{p}}$ so $[k_{\mathfrak{p}}(\sqrt[d]{x}):k_{\mathfrak{p}}]=c<d$ and $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\sqrt[d]{x} = x\cdot\zeta_c^{d(d-1)/2} = x$. When $\pm x=x$ and $\zeta_4\notin k_{\mathfrak{p}}$ this is evident from our choice of $\varepsilon_{\mathfrak{p}}$. This time we define J_{Kx}^{S} by

$$J_{Kx}^{S} = \left\{ \prod x_{\mathfrak{P}}\in J_K \;\middle|\; \begin{array}{ll} x_{\mathfrak{P}}\in (K_{\mathfrak{P}}^{\times})^n\cdot\langle x\rangle & ;\ \mathfrak{P}|\mathfrak{p}\in S(\infty) \\ x_{\mathfrak{P}}\in (\Omega^{\times})^n & ;\ \mathfrak{P}|\mathfrak{p}\in S((2)) \\ x_{\mathfrak{P}}\in (K_{\mathfrak{P}}^{\times})^{n'}\cdot\langle\delta_d,\ \varepsilon_{\mathfrak{p}}\cdot\sqrt[d]{\pm x}\rangle & ;\ \mathfrak{P}|\mathfrak{p}\in S-S(2) \end{array} \right\}.$$

Using again Theorem H we can find $u\in P_{Kx}^{S}=J_{Kx}^{S}\cap P_K$ such that

$$x=N_{K/k}u$$

satisfying (18) and

(19)′ $u\in(K_{\mathfrak{P}}^{\times})^{n'}\cdot\langle\zeta_d, \varepsilon_{\mathfrak{p}}\cdot\sqrt[d]{\pm x}\rangle$; $\mathfrak{P}|\mathfrak{p}\in S-S(2)$
$u>0$ at $\mathfrak{P}|\mathfrak{p}\in S(\infty)$ if $\mathfrak{P}$ is real in $k\{x, y\}$.

The powers of ζ_c in (20) and (21) can take the value 1 or -1 in this time so (22) becomes here

(22)′ $a\equiv\varepsilon_{\mathfrak{p}} \bmod (K_{\mathfrak{P}}^{\times})^{n}\cdot\langle-1, \sqrt{x}\rangle$; $\mathfrak{P}|\mathfrak{p}\in S-S(2)$

which implies (16). ($\sqrt{\pm x^{n/d}}\equiv 1$ is known by (8).) q.e.d.

We have an alternative proof for Proposition 1. Namely, from the orthogonality of x and y, using Theorem H in its original type (i.e. $J'=J_K$) we can find $a\in K$ satisfying (12) and (13). For giving the local conditions (14), (15), and (16), we may multiply a by a suitable element of $k^{\times}$, so as it is done in the case $l=3$ in the above proof. This method will be much easier than that in the body and moreover we can obtain the same conclusions starting from slightly lighter conditions than the strict orthogonality. But we dare take this present step for the convenience of the forthcoming Proposition 4.

Let x and y be l-independent and $k\{x, y\}=L$ so $G/(L/K)\cong Z(n)\times Z(n)$. We shall call a group extension

$$1\longrightarrow Z(n)\xrightarrow{f} G\xrightarrow{g} G(L/k)\longrightarrow 1$$

a fundamentally non-abelian central extension (abbrev. an FNAC-extension) if it is central, i.e., $\mathrm{Im}f$ is in the center of G, and $f(1+n\boldsymbol{Z})=[\bar{\sigma}_x, \bar{\sigma}_y]=\bar{\sigma}_x^{-1}\bar{\sigma}_y^{-1}\bar{\sigma}_x\bar{\sigma}_y$, $\bar{\sigma}_x^{n}=\bar{\sigma}_y^{n}=\mathrm{id}.$ taking some (accordingly any) $\bar{\sigma}_x\in g^{-1}(\sigma_x)$ and $\bar{\sigma}_y\in g^{-1}(\sigma_y)$. Take an $a\in L^{\times}$, not an lth power, and put $L\{a\}=M$. We define f: $Z(n)\cong G(M/L)$ by $f(i+n\boldsymbol{Z})=\sigma_a^{i}$; $i=0, 1, \cdots, n-1$, where σ_a: $\sqrt[n]{a}\mapsto\zeta\cdot\sqrt[n]{a}$. If M/k is Galois and the canonical exact sequence

$$1\longrightarrow Z(n)\xrightarrow{f} G(M/k)\xrightarrow{\text{can.}} G(L/k)\longrightarrow 1$$

is an FNAC-extension, we say M/k is an FNAC-extension and $\{x, y, a\}$ generates it. Then $\{y, x, a^{-1}\}$ generates the FNAC-extension M/k and vice versa. The Galois group $G(M/k)$ has the structure $G(M/k\{x\})\cong G(M/k\{y\})\cong Z(n)\times Z(n)$ and extending the actions of σ_x and σ_y arbitrarily in M/k, $G(M/k)=\langle\sigma_x\rangle\cdot G(M/k\{x\})=\langle\sigma_y\rangle\cdot G(M/k\{y\})$ are semi-direct.

Proposition 2. *Let $\{x, y\}$ be an l-independent pair in $k^{\times}$ and $a_1\in L^{\times}$; $L=k\{x, y\}$. Put $M=L\{a_1\}$. Then M/k is an FNAC-extension and $\{x, y, a_1\}$*

generates it if and only if there is an $a\in K^\times$; $K=k\{y\}$ *which is in* $a_1\cdot(L^\times)^n$ *and satisfies* (12) *and* (13).

Proof. Put $\sigma_x=\rho$ and $\sigma_y=\sigma$. Assume M/k is an FNAC-extension generated by $\{x, y, a_1\}$. Since $G(M/K)=\langle\rho\rangle\times\langle[\rho,\sigma]\rangle\cong Z(n)\times Z(n)$, from Kummer theory there is an $a\in K^\times$ such that $\sqrt[n]{a}^{[\rho,\sigma]}=\zeta\cdot\sqrt[n]{a}$, therefore $a\in a_1\cdot(L^\times)^n$, and $\sqrt[n]{a}^{\rho}=\sqrt[n]{a}$. Noting $(\sqrt[n]{a^{1-\sigma}})^{\rho-1}=\sqrt[n]{a}^{(1-\sigma)(\rho-1)}=\sqrt[n]{a}^{\sigma-\rho\sigma[\rho,\sigma]^{-1}}=\zeta$ and $\sqrt[n]{a^{1-\sigma[\rho,\sigma]^{-1}}}=1$ we obtain (12). The condition (13) is given from the first. The converse will be evident. q.e.d.

Let a and K be as in Proposition 1 and S_K be the set of all the K-extensions of $\mathfrak{p}\in S$. For the principal ideal (a) in K we can put

(23) $(a)\equiv\mathfrak{a}$ (mod n-th power, mod S)

i.e., $(a)=\mathfrak{a}$ except n-th power K-ideal and S_K-factor, where $\mathfrak{a}$ is a k-ideal having no S-factor, because the ramification group of any $\mathfrak{p}\notin S$ is in $G(M/L)$ so in the center of $G(M/k)$ by Proposition 2. From the next proposition a tripling symbol $(x, y, z)\in\langle\zeta\rangle$ is well-defined by

$$(x, y, z;\ \zeta\,|\,k)_n \qquad \text{(or simply } (x, y, z) \text{ etc.)} = \left(\frac{z}{\mathfrak{a}}\right)_n$$

where $\left(\frac{z}{\mathfrak{a}}\right)_n$ is the power residue symbol defined by $\left(\frac{k\{z\}\,|\,k}{\mathfrak{a}}\right)\colon \sqrt[n]{z}\to\left(\frac{z}{\mathfrak{a}}\right)_n\cdot\sqrt[n]{z}$, using Artin symbol $\left(\frac{k\{z\}\,|\,k}{\mathfrak{a}}\right)\in G(k\{z\}\,|\,k)$.

Proposition 3. *Let* $\{x, y\}$ *in* $k^\times$ *be* l*-independent and* $\{x, y, z\}$ *in* $k^\times$ *be strictly orthogonal. Let* $S\supset S'(x, y, z)$ *be a finite set of* k*-primes and* $\mathfrak{a}$ *be as above. Then* $\left(\frac{z}{\mathfrak{a}}\right)_n$ *does not depend on the choices of* S *and of* a *and depends only on* $\{x, y, z\}$ *mod* $(k^\times)^{n'}$.

Proof. Take another S' and another a' than S and a respectively. We may assume $S\subset S'$. We assume at first that $\{a, a'\}$ in $K^\times$ are l-independent. Denote $L=k\{x, y\}$, $M'=L\{a'\}$ and σ'_x, σ'_y, $\sigma_{a'}\in G(M'/k)$ be the analogues of σ_x, σ_y, $\sigma_a\in G(M/k)$. From (16), (a') has no $(S'-S)$-factor except n-th power so we can put

$(a')\equiv\mathfrak{a}'$ (mod n-th power mod S); $\mathfrak{a}'$ having no S'-factor.

By Proposition 2, we can construct a row-exact commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G(M/L) & \xrightarrow{\text{inj}} & G(M/k) & \longrightarrow & G(L/k) & \longrightarrow & 1 \\
 & & \downarrow \text{restr. } \phi & & \downarrow \phi & & \| \text{ id.} & & \\
1 & \longrightarrow & G(M'/L) & \xrightarrow{\text{inj}} & G(M'/k) & \longrightarrow & G(L/K) & \longrightarrow & 1
\end{array}$$

using an isomorphism ϕ such that $\phi: \sigma_x \mapsto \sigma'_x$, $\sigma_y \mapsto \sigma'_y$, $\sigma_a \mapsto \sigma_{a'}$. So, putting $M''=L\{aa'^{-1}\}$ the exact sequence

$$1 \longrightarrow G(M''/L) \xrightarrow{\text{inj}} G(M''/k) \longrightarrow G(L/k) \longrightarrow 1$$

is split because $G(MM'/L)=G(M/L)\times G(M'/L)$ and $M''=(MM')^{\langle(\sigma_a,\sigma_{a'})\rangle}$. So we can put

(24) $aa'^{-1}\equiv a_0 \bmod (L^\times)^n$ by a suitable $a_0\in k^\times$.

From (14)$\sim$(16), $M''\subset MM'$ satisfies

$$\begin{cases} M''/L \text{ is unramified at } \mathfrak{P}\,|\,\mathfrak{p}\in S(\infty) \\ M''\subset\Omega^{\mathfrak{l}} \text{ at } \mathfrak{l}\,|\,(l) \\ M''(\zeta_{n'})\{x,y\}'/k(\zeta_{n'})\{x,y\}' \text{ is fully decomposed at } \mathfrak{p}\in S-S(l)\,. \end{cases}$$

Therefore, noting to $(\langle -1, x^{n/n'}, y^{n/n'}\rangle\cdot(k_\mathfrak{p}^\times)^n)^{n'/n}=\langle x,y\rangle\cdot(k_\mathfrak{p}^\times)^{n'}$,

$$(25)\quad \begin{cases} a_0\in(k_\mathfrak{p}^\times)^n\cdot\langle x,y\rangle;\ \mathfrak{p}\in S(\infty) \\ a_0\in(\Omega^{\mathfrak{l}\times})^n;\ \mathfrak{l}\,|\,(l) \\ a_0^{n'/n}\in\langle x,y\rangle\cdot(k_\mathfrak{p}^\times)^{n'};\ \mathfrak{p}\in S-S(l)\,. \end{cases}$$

Since $(a_0)\equiv\mathfrak{a}\mathfrak{a}'^{-1}$ (mod n-th power, mod S) from (24), we have

$$\left(\frac{z}{\mathfrak{a}}\right)_n\left(\frac{z}{\mathfrak{a}'}\right)_n^{-1}=\left(\frac{z}{\mathfrak{a}\mathfrak{a}'^{-1}}\right)_n=\Pi_{\mathfrak{p}\in S(\mathfrak{a}\mathfrak{a}'^{-1})}\left(\frac{a_0,\,z\,|\,k}{\mathfrak{p}}\right)_n=\Pi_{\mathfrak{p}\in S}\left(\frac{a_0,\,z\,|\,k}{\mathfrak{p}}\right)_n^{-1}=1$$

from (25) and orthogonality of $\{x,y,z\}$. When $\{a,a'\}$ are not l-independent, take a principal prime $\mathfrak{b}=(b)$ in k such that $b\in(k_\mathfrak{p}^\times)^{n'}$ at any $\mathfrak{p}\in S\cup S(\mathfrak{a})$. Then ab satisfies the conditions of a in Proposition 1, in fact (13) follows from the l-independence of $\{a,b\}$ in L. Since $\{a,ab\}$ and $\{ab,a'\}$ are l-independent respectively, using the former arguments again we have $\left(\frac{z}{\mathfrak{a}}\right)_n=\left(\frac{z}{\mathfrak{a}\mathfrak{b}}\right)_n=\left(\frac{z}{\mathfrak{a}'}\right)_n$. q.e.d.

Later on we shall know that our (x,y,z) can have a non-trivial value, in fact we may use the forthcoming Theorem 2. But here we show this fact directly when $l\neq 2$. Take x, y, S, a, and M in Proposition 1. Multiplying a suitable element in $k^\times$ to a if necessary, we may assume that $\mathfrak{a}$ in (23) is not an l-th power ideal in k. By means of the class field theory we can pick up a $z\in k^\times$ such that $(z)=\mathfrak{z}$ is a prime principal ideal outside S, fully decomposed in M/k, $z\in(k_\mathfrak{p}^\times)^n$ at $\mathfrak{p}\in S$ but $\left(\frac{z}{\mathfrak{a}}\right)_n=\zeta$, because $k\{x,y\}/k$ is the maximal abelian subextension in M/k. Then $\{x,y,z\}$ are strictly orthogonal, l-independent, and

$$(x, y, z) = \left(\frac{z}{\mathfrak{a}}\right)_n = \zeta \neq 1 .$$

The strict orthogonality of $\{x, y, z\}$ is not entirely required in the proof of Proposition 3. Namely, let $\{x, y\}$ be strictly orthogonal and l-independent, $\{x, y, z\}$ orthogonal, and $(\xi, z|k_\mathfrak{l})_n=1$ for $\xi \in k_\mathfrak{l}^\times \cap (\Omega^{\mathfrak{l}\times})^n$ be satisfied, then $\left(\frac{z}{\mathfrak{a}}\right)_n$ is also uniquely determined after investigation of the proof. So, set $\Omega^\mathfrak{l}=$ the maximal unramified l-extension over $k_\mathfrak{l}$ for every $\mathfrak{l}|(l)$. We denote the unit group of $k_\mathfrak{l}$ by $U_\mathfrak{l}$ and put

$$U_{kn} = \{z \in k^\times \mid S(z) \subset S(l) \quad \text{and} \quad z \in U_\mathfrak{l} \cdot (k_\mathfrak{l}^\times)^n;\ \mathfrak{l}|(l)\} .$$

Then the definition of (x, y, z) can be extended to any triple elements $\{x, y, z\}$ such that $\{x, y\}$ are strictly orthogonal and l-independent, $\{x, y, z\}$ are orthogonal, and $z \in U_{kn}$. Let us think the symbol in this extended meaning. We have $U_{kn} \supset (k^\times)^n$ and $[U_{kn}: (k^\times)^n] < \infty$. Let $\{x, y\}$ be an l-independent strictly orthogonal pair such that $\mathfrak{p} \in S(x, y) - S((l))$ are all fully decomposed in $k\{U_{kn}\}$. Then we can see that

$L = k\{x, y\}$ has an unramified FNAC-extension if and only if $(x, y, z)=1$ for any $z \in U_{kn}$.

Because, if this last condition is satisfied for $\{x, y\}$, we have $\left(\frac{z}{\mathfrak{a}}\right)_n = 1$ for a fixed $a \in L^\times$ and $\mathfrak{a}$ given by Proposition 1 and (23). Using the class field theory we can pick up $a_0 \in k^\times$ such that $(a_0) \equiv \mathfrak{a}$ (mod n-th power), $a_0 > 0$ at $\mathfrak{p} \mid \infty$ if $n=2$, and $a_0 \in k_\mathfrak{l}^\times \cap (\Omega^{\mathfrak{l}\times})^n$ for every $\mathfrak{l}|(l)$. Replacing a by aa_0^{-1}, $\{x, y, aa_0^{-1}\}$ generates an FNAC-extension by Proposition 2 and it is unramified over L. Conversely let M/L be an unramified FNAC-extension generated by $\{x, y, a\}$. Then a satisfies all the conditions of Proposition 1 and $(a) \equiv 1$ mod (n-th power). So, $(x, y, z)=1$; $z \in U_{kn}$.

2. Properties of (x, y, z)

Theorem 1. *We assume that each tripling symbol can be defined*:

I *Our symbol is multiplicative with respect to each component*

(26) i) $(xx', y, z) = (x, y, z)(x', y, z)$

ii) $(x, yy', z) = (x, y, z)(x, y', z)$

iii) $(x, y, zz') = (x, y, z)(x, y, z')$.

II *When we substitute ζ by ζ^t; $t \in (\boldsymbol{Z}/n\boldsymbol{Z})^\times$ at our definition,*

(27) $(x, y, z; \zeta^t) = (x, y, z; \zeta)^{t^{-1}}$.

III *When an isomorphism* $\tau: k \cong k^\tau \subset \bar{k}$ *which can be extended to* $\Omega^{\mathfrak{l}} \cong \Omega^{\mathfrak{l}^\tau}$ *at each* $\mathfrak{l}$ *over* (l) *is given, then putting* $\zeta^\tau = \zeta^t$; $t \in (\boldsymbol{Z}/n\boldsymbol{Z})^\times$, *we have the following conjugacy relation*

$$(28)\quad (x, y, z; \zeta \,|\, k)^\tau = (x^\tau, y^\tau, z; \zeta^\tau \,|\, k^\tau) = (x^\tau, y^\tau, z^\tau; \zeta \,|\, k^\tau)^{t^{-1}}.$$

IV *When* k'/k *is a finite extension, we have the following transgression relation*

$$(29)\quad \text{i)}\quad (x', y, z \,|\, k') = (N_{k'/k}x', y, z \,|\, k)$$
$$\text{ii)}\quad (x, y', z \,|\, k') = (x, N_{k'/k}y', z \,|\, k)$$
$$\text{iii)}\quad (x, y, z' \,|\, k') = (x, y, N_{k'/k}z' \,|\, k)$$

for $x, y, z \in k^\times$ *and* $x', y', z' \in k'^\times$, *the definition of the left hand sides being given by the replacement of* $\Omega^{\mathfrak{l}}$ *to* $\Omega^{\mathfrak{l}'} = k'\Omega^{\mathfrak{l}} \subset \overline{k'_{\mathfrak{l}'}}$, *at each* k'*-prime* $\mathfrak{l}' \,|\, \mathfrak{l} \,|\, (l)$. *Here we need some assumptions for* i) *and* ii) *only when* $l=3$: *We assume for* i)

$$\begin{cases} \zeta_{3n} \in k_{\mathfrak{p}} \text{ at every } \mathfrak{p} \in S_3(x) \cap S_3(y) \cap S_3(z) - S(3) \\ \zeta_{3n} \in k'_{\mathfrak{p}'} \text{ at every } \mathfrak{p}' \in S_{k'3}(x') \cap S_{k'3}(y) \cap S_{k'3}(z) - S_{k'}(3) \end{cases}$$

and for ii)

$$\begin{cases} \zeta_{3n} \in k_{\mathfrak{p}} \text{ at every } \mathfrak{p} \in S_3(x) \cap S_3(y) \cap S_3(z) - S(3) \\ \zeta_{3n} \in k'_{\mathfrak{p}'} \text{ at every } \mathfrak{p}' \in S_{k'3}(x) \cap S_{k'3}(y') \cap S_{k'3}(z) - S_{k'}(3) \end{cases}$$

Proof. I i) Let $l \neq 2$. Let $L = k\{x, y\}$ and $a \in K = k\{y\}$ be the ones in Proposition 1, $\{x, y, a\}$ generating an FNAC-extension $M/k \supset L$ and samely $L' = k\{x', y\}$, $a' \in K$ an analogue of a, $\{x', y, a'\}$ generating an FNAC-extension $M'/k \supset L'$. Put $M'' = K\{xx', aa'\}$. Then $(aa')^{1-\sigma} \equiv xx' \bmod (K^\times)^n$, $\sigma = \sigma_y$, so

$$G(M''/K) \cong Z(n) \times Z(n).$$

From the splittings of two exact sequences $1 \to G(M/K) \to G(M/k) \to G(K/k) \to 1$ and $1 \to G(M'/K) \to G(M'/k) \to G(K/k) \to 1$ we know that $1 \to G(MM'/K) \to G(MM'/k) \to G(K/k) \to 1$ is, accordingly $1 \to G(M''/K) \to G(M''/k) \to G(K/k) \to 1$ is split. So

$$G(M''/k\{xx'\}) \cong Z(n) \times Z(n).$$

Thus, from Proposition 2, $\{xx', y, aa'\}$ can become the generator of the FNAC-extension M''/k. We may assume S is taken in common. Since $l \neq 2$, the local conditions (14)$\sim$(16) for aa' are evident. So, aa' is the one for $\{xx', y\}$ in the meaning of Proposition 1. Using $(a) \equiv \mathfrak{a}$, $(a') \equiv \mathfrak{a}'$, so $(aa') \equiv \mathfrak{a}\mathfrak{a}'$ (mod n-th power, mod S), we obtain i). Use the forthcoming (47) and iii) if $l=2$.

ii) is obtained from i) using forthcoming (45) without vicious circle.

iii) is from the multiplicativity of power residue symbol directly.

II By the replacement of ζ to ζ^t, $\sigma=\sigma_y$ in Proposition 1 is changed to σ^t because ζ is in k therefore $\zeta^\sigma=\zeta$. For a satisfying (12)~(16),

$$\begin{aligned} a^{1-\sigma^t} &= a^{(1-\sigma)(1+\sigma+\cdots+\sigma^{t-1})} \\ &\equiv x^{1+\sigma+\cdots+\sigma^{t-1}} \equiv x^t \bmod (k\{y\}^\times)^n . \end{aligned}$$

Thus we know $a^{t^{-1}}$ is that for $(x, y, z; \zeta^t)$ and

$$(x, y, z; \zeta^t) = \left(\frac{z}{\mathfrak{a}^{t^{-1}}}\right)_n = (x, y, z; \zeta)^{t^{-1}} .$$

III By this τ, the entries $\{x, y, z\}$, σ, a, and $\mathfrak{a}$ of Proposition 3 are sent to $\{x^\tau, y^\tau, z^\tau\}$, $\tau^{-1}\sigma\tau$, a^τ, and $\mathfrak{a}^\tau$ respectively. Here a^τ becomes that for (x^τ, y^τ, z^τ) about ζ^t and (12)~(16). Namely

$$(x^\tau, y^\tau, z^\tau; \zeta^\tau) = \left(\frac{z^\tau}{\mathfrak{a}^\tau}\right)_n = \left(\frac{z}{\mathfrak{a}}\right)_n^\tau = (x, y, z; \zeta)^\tau .$$

IV We shall show iii) at first. Take M of Proposition 1 for (x, y, z). Since x and y are l-independent in k' by the assumption, $M \cap k' = k$. By Proposition 2, Mk' can be that for $(x, y, z' \mid k')$. Then the assertion follows from the transgression theorem of power residue symbol

$$\left(\frac{z' \mid k'}{\mathfrak{a}}\right)_n = \left(\frac{N_{k'/k} z' \mid k}{\mathfrak{a}}\right)_n .$$

Samely as the proof of I, i) and ii) are derived from this applying the forthcoming Theorem 3. q.e.d.

As we have seen, the conditions for Theorem 1, IV, i) and ii) come from Theorem 3 (the reciprocity law). The following Proposition is used for the norm theorem and the reciprocity law.

Proposition 4. *Let $\{x, y, z\}$ in $k^\times$ be strictly orthogonal, $\{x, y\}$ be l-independent and the set S contain $S'(x, y) \cup S_{n^2}(z)$. Put $k\{y\}=K$ and $\sigma_y=\sigma$.*

I *We can find $v \in K^\times$ satisfying the following conditions*

(30) $z = N_{K/k} v$

(31) $v \in (K_{\mathfrak{P}}^\times)^n \cdot \langle z \rangle$ *at* $\mathfrak{P} \mid \mathfrak{p} \in S(\infty)$

(32) $v \in (\Omega^{I\times})^n$ *at* $\mathfrak{P} \mid \mathfrak{l} \mid (l)$

(33) $(v, K_{\mathfrak{P}}(\zeta_{n'})\{x, y\}'/K_{\mathfrak{P}}) = id.$ *at* $\mathfrak{P} \mid \mathfrak{p} \in S - S(l)$

(34) $(v) \equiv \mathfrak{B}^{1-\sigma} \pmod{n\text{-th power, mod } S}$,

$\mathfrak{B}$ being a K-divisor such that $S_K(\mathfrak{B}) \cap S_K = \emptyset$.

II *For any such v,*

$$(35)\quad (x, y, z) = \left(\frac{x|K}{\mathfrak{B}}\right)_n^{-1}.$$

III *We can make further* $\mathfrak{B}$ *prime in* K *and outside any given finite set of prime* K*-divisors.*

Proof. We use J_{Kx}^S given in the proof of Proposition 1, replacing x in J_{Kx}^S by z. Then we know again $z \in N_{K/k} P_{Kz}^S$ so we can find $v \in K^\times$ satisfying (30) $\sim$(32) and, instead of (19) and (19)',

$$v \in (K_\mathfrak{B}^\times)^{n'} \cdot \langle \zeta_d, \varepsilon_\mathfrak{p} \cdot \sqrt[d]{\pm z} \rangle ; \mathfrak{P}|\mathfrak{p} \in S - S(l), \quad d = [K_\mathfrak{B} : k_\mathfrak{p}],$$

where $\varepsilon_\mathfrak{p}$ is the same one given there and $\pm z$ indicates $-z$ only when $l=2$, $d>1$, and $\sqrt{-z} \notin k_\mathfrak{p}$, and does $+z$ in the other general case. When $d>1$ at this $\mathfrak{p}$, we have $\sqrt{\zeta_d} \in K_\mathfrak{B}$ because of (7) specially if $l=2$ and $\mathfrak{p}$ is ramified, therefore $\sqrt[d]{x}$, as well as $\sqrt[d]{y}$, is in $K_\mathfrak{B}$ and

$$(x, \zeta_d | K_\mathfrak{B})_{n'} = 1, \quad (y, \zeta_d | K_\mathfrak{B})_{n'} = 1$$

and noting that $k_\mathfrak{p}(\zeta_{n'})\{x, y\}'/k_\mathfrak{p}$ is an abelian extension,

$$(\varepsilon_\mathfrak{p} \cdot \sqrt[d]{\pm z},\ K_\mathfrak{B}(\zeta_{n'})\{x, y\}'/K_\mathfrak{B}) = (z,\ k_\mathfrak{p}(\zeta_{n'})\{x, y\}'/k_\mathfrak{p}) = id.$$

by the strict orthogonality of $\{z, x\}$ and $\{z, y\}$ and by Corollary 1 of Lemma 2. So we obtain (33). When $d=1$, $v \in (K_\mathfrak{B}^\times)^{n'} \cdot \langle z \rangle$ so (33) can be obtained from the same Corollary. Next take a $\mathfrak{P} \in S_K(v) - S_K$, if any. The semi-local theory of cohomology says that for the subgroup $\mathfrak{P}^Z$ of the divisor group of K,

$$\mathrm{H}^{-1}(G(K/k),\ \Pi_{\mathfrak{P}|\mathfrak{p}}(\mathfrak{P}^Z/\mathfrak{P}^{n^2 Z})) \cong \mathrm{H}^{-1}(G_\mathfrak{p}(K/k),\ \boldsymbol{Z}/n^2\boldsymbol{Z})$$
$$= \frac{n^2}{d}\boldsymbol{Z}/n^2\boldsymbol{Z} \subset n\boldsymbol{Z}/n^2\boldsymbol{Z};\ d = [K_\mathfrak{B} : k_\mathfrak{p}].$$

Since evidently

$$N_{K/k}(v) \equiv (z) \equiv 1 \pmod{n^2\text{-th power, mod } S},$$

the $\mathfrak{p}$-factor of (v) represents an element of the above (-1)-cohomology group, so we have

$$(v) \equiv \mathfrak{B}^{1-\sigma}\mathfrak{C}^n \pmod{n^2\text{-th power, mod } S}$$

using K-divisors $\mathfrak{B}$ and $\mathfrak{C}$ accordingly we have (34).

II Let a and $\mathfrak{a}$ be as stated in Propositions 1 and 3. Choose a $b \in k^\times$ such that $(b) = (S(\mathfrak{B})\text{-factor of } \mathfrak{a}) \times (\text{a product of } \mathfrak{p} \notin S(\mathfrak{B}))$ and $b \in (k_\mathfrak{p}^\times)^{n'}$ at $\mathfrak{p} \in S$, $S(\mathfrak{B})$ being the k-projection of $S_K(\mathfrak{B})$. Taking ab^{-1} instead of a from the first, we may assume $S(\mathfrak{a}) \cap S(\mathfrak{B}) = \emptyset$. From (14) and (15), $a \in (K_\mathfrak{B}^\times)^n \cdot \langle x \rangle$ if $\mathfrak{P} \in S_K(\infty)$ and $a \in (\Omega^{\mathrm{I}\times})^n$ if $\mathfrak{P}|\mathfrak{l}|(l)$. So, using (31), (32), and (2) we have

$$(a, v|K_{\mathfrak{P}})_n = 1\,, \qquad \text{for} \quad \mathfrak{P}|\mathfrak{p}\in S(l)\,.$$

At $\mathfrak{P}\in S_K - S_K(l)$, we have $a^{n'/n}\in\langle x, y\rangle\cdot(K_{\mathfrak{P}}^{\times})^{n'}$ (or occasionally $a,\ v\in U_{\mathfrak{P}}\cdot(K_{\mathfrak{P}}^{\times})^2$, $n=2$) from (16) therefore using (33) we have $(v, K_{\mathfrak{P}}\{a^{n'/n}\}'/K_{\mathfrak{P}})=\mathrm{id}.$ and can obtain the same identity as above. Thus

$$\begin{aligned}\left(\frac{x|K}{\mathfrak{B}}\right)_n^{-1} &= \left(\frac{a^{1-\sigma^{-1}}|K}{\mathfrak{B}}\right)_n = \left(\frac{a|K}{\mathfrak{B}^{1-\sigma}}\right)_n = \Pi_{\mathfrak{P}\in S(\mathfrak{B}^{1-\sigma})}\left(\frac{v, a|K}{\mathfrak{P}}\right)_n \\ &= \Pi_{\mathfrak{P}\in S(a)}\left(\frac{a, v|K}{\mathfrak{P}}\right)_n = \left(\frac{v|K}{\mathfrak{a}}\right)_n = \left(\frac{z|k}{\mathfrak{a}}\right)_n \\ &= (x, y, z)\,.\end{aligned}$$

III From the class field theory, we can find an element $b\in K^{\times}$ such that $b\equiv 1$ mod $(K_S^{\times})^{n'}$; $K_S=\sum_{\mathfrak{p}\in S}K_{\mathfrak{p}}$, and (b) is $\mathfrak{B}$ times a K-prime which is outside any given finite set of K-divisors. Substituting v by $vb^{\sigma-1}$ the conditions can be satisfied. q.e.d.

The next lemma is a variation of Theorem H, useful specially in the case $l=2$.

Lemma 3. *Let $\{x, y\}$ be l-independent pair in $k^{\times}$ and $L=k\{x, y\}$. Let $S\supset T$ be two finite sets of k-primes and J' be an open $G(L/k)$-subgroup of J_L containing $\Pi'_{\mathfrak{p}\notin S}L_{\mathfrak{p}}^{\times}$. Put $J''=J'\cdot L_T^{\times}\subset J_L$; $L_T=\sum_{\mathfrak{p}\in T}L_{\mathfrak{p}}$ and then $P'=J'\cap P_L$, $P''=J''\cap P_L$. We assume*

(36) $[L_P: k_{\mathfrak{p}}]\leqq n$ *at* $P|\mathfrak{p}\in T$.

Then

(37) $N_{L/k}P''\cap N_{L/k}J' = N_{L/k}P'$.

Proof. At first we remark that, when $G=Z(n)\times Z(n)\supset H$ and $[G: H]\geqq n$, the restriction map $\mathrm{Res}_{G\to H}$: $\mathrm{H}^3(G, \boldsymbol{Z})\to\mathrm{H}^3(H, \boldsymbol{Z})$ is the nil-map, accordingly about the injection map also

(38) $\mathrm{Inj}_{H\to G}$: $\mathrm{H}^{-3}(H, \boldsymbol{Z})\to\mathrm{H}^{-3}(G, \boldsymbol{Z})$ is the nil-map

(see 3, vii)). Now, we put $J'/P'=C'$ and $J''/P''=C''$, then there are canonical identifications

$$C' = C_L \quad \text{and} \quad C'' = C_L\,.$$

The class field theory says that there is commutative column-isomorphic

$$\begin{array}{ccc}\mathrm{H}^{-1}(G(L/k), L_{\mathfrak{p}}^{\times}) & \xrightarrow{(\text{can.})^{\sharp}} & \mathrm{H}^{-1}(G(L/k), C_L) \\ \downarrow\wr & & \downarrow\wr \\ \mathrm{H}^{-3}(G_{\mathfrak{p}}(L/k), \boldsymbol{Z}) & \xrightarrow{\mathrm{Inj}} & \mathrm{H}^{-3}(G(L/k), \boldsymbol{Z})\,,\end{array}$$

therefore from (36) and (38)

(39) $(\text{can.})^{\natural}$: $\mathrm{H}^{-1}(G(L/k), L_T^{\times}) \to \mathrm{H}^{-1}(G(L/k), C'')$ is the nil-map.

Let us consider the commutative row-exact diagram of cohomology groups with respect to $G(L/k)$,

$$\begin{array}{ccccccc} \mathrm{H}^{-1}(J') & \xrightarrow{g'} & \mathrm{H}^{-1}(C') & \longrightarrow & \mathrm{H}^{0}(P') & \xrightarrow{f'} & \mathrm{H}^{0}(J') \\ \downarrow & & \| & & \downarrow h & & \downarrow \\ \mathrm{H}^{-1}(J'') & \xrightarrow{g''} & \mathrm{H}^{-1}(C'') & \longrightarrow & \mathrm{H}^{0}(P'') & \xrightarrow{f''} & \mathrm{H}^{0}(J''), \end{array}$$

the columns being induced from inclusions. From (39) we have

$$\operatorname{Im} g' = \operatorname{Im} g''$$

therefore (remembering the so-called Five-Lemma)

$$(\operatorname{Ker} h) \cap (\operatorname{Ker} f') = 1 .$$

This means (37) q.e.d.

Theorem 2. *Let $\{x, y\}$ be l-independent and $\{x, y, z\}$ be strictly orthogonal in $k^{\times}$. We put $L=k\{x, y\}$. Define*

$$J_L^{(l)} = \{\prod x_P \in J_L \mid x_P \in (\Omega^{\mathfrak{l}\times})^n \quad at \quad P \mid \mathfrak{l} \in S((l))\}$$

and $P_L^{(l)}=J_L^{(l)} \cap P_L$. Then

$$(x, y, z) = 1$$

if and only if

$$z \in N_{L/k} P_L^{(l)} .$$

Proof. "If"-part. We put $k\{y\}=K$, $z=N_{L/k}w$; $w \in P_L^{(l)}$, and $N_{L/K}w = v \in K^{\times}$. Put $S=S'(x, y) \cup S_{n^2}(z)$. For $\mathfrak{p} \notin S$, L/k is unramified and

$$\mathrm{H}^{-1}(G(L/k), \prod_{P \mid \mathfrak{p}} P^{\boldsymbol{Z}}/P^{n^2\boldsymbol{Z}}) = \frac{n^2}{e}\boldsymbol{Z}/n^2\boldsymbol{Z} \subset n\boldsymbol{Z}/n^2\boldsymbol{Z}; \quad e = [L_P : k_{\mathfrak{p}}]$$

therefore we can put

(40) $(w) \equiv \prod_{\rho \in G(L/k)} B_{\rho}^{1-\rho} \pmod{n\text{-th power, mod } S}$ in L.

So, using the class field theory, we may assume from the first that

B_{ρ}; $\rho \in G(L/k)$, are all L-primes fully decomposed in L/k

multiplying a suitable element in $\prod_{\rho \in G(L/k)} (L^{\times})^{1-\rho}$ to w if necessary (see the method of Proposition 4, III). Then we obtain

(41) $(v) \equiv \mathfrak{B}^{1-\sigma} \pmod{n\text{-th power, mod } S}$ in K

taking $N_{L/K}$ of (40), where $\mathfrak{B}$ is a product of $G(L/k)$-conjugates of B_ρ's and $\sigma=\sigma_y$, so

$$(42)\quad \left(\frac{x|K}{\mathfrak{B}}\right)_n = 1\,.$$

When $l\neq 2$, (32) and (33) are satisfied for this v by itself, so $(x, y, z)=1$ by (42) and (35). When $l=2$, we put

$$I^S_{Lz} = \left\{ \prod x_P \in J^{(2)}_L \;\middle|\; \begin{array}{l} x_P\in(L_P^\times)^n\cdot\langle z\rangle;\ P|\mathfrak{p}\in S(\infty) \\ (x_P, \sqrt[z]{x}\,|L_P)_2=(x_P, \sqrt[z]{y}\,|L_P)_2=1 \quad \text{and} \\ (x_P, \zeta|L_P)_2=1;\ P|\in S_L-S_L(2)\,. \end{array} \right\}$$

Since $\sqrt[z]{x}$ mod $(L_P^\times)^2$ and $\sqrt[z]{y}$ mod $(L_P^\times)^2$ are $G_P(L/k)$-invariant at $P\in S_L-S_L(2)$ from (7), we know that I^S_{Lz} is an open $G(L/k)$-subgroup of J_L containing $\Pi'_{\mathfrak{p}\notin S}L^\times_{\mathfrak{p}}$. Now Proposition 4 shows

$$z\in N_{K/k}(P_K\cap N_{L/K}I^S_{Lz})\subset N_{L/k}I^S_{Lz}\,.$$

We apply Lemma 3 for $J'=I^S_{Lz}$ and $J''=J^{(l)}_L$ putting $T=S-S((2))$. Then

$$z\in N_{L/k}P^{(2)}_L\cap N_{L/k}I^S_{Lz}=N_{L/k}P^S_{Lz};\ P^S_{Lz}=I^S_{Lz}\cap P_L$$

and we can make $w\in P^S_{Lz}$ from the first. Let us make ρ run on a representative system of $G(L/K)/G_{\mathfrak{B}}(L/K)$; $\mathfrak{B}\in S_K-S_K(2)$. Then $v=N_{L/K}w=N_{L_P/K_{\mathfrak{B}}}(\Pi_\rho w^\rho)$, and, since

$$(w^\rho, L_P\{x, y\}'/L_P)=(w, L_{P'}\{x, y\}'/L_{P'})^\rho=1;\ P'=P^{\rho^{-1}}$$

because of $w\in P^S_{Lz}$, (33) follows from

$$(v, K_{\mathfrak{B}}\{x, y\}'/K_{\mathfrak{B}})=(\Pi_\rho w^\rho, L_P\{x, y\}'/L_P)=1\,.$$

Thus in this case again $(x, y, z)=1$ from (42).

"Only if"-part. We put again $S=S'(x, y)\cup S_{n^2}(z)$ and take $v\in K^\times$ as in Proposition 4, specially $\mathfrak{B}$ being a K-prime. From Proposition 4 and assumption $(x, y, z)=1$ we have

$$\left(\frac{x|K}{\mathfrak{B}}\right)_n = 1\,,$$

so, using further (31)~(33) and (3), we known $v\in N_{L/K}J^{(l)}_L$. By Theorem H we can make $v\in N_{L/K}P^{(l)}_L$. q.e.d.

Let us apply Lemma 3 on $S=T=S((l))$, $J'=J^{(l)}_L$, and $J''=J_L$. Then under the assumption $[L_P: k_{\mathfrak{p}}]\leqq n$; $P|\mathfrak{p}|(l)$ we have $N_{L/k}P_L\cap N_{L/k}J^{(l)}_L=N_{L/k}P^{(l)}_L$. Thus Theorem 2 becomes

Theorem 2a. *Let $\{x, y\}$ be l-independent and $\{x, y, z\}$ be strictly orthogonal*

in $k^\times$. *We put* $L=k\{x, y\}$. *If*

(43) $[L_P: k_\mathfrak{p}]\leqq n$ *at every* $P\,|\,\mathfrak{p}\,|\,(l)$

or more sufficiently if

(44) $\operatorname{rank} G(\Omega^\mathfrak{l}/k_\mathfrak{l}) = 0$ *or* 1 *at every* $\mathfrak{l}\,|\,(l)$,

then $(x, y, z)=1$ *is necessary and sufficient for* $z\in N_{L/k}L^\times$.

The next theorem was used in the proof of Theorem 1 already.

Theorem 3. *Let* $\{x, y, z\}$ *be strictly orthogonal and l-independent.*

I *Then*

(45) $(x, y, z)^{-1} = (y, x, z)$.

II *We assume only when* $l=3$,

(46) $\zeta_{3n}\in k_\mathfrak{p}$ *at any* $\mathfrak{p}\in S_3(x)\cap S_3(y)\cap S_3(z)-S(3)$.

Then, for any l,

(47) $(x, y, z)^{-1} = (z, y, x)$.

Proof. I We use the notations of Proposition 1, so $\{x, y, a\}$ generates an FNAC-extension M/k over $L=k\{x, y\}$. Since $a\in L=k\{y, x\}$ and $[\sigma_x, \sigma_y]=[\sigma_y, \sigma_x]^{-1}$ in $G(M/k)$, from Proposition 2 there is an element $b\in k\{x\}$ such that $\{y, x, b\}$ generates the FNAC-extension M/k and $b\equiv a^{-1} \bmod (L^\times)^n$. From this

$$(b)\equiv\mathfrak{a}^{-1} \text{ (mod } n\text{-th power, mod } S) \text{ in } L$$

for $\mathfrak{a}$ of (23), so noting that (b) is in $k\{x\}$,

$$(b)\equiv\mathfrak{a}^{-1} \text{ (mod } n\text{-th power, mod } S) \text{ in } k\{x\}$$

which means (45).

II To prove (47), we let at first $l\neq 3$. Let us take $v\in P_{Kz}^S$, $K=k\{y\}$, such that $N_{K/k}v=z$ and put

$$c = v^\delta;\ \delta = 1+2\sigma+\cdots+n\sigma^{n-1},\ \sigma = \sigma_y .$$

Then c behaves on (z, y, x) as a did on (x, y, z) in Proposition 1. Further, this v was the very one in Proposition 4 and satisfies all the conditions there. So we can put $(v)\equiv\mathfrak{B}^{1-\sigma}$ (mod n-th power, mod S) in K, then we have $(c)\equiv N_{K/k}\mathfrak{B}$ (mod n-th power, mod S) in K and

$$(z, y, x) = \left(\frac{x\mid k}{N_{K/k}\mathfrak{B}}\right)_n = \left(\frac{x\mid K}{\mathfrak{B}}\right)_n .$$

The last is equal to $(x, y, z)^{-1}$ by (35) in Proposition 4.

Let finally $l=3$. In this case ch instead of c behaves as ah did in Proposition 1, where $h\in k$ was

(48) $h\in\langle\zeta_3\rangle\cdot(k_\mathfrak{p}^\times)^n$ at $\mathfrak{p}\in S$ and specially $h\in(k_\mathfrak{r}^\times)^n$ at I|(3).

We investigate this condition in detail and will obtain

(49) $\left(\frac{h,\ x|k}{\mathfrak{p}}\right)_n=1$ at every $\mathfrak{p}\in S$

by a choice of h. If $\mathfrak{p}\in S_3(x)\cap S_3(y)\cap S_3(z)$, (49) at this $\mathfrak{p}$ is evident from (46) and the latter half of (48). If $\mathfrak{p}\notin S_3(x)$, $k(\sqrt[3]{x})/k$ is unramified at this $\mathfrak{p}$ so also (49) at this $\mathfrak{p}$ is easy. If ($\mathfrak{p}\notin S_3(y)$ and) $k_\mathfrak{p}(\sqrt[3]{y})=k_\mathfrak{p}$, n/d is divisible by 3 for $d=[k_\mathfrak{p}\{y\}:k_\mathfrak{p}]$ and we can obtain

$$c\equiv(v^{n/d\cdot\Sigma'})^{1+\sigma+\cdots+\sigma^{n/d-1}}\equiv 1 \bmod (K_\mathfrak{B}^\times)^n\cdot\langle x\rangle$$

seeing the analogeous formula (22)'' of a in Proposition 1. This means that we cake make $h\in k^\times\cap(k_\mathfrak{p}^\times)^n$ so have (49) at $\mathfrak{p}$. If $\mathfrak{p}\notin S_3(y)$ and $k_\mathfrak{p}(\sqrt[3]{y})\supsetneqq k_\mathfrak{p}$ so it is unramified, $\mathfrak{p}$ can not lie in $S_3(x)$ from the orthogonality of x and y at $\mathfrak{p}$ so we are induced to the previous case $\mathfrak{p}\notin S_3(x)$. If ($\mathfrak{p}\notin S_3(z)$ and) $k_\mathfrak{p}(\sqrt[3]{z})=k_\mathfrak{p}$, we have again $[k_\mathfrak{p}(\sqrt[d]{z}):k_\mathfrak{p}]<d$ so (21) becomes about our v

$$v^{\Sigma'}\equiv 1 \bmod (K_\mathfrak{p}^\times)^n\cdot\langle x\rangle$$

and h can be in $k^\times\cap(k_\mathfrak{p}^\times)^n$. If $\mathfrak{p}\notin S_3(z)$ and $k_\mathfrak{p}(\sqrt[3]{z})\supsetneqq k_\mathfrak{p}$, we have $\mathfrak{p}\notin S_3(x)$ as we have seen before. Thus (49) is proved. From the product formula of power residue symbol we have

$$\left(\frac{x\,|\,k}{(h)}\right)_n=\Pi_{\mathfrak{p}\in S}\left(\frac{h,\ x|k}{\mathfrak{p}}\right)_n^{-1}=1$$

and we have again

$$(z, y, x)=\left(\frac{x|k}{((h)\cdot N_{K/k}\mathfrak{B})}\right)_n=\left(\frac{x\,|\,k}{(h)}\right)_n\left(\frac{x\,|\,k}{N_{K/k}\mathfrak{B}}\right)_n=\left(\frac{x\,|\,k}{N_{K/k}\mathfrak{B}}\right)_n$$
$$=(x, y, z)^{-1}.$$ q.e.d.

In Theorem 3, we have settled the condition (46) only for the proof. Whether it is indispensable or not is a problem for future discussion. Of course if $\zeta_{3n}\in k$ then we can skip it and the statements of this theorem and accordingly of Theorem 1-IV will become the simpler. Anyway (46) is not weakest possible for (47). For example, if

(50) $\{\mathfrak{p}\in S_3(x)\,|\,\zeta_{3n}\notin k_\mathfrak{p}\}\subset S_3(y)\cap S_3(z)$,

then the vanishing of the product of terms of (49)

$$\Pi_{\mathfrak{p}\in S}\left(\frac{x,\ h|k}{\mathfrak{p}}\right)_n=\Pi_{\mathfrak{p}\in S}\left(\frac{\zeta,\ x|k}{\mathfrak{p}}\right)_3=1$$

can be checked investigating the above proof, which is equivalent to $\left(\frac{x\,|\,k}{(h)}\right)_n=1$ and sufficient for (47). The condition (46) implies that the left hand side of (50) is outside $S_3(y)\cap S_3(z)-S(3)$, so different from (50).

We shall give a rather noteworthy example for application of the reciprocity law. Before it we remark a matter. Denote the set of $\Omega^{\mathfrak{I}}/k_{\mathfrak{I}}$'s by $\Omega^{(l)}$. When another set $\Omega_1^{(l)}=\{\Omega_1^{\mathfrak{I}}/k_{\mathfrak{I}}\,|\,\mathfrak{I}\,|\,(l)\}$ of free pro-l extensions $\Omega_1^{\mathfrak{I}}/k_{\mathfrak{I}}$ is given, the strict orthogonality will be defined replacing $\Omega^{(l)}$ by $\Omega_1^{(l)}$ in (5). Then we say it specially $\Omega_1^{(l)}$-strictly orthogonal. When a $\Omega_1^{(l)}$-strictly orthogonal pair $\{x, y\}$ in $k^\times$ are given, the a of Proposition 1 will be called P1-element about $\Omega_1^{(l)}$, x, y, and S (or merely about x, y, and S if $\Omega_1^{(l)}=\Omega^{(l)}$). Using this a, by means of Proposition 3 we can define a tripling symbol for further element $z\in k^\times$ if $\{x, y, z\}$ are $\Omega_1^{(l)}$-strictly orthogonal, which will be denoted by $(x, y, z\,|\,\Omega_1^{(l)})$. If $\Omega_1^{\mathfrak{I}}\subset\Omega^{\mathfrak{I}}$ at each $\mathfrak{I}\,|\,(l)$, the definition of $(x, y, z\,|\,\Omega_1^{(l)})$ can be extended to $z\in k^\times$ such that $\{x, y, z\}$ are $\Omega^{(l)}$-strictly orthogonal, using (2) as we stated after Proposition 3. So, suppose like this and let a_1 be a P1-element about $\Omega_1^{(l)}$, x, y, and $S(x, y, z)$. Put

$$(a_1)\equiv\mathfrak{a}_1 \text{ (mod } n\text{-th power, mod } S(x, y, z)) \text{ in } K=k\{y\},$$

$\mathfrak{a}_1$ being a k-prime. By definition, a_1 is a P1-element about x, y, and $S(x, y, z)$ as it were and $(x, y, z)=(z/\mathfrak{a}_1)_n=(x, y, z\,|\,\Omega_1^{(l)})$. Namely, for such $\Omega_1^{(l)}$, l-independent $\Omega_1^{(l)}$-strictly orthogonal pair $\{x, y\}$, and $\Omega^{(l)}$-strictly orthogonal triple $\{x, y, z\}$,

$$(x, y, z)=(x, y, z\,|\,\Omega_1^{(l)}),$$

the right hand side being extended the confine of definition.

Now, let $n=3$, $k=\boldsymbol{Q}(\zeta)$, $\zeta=(-1+\sqrt{-3})/2$. Let $\Omega_1^{\mathfrak{I}}/k_{\mathfrak{I}}$ be the maximal unramified 3-extension at the unique $\mathfrak{I}\,|\,(3)$ and $\Omega^{\mathfrak{I}}/k_{\mathfrak{I}}$ be a free pro-3 extension of rank 2 containing $\Omega_1^{\mathfrak{I}}$ and the cyclotomic $\boldsymbol{Z}_3$-extension $k(\zeta_\infty)=k(\zeta_m\,|\,m=3^\mu;\ \mu=1, 2, \cdots)$. Let $\mathfrak{X}$ be the set of the prime ideals $\mathfrak{x}=(x)$ in k such that $x\in(\Omega_1^{\mathfrak{I}\times})^3$ (note that the class number of k is 1). We take always the generator x of (x) so that $x\in(\Omega_1^{\mathfrak{I}\times})^3$. Fix an $\mathfrak{x}\in\mathfrak{X}$ and put

$$\mathfrak{Y}=\{\mathfrak{y}=(y)\in\mathfrak{X}-\{\mathfrak{x}\}\,|\,\{x, y\} \text{ is } \Omega_1^{(l)}\text{-strictly orthogonal mod } (k^\times)^3\}$$
$$\mathfrak{Z}=\{(y)\in\mathfrak{Y}\,|\,\text{the class number of } k\{x, y\} \text{ is divisible by } 3\}.$$

Then $\{x, y, \zeta\}$ are strictly orthogonal mod $(k^\times)^3$ and 3-independent for any $\mathfrak{y}\in\mathfrak{Y}$. If we check the vanishing of values $(\zeta, y\,|\,k_{\mathfrak{y}})_3=(y, \zeta\,|\,k_{\mathfrak{I}})_3$ and $(x, y\,|\,k_{\mathfrak{y}})_3=(y, x\,|\,k_{\mathfrak{x}})_3$ we know that a k-prime (y) is in $\mathfrak{Y}$ if and only if $\mathfrak{y}$ is fully decomposed in $k\{x, \zeta\}$. In our case we have $U_{k3}=\langle\zeta\rangle\cdot(k^\times)^3$, so from the discussion after Proposition 3, the reciprocity law (47) (note here the set of (46) is vacant), and the aforementioned remark we can say that

(*) $(x, \zeta, y) = 1$ if and only if $(y) \in \mathfrak{Z}$

(Use standard knowledges of l-groups and genus fields.)

Let b be a P1-element about x, ζ, and $S(x, \zeta)$ $(=S(x))$. Put

$$(b) \equiv \mathfrak{b} \text{ (mod cubic power, mod } S(x)) \quad \text{in} \quad \tilde{k} = k(\zeta_9)$$

$\mathfrak{b}$ being in k. After b and $\mathfrak{b}$ are fixed, we can show, for any $\mathfrak{y} = (y) \nmid S(b)$ in $\mathfrak{J}$,

(**) $(x, \zeta, y) = 1$ if and only if $\left(\frac{y \mid k}{\mathfrak{b}}\right)_3 = \left(\frac{b \mid k\{x, \zeta\}}{Y}\right)_3$

for some (so, any) $Y \mid \mathfrak{y}$. Because, let $b' \in \tilde{k}$ be a P1-element about x, ζ, and $S(x, \zeta, y)$ $(=S(x, y))$ and put

$$(b') \equiv \mathfrak{b}' \text{ (mod cubic power, mod } S(x, y)) \quad \text{in} \quad \tilde{k}$$

$\mathfrak{b}'$ being in k. As in the proof of Proposition 3, we can assume $\mathfrak{b}$ and $\mathfrak{b}'$ are different k-primes and can put $bb'^{-1} \equiv b_0 \bmod (\tilde{k}^\times)^3$, $b_0 \in k^\times$. Then from (15) and (16)

$$b_0 \in k_{\mathfrak{l}}^\times \cap (\Omega^{\mathfrak{l}\times})^3$$
$$b_0 \equiv b \bmod (k\{x, \zeta\}_{\mathfrak{y}}^\times)^3;\ k\{x, \zeta\}_{\mathfrak{y}} = \textstyle\sum_{Y \mid \mathfrak{y}} k\{x, \zeta\}_Y$$

over evident relation $(b_0) \equiv \mathfrak{b}\mathfrak{b}'^{-1}$ (mod cubic power, mod $S(x)$). So

$$(x, \zeta, y) = \left(\frac{y \mid k}{\mathfrak{b}'}\right)_3 = \left(\frac{b_0^{-1}, y \mid k}{\mathfrak{b}'}\right)_3$$
$$= \left(\frac{b_0, y \mid k}{\mathfrak{b}}\right)_3 \left(\frac{b_0, y \mid k}{\mathfrak{y}}\right)_3 \left(\frac{b_0, y \mid k}{\mathfrak{l}}\right)_3$$

by product formula. Here $\left(\frac{b_0, y \mid k}{\mathfrak{b}}\right) = \left(\frac{y \mid k}{\mathfrak{b}}\right)$, $\left(\frac{b_0, y \mid k}{\mathfrak{l}}\right) = 1$ by (2), and since $\mathfrak{y}$ is fully decomposed in $k\{x, \zeta\}$,

$$\left(\frac{b_0, y \mid k}{\mathfrak{y}}\right) = \left(\frac{y, b_0 \mid k}{\mathfrak{y}}\right)^{-1} = \left(\frac{b_0 \mid k}{\mathfrak{y}}\right)^{-1} = \left(\frac{b \mid k\{x, \zeta\}}{Y}\right)^{-1}.$$

Thus (**) is proved.

Next, take a $b_k \in k$ such that $(b_k) = \mathfrak{b}$. Since $k(\sqrt[3]{y})/k$ is unramified at $\mathfrak{l}$ and $\mathfrak{b} \neq \mathfrak{l}$,

$$\left(\frac{b_k, y \mid k}{\mathfrak{l}}\right)_3 = 1$$

so there is the reciprocity law of power residue symbol

$$\left(\frac{y|k}{\mathfrak{b}}\right)_3 = \left(\frac{b_k|k}{\mathfrak{y}}\right)_3 .$$

Put $M_0 = k\{x, \zeta, bb_k^{-1}\}$ which is the unique FNAC-extension ovre $k\{x, \zeta\}/k$ unramified except at I such that $M_0 \subset \Omega^{\mathrm{I}} \cdot k_{\mathrm{I}}\{U_{\mathrm{I}}\}$ over canonical inclusion $k \subset k_{\mathrm{I}}$ because of Proposition 2. From the last equality, the right hand side condition of (**) is equivalent to saying that $\mathfrak{y}$ is fully decomposed in $M_0/k\{x, \zeta\}$, accordingly in M_0/k. Thus we obtain the next conclusion:

Take a $\mathfrak{y} \in \mathcal{Q}_f$. Then $\mathfrak{y} \in \mathcal{Z}$ if and only if it is fully decomposed in M_0/k.

From Tschevotareff density law,

$$(\text{density of } \mathcal{Z})/(\text{density of } \mathcal{Q}_f) = 1/[M_0 : k\{x, \zeta\}] = 1/3$$

as we alluded in Introduction.

3. Remarks and simple applications

i) In the above discussions k can be also an algebraic function field of one variable over finite constant field of characterestic $\neq l$, because we have used only the class field theory here.

ii) We can extend the definition of our triple symbol to any strictly orthogonal $\{x, y, z\}$, of not necessarily l-independent $\{x, y\}$. Namely, if x and y are in $k^\times$, using the class field theory we can pick up two principal prime k-ideals $(x') = \mathfrak{x}'$ and $(y') = \mathfrak{y}'$ outside $S'(x, y)$ so that $x' \in k^\times \cap (k^\times_{S'(x,y,z)})^{n'}$ and $y' \in k^\times \cap k^\times_{S'(x,y,z,x')})^{n'}$. Then we can define

$$(51)\quad (x, y, z) = (xx', yy', z)(x', yy', z)^{-1}(xx', y', z)^{-1}(x', y', z) .$$

In fact it is easy to check that the entries of each tripling in the right hand side are l-independent and strictly orthogonal, using Corollary 2 of Lemma 2. From Theorem 1-I, the value of this product does not depend on the choice of x' and y' and (x, y, z) conserves its value if $\{x, y\}$ is l-independent from the first. When $\langle x, y\rangle \not\subset (k^\times)^l$, say $y \notin (k^\times)^l$, taking only x' and defining $(x, y, z) = (xx', y, z)(x', y, z)^{-1}$ we have the same situation.

iii) After this extension of definition, the reciprocity law (Theorem 3) can remain unchanged because each triple symbol in the right hand side of (51) admits this theorem. But, the norm theorem (Theorem 2, 2a) can not hold any longer. For example, let $\{x, y\}$ be l-independent pair in $k^\times$ such that $\{x, y, 1\}$ is strictly orthogonal mod $(k^\times)^n$ and let $n = m^2$, i.e., $\nu = 2\mu$, $m = l^\mu$. Then $\{x, y, 1\}$ is strictly orthogonal mod $(k^\times)^m$. Using the same method in the end of section 1, we can find $z \in k^\times$ such that $\{x, y, z\}$ is strictly orthogonal mod $(k^\times)^n$ accordingly so mod $(k^\times)^m$ and $(x, y, z)_m = \zeta_m$ (cf. Lemma 2 and Corollaries). Then

$$(x^m, y^m, z)_n = (x, y, z)_n^m = 1$$

but, from $(x, y, z)_m \neq 1$, setting all the matters in Theorem 2a

$$z \notin N_{L/k} L^\times ; \; L = k(\sqrt[n]{x^m}, \sqrt[n]{y^m}) = k(\sqrt[m]{x}, \sqrt[m]{y}) .$$

Nevertheless we can say that when $\langle x, y\rangle \not\subset (k^\times)^l$, the norm theorem for the extended (x,y,z) can hold good because, we may assume $y \notin (k^\times)^l$ from the reciprocity law, then it is easy to see that Proposition 4 can be available as it is, which was essential for the proof of the norm theorem.

iv) For our purpose, the condition on $\Omega^{\mathfrak{l}}$ that $G(\Omega^{\mathfrak{l}}/k_{\mathfrak{l}})$ is a free pro-l group was too methodical. In fact, we have used Lemma 1 only when $F/k_{\mathfrak{l}}$ and F'/F are abelian extensions with Galois groups of exponent at most n. So, any $\Omega^{\mathfrak{l}}/k_{\mathfrak{l}}$ can be adopted in our arguments only if $G(\Omega^{\mathfrak{l}}/k_{\mathfrak{l}}) \cong \mathfrak{G}/\mathfrak{G}''$, where $\mathfrak{G}$ is the free pro-l group and $\mathfrak{G}'' = (\mathfrak{G}')'$, $\mathfrak{G}' = [\mathfrak{G}, \mathfrak{G}] \cdot \mathfrak{G}^n$, e.g. $\Omega^{\mathfrak{l}}/k_{\mathfrak{l}}$ is a cyclic extension of degree n^2. When $\xi_0 = \zeta_m, \xi_1, \cdots, \xi_s$ in $k_{\mathfrak{l}}^\times$ are l-independent and orthogonal at $\mathfrak{l}$, we can find such $\Omega^{\mathfrak{l}}/k_{\mathfrak{l}}$ containing $k_{\mathfrak{l}}\{\xi_0, \cdots, \xi_s\}$ [1], [8].

v) We fix some finite set R of k-primes. When x, y in $k^\times$ satisfy

(52) one of x and y is in $(k_{\mathfrak{p}}^\times)^{n'}$ at each $\mathfrak{p} \in R$

and all the conditions (4)$\sim$(8) outside R, we say x and y are R-strictly orthogonal. Let us substitute $S(\infty)$, $S((l))$, and S by $R \cup S(\infty)$, $S((l)) - R$, and $S \cup R$ (so $S(l)$ by $R \cup S(l)$) respectively in the conditions (14)$\sim$(16). Then, after the accordant modification of J^S_{Kx}, the Proposition 1 can stand for R-strictly orthogonal $\{x, y\}$ and the Proposition 3 for R-strictly orthogonal $\{x, y, z\}$. It is not difficult to see Theorem 1 and Porposition 4 accordingly Theorems 2, 2a, and 3 will do for R-strictly orthogonal $\{x, y, z\}$ because it needs only the same routine. We shall omit detailed discussions.

vi) Let $k = \boldsymbol{Q}$ and $n = 2$. Furuta [3] defined also symbol $[d_1, d_2, a] = \pm 1$ on $\boldsymbol{Q}^\times$ which has similar properties as ours, but there the reciprocity law is uncompleted. Further his definition requires the full decomposition of each prime factor of a in some genus field $\supset \boldsymbol{Q}(\sqrt{d_1}, \sqrt{d_2})$ so defferent from ours. Let R be any finite set of prime natural number. We fix $\Omega^2/\boldsymbol{Q}_2$ arbitrarily if $2 \in R$ but such that $\Omega^2/\boldsymbol{Q}_2$ is Galois and there is a surjection $G(\Omega^2/\boldsymbol{Q}_2) \to \mathfrak{G}/\mathfrak{G}''$ for the free pro-l group $\mathfrak{G}$ if $2 \notin R$. When we extend the definition of (x, y, z) to R-strictly orthogonal $\{x, y, z\}$, the confines of the definition of (x, y, z)'s covers properly Furuta's. Anyway both are essentially the same when the symbol is defined in both senses.

vii) Here we shall establish (38) in Lemma 3 in short. Let N be a commutative group on which $G = Z(n) \times Z(n)$ acts trivially. Take a group extension

$$1 \to N \xrightarrow{f} \bar{G} \xrightarrow{g} G \to 1$$

and take $\bar{\sigma}, \bar{\tau} \in \bar{G}$ such that $g(\bar{\sigma}) = (1, 0)$, $g(\bar{\tau}) = (0, 1)$.

The class of this group extension is determined by

$$(f^{-1}(\bar{\sigma}^{-n}), f^{-1}(\bar{\tau}^{n}), f^{-1}([\bar{\sigma}, \bar{\tau}])) \in N \times N \times N .$$

When $N=Z(n)$, by such a way we can identify

$$\mathrm{H}^2(G, Z(n)) = Z(n) \times Z(n) \times Z(n) ,$$

in fact the group of Proposition 2 provides, for example, a generator of the third factor. When $N=\boldsymbol{Z}$ on the other hand, we know $\mathrm{H}^2(G, \boldsymbol{Z}) \cong G$ therefore $\bar{G}$ is always commutative and

$$\mathrm{Im}\,(\mathrm{H}^2(G, \boldsymbol{Z}) \xrightarrow{\text{can.}^*} \mathrm{H}^2(G, Z(n))) = Z(n) \times Z(n) \times 0 .$$

For our $H \subset G$ such that $[G: H] \geqq n$, we have easily

$$f^{-1}([\bar{p}_1, \bar{p}_2]) \in N^n ;\ \bar{p}_1, \bar{p}_2 \in \bar{H} = g^{-1}(H) \subset \bar{G} .$$

We apply all these facts on the commutative row-exact diagram

$$\begin{array}{ccccccc}
\mathrm{H}^2(G, \boldsymbol{Z}) & \to & \mathrm{H}^2(G, Z(n)) & \to & \mathrm{H}^3(G, n\boldsymbol{Z}) & \to 1\ (=n\mathrm{H}^3(G, \boldsymbol{Z})) \\
\downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & \\
\mathrm{H}^2(H, \boldsymbol{Z}) & \to & \mathrm{H}^2(H, Z(n)) & \to & \mathrm{H}^3(H, n\boldsymbol{Z}) & \to 1\ (=n\mathrm{H}^3(H, \boldsymbol{Z})) .
\end{array}$$

Then the right-most vertical map becomes the nil-map, so using the isomorphism $n\boldsymbol{Z} \cong \boldsymbol{Z}$, we have

(53) $\mathrm{Im}\,(\mathrm{Res}_{G \to H}: \mathrm{H}^3(G, \boldsymbol{Z}) \to \mathrm{H}^3(H, \boldsymbol{Z})) = 0 .$

Now, using the canonical exact sequence $0 \to \boldsymbol{Z} \to \boldsymbol{R} \to \boldsymbol{R}/\boldsymbol{Z} \to 0$ of the additive group of the real numbers $\boldsymbol{R}$, we define the isomorphism $\delta_{q-1,q}$: $\mathrm{H}^{q-1}(G, \boldsymbol{R}/\boldsymbol{Z}) \cong \mathrm{H}^q(G, \boldsymbol{Z})$, $q \in \boldsymbol{Z}$, for a general G and this $\delta_{q-1,q}$ commutes with $\mathrm{Inj}_{H \to G}$ and with $\mathrm{Res}_{G \to H}$ for any $H \subset G$. By means of the cup product of cohomology group

$$\cup : (\mathrm{H}^q(G, \boldsymbol{Z}), \mathrm{H}^{-q-1}(G, \boldsymbol{R}/\boldsymbol{Z})) \to \mathrm{H}^{-1}(G, \boldsymbol{R}/\boldsymbol{Z}) = \boldsymbol{Z}/[G: 1]\boldsymbol{Z}$$

we determine an identification $\mathrm{H}^{-q-1}(G, \boldsymbol{R}/\boldsymbol{Z}) = \mathrm{Hom}(\mathrm{H}^q(G, \boldsymbol{Z}), \boldsymbol{R}/\boldsymbol{Z})$. Since

$$\mathrm{Inj}_{H \to G}(\mathrm{Res}_{G \to H}(\alpha) \cup \beta) = \alpha \cup \mathrm{Inj}_{H \to G}(\beta);\ \alpha \in \mathrm{H}^q(G, *),\ \beta \in \mathrm{H}^r(H, *)$$

in general (see [9], espcially p 160), we obtain from (53)

$$\mathrm{Im}(\mathrm{Inj}_{H \to G}: \mathrm{H}^{-3}(H, \boldsymbol{Z}) \to \mathrm{H}^{-3}(G, \boldsymbol{Z})) = 0$$

(in fact both image groups of this and of (53) are isomorph for general G and $H \subset G$).

viii) Let $\{x, y, z\}$ be strictly orthogonal in $k^\times$ and τ be an automorphism of k

such that $\Omega^{\mathfrak{l}^\tau}=(\Omega^{\mathfrak{l}})^\tau$ at every $\mathfrak{l}|(l)$, and

$$x^\tau\equiv x^a,\quad y^\tau\equiv y^b,\quad z^\tau\equiv z^c \bmod (k^\times)^n \quad\text{and}\quad \zeta^\tau=\zeta^t$$

by natural numbers a, b, c, t. Then, from Theorem 1,

$$(x, y, z)^t=(x, y, z)^\tau=(x, y, z)^{abct^{-1}}.$$

Thus we know

Proposition 5. *In such a case*

$$(x, y, z|k')_n\in\langle\zeta_m\rangle;\ m=(t^2-abc, n)\ (=g_{,}.c.m.\ (t^2-abc, n))$$

for any $k'\supset k$.

Apply Theorem 2a further. Then we obtain an example of Hasse principle:

Corollary. *Let* $x, y, z\in\boldsymbol{Q}^\times$ *and they be strictly orthogonal in* $k^\times$ *and further* $\langle x, y\rangle\subset(k^\times)^l$. *Let* $\Omega^l/\boldsymbol{Q}_l$ *be a trivial or* $\boldsymbol{Z}_l$*-extension, i.e. rank* $G(\Omega^l/\boldsymbol{Q}_l)\leqq 1$ *and put* $\Omega^{\mathfrak{l}}=\Omega^l k_{\mathfrak{l}}\subset\bar{k}_{\mathfrak{l}}$ *for every* $\mathfrak{l}|(l)$. *Then*

$$z^{(24,n)}\in N_{L/k}L^\times \qquad \text{if}\quad z\in N_{L/k}J_L$$

where $L=k\{x, y\}$.

Because, if $l\neq 2$, $(t^2-1, n)=(3, n)$ for the generator τ of $G(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ and if $l=2$, $G(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ has τ such that $t=5$ so $(t^2-1, n)=(8, n)$.

We can show an example. Let $n=5$ and $k=\boldsymbol{Q}(\zeta_5)$. Let $\Omega^{\mathfrak{l}}/k_{\mathfrak{l}}$ be the maximal unramified 5-extension, $\mathfrak{l}|(5)$. In this case we can put $U_{k5}=\langle\zeta_5, \varepsilon\rangle\cdot(k^\times)^5$, $\varepsilon=(1+\sqrt{5})/2$ the fundamental unit. Fix the generator τ of $G(k/\boldsymbol{Q})$, $\zeta^\tau=\zeta^2$, $\varepsilon^\tau\equiv\varepsilon^4 \bmod (k^\times)^5$. Let x and y in $k^\times$ be 5-independent and strictly orthogonal. Assume that $k\{x\}$ and $k\{y\}$ are Galois over $\boldsymbol{Q}$, in other words $\langle x\rangle\cdot(k^\times)^5$ and $\langle y\rangle\cdot(k^\times)^5$ are $G(k/\boldsymbol{Q})$-invariant, so we can put

$$x^\tau\equiv x^a \text{ and } y^\tau\equiv y^b \bmod (k^\times)^5;\ a, b\in\boldsymbol{Z}.$$

Then we have the next sufficient condition for the divisibility of the class number, not coming from the genus theory:

When $(a, b)=(1, 3), (1, 4), (2, 2), (2, 4),$ *or* $(3, 3)$,
$k\{x, y\}$ *has unramified quint extension, being nonabelian over* k

because $(x, y, \zeta)=1$ and $(x, y, \varepsilon)=1$ from Proposition 5, so $k\{x, y\}/k$ is contained in an FNAC-extension which is unramified over $k\{x, y\}$ as stated in the end of Section 1.

Acknowledgements. The author is indebted to Yoshihiko Yamamoto and Kumiko Nishioka for their patient corrections.

References

[1] S.P. Demuskin: *The group of maximal p-extension of local fields,* Izv. Akad. Nauk SSSR. Ser Mat. **25** (1961), 329–346.

[2] A. Frohlich: *A prime decomposition symbol for certain non-abelian number field,* Acta Sci. Math. **21** (1960), 229–246.

[3] ————: Central extensions, Galois groups, and ideal class groups on number fields, Contemporary Math. 24 (A.M.S.), 1983.

[4] Y. Furuta: *A prime decomposition symbol for a non-abelian central extension which is abelian over a bicyclic biquadratic field,* Nagoya Math. J. **79** (1980), 79–109.

[5] H. Hasse: *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraishen Zahlkörper* II, Jahresber. Deutsch. Math. Verein., 1930.

[6] H. Koch: Galoissche Theorie der p-Erweiterungen, 1970, Springer

[7] I.R. Safarevic: *On p-extensions,* Mat. Sb. **20** (1947), 351–363.

[8] A.I. Skopin: *On p-extension of local field which has the p^Mth root of* 1, Izv. Akad. Nauk SSSR. Ser Mat. **19** (1955), 445–470.

[9] E. Weiss: Cohomology of groups, Academic Press, 1969.

Department of Mathematics
Faculty of Science
Nara Women's University
Nara 630, Japan