Journal of the Mathematical Society of Japan Vol. 11, No. 2, April, 1959

Factor sets in a number field and the norm residue symbol.

By Tomio KUBOTA

(Received Nov. 13, 1958)

Let Ω be an algebraic number field of finite degree and K be an abelian extension over Ω with Galois group $A=g(K/\Omega)$.[1] Then, in the multiplicative group $\Omega^{\times}$ of non-zero elements of Ω as a trivial A-module, we can consider a factor set ζ of A consisting of roots of unity. The first problem treated in this paper is an explicit determination of the $\mathfrak{p}$-invariants $\nu_{\mathfrak{p}}(\zeta)$ of ζ as a factor set of A in K/Ω, where $\mathfrak{p}$ is a place of Ω. We obtain the following result. Let α, β be two non-zero elements of the $\mathfrak{p}$-adic completion $\Omega_{\mathfrak{p}}$ of Ω and σ, τ be elements of A canonically corresponding to α, β, respectively, by the reciprocity mapping of the local class field theory. Then, using the norm residue symbol of certain degree e we can determine the $\mathfrak{p}$-invariant $\nu_{\mathfrak{p}}(\zeta)$ (mod 1) by

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_e^{e\cdot\nu_{\mathfrak{p}}(\zeta)}=\frac{\zeta_{\sigma,\tau}}{\zeta_{\tau,\sigma}}$$

whenever $\mathfrak{p}$ is a prime ideal of Ω prime to the order of A and $\Omega_{\mathfrak{p}}$ contains sufficiently many roots of unity (§1).

Now, let G be a finite group containing in the center a cyclic group Z such that $G/Z\cong A$. If Ω contains sufficiently many roots of unity and Z is identified with a subgroup of $\Omega^{\times}$, then the factor set ξ determined by A in Z is identified with a factor set ζ of A in K/Ω and it is easily seen that K is the subfield corresponding to Z in the sence of Galois theory of a normal extension $\bar{K}$ over Ω with Galois group G if and only if ζ splits as a factor set of A in K/Ω, i. e., all the $\mathfrak{p}$-invariants of ζ are equal to 0. This fact, composed with the formula above, is naturally applicable to the problem of determining whether an abelian extension K/Ω with Galois group A is embeddable in a normal extension $\bar{K}/\Omega$ with Galois group G. In fact, we see in §2 that a necessary and sufficient condition for certain types of K to be embeddable is expressed by some bilinear congruences concerning a homomorphism κ, attached to K by means of class field theory, of the idèle class group of Ω into A.

1) Galois groups will be denoted by this notation.

In the last § 3, we consider as examples dihedral and quaternion extensions over the rational number field P and we have, among others, the following result. Let A be an abelian group of the type (2, 2) and $p_1,\cdots,p_t$ be prime numbers congruent to 1 mod 4. Suppose an extension K over P with Galois group A to be unramified at every rational prime number except $p_1,\cdots,p_t$. Then K is determined in a definite way by rational integers $x_1, y_1, x_2, y_2,\cdots, x_t, y_t$, and K is embeddable in a dihedral (and equivalently in a quaternion) extension over P if and only if x, y satisfy the simultaneous bilinear congruences $f_i(x, y) \equiv 0 \pmod 2$, where $f_i (i=1,\cdots,t)$ is defined by

$$f_i(x, y) = \sum_{j=1}^{t} \frac{1}{2}\left\{1-\left(\frac{p_i}{p_j}\right)\right\}(x_i y_j + x_j y_i)$$

and we set $\left(\frac{p_i}{p_i}\right)=1$. From this fact we see also that the number of the dihedral or the quaternion extensions over P unramified at every rational prime number except $p_1,\cdots,p_t$ is determined by t and by the number of solutions of $f_i(x, y) \equiv 0 \pmod 2$.

§ 1. Determination of $\mathfrak{p}$-invariants.

1. At the beginning we introduce the notion of G-extension over a field. Let Ω[2] be an algebraic number field of finite degree and G be a finite group. Then we understand by a G-extension over Ω a homomorphism κ into G of the Galois group of the algebraic closure over Ω. Of course a quite similar definition is possible for an arbitrary basic field. A G-extension κ over Ω determines by Galois theory an algebraic extension K_κ of finite degree over Ω. We call K_κ the *corresponding field* of κ. For the sake of convenience we regard properties of K_κ as those of κ, e. g., we say κ is ramified at a prime ideal $\mathfrak{p}$ of Ω whenever K_κ is ramified at $\mathfrak{p}$. In the case where $G=A$ is an abelian group, the class field theory implies that κ may be considered a homomorphism into A of the idèle class (or idèle) group of Ω. Furthermore, restricting in this case κ to the $\mathfrak{p}$-components of idèles for a place $\mathfrak{p}$ of Ω, we get in a natural way an A-extension $\kappa_\mathfrak{p}$ over the $\mathfrak{p}$-adic field $\Omega_\mathfrak{p}$, which we call the *$\mathfrak{p}$-component* of κ.

Now, in the multiplicative group $\Omega^\times$, under trivial operation of A, of non-zero elements of Ω, we consider a factor set ζ of A consisting of roots of unity. For such a ζ, the factor set relation $\xi_{\sigma,\tau\rho}\xi_{\tau,\rho} = \xi_{\sigma\tau,\rho}\xi^{\rho}_{\sigma,\tau}$ turns out $\zeta_{\sigma,\tau\rho}\zeta_{\tau,\rho} = \zeta_{\sigma\tau,\rho}\zeta_{\sigma,\tau}$. Let κ be an A-extension over Ω with its corresponding field K_κ. Since then κ maps the Galois group $g_\kappa = g(K_\kappa/\Omega)$ into A, we can

2) We observe in the sequel one and the same number field Ω.

attach to every κ a factor set ζ^{κ} of g_{κ} in K_{κ}/Ω by setting $\zeta^{\kappa}_{\sigma,\tau}=\zeta_{\kappa(\sigma),\kappa(\tau)}$ for every $\sigma,\tau\in g_{\kappa}$. We call ζ^{κ} the *induced factor* set. We now propose to observe the $\mathfrak{p}$-invariant $\nu_{\mathfrak{p}}(\zeta,\kappa)$ of ζ^{κ}. Since the $\mathfrak{p}$-component $\kappa_{\mathfrak{p}}$ of κ determines in a maximal abelian extension over $\Omega_{\mathfrak{p}}$ the corresponding field $K_{\kappa}^{\mathfrak{p}}$ with the Galois group $g_{\kappa}^{\mathfrak{p}}=g(K_{\kappa}^{\mathfrak{p}}/\Omega_{\mathfrak{p}})$ and with the induced factor set $\zeta^{\kappa_{\mathfrak{p}}}$, it suffices for us only to determine the $\mathfrak{p}$-invariant of $\zeta^{\kappa_{\mathfrak{p}}}$. Furthermore, we may assume without any loss of generality that the order of A is a power of a prime number l and ζ consists of roots of unity whose orders are powers of l.

From now on, if no confusion is possible, we write $K^{\mathfrak{p}}$ for $K_{\kappa}^{\mathfrak{p}}$, $g^{\mathfrak{p}}$ for $g_{\kappa}^{\mathfrak{p}}=g(K_{\kappa}^{\mathfrak{p}}/\Omega_{\mathfrak{p}})$ and $\zeta_{\sigma,\tau}$ for $\zeta_{\kappa_{\mathfrak{p}}(\sigma),\kappa_{\mathfrak{p}}(\tau)}=\zeta^{\kappa_{\mathfrak{p}}}_{\sigma,\tau}$, where σ,τ mean elements of $g^{\mathfrak{p}}$. Besides, we settle the assumption that $\mathfrak{p}$ is prime to l and $\Omega_{\mathfrak{p}}$ contains a primitive ec-th root of unity, where e is the ramification order of κ at $\mathfrak{p}$ and c is determined by roots of unity appearing in ζ as the highest of their orders.

Under the assumption, if $T^{\mathfrak{p}}$ is the inertia field of $K^{\mathfrak{p}}/\Omega_{\mathfrak{p}}$, then $g(T^{\mathfrak{p}}/\Omega_{\mathfrak{p}})$ is cyclic of order $f=(T^{\mathfrak{p}}:\Omega_{\mathfrak{p}})$ and $g(K^{\mathfrak{p}}/T^{\mathfrak{p}})$ is cyclic of order e. Now, denoting by $\pi_{\mathfrak{p}}$ a definite generator of the prime ideal of $\Omega_{\mathfrak{p}}$, we fix a Frobenius automorphism $\varphi=\left(\frac{\pi_{\mathfrak{p}},K^{\mathfrak{p}}/\Omega_{\mathfrak{p}}}{\mathfrak{p}}\right)$ of $K^{\mathfrak{p}}/\Omega_{\mathfrak{p}}$. Next, setting $\tilde{K}^{\mathfrak{p}}=K^{\mathfrak{p}}(\sqrt[e]{\pi_{\mathfrak{p}}})$ and denoting by $\zeta_{\mathfrak{p}}$ a definite root of unity in $\Omega_{\mathfrak{p}}$ such that the order of $\zeta_{\mathfrak{p}}$ is the highest possible power of l, we fix another automorphism $\tilde{\omega}=\left(\frac{\zeta_{\mathfrak{p}},\tilde{K}^{\mathfrak{p}}/\Omega_{\mathfrak{p}}}{\mathfrak{p}}\right)$ of $\tilde{K}^{\mathfrak{p}}/\Omega_{\mathfrak{p}}$. The restriction ω to $K^{\mathfrak{p}}$ of $\tilde{\omega}$ is a generator of $g(K^{\mathfrak{p}}/T^{\mathfrak{p}})$ and we have $\sqrt[e]{\pi_{\mathfrak{p}}}^{\tilde{\omega}}=\zeta_e\sqrt[e]{\pi_{\mathfrak{p}}}$ with a definite primitive e-th root ζ_e of unity. We have also for every $\sigma\in g^{\mathfrak{p}}$ a unique decomposition $\sigma=\sigma_{\varphi}\sigma_{\omega}$ with $\sigma_{\varphi}=\varphi^{i}$ $(0\leqq i<f)$ and $\sigma_{\omega}\in\{\omega\}$.[3)]

2. After these preliminaries, we can arrive at an exposition of the $\mathfrak{p}$-invariant $\nu_{\mathfrak{p}}(\zeta)=\nu_{\mathfrak{p}}(\zeta,\kappa)$ of $\zeta^{\kappa_{\mathfrak{p}}}$. We proceed quite similarly to Artin [**1**, Chap. 6, 4]. Set $\zeta_{\omega}=\zeta_{\omega,1}\zeta_{\omega,\omega}\cdots\zeta_{\omega,\omega^{e-1}}$. Then, under the assumption in **1**, there is $\bar{\zeta}_{\omega}\in\Omega_{\mathfrak{p}}$ such that $\zeta_{\omega}=\bar{\zeta}_{\omega}^{\,e}$. Hence, if we set $a_1=\zeta^{-1}_{\omega,1}$, $a_{\omega^i}=\zeta_{\omega,\omega}\cdots\zeta_{\omega,\omega^{i-1}}$ for $i>1$ and $a_{\sigma}=1$ for $\sigma\notin\{\omega\}$, then the factor set $\zeta^{(1)}_{\sigma,\tau}=\zeta_{\sigma,\tau}\cdot\frac{a_{\sigma}^{\tau}a_{\tau}}{a_{\sigma\tau}}$ fills

$$\zeta^{(1)}_{\omega^i,\omega^j}=\begin{cases}1 & \text{for } i+j<e\\ \zeta_{\omega} & \phantom{\text{for }} i+j\geqq e\end{cases}\qquad (0\leqq i,j<e),$$

and, if further we set $b_{\omega^i}=\bar{\zeta}^{-(1+\omega+\cdots+\omega^{i-1})}=\bar{\zeta}_{\omega}^{-i}$ and $b_{\sigma}=1$ for $\sigma\notin\{\omega\}$, then, for the factor set $\zeta^{(2)}_{\sigma,\tau}=\zeta^{(1)}_{\sigma,\tau}\cdot\frac{b_{\sigma}^{\tau}b_{\tau}}{b_{\sigma\tau}}$, we have $\zeta^{(2)}_{\omega^i,\omega^j}=1$. Moreover, if we, using the decomposition $\sigma=\sigma_{\varphi}\sigma_{\omega}$ for $\sigma\in g^{\mathfrak{p}}$ at the last part of **1**, set $c_{\sigma}=\zeta^{(2)}_{\sigma_{\omega},\sigma_{\varphi}}$ and

3) The symbol { } stands for the group generated by the element in it.

$\zeta^{(3)}_{\sigma,\tau}=\zeta^{(2)}_{\sigma,\tau}\cdot\frac{c^{\tau}_{\sigma}c_{\tau}}{c_{\sigma\tau}}$, then we have $\zeta^{(3)}_{\sigma_{\omega},\sigma_{\varphi}}=\zeta^{(2)}_{\sigma_{\omega},\sigma_{\varphi}}\zeta^{(2)}_{\sigma_{\omega},1}\zeta^{(2)}_{1,\sigma_{\varphi}}\zeta^{(2)-1}_{\sigma_{\omega},\sigma_{\varphi}}=1$, $\zeta^{(3)}_{\omega^i,\tau}=\zeta^{(3)}_{\omega^i,\tau_{\omega}\tau_{\varphi}}=\zeta^{(3)}_{\omega^i\tau_{\omega},\tau_{\varphi}}\zeta^{(3)}_{\omega^i,\tau_{\omega}}\zeta^{(3)-1}_{\tau_{\omega},\tau_{\varphi}}=1$, $\zeta^{(3)}_{\sigma\omega^i,\tau}=\zeta^{(3)}_{\sigma,\tau}\zeta^{(3)}_{\omega^i,\sigma\tau}\zeta^{(3)-1}_{\omega^i,\sigma}=\zeta^{(3)}_{\sigma,\tau}$, and $\zeta^{(3)}_{\sigma,\omega_1\omega_2}=\zeta^{(3)}_{\sigma,\omega_1}\zeta^{(3)}_{\sigma,\omega_2}$ for ω_1, $\omega_2\in\{\omega\}$. Therefore we see that $\zeta^{(3)}_{\sigma,\omega}$ is an e-th root of unity and that there is $\Phi_{\sigma}\in K^{\mathfrak{p}}$ such that we have $\zeta^{(3)}_{\sigma,\omega}=\Phi^{1-\omega}_{\sigma}$. Moreover, we may assume that Φ_{σ} depends only on σ_{φ} and that we have $\Phi_1=1$. If we set here $\beta_{\sigma,\tau}=\zeta^{(3)}_{\sigma,\tau}\cdot\frac{\Phi^{\tau}_{\sigma}\Phi_{\tau}}{\Phi_{\sigma\tau}}$, then $\beta_{\sigma,\tau}$ is the lift to $K^{\mathfrak{p}}/\Omega_{\mathfrak{p}}$ of a factor set of $T^{\mathfrak{p}}/\Omega_{\mathfrak{p}}$ and its $\mathfrak{p}$-invariant is determined whenever the $\mathfrak{p}$-exponent $n(\beta_{\varphi})$ of $\beta_{\varphi}=\beta_{\varphi,1}\beta_{\varphi,\varphi}\cdots\beta_{\varphi,\varphi^{f-1}}$ is known. Denoting by a parenthesis a principal ideal, we have

$$(\beta_{\varphi})=\prod_{i=0}^{f-1}\left(\zeta^{(3)}_{\varphi,\varphi^i}\cdot\frac{\Phi^{\varphi^i}_{\varphi}\Phi_{\varphi^i}}{\Phi_{\varphi^{i+1}}}\right)=\prod_{i=0}^{f-1}\left(\Phi_{\varphi}\cdot\frac{\Phi_{\varphi^i}}{\Phi_{\varphi^{i+1}}}\right)=(\Phi_{\varphi})^f\,.$$

On the other hand, since $K^{\mathfrak{p}}$ is obtained by adjunction to $T^{\mathfrak{p}}$ of an element of the form $\sqrt[e]{\pi_{\mathfrak{p}}}\cdot\zeta_0$, where ζ_0 is a root of unity in $\tilde{K}^{\mathfrak{p}}$ such that the order of ζ_0 is a power of l, and since $\tilde{\omega}$ operates trivially on such a root of unity, we may take as Φ_{φ} the element $(\sqrt[e]{\pi_{\mathfrak{p}}}\cdot\zeta_0)^m$, where m is determined by $\zeta^{(3)}_{\varphi,\omega}=\zeta_e^{-m}$. Therefore we have finally

$$\nu_{\mathfrak{p}}(\zeta)\equiv\frac{n(\beta_{\varphi})}{f}\equiv\frac{m}{e}\qquad(\mathrm{mod}\ 1)\,.$$

Since, from the definition, $\zeta^{(3)}$ and ζ are mutually cohomologous as cocycles of $g^{\mathfrak{p}}$ in the multiplicative group $\Omega_{\mathfrak{p}}^{\times}$ of non-zero elements of $\Omega_{\mathfrak{p}}$ and since we have $\zeta^{(3)}_{\varphi,\omega}=\frac{\zeta^{(3)}_{\varphi,\omega}}{\zeta^{(3)}_{\omega,\varphi}}$, we have $\zeta^{(3)}_{\varphi,\omega}=\frac{\zeta_{\varphi,\omega}}{\zeta_{\omega,\varphi}}$. Thus m is directly computed by $\zeta_e^m=\frac{\zeta_{\omega,\varphi}}{\zeta_{\varphi,\omega}}$.

3. Let us continue the observation of the same subject. The norm residue symbol $\left(\frac{\zeta_{\mathfrak{p}},\pi_{\mathfrak{p}}}{\mathfrak{p}}\right)_e$ is defined as Hasse [2, § 11], by $\sqrt[e]{\pi_{\mathfrak{p}}}^{\tilde{\omega}}=\left(\frac{\zeta_{\mathfrak{p}},\pi_{\mathfrak{p}}}{\mathfrak{p}}\right)_e\cdot\sqrt[e]{\pi_{\mathfrak{p}}}$. This, compared with the definition of ζ_e in **1**, yields $\zeta_e=\left(\frac{\zeta_{\mathfrak{p}},\pi_{\mathfrak{p}}}{\mathfrak{p}}\right)_e$ and therefore we have $\left(\frac{\zeta_{\mathfrak{p}},\pi_{\mathfrak{p}}}{\mathfrak{p}}\right)_e^m=\frac{\zeta_{\omega,\varphi}}{\zeta_{\varphi,\omega}}$. Thus we obtain

THEOREM 1. *Let A be an abelian group whose order is a power of a prime number l, κ be an A-extension over Ω, ζ be a factor set of A in the multiplicative group $\Omega^{\times}$, as a trivial A-group, of non-zero elements of Ω and ζ^{κ} be the induced factor set. Assume that, for a prime ideal $\mathfrak{p}$ of Ω prime to l, the $\mathfrak{p}$-completion $\Omega_{\mathfrak{p}}$ contains a primitive ec-th root of unity, where e is the ramification order of κ at $\mathfrak{p}$ and c is the highest order of roots of unity appearing in ζ. Let further $\kappa_{\mathfrak{p}}$ be the $\mathfrak{p}$-component of κ, $\pi_{\mathfrak{p}}$ be a generator of the prime ideal of $\Omega_{\mathfrak{p}}$ and $\zeta_{\mathfrak{p}}$ be a root of unity in $\Omega_{\mathfrak{p}}$ such that the order of $\zeta_{\mathfrak{p}}$ is the highest possible power of l.*

Then $\left(\frac{\zeta_{\mathfrak{p}}, \pi_{\mathfrak{p}}}{\mathfrak{p}}\right)_e$ *is a primitive e-th root of unity in* $\Omega_{\mathfrak{p}}$ *and the* $\mathfrak{p}$*-invariant* $\nu_{\mathfrak{p}}(\zeta, \kappa)$ *of* ζ^{κ} *is determined by*

$$\nu_{\mathfrak{p}}(\zeta, \kappa) \equiv \frac{m}{e} \qquad (\mathrm{mod}\ 1),$$

whenever m is chosen so that we have

$$\left(\frac{\zeta_{\mathfrak{p}}, \pi_{\mathfrak{p}}}{\mathfrak{p}}\right)_e^m = \frac{\zeta_{\omega,\varphi}}{\zeta_{\varphi,\omega}}$$

with $\varphi = \kappa_{\mathfrak{p}}(\pi_{\mathfrak{p}})$, $\omega = \kappa_{\mathfrak{p}}(\zeta_{\mathfrak{p}})$.

If we define for every pair σ, τ of elements of A a function $\lambda(\sigma, \tau) = \frac{\zeta_{\sigma,\tau}}{\zeta_{\tau,\sigma}}$, then we have $\lambda(\sigma\sigma', \tau) = \lambda(\sigma, \tau)\lambda(\sigma', \tau)$, $\lambda(\sigma, \tau\tau') = \lambda(\sigma, \tau)\lambda(\sigma, \tau')$. We call the function λ the *bi-character* attached to ζ.

Since $\zeta_{\mathfrak{p}}, \pi_{\mathfrak{p}}$ in theorem 1, together with the kernel of $\kappa_{\mathfrak{p}}$, generates the whole multiplicative group $\Omega_{\mathfrak{p}}^{\times}$ of non-zero elements of $\Omega_{\mathfrak{p}}$, it follows from the property of $\lambda(\sigma, \tau)$ as a bi-character that we have

COROLLARY. *Notations and assumptions being as in theorem* 1, *let* α, β *be any two of non-zero element of* $\Omega_{\mathfrak{p}}$ *and write* $\zeta^{\kappa_{\mathfrak{p}}}_{\alpha,\beta}$ *for* $\zeta_{\kappa_{\mathfrak{p}}(\alpha), \kappa_{\mathfrak{p}}(\beta)}$. *Then we have*

$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_e^m = \frac{\zeta^{\kappa_{\mathfrak{p}}}_{\alpha,\beta}}{\zeta^{\kappa_{\mathfrak{p}}}_{\beta,\alpha}}$$

where m is a rational integer with $\nu_{\mathfrak{p}}(\zeta, \kappa) \equiv \frac{m}{e}$ (mod 1).

§ 2. Applications to certain non-abelian extensions.

4. Let Z be a finite cyclic group,[4] A be a finite abelian group and G be an extension of Z by A such that Z is in the center of G. Then, a G-extension $\bar{\kappa}$ over Ω corresponds by the mapping $G \to G/Z = A$ to an A-extension κ over Ω, which we call the A-part of $\bar{\kappa}$. The corresponding field K_{κ} of the A-part κ of a G-extension $\bar{\kappa}$ over Ω is a subfield of the corresponding field $K_{\bar{\kappa}}$ of $\bar{\kappa}$. If two G-extensions $\bar{\kappa}_1, \bar{\kappa}_2$ over Ω have the same A-part $\kappa_1 = \kappa_2$, then, setting $\bar{\kappa}_1^{-1}\bar{\kappa}_2(\sigma) = \bar{\kappa}_1(\sigma)^{-1}\bar{\kappa}_2(\sigma)$ for every element σ of the Galois group of the algebraic closure Ω over Ω, $\bar{\kappa}_1^{-1}\bar{\kappa}_2$ is a Z-extension over Ω. Conversely, if $\bar{\kappa}$ is a G-extension over Ω and if we set $\bar{\kappa}\kappa_0(\sigma) = \bar{\kappa}(\sigma)\kappa_0(\sigma)$ with any Z-extension κ_0 over Ω, then $\bar{\kappa}\kappa_0$ is a G-extension over Ω which has the same A-part as $\bar{\kappa}$.

Let, for a moment, G be an arbitrary finite group and consider any G-

4) That Z is cyclic is not necessary here, but added for the sake of later observations.

extension κ over Ω and any finitely algebraic extension L over Ω. Then the restriction κ/L of κ to the Galois group $g(\Omega/L)$ is a G-extension over Ω and the corresponding field of κ/L is the composite field $K_\kappa L$. In particular, if $G=A$ is abelian, then, by a theorem of class field theory, we have $\kappa/L(\boldsymbol{a})=\kappa(N_{L/\Omega}\boldsymbol{a})$ for any idèle $\boldsymbol{a}$ of L, where we regard A-extensions as homomorphisms of idèle groups.

Now, taking again a special type of group G with $G/Z\cong A$ as above, consider two G-extensions $\bar\kappa_1, \bar\kappa_2$ over Ω with the same A-part κ and set $\bar\kappa_1^{-1}\bar\kappa_2=\kappa_0$. Then, we have $\bar\kappa_2/K_\kappa=\bar\kappa_1/K_\kappa\cdot\kappa_0/K_\kappa$ and therefore, regarding $\bar\kappa_1/K_\kappa$, $\bar\kappa_2/K_\kappa$ as homomorphisms of the idèle group of K_κ and κ_0 a homomorphism of the idèle group of Ω, we have $\bar\kappa_2/K_\kappa(\boldsymbol{a})=\bar\kappa_1/K_\kappa(\boldsymbol{a})\cdot\kappa_0(N_{K_\kappa/\Omega}\boldsymbol{a})$.

5. Let A, G and Z be as in **4**, ξ be the factor set of $A=G/Z$ in Z and assume that there is a definite isomorphism θ of Z into the group of roots of unity in Ω. Then we can formulate as follows an elementary result concerning existence of certain meta-abelian extensions over Ω.

LEMMA 1. *In order that an A-extension κ over Ω is the A-part of a G-extension $\bar\kappa$ over Ω, it is necessary and sufficient that the induced factor set $\xi^{\theta\kappa}$ of K_κ/Ω splits as a factor set of $g(K_\kappa/\Omega)$ in the multiplicative $g(K_\kappa/\Omega)$-group $K_\kappa^\times$ of non-zero elements of K_κ.*

PROOF. Suppose that $\xi^{\theta\kappa}$ splits. Then we have $\xi^{\theta\kappa}=\dfrac{\beta_\sigma^\tau\beta_\tau}{\beta_{\sigma\tau}}$ with $\beta\in K_\kappa$, $\sigma,\tau\in g(K_\kappa/\Omega)$. Denoting by c the order of Z, we have $(\xi^{\theta\kappa})^c=1$, whence $\beta_\sigma^{-c}=\gamma^{1-\sigma}$ with $\gamma\in K_\kappa$. Now, consider the field $K_\kappa(\sqrt[c]{\gamma})$, set $\bar\kappa(\rho)=\zeta_\rho{}^{\theta^{-1}}$ for the automorphism ρ with $\sqrt[c]{\gamma}^\rho=\zeta_\rho\sqrt[c]{\gamma}$ of $K_\kappa(\sqrt[c]{\gamma})/K_\kappa$ and set $\bar\kappa(\bar\sigma)=u_{\kappa(\sigma)}$ for the prolongation $\bar\sigma$, with $\sqrt[c]{\gamma}^{\bar\sigma}=\beta_\sigma\sqrt[c]{\gamma}$, of $\sigma\in g(K_\kappa/\Omega)$ to $K_\kappa(\sqrt[c]{\gamma})/\Omega$, where u means a system of representatives of G/Z corresponding to the factor set ξ. Then we have

$$(\sqrt[c]{\gamma})^{\bar\sigma\bar\tau^{-1}\bar\sigma\bar\tau}=\frac{\beta_\sigma^\tau\beta_\tau}{\beta_{\sigma\tau}}\cdot\sqrt[c]{\gamma}=\xi^{\theta\kappa}_{\sigma,\tau}\cdot\sqrt[c]{\gamma}=\xi^{\theta}_{\kappa(\sigma),\kappa(\tau)}\cdot\sqrt[c]{\gamma}$$

and consequently $\bar\kappa(\bar\sigma\bar\tau^{-1}\bar\sigma\bar\tau)=\xi_{\kappa(\sigma),\kappa(\tau)}$ for $\sigma,\tau\in g(K_\kappa/\Omega)$. Therefore, if we set generally $\bar\kappa(\bar\sigma\rho)=\bar\kappa(\bar\sigma)\bar\kappa(\rho)$ for every $\sigma\in g(K_\kappa/\Omega)$ and for every $\rho\in g(K_\kappa(\sqrt[c]{\gamma})/K_\kappa)$, then $\bar\kappa$ is a G-extension over Ω with the A-part κ and with the corresponding field $K_{\bar\kappa}=K_\kappa(\sqrt[c]{\gamma})$. Conversely, if $\bar\kappa$ is a G-extension over Ω with A-part κ and with the corresponding field $K_{\bar\kappa}$, then we have $K_{\bar\kappa}=K_\kappa(\sqrt[c]{\gamma})$ with $\gamma\in K_\kappa$. We may assume that we have $\sqrt[c]{\gamma}^\rho=\bar\kappa(\rho)^\theta\cdot\sqrt[c]{\gamma}$ for every automorphism ρ of $K_\kappa(\sqrt[c]{\gamma})/K_\kappa$. We can also find an element $\beta_\sigma\in K_\kappa$ such that we have $\beta_\sigma^{-c}=\gamma^{1-\sigma}$. Denoting by $\bar\sigma$ a prolongation, with $\sqrt[c]{\gamma}^{\bar\sigma}=\beta_\sigma\sqrt[c]{\gamma}$, of any $\sigma\in g(K_\kappa/\Omega)$ to $K_{\bar\kappa}/\Omega$, we have

$$(\sqrt[c]{\gamma})^{\bar\sigma\bar\tau^{-1}\bar\sigma\bar\tau}=\frac{\beta_\sigma^\tau\beta_\tau}{\beta_{\sigma\tau}}\cdot\sqrt[c]{\gamma}=(\bar\kappa(\bar\sigma\bar\tau)^{-1}\bar\kappa(\bar\sigma)\bar\kappa(\bar\tau))^\theta\cdot\sqrt[c]{\gamma}$$

for $\sigma, \tau \in g(K_\kappa/\Omega)$. Since the set of elements $\bar{\kappa}(\bar{\sigma}\bar{\tau})^{-1}\bar{\kappa}(\bar{\sigma})\bar{\kappa}(\bar{\tau})$ is a factor set of $\kappa(g(K_\kappa/\Omega))$ in Z equivalent with the restriction of ξ to $\kappa(g(K_\kappa/\Omega))$, $\xi^{\theta\kappa}$ splits as a factor set of $g(K_\kappa/\Omega)$ in the $g(K_\kappa/\Omega)$-group $K_\kappa^\times$.

6. Now we deal arithmetically with the existence of G-extensions $\bar{\kappa}$ over Ω such that $\bar{\kappa}$ has an A-extension κ as the A-part. Since A is nilpotent, it suffices to consider the case where the order of G is a power of a prime number l. We assume that there is a definite isomorphism of Z into the group of roots of unity in Ω and that Ω contains a primitive n_0-th root of unity, where n_0 is the exponent, i.e., the largest element order of A. Furthermore, denoting by $S=\{\mathfrak{p}_1, \mathfrak{p}_2, \cdots\}$ the set of all ramification places of κ, we assume that every $\mathfrak{p}_i$ is a principal prime ideal of Ω prime to l and that the $\mathfrak{p}_i$-completion $\Omega_{\mathfrak{p}_i}$ contains a primitive n_0c-th root of unity, where c is the order of Z.

Let now ζ_{n_0} be a definite primitive n_0-th root of unity and, denoting by π_i an element of Ω which generates the prime ideal $\mathfrak{p}_i$, fix a root ζ_i of unity in $\Omega_{\mathfrak{p}_i}$ such that we have $\left(\frac{\zeta_i, \pi_i}{\mathfrak{p}_i}\right)_{n_0}=\zeta_{n_0}$ and that the order of ζ_i is a power of l. Such a ζ_i is then a root of unity in $\Omega_{\mathfrak{p}_i}$ whose order is the largest possible power of l. Since π_i is a unit in $\Omega_{\mathfrak{p}_j}$ $(i \neq j)$, we can choose m_{ij} such that π_i is the product of the power $\zeta_i^{-m_{ij}}$ by a unit of $\Omega_{\mathfrak{p}_j}$ which is a n_0-th power residue mod $\mathfrak{p}_j$. We set formally $m_{ii}=0$. The congruence class m_{ij} mod n_0 is thus uniquely determined. Next, decomposing A into a direct product $\{\sigma_1\}\times\{\sigma_2\}\times\cdots$ of cyclic groups, we define $x_{i\iota}$ by setting $\kappa_i(\zeta_i)=\sigma_1^{x_{i1}}\sigma^{x_{i2}}\cdots$, where κ_i is the $\mathfrak{p}_i$-component of κ. Moreover, denoting by ζ the image by the definite isomorphism of a factor set of $A=G/Z$ in Z, we set $\lambda(\sigma_\iota, \sigma_\upsilon)=\frac{\zeta_{\sigma_\iota,\sigma_\upsilon}}{\zeta_{\sigma_\upsilon,\sigma_\iota}}=\zeta_{n_0}^{c_{\iota\upsilon}}$. This $c_{\iota\upsilon}$ is unique mod n_0.

Let now ν_i be the $\mathfrak{p}_i$-invariant of the induced factor set ζ^κ. Then, since the ramification order of κ at $\mathfrak{p}_i$ divides n_0, it follows from Theorem 1 and from a property of the norm residue symbol that we have $\zeta_{n_0}^{n_0\nu_i}=\lambda(\kappa_i(\zeta_i), \kappa_i(\pi_i))$. Hence, by the product relation $\prod_j \kappa_j(\pi_i)=1$ and by the property of λ as a bi-character, we have

$$\begin{aligned}\lambda(\kappa_i(\zeta_i), \kappa_i(\pi_i)) &= \lambda(\kappa_i(\zeta_i), \prod_{j(\neq i)} \kappa_j(\pi_i)^{-1}) = \prod_j \lambda(\kappa_i(\zeta_i), \kappa_j(\zeta_j))^{m_{ij}} \\ &= \prod_{j,\iota,\upsilon} \lambda(\sigma_\iota, \sigma_\upsilon)^{m_{ij}x_{i\iota}x_{j\upsilon}} = \zeta_{n_0}^{\Sigma m_{ij}c_{\iota\upsilon}x_{i\iota}x_{j\upsilon}}.\end{aligned}$$

Therefore it is necessary and sufficient for the induced factor set ζ^κ to split that we have

$$F(x)=\sum_{j,\iota,\upsilon} m_{ij}c_{\iota\upsilon}x_{i\iota}x_{j\upsilon}\equiv 0 \qquad (\text{mod } n_0)$$

for every i.

Thus the existence of a G-extension $\bar{\kappa}$ which has κ as its A-part rests upon the restriction κ_U of κ to the unit idèle group $\boldsymbol{U}$ of Ω. Moreover the condition for the existence does not depend on the factor set ζ itself, but only on the bi-character λ.

§ 3. Examples.

7. We now propose to observe, as examples, normal extensions of degree 8 over the rational number field P. There are two non-abelian groups of order 8: the dihedral group G_1 and the quaternion group G_2. These two groups are extensions of a cyclic group Z of order 2 by the group A consisting of 1, σ_1, σ_2 and $\sigma_3=\sigma_1\sigma_2$. Identifying Z with the group of ±1, factor set $\xi^{(1)}$, $\xi^{(2)}$ of G_1/Z, G_2/Z are as follows.

The dihedral group

$\xi^{(1)}_{\sigma,\tau}$:

$\sigma \backslash \tau$	1	σ_1	σ_2	σ_3
1	1	1	1	1
σ_1	1	−1	1	−1
σ_2	1	−1	1	−1
σ_3	1	1	1	1

The quaternion group

$\xi^{(2)}_{\sigma,\tau}$:

$\sigma \backslash \tau$	1	σ_1	σ_2	σ_3
1	1	1	1	1
σ_1	1	−1	1	−1
σ_2	1	−1	−1	1
σ_3	1	1	−1	−1

These two factor sets have one and the same bi-character

$$\lambda(\sigma,\tau)=\frac{\xi^{(1)}_{\sigma,\tau}}{\xi^{(1)}_{\tau,\sigma}}=\frac{\xi^{(2)}_{\sigma,\tau}}{\xi^{(2)}_{\tau,\sigma}}:$$

$\sigma \backslash \tau$	1	σ_1	σ_2	σ_3
1	1	1	1	1
σ_1	1	1	−1	−1
σ_2	1	−1	1	−1
σ_3	1	−1	−1	1

Now, let $S=\{p_1,\cdots,p_t\}$ be a set of positive rational prime numbers with $p_i\equiv1 \pmod 4$. Denote by ζ_i a root of unity in the p_i-completion P_{p_i} such that the order of ζ_i is the largest possible power of 2. Since the rational number field P is of class number 1, a homomorphism κ of the idèle class group of P is determined by its restriction κ_U to the unit idèle group $\boldsymbol{U}$ of P. On the other hand, since -1 is a square in P_{p_i}, it is easily seen that every mapping κ_U of $\boldsymbol{U}$ into the cyclic group Z of order 2 is the restriction to $\boldsymbol{U}$ of a Z-extension over P whenever the p-component of κ_U is trivial for every place $q \notin S$ of P. Taking $A_1 = \{1, \sigma_1\}$ or $A_2 = \{1, \sigma_2\}$ instead of Z, we come to a similar conclusion. Therefore we have

LEMMA 2. *Let $S = \{p_1, \cdots, p_t\}$ be a set of prime numbers with $p_i \equiv 1 \pmod 4$, Z be a cyclic group of order 2 and A be a non-cyclic group of order 4. Then the number of all Z-resp. A-extensions over P unramified at every place $q \notin S$ is equal to 2^t resp. 4^t.*

Now, p_i is a generator of the prime ideal of P_{p_i} and we have $\left(\frac{\zeta_i, p_i}{p_i}\right) = -1$. Furthermore, setting $m_{ij} = \frac{1}{2}\left\{1 - \left(\frac{p_i}{p_j}\right)\right\}$, p_i is a square in Ω_{p_j} $(i \neq j)$ if and only if $m_{ij} = 0$. On the other hand we set formally $\left(\frac{p_i}{p_i}\right) = 1$ and, if κ is an A-extension with p_i-component κ_i, we set $\kappa_i(\zeta_i) = \sigma_1^{x_i}\sigma_2^{x_i}$. Moreover, setting $\lambda(\sigma_\iota, \sigma_\upsilon) = (-1)^{c_{\iota\upsilon}}$, we have $c_{11} = c_{22} = 0$, $c_{12} = c_{21} = 1$. Therefore, if we denote by $\nu_i(\kappa)$ the p_i-invariant of the induced factor set $\xi^{(1)\kappa}$, then it follows from **6** that $\nu_i(\kappa)$ is also equal to the p_i-invariant of $\xi^{(2)\kappa}$ and that we have

$$2 \cdot \nu_i(\kappa) \equiv f_i(x, y) = \sum_{j=1}^{t} \frac{1}{2}\left\{1 - \left(\frac{p_i}{p_j}\right)\right\}(x_i y_j + x_j y_i) \pmod 2 .$$

Suppose now that κ is an A-extension unramified at every place $q \notin S$. Then $\xi^{(1)\kappa}$ splits if and only if we have $2 \cdot \nu_i(\kappa) \equiv f_i(x, y) \equiv 0 \pmod 2$ for every i. If this is the case, then we can find a G_1-extension $\bar{\kappa}^{(1)}$ over P such that κ is the A-part of $\bar{\kappa}^{(1)}$. Let $K_{\bar{\kappa}^{(1)}}$ be the corresponding field of $\bar{\kappa}^{(1)}$ and take $\gamma \in K_\kappa$ such that $K_{\bar{\kappa}^{(1)}} = K_\kappa(\sqrt{\gamma})$. Then, since $\gamma^{1-\sigma}$ is a square in K for every $\sigma \in g(K_\kappa/P)$, we see that the $\mathfrak{P}$-exponent of the principal ideal (γ) is congruent mod. 2 to the $\mathfrak{P}^\sigma$-exponent of (γ) for every prime ideal $\mathfrak{P}$ of K_κ and therefore there is a rational number such that the $\mathfrak{P}$-exponent of $(\gamma_0\gamma)$ is even whenever $\mathfrak{P}$ is prime to all the p_i. Consider the Z-extension κ_0 over P whose corresponding field is $P(\sqrt{\gamma_0})$. Then, since the product of $\bar{\kappa}^{(1)}/K_\kappa$ by κ_0/K_κ has the corresponding field $K_\kappa(\sqrt{\gamma\gamma_0})$, it follows from **4** that $\bar{\kappa}^{(1)}\kappa_0$ is a G_1-extension over P with the A-part κ and with the corresponding field $K_{\bar{\kappa}^{(1)}\kappa_0} = K_\kappa(\sqrt{\gamma\gamma_0})$. We see also that the ramification prime ideals of $K_{\bar{\kappa}^{(1)}\kappa_0}/K_\kappa$ must divide either p_i or 2. If in particular all p_i are $\equiv 1 \pmod 8$, then 2 decomposes completely in K_κ and therefore either $K_\kappa(\sqrt{\gamma_0\gamma})/K_\kappa$ or $K_\kappa(\sqrt{-\gamma_0\gamma})/K_\kappa$ is unramified at prime factors of 2. Thus, in this case we can choose a G_1-extension over P which has A-part κ and is unramified at every prime number $q \notin S$. At the same time, it follows from **4**, especially from the last formula in **4**, that the number of all such G_1-extensions over P is equal to the number of all Z-extensions over P unramified at every place $q \notin S$. The number of these Z-extensions is, by Lemma 2, equal to 2^t. Since the situation is exactly the same for G_2-extensions over P, we have

THEOREM 2. *Let $S=\{p_1,\cdots,p_t\}$ be a set of positive rational prime numbers with $p_i \equiv 1 \pmod 8$. Consider t bilinear forms*

$$f_i(x, y)=\sum_{j=1}^{t} \frac{1}{2}\left\{1-\left(\frac{p_i}{p_j}\right)\right\}(x_i y_j+x_j y_i)$$

of variables x_i, y_j $(1 \leqq i \leqq t)$, where we set $\left(\frac{p_i}{p_i}\right)=1$. Denote by G_1, G_2 the dihedral and the quaternion group respectively. Then the number of all G_1-extensions over the rational number field P which are unramified at every prime number $q \notin S$ is equal to the number of all G_2-extensions over P with the same property, and the number is equal to 2^t-times the number of solutions mod. 2 of the simultaneous bi-linear congruences $f_i(x, y) \equiv 0 \pmod 2$ $(1 \leqq i \leqq t)$.

If we have $\left(\frac{p_i}{p_j}\right)=1$ for every i, j, then all the forms $f_i(x, y)$ in theorem 2 vanish identically mod. 2 and, again by Lemma 2, there are 4^t A-extensions over P unramified at every place $q \notin S$. Therefore we have

COROLLARY. *Using same notations as in theorem 2, suppose that we have $\left(\frac{p_i}{p_j}\right)=1$ for every i, j. Then, there are 8^t G_1-extensions over P which are unramified at every prime number $q \notin S$, and there are the same number of G_2-extensions over P with the same property.*

Considering from a slightly different point of view, we have

THEOREM 3. *Let K be a non-cyclic abelian biquadratic field over the rational number field P and let $S=\{p_1,\cdots,p_t\}$ be the set of prime numbers at which K is ramified. Assume that we have $p_i \equiv 1 \pmod 4$ for every p_i. Then the existence of an overfield of K which is a dihedral extension over P implies the existence of an overfield of K which is a quaternion extension over P, and vice versa. Furthermore, the existence is certainly the case whenever we have additionally $\left(\frac{p_i}{p_j}\right)=1$ for every i, j.*

Mathematical Institute,
Nagoya University.

References

[1] E. Artin, Algebraic numbers and algebraic functions I, Princeton, 1951.
[2] H. Hasse, Bericht II, 1930.
[3] A. Scholz, Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I, Math. Zeitschr., **42** (1936), 161–188.
[4] E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordung p^f, J. Reine Angew. Math., **174** (1936), 337–245.