Journal of the Mathematical Society of Japan Vol. 5, Nos. 3~4, November, 1953.

# A note on Kummer extensions

By Kenkichi IWASAWA

(Received April 20, 1953)

**1.** Let $k$ be an arbitrary field and $Z(k)$ the set of all integers $n\geqq 1$ such that $k$ contains a primitive $n$-th root of unity. It is clear that, if $Z(k)$ contains $m$ and $n$, it also contains the least common multiple of these two integers. Therefore the set of all rational numbers with denominators in $Z(k)$ is an additive group $R(k)$ containing the group of all integers $Z$, and the quotient group $\bar{R}(k)=R(k)/Z$ is isomorphic with the multiplicative group $W(k)$ of all roots of unity in $k$.

We now take an algebraic closure $\Omega$ of $k$ and consider the subfield $K$ of $\Omega$ obtained by adjoining all $\alpha^{1/n}$ to $k$, where $\alpha$ is an arbitrary element in $k$ and $n$ is an arbitrary integer in $Z(k)$. $K$ is obviously the composite of all finite Kummer extensions of $k$ contained in $\Omega$ and hence, may be called the *Kummer closure* of $k$ in $\Omega$. $K/k$ is clearly an abelian extension and its structure is independent of the choice of the algebraic closure $\Omega$ of $k$. In particular, the structure of the Galois group $G(K/k)$ of $K/k$ is an invariant of the field $k$, and we shall show in the following how we can describe it by means of groups which depend solely on the ground field $k$.

**2.** We shall first define a symbol $(\sigma, \alpha, r)$ for arbitrary $\sigma$ in $G=G(K/k)$, $\alpha\neq 0$ in $k$ and $r$ in $R(k)$. Namely, we express $r$ as a fraction $\frac{m}{n}$ with denominator $n$ in $Z(k)$ and choose an elemnt $a$ in $K$ such that $a^n=\alpha^m$. The symbol $(\sigma, \alpha, r)$ is then defined by

$$(\sigma, \alpha, r)=a^{\sigma-1}.$$

It is easy to see that $(\sigma, \alpha, r)$ is an $n$-th root of unity in $k$ and is independent of the choice of the fractional expression $\frac{m}{n}$ of $r$ and, also, of the choice of $a$ in $K$ such that $a^n=\alpha^m$.

The symbol $(\sigma, \alpha, r)$, defined uniquely in this way, has the following properties which can be verified easily from the definition:

1) $(\sigma_1\sigma_2, \alpha, r)=(\sigma_1, \alpha, r)(\sigma_2, \alpha, r)$,
2) $(\sigma, \alpha_1\alpha_2, r)=(\sigma, \alpha_1, r)(\sigma, \alpha_2, r)$,
3) $(\sigma, \alpha, r_1+r_2)=(\sigma, \alpha, r_1)(\sigma, \alpha, r_2)$,
4) $(\sigma, \alpha, m)=1, \qquad m \in Z$.

From 3), 4), it follows that $(\sigma, \alpha, r)$ essentially depends upon $\sigma$, $\alpha$ and the residue class $\bar{r}$ or $r$ mod. $Z$ and that we may therefore put $(\sigma, \alpha, r)=(\sigma, \alpha, \bar{r})$. The new symbol $(\sigma, \alpha, \bar{r})$ then has properties similar to 1), 2), 3) above.

We now fix $\sigma$ and $\alpha$ and consider a mapping $\varphi_{\sigma,\alpha}$ of $\bar{R}(k)$ into $W(k)$ defined by

$$\varphi_{\sigma,\alpha}(\bar{r})=(\sigma, \alpha, \bar{r}).$$

By 3), $\varphi_{\sigma,\alpha}$ is a homomorphism of $\bar{R}(k)$ into $W(k)$, i.e. an element of the group of homomorphisms Hom $(\bar{R}(k), W(k))$. We then define, for any fixed $\sigma$, a mapping $f_\sigma$ of the multiplicative group $k^*$ of $k$ into Hom $(\bar{R}(k), W(k))$ by

$$f_\sigma(\alpha)=\varphi_{\sigma,\alpha}.$$

$f_\sigma$ is again a homomorphism by 2), i.e. an element of the group of homomorphisms Hom $(k^*$, Hom $(\bar{R}(k), W(k)))$. We finally define a mapping $\Phi$ of $G$ into Hom $(k^*$, Hom $(\bar{R}(k), W(k)))$ by

$$\Phi: \quad \sigma \to f_\sigma.$$

$\Phi$ is a homomorphism by 1) and is, in fact, an isomorphism, for, if $f_\sigma$ is the identity, $(\sigma, \alpha, r)=1$ for every $\alpha$ in $k^*$ and every $r$ in $R(k)$, and it follows from the definition of $(\sigma, \alpha, r)$ that each $\alpha^{1/n}$ is invariant under $\sigma$, and that $\sigma$ is, consequently, the identity of the group $G=G(K/k)$.

We now consider $W(k)$, $\bar{R}(k)$ and $k^*$ as discrete groups and introduce the so-called compact convergence topology[1] in Hom $(\bar{R}(k), W(k))$ and Hom $(k^*$, Hom $(\bar{R}(k), W(k)))$. It is then easy to see that both

1) Cf. N. Bourbaki, Topologie générale, Chap. X.

these groups become topological groups and that a fundamental system of neighborhoods of the identity in $H=\text{Hom}(k^*, \text{Hom}(\bar{R}(k), W(k)))$ is given by the family of subsets $U(\alpha_1, \cdots, \alpha_s; n)$, where the set $U(\alpha_1, \cdots, \alpha_s; n)$ is defined for any finite set of elements $\alpha_1, \cdots, \alpha_s$ in $k^*$ and for any integer $n$ in $Z(k)$, and consists of elements $f$ in $H$ such that $f(\alpha_i)$ in $\text{Hom}(\bar{R}(k), W(k))$ maps the residue class of $\frac{1}{n}$ mod. $Z$ to the unity element 1 in $W(k)$. Therefore, an element $\sigma$ of $G$ is contained in $\Phi^{-1}(U(\alpha_1, \cdots, \alpha_s; n))$ if and only if $\left(\sigma, \alpha_i, \frac{1}{n}\right)=1$ for $i=1, \cdots, s$, and, taking $a_i$ in $K$ with $a_i^n=\alpha_i$ and putting $E=k(a_1, \cdots, a_s)$, we see that $\Phi^{-1}(U(\alpha_1, \cdots, \alpha_s; n))$ coincides with the Galois group $G(K/E)$ of $K/E$. But, since $E/k$ is a finite extension, $G(K/E)$ is an open subgroup of $G$ in Krull's topology of the Galois group $G=G(K/k)$. Therefore $\Phi$ is a continuous mapping of $G$ into $H$.

We shall next show that the image $\Phi(G)$ of $G$ is everywhere dense in $H$. Let $f$ be an arbitrary element of $H$ and $U(\alpha_1, \cdots, \alpha_s; n)$ an arbitrary neighborhood of the identity as given above. We prove that there exists an element $\sigma$ in $G$ such that $f^{-1}f_\sigma$ is contained in $U(\alpha_1, \cdots, \alpha_s; n)$; namely, such that

$$f(\alpha_i)\left(\frac{1}{n}\right)^{2)}=\left(\sigma, \alpha_i, \frac{1}{n}\right), \qquad i=1, \cdots, s.$$

To see this, we consider a function $\chi(\alpha)$ of $k^*$ defined by

$$\chi(\alpha)=f(\alpha)\left(\frac{1}{n}\right).$$

Since $\chi(\alpha)$ is obviously a character of $k^*$ and is trivial on the subgroup $(k^*)^n$, it follows from the theory of Kummer extensions that there exists a $k$-automorphism $\sigma$ of the field $K_n$ generated over $k$ by all $n$-th roots of elements in $k$, such that

$$\chi(\alpha)=(\alpha^{1/n})^{\sigma-1}.$$

Denoting an extension of $\sigma$ in the Galois group $G$ of $K/k$ again by $\sigma$, we see immediately from the definition of $(\sigma, \alpha, r)$ that

2) Here $\frac{1}{n}$ stands for the residue class of $\frac{1}{n}$ mod. $Z$.

$$\chi(\alpha)=\left(\sigma, \alpha, \frac{1}{n}\right),$$

which proves the assertion.

We have thus shown that $\Phi$ is a continuous isomorphism of $G$ into $H$ and the image $\Phi(G)$ of $G$ is everywhere dense in $H$. But, since $G$ is a compact group as the Galois group of $K/k$, $\Phi$ must be an isomorphism of $G$ onto $H$, and we have thus obtained the following

THEOREM 1. *Let $k$ be an arbitrary field and $K$ the Kummer closure of $k$ in an algebraic closure of $k$. Then the Galois group of $K/k$ is canonically isomorphic with the group of homomorphisms* $\mathrm{Hom}(k^*, \mathrm{Hom}(\bar{R}(k), W(k)))$ *which is attached to the field $k$ as described above.*

**3.** Now, it is easy to see that the group of roots of unity $W(k)$ of a field $k$ is isomorphic with a subgroup of the group of ordinary roots of unity $W_0=\{e^{2\pi ir};\ r=\text{rationals}\}$. Therefore, taking such an isomorphism $g$ of $W(k)$ into $W_0$, every element $\varphi$ of $\mathrm{Hom}(\bar{R}(k), W(k))$ defines a character $g\circ\varphi$ of the discrete group $\bar{R}(k)$. Moreover, using the fact that $\bar{R}(k)$ is isomorphic with $W(k)$, it can be seen that every character of $\bar{R}(k)$ can be written in the form $g\circ\varphi$ with some $\varphi$ in $\mathrm{Hom}(\bar{R}(k), W(k))$ and that $\mathrm{Hom}(\bar{R}(k), W(k))$ is consequently isomorphic with the character group $\widetilde{W}(k)$ of $W(k)$, both being considered as topological groups. Hence the Galois group $G$ of the Kummer closure $K$ of $k$ is isomorphic with the group of homomorphisms $\mathrm{Hom}(k^*, \widetilde{W}(k))$, and, though such a description of $G$ is not canonical (unlike the one as given in Theorem 1), it is useful when we only consider the structure of $G$ as a topological group and not a canonical description of it.

Let, for instance, $k$ be a field of characteristic 0 containing all roots of unity. Every finite abelian extension of $k$ is then a Kummer extension and the Kummer closure $K$ of $k$ coincides with the maximal abelian extension $A$ over $k$. Moreover, in such a case, the group $W(k)$ is isomorphic with the group $W_0$. Hence the Galois group $G(A/k)$ of the maximal abelian extension $A$ over $k$ is isomorphic with the group of homomorphisms $\mathrm{Hom}(k^*, \widetilde{W}_0)$ of $k^*$ into the character group $\widetilde{W}_0$ of $W_0$. To determine the structure of the group $G(A/k)$

more explicitly, we have, therefore, only to study the structure of the multiplicative group $k^*$ of $k$, and we shall do this in the following sections for a certain kind of algebraic number field containing all roots of unity.

**4.** We shall first define a special type of abelian group and give some simple properties which will be used later. Let $G$ be an abelian group and $T$ the torsion subgroup of $G$. We call $G$ a *regular* abelian group when the factor group $G/T$ is free abelian. The following properties of regular abelian groups are immediate consequences of the definition:

$\alpha$) an abelian group $G$ is regular if and only if it is the direct product of its torsion subgroup $T$ and a free abelian subgroup of $G$,

$\beta$) if $H$ is a subgroup of an abelian group $G$ and if every element of $H$ has finite order, $G/H$ is regular if and only if $G$ is regular,

$\gamma$) a subgroup of a regular abelian group is regular,

$\delta$) the direct product of a finite number of regular abelian groups is regular,

$\varepsilon$) if $\{H_i\}$ is a finite set of subgroups of an abelian group $G$ such that their intersection is $e$ and if every $G/H_i$ is regular, then $G$ itself is also regular.[3)]

We shall now prove the following lemmas:

LEMMA 1. *Let $G$ be a regular abelian group and let $\{\sigma\}$ be a finite set of endomorphisms of $G$. If $H$ is the subgroup of $G$ consisting of all elements of $G$ which are invariant under all $\sigma$, then $G/H$ is also a regular abelian group.*

PROOF. For each $\sigma$, let $H_\sigma$ denote the kernel of the endomorphism $\tau(a)=\sigma(a)a^{-1}$ of $G$. Since $G/H_\sigma$ is isomorphic with $\tau(G)$ and $\tau(G)$ is regular by $\gamma$), $G/H_\sigma$ is also regular. But, as $H$ is clearly the intersection of all $H_\sigma$, $G/H$ is regular by $\varepsilon$).

LEMMA 2. *Let $G$ be an abelian group and $H$ a subgroup of $G$. If $H$ and $G/H$ are both regular and if the orders of elements of the torsion subgroup of $G/H$ are bounded, then $G$ is also regular.*

PROOF. Let $U$ be the torsion subgroup of $H$. By $\beta$) above, it suffices to show that $G/U$ is regular. We may therefore assume that $U=e$ and $H$ is free abelian. Let $V$ be the subgroup of $G$ containing

3) Notice that $G$ is isomorphic with a subgroup of the direct product of all $G/H_i$.

$H$ such that $V/H$ is the torsion subgroup of $G/H$. By the assumption, there is an integer $m$ such that $V^m$ is contained in $H$. If we then denote by $T$ the kernel of the endomorphism $\sigma(a)=a^m$ of $V$, $V/T$ is isomorphic with the subgroup $V^m$ of the free abelian group $H$ and, hence, is again free abelian. On the other hand, since $G/H$ is regular, $G/V$ is also free abelian. Therefore $G/T$ is free abelian and $G$ is regular, for $T$ must be the torsion subgroup of $G$.[4]

**5.** We shall now study the structure of the multiplicative groups of a certain class of algebraic number fields by applying the result of the preceding section. If there will be no risk of confusion, we shall denote, for simplicity, the multiplicative group of a field $k$ by the same letter $k$, instead of $k^*$.

LEMMA 3. *The multiplicative group of a finite algebraic number field E is regular.*

PROOF. Since the group of ideals of $E$ is obviously free abelian, so is the subgroup of principal ideals of $E$. But the latter group is isomorphic with the factor group $E/U$ of the multiplicative group of $E$ modulo the group of units of $E$, and, as $U$ is regular by Dirichlet's theorem, $E$ is also regular by Lemma 2.

LEMMA 4. *Let E be a finite algebraic number field and let F be a finite extension of E. Then the factor group F/E is regular.*

PROOF. Let $K$ be a finite Galois extension of $E$ containing $F$. Since $F/E$ is a subgroup of the factor group $K/E$, it suffices to show that $K/E$ is regular. But $K$ is regular by Lemma 3 and $E$ is the subgroup of $K$ consisting of all elements of $K$ which are invariant under the Galois automorphisms of the extension $K/E$. The group $K/E$ is therefore regular by Lemma 1.

LEMMA 5. *Let E be a finite algebraic number field and let A be an abelian extension of E containing all roots of unity. Denote by W the group of roots of unity in A and by N the subgroup of A containing E such that N/E is the torsion subgroup of A/E. If m is the order of the finite group $E \frown W$, $N^m$ is contained in the group EW.*

PROOF. Let $p$ be an arbitrary prime number and let $p^e$ ($e \geq 0$) be the $p$-part of the order $m$. To prove the theorem, it suffices to

4) In general, an abelian group $G$ is not regular even when $H$ and $G/H$ are both regular groups. Example: $G$ = the additive group of rationals, $H$ = the additive group of integers.

show that $N$ contains no element of order $p^{e+1}$ modulo $EW$. For the proof, we assume that there exists an element $\xi$ of order $p^{e+1}$ modulo $EW$ and show that such an assumption leads to a contradiction. Let $\xi^{p^{e+1}}=\alpha\omega$ with $\alpha$ in $E$, $\omega$ in $W$. Taking a $p^{e+1}$-th root $\omega'$ of $\omega^{-1}$ and replacing $\xi$ by $\xi\omega'$, we may assume that

$$\xi^{p^{e+1}}=\alpha\,, \qquad \alpha\in E\,.$$

Let $f(x)$ be the minimal polynomial of $\xi$ over $E$ and $n$ the degree of $f(x)$. Since $f(x)$ is a divisor of $x^{p^{e+1}}-\alpha=\prod(x-\eta\xi)$, where $\eta$ runs over all $p^{e+1}$-th roots of unity, the constant term of $f(x)$ must be of the form $\eta_1\xi^n$ with a suitable $p^{e+1}$-th root of unity $\eta_1$. It follows that $\xi^n$ is contained in $EW$ and, consequently, that $n=p^{e+1}$, $f(x)=x^{p^{e+1}}-\alpha$. Therefore $K=E(\xi)$ is an abelian extension of degree $p^{e+1}$ over $E$ and it contains a primitive $p^{e+1}$-th root of unity $\zeta$. Since $\zeta$ is not contained in $E$, while $\zeta^p$ is in $E$, the intermediate field $E(\eta)$ of $K/E$ must be an extension of degree $p$ over $E$, and we see, in particular, that $e\geq 1$. The constant term of the minimal polynomial of $\xi$ over $F=E(\zeta)$ is again of the form $\eta_2\xi^{p^e}$ with a suitable $p^{e+1}$-th root of unity $\eta_2$ and it follows that $\beta=\xi^{p^e}$ is in $F$ and $F=E(\beta)$. Now, since $F=E(\zeta)=E(\beta)$ is a Kummer extension of degree $p$ over $E$ such that $\zeta^p$ and $\beta^p$ are both contained in $E$, the product of $\beta$ with a suitable power of $\zeta$ must be in $E$. But $\beta=\xi^{p^e}$ is then contained in $EW$ and this contradicts the assumption that the order of $\xi$ modulo $EW$ is $p^{e+1}$. The lemma is therefore proved.

We now consider an arbitrary abelian extension $A$ of a finite algebraic number field $k$ and prove that the multiplicative group of $A$ is regular. Let $A'$ be the field obtained by adjoining all roots of unity to $A$. $A'$ is then still abelian over $k$ and the multiplicative group $A$ is a subgroup of the multiplicative group $A'$. Hence it suffices to show that $A'$ is regular, and we may assume from the beginning that $A$ contains all roots of unity.

Let $E$ and $F$ be finite extensions of $k$ such that $E\subseteq F\subseteq A$ and let $W$ be again the group of all roots of unity in $A$. Since $(F\frown W)E/E$ is a finite group and $F/E$ is regular by Lemma 4, the group $F/(F\frown W)E$ is again regular by $\beta$) above. But, since we have the isomorphism

$$FW/EW \cong F/(F \frown W)E,$$

$FW/EW$ is also a regular abelian group. On the other hand, if we denote by $N_E$ the subgroup of $A$ containing $E$ such that $N_E/E$ is the torsion subgroup of $A/E$, and by $N_F$ the corresponding group for $F$, the orders of elements of $N_F/FW$ are bounded by Lemma 5. Therefore $N_F/EW$ is regular by Lemma 2. Since $N_E/EW$ is obviously the torsion subgroup of $N_F/W$, it follows that $N_F/N_E$ is a free abelian group.

Now, let

$$k=E_0 \subseteqq E_1 \subseteqq E_2 \subseteqq \cdots$$

be a sequence of finite extensions of $k$ such that $A$ is the union of all these $E_n$, and let $N_n=N_{E_n}$ be the subgroup of $A$ containing $E_n$ such that $N_n/E_n$ is the torsion subgroup of $A/E_n$. By what we have proved above, every factor group $N_n/N_{n-1}$ $(n=1, 2, \cdots)$ is a free abelian group. Since the group $A$ is obviously the union of all $N_n$, it follows immediately that $A/N_0$ is also free abelian. On the other hand, considering $E_0W/W$ instead of $FW/EW$ and using a similar argument, we can see easily that $N_0$ is a regular abelian group. It then follows from Lemma 2 that the group $A$ is also regular, thus proving our previous contention. By $\alpha$) above, our result can be stated as follows:

THEOREM 2. *The multiplicative group of an abelian extension $A$ of a finite algebraic number field is the direct product of a free abelian group and the group of roots of unity in $A$.*

**6.** We now change our notation and denote by $k$ an algebraic number field which contains all roots of unity and which is an abelian extension of a finite algebraic number field. As we have seen in § 3, the Galois group $G(A/k)$ of the maximal abelian extension $A$ over $k$ is isomorphic with the group of homomorphisms $\mathrm{Hom}(k^*, \tilde{W}_0)$. In this section, we shall determine the structure of the latter group using the result of § 5.

By Theorem 2, the multiplicative group $k^*$ of $k$ is the direct product of the group of roots of unity in $k$, $W(k)$, and a free abelian group $U$ which has, as readily seen, a countable number of free generators $u_1, u_2, \cdots$. Let $\varphi$ be any homomorphism in $\mathrm{Hom}(k^*, \tilde{W}_0)$.

We shall show that the character $\chi=\varphi(\omega)$ of $W_0$ is trivial for any root of unity $\omega$ in $W(k)$. To see this, let $\zeta$ be an arbitrary root of unity in $W_0$ and let $\zeta^n=1$. If we take $\omega_1$ in $W(k)$ such that $\omega_1^n=\omega$ and put $\chi_1=\varphi(\omega_1)$, we have

$$\chi=\chi_1^n\,,$$
$$\chi(\zeta)=\chi_1^n(\zeta)=\chi_1(\zeta^n)=\chi_1(1)=1\,,$$

which proves our assertion. Hence, a homomorphism $\varphi$ in Hom $(k^*, \tilde{W}_0)$ is completely determined by its values $\varphi(u_i)$ for the basis $u_i$, $i=1, 2, \cdots$. On the other hand, since the $u_i$ are free generators of the group $U$, there exists at least one homomorphism $\varphi$ in Hom $(k^*, \tilde{W}_0)$ satisfying $\varphi(u_i)=\chi_i$ for any given sequence of characters $\chi_i$ in $\tilde{W}_0$. It then follows immediately that the mapping

$$\varphi\rightarrow(\varphi(u_1),\ \varphi(u_2), \cdots)$$

gives a topological isomorphism of Hom $(k^*, \tilde{W}_0)$ with the direct product of a countable number of copies $\tilde{W}_0^{(i)}$ of the group $\tilde{W}_0$.

We have therefore the following theorem:

THEOREM 3. *Let $k$ be an abelian extension of a finite algebraic number field containing all roots of unity and let $A$ be the maximal abelian extension of $k$. Then the Galois group of $A/k$ is isomorphic with the direct product of a countable number of groups each of which is isomorphic with the character group of the group of roots of nuity in $k$.*

**7.** We add here some remarks on the above result. Let $k$ and $A$ be as in Theorem 3. Let $A_0=k$, $A_1=A$ and let, in general, $A_n$ be the maximal abelian extension of $A_{n-1}$ $(n\geqq 2)$. We can determine the structure of the multiplicative group of $A_n$ $(n\geqq 1)$ by a method similar to that of § 5 and, then, by using the result of § 3, we can also prove that the Galois group of the extension $A_n/A_{n-1}$ is always isomorphic with the direct product of a countable number of copies $\tilde{W}_0^{(i)}$ of the group $\tilde{W}_0$. In other words, if we take the maximal solvable extension $\Sigma$ of $k$ and denote by $G_n$ the $n$-th topological commutator group of the Galois group $G(\Sigma/k)$ of $\Sigma/k$ $(G_0=G(\Sigma/k))$, we have

$$G_{n-1}/G_n\cong\prod_{i=1}^{\infty}\tilde{W}_0^{(i)}\,,\qquad n=1, 2, \cdots.$$

This gives considerable information about the group $G(\Sigma/k)$, though we can determine the structure of $G(\Sigma/k)$ completely by an entirely different method.[5]

University of Tokyo
Massachusetts. Institute of Technology.

5) Cf. the author's forthcoming paper "On solvablè extensions of algebraic number fields".