T. Kubota and S. Oka
Nagoya Math. J.
Vol. 160 (2000), 135–142

ON THE DEDUCTION OF THE CLASS FIELD THEORY FROM THE GENERAL RECIPROCITY OF POWER RESIDUES

TOMIO KUBOTA AND SATOMI OKA

Abstract. We denote by (A) Artin's reciprocity law for a general abelian extension of a finite degree over an algebraic number field of a finite degree, and denote two special cases of (A) as follows: by (AC) the assertion (A) where K/F is a cyclotomic extension; by (AK) the assertion (A) where K/F is a Kummer extension. We will show that (A) is derived from (AC) and (AK) only by routine, elementarily algebraic arguments provided that $n = (K : F)$ is odd. If n is even, then some more advanced tools like Proposition 2 are necessary. This proposition is a consequence of Hasse's norm theorem for a quadratic extension of an algebraic number field, but weaker than the latter.

§0. Introduction

Let K/F be an abelian extension of a finite degree over an algebraic number field F of a finite degree, and let $(\frac{K/F}{\mathfrak{a}})$ be the Artin symbol of an ideal $\mathfrak{a}$ of F. Then, the essential part of Artin's reciprocity law for K/F is the following assertion:

(A) There exists an ideal $\mathfrak{m}$ of F depending only on K/F such that $(\frac{K/F}{\mathfrak{a}}) = 1$ holds whenever $\mathfrak{a} = (\alpha)$ is a principal ideal generated by a totally positive integer α of F satisfying the congruence $\alpha \equiv 1 \pmod{\mathfrak{m}}$.

We denote two special cases of (A) as follows:

(AC) The assertion (A) where K/F is a cyclotomic extension.

(AK) The assertion (A) where K/F is a Kummer extension.

Since every abelian extension is contained in a field which is obtained by two successive extensions of the basic field, one cyclotomic and the other Kummer, it may be asked whether or not the assertion (A) is an evident

Received November 12, 1999.
2000 Mathematics Subject Classification: Primary:11R37, Secondary:11E12.

consequence of (AC) and (AK). The aim of the present paper is to give an answer to the question. As is shown in Section 1, (A) is derived from (AC) and (AK) only by routine, elementarily algebraic arguments provided that $n = (K : F)$ is odd. If n is even, then some more advanced tools are necessary. In Section 2, we shall derive (A) from (AC) and (AK) using additionally the norm theorem for quadratic extensions obtained by adjoining $i = \sqrt{-1}$.

The present work is motivated by [1]. Logically, however, both papers are independent of each other.

§1. The odd case

In this section, we denote by F an algebraic number field of finite degree, by K/F a cyclic extension of degree $q = p^g$, p being an odd prime, and will deduce (A), Artin's reciprocity law, from (AC) and (AK).

The problem is first reduced to the case where F contains the p-th roots of unity. In fact, if F_1 and K_1 are obtained by adjoining the p-th roots of unity to F and K, respectively, then $m = (F_1 : F)$ divides $p - 1$, and $(\frac{K_1/F_1}{\mathfrak{a}}) = (\frac{K_1/F}{\mathfrak{a}})^m$ for an ideal $\mathfrak{a}$ of F. Therefore, if (A) is true for K_1/F_1, then(A) is true for K/F, as m is prime to p.

So, in the rest of this section, we assume that F contains the p-th roots of unity, but does not contain all the q-th roots of unity. Denote by $\mu_{(n)}$ the group of the n-th roots of unity, and, for a general number field L containing $\mu_{(n)}$, define the symbol $\langle \alpha, \sigma | L \rangle_n \in \mu_{(n)}$ by

$$(\alpha^{1/n})^\sigma = \langle \alpha, \sigma | L \rangle_n \cdot \alpha^{1/n}, \tag{1}$$

where $\alpha \in L$, $(\alpha \neq 0)$, and $\sigma \in \mathrm{Gal}(\bar{L}/L)$, $\bar{L}$ being the algebraic closure of L. This definition is independent of the choice of $\alpha^{1/n}$.

Coming back to our K/F, we take a generator ξ of $\mu_{(q)}$, put $F_1 = F(\xi)$, $K_1 = K(\xi)$, and, taking a generator τ of $\mathrm{Gal}(F_1/F)$, fix an $r \in \mathbf{Z}$ by the following multiplicative relation: $\zeta^{r\tau} = \zeta$, i.e., $rr' \equiv 1 \pmod{q}$, if $\zeta^\tau \equiv \zeta^{r'}$, $(r' \in \mathbf{Z})$. Furthermore, we determine an element $\hat{\tau}$ of the group ring over $\mathbf{Z}$ of $\mathrm{Gal}(F_1/F)$ by

$$\hat{\tau} = 1 + r\tau + (r\tau)^2 + \cdots + (r\tau)^{m-1}, \quad (m = (F_1 : F)). \tag{2}$$

If $\alpha \in F_1$ is such that $K_1 = F_1(\alpha^{1/q})$, and if τ denotes also a prolongation of the original τ to $\bar{\mathbf{Q}}$, then the fact that K_1/F is abelian entails

$$(\alpha^{1/q})^{1-r\tau} = \gamma, \quad (r \in F_1),$$

and

$$\gamma^{\hat{\tau}} = (\alpha^{1/q})^{(1-r\tau)\hat{\tau}} = (\alpha^{1/q})^{1-r^m}.$$

It follows from this and from

$$1 - r^m = qc, \quad ((c,q) = 1),$$

that

$$\alpha^c = \gamma^{\hat{\tau}}. \tag{3}$$

On the other hand, since

$$\begin{aligned}(\gamma^{1/q})^{\tau^j\sigma\tau^{-j}} &= (\langle\gamma^{\tau^j}, \sigma|F_1\rangle_q(\gamma^{1/q})^{\tau^j})^{\tau^{-j}} \\ &= \langle\gamma^{r^j\tau^j}, \sigma|F_1\rangle_q \cdot \gamma^{1/q}\end{aligned}$$

holds for every power τ^j of τ, we obtain

$$\langle\gamma, \tau^j\sigma\tau^{-j}|F_1\rangle_q = \langle\gamma^{r^j\tau^j}, \sigma|F_1\rangle_q \tag{4}$$

for any $\sigma \in \mathrm{Gal}(\bar{F}_1/F_1)$. Regard σ to be an element of $\mathrm{Gal}(\bar{F}/F)$, and let $t_{F\to F_1}\sigma$ be the transfer of σ into $\mathrm{Gal}(\bar{F}_1/F_1)$. Then,

$$t_{F\to F_1}\sigma = \prod_{j=0}^{m-1} \tau^j\sigma\tau^{-j}$$

yields

$$\langle\gamma^{\hat{\tau}}, \sigma|F_1\rangle_q = \langle\gamma, t_{F\to F_1}\sigma|F_1\rangle_q. \tag{5}$$

Therefore, (3) implies

$$\langle\alpha^c, \sigma|F_1\rangle_q = \langle\gamma, t_{F\to F_1}\sigma|F_1\rangle_q. \tag{6}$$

Assume now a modulus $\tilde{\mathfrak{m}}$, including infinite primes, is sufficiently big so that every ideal $\mathfrak{a}$ of F with $\mathfrak{a} \equiv 1 \pmod{\tilde{\mathfrak{m}}}$ satisfies $(\frac{F_1/F}{\mathfrak{a}}) = 1$, and has no prime factor ramifying in the Galois closure of $K_1(\gamma^{1/q})/F$. Assume moreover that, $\tilde{\mathfrak{m}}$ being viewed as a modulus of F_1, every ideal $\mathfrak{a}_1$ of F_1 with $\mathfrak{a}_1 \equiv 1 \pmod{\tilde{\mathfrak{m}}}$ satisfies $(\frac{F_1(\gamma^{1/q})/F_1}{\mathfrak{a}_1}) = 1$. Then, for the maximal abelian subfield K^* of $K_1(\gamma^{1/q})/F$, $(\frac{K^*/F}{\mathfrak{a}})$ is induced by some $\sigma \in \mathrm{Gal}(\bar{F}_1/F_1)$, and it follows from the relationship between Frobenius automorphism and the transfer that $t_{F\to F_1}\sigma$ indues $(\frac{F_1(\gamma^{1/q})/F_1}{\mathfrak{a}})$[1)]. If $\mathfrak{a} \equiv 1 \pmod{\tilde{\mathfrak{m}}}$, then the

[1)] Proved by Chevalley [1] for the first time.

latter autmorphism is 1. So, the right hand side of (6) is 1, and the fact that the left hand side of (6) is 1 means that the restriction of σ to K_1 is 1. Hence, $(\frac{K/F}{\mathfrak{a}}) = 1$. This proves Artin's reciprocity law for the odd case. In the above arguments, (AC) and (AK) are fully used.

§2. The even case

In this section, we put $q_0 = 2^{g_0}$, and denote by q_0 a cyclic extension of degree q_0 over an algebraic number field F. Let ζ_0 be a generator of the group $\mu_{(q_0)}$ of the q_0-th roots of unity, and assume that $F(\zeta_0) = F_{q_0}$ is cyclic over F. Then, the assertion (A) for K/F can be proved exactly as in the odd case. For, using ζ_0 and F_{q_0} instead of ζ and F_1 in Section 1, respectively, we have as in Section 1 a multiplicative relation $\zeta_0^{r\omega} = \zeta_0$ with a generator ω of $\mathrm{Gal}(F_{q_0}/F)$ and with $r \in \mathbf{Z}$.

So, in the rest of this section, we treat the case where F_{q_0}/F is not cyclic. For this purpose, we need the following

PROPOSITION 1. *Let F be an algebraic number field, let $q = 2^g$ be a power of 2, denote by ζ a generator of the group $\mu_{(q)}$ of the q-th roots of unity, put $F_q = F(\zeta)$, and put $F_{q,0} = F(\zeta + \zeta^{-1})$. Furthermore, denote by τ a generator of* $\mathrm{Gal}(\cup F_{q,0}/F)$, *$(q = 2^g, g = 1, 2, \ldots)$. Assume now, for a power $q_0 = 2^{g_0}$ of 2, β_0 in $F_{q_0,0}$ has the property that $\beta_0^{1-\tau}$ is a norm from $F_q = F_{q_0,0}(i)$. Then, there exists $\delta \in F$ such that $\delta\beta_0$ is a norm from $F_q = F_{q,0}(i)$ to $F_{q,0}$ for a sufficiently large $q = 2^g$.*

This proposition follows immediately from Proposition 2, because there exists by the assumption an element δ of F such that $\delta\beta_0$ is totally positive.

PROPOSITION 2. *Let F, F_q and $F_{q,0}$ be as in Proposition* 1, *then, a totally positive element β of F is a norm from F_q to $F_{q,0}$ for a sufficiently large $q = 2^g$.*

A proof of this proposition will be given in Section 3, where the norm theorem for relatively quadratic extensions is applied.

Coming back to the proof of (A), let K/F be a cyclic extension of degree $q_0 = 2^{g_0}$, let ζ be a generator of the group $\mu_{(q)}$ of the q-th roots of unity for a general large power $q = 2^g$ of 2, put $K_q = K(\zeta)$, and in particular let ζ_0 be a generator of $\mu_{(q_0)}$. Then, $K_{q_0} = K(\zeta_0)$ is a Kummer extension over $F_{q_0} = F(\zeta_0)$, and there exists an $\alpha_0 \in F_{q_0}$ such that $K_{q_0} = F_{q_0}(\alpha_0^{1/q_0})$.

Denote by τ also a prolongation to $\bar{\mathbf{Q}}$ of τ in Proposition 1, and on the other hand, denote by ω a generator of $\mathrm{Gal}(F(i)/F)$ as well as its prolongation to $\bar{\mathbf{Q}}$. Then, $i^{\omega} = -i$, and ω is independent of τ on $F_q = F(\zeta)$, as F_{q_0}/F is not cyclic by the assumption. Namely, $F_{q,0}$ being as in Proposition 1, one may assume that τ and ω are trivial on $F(i)$ and $F_{q,0}$, respectively, and in addition that there exists an $r \in \mathbf{Z}$ independent of g satisfying the multiplicative relation $\zeta^{r\tau} = \zeta$ in the same form as in Section 1.

Since $F_{q_0}/F_{q_0,0}$ is abelian,

$$(\alpha_0^{1/q_0})^{1+\omega} = \beta_0, \quad (\beta_0 \in F_{q_0,0}), \tag{7}$$

holds. Since $K_{q_0}/F(i)$ is abelian,

$$(\alpha_0^{1/q_0})^{1-r\tau} = \gamma_0, \quad (\gamma_0 \in F_{q_0}), \tag{8}$$

holds[2)]. Moreover, since K_{q_0}/F is abelian, it follows from (7) and (8) that

$$\beta_0^{1-r\tau} = \gamma_0^{1+\omega}, \tag{9}$$

and Proposition 1, applied to this β_0, shows that there extists a $\delta \in F$ with

$$\delta\beta_0 = \eta^{1+\omega}, \quad (\eta \in F_q), \tag{10}$$

where $q = 2^g$ is a sufficiently high power of 2. Put here

$$\alpha = \alpha_0^{q/q_0}\delta^{q/2}\eta^{-q} \in F_q. \tag{11}$$

Then, a computation using $\alpha^{1/q} = \alpha_0^{1/q_0}\delta^{1/2}\eta^{-1}$ shows

$$(\alpha^{1/q})^{1-r\tau} = \gamma \tag{12}$$

with

$$\gamma = \pm\gamma_0\delta^{(1-r)/2}\eta^{-(1-r\tau)} \in F_q.$$

A further computation using (9) and (10) shows

$$\begin{aligned}\gamma^{1+\omega} &= \gamma_0^{1+\omega}\delta^{1-r}(\delta\beta_0)^{-(1-r\tau)} \\ &= \beta_0^{1-r\tau}\beta^{-(1-r\tau)} = 1,\end{aligned}$$

[2)] Standard Kummer theory.

and consequently

$$\gamma = \theta^{1-\omega}, \quad (\theta \in F_q)\ ^{3)}. \tag{13}$$

Put next

$$\hat{\tau} = 1 + r\tau + (r\tau)^2 + \cdots + (r\tau)^{m-1}, \quad (m = (F_q : F(i))),$$

in analogy to (2). Then, similarly to (3), it follows from (12) that $\alpha^c = \gamma^{\hat{\tau}}$, $((c,2)=1)$, and this, combined with (13), implies

$$\alpha^c = \theta^{\hat{\tau}(1-\omega)}. \tag{14}$$

If σ is an arbitrary element of $\mathrm{Gal}(\bar{\mathbf{Q}}/F_q)$, then the equality

$$\begin{aligned}(\theta^{1/q})^{\omega\sigma\omega^{-1}} &= (\langle\theta^{\omega}, \sigma|F_q\rangle_q \cdot (\theta^{1/q})^{\omega})^{\omega^{-1}} \\ &= \langle\theta^{-\omega}, \sigma|F_q\rangle_q \cdot \theta^{1/q}\end{aligned}$$

holds with the symbol in (1) so that

$$\langle\theta, \omega\sigma\omega^{-1}|F_q\rangle = \langle\theta^{-\omega}, \sigma|F_q\rangle_q,$$

while the equality

$$\langle\theta, \tau^j\sigma\tau^{-j}|F_q\rangle_q = \langle\theta^{\gamma^j\tau^j}, \sigma|F_q\rangle_q,$$

like (4), holds for every power τ^j of τ. These two formulas imply the relation

$$\langle\theta^{\hat{\tau}(1-\omega)}, \sigma|F_q\rangle_q = \langle\theta, t_{F\to F_q}\sigma|F_q\rangle_q$$

which is similar to (5), and from (14) follows

$$\langle\alpha^c, \sigma|F_q\rangle_q = \langle\theta, t_{F\to F_q}\sigma|F_q\rangle_q \tag{15}$$

as (6).

Assume now a modulus $\tilde{\mathfrak{m}}$ of F to be big enough so that an ideal $\mathfrak{a}$ of F with $\mathfrak{a} \equiv 1 \pmod{\tilde{\mathfrak{m}}}$ contains no ramifying prime factor in the Galois closure of $K_q(\theta^{1/q})/F$, and satisfies $(\frac{F_q/F}{\mathfrak{a}}) = 1$ as well as $(\frac{F(\delta^{1/2})/F}{\mathfrak{a}}) = 1$; this is certainly possible in our situation, because $F(\delta^{1/2})/F$ is a Kummer extension. Furthermore, $\tilde{\mathfrak{m}}$ being viewed as a modulus of F_q, assume that $(\frac{F_q(\theta^{1/q})/F_q}{\mathfrak{a}_1}) = 1$, for every ideal $\mathfrak{a}_1$ of F_1 with $\mathfrak{a}_1 \equiv 1 \pmod{\tilde{\mathfrak{m}}}$. Then, for

[3)] Hilbert's theorem 90.

the maximal abelian subfield K^* of the Galois closure of $K(\theta^{1/q})/F$, the automorphism $(\frac{K^*/F}{\mathfrak{a}})$ is induced by some $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/F_q)$, and $t_{F\to F_q}\sigma$ induces $(\frac{F_q(\theta^{1/q})/F_q}{\mathfrak{a}})$ due to the relationship between Frobenius autmorphism and the transfer (cf. §1). If $(\frac{F_q(\theta^{1/q})/F_q}{\mathfrak{a}})$ then the latter symbol is 1, which means the right hand side of (15) is 1. Hence, the left hand side of (15) is 1. Therefore, it follows from (11) and from the assumption that

$$\begin{aligned} 1 &= \langle \alpha^c, \sigma|F_q\rangle_q = \langle \alpha_0^{cq/q_0}\delta^{q/2}, \sigma|F_q\rangle_q \\ &= \langle \alpha_0^c, \sigma|F_{q_0}\rangle_{q_0}\langle \delta, \sigma|F\rangle_2 = \langle \alpha_0^c, \sigma|F_{q_0}\rangle_{q_0}; \end{aligned}$$

namely, the restriction of σ to K is 1. Thus, $(\frac{K/F}{\mathfrak{a}}) = 1$. This proves Artin's reciprocity law for the even case, where (AC) and (AK) are fully used as in the odd case.

§3. A proof of Proposition 2 on the basis of a local-global principal

In this section, we will show that Proposition 2 is easily derived from the norm theorem for relatively quadratic extensions obtained by adjoining i. With the same notation as in Proposition 2, we denote by $(\alpha, \beta|F_{q,0})_{\mathfrak{q}}$ Hilbert-Hasse's norm residue symbol of degree 2 over $F_{q,0}$ with respect to a place $\mathfrak{q}$ of $F_{q,0}$, suppose that $\mathfrak{q}$ is over a place $\mathfrak{p}$ of F, and denote temporarily by L and L' the completion by $\mathfrak{p}$ of F and the completion by $\mathfrak{a}$ of $F_{q,0}$, respectively. Furthermore, we write $(\alpha, \beta|L')$, etc., for the prolongations of symbols $(\alpha, \beta|F_{q,0})_{\mathfrak{a}}$, etc., to the completions. Then, a basic theorem of local class field theory implies

$$(\alpha, \beta|L') = (\alpha, N_{L'/L}\beta|L).$$

Therefore, if $\alpha, \beta \in L$ and $(L' : L) = 2^m$, $(m > 0)$, $N_{L'/L}\beta = \beta^{2^m}$ is a square in L so that $(\alpha, N_{L'/L'}\beta|L) = 1$ and $(\alpha, \beta|L) = 1$. This means that $(\alpha, \beta|F_{q,0})_{\mathfrak{q}} = 1$ for every $\alpha, \beta \in F$, whenever the $\mathfrak{q}$-complection of $F_{q,0}$ is an actual extension of the $\mathfrak{p}$-completion of F. On the other hand, a prime ideal $\mathfrak{p}$ of F decomposes completely in $F_{q,0}$ if and only if $N\mathfrak{p} \equiv \pm 1 \pmod q$. If this is the case, $N\mathfrak{p} \pm 1 \geq q$. Accordingly, if q is bigger than $N\mathfrak{p}+1$, then $\mathfrak{p}$ does not decompose completely in $F_{q,0}$. In other words, it is impossible that a prime ideal of F unlimitedly continues to split in the increasing chain of $F_{q,0}$. Thus, there exists a power q of 2 such that $(\alpha, \beta|F_{q,0})_{\mathfrak{q}} = 1$ for every finite place $\mathfrak{q}$ over a given $\mathfrak{p}$. In addition, $(\alpha, \beta|F_{q,0})_{\mathfrak{a}} = 1$, whenever

α, β and $\mathfrak{a}$ are prime to 2, and $(\alpha, \beta | F_{q,0})_{\mathfrak{q}} = 1$ holds for all infinite places, provided that β is totally positive. Hence, putting in particular $\alpha = -1$, Proposition 2 follows from Hasse's norm theorem for relatively quadratic extensions.

Proposition 2, a considerably weaker assertion than the norm theorem, may have a fairly simple or elementary proof. An easier proof of Proposition 2 gives rise to an easier construction of the class field theory.

References

[1] C. Chevalley, *Deux théorèmes d'arithmétique*, J. Math. Soc. Japan, **3-1** (1951), 36–44.

[2] T. Kubota, *Geometry of numbers and class field theory*, Japan. J. Math., **13-2** (1987), 235–275.

Tomio Kubota
Department of Mathematics
Meijo University
Shiogamaguchi 1-501, Tenpaku-ku
Nagoya, 468-8502, Japan

Satomi Oka
Department of Mathematics
Meijo University
Shiogamaguchi 1-501, Tenpaku-ku
Nagoya, 468-8502, Japan