RECIROCITY LAWS THROUGH FORMAL GROUPS

OLEG DEMCHENKO AND ALEXANDER GUREVICH

(Communicated by Matthew A. Papanikolas)

Abstract. A relation between formal groups and reciprocity laws is studied following the approach initiated by Honda. Let \( \xi \) denote an \( m \)th primitive root of unity. For a character \( \chi \) of order \( m \), we define two one-dimensional formal groups over \( \mathbb{Z}[\xi] \) and prove the existence of an integral homomorphism between them with linear coefficient equal to the Gauss sum of \( \chi \). This allows us to deduce a reciprocity formula for the \( m \)th residue symbol which, in particular, implies the cubic reciprocity law.

INTRODUCTION

In the pioneering work [H2], Honda related the quadratic reciprocity law to an isomorphism between certain formal groups. More precisely, he showed that the multiplicative formal group twisted by the Gauss sum of a quadratic character is strongly isomorphic to a formal group corresponding to the \( L \)-series attached to this character (the so-called \( L \)-series of Hecke type). From this result, Honda deduced a reciprocity formula which implies the quadratic reciprocity law. Moreover he explained that the idea of this proof comes from the fact that the Gauss sum generates a quadratic extension of \( \mathbb{Q} \), and hence, the twist of the multiplicative formal group corresponds to the \( L \)-series of this quadratic extension (the so-called \( L \)-series of Artin type). Proving the existence of the strong isomorphism, Honda, in fact, shows that these two \( L \)-series coincide, which gives the reciprocity law.

Childress and Stopple [CS1], [CS2] made an attempt to generalize Honda’s results to the higher reciprocity law. They proved that a twisted higher-dimensional multiplicative formal group is strongly isomorphic to a formal group corresponding to a matrix \( L \)-series of Hecke type. In [CS1], they study formal groups over local fields whose dimension is equal to the degree of the local field extension generated by a root of unity corresponding to the order of the character. In [CS2], the object of their research is formal groups over global fields of dimension \( p - 2 \), where the character is defined modulo \( p \). In fact, none of these papers contains a reciprocity result. Later, Childress and Grant [CG] applied the construction from [CS2] and deduced from it a partial result on the way to the Eisenstein reciprocity law. Grant [G] combined this approach with a generalized Stickelberger relation for commutative group varieties with complex multiplication and obtained in this manner a geometric proof of the Eisenstein reciprocity.

Received by the editors September 7, 2011.
2010 Mathematics Subject Classification. Primary 11A15, 14L05.

The first author was partially supported by RFBR grant 11-01-00588a, by Saint Petersburg State University research grant 6.38.75.2011, and by Grant-in-Aid (No. S-23224001) for Scientific Research, JSPS.

The second author was partially supported by ISF Center of Excellency grant 1691/10.

©2012 American Mathematical Society
Reverts to public domain 28 years from publication.
1591
In the present note, our aim is to give an alternative generalization of Honda’s results. Having in mind a character of order $m$, we define a formal group $G$ depending only on $m$. This formal group plays the same role as the multiplicative formal group in Honda’s considerations. Then a formal group $H$ corresponding to the $L$-series of a character $\chi$ (which is of Hecke type) is introduced, and the existence of an integral homomorphism from $H$ to $G$ with linear coefficient equal to the Gauss sum $g$ of $\chi$ is proved. This is, of course, equivalent to the fact that $H$ is strictly isomorphic to $G$ twisted by $g$. Since the latter formal group can be interpreted as coming from the $L$-series of the extension generated by $g$ (which is of Artin type), one can deduce from it a reciprocity formula for the $m$th residue symbol. This formula is an essential step in the proof of various reciprocity laws. To illustrate this, we show that it implies the cubic reciprocity law and a special case of the biquadratic reciprocity law. Moreover, combined with the Stickelberger relation, our formula gives the Eisenstein reciprocity law (see [IR]).

Our main tool is the theory of formal group types developed by Honda in [H1]. It allows us to avoid heavy computations with formal power series typical to [CG] and to keep all proofs only a few lines long. Unlike [CS1], [CS2] and [CG], we do not consider higher-dimensional formal groups, but only one-dimensional formal groups whose $p$-height is equal to the degree of the extension of $\mathbb{Q}_p$ generated by an $m$th root of unity. In the case where a primitive $m$th root of unity belongs to $\mathbb{Q}_p$, the formal group appearing in [CS1] is one-dimensional, and the construction described there becomes equivalent to ours up to a $p$-integral isomorphism. Notice that this approach has never been developed for proving a reciprocity result. The reciprocity formula established in this note is similar to that from [CG], but it has fewer restrictions on the parameters involved.

The outline of the paper is as follows. The main results related to types of formal groups are summarized in Section 1. Further, we recall Honda’s proof of the quadratic reciprocity (Section 2) applying formal group types instead of performing computations with formal power series. A higher reciprocity formula for the $m$th residue symbol (Theorem 3.3) is proved in Section 3. In Section 4, this reciprocity formula is applied for the cases $m = 3$ and $m = 4$, and another simple reciprocity formula (Proposition 4.1) is obtained. Performing standard manipulations with residue symbols we deduce from it the cubic reciprocity law (Proposition 4.2).

1. Preliminaries on formal groups

A one-parameter commutative formal group law (or just formal group) over a ring $A$ is a formal power series $F \in A[[x,y]]$ such that $F(x,0) = x$; $F(F(x,y),z) = F(x,F(y,z))$; $F(x,y) = F(y,x)$. Given a formal group $F$ over $A$, one can define a group structure on the set of formal power series over $A$ without constant term as follows: $f +_F g = F(f(x),g(x))$. For formal groups $F$ and $F'$ over $A$ a homomorphism from $F$ to $F'$ is a formal power series $f \in A[[x]]$ without constant term such that $F(f(x),y) = F'(f(x),y)$.

If $\lambda \in A[[x]]$ is such that $\lambda(x) \equiv x \mod \deg 2$, then there exists a unique inverse under composition $\lambda^{-1}$, and $F(x,y) = \lambda^{-1}(\lambda(x) + \lambda(y))$ is a formal group over $A$. The formal power series $\lambda_a(x) = x$ defines the additive formal group $F_a(x,y) = x + y$, and $\lambda_m(x) = -\log(1 - x) = \sum_{i=1}^{\infty} x^i/i$ gives the multiplicative formal group $F_m(x,y) = x + y - xy$. If $\lambda, \lambda' \in A[[x]]$, $c \in A$, then $\lambda'^{-1} \circ c \lambda \in A[[x]]$ is a homomorphism from $F$ to $F'$. Finally, suppose that $\text{char } A = 0$. Then for
any formal group $F$ over $A$, there exists a unique $\lambda \in A \otimes \mathbb{Z} \mathbb{Q}[[x]]$, $\lambda(x) \equiv x \mod \deg 2$, such that $F(x, y) = \lambda^{-1}(\lambda(x) + \lambda(y))$. In this case, the homomorphism $\lambda^{-1} \circ c\lambda \in A \otimes \mathbb{Z} \mathbb{Q}[[x]]$ from $F$ to $F'$ will be denoted by $[c]_{F,F'}$.

Let $K$ be a finite unramified extension of $\mathbb{Q}_p$ with integer ring $O_K$ and Frobenius automorphism $\Delta_p$. Extend $\Delta_p$ to a $\mathbb{Q}_p$-automorphism of $K[[x]]$ such that $\Delta_p(x) = x^p$. Let $E = O_K[[\Delta_p]]$ denote a noncommutative $\mathbb{Q}_p$-algebra with multiplication rule $\Delta_p a = a^{\Delta_p} \Delta_p$, where $a \in O_K$. It gives a left $E$-module structure on $K[[x]]$.

Let $u \in E$ be such that $u \equiv p \mod \Delta_p$. A power series $\lambda \in K[[x]]$ is said to be of type $u$ if $\lambda(x) \equiv x \mod \deg 2$ and $u\lambda \equiv 0 \mod p$. For instance, $\lambda_m$ is of type $p - \Delta_p$ for any prime $p$.

**Proposition 1.1 (Theorem 2).** If $\lambda \in K[[x]]$ is of type $u$, then $F(x, y) = \lambda^{-1}(\lambda(x) + \lambda(y)) \in O_K[[x,y]]$.

**Proposition 1.2 (Theorem 3).** Let $\lambda, \lambda' \in K[[x]]$ be of types $u, u'$, respectively, $c \in O_K$. Then $[c]_{F,F'} \in O_K[[x]]$ if and only if there exists $w \in E$ such that $wu = u'c$.

2. **QUADRATIC RECIPROCITY LAW**

For an odd prime $q$, let $\chi$ be the Legendre symbol $\chi(n) = (\frac{n}{q})$ and $\zeta$ be a primitive $q$th root of unity. The following properties of the Gauss sum $g = \sum_{n=1}^{q-1} \chi(n)\zeta^n$ are well known: $\chi(i)g = \sum_{n=1}^{q-1} \chi(n)\zeta^ni$ and $g^2 = eq$, where $e = (-1)^{(q-1)/2}$.

It is easy to see that the power series $\mu(x) = \sum_{i=1}^{\infty} \chi(i)x^i/i$ is of type $p - \chi(p)\Delta_p$ for any prime $p$; thus $H(x, y) = \mu^{-1}(\mu(x) + \mu(y)) \in \mathbb{Z}[[x, y]]$ by Proposition 1.1.

**Proposition 2.1 (cf. Theorem 1).** $[g]_{H,F_m} \in \mathbb{Z}[[\zeta]][[x]]$.

**Proof.** We have

$$\lambda_m^{-1}(g\mu(x)) = \lambda_m^{-1}\left(\sum_{n=1}^{q-1} \chi(n)\lambda_m(\zeta^n x)\right) = \sum_{n=1}^{q-1}(\lambda_m^{-1}(\chi(n)\lambda_m(\zeta^n x))).$$

Clearly, $[\chi(n)]_{F_m,F_m} \in \mathbb{Z}[[x]]$, so $[g]_{H,F_m} \in \mathbb{Z}[[\zeta]][[x]]$. □

**Proposition 2.2.** If $p \neq q$ is an odd prime, then $\left(\frac{q}{p}\right) = \left(\frac{eq}{p}\right)$.

**Proof.** For any odd prime $p \neq q$, the extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is unramified. By Propositions 2.1 and 2.2 there exists $w \in E$ such that $w(p - \chi(p)\Delta_p) = (p - \Delta_p)g$. This implies that $w = g$ and $g\chi(p) = g\Delta_p$. Then we get $\left(\frac{p}{q}\right) = \chi(p) = g^{\Delta_p}/g \equiv g^{p-1} = (eq)^{(p-1)/2} \equiv \left(\frac{eq}{p}\right) \mod p$. Hence, $\left(\frac{q}{p}\right) = \left(\frac{eq}{p}\right)$. □

Taking into account that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, Proposition 2.2 implies

**Quadratic reciprocity law.** If $p \neq q$ are odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$
3. HIGHER RECIPROCITY FORMULA

Let \( m \) be a positive integer and \( \xi \) be a primitive \( m \)th root of unity. For any prime \( p \nmid m \), denote by \( d_p \) the degree of the extension \( \mathbb{Q}_p(\xi)/\mathbb{Q}_p \). Let \( D \) be the set of positive integers \( l \) such that \( d_p \mid \nu_p(l) \) for any prime \( p \nmid m \) and \( \nu_p(l) = 0 \) for any prime \( p \mid m \). For any positive integer \( l = \prod_{i=1}^{k} p_i^{t_i} \), where \( p_1, \ldots, p_k \) are distinct primes, define \( \Psi(l) = \prod_{i=1}^{k} p_i^{(d_p-1)t_i/d_p} \) if \( l \in D \) and \( \Psi(l) = 0 \) if \( l \notin D \). Further, suppose that \( \tau: \mathbb{Z} \rightarrow \{\xi^i \mid i \in \mathbb{Z}\} \cup \{0\} \) is a multiplicative map, i.e., \( \tau(l_1l_2) = \tau(l_1)\tau(l_2) \) for any relatively prime \( l_1, l_2 \in \mathbb{Z} \). Put \( \lambda_r(x) = \sum_{i=1}^{\infty} \Psi(l)\tau(l)x^i/l \).

**Lemma 3.1.** The power series \( \lambda_r \) is of type \( p - \tau(p^{d_p})\Delta_{p^d} \) for any prime \( p \nmid m \).

**Proof.** For any prime \( p \nmid m \), we have

\[
(p - \tau(p^{d_p})\Delta_{p^d}) \lambda_r = (p - \tau(p^{d_p})\Delta_{p^d}) \sum_{(l,p)=1}^{\infty} \sum_{j=0}^{\infty} \frac{\Psi(l)\tau(l)\Psi(p^{jd_p})\tau(p^{jd_p})}{l^{p^d}}x^j/l^{p^d} = (p - \tau(p^{d_p})\Delta_{p^d}) \sum_{(l,p)=1}^{\infty} \frac{\Psi(l)\tau(l)\Psi(p^{jd_p})\tau(p^{jd_p})}{l^{p^d}}x^j/l^{p^d}
\]

\[
= \sum_{(l,p)=1}^{\infty} \frac{p\Psi(l)\tau(l)}{l} x^l \equiv 0 \mod p. \quad \square
\]

Lemma 3.1 and Proposition 1.1 imply that \( F_r(x,y) = \lambda_r^{-1}(\lambda_r(x) + \lambda_r(y)) \in \mathbb{Z}_p[\xi][[x,y]] \) for any prime \( p \nmid m \). Since \( \lambda_r \in \mathbb{Z}_p[\xi][[x]] \) for any prime \( p \mid m \), we conclude that \( F_r \in \mathbb{Z}[\xi][[x,y]] \).

Define \( i: \mathbb{Z} \rightarrow \{\xi^i \mid i \in \mathbb{Z}\} \cup \{0\} \) as \( i(l) = 1 \) for any \( l \in \mathbb{Z} \) and put \( \kappa = \lambda_i, G = F_i \). Clearly, \( G \in \mathbb{Z}[[x,y]] \).

The formal group \( G \) will play the same role as \( F_m \) in the previous section. If \( m = 2 \), then \( \mathbb{Q}_p(\xi) = \mathbb{Q}_p \) and \( d_p = 1 \) for any odd prime \( p \). Hence, \( \Psi(l) = 1 \) for odd \( l \), \( \kappa(x) = \sum_{(l,2) = 1} x^l/l \), and \( G(x,y) = (x + y)(1 + xy)^{-1} \). This formal group could be used in the previous section instead of \( F_m \).

Let \( q \) be a prime such that \( q \equiv 1 \mod m \), \( \chi \) be a nontrivial character modulo \( q \) of order \( m \), and \( \zeta \) be a primitive \( q \)th root of unity. The following properties of the Gauss sum \( g = \sum_{n=1}^{q-1} \chi(n)^{-1}\zeta^n \) can be easily proved: \( \chi(l)g = \sum_{n=1}^{q-1} \chi(n)^{-1}\zeta^{nl} \) and \( g^m \in \mathbb{Q}(\xi) \) (see [IR] Propositions 8.2.1 and 8.3.3). Now put \( \mu = \chi, H = F_\chi \).

**Theorem 3.2.** \( [g]_{H,G} \in \mathbb{Z}[\xi,\zeta][[x]] \).

**Proof.** We have

\[
\kappa^{-1}(g\mu(x)) = \kappa^{-1}\left(\sum_{n=1}^{q-1} \chi(n)^{-1}\kappa(\zeta^n x)\right) = \sum_{n=1}^{q-1} \kappa^{-1}(\chi(n)^{-1}\kappa(\zeta^n x)).
\]

Since for any prime \( p \nmid m \), the extension \( \mathbb{Q}_p(\xi)/\mathbb{Q}_p \) is unramified, and the type of \( \kappa \) commutes with \( \xi \) in \( E \), Proposition 1.2 implies that \( [\chi(n)^{-1}]_{G,G} \in \mathbb{Z}[\xi][[x]] \), and hence, \( [g]_{H,G} \in \mathbb{Z}[\xi,\zeta][[x]] \). For any prime \( p \mid m \), we have \( \kappa \in \mathbb{Z}_p[[x]] \), and therefore \( [g]_{H,G} \in \mathbb{Z}_p[[\xi,\zeta]][[x]] \). Thus \( [g]_{H,G} \in \mathbb{Z}[\xi,\zeta][[x]] \), as required. \( \square \)

**Theorem 3.3** ([IR] Proposition 14.5.3). If \( \rho \) is a prime ideal in \( \mathbb{Q}(\xi) \) such that \( mq \notin \rho \), then \( \chi(N\rho) = (\frac{q^m}{p})_m \), where \( N \) denotes the norm of the ideal in \( \mathbb{Q}(\xi) \).
Proof. Denote \( p = \text{char } \mathbb{Z}[\xi]/\rho \). Then \( p \mid mq \), the extension \( \mathbb{Q}_p(\xi, \zeta)/\mathbb{Q}_p \) is unramified, and \( N\rho = p^{d\rho} \). According to Theorem 3.2 and Proposition 1.2 there exists \( w \in E \) such that \( w(p - \chi(p^{d\rho})\Delta_{\rho}^{d\rho}) = (p - \Delta_{\rho}^{d\rho})g \). This yields \( w = g \) and \( g\chi(p^{d\rho}) = g\Delta_{\rho}^{d\rho} \). Therefore, \( \chi(N\rho) = \chi(p^{d\rho}) = g\Delta_{\rho}^{d\rho}/g \equiv g^{p^{d\rho}-1} = (g^m)(p^{d\rho}-1)/m \equiv (g^m)_m \mod \rho \), and hence, \( \chi(N\rho) = (g^m)_m \). \( \square \)

Unlike \([IR]\), where Theorem 3.3 is proved through manipulations with Gauss sums, we deduce it directly from Theorem 3.2, showing in this way the intimate relation between reciprocity laws and certain formal group homomorphisms.

4. Cubic and biquadratic reciprocity

We keep the notation of the previous section and suppose that \( m = 3 \) or 4. In both cases \([\mathbb{Q}(\xi) : \mathbb{Q}] = 2\), and hence, there is a conjugation on \( \mathbb{Q}(\xi) \) denoted by \( \bar{\rho} \). Clearly, \( \xi = \xi^{m-1} \). Moreover, \( \mathbb{Z}[\xi] \) is a principal ideal domain, and for every \( \alpha \in \mathbb{Z}[\xi] \) we have \( N(\alpha) = \alpha\bar{\alpha} \). Finally, a prime element \( \alpha \in \mathbb{Q}(\xi) \) is called primary if \( 3 \mid \alpha - 2 \) for \( m = 3 \) and if \( (1 + \xi)^3 \mid \alpha - 1 \) for \( m = 4 \).

Let \( \varphi \) be a primary prime element in \( \mathbb{Q}(\xi) \) dividing \( q \). Since \( q \equiv 1 \mod m \), we conclude that \( N(\varphi) = q \). Further, suppose that \( \chi(n) = (\frac{n}{\varphi})_m \).

Proposition 4.1. If \( m = 3 \) or 4 and \( \rho \in \mathbb{Q}(\xi) \) is a prime element such that \( \rho \mid mq \), then \( (\frac{N(\rho)}{\varphi})_m = (\frac{\varphi}{N(\rho)})_m \).

Proof. One can show that \( g^m = \varphi\bar{\varphi}^{m-1} \) (see \([IR]\), Corollary in §9.4 and Proposition 9.9.5). Besides, it is clear that \( (\frac{a}{\rho})_m^{m-1} = (\frac{a}{\rho})_m \) for any \( a \in \mathbb{Z}[\xi] \). Then applying Theorem 3.3 we get \( (\frac{N(\rho)}{\varphi})_m = (\frac{g^m}{\varphi})_m = (\frac{\varphi\bar{\varphi}^{m-1}}{\rho})_m = (\frac{\varphi}{\rho})_m (\frac{\bar{\varphi}}{\rho})_m^{m-1} = (\frac{\varphi}{\rho})_m (\frac{\bar{\varphi}}{\rho})_m \).

From now on suppose that \( m = 3 \). In this case, we can deduce the cubic reciprocity law.

Proposition 4.2. If \( \rho \in \mathbb{Q}(\xi) \) is a primary prime element such that \( \rho \mid 3q \), then \( (\frac{\bar{\varphi}}{\rho})_3 = (\frac{\varphi}{\rho})_3 \).

Proof. If \( \rho \in \mathbb{Q} \), then \( N(\rho) = \rho^2 \), and Proposition 4.1 implies \( (\frac{\varphi}{\rho})_3 = (\frac{\bar{\varphi}}{\rho})_3 \). Therefore \( (\frac{\varphi}{\rho})_3 = (\frac{\bar{\varphi}}{\rho})_3 \). If \( \rho \notin \mathbb{Q} \), then \( N(\rho) = \rho\bar{\rho} \equiv 1 \mod 3 \) is prime in \( \mathbb{Q} \).

Since \( g^3 = \varphi\bar{\varphi}^2 \), Theorem 3.3 implies that \( (\frac{g^3}{\rho})_3 = \frac{\varphi\bar{\varphi}^2}{\rho})_3 \) and by symmetry \( (\frac{\varphi\bar{\varphi}^2}{\rho})_3 = (\frac{g^3}{\rho})_3 \). Then \( (\frac{\varphi}{\rho})_3 (\frac{\bar{\varphi}^2}{\rho})_3 = (\frac{\varphi\bar{\varphi}^2}{\rho})_3 = (\frac{g^3}{\rho})_3 = (\frac{\varphi}{\rho})_3 (\frac{\bar{\varphi}}{\rho})_3 \), and hence, \( (\frac{\varphi}{\rho})_3 = (\frac{\bar{\varphi}}{\rho})_3 \). \( \square \)

Taking into account that \( (\frac{\varphi}{\rho})_3 = 1 \) for any distinct primary \( \pi, \rho \in \mathbb{Q} \), Proposition 4.2 implies

Cubic reciprocity law. If \( \pi, \rho \in \mathbb{Q}(\xi) \) are distinct primary prime elements which do not divide 3, then \( (\frac{\varphi}{\pi})_3 = (\frac{\bar{\varphi}}{\rho})_3 \).
References


Department of Mathematics and Mechanics, Saint Petersburg State University, Universitetsky pr. 28, Stary Petergof, 198504 Saint Petersburg, Russia
E-mail address: vasja@eu.spb.ru

Einstein Institute of Mathematics, Hebrew University of Jerusalem, Givat Ram, 91904 Jerusalem, Israel
E-mail address: gurevich@math.huji.ac.il