POWER RECIPROCITY

YIHANG ZHU

1. General reciprocity for power residue symbols

1.1. **The product formula.** Let K be a number field. Suppose $K \supset \mu_m$. We will consider the m-th norm-residue symbols for the localizations K_v of K. We will omit m from the notation when convenient.

Let v be a place of K. Recall that for $a, b \in K_v^\times$, we define

$$(a,b)_{K_v} = (a,b)_v := \frac{\rho_v(a) b^{1/m}}{b^{1/m}} \in \mu_m,$$

where $\rho_v : K_v^\times \to \mathfrak{G}_{K_v}^{\mathrm{ab}}$ is the local Artin map. Recall, when $v = \mathfrak{p}$ is a non-archimedean place coprime to m, we have the following formula (tame symbol)

$$(a,b)_v \equiv \left[(-1)^{\alpha\beta}\frac{b^\alpha}{a^\beta}\right]^{(q-1)/m} \mod \mathfrak{p},$$

where $q = \mathrm{N}\,\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|, \alpha = v(a), \beta = v(b)$. ($v$ is normalized so that its image is $\mathbb{Z}$.)

In particular, if $a, b \in \mathcal{O}_v^\times$, then $(a,b)_v = 1$; if $a = \pi$ is a uniformizer in K_v and $b \in \mathcal{O}_v^\times$,

$$(\pi, b)_v \equiv b^{(q-1)/m} \mod \mathfrak{p}.$$

Suppose v is an archimedean place. If v is complex, then $(,)_v = 1$. If v is real, then by assumption $\mathbb{R} \supset \mu_m$, so $m = 2$. In this case we easily see that $(a,b)_v = \begin{cases} -1, & a < 0, b < 0 \\ 1, & \text{otherwise} \end{cases}, \forall a, b \in \mathbb{R}^\times$.

The following statement is an incarnation of Artin reciprocity.

Proposition 1.2 (Product formula)**.** *Let $a, b \in K^\times$. Then for almost all places v, we have $(a,b)_v = 1$, and we have*

$$\prod_v (a,b)_v = 1.$$

Proof. $[\prod_v (a,b)_v] b^{1/m} = [\prod_v \rho_v(a)] b^{1/m}$. But by the local global compatibility of the Artin map and the fact that the global Artin map factors throught $K^\times \backslash \mathbb{A}_K^\times$, we conclude that $\prod_v \rho_v(a) = 1 \in G_K^{\mathrm{ab}}$. □

1.3. **Calculating the norm residue symbols in the non-tame case.** In certain cases, the product formula provides a way of computing the norm-residue symbol $(,)_{K_v,m}$ when the residue characteristic of K_v divides m.

Example 1.4. $K=\mathbb{Q}, m=2$. We would like to compute $(,)_{\mathbb{Q}_2}$. We have $\mathbb{Q}_2^\times/2 \cong 2^{\mathbb{Z}/2\mathbb{Z}}\times\mathbb{Z}_2^\times/2 \cong 2^{\mathbb{Z}/2\mathbb{Z}}\times(\mathbb{Z}/8\mathbb{Z})^\times$. To know $(,)_{\mathbb{Q}_2,2}$, it suffices to compute the pairing between $2,3,5$. We have

$$(2,2)_{\mathbb{Q}_2}=\prod_{p\neq 2}(2,2)_{\mathbb{Q}_p}=1,$$
$$(2,3)_{\mathbb{Q}_2}=(2,3)_{\mathbb{Q}_3}=-1,$$
$$(2,5)_{\mathbb{Q}_2}=(2,5)_{\mathbb{Q}_5}=-1,$$
$$(3,3)_{\mathbb{Q}_2}=(3,3)_{\mathbb{Q}_3}=(3,-1)_{\mathbb{Q}_3}=-1,$$
$$(3,5)_{\mathbb{Q}_2}=(3,5)_{\mathbb{Q}_3}(3,5)_{\mathbb{Q}_5}=-1\times -1=1,$$
$$(5,5)_{\mathbb{Q}_2}=(5,5)_{\mathbb{Q}_5}=(5,-1)_{\mathbb{Q}_5}=1.$$

Example 1.5. $K=\mathbb{Q}(\zeta_3), m=3$. We would like to compute $(,)_v$ where v is the unique place over 3. This is needed for the cubic reciprocity. We partially follow the hints of an exercise in Joe Rabinoff's notes. Let $\zeta=\zeta_3, \lambda=1-\zeta$, $\eta_i=1-\lambda^i$. We have $3\mathcal{O}_K=\lambda^2\mathcal{O}_K$, and λ is a uniformizer of K_v. As usual let $U^{(i)}=1+\lambda^i\mathcal{O}_v$. Using the exponential isomorphism, we see that $U^{(2)}\xrightarrow{\sim}\lambda^2\mathcal{O}_v$, identifying $U^{(4)}\subset U^{(2)}$ with $\lambda^4\mathcal{O}_v=3\lambda^2\mathcal{O}_v\subset\lambda^2\mathcal{O}_v$. Hence $U^{(4)}\subset(K_v^\times)^3$, and $K_v^\times/3$ is a 4-dimensional $\mathbb{F}_3$ vector space, with a basis given by $\lambda,\eta_1,\eta_2,\eta_3$. We need to compute the pairings $(,)_v$ between them. Firstly, -1 is a cubic, so $(a,a)_v=(a,-a)_v=1, \forall a\in K_v^\times$. We have

$$\eta_{i+j}=\eta_j+\lambda^j\eta_i,$$
$$1=\eta_j/\eta_{i+j}+\lambda^j\eta_i/\eta_{i+j}.$$

Using $(a,a)=1$ and $(\eta_k,\lambda^k)=1$ since $\eta_k+\lambda^k=1$, we have

$$1=(\eta_j/\eta_{i+j},\lambda^j\eta_i/\eta_{i+j})=(\eta_j,\eta_i)(\eta_{i+j},\eta_j)(\eta_i,\eta_{i+j})(\lambda,\eta_{i+j})^j \tag{1}$$

Therefore if $i+j\geq 4$, we have $(\eta_i,\eta_j)=1$. So the only left case for (η_i,η_j) is $i=1,j=2$. This we can use the product formula to compute. $\eta_1=\zeta\in\mathcal{O}_K^\times$ is a unit.

$$\eta_2=1-\lambda^2=1-(1-\zeta)^2=2\zeta-\zeta^2=1+3\zeta,$$

hence

$$\mathrm{N}_{K/\mathbb{Q}}\,\eta_2=(1+3\zeta)(1+3\zeta^2)=1+3\zeta+3\zeta^2+9=1-3+9=7.$$

Namely, $w=(\eta_2)$ is a split prime over 7. Hence

$$(\eta_1,\eta_2)_v=(\eta_1,\eta_2)_w^{-1}=(\eta_2,\eta_1)_w\equiv\eta_1^{(7-1)/3}\in\mathbb{F}_7.$$

But $\eta_1^{(7-1)/3}=\zeta^2$. We conclude that $(\eta_1,\eta_2)_v=\zeta^2$. Now it remains to compute (λ,η_i). For $i=1,2$, we have $(\lambda,\eta_i)^i=(\lambda^i,\eta_i)=1$ since $\lambda^i+\eta_i=1$. So $(\lambda,\eta_i)=1, i=1,2$. To compute (λ,η_3), we set $i=2,j=1$ in formula (1), then

$$1=(\eta_1,\eta_2)(\eta_3,\eta_1)(\eta_2,\eta_3)(\lambda,\eta_3)=(\eta_1,\eta_2)(\lambda,\eta_3),\Longrightarrow(\lambda,\eta_3)=\zeta.$$

In summary, we have the following table.

	λ	η_1	η_2	η_3
λ	1	1	1	ζ
η_1	1	1	ζ^2	1
η_2	1	ζ	1	1
η_3	ζ^2	1	1	1

1.6. **The reciprocity law.**

Definition 1.7. Let $a \in K^\times$, and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Suppose a is coprime to $\mathfrak{p}$, and suppose $\mathfrak{p}$ is coprime to m. Then we define the power residue symbol to be

$$\left(\frac{a}{\mathfrak{p}}\right) := (\pi_\mathfrak{p}, a)_\mathfrak{p}$$

for any uniformizer $\pi_\mathfrak{p}$ of $\mathfrak{p}$. That this is well defined follows from the formula for tame symbols. In particular

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{(\mathrm{N}\,\mathfrak{p}-1)/m} \mod \mathfrak{p}.$$

The power residue symbol is a generalization of the Legendre symbol.

Definition 1.8. Let $a \in K^\times$. Let $\mathfrak{b} = \prod \mathfrak{p}^{e_\mathfrak{p}}$ be a fractional ideal of K. Suppose a is coprime to $\mathfrak{b}$, and suppose $\mathfrak{b}$ is coprime to m. We define the generalized Jacobi symbol to be

$$\left(\frac{a}{\mathfrak{b}}\right) := \prod_\mathfrak{p} \left(\frac{a}{\mathfrak{p}}\right)^{e_\mathfrak{p}}.$$

Here when $e_\mathfrak{p} = 0$, we understand the corresponding term as 1 by conventions. When $\mathfrak{b} = b\mathcal{O}_K$ is principal, we write $\left(\frac{a}{b}\right) := \left(\frac{a}{\mathfrak{b}}\right)$.

Remark 1.9. The generalized Jacobi symbol is evidently multiplicative in both variables in $K^\times$ and I_K.

Theorem 1.10 (Reciprocity law for generalized Jacobi symbols)**.** *Let $a, b \in K^\times$. Suppose a and b are coprime to each other. Also suppose both a and b are coprime to m. Then we have*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v|m\infty} (a,b)_v.$$

Proof.

$$\begin{aligned} LHS &= \prod_{v|b} \left(\frac{a}{v}\right)^{v(b)} \prod_{v|a} \left(\frac{b}{v}\right)^{-v(a)} = \prod_{v|b} (\pi_v, a)_v^{v(b)} \prod_{v|a} (\pi_v, b)_v^{-v(a)} \\ &= \prod_{v|b} (b,a)_v \prod_{v|a} (a,b)_v^{-1} = \prod_{v|ab} (b,a)_v = \prod_{v|m\infty} (a,b)_v. \end{aligned}$$

The last equality follows from the product formula. □

Remark 1.11. When $m \geq 3$, then the archimedean places make no contribution since they are all complex.

Remark 1.12. By the theorem, obtaining a power reciprocity law is equivalent to computing the pairings $(,)_v$ for $v|m$. We have done this in Examples 1.4 and 1.5, which will produce quadratic reciprocity and cubic reciprocity. However, in general, the explicit calculation of $(a,b)_v$ for $v|m$ is a highly nontrivial task. Complete answers to this were only obtained no earlier than 1970s. For reference see Neukirch: Algebraic Number Theory or the book Invitation to Higher Local Fields.

2. Cubic reciprocity

Using Examples 1.4,1.5, and Theorem 1.10, we can deduce quadratic and cubic reciprocity. We only work out cubic reciprocity. Thus we keep the notation in Example 1.5. Recall that (λ) is the ramified prime over 3. We write v for this place. We say $a \in K^\times$ is *primary* if $a \in \pm 1 + 3\mathcal{O}_K$. This implies $a \in K^\times/3$ is spanned by η_2 and η_3.

Theorem 2.1 (Cubic reciprocity, Gauss-Eisenstein)**.** *Let $a, b \in K^\times$ be primary. In particular they are coprime to 3. Suppose a and b are coprime to each other, then*

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right).$$

Proof. By Example 1.5, we have $(a, b)_v = 1$ for the place v above 3. □

Remark 2.2. If $a \in \mathcal{O}_K$ is coprime to λ, then $a \in a_1 + 3\mathcal{O}_K$, for $a_1 \in \{\pm 1, \pm\zeta, \pm\zeta^2\}$. In other words, $a\mathcal{O}_K = a'\mathcal{O}_K$ for some $a' \in \pm 1 + 3\mathcal{O}_K$ primary. Note that for b coprime to a, the symbol $\left(\frac{b}{a}\right)$ only depends on $a\mathcal{O}_K$, so we may always replace a by a' to calculate it.

Theorem 2.3 (Complementary laws)**.** *Let $a \in K^\times$ be primary. Write $a = \pm(1 + 3(m + n\zeta))$ with $m, n \in \mathbb{Z}$. Then*

$$\left(\frac{\zeta}{a}\right) = \zeta^{-m-n}, \left(\frac{\lambda}{a}\right) = \zeta^m.$$

Proof. Since $\left(\frac{-}{a}\right)$ by definition only depends on $a\mathcal{O}_K$, we may assume $a = 1+3(m+n\zeta)$. Since ζ is a unit,by Theorem 1.10 we have

$$\left(\frac{\zeta}{a}\right) = (\zeta, a)_v.$$

Applying the logarithm and comparing coefficients it is not hard to see $a = \eta_2^{m+n}\eta_3^m \in K_v^\times/3$. Recall $\zeta = \eta_1$, so we obtain the desired value of $\left(\frac{\zeta}{a}\right)$ from the calculation in Example 1.5. Next we use the product formula to compute

$$\left(\frac{\lambda}{a}\right) = \prod_{\mathfrak{p}|a} \left(\frac{\lambda}{\mathfrak{p}}\right)^{v_\mathfrak{p}(a)} = \prod_{\mathfrak{p}|a} (a, \lambda)_\mathfrak{p} = (a, \lambda)_v^{-1} = (\lambda, a)_v = (\lambda, \eta_2^{m+n}\eta_3^m)_v = \zeta^m.$$

□

Remark 2.4. Using the complementary law and the remark before it, we can reduce the calculation of any $\left(\frac{b}{a}\right)$ with a coprime to λ and a, b coprime to each other, to the case a, b are primary.

Example 2.5. Let $p \in \mathbb{Z}$ be a prime number not equal to 3. Let $a \in \mathbb{Z}$ be coprime to p. We ask the question of whether a is a cubic in $\mathbb{F}_p$. If $p \equiv 2 \mod 3$, then $x \mapsto x^3$ is an automorphism of $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, so the answer is always positive. We assume $p \equiv 1 \mod 3$. Then p is split in K. Write $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. We may take $\pi \in \mathcal{O}_K$ primary such that $\mathfrak{p} = \pi\mathcal{O}_K$. Noting that $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$, we see that a is a cubic in $\mathbb{F}_p$ iff

$$\left(\frac{a}{\pi}\right) = 1.$$

But the last symbol can be computed using the reciprocity laws above.

For example, we take $a = 2, p = 61$. We have $61 = (7 + 2\sqrt{-3})(7 - 2\sqrt{-3})$. The number $7 + 2\sqrt{-3}$ is not primary. We have

$$7 + 2\sqrt{-3} + \frac{1 - \sqrt{-3}}{2} = 3\frac{5 + \sqrt{-3}}{2} \equiv 0 \mod 3,$$

so $7 + 2\sqrt{-3} \equiv \frac{-1+\sqrt{-3}}{2} = \zeta \mod 3$. We take $\pi = (7 + 2\sqrt{-3})\zeta^2 = \frac{-1-9\sqrt{-3}}{2}$ to be the primary representative. Note $a = 2$ is also primary, and it is an inert prime in K. We compute

$$\left(\frac{2}{\pi}\right) = \left(\frac{\pi}{2}\right) \equiv \pi^{(2^2-1)/3} = \pi \mod 2.$$

But $\pi \equiv \frac{-1-\sqrt{-3}}{2} = \zeta^2 \mod 2$, hence $\left(\frac{2}{\pi}\right) = \zeta^2 \neq 1$. We conclude that 2 is not a cubic in $\mathbb{F}_{61}$.

Let's try $a = 7, p = 61$. Then

$$\left(\frac{7}{\pi}\right) = \left(\frac{\pi}{7}\right) = \left(\frac{\pi}{\mathfrak{q}}\right)\left(\frac{\pi}{\bar{\mathfrak{q}}}\right),$$

where $\mathfrak{q}, \bar{\mathfrak{q}}$ are the two split primes over 7. Reduced modulo $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ respectively, the two symbols are congruent to $\tilde{\pi}^{(7-1)/3} = \tilde{\pi}^2$, where $\tilde{\pi}$ is the respective reduction of π. But the two reductions of π can be computed by plugging the two square roots of -3 in $\mathbb{F}_7$, namely ± 2, into the formula $\pi = \frac{-1-9\sqrt{-3}}{2}$. We get $\tilde{\pi} = 1$ or 5, so $\tilde{\pi}^2 = 1$ or 4 in $\mathbb{F}_7$. Hence exactly one of $\left(\frac{\pi}{\mathfrak{q}}\right)$ and $\left(\frac{\pi}{\bar{\mathfrak{q}}}\right)$ is equal to 1, so $\left(\frac{7}{\pi}\right) \neq 1$, and 7 is not a cubic modulo 61.

Theorem 2.6 (Euler's conjecture)**.** *Let $p \in \mathbb{Z}$ be a prime. p is of the form $x^2 + 27y^2, x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 3$ and 2 is a cubic modulo p.*

Proof. Suppose $p = x^2 + 27y^2$. Then $p \equiv 1 \mod 3$. We prove 2 is a cubic modulo p. We have $p = (x+3y\sqrt{-3})(x-3y\sqrt{-3})$. Since $x \neq 0$, the number $\pi = x+3y\sqrt{-3}$ is primary. As in the previous example, we need only prove $\left(\frac{2}{\pi}\right) = 1$. As before, we have

$$\left(\frac{2}{\pi}\right) = \left(\frac{\pi}{2}\right) \equiv \pi \mod 2.$$

But $\pi = x - 3y + 6y\frac{1+\sqrt{-3}}{2} \equiv x - 3y \equiv x - y \mod 2$. We know x and y have unequal parity since $p = x^2 + 27y^2$ is odd. Hence $\left(\frac{2}{\pi}\right) = 1$, as desired.

Conversely, suppose $p \equiv 1 \mod 3$ and 2 is a cubic modulo p. Write $p = \pi\bar{\pi}$ with π a primary element in $\mathcal{O}_K$. The fact that 2 is a cubic modulo p means that $\left(\frac{2}{\pi}\right) = 1$. But the same computation as before implies that $\pi \in 1 + 2\mathcal{O}_K$. Let $\pi = 1 + 2(a + b\frac{1+\sqrt{-3}}{2}) = 1 + 2a + b + b\sqrt{-3}, a, b \in \mathbb{Z}$. By assumption π is primary, so $\pi = \pm 1 + 3(u + v\frac{1+\sqrt{-3}}{2}), u, v \in \mathbb{Z}$. Comparing coefficients of $\sqrt{-3}$ we see that $3v/2 = b$, so b is divisible by 3. Hence

$$p = \pi\bar{\pi} = (1 + 2a + b)^2 + 3b^2 = (1 + 2a + b)^2 + 27(b/3)^2.$$

□

Example 2.7. We have seen that 2 is not a cubic modulo 61. This can be alternatively checked by showing $61 \neq x^2 + 27y^2$ for any $x, y \in \mathbb{Z}$. We have $43 = 4^2 + 27$ is a prime, so 2 is a cubic modulo 43.