Kronecker-Jacobi symbol and Quadratic Reciprocity

Let $\mathbb{Q}$ be the field of rational numbers, and let $b \in \mathbb{Q},\ b \neq 0$. For a (positive) prime integer p, the Artin symbol

$$\left(\frac{\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}}{p}\right)$$

has the value 1 if $\mathbb{Q}(\sqrt{b}\,)$ is the splitting field of p in $\mathbb{Q}(\sqrt{b}\,)$, 0 if p is ramified in $\mathbb{Q}(\sqrt{b}\,)$, and -1 otherwise (i.e., if $\mathbb{Q}(\sqrt{b}\,) \neq \mathbb{Q}$ and p is inertial). Here we have identified the Galois group $\mathrm{Aut}\big(\mathbb{Q}(\sqrt{b}\,)\big)$ with a subgroup of the multiplicative group $\{\pm 1\}$.

For arbitrary positive rational $a = \prod_{i=1}^{m} p_i^{n_i}$, we set

$$\left(\frac{\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}}{a}\right) := \prod_{i=1}^{m} \left(\frac{\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}}{p_i}\right)^{n_i} \qquad (:= 1 \text{ if } m = 0,\ \text{i.e., } a = 1).$$

This gives rise to a homomorphism (reciprocity map) from the multiplicative group of non–zero rational numbers $a > 0$ relatively prime to the discriminant $d(b)$ of $\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}$, into the Galois group of $\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}$.

Exercise. If $\mathrm{div}(a)$ is the norm of a divisor of $\mathbb{Q}(\sqrt{b}\,)$, and $(a, d(b)) = 1$, then a lies in the kernel of the reciprocity map.

For any $0 \neq x \in \mathbb{Q}$, the *sign* of x is

$$\mathrm{sgn}(x) := x/|x| = (-1)^{\varepsilon(x)} \quad \text{where} \quad \varepsilon(x) := (\mathrm{sgn}(x) - 1)/2.$$

The number x can be written uniquely in the form

$$x = x' y^2, \quad \text{where} \quad x' = (-1)^{\varepsilon(x)} p_1 p_2 \dots p_m$$

with $m \geq 0$ distinct primes p_i.

For nonzero rational b, a, define the *Kronecker symbol*

$$\left(\frac{b}{a}\right) := (-1)^{\varepsilon(a)\varepsilon(b)} \left(\frac{\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}}{|a'|}\right)$$

One checks that:

(i) $$\left(\frac{b}{1}\right) = \left(\frac{1}{a}\right) = 1; \qquad \left(\frac{b}{-1}\right) = (-1)^{\varepsilon(b)} = \operatorname{sgn}(b).$$

(ii) $$\left(\frac{b}{a}\right) = \left(\frac{b'}{a'}\right) = \left(\frac{d(b)}{d(a)}\right). \qquad \left(\text{Recall: } d(b) = \begin{cases} b' & \text{if } b' \equiv 1 \pmod 4 \\ 4b' & \text{otherwise} \end{cases}\right)$$

(iii) $\left(\frac{b}{a}\right) \neq 0$ iff a' and $d(b)$ are relatively prime.

(iv) $\left(\frac{b}{a_1 a_2}\right) = \left(\frac{b}{a_1}\right)\left(\frac{b}{a_2}\right)$ as long as the right hand member does not vanish.

Well–known facts about behavior of primes in quadratic number fields give, further:

(v) If p is an odd prime and b is an integer then $\left(\frac{b}{p}\right)$ is just the usual Legendre symbol.

(vi) If 2 does not divide $d(b)$ (i.e., $d(b) = b' \equiv 1 \pmod 4$), then

$$\left(\frac{b}{2}\right) = (-1)^{\frac{b'-1}{4}} = (-1)^{\frac{b'^2-1}{8}} = \pm 1 \text{ according as } b' \text{ is or is not a square mod } d(2) = 8.$$

Now (iv), (v), (vi) allow us to define $\left(\frac{b}{a}\right)$ solely in terms of Legendre symbols, to wit:

$$\left(\frac{b}{a}\right) = (-1)^{\varepsilon(a)\varepsilon(b)} \prod_{\substack{p \text{ prime} \\ p | a'}} \left(\frac{d(b)}{p}\right)$$

(This is how it was done originally). From this definition, one gets at once:

(vii) $\left(\frac{b_1 b_2}{a}\right) = \left(\frac{b_1}{a}\right)\left(\frac{b_2}{a}\right)$ as long as the right hand member does not vanish.

(viii) If $a > 0$ and b_1, b_2 are integers with $b_1 \equiv b_2 \pmod{d(a)}$, then

$$\left(\frac{b_1}{a}\right) = \left(\frac{b_2}{a}\right)$$

(If a is an odd positive integer, it is even sufficient that $b_1 \equiv b_2 \pmod a$)

The heart of the reciprocity law lies in the following fact.

THEOREM. *The mapping* $a \mapsto \left(\dfrac{b}{a}\right)$ *induces a homomorphism* χ_b *from the multiplicative group* $\left(\mathbb{Z}/d(b)\mathbb{Z}\right)^*$ *of units in* $\mathbb{Z}/d(b)\mathbb{Z}$ *onto the Galois group* $\mathrm{Aut}\big(\mathbb{Q}(\sqrt{b}\,)\big)$. *This* χ_b, *called the* quadratic character of $\mathbb{Q}(\sqrt{b}\,)/\mathbb{Q}$ *when* $\mathbb{Q}(\sqrt{b}\,) \neq \mathbb{Q}$ *(i.e.,* $b' \neq 1$*), is the unique homomorphism taking any odd prime* p *not dividing* b *to the Legendre symbol* $\left(\dfrac{b'}{p}\right)$.

In other words:

$(*)$ if $a'_1 \equiv a'_2 \pmod{d(b)}$ then $\left(\dfrac{b}{a_1}\right) = \left(\dfrac{b}{a_2}\right)$.

Moreover, if $\mathbb{Q}(\sqrt{b}\,) \neq \mathbb{Q}$ then there exists a with $\left(\dfrac{b}{a}\right) = -1$.

Proof. Uniqueness is shown by replacing a by $a_{[n]} := a' + nd(b)$ where n is such that $a_{[n]}$ is positive and odd, and then factoring $a_{[n]}$ into primes. (Such an n clearly exists if a' is odd or if a' is even and relatively prime to $d(b)$—so that $d(b)$ is odd.)

It is an exercise to show that the unique quadratic number field with discriminant d (namely $\mathbb{Q}(\sqrt{d}\,)$) is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_d)$, where ζ_d is a primitive $|d|$-th root of unity. [Start with the facts that $\mathbb{Q}(\sqrt{\pm 2}\,) \subset \mathbb{Q}(\zeta_8)$ and that for an odd prime p, $\mathbb{Q}(\sqrt{p^*}\,) \subset \mathbb{Q}(\zeta_p)$.]

For any prime p, $\left(\frac{b}{p}\right)$ is the image of p under the Artin map into $\mathbb{Q}(\sqrt{b}\,)$, hence the restriction of the image of p under the Artin map into $\mathbb{Q}(\zeta_d)$ $(d := d(b))$, i.e., the automorphism taking ζ_d to ζ_d^p. Here, in view of (iv), we can replace p by any positive integer a; and furthermore, to do the same for negative a, it will suffice to do it for -1, i.e., to show that the automorphism θ taking ζ_d to ζ_d^{-1} takes $\sqrt{b}$ to $\left(\frac{b}{-1}\right)\sqrt{b} = \mathrm{sgn}(b)\sqrt{b}$. But this follows at once from the fact that the fixed field of θ is $\mathbb{Q}(\zeta_d) \cap \mathbb{R}$ whenever $|d| > 1$.

Surjectivity of χ_b results from its factorization as

$$\left(\mathbb{Z}/d(b)\mathbb{Z}\right)^* \xrightarrow{\sim} \mathrm{Aut}\big(\mathbb{Q}(\zeta_d)\big) \twoheadrightarrow \mathrm{Aut}\big(\mathbb{Q}(\sqrt{b}\,)\big).$$

Q.E.D.

COROLLARY 1. *For any odd integer* a,

$$\left(\frac{-1}{a}\right) = \mathrm{sgn}(a).(-1)^{\frac{|a|-1}{2}} = (-1)^{\frac{a-1}{2}}$$

$\big(= \pm 1$ *according as* a *is or is not a square* mod $d(-1) = -4\big)$.

Proof. Since $d(-1) = -4$, the Theorem (with $b = -1$) reduces the problem to the two simple cases $a = 1$, $a = 3$.

Corollary 2. *For any odd integer a,*

$$\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$$

$\big(= \pm 1$ *according as a is or is not a square* mod $d(2) = 8\big)$.

Proof. Since $d(2) = 8$, the Theorem (with $b = 2$) reduces the problem to the simple cases $a = 1, 3, 5, 7$.

Corollary 3. *If q is an odd prime, $q^* = (-1)^{\frac{q-1}{2}} q$, and $a \neq 0$ is an integer, then*

$$\left(\frac{q^*}{a}\right) = \left(\frac{a}{q}\right)$$

Proof. Note that $d(q^*) = q$. So for variable a with $(a, q) = 1$, $\left(\frac{q^*}{a}\right)$ and $\left(\frac{a}{q}\right)$ are both homomorphisms of the (cyclic) group of units in $\mathbb{Z}/q\mathbb{Z}$ onto a group of order 2. But there is only one such homomorphism, hence the assertion holds in this case.

Corollary 4. *Let b be any odd integer, set $b^* := (-1)^{\frac{b-1}{2}} b$ (so that $d(b^*) = b^*$), and let $a \neq 0$ be an integer. Then*

$$\left(\frac{b^*}{a}\right) = \left(\frac{a}{|b|}\right)$$

Proof. We may assume that b is square–free, and $(a, b) = 1$; and then use $b_1^* b_2^* = (b_1 b_2)^*$ and $b^* = |b|^*$ to reduce, via (iv) and (vii), to Corollary 3.

Combining these corollaries we obtain the reciprocity law for the Kronecker symbol:

If $(a, d(b)) = (b, d(a)) = 1$, then, with $a' = 2^m a_0, b' = 2^n b_0$, ($a_0$ and b_0 odd), it holds that

$$\boxed{\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a_0-1}{2}\cdot\frac{b_0-1}{2} + \varepsilon(a)\varepsilon(b)}}$$

Proof. We can replace a by a' and b by b' (see (ii)), i.e., we may assume that a and b are squarefree integers. Then at least one of a, b must be odd; we may assume b odd.

Now if $b \equiv 1 \pmod 4$ then $\frac{b_0-1}{2}$ is even, $b_0 = b = b^*$, and by Corollary 4,

$$\left(\frac{b}{a}\right) = \left(\frac{b^*}{a}\right) = \left(\frac{a}{|b|}\right) = (-1)^{\varepsilon(a)\varepsilon(b)}\left(\frac{a}{b}\right),$$

whence the assertion in this case.

If $b \equiv 3 \pmod 4$ then $b_0 = b = -b^*$, $a = a_0$ (since $1 = (a, d(b) = (a, 4b))$, and by (vii), (vi) and Corollary 4,

$$\left(\frac{b}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{b^*}{a}\right) = (-1)^{\frac{a_0-1}{2}}\left(\frac{a}{|b|}\right) = (-1)^{\frac{a_0-1}{2}\cdot\frac{b_0-1}{2}}(-1)^{\varepsilon(a)\varepsilon(b)}\left(\frac{a}{b}\right),$$

whence the assertion in this case too. Q.E.D.

Remark. The kernel of χ_b consists of all residue classes in $\mathbb{Z}/d(b)\mathbb{Z}$ of norms of ideals in the ring of integers of $\mathbb{Q}(\sqrt{b})$ which are relatively prime to $d(b)$.

Sufficiency follows from the exercise on page 1. When p is prime, and $\chi_b(p) := \left(\frac{b}{p}\right) = 1$ then p splits in $\mathbb{Q}(\sqrt{b})$, so p is a norm. Then use Dirichlet's theorem on primes in arithmetic progressions to see that for any integer a with $(a, d(b)) = 1$, there exists a prime p such that $p \equiv a \pmod{d(b)}$.

Example. 4177 is a prime number. Is 2819 a quadratic residue or non–residue?

$$\begin{aligned}(2819/4177) &= (4177/2819) = (1358/2819)\\ &= (2/2819)(679/2819) = -(679/2819)\\ &= (2819/679) = (103/679) = -(679/103)\\ &= -(61/103) = -(103/61) = -(42/61)\\ &= -(2/61)(21/61) = (61/21) = (19/21)\\ &= (21/19) = (2/19) = -1 \qquad \text{(nonresidue)}.\end{aligned}$$

Exercises.

1. Check that $\left(\frac{5}{6}\right) = 1$, and that 5 is not a square (mod 6).
2. Show that $(50009/129061) = -1$. (129061 is prime.)
3. Try to show, without using the Theorem, that for integers a, b with $0 < a < d(b)$,

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

Remarks. 1. The key to the above approach to reciprocity was the fact that any quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic field. An important theorem (Kronecker–Weber) states that *any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field*. It follows, as in the above proof, that if $K/\mathbb{Q}$ is an abelian extension, with, say $K \subseteq \mathbb{Q}(\sqrt[n]{1})$ then the splitting field of a prime p which does not ramify in K depends only on the residue class of p in $\mathbb{Z}/n\mathbb{Z}$. Similar simple decomposition laws hold for abelian extensions of arbitrary number fields; this is a basic fact of class field theory.

2. In more sophisticated treatments of reciprocity, sign complications are dealt with more elegantly in terms of behavior at the "infinite prime."