

QUADRATIC RECIPROCITY IN ABSTRACT NUMBER RINGS

ADRIAN BRUNYATE AND PETE L. CLARK

ABSTRACT. In 1872, Zolotarev gave a striking new proof of quadratic reciprocity by interpreting the Legendre symbol $\left(\frac{a}{p}\right)$ as the *sign* of the permutation $x \mapsto ax$ of $\mathbb{Z}/p\mathbb{Z}$. Here we revisit Zolotarev's construction in the context of *abstract number rings*: Dedekind domains with finite quotients. We are able to carry out two thirds of Zolotarev's proof in this general context: we can (i) identify Jacobi symbols with signs of certain permutations of residue class rings and (ii) show that $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)$ is equal to the *Zolotarev signature*, the sign of a certain permutation on $R/(ab)$. When $R = \mathbb{Z}$, Zolotarev also (iii) directly computed the Zolotarev signature; this probably has no analogue in a general abstract number ring. However, we can (and do!) compute the Zolotarev signature when $R = \mathbb{F}_q[t]$ for q an odd prime power, obtaining a new proof of the Dedekind-Artin quadratic reciprocity law.

1. ABSTRACT QUADRATIC RECIPROCITY

1.1. Abstract number rings.

An **abstract number ring** is a domain R which is a finite-quotient domain – for each nonzero ideal I of R , R/I is finite – and a Dedekind domain.

Theorem 1. *Let R be a finite-quotient domain with fraction field K , let L/K be a finite field extension, and let S be a ring with $R \subset S \subset L$. Then S is a finite-quotient domain.*

Proof. See [CL70, Thm. 4.1, Cor. 4.6] and [LM72, Thm. 2.3]. \square

Corollary 2. *Let R be a finite-quotient domain with fraction field K .*

- a) *The integral closure \tilde{R} of R in K is an abstract number ring.*
- b) *In particular, R itself is an abstract number ring iff it is integrally closed in K .*

Proof. a) By Theorem 1, \tilde{R} is a finite-quotient domain, hence Noetherian of Krull dimension at most one. Moreover it is integrally closed, so it is a Dedekind domain and thus by definition an abstract number ring. Part b) follows immediately. \square

For a nonzero ideal I in a finite-quotient domain R , we define the **norm** $|I| = \#R/I$. Also put $|(0)| = 0$. Ideals I and J of R are **coprime** if $I + J = R$.

Theorem 3. *Let R be a finite quotient domain.*

- a) *If I, J are coprime ideals of R , then $|IJ| = |I||J|$.*
- b) *If I, J are ideals of R with I invertible, then $|IJ| = |I||J|$.*
- c) *The following are equivalent:*

This note was inspired by the second author's reading of [Ba11]. Thanks also to Keith Conrad and Robert Varley for their interest and helpful comments.

- (i) R is a Dedekind domain, and thus an abstract number ring.
(ii) For all ideals I, J of R , $|IJ| = |I||J|$.

Proof. We may assume $I, J \neq 0$. a) By the Chinese Remainder Theorem (CRT),

$$|IJ| = \#(R/IJ) = \#(R/I) \cdot \#(R/J) = |I| |J|.$$

b) For a nonzero prime ideal \mathfrak{p} of R , put $|I|_{\mathfrak{p}} = \#R_{\mathfrak{p}}/IR_{\mathfrak{p}}$. We CLAIM

$$(1) \quad |I| = \prod_{\mathfrak{p} \in \text{MaxSpec } R} |I|_{\mathfrak{p}}.$$

To see this, let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be an irredundant primary decomposition of I , with $\mathfrak{p}_i = \text{rad}(\mathfrak{q}_i)$. Then $\{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ are pairwise coprime, so by CRT we have

$$R/I \cong \prod_{i=1}^n R/\mathfrak{q}_i.$$

Since R/\mathfrak{q}_i is a local ring with maximal ideal corresponding to \mathfrak{p}_i , it follows that $|\mathfrak{q}_i| = |\mathfrak{q}_i R_{\mathfrak{p}_i}|$, establishing the claim. We are thus reduced to the local case, so we may assume $I = (xR)$ is principal. Using the short exact sequence

$$0 \rightarrow \frac{xR}{xJ} \rightarrow \frac{R}{xJ} \rightarrow \frac{R}{x} \rightarrow 0$$

together with the isomorphism $R/J \xrightarrow{\cdot x} \frac{xR}{xJ}$ gives $\#R/IJ = \#R/I \cdot \#R/J$.

- c) (i) \implies (ii): Since R is a Dedekind domain, I is invertible and part b) applies.
(ii) \implies (i): See [BW66]. (We will not use this implication.) \square

1.2. The Jacobi Symbol.

A nonzero ideal I of an abstract number ring is **odd** if $|I|$ is odd. Similarly, a nonzero element $x \in R$ is odd if xR is odd.

Remark 1.1: If $2 \in R^\times$ then every nonzero ideal of R is odd. On the other hand, if R has characteristic 2 then every ideal of R is even and what follows is vacuous.

For $a \in R$ and an odd prime ideal \mathfrak{p} , we define the **Legendre symbol** $\left(\frac{a}{\mathfrak{p}}\right)$: it is 0 if $a \in \mathfrak{p}$, 1 if $a \notin \mathfrak{p}$ and $a \equiv x^2 \pmod{\mathfrak{p}}$, and -1 if $a \notin \mathfrak{p}$ and $a \not\equiv x^2 \pmod{\mathfrak{p}}$.

More generally, let \mathfrak{b} be any odd ideal of R . Since R is Dedekind, there are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i$, and of course this factorization is unique up to reordering. Moreover, because the norm map is multiplicative, each \mathfrak{p}_i is an odd prime ideal. This allows us to define, for every $a \in R$ which is relatively prime to \mathfrak{b} – i.e., such that $aR + \mathfrak{b} = R$ – the **Jacobi symbol**

$$\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a}{\prod_{i=1}^r \mathfrak{p}_i}\right) = \prod_{i=1}^r \left(\frac{a}{\mathfrak{p}_i}\right).$$

1.3. The Zolotarev Symbol.

Let \mathfrak{r} be a finite ring, and let $a \in \mathfrak{r}^\times$. Then the map $m_a : \mathfrak{r} \rightarrow \mathfrak{r}$ by $x \mapsto xa$ is a

permutation of the finite set \mathfrak{r} , so it has a well-defined **signature** $\epsilon(m_a) \in \{\pm 1\}$. In this way we define the **Zolotarev symbol**

$$\left[\frac{a}{\mathfrak{r}} \right] = \epsilon(m_a).$$

Since for $a, b \in \mathfrak{r}^\times$, $\epsilon(m_{ab}) = \epsilon(m_a m_b) = \epsilon(m_a)\epsilon(m_b)$, $\left[\frac{\cdot}{\mathfrak{r}} \right]$ gives a homomorphism from \mathfrak{r}^\times to $\{\pm 1\}$. In particular the Zolotarev symbol is trivial if $\#\mathfrak{r}^\times$ is odd.

Remark 1.2: In all cases, 0 is a fixed point of m_a , so it would be equivalent to define the Zolotarev symbol as the sign of m_a on $\mathfrak{r}^\bullet = \mathfrak{r} \setminus \{0\}$. When \mathfrak{r} is a field, we have $\mathfrak{r}^\bullet = \mathfrak{r}^\times$, so $\left[\frac{a}{\mathfrak{r}} \right]$ is equal to the sign of m_a on the unit group \mathfrak{r}^\times . For a general finite ring \mathfrak{r} , however, the sign of m_a on \mathfrak{r}^\times *need not* be equal to the sign of m_a on \mathfrak{r}^\bullet . As we will see in the proof of Theorem 6, in order to relate the Jacobi symbol $\left(\frac{a}{b} \right)$ to a Zolotarev symbol, we need to include the action of m_a on $\mathfrak{r}^\bullet \setminus \mathfrak{r}^\times$.

1.4. Sum and Product Lemmas.

Lemma 4. *Let X_1, \dots, X_r be finite sets, and let $S : \prod_{i=1}^r \text{Sym } X_i \rightarrow \text{Sym } \prod_{i=1}^r X_i$ be the natural map: $\sigma = (\sigma_1, \dots, \sigma_r) \mapsto (x_i \in X_i \mapsto \sigma_i(x_i))$. Then for all $\sigma = (\sigma_1, \dots, \sigma_r) \in \prod_{i=1}^r \text{Sym } X_i$,*

$$(2) \quad \epsilon(S(\sigma)) = \prod_{i=1}^r \epsilon(\sigma_i).$$

Proof. Since S and ϵ are homomorphisms, we have

$$\epsilon(S(\sigma)) = \epsilon(S((\sigma_1, \dots, \sigma_r))) = \epsilon(S(\sigma_1, 1, \dots, 1)) \cdots \epsilon(S(1, \dots, 1, \sigma_r)).$$

For $1 \leq i \leq r$, the cycle type of $S(1, \dots, \sigma_i, \dots, 1)$ is the same as the cycle type of σ (up to 1-cycles), so $\epsilon(S(1, \dots, \sigma_i, \dots, 1)) = \epsilon(\sigma_i)$. \square

Lemma 5. *Let X_1, \dots, X_r be nonempty finite sets, with $n_i = \#X_i$. Put $X = \prod_{i=1}^r X_i$ and $n = \prod_{i=1}^r n_i$. Let $P : \prod_{i=1}^r \text{Sym } X_i \rightarrow \text{Sym } X$ be the natural map:*

$$P : (\sigma_1, \dots, \sigma_r) \mapsto (x_1, \dots, x_r) \mapsto (\sigma_1(x_1), \dots, \sigma_r(x_r)).$$

a) *Then, for all $\sigma = (\sigma_1, \dots, \sigma_r) \in \prod_{i=1}^r \text{Sym } X_i$ we have*

$$(3) \quad \epsilon(P(\sigma)) = \prod_{i=1}^r \epsilon(\sigma_i)^{\frac{n}{n_i}}.$$

b) *In particular if each n_i is odd, then*

$$(4) \quad \epsilon(P(\sigma)) = \prod_{i=1}^r \epsilon(\sigma_i).$$

Proof. a) Since P and ϵ are homomorphisms, we have

$$\epsilon(P(\sigma)) = \epsilon(P((\sigma_1, \dots, \sigma_r))) = \epsilon(P(\sigma_1, 1, \dots, 1)) \cdots \epsilon(P(1, \dots, 1, \sigma_r)).$$

For $1 \leq i \leq r$, if the cycle type of σ_i is (a_1, \dots, a_k) , then the cycle type of $P(1, \dots, \sigma_i, \dots, 1)$ on X is $(a_1, \dots, a_1, a_2, \dots, a_2, \dots, a_k, \dots, a_k)$, each a_j occurring $\frac{n}{n_i}$ times. Thus the sign of $P(1, \dots, \sigma_i, \dots, 1)$ is $\epsilon(\sigma_i)^{\frac{n}{n_i}}$. Part b) follows. \square

1.5. Zolotarev's First Lemma.

Let R be an abstract number ring, a an element of R and \mathfrak{b} an odd ideal of R , and suppose a and \mathfrak{b} are relatively prime, so $\left(\frac{a}{\mathfrak{b}}\right) \in \{\pm 1\}$. Then (the image of) a is a unit in the finite ring $R/(\mathfrak{b})$, so the Zolotarev symbol $\left[\frac{a}{R/\mathfrak{b}}\right]$ is defined.

For a nonzero ideal \mathfrak{b} of R , put $U(\mathfrak{b}) = (R/\mathfrak{b})^\times$.

Theorem 6. (*Zolotarev's First Lemma*) *We have*

$$\left(\frac{a}{\mathfrak{b}}\right) = \left[\frac{a}{R/\mathfrak{b}}\right].$$

Proof. Write $\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, with the \mathfrak{p}_i 's *distinct* primes, so by definition

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{i=1}^r \left(\frac{a}{\mathfrak{p}_i^{e_i}}\right) = \prod_{i=1}^r \left(\frac{a}{\mathfrak{p}_i}\right)^{e_i}.$$

Step 1: The Chinese Remainder Theorem gives a canonical ring isomorphism

$$\pi : R/\mathfrak{b} \xrightarrow{\sim} \prod_{i=1}^r R/\mathfrak{p}_i^{e_i},$$

which upon passage to unit groups yields a canonical group isomorphism

$$(5) \quad \pi^\times : (R/\mathfrak{b})^\times \xrightarrow{\sim} \prod_{i=1}^r (R/\mathfrak{p}_i^{e_i})^\times.$$

We use π^\times to reduce the computation of $\left[\frac{a}{R/\mathfrak{b}}\right]$ to the computation of the sign of multiplication by $\pi^\times(a)$ on $\prod_{i=1}^r (R/\mathfrak{p}_i^{e_i})^\times$. Applying Lemma 5b), we get

$$\left[\frac{a}{R/\mathfrak{b}}\right] = \prod_{i=1}^r \left[\frac{a}{R/\mathfrak{p}_i^{e_i}}\right].$$

Step 2: We claim that for an odd prime ideal \mathfrak{p} and any a coprime to \mathfrak{p} ,

$$\left[\frac{a}{R/\mathfrak{p}}\right] = \left(\frac{a}{\mathfrak{p}}\right).$$

Both the Legendre symbol $\left(\frac{\cdot}{\mathfrak{p}}\right)$ and the Zolotarev symbol $\left[\frac{\cdot}{R/\mathfrak{p}}\right]$ give group homomorphisms from $U(\mathfrak{p})$ to $\{\pm 1\}$. Since R/\mathfrak{p} is a finite field of odd order, $U(\mathfrak{p}) = (R/\mathfrak{p})^\times$ is cyclic of even order, and thus there is exactly one nontrivial homomorphism from $U(\mathfrak{p})$ to $\{\pm 1\}$, the one that takes any fixed generator g of the group to -1 . Since $[U(\mathfrak{p}) : U(\mathfrak{p})^2] = 2$, the Legendre symbol is nontrivial. On the other hand multiplication by the generator g fixes 0 and cyclically permutes $U(\mathfrak{p})$: since $\#U(\mathfrak{p})$ is even, this permutation has sign -1 .

Step 3: Let \mathfrak{p} be an odd prime ideal of R , $a \in R$ coprime to \mathfrak{p} , and $e \in \mathbb{Z}^+$. Let $\epsilon_e(a)$ be the sign of multiplication by a on the unit group $U(\mathfrak{p}^e)$. We CLAIM

$$\epsilon_e(a) = \epsilon_1(a) = \left[\frac{a}{R/\mathfrak{p}}\right]$$

and

$$\left[\frac{a}{R/\mathfrak{p}^e}\right] = \left[\frac{a}{R/\mathfrak{p}}\right]^e.$$

We go by induction on e : $e = 1$ is trivial. Suppose $e > 1$ and the claim holds for $e - 1$. The map on units induced by $R/\mathfrak{p}^e \rightarrow R/\mathfrak{p}^{e-1}$ yields a *split* exact sequence

$$1 \rightarrow P_e \rightarrow U(\mathfrak{p}^e) \rightarrow U(\mathfrak{p}^{e-1}) \rightarrow 1$$

with P_e a finite abelian p -group. Since R is a Dedekind domain, $R_{\mathfrak{p}}$ is a DVR, with uniformizing element π , say. Then multiplication by π induces an $R_{\mathfrak{p}}$ -module isomorphism $\varphi_{\pi} : R/\mathfrak{p}^{e-1} = R_{\mathfrak{p}}/(\pi R_{\mathfrak{p}})^{e-1} \xrightarrow{\sim} \pi R_{\mathfrak{p}}/(\pi R_{\mathfrak{p}})^e = \mathfrak{p}R/\mathfrak{p}^e$. It follows that multiplication by a on R/\mathfrak{p}^{e-1} and on $\mathfrak{p}R/\mathfrak{p}^e$ are bijections conjugate under φ_{π} and therefore have the same sign. Together with Lemma 4 this gives

$$\left[\frac{a}{R/\mathfrak{p}^e} \right] = \epsilon_e(a) \cdot \left[\frac{a}{R/\mathfrak{p}^{e-1}} \right].$$

The Zolotarev symbol is trivial on the odd order group P_e . By Lemma 5,

$$\epsilon_e(a) = \epsilon_{e-1}(a)^{\#P} = \epsilon_{e-1}(a) = \epsilon_1(a) = \left[\frac{a}{R/\mathfrak{p}} \right].$$

By induction,

$$\left[\frac{a}{R/\mathfrak{p}^e} \right] = \epsilon_e(a) \left[\frac{a}{R/\mathfrak{p}^{e-1}} \right] = \left[\frac{a}{R/\mathfrak{p}} \right] \left[\frac{a}{R/\mathfrak{p}} \right]^{e-1} = \left[\frac{a}{R/\mathfrak{p}} \right]^e.$$

Step 4: Putting it all together,

$$\left[\frac{a}{R/\mathfrak{b}} \right] = \prod_{i=1}^r \left[\frac{a}{R/\mathfrak{p}_i^{e_i}} \right] = \prod_{i=1}^r \left[\frac{a}{R/\mathfrak{p}_i} \right]^{e_i} = \prod_{i=1}^r \left(\frac{a}{\mathfrak{p}_i} \right)^{e_i} = \prod_{i=1}^r \left(\frac{a}{\mathfrak{p}_i^{e_i}} \right) = \left(\frac{a}{\mathfrak{b}} \right).$$

□

1.6. Zolotarev's Second Lemma.

Let a and b be relatively prime elements in an abstract number ring R . Let

$$\pi : R/(ab) \rightarrow R/(a) \times R/(b)$$

be the Chinese Remainder Theorem isomorphism. We will define three permutations A, B, Z of $R/(ab)$. Choose coset representatives $x_0, \dots, x_{|a|-1}$ for (a) in R and $y_0, \dots, y_{|b|-1}$ for (b) in R . For any $m \in R$, there is a pair (x_i, y_j) such that

$$m \equiv bx_i + y_j \pmod{ab}.$$

Indeed, there is y_j such that $m - y_j = bz$ and x_i such that $z - x_i = az'$ and then

$$bx_i + y_j = b(z - az') + m - bz = m - abz' \equiv m \pmod{ab}.$$

The pair (x_i, y_j) is unique: if $bx_i + y_j \equiv bx_{i'} + y_{j'} \pmod{ab}$, then $b(x_i - x_{i'}) = y_{j'} - y_j + abz$, so $y_j \equiv y_{j'} \pmod{b}$ and thus $y_j = y_{j'}$; thus $a \mid b(x_i - x_{i'})$ and since a and b are coprime, $a \mid x_i - x_{i'}$ and thus $x_i = x_{i'}$.

We may therefore define permutations

$$\alpha \in \text{Sym}(R/(a) \times R/(b)), (x_i \bmod a, y_j \bmod b) \mapsto (bx_i + y_j \bmod a, y_j \bmod b)$$

and

$$\beta \in \text{Sym}(R/(a) \times R/(b)), (x_i \bmod a, y_j \bmod b) \mapsto (x_i \bmod a, x_i + ay_j \bmod b).$$

Note that α and β do depend upon our choices of coset representatives. Also put

$$A = \pi^{-1} \circ \alpha \circ \pi, B = \pi^{-1} \circ \beta \circ \pi \in \text{Sym}(R/(ab)),$$

and finally

$$Z = B \circ A^{-1} \in \text{Sym}(R/(ab)), \quad bx_i + y_j \bmod ab \mapsto x_i + ay_j \bmod ab.$$

Theorem 7. (*Zolotarev's Second Lemma*) For a, b coprime odd elements of R ,

$$\epsilon(A) = \left[\frac{b}{R/(a)} \right], \quad \epsilon(B) = \left[\frac{a}{R/(b)} \right].$$

Proof. Note that $\epsilon(A) = \epsilon(\alpha)$ and $\epsilon(B) = \epsilon(\beta)$. Now $\alpha = \alpha_2 \circ \alpha_1$, where

$$\alpha_1(x_i, y_j) = (bx_i, y_j), \quad \alpha_2(x_i, y_j) = (x_i + y_j, y_j).$$

Since $|b|$ is odd, Lemma 5 gives $\epsilon(\alpha_1) = \left[\frac{b}{R/(a)} \right]$. The permutation α_2 is the direct sum of the $|b|$ permutations $\alpha_{2,j} : (x, y_j) \mapsto (x + y_j, y_j)$ on $R/(a) \times \{y_j\}$ for $1 \leq j \leq |b|$. Each $\alpha_{2,j}$ is either trivial or an $|a|$ -cycle, so $\epsilon(\alpha_{2,j}) = 1$ for all j . By Lemma 4 we have $\epsilon(\alpha_2) = \prod_{j=1}^{|b|} \epsilon(\alpha_{2,j}) = 1$, so $\epsilon(A) = \epsilon(\alpha) = \epsilon(\alpha_1)\epsilon(\alpha_2) = \left[\frac{b}{R/(a)} \right]$. A very similar argument gives $\epsilon(B) = \epsilon(\beta) = \left[\frac{a}{R/(b)} \right]$. \square

1.7. Abstract Quadratic Reciprocity.

For coprime $a, b \in R$, we define the **Zolotarev signature**

$$z(a, b) = \epsilon(Z) \in \{\pm 1\}.$$

Theorem 8. (*Abstract Quadratic Reciprocity*) Let a and b be coprime odd elements in an abstract number ring R . Then

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

Proof. Applying Theorem 7 and then Theorem 6 gives

$$z(a, b) = \epsilon(B \circ A^{-1}) = \epsilon(A) \cdot \epsilon(B) = \left[\frac{a}{R/(b)} \right] \left[\frac{b}{R/(a)} \right] = \left(\frac{a}{b} \right) \left(\frac{b}{a} \right). \quad \square$$

Remark 1.3: By Theorem 8, the sign of the Zolotarev permutation Z does not depend on the choices of coset representatives for (a) and (b) in R . However, the cycle type of Z may depend on these choices. Take $R = \mathbb{Z}$, $a = 3$, $b = 5$. Taking $\{0, 1, 2\}$ and $\{0, 1, 2, 3, 4\}$ as coset representatives for $\mathbb{Z}/(3)$ and $\mathbb{Z}/(5)$ then we get a permutation of $\mathbb{Z}/(15)$ with three fixed points. Taking $\{0, 10, 5\}$ and $\{0, 6, 12, 3, 9\}$ as coset representatives we get a permutation with only one fixed point.

2. CLASSICAL QUADRATIC RECIPROCITY

2.1. The Quadratic Reciprocity Law of Legendre-Gauss-Jacobi.

For any positive integer c , let $[0, c-1]$ be $\{0, 1, \dots, c-1\}$ with its standard ordering. We shall use $[0, c-1]$ as a set of coset representatives for $\mathbb{Z}/(c)$. Let $a, b \in \mathbb{Z}^+$ be coprime. For all $(i, j) \in [0, a-1] \times [0, b-1]$, we have $0 \leq bi + j, i + aj \leq n-1$, so

$$Z(bi + j) = i + aj.$$

For all $i, i' \in [0, a-1]$ and all $j, j' \in [0, b-1]$, we have:

$$bi + j < bi' + j' \iff (i < i') \text{ or } (i = i' \text{ and } j < j')$$

and

$$i + aj < i' + aj' \iff (j < j') \text{ or } (j = j' \text{ and } i < i'),$$

so a pair $(m, m') = (bi + j, bi' + j') \in [0, ab - 1]^2$ is an inversion for Z if and only if

$$bi + j = m < m' = bi' + j', \quad i + aj = Z(m) > Z(m') = i' + aj' \iff i < i', \quad j' < j.$$

The number of inversions is thus $\binom{a}{2} \binom{b}{2} = \frac{a(a-1)b(b-1)}{4}$, so – since ab is odd –

$$z(a, b) = (-1)^{\frac{a(a-1)b(b-1)}{4}} \equiv (-1)^{\frac{(a-1)(b-1)}{4}} \pmod{2}.$$

This computation along with Theorem 8 yields the following classical result.

Theorem 9. (Jacobi) For coprime odd $a, b \in \mathbb{Z}^+$, we have

$$(6) \quad \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{(a-1)(b-1)}{4}}.$$

2.2. The first supplement.

Theorem 10. For any odd positive integer n , we have

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

Proof. By Theorem 6, $\left(\frac{-1}{n}\right)$ is the sign of multiplication by -1 on $\mathbb{Z}/n\mathbb{Z}$. We endow $\{0, \dots, n-1\}$ with the standard ordering and count the inversions. For each of the $\binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$ ordered pairs $1 \leq i < j \leq n-1$, $m_{-1}(i) = n-i > n-j = m_{-1}(j)$, so there are $\binom{n-1}{2}$ inversions. Since n is odd, $\binom{n-1}{2} \equiv \frac{n-1}{2} \pmod{2}$.

(Or: since n is odd, m_{-1} is the product of $\frac{n-1}{2}$ transpositions $x \mapsto -x \mapsto x$.) \square

2.3. The second supplement.

Theorem 11. For any odd positive integer n , we have

$$(7) \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Proof. By Theorem 6, $\left(\frac{2}{n}\right)$ is the sign of multiplication by 2 on $(\mathbb{Z}/n\mathbb{Z})^\bullet$. Again we count inversions using the standard ordering on $\{0, \dots, n-1\}$: for $0 < i < j \leq n-1$, if $m_2(i) > m_2(j)$ then $i \leq \frac{n-1}{2}$. There is one inversion with $i = 1$, two with $i = 2$, and so forth, up to $\frac{n-1}{2}$ with $i = \frac{n-1}{2}$, for a total of $\frac{\binom{n-1}{2}(\frac{n-1}{2}+1)}{2} = \frac{n^2-1}{8}$. \square

2.4. Comments.

In essence the above proof of quadratic reciprocity is due to Zolotarev [Zo72]. (We also acknowledge [Ba11] and [PM-Z] as more proximate influences.) However, our nomenclature is slightly misleading in that Zolotarev proved ‘‘Zolotarev’s First Lemma’’ (Theorem 6) for the Legendre symbol rather than the Jacobi symbol. It seems that the Jacobi symbol version was first given by M. Lerch.

Theorem 12. (Lerch [Le96]) Let $a, b \in \mathbb{Z}^+$ be relatively prime. Then:

- a) If b is odd, $\left[\frac{a}{\mathbb{Z}/(b)}\right] = \left(\frac{a}{b}\right)$.
- b) If $b \equiv 2 \pmod{4}$, then $\left[\frac{a}{\mathbb{Z}/(b)}\right] = 1$.
- c) If $b \equiv 0 \pmod{4}$, then $\left[\frac{a}{\mathbb{Z}/(b)}\right] = (-1)^{\frac{a-1}{2}}$.

Several authors have commented that the Zolotarev(-Lerch) approach to quadratic reciprocity – i.e., identification of the Jacobi symbol as a Zolotarev symbol – seems to be a conceptual improvement [Co97, p. 132], [Tz02] – to the extent that its omission in the standard textbook treatments of quadratic reciprocity is rather puzzling. Lerch’s contribution in particular is sufficiently poorly known so as to have been independently rediscovered several times, e.g. by M. Szyjewski [Sz10] (and also by us: we were not aware of [Le96] when this paper was first written, but only discovered it when a MathSciNet search of “Jacobi symbol” led us to [Tz02]).

3. QUADRATIC RECIPROCITY IN $\mathbb{F}_q[t]$

Let q be an odd prime power; put $R = \mathbb{F}_q[t]$. Then R is a PID, and for nonzero $a \in (\mathbb{F}_q[t])$, $|a| = \#R/(a) = q^{\deg a}$. In particular, R is an abstract number ring. But the rings \mathbb{Z} and $\mathbb{F}_q[t]$ behave similarly in many further respects: e.g. both \mathbb{Z} and $\mathbb{F}_q[t]$ have finite unit groups, and every nonzero ideal comes with a distinguished generator: in \mathbb{Z} , we may take the positive generator of any nonzero ideal, while in \mathbb{F}_q we may take the monic generator. Restricting to such generators, one gets very clean formulas for the Zolotarev signature.

In this section we will give a direct computation of the Zolotarev signature $\epsilon(a, b)$ when $a, b \in \mathbb{F}_q[t]$ are coprime monic polynomials of positive degree. Here is the key idea: when $R = \mathbb{F}_q[t]$, $R/(ab)$ has the structure of a finite-dimensional \mathbb{F}_q -vector space and – with the natural choices for coset representatives – the Zolotarev permutation Z of $R/(ab)$ turns out to be \mathbb{F}_q -linear.

3.1. The Sign of an \mathbb{F}_q -Linear Automorphism.

Lemma 13. *Let V be a finite-dimensional \mathbb{F}_q -vector space, and let $\mathrm{GL}(V)$ denote the group of all \mathbb{F}_q -linear automorphisms of V .*

- a) *Every $m \in \mathrm{GL}(V)$ is a permutation of the finite set V and thus has a sign $\epsilon(m)$.*
b) *For all $m \in \mathrm{GL}(V)$, we have*

$$\epsilon(m) = \det(m) \pmod{\mathbb{F}_q^{\times 2}}.$$

Proof. Part a) is immediate. As for b): recall that the commutator subgroup $[\mathrm{GL}(V), \mathrm{GL}(V)]$ of $\mathrm{GL}(V)$ is $\mathrm{SL}(V)$. Indeed, $\mathrm{SL}(V)$ is perfect unless $\dim V = 2$ and $q \in \{2, 3\}$ [AB, p. 59]; since $[\mathrm{GL}(V), \mathrm{GL}(V)] \subset \mathrm{SL}(V)$, this suffices. One easily computes that $[\mathrm{GL}_2(\mathbb{F}_3), \mathrm{GL}_2(\mathbb{F}_3)] = \mathrm{SL}_2(\mathbb{F}_3)$.

Thus every homomorphism from $\mathrm{GL}(V)$ to the commutative group $\{\pm 1\}$ factors through $\mathrm{GL}(V)/\mathrm{SL}(V) \xrightarrow{\sim} \mathbb{F}_q^\times$. Since \mathbb{F}_q^\times is odd order cyclic, there is a unique nontrivial homomorphism $\mathrm{GL}(V) \rightarrow \{\pm 1\}$. Let $u \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$, and let D be the diagonal matrix with entries $u, 1, \dots, 1$. By Lemma 5, $\epsilon(D) = -1$. So the sign map $\mathrm{GL}(V) \rightarrow \{\pm 1\}$ is nontrivial and thus coincides with $m \mapsto \det(m) \pmod{\mathbb{F}_q^{\times 2}}$. \square

3.2. The Quadratic Reciprocity Law of Dedekind-Artin.

Theorem 14. *For coprime odd monic polynomials $a, b \in \mathbb{F}_q[t]$, we have*

$$z(a, b) = (-1)^{\frac{(|a|-1)(|b|-1)}{4}}.$$

Equivalently, $z(a, b) = -1$ iff $q \equiv 3 \pmod{4}$ and $\deg a, \deg b$ are both odd.

Proof. Put $A = \deg a$, $B = \deg b$. Then $V_a = \mathbb{F}_q[t]/(a)$, $V_b = \mathbb{F}_q[t]/(b)$ and $V = \mathbb{F}_q[t]/(ab)$ are \mathbb{F}_q -vector spaces, of dimensions A , B and $A + B$, respectively. As

coset representatives for V we take the set of polynomials of degrees less than A , less than B and less than $A + B$, respectively. For $x, y \in V_a \times V_b$, we have

$$Z^{-1} : V \rightarrow V, \quad x + ay \mapsto bx + y.$$

Let $e_1 = 1, e_2 = t, \dots, e_{A+B} = t^{A+B-1}$, $V_1 = \langle e_1, \dots, e_A \rangle$ and $V_2 = \langle e_{A+1}, \dots, e_B \rangle$, so $V = V_1 \oplus V_2$. Morally speaking we wish to identify the vector space $V = V_1 \oplus V_2$ with the vector space $V_a \oplus V_b$; to do so we introduce the isomorphism

$$\iota : V_a \oplus V_b \xrightarrow{\sim} V_1 \oplus V_2 = V, \quad (x, y) \mapsto (x, t^a y).$$

Let

$$\mathcal{L}_1 : V_a \oplus V_b \rightarrow V, \quad (x, y) \mapsto x + ay,$$

$$L_1 = \mathcal{L}_1 \circ \iota^{-1} : V \rightarrow V,$$

$$\mathcal{L}_2 : V_a \oplus V_b \rightarrow V, \quad (x, y) \mapsto bx + y,$$

$$L_2 = \mathcal{L}_2 \circ \iota^{-1} : V \rightarrow V,$$

so

$$Z^{-1} = L_2 \circ L_1^{-1} = \mathcal{L}_2 \circ \mathcal{L}_1^{-1}.$$

Then, with respect to the basis (e_1, \dots, e_{A+B}) of V , L_1 is given by the matrix

$$M_1 = \begin{bmatrix} 1 & 0 & \dots & 0 & a_0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & a_1 & a_0 & \dots & * \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & a_{A-1} & a_{A-2} & \dots & * \\ 0 & 0 & \dots & 0 & 1 & a_{A-1} & \dots & * \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{bmatrix},$$

so is strictly upper triangular. With respect to the same basis, L_2 is given by

$$M_2 = \begin{bmatrix} b_0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ b_1 & b_0 & \dots & * & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ b_{B-1} & b_{B-2} & \dots & * & 0 & 0 & \dots & 1 \\ 1 & b_{B-1} & \dots & * & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & * & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Then, if $P : V \rightarrow V$ is the linear map which carries the basis $(e_1, \dots, e_A, e_{A+1}, \dots, e_B)$ to the basis $(e_{A+1}, \dots, e_B, e_1, \dots, e_A)$, $M_2 \circ P = M_3$ is strictly upper triangular. So $\det M_1 = \det M_3 = 1$, and thus

$$\det Z^{-1} = \det P^{-1}.$$

Now P is the matrix associated to the permutation which moves each of the A basis vectors (e_1, \dots, e_A) past all B basis vectors e_{A+1}, \dots, e_B , so it has sign $(-1)^{AB}$, and thus $\det P^{-1} = \det P = (-1)^{AB}$. Applying Lemma 13, we get

$$\epsilon(Z) = (-1)^{AB} \pmod{\mathbb{F}_q^{\times 2}}.$$

Finally, $(-1)^{AB}$ is *not* a square in \mathbb{F}_q^\times iff A, B are both odd and -1 is not a square in \mathbb{F}_q^\times , i.e., iff A and B are both odd and $q \equiv 3 \pmod{4}$. \square

Combining Theorem 14 with Abstract Quadratic Reciprocity, we recover the quadratic reciprocity law of Dedekind-Artin [De57], [Ar24].

Theorem 15. *Let q be an odd prime power, and let $R = \mathbb{F}_q[t]$, an abstract number ring. For coprime odd monic polynomials $a, b \in R$, we have $\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = 1$ unless $q \equiv 3 \pmod{4}$ and $\deg a, \deg b$ are both odd, in which case $\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = -1$. Equivalently:*

$$(8) \quad \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{(a|-1)(b|-1)}{4}}.$$

REFERENCES

- [AB] J.L. Alperin and R.B. Bell, *Groups and representations*. Graduate Texts in Mathematics, 162. Springer-Verlag, New York, 1995.
- [Ar24] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen*. Math. Zeit. 19 (1924), 153–246.
- [Ba11] M. Baker, *Zolotarev’s magical proof of the law of quadratic reciprocity*. 2011
- [BW66] H.S. Butts and L.I. Wade, *Two criteria for Dedekind domains*. Amer. Math. Monthly 73 (1966), 14–21.
- [CL70] K.L. Chew and S. Lawn, *Residually finite rings*. Canad. J. Math. 22 (1970), 92–101.
- [Co97] J.H. Conway, *The sensual (quadratic) form*. With the assistance of Francis Y. C. Fung. Carus Mathematical Monographs, 26. Mathematical Association of America, Washington, DC, 1997.
- [De57] R. Dedekind, *Abriss einer Theorie der höheren Congruenzen in Bezug auf einer reellen Primzahl-Modulus*. J. reine und Angew. Math. 54 (1857), 1–26.
- [Le96] M. Lerch, *Sur un théorème de Zolotarev*. Bull. Intern. de l’Acad. François Joseph 3 (1896), 34–37.
- [LM72] K.B. Levitz and J.L. Mott, *Rings with finite norm property*. Canad. J. Math. 24 (1972), 557–565.
- [PM-Z] Zolotarev’s Lemma, <http://planetmath.org/encyclopedia/ZolotarevsLemma.html>
- [Sz10] M. Szyjewski, *Zolotarev’s Proof of Gauss Reciprocity for Jacobi Symbol*, 2010 conference abstract available at http://z2.math.us.edu.pl/alant/pdf/abstract_55.pdf
- [Tz02] P. Tzermias, *A note on a paper by J. L. Brenner: “A new property of the Jacobi symbol”* [Duke Math. J. 29 (1962), 29–31]. Int. J. Math. Math. Sci. 31 (2002), 701–702.
- [Zo72] G. Zolotarev, *Nouvelle démonstration de la loi de de réciprocité de Legendre*. Nouvelles Annales de Mathématiques, 2e série 11 (1872), 354–362.

DEPARTMENT OF MATHEMATICS, BOYD GRADUATE STUDIES RESEARCH CENTER, UNIVERSITY OF GEORGIA, ATHENS, GA 30602-7403, USA

E-mail address: brunyate@math.uga.edu

E-mail address: pete@math.uga.edu