Ramanujan J (2015) 37:25–50
DOI 10.1007/s11139-014-9635-y

Extending the Zolotarev–Frobenius approach to quadratic reciprocity

Adrian Brunyate · Pete L. Clark

Received: 28 January 2013 / Accepted: 1 September 2014 / Published online: 11 November 2014

Abstract In 1872, Zolotarev observed that the Legendre symbol $\left(\frac{a}{p}\right)$ is the sign of the permutation of $\mathbb{Z}/p\mathbb{Z}$ induced by multiplication by a and used this to prove the quadratic reciprocity law. We pursue Zolotarev's formalism in a more general setup, which can be expressed in terms of a Dedekind domain R with finite residue fields or in terms of finite principal commutative rings. In this level of generality we define and compute *Zolotarev symbols*—by comparison to *Jacobi symbols*, when the residue rings have odd order—and arrive at *Zolotarev reciprocity*, a sort of "potential quadratic reciprocity law". To realize this potential one must compute the sign of a certain permutation. When $R = \mathbb{Z}$, this was done by Zolotarev. When $R = \mathbb{F}_q[t]$ for an odd prime power q, we compute the sign of this permutation and obtain a new proof of the quadratic reciprocity law of Dedekind and Artin.

Keywords Quadratic reciprocity · Signature · Jacobi symbol · Zolotarev permutation · Abstract number ring · Finite principal ring

Mathematics Subject Classification Primary 11A15 · 13F05 · 13F10

A. Brunyate · P. L. Clark (✉)
Department of Mathematics, Boyd Graduate Studies Research Center,
University of Georgia, Athens, GA 30602-7403, USA
e-mail: plclark@gmail.com

A. Brunyate
e-mail: brunyate@math.uga.edu

1 Introduction

Terminology: A *ring* has a multiplicative identity but need not be commutative. A *domain* is a commutative ring without nonzero zero-divisors. A *principal ring* is a ring in which every ideal is singly generated.

1.1 Zolotarev and Frobenius

For an odd (positive!) prime number p and an integer a coprime to p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is 1 if a is a square in $\mathbb{Z}/p\mathbb{Z}$ and -1 if it is not a square in $\mathbb{Z}/p\mathbb{Z}$. Recall the quadratic reciprocity law: for odd primes $\ell \neq p$, we have

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{(\ell-1)(p-1)}{4}}.$$

The first complete proof was given by Gauss; there are now hundreds of proofs. We are interested in an 1872 argument of G. Zolotarev, which proceeds in three steps:
First Zolotarev Lemma: The Legendre symbol $\left(\frac{a}{p}\right)$ is the sign of the permutation $x \mapsto ax$ of $\mathbb{Z}/p\mathbb{Z}$.

Second Zolotarev Lemma: For $\ell \neq p$ odd primes, there are permutations A and B on $\mathbb{Z}/\ell p\mathbb{Z}$ with respective signs $\left(\frac{p}{\ell}\right)$ and $\left(\frac{\ell}{p}\right)$.

Quadratic reciprocity: Therefore $\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right)$ is equal to the sign of the permutation $Z = B \circ A^{-1}$. This "Zolotarev permutation" Z has a down-to-earth combinatorial description—e.g. [4] elegantly describes Z in terms of dealing cards into a rectangular array in rows and picking them up in columns—and a short, elementary argument shows that its sign is $(-1)^{\frac{(\ell-1)(p-1)}{4}}$.

If a and b are coprime positive integers, b is odd and has prime power factorization $b = \prod_{i=1}^{n} p_i^{e_i}$, the *Jacobi symbol* $\left(\frac{a}{b}\right)$ is $\prod_{i=1}^{n}\left(\frac{a}{p_i}\right)^{e_i}$. Jacobi used his symbol to extend quadratic reciprocity: for odd coprime $a, b \in \mathbb{Z}^+$, we have

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

Frobenius extended the First Zolotarev Lemma [18] as follows.

Zolotarev–Frobenius Lemma: For odd coprime $a, b \in \mathbb{Z}^+$, the Jacobi symbol $\left(\frac{a}{b}\right)$ is the sign of the permutation $x \mapsto ax$ on $\mathbb{Z}/b\mathbb{Z}$. The rest of Zolotarev's argument extends verbatim, proving Jacobian quadratic reciprocity.

1.2 Zolotarev reciprocity in abstract number rings

We find the Zolotarev–Frobenius approach to quadratic reciprocity beautiful and intriguing. (We are not alone: Conway has remarked [11, p. 132] that the Zolotarev–Frobenius interpretation of the Jacobi symbol seems to be a conceptual improvement over the standard definition.) Strangely, it has received only scattered attention in the literature. We were motivated to gain a deeper algebraic understanding of the Zolotarev–Frobenius approach, with the goal of carrying out a "Zolotarev-style proof of quadratic reciprocity" in a ring other than $\mathbb{Z}$.

The last—vague—sentence is a faithful description of our original intent. With the benefit of hindsight we can give a more precise description: let a and b be elements of a domain R such that $\langle a \rangle$ and $\langle b \rangle$ factor into products of prime ideals, $\langle a, b \rangle = R$ and $R/(a)$, $R/(b)$ are finite of odd order. Then, as we will see in Sect. 3.1, one can define the Jacobi symbol $\left(\frac{a}{b}\right)$ in this context, and a *Jacobian Quadratic Reciprocity Law* is a characterization of when $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ holds.

In Sect. 3 we give a Zolotarev-style approach to Jacobian quadratic reciprocity laws. For a finite ring $\mathfrak{r}$ and $a \in \mathfrak{r}^\times$, we can define a *Zolotarev symbol* $\left[\frac{a}{\mathfrak{r}}\right]$ as the sign of the permutation $x \mapsto ax$ on $\mathfrak{r}$. When $\mathfrak{r}$ is an odd order finite field, $\left[\frac{a}{\mathfrak{r}}\right] = 1$ iff a is a square in $\mathfrak{r}$: this is essentially Zolotarev's First Lemma. Consider next $\mathfrak{r} = \mathbb{Z}/n\mathbb{Z}$. When n is odd, Frobenius's result is equivalent to the identity $\left[\frac{a}{n}\right] = \left(\frac{a}{n}\right)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. A result of Lerch [27] gives an evaluation of $\left[\frac{a}{n}\right]$ when n is even.

Our Theorem 3.6 evaluates Zolotarev symbols $\left[\frac{a}{\mathfrak{r}}\right]$ in any finite commutative principal ring $\mathfrak{r}$. When $\#\mathfrak{r}$ is odd, the evaluation is again in terms of the Jacobi symbol $\left(\frac{a}{\mathfrak{r}}\right)$, which can be defined in any such ring.

The two instances of Jacobi symbols described above reflect an important equivalence. It is a well-known exercise that if R is a domain in which ideals factor uniquely into primes (i.e., a Dedekind domain), for every nonzero ideal I of R, the quotient R/I is a principal ring. Less widely known is the converse (Theorem 2.9). Thus a domain R is a Dedekind domain such that $R/(a)$ is finite for every nonzero $a \in R$ iff for every nonzero ideal I of R, R/I is a finite principal ring. We call such rings *abstract number rings*, and it is this class of rings in which we pursue Zolotarev's approach to quadratic reciprocity.

Indeed, we have already mentioned generalizations of Zolotarev's First Lemma and its extensions by Frobenius and Lerch to finite principal rings, and there is an immediately equivalent formulation in terms of abstract number rings. Using the equality of Zolotarev and Jacobi symbols for odd ideals in an abstract number ring, we establish our version of Zolotarev's Second Lemma: $\left(\frac{b}{a}\right)$ and $\left(\frac{a}{b}\right)$ are realized as the signs of permutations A and B on $R/(ab)$. Then we define the *Zolotarev permutation* $Z = B \circ A^{-1}$, given by a certain explicit formula on coset representatives. We deduce *Zolotarev reciprocity*:

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

1.3 Two applications

Zolotarev reciprocity does give a characterization of when $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$—but a rather complicated one, whose usefulness remains to be seen. Our perspective is to view Zolotarev reciprocity as a "potential quadratic reciprocity law". In fact it presents us with a large class of intriguing challenges: namely to give an "explicit" evaluation of $\epsilon(Z)$ and thereby deduce a Jacobian quadratic reciprocity law.

In the second part of this paper we present two instances in which this potential can be realized: namely, we give a direct, self-contained evaluation of $\epsilon(Z)$ and thus deduce a Jacobian quadratic reciprocity law in R. In Sect. 4 we treat the classical case $R = \mathbb{Z}$. This really is Zolotarev's classical argument, but we give it here so as to record a complete Zolotarev-style proof of *Jacobian* quadratic reciprocity. In Sect. 5 we treat the case $R = \mathbb{F}_q[t]$ for an odd order finite field R, recovering the quadratic law of Dedekind–Artin. Here are two key ideas in the proof: first, with a natural choice of coset representatives Z is an $\mathbb{F}_q$-linear map, so linear algebra can be used. Second, if V is a finite-dimensional vector space over $\mathbb{F}_q$ and $g \in \mathrm{GL}\, V$ is a linear map, then g induces a permutation of V and its sign is 1 iff $\det g \in \mathbb{F}_q^{\times 2}$.

1.4 Zolotarev symbols in matrix rings

Our evaluation of Z in the $R = \mathbb{F}_q[t]$ case suggests the feasibility of evaluating Zolotarev symbols in certain noncommutative rings. In Sect. 6 we compute all Zolotarev symbols in the ring of $n \times n$ matrices over any finite principal commutative ring $\mathfrak{r}$. When $\mathfrak{r} = \mathbb{Z}/n\mathbb{Z}$ we recover a result of Lehmer (Theorem 7.3).

1.5 Further contents of the paper

We have another goal beyond proofs of the results mentioned above. The literature concerning number-theoretic aspects of signatures of group actions is scattered to a remarkable degree: republication of results which are more than a century old is common. We wish to provide a firm foundation for future work as well as a clear picture of what has already been done. To this end, Sect. 2 of the paper is foundational: in Sect. 2.1 we treat general aspects of signatures of group actions on finite sets, arriving in particular at Theorem 2.4, which gives necessary and sufficient conditions for the Cayley representation of a finite group to have nontrivial signature. In Sect. 2.2 we establish the equivalence between abstract number rings and finite principal commutative rings. In particular we record the result that any finite principal commutative ring is a quotient of the ring of integers of some number field. Sect. 7 is a guide to the history and literature on Zolotarev-style reciprocity.

Our literature search was performed after most of the main results of the paper were obtained, in some form. We then found some duplication of past work. In response we have not hesitated to take this prior work into account. In many cases this spurred us towards more general results. Our work recovers many previously published results as special cases including work of Dressler and Shult [17], Frobenius [18], Lerch [27], Lehmer [26], Morton [29], Nečaev [30], Riesz [31], Schur [34], Slavutskiĭ [36],

Szyjewski [37] (and of course Zolotarev [38]). In fact, we recover all previous results on Zolotarev's approach to quadratic reciprocity. . .provided this taken in the sense made precise in this introduction, which is relatively broad but hardly all-encompassing. Other interesting takes on "Zolotarev's approach to quadratic reciprocity" have been given by Cartier [8], Duke and Hopkins [16] and Hablicsek and Mantilla-Soler [20]. These are discussed briefly in Sect. 7. A Zolotarev-style approach to two-powered higher rational reciprocity laws has recently been given by Budden et al. [6].

The prospect of using Zolotarev reciprocity to deduce new quadratic reciprocity laws in abstract number rings seems intriguing but difficult: to the best of our knowledge, the question of in which abstract number rings one can hope for a satisactory Jacobian quadratic reciprocity law is wide open. We hope that this paper will serve to arouse more interest and work in this area.

2 Algebraic preliminaries

2.1 The signature homomorphism associated to a finite G-set

Let G be a group which acts on a finite set X via $\bullet : G \times X \to X, (g, x) \mapsto g \bullet x$. The action can be expressed as a group homomorphism $\rho : G \to \operatorname{Sym} X,\ g \mapsto g\bullet$ from G into the group of bijections on X. Let $(X', \bullet')$ be anther G-set. An isomorphism of G-sets is a bijection $f : X \to X'$ such that $g \bullet' f(x) = f(g \bullet x)$ for all $g \in G,\ x \in X$. Such a bijection f induces a group homomorphism $\operatorname{Sym} f : \operatorname{Sym} X \to \operatorname{Sym} X',\ \iota \mapsto \alpha \circ \iota \circ \alpha^{-1}$, such that $\rho' = \operatorname{Sym} f \circ \rho$.

Let $n \geq 2$. Recall: every $\sigma \in S_n$ has a *signature* $\epsilon(\sigma) \in \{\pm 1\}$, and $\epsilon : S_n \to \{\pm 1\}$ is a nontrivial group homomorphism. For $n = 0, 1$ the groups $S_0 = \operatorname{Sym} \varnothing$ and S_1 are trivial, and we define $\epsilon : S_n \to \{\pm 1\}$ to be the unique homomorphism.

For $n \geq 2$, the signature is the only nontrivial homomorphism $\varphi : S_n \to \{\pm 1\}$: since all 2-cycles are conjugate in S_n and S_n is generated by the 2-cycles, for every 2-cycle τ we must have $\varphi(\tau) = -1$, and this determines φ. So if $\alpha \in \operatorname{Aut} S_n$, then $\epsilon \circ \alpha = \epsilon$. Thus for any set X of cardinality n there is a signature homomorphism $\epsilon_X : \operatorname{Sym} X \to \{\pm 1\}$: choose $F : \operatorname{Sym} X \xrightarrow{\sim} S_n$ and put $\epsilon_X = \epsilon \circ F$: this does not depend on the choice of F. Finally, when X is a G-set, we put

$$\epsilon_X = \epsilon \circ F \circ \rho : G \to \{\pm 1\}.$$

Lemma 2.1 *Let G be a group and (X, ρ) a finite G-set.*

(a) *If X' is a G-set which is isomorphic to X, then for all $g \in G$, $\rho_X(g)$ and $\rho_{X'}(g)$ have the same cycle type, hence also $\epsilon_X = \epsilon_{X'}$.*
(b) *Let G' be a group and (X', ρ') a G'-set. Suppose there is a group isomorphism $\alpha : G \to G'$ and a bijection $f : X \to X'$ which are compatible in the sense that $\operatorname{Sym} f \circ \rho = \rho' \circ \alpha$. Then for all $g \in G$, $\rho_X(g)$ and $\rho_{X'}(\alpha(g))$ have the same cycle type, hence also $\epsilon_X(g) = \epsilon_{X'}(\alpha(g))$.*
(c) *Let G' be a group and $\alpha : G' \to G$ a group isomorphism. We can endow X with the structure of a G'-set via $\rho \circ \alpha$. Then for all $g' \in G'$, $\epsilon_X(g') = \epsilon_X(\alpha(g'))$.*

Proof (a) If $f : X \to X'$ be an isomorphism of G-sets, then $\operatorname{Sym} f : \operatorname{Sym} X \to \operatorname{Sym} X'$ preserves cycle types, and the result follows immediately.
(b) Again the result follows from the fact that $\operatorname{Sym} f$ preserves cycle types.
(c) Composing a map with an isomorphism does not change its kernel, and signature maps are determined by their kernels. □

The proofs of the following two results are routine, and we omit them.

Lemma 2.2 (Sum Lemma) *Let $X_1, \ldots, X_r$ be finite sets, and let $S : \prod_{i=1}^r \operatorname{Sym} X_i \to \operatorname{Sym} \coprod_{i=1}^r X_i$ be the natural map:*

$$\sigma = (\sigma_1, \ldots, \sigma_r) \mapsto (x_i \in X_i \mapsto \sigma_i(x_i)) .$$

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

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

Lemma 2.3 (Product Lemma) *Let $X_1, \ldots, X_r$ 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 $P : \prod_{i=1}^r \operatorname{Sym} X_i \to \operatorname{Sym} X$ be the natural map:*

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

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

$$\epsilon(P(\sigma)) = \prod_{i=1}^{r} \epsilon(\sigma_i)^{\frac{n}{n_i}} . \tag{2}$$

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

$$\epsilon(P(\sigma)) = \prod_{i=1}^{r} \epsilon(\sigma_i). \tag{3}$$

Let G be a finite group. For $a \in \mathbb{Z}^+$ with $\gcd(a, \#G) = 1$, the map $g \mapsto g^a$ is a bijection on G, so $g^{\frac{1}{a}}$ is well-defined. It follows that $g^{\frac{\#G}{2}}$ is always well-defined.

Let G be a finite group acting on itself on the left: $\rho_G : G \to \operatorname{Sym} G,\ g \mapsto g\bullet$. The associated *Cayley signature* ϵ_G is easily understood.

Theorem 2.4 *Let G be a finite group and let $g \in G$. Put $N = \#G$ and $a = \#\langle g \rangle$.*

(a) *If $g \in G$ has order a, then $\rho_G(g)$ is a union of $\frac{\#G}{a}$ a-cycles.*
(b) *The following are equivalent:*
  (i) $\epsilon_G(g) \neq 1$.
  (ii) *a is even and $\frac{N}{a}$ is odd.*
  (iii) *(Euler Criterion) $g^{\frac{N}{2}} \neq 1$.*

(c) *(Morton* [29]*) The following are equivalent:*
  (i) *The signature map ϵ_G is nontrivial.*
  (ii) *The 2-Sylow subgroups of G are cyclic and nontrivial.*
(d) *If ϵ_G is nontrivial, its kernel K is the unique index 2 subgroup of G.*

Proof (a) The cycles of $\epsilon_G(g)$ are the right cosets of $\langle g \rangle$ in G.

(b) By (a), $\epsilon_G(g) = (-1)^{(a-1)\frac{N}{a}}$, so (i) $\iff$ (ii). If a is odd, then $g^{\frac{N}{2}}$ has odd order and order dividing 2, so $g^{\frac{N}{2}} = 1$. Now assume that a, and hence N, is even. Then the order of $g^{\frac{N}{2}} = \frac{a}{\gcd a, \frac{N}{2}}$. Thus $g^{\frac{N}{2}} = 1$ iff $\gcd\left(a, \frac{N}{2}\right) = a$ iff $a \mid \frac{N}{2}$ iff $\frac{N}{a}$ is even.

(c) By part (a), ϵ_G is nontrivial iff there is $g \in G$ such that $\langle g \rangle$ has even order and odd index. If so, $\langle g \rangle$ is a cyclic, nontrivial 2-Sylow subgroup. Conversely, a generator g of a nontrivial cyclic 2-Sylow subgroup has even order and odd index.

(d) If ϵ_G is nontrivial, then $K = \operatorname{Ker} \epsilon$ is an index 2 subgroup of G, so it's enough to show that G has exactly one index 2 subgroup. By part (b) G has a cyclic 2-Sylow subgroup P. It is a theorem of Cayley (!) that there is a normal subgroup N of G such that $G = N \rtimes P$: see e.g. [12, Cor. 1.14]. On the other hand, let O be the subgroup of G generated by all odd order elements; then O is normal, G/O is a 2-group, and O is minimal with these properties. It follows that $N = O$. If H is an index 2 subgroup, it is normal and G/H is a 2-group, so $H \supset N$. Since $G/N \cong P$ is even order cylic, there is precisely one index 2 subgroup of G containing N. □

Remark 2.5 The converse of Theorem 2.4(d) does not hold. First, S_n has a unique index 2 subgroup for all $n \geq 2$. The dihedral group D_4 is a Sylow 2-subgroup of S_4, and it follows that for all $n \geq 4$, the Sylow 2-subgroups of S_n are noncommutative. Moreover, in Sect. 5 we will recall—and crucially use—that for any finite-dimensional vector space V over an odd order finite field, $\mathrm{GL}\, V$ has a unique index 2 subgroup. However, when $\dim V \geq 2$ the Sylow 2-subgroups of $\mathrm{GL}\, V$ are noncyclic.

Lemma 2.6 *Let H be a normal subgroup of G; put $G' = G/H$ and $q : G \to G'$.*

(a) *If ϵ_G and $\epsilon_{G'}$ are both trivial or both nontrivial, then*

$$\epsilon_G = \epsilon_{G'} \circ q. \tag{4}$$

(b) *If H has odd order, then* (4) *holds.*

Proof (a) Certainly (4) holds if ϵ_G and $\epsilon_{G'}$ are both trivial, so suppose both are nontrivial. Then $\operatorname{Ker} \epsilon_{G'} \circ q$ is an index 2 subgroup of G. By Theorem 2.4(c), if ϵ_G is nontrivial there is a unique index 2 subgroup, so $\operatorname{Ker} \epsilon_{G'} \circ q = \operatorname{Ker} \epsilon_G$, and two homomorphisms into $\{\pm 1\}$ are equal iff their kernels are equal.

(b) Let P be a Sylow 2-subgroup of G. Then PH/H is a 2-Sylow subgroup of G'. Since $\#H$ is odd and P is a 2-group, $PH/H \cong P/(P \cap H) = P$. Thus by Theorem 2.4(b), ϵ_G is nontrivial iff $\epsilon_{G'}$ is nontrivial, so part (a) applies. □

Theorem 2.7 (Tower Theorem) *Let $e \in \mathbb{Z}^+$. For $1 \leq i \leq e$, let G_i be a finite group and let P_i be a Sylow 2-subgroup of G_i. For $2 \leq i \leq e$, let $q_i : G_i \to G_{i-1}$ be a surjective homomorphism. For $1 \leq i \leq e$, let $\epsilon_i = \epsilon_{G_i} \circ q_{i+1} \circ \cdots \circ q_e$, and let $E = \prod_{i=1}^{e} \epsilon_i : G \to \{\pm 1\}$.*

(a) *If for no* $1 \leq i \leq e$ *is* P_i *nontrivial cyclic, then* E *is trivial.*
(b) *Otherwise let* ℓ *and* u *be the least and greatest indices* i *such that* P_i *is nontrivial cyclic. Then* $E = \epsilon_a^{u-\ell+1}$.

Proof (a) If no P_i is nontrivial cyclic then ϵ_{G_i} is trivial for all i, so E is trivial. (b) By Theorem 2.4(b), ϵ_{G_i} and thus ϵ_i is trivial unless $\ell \leq i \leq u$. Since for all $1 \leq i \leq e$, $d_i(P_i) \cong P_{i-1}$, as i ranges from 1 to e, we find: if $i < \ell$, P_i is trivial; if $\ell \leq i \leq u$, P_i is nontrivial cyclic; and if $u < i \leq e$ then P_i is not cyclic. Thus $E = \prod_{i=\ell}^{u} \epsilon_i$, and by Lemma 2.6(a) $\epsilon_\ell = \epsilon_{\ell+1} = \ldots = \epsilon_u$, so $E = \epsilon_\ell^{u-\ell+1}$. □

2.2 Abstract number rings and finite principal rings

Proposition 2.8 *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be nonzero ideals in the Dedekind domain* R.

(a) *The* R*-modules* $R/\mathfrak{a}$ *and* $\mathfrak{b}/\mathfrak{ab}$ *are isomorphic.*
(b) $\#R/\mathfrak{ab} = \#R/\mathfrak{a} \cdot \#R/\mathfrak{b}$.

Proof (a) See e.g. [13, Thm. 18.24].
(b) We have a short exact sequence

$$0 \to \mathfrak{a}/\mathfrak{ab} \to R/\mathfrak{ab} \to R/\mathfrak{a} \to 0.$$

Using this and part (a) we get

$$\#R/\mathfrak{ab} = \#\mathfrak{a}/\mathfrak{ab}\#R/\mathfrak{a} = \#R/\mathfrak{a}\#R/\mathfrak{b}.$$

□

Theorem 2.9 (Asano, Jensen) *For a domain* R*, the following are equivalent:*

(i) R *is a Dedekind domain.*
(ii) *If* $\mathfrak{b}$ *is an ideal of* R *and* $0 \neq a \in \mathfrak{b}$*, then there is* $b \in \mathfrak{b}$ *such that* $\mathfrak{b} = \langle a, b \rangle$.
(iii) *For every nonzero ideal* $\mathfrak{b}$ *of* R*, the quotient* $R/\mathfrak{b}$ *is a principal ring.*

Proof See [3,25] or [9, Thm. 20.11].[1] □

A *residually finite ring* is a ring in which the quotient by every nonzero ideal is finite. For a nonzero ideal I in a residually finite ring R, we put $|I| = \#R/I$.

Theorem 2.10 *For a residually finite domain* R*, the following are equivalent:*

(i) R *is a Dedekind domain.*
(ii) *For all nonzero ideals* I, J *of* R, $|IJ| = |I||J|$.

Proof (i) $\implies$ (ii) by Proposition 2.8(b) above.
(ii) $\implies$ (i): This is a result of Butts and Wade [7, Thm. 2]. □

[1] In [24, p. 630] Jacobson attributes this result to H. Sah. It seems that this refers to Chih-Han Sah (1934–1997), but we have not been able to trace the result back to him.

An *abstract number ring* is a residually finite Dedekind domain. Examples:

- The ring of integers $\mathbb{Z}_K$ of a number field K.
- The coordinate ring $\mathbb{F}_q[C^\circ]$ of a nonsingular integral affine curve $C^\circ/\mathbb{F}_q$.
- Any localization or completion of either of the above.

(There are also more exotic examples: Goldman constructed abstract number rings with unit group ± 1 and nontorsion ideal class group [19, Cor. (1) and (2)].)

Let $\mathfrak{r}$ be a finite commutative ring. Then $\mathfrak{r}$ has finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, and each $\mathfrak{p}_i$ is maximal. Thus $\bigcap_{i=1}^r \mathfrak{p}_i = \prod_{i=1}^r \mathfrak{p}_i$ is the nilradical of $\mathfrak{r}$; since $\mathfrak{r}$ is finite, this is a nilpotent ideal: there is $E \in \mathbb{Z}^+$ such that $\prod_{i=1}^r \mathfrak{p}_i^E = 0$. For $1 \leq i \leq r$, let $e_i \in \mathbb{Z}^+$ be minimal such that $\mathfrak{p}_i^a = \mathfrak{p}_i^b$ for all $a, b \geq e_i$. Then

$$(0) = \bigcap_{i=1}^r \mathfrak{p}_i^{e_i} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}.$$

The Chinese Remainder Theorem gives a canonical isomorphism

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

say. Each $\mathfrak{r}_i$ is Artinian local with maximal ideal $\mathfrak{p}_i/\mathfrak{p}_i^{e_i}$.

Lemma 2.11 *Let $\mathfrak{r}$ be a finite local commutative ring with maximal ideal $\mathfrak{p}$. Let e be the least positive integer such that $\mathfrak{p}^e = (0)$. The following are equivalent:*

(i) *$\mathfrak{r}$ is a principal ring: every ideal of $\mathfrak{r}$ is principal.*
(ii) *$\mathfrak{p}$ is principal.*
(iii) *The length of $\mathfrak{r}$ as an $\mathfrak{r}$-module is e.*
(iv) *Every ideal of $\mathfrak{r}$ is of the form $\mathfrak{p}^i$ for a unique $0 \leq i \leq e$.*
(v) *$\mathfrak{r}$ is a chain ring: the ideals of $\mathfrak{r}$ are linearly ordered under inclusion.*

Proof (i) $\implies$ (ii) is immediate.

(ii) $\implies$ (iii): Suppose $\mathfrak{p} = (\pi)$. Every $x \in \mathfrak{r}$ may be written as $\pi^i u$ for a unique $0 \leq i \leq e$ and $u \in \mathfrak{r}^\times$. It follows that for every ideal $\mathfrak{b}$ of $\mathfrak{r}$, if i is the least natural number such that $\pi^i \in \mathfrak{b}$, then $\mathfrak{b} = (\pi^i) = \mathfrak{p}^i$.

(iii) $\implies$ (iv): Let $\mathfrak{b}$ be an ideal of $\mathfrak{r}$, and let i be the largest natural number such that $\mathfrak{b} \subset \mathfrak{p}^i$. If $\mathfrak{p}^{i+1} + \mathfrak{b} \subsetneq \mathfrak{p}^i$ then

$$0 = \mathfrak{p}^e \subset \mathfrak{p}^{e-1} \subset \cdots \subset \mathfrak{p}^{i+1} \subset \mathfrak{p}^{i+1} + \mathfrak{b} \subset \mathfrak{p}^i \subset \cdots \subset \mathfrak{p} \subset \mathfrak{r}$$

is a chain of ideals in $\mathfrak{r}$ of length at least $e + 1$, contradiction. So $\mathfrak{p}^{i+1} + \mathfrak{b} = \mathfrak{p}^i$, and then applying Nakayama's Lemma to the module $\mathfrak{p}^i$ we get $\mathfrak{b} = \mathfrak{p}^i$.

(iv) $\implies$ (v) is immediate.

(v) $\implies$ (i): Since $\mathfrak{r}$ is finite, among all ideals properly contained in $\mathfrak{p}$ there is a unique largest ideal, say $\mathfrak{b}$. Then any element of $\mathfrak{p} \backslash \mathfrak{b}$ must generate $\mathfrak{p}$. □

Theorem 2.12 *For a commutative ring $\mathfrak{r}$, the following are equivalent:*

(i) *There is a number field K and a nonzero ideal I in $\mathbb{Z}_K$ with $\mathbb{Z}_K/I \cong \mathfrak{r}$.*
(ii) *There is a nonzero ideal I in an abstract number ring R with $R/I \cong \mathfrak{r}$.*
(iii) *$\mathfrak{r}$ is a finite principal ring.*

Proof (i) $\implies$ (ii) is clear. (ii) $\implies$ (iii) follows from Theorem 2.9.

(iii) $\implies$ (i): Step 1: Suppose $\mathfrak{r}$ is local. Then by [23, Thm. 1] there is a Dedekind domain R and an ideal I such that $R/I \cong \mathfrak{r}$. By CRT I must be a prime power $\mathfrak{p}^e$. Let $R_\mathfrak{p}$ be the completion at $\mathfrak{p}$; then $\mathfrak{r} \cong R/I \cong \mathbb{R}_\mathfrak{p}/(\mathfrak{p}R_\mathfrak{p})^e$, so—replacing R by $R_\mathfrak{p}$—we may assume that R is a complete discrete valuation ring. The residue field $R/\mathfrak{p}$ is finite, so isomorphic to $\mathbb{F}_q$, with $q = p^f$, say. By the Cohen structure theory [35, Ch. II] R is isomorphic either to the ring of integers in a p-adic field or to the formal power series ring $\mathbb{F}_q[[t]]$. In the former case we're done: R is the completion of some prime ideal in some number field, so it suffices to treat the latter case, in which $\mathfrak{r} \cong \mathbb{F}_q[t]/(t^e)$. Let K be any p-adic field with residue field $\mathbb{F}_q$ and ramificaiton index at least e, for instance $\mathbb{Q}_p(\zeta_{q-1}, p^{\frac{1}{e}})$, let R_K be the ring of integers of K and $\mathfrak{p}_K$ its maximal ideal. Then $R_K/\mathfrak{p}_K^e \cong \mathbb{F}_q[t]/(t^e)$. Then $p \in \mathfrak{p}_K^e$ so $R_K/\mathfrak{p}_K^e$ has characteristic p and thus the Teichmüller lift $\mathbb{F}_q \to R_K/\mathfrak{p}_K^e$ is an isomorphism [35, Prop. II.8]. Let π_K be a generator of $\mathfrak{p}_K$. There is then a unique $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q[t] \to R_K$ which maps t to π_K, and passing to the quotient gives a homomorphism $\Phi : \mathbb{F}_q[t]/(t^e) \to R_K/\mathfrak{p}_K^e$ which is injective since it kills no power of t smaller than t^e. By Theorem 2.10(b) both source and target are finite rings of order q^e, so Φ is an isomorphism.

Step 2: Let $\mathfrak{r} = \prod_{i=1}^r \mathfrak{r}_i$ be the decomposition into local rings; let e_i be the length of $\mathfrak{r}_i$. Since $\mathfrak{r}$ is principal, so is each $\mathfrak{r}_i$, so by Step 1 for each $1 \le i \le r$ there is a p_i-adic field K_i with integer ring R_{K_i} and maximal ideal $\mathfrak{p}_{K_i}$ such that $R_{K_i}/(\mathfrak{p}_{K_i})^e \cong \mathfrak{r}_i$. By a standard weak approximation/Krasner's Lemma argument there is a number field K and maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ such that the completion of K at $\mathfrak{p}_i$ is K_i. It follows that $\mathbb{Z}_K/\prod_{i=1}^r \mathfrak{p}_i^{e_i} \cong \mathfrak{r}$. □

Remark 2.13 When $\mathfrak{r}$ is local, Theorem 2.12 is due to Nečaev [30]. The general case emerged in a MathOverflow discussion [22] in which the second author participated and in which the most important contribution was made by Conrad.

3 Zolotarev symbols and Zolotarev reciprocity

3.1 Jacobi symbols

A ring R is *even* (resp. *odd*) if it is finite of even (resp. odd) order. An ideal I in a ring R is *even* (resp. *odd*) if R/I is even (resp. odd). An element $a \in R$ is *even* (resp. *odd*) if $\langle a \rangle$ is even (resp. odd).

For an odd field k and $a \in k^\times$, we define the *Legendre symbol* $\left(\frac{a}{k}\right)$ to be 1 if a is a square in k and -1 otherwise.

Let $\mathfrak{r}$ be a finite principal commutative ring, with local decomposition $\mathfrak{r} = \prod_{i=1}^r \mathfrak{r}_i$, $\mathfrak{p}_i$ the maximal ideal of $\mathfrak{r}_i$, e_i the length of $\mathfrak{r}_i$ and $k_i = \mathfrak{r}_i/\mathfrak{p}_i$ the residue field.

To ease notation, for $a \in \mathfrak{r}$ we write a for the image of a under any quotient map. If $\mathfrak{r}$ is odd, then for $a \in \mathfrak{r}^\times$ we define the *Jacobi symbol*

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

Let R be an abstract number ring. If $\mathfrak{p}$ is an odd prime ideal of R and $a \in R \backslash \mathfrak{p}$, we define the *Legendre symbol*

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

If $a \in R$ and $\mathfrak{b}$ is an odd ideal of R with $\langle a \rangle + \mathfrak{b} = R$, we define the *Jacobi symbol*

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

The following result is an immediate consequence of the definition.

Lemma 3.1 (a) *Let $\mathfrak{r}$ be an odd principal commutative ring, with local decomposition $\mathfrak{r} = \prod_{i=1}^{r} \mathfrak{r}_i$. Then for all $a \in \mathfrak{r}$, $\left(\frac{a}{\mathfrak{r}}\right) = \prod_{i=1}^{r} \left(\frac{a}{\mathfrak{r}_i}\right)$.*

(b) *Let $\mathfrak{b}$ be an odd prime ideal in the abstract number ring R. Let $\mathfrak{b} = \prod_{i=1}^{R} \mathfrak{q}_i$ be its factorization into not necessarily distinct prime ideals. Then for any $a \in R$ which is prime to $\mathfrak{b}$,*

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{i=1}^{R} \left(\frac{a}{\mathfrak{q}_i}\right). \tag{5}$$

3.2 Zolotarev symbols

Let $\mathfrak{r}$ be a finite ring. Then both the additive group $(\mathfrak{r}, +)$ and the unit group $(\mathfrak{r}^\times, \cdot)$ act on $\mathfrak{r}$, giving rise to signature homomorphisms. We are interested in the signatures of the permutations $s_a : x \mapsto x + a$ for $a \in \mathfrak{r}$ and $m_a : x \mapsto xa$ for $a \in \mathfrak{r}^\times$. The former is a special case of Theorem 2.4: we record the result.

Lemma 3.2 *Let n be the order of a in $(\mathfrak{r}, +)$.*

(a) $\epsilon(s_a) = (-1)^{\frac{(n-1)\#\mathfrak{r}}{n}}$.
(b) *Since $n \mid \#\mathfrak{r}$, $\epsilon(s_a) = 1$ if $\#\mathfrak{r}$ is odd.*

We define the *Zolotarev symbol* $\left[\frac{a}{\mathfrak{r}}\right] = \epsilon(m_a)$.

Remark 3.3 For $a \in \mathfrak{r}^\times$, let $a_m : x \mapsto xa$, and let $\iota^a : \mathfrak{r} \to \mathfrak{r}$ by $x \mapsto a^{-1}xa$. Since $m_a \circ \iota^a = a_m$, we have $\epsilon(m_a) = \epsilon(a_m)$.

Let $\mathfrak{r}$ be a finite commutative ring. As in §1.2 there is a canonical isomorphism

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

with $\mathfrak{r}_i$ a local ring with maximal ideal $\mathfrak{p}_i$, length e_i and residue field $k_i = \mathfrak{r}/\mathfrak{p}_i$. We call the $\mathfrak{r}_i$'s the *local factors* of $\mathfrak{r}$. Put $n_i = \#\mathfrak{r}_i$ and $n = \#\mathfrak{r}$. Let

$$\pi^\times : \mathfrak{r}^\times \xrightarrow{\sim} \prod_{i=1}^{r} \mathfrak{r}_i^\times$$

be the induced isomorphism on the unit group. Then $\pi^\times$ and π are compatible in the sense of Lemma 2.1, so for $a \in \mathfrak{r}^\times$, $[\frac{a}{\mathfrak{r}}]$ is equal to the signature of $\pi^\times(a)$ acting on $\prod_{i=1}^r \mathfrak{r}_i$. Applying the Product Lemma we get

$$\left[\frac{a}{\mathfrak{r}}\right] = \prod_{i=1}^{r} \left[\frac{a}{\mathfrak{r}_i}\right]^{\frac{n}{n_i}}. \tag{6}$$

Thus for commutative rings the computation of Zolotarev symbols is reduced to the local case. Further, by looking at the parities of $\frac{n}{n_i}$ we get the following result.

Proposition 3.4 *Let $\mathfrak{r} = \prod_{i=1}^r \mathfrak{r}_i$ be a finite commutative ring.*

(a) *If $\mathfrak{r}$ is odd, then $[\frac{\cdot}{\mathfrak{r}}] = \prod_{i=1}^r [\frac{\cdot}{\mathfrak{r}_i}]$.*

(b) *If $\mathfrak{r}$ has exactly one even local factor $\mathfrak{r}'$, then $[\frac{\cdot}{\mathfrak{r}}] = [\frac{\cdot}{\mathfrak{r}'}]$.*

(c) *If $\mathfrak{r}$ has more than one even local factor, the Zolotarev symbol $\left[\frac{\cdot}{\mathfrak{r}}\right]$ is trivial.*

3.3 First Zolotarev Lemma

When q is a prime, the following result is Zolotarev's original observation and the first of three steps of his proof of the quadratic reciprocity law in $\mathbb{Z}$.

Lemma 3.5 (First Zolotarev Lemma) *For any odd prime power q and $a \in \mathbb{F}_q^\times$, we have $\left[\frac{a}{\mathbb{F}_q}\right] = \left(\frac{a}{\mathbb{F}_q}\right)$.*

Proof Since $\mathbb{F}_q^\times$ is cyclic of even order, $a \mapsto \left(\frac{a}{\mathbb{F}_q}\right)$ is the unique nontrivial group homomorphism from $\mathbb{F}_q^\times$ to $\{\pm 1\}$. On the other hand, if a is a generator of $\mathbb{F}_q^\times$, the cycle type of m_a is $(q-1, 1)$, so $\left[\frac{a}{\mathbb{F}_q}\right] = -1$. □

3.4 A generalization of the Zolotarev–Frobenius–Lerch theorem

Theorem 3.6 *Let $\mathfrak{r}$ be a finite principal ring.*

(a) *If $\mathfrak{r}$ is odd, then the Zolotarev symbol $[\frac{\cdot}{\mathfrak{r}}]$ is equal to the Jacobi symbol $(\frac{\cdot}{\mathfrak{r}})$.*

(b) *Suppose* $\mathfrak{r}$ *has exactly one even local factor* $\mathfrak{r}'$*, with maximal ideal* $\mathfrak{p}$*, length* e *and residue field* $k \cong \mathbb{F}_{2^f}$*. Then:*
  (i) *The Zolotarev symbol* $[\frac{\cdot}{\mathfrak{r}}]$ *is trivial iff at least one of the following holds:*
    - $e = 1$.
    - $f \geq 2$.
    - $e \geq 3$, $f = 1$ *and* $\mathfrak{r}'/\mathfrak{p}^2$ *has characteristic* 2.
  (ii) *In all other cases* $\#(\mathfrak{r}'/\mathfrak{p}^2)^\times = 2$*, and* $[\frac{a}{\mathfrak{r}}] = 1 \iff a - 1 \in \mathfrak{p}^2$.

(c) *If* $\mathfrak{r}$ *has more than one even local factor then the Zolotarev symbol* $[\frac{\cdot}{\mathfrak{r}}]$ *is trivial.*

Proof Step 1: Using Lemma 3.1 and Proposition 3.4 we reduce to the case in which $\mathfrak{r}$ is local, with maximal ideal $\mathfrak{p} = (\pi)$, length e, and residue field $k = \mathbb{F}_q = \mathbb{F}_{p^f}$.

Step 2: For $1 \leq i \leq e$ put $U_i = (R/\mathfrak{p}_i)^\times$; let U_0 be the trivial group. For $1 \leq i \leq r$ the quotient maps $R/\mathfrak{p}^i \to R/\mathfrak{p}^{i-1}$ restrict to give surjective group homomorphisms $q_i : U_i \to U_{i-1}$; let $P_i = \operatorname{Ker} q_i$, so we have short exact sequences

$$1 \to P_i \to U_i \to U_{i-1} \to 1. \tag{7}$$

Since $\mathfrak{r}/\mathfrak{p}^i = U_i \coprod \mathfrak{p}/\mathfrak{p}^i$ and $\#\mathfrak{p}/\mathfrak{p}^i = q^{i-1}$, we have $\#U_i = q^{i-1}(q-1)$ for all $1 \leq i \leq r$, $\#P_1 = q - 1$ and $\#P_i = q$ for all $2 \leq i \leq e$. We claim that P_i is a p-torsion group for all $i \geq 2$. Indeed, for $x \in P_i$ we have $x \equiv 1 \pmod{\pi}^{i-1}$. Since $i \geq 2$ this implies $x \equiv 1 \pmod{\pi}$, so $1 + x + \ldots + x^{p-1} \equiv 0 \pmod{\pi}$ and thus $\pi^i = \pi^{i-1}\pi \mid (x-1)(1 + x + \ldots + x^{p-1}) = x^p - 1$.

For $1 \leq i \leq e$ let ϵ_i denote the composite homomorphism $U_e \to U_i \xrightarrow{\epsilon_{U_i}} \{\pm 1\}$, as in Theorem 2.7. For all $1 \leq i \leq e$, $\cdot\pi$ is a U_e-set isomorphism $\mathfrak{r}/\mathfrak{p}^{i-1} \to \mathfrak{p}/\mathfrak{p}^i$. So applying the Sum Lemma to $\mathfrak{r}/\mathfrak{p}^i = U_i \coprod \mathfrak{p}/\mathfrak{p}^i \cong U_i \coprod R/\mathfrak{p}^{i-1}$, we get

$$\forall 1 \leq i \leq e,\ \forall a \in \mathfrak{r}^\times,\ \left[\frac{a}{\mathfrak{r}/\mathfrak{p}^i}\right] = \epsilon_i(a)\left[\frac{a}{\mathfrak{r}/\mathfrak{p}^{i-1}}\right],$$

and thus by induction and the Tower Theorem,

$$\left[\frac{a}{\mathfrak{r}}\right] = \prod_{i=1}^{e} \epsilon_i(a) = \epsilon_\ell(a)^{u-\ell+1}.$$

It remains to compute the parameters ℓ and u. Since a finite commutative group has nontrivial cyclic 2-Sylow subgroup iff it has exactly one element of order 2, as we start at $i = 1$ and increase to e we want to determine the thresholds ℓ and u at which T_i acquires an order 2 element and then a second order 2 element.

Step 3: Suppose that $\mathfrak{r}$ is odd. Then $U_1 = k_1^\times$ is cyclic of even order so ϵ_1 is nontrivial: $\ell = 1$. The Legendre symbol $\left(\frac{\cdot}{k}\right)$ is also a nontrivial homomorphism to $\{\pm 1\}$, so by Theorem 2.4(d), $\epsilon_1 = \left(\frac{\cdot}{k}\right)$. Since $U_{i-1} = U_i/P_i$ and $\#P_i = q$ is odd, by Lemma 2.6 and induction, each ϵ_i is nontrivial: $u = e$. So $[\frac{a}{\mathfrak{r}}] = \left(\frac{a}{k}\right)^e = \left(\frac{a}{\mathfrak{r}}\right)$.

Step 4: Suppose that $\mathfrak{r}$ is even. Since $\#U = q - 1$ is odd, ϵ_1 is trivial.

- Thus if $e = 1$, $[\frac{\cdot}{\mathfrak{r}}] = \epsilon_1$ is trivial.
- Suppose $f \geq 2$. Then for all $i \geq 2$, P_i is a 2-torsion group of order $q = 2^f$, so T_i is not cyclic. Thus every ϵ_i is trivial, so $[\frac{\cdot}{\mathfrak{r}}]$ is trivial.
  We may now suppose $f = 1$. Then U_1 is the trivial group and U_2 has order 2 hence T_2 is nontrivial cyclic: $\ell = 2$.
- So if $(e, f) = (2, 1)$, then $[\frac{a}{\mathfrak{r}}] = \epsilon_2(a)$.
  We may now suppose that $e \geq 3$. By Theorem 2.12, there is a 2-adic field K with ring of integers R_K and maximal ideal $\mathfrak{p}_K = (\pi_K)$ and $e \in \mathbb{Z}^+$ such that $\mathfrak{r} \cong R_K/\mathfrak{p}_K^e$. It follows that for all $1 \leq i \leq e$, $\mathfrak{r}/\mathfrak{p}^i \cong R_K/\mathfrak{p}_K^i$.
- Suppose $\mathfrak{r}/\mathfrak{p}^2 \cong R_K/\mathfrak{p}_K^2$ has characteristic 4. Then $2 \in \mathfrak{p}_K \backslash \mathfrak{p}_K^2$ is a uniformizer, so the ramification index $e(K/\mathbb{Q}_2) = 1$. Since also $f(K/\mathbb{Q}_2) = 1$, $K = \mathbb{Q}_2$, $R = \mathbb{Z}_2$ and $\mathfrak{r} \cong \mathbb{Z}/2^e\mathbb{Z}$. In this case the structure of U_i was known to Gauss: for $i \geq 2$, $U_i \cong \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{i-2}$, so T_i is not cyclic: $u = 2$ and $[\frac{\cdot}{\mathfrak{r}}] = \epsilon_2$.
- Finally we suppose that $e \geq 3$, $f = 1$ and $\mathfrak{r}/\mathfrak{p}^2$ has characteristic 2, so $e(K/\mathbb{Q}_p) \geq 2$. We claim $u = 3$, hence $[\frac{\cdot}{\mathfrak{r}}] = \epsilon_2^2$ is trivial. To see this, for $i \geq 1$, let

$$\widetilde{U_i} = \mathrm{Ker}\left(R_K^\times \to (R_K/\mathfrak{p}_K^i)^\times\right),$$

  so that for all $1 \leq i \leq e$,

$$\widetilde{U_1}/\widetilde{U_i} \cong (R_K/\mathfrak{p}_K^i)^\times \cong U_i.$$

Now, following [14, Prop. 5], we observe:

$$(1 + \pi_K)^2 = 1 + 2\pi_K + \pi_K^2 \not\equiv 1 \pmod{\pi_K^3},$$

since $\pi_K^3 \mid 2\pi_K$ but $\pi_K^3 \nmid \pi_K^2$. Since $\#U_3 = 4$, U_3 is cyclic. Then $\epsilon_2 = \epsilon_3$ by Lemma 2.6. Finally, for every $x \in R_K$,

$$(1 + x\pi)^4 = 1 + 4\pi x + 6\pi^2 x^2 + 4\pi^3 x^3 + \pi^4 x^2 \equiv 1 \pmod{\pi_K^4}.$$

Thus U_4 has order 8 and exponent 4 so T_4 is not cyclic. □

Corollary 3.7 *Let $\mathfrak{b}$ be an odd ideal in an abstract number ring R, and let $a \in R$ be prime to $\mathfrak{b}$. Then*

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

3.5 Second Zolotarev Lemma

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

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

be the Chinese Remainder Theorem isomorphism. We will define three permutations A, B, Z of $R/(ab)$. Choose coset representatives $x_0, \ldots, x_{|a|-1}$ for (a) in R and $y_0, \ldots, y_{|b|-1}$ 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

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

and

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

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

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

and finally

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

Theorem 3.8 (Second Zolotarev Lemma) *For a, b coprime odd elements of R,*

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

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

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

Since $|b|$ is odd, by Lemma 2.3 $\epsilon(\alpha_1) = \left[\frac{b}{R/(a)}\right]$. The permutation α_2 is the direct sum of the permutations $\alpha_{2,j} : (x, y_j) \mapsto (x + y_j, y_j)$ on $R/(a) \times \{y_j\}$ for $1 \le j \le |b|$. By Lemma 3.2, $\epsilon(\alpha_{2,j}) = 1$ for all j. By Lemma 2.2, $\epsilon(\alpha_2) = 1$, so $\epsilon(A) = \epsilon(\alpha) = \epsilon(\alpha_1)\epsilon(\alpha_2) = \left[\frac{b}{R/(a)}\right]$. A very similar argument gives $\epsilon(B) = \epsilon(\beta) = \left[\frac{a}{R/(b)}\right]$. □

3.6 Zolotarev reciprocity

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

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

Theorem 3.9 (Zolotarev 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 Appplying Theorem 3.8 and Corollary 3.7 gives

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

□

Remark 3.10 By Theorem 3.9, the signature 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: we give an example.

Let $R = \mathbb{Z}, a = 3, b = 5$. 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.

4 Quadratic reciprocity in $\mathbb{Z}$

4.1 The quadratic reciprocity law of Gauss–Jacobi

For any positive integer c, let $[0, c-1]$ be $\{0, 1, \ldots, c-1\}$ 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 iff

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

So the number of inversions is $\binom{a}{2}\binom{b}{2} = \frac{a(a-1)b(b-1)}{4}$. Thus we get

$$z(a, b) = (-1)^{\frac{(a-1)(b-1)}{4}} \text{ when } a \text{ and } b \text{ are both odd.}$$

This computation along with Theorem 3.9 yields the following result.

Theorem 4.1 (Jacobi) *For coprime odd $a, b \in \mathbb{Z}^+$, we have*

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

4.2 Supplementary laws

Theorem 4.2 *Let $\mathfrak{b}$ be an odd ideal in an abstract number ring R. Then*

$$\left(\frac{-1}{\mathfrak{b}}\right) = \left[\frac{-1}{R/\mathfrak{b}}\right] = (-1)^{\frac{|\mathfrak{b}|-1}{2}}.$$

Proof By Corollary 3.7, $\left(\frac{-1}{\mathfrak{b}}\right) = \left[\frac{-1}{R/\mathfrak{b}}\right]$. Since $R/\mathfrak{b}$ is odd, the only $x \in R/\mathfrak{b}$ with $2x = 0$ is $x = 0$. Thus $[\frac{-1}{\mathfrak{r}}]$ is a product of $\frac{|\mathfrak{b}|-1}{2}$ 2-cycles $x \mapsto -x \mapsto x$. □

Theorem 4.3 *For any odd positive integer b, we have*

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}. \tag{9}$$

Proof By Corollary 3.7, $\left(\frac{2}{b}\right)$ is the signature of multiplication by 2 on $\mathbb{Z}/b\mathbb{Z}$. We count inversions using the standard ordering on $\{0, \ldots, b-1\}$: for $0 < i < j \leq b-1$, if $m_2(i) > m_2(j)$ then $i \leq \frac{b-1}{2}$. There is one inversion with $i = 1$, two with $i = 2$, and so forth, up to $\frac{b-1}{2}$ with $i = \frac{b-1}{2}$, for a total of $\frac{(\frac{b-1}{2})(\frac{b-1}{2}+1)}{2} = \frac{b^2-1}{8}$. □

5 Quadratic reciprocity in $\mathbb{F}_q[t]$

5.1 The signature of an $\mathbb{F}_q$-linear automorphism

Theorem 5.1 *Let q be an odd prime power, 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 $m \in \mathrm{GL}(V)$ permutes the finite set V and thus has a signature $\epsilon(m)$.*

(b) *For all* $m \in \mathrm{GL}(V)$*, we have*

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

Proof (a) is immediate. As for (b), the idea is to show on the one hand that there is exactly one nontrivial homomorphism $\mathrm{GL}(V) \to \{\pm 1\}$ and then to exhibit some element $D \in \mathrm{GL}(V)$ with $\epsilon(D) = -1$. Indeed:

For any finite-dimensional vector space over a field F of cardinality greater than 2, the commutator subgroup of $\mathrm{GL}(V)$ is the special linear group $\mathrm{SL}(V)$ [2, Thm. 4.7]. 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 even order cyclic, there is a unique nontrivial homomorphism $\mathrm{GL}(V) \to \{\pm 1\}$.

Let $u \in \mathbb{F}_q^{\times} \backslash \mathbb{F}_q^{\times 2}$, and let D be the diagonal matrix with entries $u, 1, \ldots, 1$. By Lemma 2.3, $\epsilon(D) = -1$. So the signature homomorphism $\mathrm{GL}(V) \to \{\pm 1\}$ is nontrivial and coincides with $m \mapsto \det(m) \pmod{\mathbb{F}_q^{\times 2}}$. □

5.2 The quadratic reciprocity law of Dedekind–Artin

Theorem 5.2 *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 $A = \deg a$, $B = \deg b$, $a = \sum_{i=0}^{A-1} a_i t^i + t^A$, $b = \sum_{i=0}^{B-1} b_i t^i + t^B$. 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_a, V_b, 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

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

Let $e_1 = 1, e_2 = t, \ldots, e_{A+B} = t^{A+B-1}$, $V_1 = \langle e_1, \ldots, e_A \rangle$ and $V_2 = \langle e_{A+1}, \ldots, e_{A+B} \rangle$, 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

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

Let

$$\mathcal{L}_1 : V_a \oplus V_b \to V,\ (x, y) \mapsto x + ay,\ \mathcal{L}_2 : V_a \oplus V_b \to V,\ (x, y) \mapsto bx + y,$$

$$L_i = \mathcal{L}_i \circ \iota^{-1} : V \to V,\ i \in \{1, 2\}$$

so $Z^{-1} = L_2 \circ L_1^{-1} = \mathcal{L}_2 \circ \mathcal{L}_1^{-1}$. With respect to the basis $(e_1, \ldots, e_{A+B})$ of V, L_1 is given by the matrix

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

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

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

Then, if $P : V \to V$ is the linear map which carries the basis $(e_1, \ldots, e_A, e_{A+1}, \ldots, e_B)$ to the basis $(e_{A+1}, \ldots, e_B, e_1, \ldots, e_A)$, $M_2 \circ P = M_3$ 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 $(e_1, \ldots, e_A)$ past all B basis vectors $e_{A+1}, \ldots, e_B$, so it has signature $(-1)^{AB}$, and thus $\det Z = \det P = (-1)^{AB}$. Applying Lemma 5.1, 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 $q \equiv 3 \pmod 4$. □

Combining Theorem 5.2 with Zolotarev Reciprocity, we recover the quadratic reciprocity law of Dedekind–Artin [15], [1].

Theorem 5.3 *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:*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{(|a|-1)(|b|-1)}{4}}. \tag{10}$$

6 Zolotarev symbols in matrix rings

Theorem 6.1 *Let $n \geq 2$, let $\mathfrak{r}$ be a finite commutative ring of order m, and let $\epsilon : \mathrm{GL}_n(\mathfrak{r}) \to \{\pm 1\}$ be the signature homomorphism of the linear action of $\mathrm{GL}_n(\mathfrak{r})$ on $\mathfrak{r}^n$. Write $\mathfrak{r} = \mathfrak{r}_o \times \mathfrak{r}'$, with $\#\mathfrak{r}_o = m_o$ odd and $\#\mathfrak{r}' = m'$ a power of 2.*

(a) *If $\mathfrak{r}$ is odd, then for all $g \in \mathrm{GL}_n(\mathfrak{r})$,*

$$\epsilon(g) = \left[\frac{\det g}{\mathfrak{r}}\right]. \tag{11}$$

Thus if $\mathfrak{r}$ is odd and principal,

$$\epsilon(g) = \left(\frac{\det g}{\mathfrak{r}}\right). \tag{12}$$

(b) *If $m' > 2$, then ϵ is trivial.*
(c) *If $m' = 2$—so $\mathfrak{r} = \mathfrak{r}_o \times \mathbb{F}_2$—then:*
  (i) *if $n \geq 3$, then ϵ is trivial.*
  (ii) *If $n = 2$, then $\epsilon(g)$ is the signature of the homomorphic image $g' \in \mathrm{GL}_2(\mathbb{F}_2)$ acting on $\mathbb{F}_2^2$. This map is nontrivial and cannot be expressed in terms of* $\det g$.

Proof Step 0. We reduce to either the case $m = m_o$ is odd or $m = m'$ is a power of 2. This is clear if $m' = 1$, so suppose $m' > 1$. The decomposition $\mathfrak{r} = \mathfrak{r}_o \times \mathfrak{r}'$ induces a decomposition $\mathrm{GL}_n(\mathfrak{r}) = \mathrm{GL}_n(\mathfrak{r}_o) \times \mathrm{GL}_n(\mathfrak{r}')$. For $g \in G$, write $g = (g_o, g')$. By the Product Lemma, $\epsilon(g) = \epsilon(g_o)^{(m')^n}\epsilon(g')^{(m_o)^n} = \epsilon(g')$, so we may assume $\mathfrak{r} = \mathfrak{r}'$.

Step 1: For i, j distinct elements of $\{1, \ldots, n\}$ and $\alpha \in \mathfrak{r}^\bullet$, let $E_{i,j}(\alpha) \in \mathrm{GL}_n(\mathfrak{r})$ be the matrix which is obtained from the identity matrix by changing (i, j) entry from 0 to α. Such an element is called a *transvection*; notice that $E_{ij}(\alpha)^{-1} = E_{ij}(\alpha)$ and $\det E_{ij}(\alpha) = 1$, so the subgroup of $\mathrm{GL}_n(\mathfrak{r})$ generated by transvections is contained in $\mathrm{SL}_n(\mathfrak{r})$. Because $\mathfrak{r}$ is a semilocal ring, $\mathrm{SL}_n(\mathfrak{r})$ is generated by transvections [21, Thm. 4.3.9]. It follows that every $g \in \mathrm{GL}_n(\mathfrak{r})$ can be written as a finite product of transvections together with a diagonal matrix $\mathrm{diag}(\det(g), 1, 1, \ldots, 1)$. In all cases except the exceptional one $(m', n) = (2, 2)$, the claimed answer is visibly multiplicative in g, so it suffices to determine the signature of a transvection $E_{ij}(\alpha)$ and the signature of $\mathrm{diag}(\alpha, 1, 1, \ldots, 1)$ for $\alpha \in \mathfrak{r}^\times$.

Step 2: We claim that in all cases except $(m', n) = (2, 2)$ we have $\epsilon(E_{ij}(\alpha)) = 1$. The effect of the transvection $E_{ij}(\alpha)$ on the vector $x = (x_1, \ldots, x_n) \in \mathfrak{r}^n$ is to replace

x_i by $x_i + \alpha x_j$. The other $n-2$ coordinates of x are immaterial: more formally, the cycle type of $E_{ij}(\alpha)$ is m^{n-2} times the cycle type of

$$e(\alpha) : (x, y) \in \mathfrak{r}^2 \mapsto (x + \alpha y, y).$$

If m is even and $n > 2$ this already shows $\epsilon(E_{ij}(\alpha)) = 1$. Otherwise

$$\epsilon(E_{ij}(\alpha)) = \epsilon(e_\alpha) = \prod_{y \in R} \epsilon_{(\mathfrak{r},+)}(\alpha y) = \epsilon_{(\mathfrak{r},+)}\left(\sum_{y \in \mathfrak{r}} \alpha y\right) = \epsilon_{(\mathfrak{r},+)}\left(\sum_{y \in \mathfrak{r}} y\right),$$

so by Theorem 2.4, $\epsilon(E_{ij}(\alpha)) = 1$ iff $Y = \sum_{y \in \mathfrak{r}} y$ has odd order or even index. Certainly Y has odd order if $m = \#\mathfrak{r}$ is odd, giving the result in this case. Now suppose m is even. The sum of all the elements in a finite commutative group has order at most 2, since every element of order greater than 2 cancels with its additive inverse. So if $m' > 2$, then since it is a power of 2, Y has even index in $(\mathfrak{r}, +)$ and $\epsilon(E_{ij}(\alpha)) = 1$. Finally, if $(m', n) = (2, 2)$ then we get the signature of $+1$ on $\mathbb{F}_2$, which is -1.

Step 3: The evaluation of $\epsilon(\mathrm{diag}(\alpha, 1, \ldots, 1))$ is familiar from the proof of Theorem 5.1: the cycle type is m^{n-1} times that of $\alpha\cdot$ on $\mathfrak{r}$. So if m is odd,

$$\epsilon(\mathrm{diag}(\alpha, 1, \ldots, 1)) = \left[\frac{\alpha}{\mathfrak{r}}\right],$$

whereas if m is even then since $n \geq 2$,

$$\epsilon(\mathrm{diag}(\alpha, 1, \ldots, 1)) = 1.$$

Step 4: If m is odd, any $g \in \mathrm{GL}_n(\mathfrak{r})$ is a product of transvections—all of which have signature 1—and $\mathrm{diag}(\det g, 1, \ldots, 1)$, with signature $\left[\frac{\det g}{\mathfrak{r}}\right]$, so $\epsilon(g) = \left[\frac{\det g}{\mathfrak{r}}\right]$. If $\mathfrak{r}$ is principal, then by Corollary 3.7 $\epsilon(g) = \left(\frac{\det g}{\mathfrak{r}}\right)$.

If m is even but $(m, n) \neq (2, 2)$, then any $g \in \mathrm{GL}_n(\mathfrak{r})$ is a product of transvections and $\mathrm{diag}(\deg g, 1, \ldots, 1)$, all of which have trivial signature, so $\epsilon(g) = 1$.

In the final case have $\epsilon(g) = \epsilon(g')$, where g' is the image of g in $\mathrm{GL}_2(\mathbb{F}_2)$ acting on $\mathbb{F}_2^2$. In this case, as we have seen, any transvection has signature -1, so that the signature homomorphism $\epsilon : \mathrm{GL}_2(\mathbb{F}_2) \to \{\pm 1\}$ is nontrivial. We can be more explicit: $\#\,\mathrm{GL}_2(\mathbb{F}_2) = 6$, and the three elements g for which $\epsilon(g) = -1$ are the two transvections $E_{12}(1)$, $E_{21}(1)$ and the transposition $T = E_{12}(1)E_{21}(1)E_{12}(1)$.[2] Since every matrix in $\mathrm{GL}_2(\mathbb{F}_2)$ has determinant 1, this homomorphism does not factor through the determinant map. □

Corollary 6.2 *Let $n \geq 2$, and let $\mathfrak{r}$ be a finite commutative ring. Then:*

[2] In fact, $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to S_3 so has a unique index 2 subgroup, and thus $\epsilon : \mathrm{GL}_2(\mathbb{F}_2) \to \{\pm 1\}$ is the unique nontrivial homomorphism.

(a) *If* $\mathfrak{r}$ *is odd, then for all* $g \in R$,

$$\left[\frac{g}{M_n(\mathfrak{r})}\right] = \left[\frac{\det g}{\mathfrak{r}}\right]^n.$$

If $\mathfrak{r}$ *is moreover a principal ring, then*

$$\left[\frac{g}{M_n(\mathfrak{r})}\right] = \left(\frac{\det g}{\mathfrak{r}}\right)^n.$$

(b) *If* $\mathfrak{r}$ *is even, then the Zolotarev symbol* $\left[\frac{\cdot}{M_n(\mathfrak{r})}\right]$ *is trivial.*

Proof We have $M_n(\mathfrak{r}) = \prod_{i=1}^n \mathfrak{r}^n$, and the action of G on $M_n(\mathfrak{r})$ is the n-fold Cartesian product of its action on n copies of $\mathfrak{r}^n$. The result now follows immediately from Theorem 6.1, the Product Lemma and Corollary 3.7. □

Remark 6.3 The special linear group $\mathrm{SL}_n(\mathfrak{r})$ is also generated by transvections when $\mathfrak{r}$ is a Euclidean ring [28]. Any Artinian principal ring is Euclidean [10, Cor. 24], so this gives a more elementary approach to Step 1 of the proof of Theorem 6.1 when $\mathfrak{r}$ is principal.

Taking $\mathfrak{r}$ to be an odd finite field in Theorem 6.1, we get another proof of Theorem 5.1. In fact these arguments are closely related: arguments are closely related: let $\mathfrak{r}$ be a commutative local ring. Let $n \geq 2$; if $2 \notin \mathfrak{r}^\times$ we suppose $n \geq 3$. Then $\mathrm{SL}_n(\mathfrak{r})$ is the commutator subgroup of $\mathrm{GL}_n(\mathfrak{r})$ [28] (and the proof is by comparison with the subgroup generated by the transvections). When this holds, the index 2 subgroups of $\mathrm{GL}_n(\mathfrak{r})$ correspond to the index 2 subroups of $\mathfrak{r}^\times$. In particular, if $\mathfrak{r}^\times$ is odd order cyclic, then $\mathrm{GL}_n(\mathfrak{r})$ has no index 2 subgroups, so *all* signature maps for $\mathrm{GL}_n(\mathfrak{r})$ are trivial. If $\mathfrak{r}^\times$ is even order cyclic, then $\mathrm{GL}_n(\mathfrak{r})$ has a unique index 2 subgroup, so to compute any signature map for $\mathrm{GL}_n(\mathfrak{r})$ it is enough to decide whether it is nontrivial. In the case of Theorems 5.1 and 6.1 this is easily done by evaluating at $\mathrm{diag}(\alpha, 1, \ldots, 1)$. Unfortunately this approach does not work in the general case.

7 Some comments on the history and literature

In this final section we discuss some of the history of Zolotarev's approach to quadratic reciprocity and give a guide to the literature on this subject.

The roots of an approach to quadratic reciprocity via permutation groups go all the way back to Gauss's Lemma, but in that approach the underlying group theory remains below the surface, making the approach (to our taste) conceptually obscure.

The story properly begins with an 1872 paper of Zolotarev [38]. Zolotarev gives Corollary 3.7 in the case $R = \mathbb{Z}$ and $\mathfrak{b} = p$ an odd prime. It is a brilliant observation, the more so because the proof is almost trivial. It amounts to: (i) $U(p)$ has a unique index 2 subgoup, and (ii) a generator of $U(p)$ acts as a $(p-1)$-cycle hence has signature -1. He then showed that for odd primes $\ell \neq p$ there are permutations A and B on $\mathbb{Z}/\ell p\mathbb{Z}$ with $\epsilon(A) = [\frac{\ell}{p}]$ and $\epsilon(B) = [\frac{p}{\ell}]$ and such that the sign of $Z = B \circ A^{-1}$

can be computed combinatorially. Our treatment of this material in Sects. 3.4 and 4.1 was also influenced by [4,39]. All these expositions follow Zolotarev's original work closely...with a single exception.

Namely, Zolotarev's treatment was for the Legendre symbol, whereas in Sect. 4.1 we proved quadratic reciprocity for the Jacobi symbol. This necessitates knowing $[\frac{a}{b}] = \left(\frac{a}{b}\right)$ for coprime positive integers a and b with b odd: given this, the rest of Zolotarev's argument applies verbatim. This result was proven by G. Frobenius. Although he did not publish it until 1914 [18], according to [8, p. 37] Frobenius's generalization was made "immédiatement" upon seeing Zolotarev's work.

Curiously, this *Zolotarev–Frobenius Lemma* is well known in the francophone literature—it is even treated in the French wikipedia—but is much harder to find in the anglophone literature. Rediscoveries of this result by non-francophone authors have been and continue to be common—e.g. [5,37]—and we were not aware of Frobenius's paper when this work was begun. In particular we know of no number theory text which gives a direct proof of the Zolotarev–Frobenius Lemma.

So far as we know the first publication which includes a proof of Zolotarev–Frobenius is an 1896 paper of Lerch [27]. In fact Lerch proved a stronger result.

Theorem 7.1 (Lerch) *Let $a, b \in \mathbb{Z}^+$ be coprime. Then:*

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

Our Theorem 3.6 is thus the generalization of Lerch's Theorem to any finite principal ring (equivalently, to any proper quotient of an abstract number ring).

Why are the French so much more knowledgeable about Zolotarev–Frobenius than the rest of the mathematical community? We think it is because of a 1970 paper of Cartier [8]. Cartier's paper is not reviewed in Math Reviews! But it is a remarkable piece of work, an elegant, lucid exposition which contains new results. Our Corollary 3.7 appears in [8], stated in the case of quotients of a number ring $\mathbb{Z}_K$, but by Theorem 2.12 these yield every finite principal ring (and his proof works verbatim for odd ideals in any abstract number ring). Theorem 5.1 appears as well [8, p. 41] (and again we rediscovered this result for ourselves).

It remains an expository challenge to give a simple, direct, self-contained proof of the Zolotarev–Frobenius Lemma. A reasonable specimen is given in a two page note of Dressler and Shult [17]. However they use the cyclicity of the unit group $U_e = (\mathbb{Z}/p^e\mathbb{Z})^\times$ for an odd prime p. But it seems to us that the merit of the odd order case is that one does not need to know the structure of U_e. And in fact in other odd residue rings of abstract number rings these groups need not be cyclic: for any odd prime ideal $\mathfrak{p}$ in $\mathbb{F}_q[t]$, the minimal number of generators of U_e tends to infinity with e [32, Prop. 1.6].

The Frobenius part of Zolotarev–Frobenius can be bypassed entirely, as observed by Rousseau [33]: the latter two thirds of Zolotarev's argument shows the Zolotarev symbols $[\frac{a}{b}]$ satisfy the quadratic reciprocity law. One can then use this reciprocity law to show inductively that $[\frac{a}{p_1 \cdots p_r}] = \prod_{i=1}^r [\frac{a}{p_i}]$, and by Zolotarev's Lemma, the

latter expression is equal to $\prod_{i=1}^{r} \left(\frac{a}{p_i}\right) = \left(\frac{a}{p_1 \cdots p_r}\right)$. This approach is not available to us in the case of a general odd residue ring of an abstract number ring because we do not have an explicit reciprocity law!

Cartier's approach to Corollary 3.7 uses the following result.

Theorem 7.2 (Cartier) *Let u be an automorphism of a finite* odd order *group G.*

(a) *(Generalized Gauss's Lemma) Let $S \subset G \backslash \{e\}$ be such that $S \cap S^{-1} = \varnothing$ and $S \cup S^{-1} = G$. Then the signature of u on G is $(-1)^{\#(u(S) \cap S^{-1})}$.*

(b) *If u stabilizes a normal subgroup N of G, the signature of u on G is equal to the signature of u on N times the signature of the induced automorphism on G/N.*

There are in fact several killing blows in the odd order case. For instance the kernel K of $U_e \to U_1$ has order q^{e-1} and U_1 has order $q - 1$, so

$$1 \to K \to U_e \to U_1 \to 1$$

splits: $U_e \cong K \times U_1$. One can then apply the Product Lemma to get $\epsilon_e = \epsilon_K \epsilon_1$; and since K has odd order, ϵ_K is trivial. This was the argument in an earlier version of this paper, and Cartier makes this remark as well [8, p. 39]. Cartier's approach exploits the properties of the signature of an automorphism of a group of odd order, whereas our approach exploits the isomorphisms $\mathfrak{p}_i/\mathfrak{p}_{i+1} \cong R/\mathfrak{p}_i$ to express the signature as a product of Cayley signatures ϵ_G.

Cartier defines a symbol $\left(\frac{u}{G}\right)$, the signature of an automorphism u of a finite group G. Every Zolotarev symbol $\left[\frac{a}{\mathfrak{r}}\right]$ is a Cartier symbol on the underlying additive group $(\mathfrak{r}, +)$, but the systematic study of $\left(\frac{u}{G}\right)$ when $\#G$ is even seems difficult.

There is also the quadratic symbol $\left(\frac{a}{G}\right)$ of Duke and Hopkins: here $(G, \cdot)$ is a finite group, $a \in \mathbb{Z}^+$ is coprime to $\#G$ and the symbol is the signature of the permutation $C \mapsto C^a$ on *conjugacy classes* of G. When G is commutative, we may write G additively and view it as the underlying additive group of some $\mathfrak{r}_G = \prod_{i=1}^{f} \mathbb{Z}/d_i\mathbb{Z}$. Then the symbol $\left(\frac{a}{G}\right)$ becomes the Zolotarev symbol $\left[\frac{a}{\mathfrak{r}_G}\right]$, with the additional restriction that a lies in the prime subring $\mathbb{Z} \cdot 1$ of $\mathfrak{r}_G$. Duke–Hopkins show that when $\#G$ is even, $\left(\frac{a}{G}\right)$ iff $4 \mid \#G$ and G has exactly one element of order 2. This implies the even order case of Lerch's Theorem and is a special case of Theorem 3.6. It can happen that $\left[\frac{a}{\mathfrak{r}_G}\right] = 1$ for all $a \in \mathbb{Z} \cdot 1 \cap \mathfrak{r}_G^\times$ but $\left[\frac{a}{\mathfrak{r}_G}\right] = -1$ for some $a \in \mathfrak{r}_G^\times$. When G is noncommutative, the Duke–Hopkins symbol is not a Cartier symbol.

If G is a finite group and $a \in \mathbb{Z}^+$ is coprime to $\#G$, Hablicsek and Mantilla-Soler consider the signature of the permutation $g \mapsto g^a$ on G—in the noncommutative case this need not be a group automorphism of G—and prove a reciprocity law for a class of groups including all nilpotent groups and all odd order groups [20].

Theorem 6.1 is a generalization of the following result of Lehmer [26].

Theorem 7.3 (Lehmer) *Let $m, n \in \mathbb{Z}^+$ with $n \geq 2$, and put $G = \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z})$. Consider the signature map $\epsilon : G \to \{\pm 1\}$ for the linear action of G on $(\mathbb{Z}/m\mathbb{Z})^n$.*

(a) *If m is odd, then for all $g \in G$, $\epsilon(g) = \left(\frac{\det g}{m}\right)$.*

(b) *If m is even, then:*

(i) *If $n \geq 3$ or $m \equiv 0 \pmod 4$ then ϵ is trivial.*

(ii) *If $n = 2$ and $m \equiv 2 \pmod 4$, for $g \in G$ let $g' = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in M_n(\mathbb{Z})$ be the unique matrix with entries in $\{0, 1\}$ which is congruent to g modulo 2. Then*

$$\epsilon(g) = (-1)^{(a'+b'+c'+d')}(a'd' - b'c').$$

Lehmer attributes the case of odd m to Schur [34].

Acknowledgments Thanks to Keith Conrad and Robert Varley for their interest and helpful comments. This note was inspired by the second author's reading of [4].

References

1. Artin, E.: Quadratische Körper im Gebiete der höheren Kongruenzen. Math. Zeit. **19**, 153–246 (1924)
2. Artin, E.: Geometric Algebra. Interscience Publishers, Inc., New York (1957)
3. Asano, K.: Über kommutative Ringe, in denen jedes Ideal als Produkt von Primidealen darstellbar ist. J. Math. Soc. Jpn. **3**, 82–90 (1951)
4. Baker, M.: Zolotarev's Magical Proof of the Law of Quadratic Reciprocity. http://people.math.gatech.edu/~mbaker/pdf/zolotarev.pdf
5. Brenner, J.L.: A new property of the Jacobi symbol. Duke Math. J. **29**, 29–32 (1962)
6. Budden, M., Eastman, S., King, S., Moisant, A.: Permutations of rational residues.Acta Univ. Apulensis Math. Inform. No. **28**, 333–339 (2011)
7. Butts, H.S., Wade, L.I.: Two criteria for Dedekind domains. Am. Math. Mon. **73**, 14–21 (1966)
8. Cartier, P.: Sure un généralization des symboles de Legendre-Jacobi. Enseign. Math. **16**, 31–48 (1970)
9. Clark, P.L.: Commutative Algebra. http://math.uga.edu/~pete/integral.pdf
10. Clark, P.L.: A Note on Euclidean Order Types . Order. doi:10.1007/s11083-014-9323-y
11. Conway, J.H.: The Sensual (quadratic) Form. With the assistance of Francis Y. C. Fung. Carus Mathematical Monographs, 26. Mathematical Association of America, Washington, DC (1997)
12. Craven, D.A.: The Theory of Fusion Systems. An Algebraic Approach. Cambridge Studies in Advanced Mathematics, 131. Cambridge University Press, Cambridge (2011)
13. Curtis, C.W., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Reprint of the 1962 original. AMS Chelsea Publishing, Providence, RI (2006)
14. Dalawat, C.S.: Wilson's theorem. J. Théor. Nr. Bordx. **21**, 517–521 (2009)
15. Dedekind, R.: Abriss einer Theorie der höheren Congruenzen in Bezug auf einer reellen Primzahl-Modulus. J. Reine Angew. Math. **54**, 1–26 (1857)
16. Duke, W., Hopkins, K.: Quadratic reciprocity in a finite group. Am. Math. Mon. **112**, 251–256 (2005)
17. Dressler, R.E., Shult, E.E.: A simple proof of the Zolotarev–Frobenius theorem. Proc. AMS **54**, 53–54 (1975)
18. Frobenius, G.: Über das quadratische Reziprozitdätsgesetz. I, S.-B. Preuss. Akad. Wiss. Berlin, pp. 335–349 (1914)
19. Goldman, O.: On a special class of Dedekind domains. Topology **3**(suppl. 1), 113–118 (1964)
20. Hablicsek, M., Mantilla-Soler, G.: Power map permutations and symmetric differences in finite groups. J. Algebra Appl. **10**, 947–959 (2011)
21. Hahn, A.J., O'Meara, O.T.: The Classical Groups and K-theory. Grundlehren der Mathematischen Wissenschaften, vol. 291. Springer, Berlin (1989)
22. http://mathoverflow.net/questions/72229/quotients-of-number-rings
23. Hungerford, T.W.: On the structure of principal ideal rings. Pac. J. Math. **25**, 543–547 (1968)
24. Jacobson, N.: Basic Algebra II, 2nd edn. W. H. Freeman and Company, New York (1989)
25. Jensen, C.U.: On the characterizations of Prüfer rings. Math. Scand. **13**, 90–98 (1963)
26. Lehmer, D.H.: The characters of linear permutations. Linear Multilinear Algebra **4**, 1–16 (1976)
27. Lerch, M.: Sur un théorème de Zolotarev. Bull. Intern. de l'Acad. Fr. Joseph **3**, 34–37 (1896)

28. Litoff, O.: On the commutator subgroup of the general linear group. Proc. Am. Math. Soc. **6**, 465–470 (1955)
29. Morton, P.: A generalization of Zolotarev's theorem. Am. Math. Mon. **86**, 374–375 (1979)
30. Nečaev, A.A.: The structure of finite commutative rings with unity. Mat. Zametki **10**, 679–688 (1971)
31. Riesz, M.: Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques. Math. Scand. **1**, 159–169 (1953)
32. Rosen, M.: Number Theory in Function Fields. Graduate Texts in Mathematics, vol. 210. Springer, New York (2002)
33. Rousseau, G.: On the Jacobi symbol. J. Number Theory **48**, 109–111 (1994)
34. Schur, I.: Uber die Gausschen Summen. K. Gesell. Wiss. Göttingen, Nachrichten, Math.-Phys. Kl., 147–153 (1921)
35. Serre, J.-P.: Corps Locaux. Hermann, Paris (1962)
36. Slavutskiĭ, I.Š.: A generalization of a lemma of Zolotarev. Rev. Math. Pures Appl. (Bucarest) **8**, 455–457 (1963)
37. Szyjewski, M.: Zolotarev's proof of Gauss reciprocity and Jacobi symbols. Serdica Math. J. **37**, 251–260 (2011)
38. Zolotarev, G.: Nouvelle démonstration de la loi de de réciprocité de Legendre. Nouv. Ann. Math. **2e série 11**, 354–362 (1872)
39. Zolotarev's Lemma. http://planetmath.org/encyclopedia/ZolotarevsLemma.html