RECIPROCITY BY RESULTANT IN $k[t]$

PETE L. CLARK AND PAUL POLLACK

Abstract. Let k be a perfect field with procyclic absolute Galois group and containing a primitive nth root of unity. We define a degree n power residue symbol $\left(\frac{a}{b}\right)_n$ in the ring $k[t]$, show that it is equal to "the character of the resultant $\mathrm{Res}(b,a)$" and deduce a reciprocity law. We are motivated by commonalities between the classical case $k = \mathbb{F}_q$ and the novel but very simple case $k = \mathbb{R}$.

1. Introduction

1.1. **Quadratic reciprocity in a PID.** In this paper we explore quadratic and higher reciprocity laws in the ring $k[t]$ of polynomials over a suitable class of fields k.

Here is a simple setup for pursuing abstract algebraic generalizations of quadratic reciprocity: let R be a PID. We say that $a, b \in R$ are **coprime** if a and b are nonzero and $(a,b) = R$. For coprime $a, p \in R$ such that (p) is a prime ideal, we define the **Legendre symbol** $\left(\frac{a}{p}\right)$ to be 1 if a is a square in the field $R/(p)$ and -1 otherwise. For coprime $a, b \in R$, let $b = up_1 \cdots p_r$ for a unit $u \in R^\times$ and prime elements $p_1, \ldots, p_r \in R$. We define the **Jacobi symbol**

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right).$$

The value of $\left(\frac{a}{b}\right)$ does not change if b is replaced with another generator of (b), but this value does in general depend on the chosen generator a of (a).

We begin with the following two classical results.

Theorem 1 (Quadratic Reciprocity in $\mathbb{Z}$)**.**

a) (Gauss) *Let p and q be distinct odd prime numbers. Then*

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

b) (Jacobi) *Let a and b be coprime odd positive integers. Then*

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

Theorem 2 (Quadratic Reciprocity in $\mathbb{F}_q[t]$)**.**
Let q be an odd prime power, and let $a, b \in \mathbb{F}_q[t]$ be coprime monic polynomials. Then

$$\left(\frac{a}{b}\right) = (-1)^{\frac{q-1}{2}\deg a \deg b} \left(\frac{b}{a}\right). \tag{1}$$

Dedekind stated Theorem 2, when q is prime, in [De57] but did not prove it: he felt that Gauss's fifth proof of Theorem 1 carried over with little change ("the deductions [...] are so similar to the ones in the cited treatise of Gauss that no one can escape finding the complete proof.") The first published proof is due to Kühne [Kü02].

1.2. **A low-hanging quadratic reciprocity law.** We now give a further simple, but motivational, quadratic reciprocity law.

Theorem 3 (Quadratic Reciprocity in $\mathbb{R}[t]$)**.**
Let $a, b \in \mathbb{R}[t]$ be coprime monic polynomials. Then

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

In contrast to Theorems 1 and 2, direct calculation suffices to prove Theorem 3: an irreducible polynomial in $\mathbb{R}[t]$ has degree at most 2. For $A \in \mathbb{R}^\times$ we put

$$\operatorname{sgn}(A) := \begin{cases} 1 & \text{if } A > 0, \\ -1 & \text{if } A < 0. \end{cases}$$

Evaluation at A gives an isomorphism $\mathbb{R}[t]/(t-A) \xrightarrow{\sim} \mathbb{R}$. For $a \in \mathbb{R}[t]$ with $a(A) \neq 0$ we have

$$\left(\frac{a}{t-A}\right) = \operatorname{sgn}(a(A))$$

and it follows that for $a, b \in \mathbb{R}[t]$ with $a(A)b(A) \neq 0$ we have

$$\left(\frac{ab}{t-A}\right) = \operatorname{sgn}(a(A)b(A)) = \operatorname{sgn}(a(A)) \operatorname{sgn}(b(A)) = \left(\frac{a}{t-A}\right)\left(\frac{b}{t-A}\right).$$

Let $Q \in \mathbb{R}[t]$ be monic irreducible quadratic. Then $Q(\mathbb{R}) \subset \mathbb{R}^{>0}$, so for all $A \in \mathbb{R}$ we have

$$\left(\frac{Q}{t-A}\right) = \operatorname{sgn}(Q(A)) = 1.$$

In $\mathbb{R}[t]/(Q) \cong \mathbb{C}$ every element is a square, so for all $a \in \mathbb{R}[t]$ with a, Q coprime we have

$$\left(\frac{a}{Q}\right) = 1,$$

and thus certainly for $a, b \in \mathbb{R}[t]$ with ab, Q coprime we have

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

It follows that both sides of (2) are multiplicative in both a and b, so it suffices to verify the equation when a and b are irreducible. By the above considerations, both sides evaluate to 1 unless $a = t - A$ and $b = t - B$ for $A \neq B \in \mathbb{R}$, and then

$$\left(\frac{a(t)}{b(t)}\right)\left(\frac{b(t)}{a(t)}\right) = \operatorname{sgn}(B-A)\operatorname{sgn}(A-B) = -1 = (-1)^{\deg a \deg b},$$

completing the proof.

Theorem 2 looks strikingly similar to Theorem 3. The only difference is that the $(-1)^{\frac{q-1}{2}}$ over $\mathbb{F}_q$ is replaced by -1 over $\mathbb{R}$. This can be understood as follows: we have $[\mathbb{F}_q^\times : \mathbb{F}_q^{\times 2}] = 2 = [\mathbb{R}^\times : \mathbb{R}^{\times 2}]$, and thus in either field k we have a unique nontrivial quadratic character – i.e., a unique nontrivial group homomorphism $\chi \colon k^\times \to \{\pm 1\}$. Namely:

$$\chi \colon \mathbb{F}_q^\times \mapsto \{\pm 1\},\ a \mapsto a^{\frac{q-1}{2}}, \qquad \chi \colon \mathbb{R}^\times \mapsto \{\pm 1\},\ a \mapsto \operatorname{sgn}(a).$$

Thus if k is either $\mathbb{F}_q$ or $\mathbb{R}$, then for coprime monic polynomials $a, b \in k[t]$ we have

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

1.3. **Reciprocity by resultant.** Here is another way to look at the proof of Theorem 3: for coprime monic $a, b \in \mathbb{R}[t]$, let A (resp. B) be the "split part" of a (resp. b) – i.e., the largest monic divisor of a that has only real roots. Then the above considerations show

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

If we write out

$$A = (t - \alpha_1) \cdots (t - \alpha_r), \quad B = (t - \beta_1) \cdots (t - \beta_s),$$

then using the bimultiplicativity of Jacobi symbols established above, we get

$$\left(\frac{A}{B}\right) = \prod_{1 \leq 1 \leq r,\ 1 \leq j \leq s} \left(\frac{t - \alpha_i}{t - \beta_j}\right) = \operatorname{sgn} \left(\prod_{1 \leq i \leq r,\ 1 \leq j \leq s} (\beta_j - \alpha_i) \right) = \operatorname{sgn} \operatorname{Res}(B, A),$$

where $\operatorname{Res}(B, A) \in \mathbb{R}[t]$ is the resultant of the polynomials B and A. This motivates us to examine the connection between Jacobi symbols and resultants for all coprime monic $a, b \in \mathbb{R}[t]$. Let $\alpha, \beta \in \mathbb{C} \setminus \mathbb{R}$ be such that $\alpha \notin \{\beta, \overline{\beta}\}$ and let $A \in \mathbb{R}$. Then we have

$$\operatorname{sgn} \operatorname{Res}((t - \alpha)(t - \overline{\alpha}), t - A)) = \operatorname{sgn} \left((\alpha - A)\overline{(\alpha - A)} \right) = 1 = \left(\frac{t - A}{(t - \alpha)(t - \overline{\alpha})} \right),$$

$$\operatorname{sgn} \operatorname{Res}(t - A, (t - \alpha)(t - \overline{\alpha})) = \operatorname{sgn} \left((A - \alpha)\overline{(A - \alpha)} \right) = 1 = \left(\frac{(t - \alpha)(t - \overline{\alpha})}{t - A} \right),$$

and

$$\begin{aligned} \operatorname{sgn}(\operatorname{Res}((t - \alpha)(t - \overline{\alpha}), (t - \beta)(t - \overline{\beta}))) &= \operatorname{sgn}((\alpha - \beta)\overline{(\alpha - \beta)}(\alpha - \overline{\beta})\overline{(\alpha - \overline{\beta})}) \\ &= 1 = \left(\frac{(t - \beta)(t - \overline{\beta})}{(t - \alpha)(t - \overline{\alpha})} \right). \end{aligned}$$

Because $\operatorname{Res}(a, b)$ is also bimultiplicative, this establishes the following:

Theorem 4. *Let $a, b \in \mathbb{R}[t]$ be coprime monic polynomials. Then*

$$\left(\frac{a}{b}\right) = \operatorname{sgn} \operatorname{Res}(b, a). \tag{3}$$

For any field k and monic $a, b \in k[t]$, we have the (obvious!) **primordial reciprocity law**

$$\operatorname{Res}(b, a) = (-1)^{\deg a \deg b} \operatorname{Res}(a, b). \tag{4}$$

We observe that (3) and (4) immediately imply (2).

It is natural to ask: does the analogous identity hold in $\mathbb{F}_q[t]$? Indeed it does:

Theorem 5. *Let $a, b \in \mathbb{F}_q[t]$ be coprime monic polynomials. Then*

$$\left(\frac{a}{b}\right) = \operatorname{Res}(b, a)^{\frac{q-1}{2}}. \tag{5}$$

We observe that (5) and (4) immediately imply (1). Ore gave a proof of Theorem 2 centered around (5) in 1934 [Or34]. Several years earlier, Schmidt had proved Theorem 2 by an equivalent approach [Sc27], but without drawing attention to the fact that the expressions appearing in his proof could be described as resultants. (Both authors treat not only quadratic reciprocity, but the higher reciprocity law described below in Theorem 6.) We believe that Ore's decision to make Theorem 5 explicit was a wise one; indeed, one of the main points of this note to is demonstrate that (5) is a harbinger of a more general phenomenon. Contemporary expositions (e.g. [R, Ch. 3], [T, §1.4]) seem to follow Schmidt rather than Ore, so that Theorem 5 is no longer well known. The present authors learned of Theorem 5 from a more recent paper of Hsu [Hs03], who seems to have independently rediscovered it.

And now the plot thickens: already in 1902, Kühne gave a *higher* reciprocity law in $\mathbb{F}_q[t]$. For this, let $n \in \mathbb{Z}^+$ be such that $n \mid q-1$: equivalently, $\mathbb{F}_q$ contains the nth roots of unity.[1] Let $\mu_n \subset \mathbb{F}_q^\times$ be the subgroup of nth roots of unity. Then $[\mathbb{F}_q^\times : \mathbb{F}_q^{\times n}] = n$, and the map

$$\chi_n \colon \mathbb{F}_q^\times \to \mu_n, \quad a \mapsto a^{\frac{q-1}{n}}$$

induces an isomorphism $\mathbb{F}_q^\times / \mathbb{F}_q^{\times n} \to \mu_n$. Now for coprime $a, p \in \mathbb{F}_q[t]$ with p irreducible, we define the **nth power residue symbol**

$$\left(\frac{a}{p}\right)_n := \chi_{n, \mathbb{F}_q[t]/(p)}(a \bmod p) = a^{\frac{q^{\deg p}-1}{n}};$$

this extends by bimultiplicativity to a symbol $\left(\frac{a}{b}\right)_n$ defined for all $a, b \in \mathbb{F}_q[t] \setminus \{0\}$. Then we have the following result:

Theorem 6. *Let q be a prime power, and let $n \mid q-1$ be a positive integer. Let $a, b \in \mathbb{F}_q[t]$ be coprime monic polynomials. Then:*

a) (Ore) $\left(\frac{a}{b}\right)_n = \chi_n(\mathrm{Res}(b, a))$.
b) (Kühne) $\left(\frac{a}{b}\right)_n = \chi_n(-1)^{\deg a \deg b} \left(\frac{b}{a}\right)_n = (-1)^{\frac{q-1}{n} \deg a \deg b} \left(\frac{b}{a}\right)_n$.

Again we observe that via the primordial law (4), Theorem 6a) implies Theorem 6b).

1.4. **Statement of the Main Theorem.** This brings us to a more precise goal: to generalize this "reciprocity by resultant" to $k[t]$ for other fields k. Let us begin with the $n = 2$ case, in which we want a character $\chi_2 \colon k^\times \to \{\pm 1\}$ such that for all coprime monic $a, b \in k[t]$ we have

$$\left(\frac{a}{b}\right) = \chi_2(\mathrm{Res}(b, a)). \tag{6}$$

If this holds, then since $\chi_2(\mathrm{Res}(b, a))$ is bimultiplicative, the Jacobi symbol $\left(\frac{a}{b}\right)$ must be bimultiplicative as well. The following result shows that this places severe restrictions on k.

Lemma 7. *For a nonzero prime element p in a PID R, the following are equivalent:*

(i) *The map $a \in (R/p)^\times \mapsto \left(\frac{a}{p}\right) \in \{\pm 1\}$ is a group homomorphism.*
(ii) *The field $l := R/(p)$ has at most two square classes: $[l^\times : l^{\times 2}] = 2$.*

Proof. Let $x, y \in l^\times$. The homomorphism property of (i) fails iff there are nonsquares $x, y \in l^\times$ such that xy is also not a square iff the group $l^\times / l^{\times 2}$ has more than two elements. $\square$

[1] Here and hereafter, when we say a field k "contains the nth roots of unity," we mean that the group of nth roots of unity in k has order n. This implies that the characteristic of k does not divide n.

Thus in order for (6) to hold, we need every monogenic finite extension of k to have at most two square classes. Henceforth we shall assume k is perfect, so the above condition becomes that every finite extension of k has at most two square classes. More generally, if a perfect field k contains the nth roots of unity μ_n for some $n \in \mathbb{Z}^+$, and if by an nth power residue symbol $\left(\frac{a}{b}\right)_n$ we mean a map to μ_n such that when b is irreducible we have $\left(\frac{a}{b}\right)_n = 1$ iff a is an nth power in $k[t]/(b)$, then if there is a character $\chi_n \colon k^\times \to \mu_n$ such that $\left(\frac{a}{b}\right)_n = \chi_n(\mathrm{Res}(b,a))$, the symbol $\left(\frac{a}{b}\right)_n$ is bimultiplicative, and it follows for every finite extension l/k, the group $l^\times/l^{\times n}$ is cyclic, so $\overline{k}/l$ has at most one cyclic degree n subextension.

These considerations lead us to the following class of fields. A **perfect procyclic field** is a pair (k, F) where k is a perfect field and F is a topological generator of $\mathfrak{g}_k \coloneqq \mathrm{Aut}(\overline{k}/k)$: that is, $\mathfrak{g}_k = \overline{\langle F \rangle}$. A perfect field k with algebraic closure $\overline{k}$ admits a topological generator iff for all $d \in \mathbb{Z}^+$ there is at most one degree d subextension of $\overline{k}/k$. If k is perfect procyclic and l/k is a degree d subextension of $\overline{k}/k$, then we endow l with the structure of a perfect procyclic field by taking the topological generator F^d of $\mathfrak{g}_l$.

Example 8.

a) For any prime power q, $(\mathbb{F}_q, F \colon x \mapsto x^q)$ is a perfect procyclic field, with $\mathfrak{g}_{\mathbb{F}_q} \cong \hat{\mathbb{Z}}$.
b) A field k is **real-closed** if it can be ordered and $k(\sqrt{-1})$ is algebraically closed. Then $\mathfrak{g}_k = \{1, F\}$ has order 2 and (k, F) is a perfect procyclic field.
c) Let C be an algebraically closed field of characteristic 0, and let $k = C(\!(X)\!)$ be the Laurent series field over C. The Puiseux series field $\bigcup_{d \in \mathbb{Z}^+} C(\!(X^{\frac{1}{d}})\!)$ is an algebraic closure of k. Choose for each $d \in \mathbb{Z}^+$ a primitive dth root of unity $\zeta_d \in C$ such that for all $m, n \in \mathbb{Z}^+$ we have $\zeta_{mn}^m = \zeta_n$. Let $F \in \mathfrak{g}_k$ be the unique element such that for all $d \in \mathbb{Z}^+$, we have $F(X^{\frac{1}{d}}) = \zeta_d X^{\frac{1}{d}}$. Then (k, F) is a perfect procyclic field with $\mathfrak{g}_k \cong \hat{\mathbb{Z}}$. Such fields are called **quasi-finite** and appear in a generalization of local class field theory due to Moriya, Schilling, Whaples, Serre and Sekiguchi [S, Ch. XIII].
d) If (k, F) is perfect procyclic and l/k is any subextension of $\overline{k}/k$, then l can be given the structure of a perfect procyclic field (in fact canonically, though we will not need this when $[l : k]$ is infinite).
e) The perfect fields with procyclic absolute Galois group form an elementary class, so an ultraproduct of such fields can be given the structure of a perfect procyclic field.
f) (Artin-Quigley [Qu62]) Let K/k be a a field extension with K algebraically closed. Let $\alpha \in K \setminus k$, and let l be a subextension of K/k that is maximal with respect to the exclusion of α. (Such fields exist by Zorn's Lemma.) Then K is an algebraic closure of l and $[l(\alpha) : l] = p$ is a prime number. Moreover:
   - Either l is perfect or k has characteristic p.
   - If l is perfect, then $\mathfrak{g}_l = \mathrm{Aut}(K/l)$ is isomorphic either to $\mathbb{Z}/2\mathbb{Z}$ or to $\mathbb{Z}_p$. In particular, l can be given the structure of a perfect procyclic field.
   - If l is not perfect, then K/l is purely inseparable, and for all $n \in \mathbb{Z}^+$ there is a unique subextension l_n of K/k with $[l_n : l] = p^n$. Thus $K = \bigcup_n l_n$.
   - If α is transcendental over k, then for all prime numbers p there is a subextension l of K/k that is maximal with respect to the exclusion of α with $[l(\alpha) : l] = p$. When p is the characteristic of k, l can moreover be chosen to be perfect and can also be chosen to be imperfect. It follows that there are imperfect fields having within their algebraic closure at most one degree n field extension for all $n \in \mathbb{Z}^+$.

Let $n \in \mathbb{Z}^+$, let (k, F) be a perfect procyclic field that contains the nth roots of unity, and let $\mu_n \subset k^\times$ be the group of nth roots of unity in k. We define a homomorphism

$$\chi_{k,n} \colon k^\times \to \mu_n$$

as follows: for $\alpha \in k^\times$, let $\alpha^{1/n}$ be any nth root of α in $\overline{k}$, and put

$$\chi_{k,n}(\alpha) \coloneqq \frac{F(\alpha^{1/n})}{\alpha^{1/n}}.$$

This does not depend on the choice of $\alpha^{1/n}$. Then $\chi_{k,n}$ induces an injective homomorphism

$$\chi_n \colon k^\times / k^{\times n} \hookrightarrow \mu_n.$$

Moreover, $\chi_{k,n}$ is obtained by composing the Kummer isomorphism $k^\times/k^{\times n} \xrightarrow{\sim} \operatorname{Hom}(\mathfrak{g}_k, \mu_n)$ with the homomorphism $\operatorname{Hom}(\mathfrak{g}_K, \mu_n) \to \mu_n$ obtained by evaluating at the topological generator F. It follows that if m_n is the gcd of n and the supernatural order of $\mathfrak{g}_k$ – in other words, the largest divisor d of n such that $\mathfrak{g}_k$ has a finite quotient of order d – then $k^{\times n} = k^{\times m_n}$ and

$$\chi_{k,n} \colon k^\times / k^{\times n} = k^\times / k^{\times m_n} \xrightarrow{\sim} \mu_{m_n} \subset \mu_n.$$

Let $a, p \in k[t]$ be coprime polynomials with p irreducible of degree d. Let l_d/k be the unique degree d subextension of $\bar{k}/k$, so that (l_d, F^d) is perfect procyclic. Let $\iota \colon k[t]/(p) \xrightarrow{\sim} l_d$ be a k-algebra isomorphism. Then we define the **nth power residue symbol**

$$\left(\frac{a}{p}\right)_n \coloneqq \chi_{l_d,n}(\iota(a \bmod p)).$$

We claim that this symbol does not depend upon the choice of ι. Indeed, the k-algebra isomorphisms from $k[t]/(p)$ to l_d are precisely the maps $F^i \circ \iota$ for some $0 \leq i < d$. For $\alpha \in k[t]/(p)$, let $\iota(\alpha)^{\frac{1}{n}}$ be an nth root of $\iota(\alpha)$. Then $F^i(\iota(\alpha)^{1/n})$ is an nth root of $F^i(\iota(\alpha))$, so

$$\chi_{l_d,n}(F^i(\iota(\alpha))) = \frac{F^d(F^i(\iota(\alpha)^{1/n}))}{F^i(\iota(\alpha)^{1/n})} = F^i\left(\frac{F^d(\iota(\alpha)^{1/n})}{\iota(\alpha)^{1/n}}\right) = \frac{F^d(\iota(\alpha)^{1/n})}{\iota(\alpha)^{1/n}} = \chi_{l_d,n}(\iota(\alpha))$$

since $\frac{F(\iota(\alpha)^{1/n})}{\iota(\alpha)^{1/n}} \in \mu_n \subset k$, establishing the claim. This permits us to identify $k[t]/(p)$ with l_d and $\left(\frac{\cdot}{p}\right)$ with $\chi_{l_d,n}$. For $a, b \in k[t]$ coprime monic polynomials, write $b = up_1 \cdots p_r$ as above and put $\left(\frac{a}{b}\right)_n \coloneqq \prod_{i=1}^r \left(\frac{a}{p_i}\right)_n$. The bimultiplicativity of $\left(\frac{a}{b}\right)_n$ is immediate from the definition.

At last we can state the main result of this note.

Theorem 9. *Let $n \in \mathbb{Z}^+$, and let k be a perfect procyclic field that contains the nth roots of unity. Let $a, b \in k[t]$ be coprime polynomials. Then:*

a) *If b is monic, we have*

$$\left(\frac{a}{b}\right)_n = \chi_{k,n}(\operatorname{Res}(b, a)). \tag{7}$$

b) *If a and b are monic, we have*

$$\left(\frac{a}{b}\right)_n = \chi_{k,n}(-1)^{\deg a \deg b} \left(\frac{b}{a}\right)_n. \tag{8}$$

Once again we observe that via (4), Theorem 9a) implies Theorem 9b).

Theorem 9 recovers all the reciprocity results in $k[t]$ discussed above and via Example 8 gives new ones. Here is one application:

Corollary 10. *Let k be a perfect procyclic field containing the nth roots of unity for all $n \in \mathbb{Z}^+$ – e.g. $k = \mathbb{C}((X))$. Let $a, b \in k[t]$ be coprime monic polynomials. Then:*

a) *We have $\left(\frac{a}{b}\right)_n = \left(\frac{b}{a}\right)_n$.*
b) *If a and b are moreover irreducible, then a is an nth power modulo b iff b is an nth power modulo a.*

Proof. For all $n \in \mathbb{Z}^+$, the hypothesis implies that -1 is an nth power, so $\chi_{k,n}(-1) = 1$. □

2. Proof of the Main Theorem

Once again, it is enough to show (7), for then the primordial reciprocity law (4) gives (8).

For a commutative ring k and a k-algebra l that is finite-dimensional and free as a k-module, let $N_{l/k} \colon l \to k$ be the norm map: that is, for $x \in l$, $N_{l/k}(x)$ is the determinant of $x\bullet \in \operatorname{End}_k(l)$. Thus $N_{l/k} \colon l^\times \to k^\times$ is a group homomorphism.

Lemma 11. *Let k be a commutative ring, let $a, b \in k[t] \setminus \{0\}$ with b monic. Then*

$$N_{k[t]/(b)\big/k}(a \bmod b) = \operatorname{Res}(b, a). \tag{9}$$

Proof. Myerson gives a simple, short proof in [My83]. The lemma itself may have appeared for the first time in a 1936 monograph of Chebotarev (see [C, eq. (3.11), p. 17]). Several apparently independent rediscoveries are referenced in [My90]. □

Let (k, F) be a perfect procyclic field containing the nth roots of unity μ_n. Because both sides of (7) are multiplicative in b, it suffices to treat the case in which $b = p$ is monic irreducible, say of degree d. As justified above, we identify $k[t]/(p)$ with $l_d \subset \overline{k}$ and $\left(\frac{\cdot}{p}\right)_n$ with $\chi_{l_d,n} \colon l_d^\times \to \mu_n$. Then by Lemma 11 it suffices to show that

$$\chi_{l_d,n} = \chi_{k,n} \circ N_{l_d/k}.$$

So let $\alpha \in l_d^\times$. Then we have

$$N_{l_d/k}(\alpha) = \prod_{i=0}^{d-1} F^i(\alpha).$$

Since $\prod_{i=0}^{d-1} F^i(\alpha^{1/n})$ is an nth root of $\prod_{i=0}^{d-1} F^i(\alpha)$, we have

$$\chi_{n,k}(N_{l_d/k}(\alpha)) = \frac{F(N_{l_d/k}(\alpha)^{1/n})}{N_{l_d/k}(\alpha)^{1/n}} = \frac{F(\prod_{i=0}^{d-1} F^i(\alpha^{1/n}))}{\prod_{i=0}^{d-1} F^i(\alpha^{1/n})} = \frac{F^d(\alpha^{1/n})}{\alpha^{1/n}} = \chi_{n,\ell_d}(\alpha).$$

3. Comments and complements

3.1. Procyclic absolute Galois groups.

Proposition 12.

a) *Let k be a field with procyclic absolute Galois group $\mathfrak{g}_k$. Then exactly one of the following holds:*
   (i) *k is separably closed. Equivalently, $\mathfrak{g}_k$ is the trivial group.*

(ii) *k is real-closed. Equivalently, $\mathfrak{g}_K$ has order 2.*
(iii) *There is a nonempty set S of prime numbers such that as topological groups, we have $\mathfrak{g}_k \cong \prod_{\ell \in S} \mathbb{Z}_\ell$.*

b) *Conversely, if G is the trivial group, the group of order 2 or $\prod_{\ell \in S} \mathbb{Z}_\ell$ for some nonempty set of prime numbers S, then there is a perfect field k with absolute Galois group $\mathfrak{g}_k \cong G$.*

Proof. Let G be a procyclic group. Then $G = \prod_\ell G_\ell$, where the product extends over the prime numbers and each G_ℓ is isomorphic to a quotient of $\mathbb{Z}_\ell$ – i.e., isomorphic either to $\mathbb{Z}_\ell$ itself or to $\mathbb{Z}/\ell^a\mathbb{Z}$ for some $a \in \mathbb{Z}^+$. Thus if G is torsionfree, then there is a subset S of the prime numbers such that $G \cong \prod_{\ell \in S} \mathbb{Z}_\ell$. Each of these groups occurs up to isomorphism as a closed subgroup of the absolute Galois group of $\mathbb{F}_p$, so occurs as the absolute Galois group of an algebraic extension of $\mathbb{F}_p$.

Now let k be a (not necessarily perfect) field, with absolute Galois group $\mathfrak{g}_k = \mathrm{Aut}(k^{\mathrm{sep}}/k) = \mathrm{Aut}(\overline{k}/k)$. Let $\sigma \in \mathfrak{g}_k$ be a nontrivial element of finite order. By a theorem of Artin-Schreier [Cl-FT, Thm. 15.24], the automorphism σ has order 2 and $\overline{k}^{\langle \sigma \rangle}$ is real-closed. Moreover, by [E, Prop. 19.4.3], $\langle \sigma \rangle$ is self-normalizing in $\mathfrak{g}_k$, which is impossible if $\mathfrak{g}_k$ is commutative of order greater than 2. □

3.2. **Supplementary Laws.**

When $R = \mathbb{Z}$, $\mathbb{F}_q[t]$ or $\mathbb{R}[t]$, to compute all Legendre symbols one needs some supplements to the quadratic reciprocity law:

Proposition 13.

a) *For all odd $b \in \mathbb{Z}^+$, we have $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.*

b) *For all odd $b \in \mathbb{Z}^+$, we have $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.*

c) *For q an odd prime power, $u \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q[t] \setminus \{0\}$, we have $\left(\frac{u}{b}\right) = u^{\frac{q-1}{2}\deg b}$.*

d) *Let $A \in \mathbb{R}^\times$, and let $b \in \mathbb{R}[t] \setminus \{0\}$. Then we have $\left(\frac{A}{b}\right) = \mathrm{sgn}(A)^{\deg b}$.*

In all cases, after checking that both sides of the claimed identity are multiplicative in b, we reduce to the case in which $b = p$ is a prime element. Then part a) is a consequence of the "Euler relation" $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$: this is just the explicit form of the quadratic character $\chi_2 \colon \mathbb{F}_q^\times \to \{\pm 1\}$. Similar remarks apply to part c) upon observing that $\frac{q^{\deg b}-1}{2} = \frac{q-1}{2}(1+q+\cdots+q^{\deg b-1})$ and that u is fixed by the qth power map. Part d) is easy to prove.

Thus the only part with any depth is part b) – which has no analogue in the $k[t]$ case. In fact it follows from Theorem 1 and Proposition 13a): for odd $n \geq 3$, we have

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n-2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n}{n-2}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{2}{n-2}\right) = \ldots$$
$$= (-1)^{\frac{n-1}{2}}(-1)^{\frac{n-3}{2}}\cdots(-1)^1\left(\frac{2}{1}\right) = (-1)^{1+\ldots+\frac{n-1}{2}} = (-1)^{\frac{n^2-1}{8}}.$$

Proposition 13c) combines with Theorem 2 to give a reciprocity statement for $\left(\frac{a}{b}\right)_n$ for all coprime $a, b \in \mathbb{F}_q[t]$ and $n \mid q-1$: see e.g. [R, Thm. 3.5].

In our generalized setting, the notion of a supplementary law becomes tautologous. Indeed, if k is a perfect procyclic field containing the nth roots of unity, then for $u \in k^\times$ and irreducible $p \in k[t]$ of degree d, we have $\left(\frac{u}{p}\right) = \chi_{l_d,n}(u)$ – by definition!

3.3. **Concerning the case $k = \mathbb{R}$.** Several years ago the first author found Theorem 3 while exploring representation theorems for binary quadratic forms over $\mathbb{F}_q[t]$ and over $\mathbb{R}[t]$. For instance, Proposition 13c) applies to prove a result of Leahey [Le67] and Gerstein [Ge04, p. 133, Prop.]:

Proposition 14. *Let q be an odd prime power, and let $D \in \mathbb{F}_q^\times$ be such that $-D \notin \mathbb{F}_q^{\times 2}$. For $c \in \mathbb{F}_q[t] \setminus \{0\}$, the following are equivalent:*

(i) *There are $x, y \in \mathbb{F}_q[t]$ such that $x^2 + Dy^2 = c$.*
(ii) *For every monic irreducible $p \in \mathbb{F}_q[t]$ of odd degree, there is $r \geq 0$ such that $p^{2r} \mid c$ and $p^{2r+1} \nmid c$.*

Similarly Proposition 13d) applies to prove the following well-known analogue of Fermat's Two Squares Theorem in $\mathbb{R}[t]$:

Proposition 15. *Let $c \in \mathbb{R}[t]$. Then there are $x, y \in \mathbb{R}[t]$ such that $x^2+y^2 = c$ iff $c(\mathbb{R}) \subset \mathbb{R}^{\geq 0}$.*

Concerning precedents of Theorem 3 in the literature, we found (only) the following ones:

- In [Kn66a] and [Kn66b], J.T. Knight develops some foundations of a theory of quadratic forms over $\mathbb{R}[t]$. In [Kn66a, Prop. 2.7] he gives the analogue in $\mathbb{R}(t)$ of Hilbert's reciprocity law for quaternion algebras. He then writes "This is a much weaker result than the classical analogue, and is not worth deducing the trivial law of quadratic reciprocity from." However, on the first page of [Kn66b], Knight writes: "We can also develop a theory of quadratic residues in $\mathbb{R}[t]$, defining the generalised Legendre symbol $\left\{\frac{\alpha}{\beta}\right\}$ to be 1 or -1 according as $x^2 \equiv \alpha \pmod{\beta}$ has or has not a root $[\ldots]$ we invite the reader to verify: Lemma 1.2. Suppose $(\alpha, \beta) = 1$; then $\left\{\frac{\alpha}{\beta}\right\} = 1$ iff $\forall \xi \in \mathbb{R}$, $\beta(\xi) = 0 \implies \alpha(\xi) > 0$." When β is irreducible, Knight's symbol $\left\{\frac{\alpha}{\beta}\right\}$ coincides with the Legendre symbol, but in general it does not correspond to the Jacobi symbol. This symbol does not appear elsewhere in [Kn66b].
- In an unpublished preprint of T.J. Ford from circa 1995 [Fo95], Theorem 3 appears in the case in which a and b are irreducible (from which the general case follows by bimultiplicativity). Ford deduces it from a reciprocity law in the Brauer group of $\mathbb{R}(t)$. On the one hand, this is an amusingly erudite proof of such a simple result, and this informed our decision to include a straightforward, elementary proof. On the other hand, Ford's approach is quite interesting. It may be possible to prove our Theorem 9 via similar Brauer group considerations. (For starters: If k is perfect procyclic and *not* real-closed, then the Brauer group of $k(\!(t)\!)$ is canonically isomorphic to $\operatorname{Hom}(\mathfrak{g}_K, \mathbb{Q}/\mathbb{Z})$, which is a subgroup of $\mathbb{Q}/\mathbb{Z}$. If k is real-closed then the Brauer group of $k(\!(t)\!)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.)

3.4. **Reciprocity by resultant over $\mathbb{Z}$.** We conclude with a brief discussion of proofs of quadratic reciprocity in $\mathbb{Z}$ that go via the primordial reciprocity law. Here we relied on Lemmermeyer's invaluable compendium [Le] to locate relevant references.

In 1876, Kronecker [Kr76] showed that for all odd coprime positive integers a, b, the Jacobi symbol $\left(\frac{a}{b}\right)$ satisfies

$$\left(\frac{a}{b}\right) = \operatorname{sgn}\left(\prod_{\substack{0<u<a/2 \\ 0<v<b/2}} \left(\frac{u}{a} - \frac{v}{b}\right)\right). \tag{10}$$

The right-hand side of (10) can be interpreted as the sign of a resultant: Let f be any real-valued, strictly decreasing function on $[0,1/2]$. For each odd positive integer m, put

$$\Psi_m(x) \coloneqq \prod_{0<w<m/2} \left(x - f\left(\frac{w}{m}\right)\right),$$

so that $\Psi_m(x) \in \mathbb{R}[x]$ is monic of degree $\frac{m-1}{2}$. Since $\frac{u}{a} - \frac{v}{b}$ has the same sign as $f\left(\frac{v}{b}\right) - f\left(\frac{u}{a}\right)$, eq. (10) implies that

$$\left(\frac{a}{b}\right) = \operatorname{sgn} \operatorname{Res}(\Psi_b, \Psi_a). \tag{11}$$

Theorem 1b) follows immediately via the primordial reciprocity law.

Introducing resultants in this way appears somewhat perverse: the identity (10) on its own immediately implies the reciprocity law! But for certain f, one can prove (11) independently of (10), and thus derive a fresh proof of Theorem 1. Pocklington [Po44], explicitly motivated by (10), proves (11) directly for (distinct, odd) primes a, b, and $f(x) = 2\cos(2\pi x)$. Theorem 1a) follows immediately. See [ACL13] for a different proof of (11) for prime a, b, with the same $f(x)$. Taking instead $f(x) = 2\cos(2\pi x) - 2 = -4\sin^2(\pi x)$, Hambleton and Scharashkin prove (11) for primes a, b in [HS10]. Already in 1900, Fischer [Fi00] had shown that $\left(\frac{a}{b}\right) = \operatorname{sgn} \operatorname{Res}(\Phi_a, \Phi_b)$ for all odd coprime positive a, b, where now $f(x) = 4\sin^2(\pi x)$. This last $f(x)$ is increasing on $[0,1/2]$ rather than decreasing, which explains why the roles of a and b are reversed vis-à-vis (11); of course this does not affect the deduction of the reciprocity law. We remark that for all of these (closely related) choices of f, each of the polynomials $\Psi_m(x)$ belong to $\mathbb{Z}[x]$, and all of the resultants that appear come out as ± 1, so that in fact it is not necessary to apply the sgn function.

4. Acknowledgments

We thank Daniel B. Shapiro for suggesting we consider the examples of Artin-Quigley.

References

[ACL13] ACL (`https://mathoverflow.net/users/10696/acl`), *What's the "best" proof of quadratic reciprocity?*, MathOverflow, URL: `https://mathoverflow.net/q/128198` (version: 2013-04-20)

[C] N.G. Chebotarev, *Galois Theory.* United Scientific-Technical Publishing House, NKTP, USSR. Moscow, Leningrad, 1936. (Russian)

[Cl-FT] P.L. Clark, *Field Theory.* URL: `http://math.uga.edu/~pete/FieldTheory.pdf`

[De57] R. Dedekind, *Abriss einer Theorie der höheren Kongruenzen in Bezug auf einer reellen Primzahl-Modulus.* J. Reine Angew. Math. 54 (1857), 1–26.

[E] I. Efrat, *Valuations, orderings, and Milnor K-theory.* Mathematical Surveys and Monographs, 124. American Mathematical Society, Providence, RI, 2006.

[Fi00] E. Fischer, *Ueber Eisenstein's Beweis des quadratischen Reciprocitätsgesetzes*, Monatsh. f. Math. 11 (1900), 176–182.

[Fo95] T.J. Ford, *Division algebras and quadratic reciprocity*, preprint. URL: `http://math.fau.edu/ford/preprints/darff/darff.pdf`

[Ge04] L.J. Gerstein, *On representation by quadratic $\mathbb{F}_q[x]$-lattices.* Algebraic and arithmetic theory of quadratic forms, 129–134, Contemp. Math., 344, Amer. Math. Soc., Providence, RI, 2004.

[HS10] S. Hambleton and V. Scharaschkin, *Quadratic reciprocity via resultants.* Int. J. Number Theory 6 (2010), 1413–1417.

[Hs03] C.-N. Hsu, *On polynomial reciprocity law.* J. Number Theory 101 (2003), 13-–31.

[Kn66a] J.T. Knight, *Quadratic forms over $\mathbb{R}(t)$.* Proc. Cambridge Philos. Soc. 62 (1966), 197-–205.

[Kn66b] ———, *Binary integral quadratic forms over $\mathbb{R}(t)$.* Proc. Cambridge Philos. Soc. 62 (1966), 433—440.

[Kr76] L. Kronecker, *Ueber das Reciprocitätsgesetz.* Monatsber. Berlin (1876), 331–341; Werke II, 11–23.

[Kü02] H. Kühne, *Eine Wechselbeziehung zwischen Funktionen mehrerer Unbestimmter, die zu Reziprozitätsgesetzen führt.* J. Reine Angew. Math. 124 (1902), 121–133.

[Le] F. Lemmermeyer, *Proofs of the quadratic reciprocity law.* URL: `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`

[Le67] W. Leahey, *Sums of squares of polynomials with coefficients in a finite field.* Amer. Math. Monthly 74 (1967), 816–819.

[My83] G. Myerson, *On resultants.* Proc. Amer. Math. Soc. 89 (1983), 419-–420.

[My90] ———, *Norms in polynomial rings.* Bull. Amer. Math. Soc. 41 (1990), 381–386.

[Or34] O. Ore, *Contributions to the theory of finite fields.* Trans. Amer. Math. Soc. 36 (1934), 243–274.

[Po44] H.C. Pocklington, *Quadratic and higher reciprocity of modular polynomials.* Proc. Cambridge Phil. Soc. 40 (1944), 212–214.

[Qu62] F. Quigley, *Maximal subfields of an algebraically closed field not containing a given element.* Proc. Amer. Math. Soc. 13 (1962), 562–566.

[R] M. Rosen, *Number theory in function fields.* Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.

[S] J.-P. Serre, *Corps Locaux.* Hermann, Paris, 1962.

[Sc27] F.K. Schmidt, *Zur Zahlentheorie in Körpern von der Charakteristik p*, Sitz. Phys-Med Soc. zu Erlangen 58-59 (1926–1927), 159–172.

[T] D. Thakur, *Function field arithmetic.* World Scientific Publishing Co., Inc., River Edge, NJ, 2004.