QUADRATIC RECIPROCITY IN CHARACTERISTIC 2

KEITH CONRAD

1. Introduction

Let $\mathbf{F}$ be a finite field. When $\mathbf{F}$ has odd characteristic, the quadratic reciprocity law in $\mathbf{F}[T]$ lets us decide whether or not a quadratic congruence $f \equiv x^2 \bmod \pi$ is solvable, where the modulus π is irreducible in $\mathbf{F}[T]$ and $f \not\equiv 0 \bmod \pi$. This is similar to the quadratic reciprocity law in $\mathbf{Z}$. We want to develop an analogous reciprocity law when $\mathbf{F}$ has characteristic 2.

At first it does not seem that there is an analogue: when $\mathbf{F}$ has characteristic 2, every element of the finite field $\mathbf{F}[T]/\pi$ is a square, so the congruence $f \equiv x^2 \bmod \pi$ is always solvable (and uniquely, at that). This is uninteresting. The correct quadratic congruence to try to solve in characteristic 2 is

$$f \equiv x^2 + x \bmod \pi.$$

One reason that $x^2 + x$ in characteristic 2 is the right analogue of x^2 outside of characteristic 2 is that both are related to normalized quadratic polynomials with distinct roots. Outside of characteristic 2, any quadratic polynomial $h(x) = x^2 + ax + b$ can have its linear term removed by completing the square:

$$x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4},$$

which, after rewriting $x + a/2$ as x, looks like $x^2 - d$ for $d = (a^2 - 4b)/4$. Note $a^2 - 4b$ is the discriminant of $h(x)$, so the polynomial has distinct roots (possibly lying in a larger field) exactly when $d \neq 0$.

In characteristic 2, a quadratic polynomial with distinct roots *must* have a linear term, since a double root r (possibly in a larger field) yields a polynomial

$$(x - r)^2 = x^2 - r^2,$$

where the linear term does not occur. Given a quadratic $h(x) = x^2 + ax + b$ with a linear term, so $a \neq 0$, we can't complete the square but we can simplify the shape of the polynomial as

$$\frac{h(x)}{a^2} = \left(\frac{x}{a}\right)^2 + \frac{x}{a} + \frac{b}{a^2}.$$

Rewriting x/a as x, this polynomial has the form $x^2 + x + c$. This passage from $x^2 + ax + b$ to $x^2 + x + c$ is the characteristic 2 analogue of completing the square.

While squaring is multiplicative ($(xy)^2 = x^2y^2$), the function $\wp(x) = x^2 + x$ in characteristic 2 is additive:

$$\wp(x + y) = (x + y)^2 + x + y = x^2 + y^2 + x + y = \wp(x) + \wp(y).$$

Also,

$$\wp(x)^2 = (x^2 + x)^2 = x^4 + x^2 = \wp(x^2),$$

so $\wp$ commutes with squaring. For fields F, squaring on $F^\times$ (multiplicative group) outside of characteristic 2 is analogous to applying $\wp$ on F (additive group) in characteristic 2. For instance, if r is a root of $x^2 = a$ and $a \neq 0$ then the two roots are $\pm r$, while in characteristic 2 if r is a root of $x^2 + x = a$ (any a) then the roots are r and $r + 1$. The role of $\{\pm 1\}$ (solutions to $x^2 = 1$) outside of characteristic 2 is played by $\{0, 1\}$ (solutions to $x^2 + x = 0$) in characteristic 2. Table 1 summarizes the analogies.

char $F \neq 2$	char $F = 2$
$F^\times$	F
x^2	$\wp(x)$
$x^2 - d, d \neq 0$	$\wp(x) + c$
$x^2 = y^2 \Leftrightarrow x = \pm y$	$\wp(x) = \wp(y) \Leftrightarrow x = y$ or $y + 1$
± 1	0, 1

TABLE 1. Analogies in characteristic 2

Here is an outline of the remaining sections. In Section 2, we define a quadratic residue symbol on $\mathbf{F}[T]$ when $\mathbf{F}$ has characteristic 2, verify a few of its properties, and state the quadratic reciprocity law on $\mathbf{F}[T]$. Section 3 defines the trace on finite fields and shows its relevance to the characteristic 2 quadratic residue symbol. The quadratic reciprocity law is proved in Section 4 and applications are given in Section 5. A second proof of the quadratic reciprocity law is given in Section 6 using residues of differential forms. Finally, in Section 7 we generalize quadratic reciprocity in characteristic 2 to p-power reciprocity on $\mathbf{F}[T]$ when $\mathbf{F}$ is a finite field with characteristic p.

The notation $\mathbf{F}$ *is always meant to be a finite field, which except in Sections* 3 *and* 7 *has characteristic* 2.

2. The characteristic 2 quadratic residue symbol

Definition 2.1. For monic irreducible π in $\mathbf{F}[T]$ and any $f \in \mathbf{F}[T]$, set

$$[f, \pi) = \begin{cases} 0, & \text{if } f \equiv x^2 + x \bmod \pi \text{ for some } x \in \mathbf{F}[T], \\ 1, & \text{if } f \not\equiv x^2 + x \bmod \pi \text{ for any } x \in \mathbf{F}[T]. \end{cases}$$

The values 0 and 1 for $[f, \pi)$ are understood to live in characteristic 2.

Example 2.2. In Table 2 we list $x^2 + x$ as x runs over $\mathbf{F}_2[T]/(T^3 + T + 1)$. For instance, $[T + 1, T^3 + T + 1) = 1$ since $T + 1$ does not occur in the right column.

The classical Legendre symbol $(\frac{\cdot}{p})$ for $p \neq 2$ has its "multiplicative" values ± 1 defined on integers not divisible by p, while we set $(\frac{a}{p}) = 0$ in the singular case $a \equiv 0 \bmod p$ in order that the Legendre symbol is multiplicative in a for all a. By contrast, the symbol $[\cdot, \pi)$ has its two "additive" values 0 and 1 defined on all of $\mathbf{F}[T]$ without the need for a third value to cover any kind of singular case. (This is related to the fact that $x^2 + x + c$ never has multiple roots in characteristic 2 while $x^2 - d$ in characteristic not 2 has multiple roots if $d = 0$.)

We write the characteristic 2 symbol as $[f, \pi)$, with a square bracket next to f, because this symbol will behave additively in f rather than multiplicatively. The notation will serve as a reminder that the symbol is not multiplicative in f.

To get used to the notation, we prove two quick results.

x	$x^2 + x \bmod T^3 + T + 1$
0	0
1	0
T	$T^2 + T$
$T + 1$	$T^2 + T$
T^2	T
$T^2 + 1$	T
$T^2 + T$	T^2
$T^2 + T + 1$	T^2

TABLE 2. Computing $[f, T^3 + T + 1)$ in $\mathbf{F}_2[T]$

Theorem 2.3. *For $f \in \mathbf{F}[T]$, the number of solutions to $x^2 + x \equiv f \bmod \pi$ is $1 + (-1)^{[f,\pi)}$.*

The sum $1 + (-1)^{[f,\pi)}$ is understood to live in characteristic 0. It is either 0 or 2.

Proof. When there is a solution, adding 1 to it gives another solution, so there are two solutions. In this case, $1 + (-1)^{[f,\pi)} = 2$. When there is no solution, $[f, \pi) = 1$ and $1 + (-1)^{[f,\pi)} = 0$. □

Theorem 2.3 is analogous to the formula $1 + (\frac{a}{p})$ for the number of solutions to $x^2 \equiv a \bmod p$ when $p \neq 2$, which holds for all integers a (including $a \equiv 0 \bmod p$).

Theorem 2.4. *For f and g in $\mathbf{F}[T]$ with $f \not\equiv 0 \bmod \pi$, the congruence $x^2 + fx + g \equiv 0 \bmod \pi$ is solvable if and only if $[g/f^2, \pi) = 0$, where g/f^2 is interpreted as an element of $\mathbf{F}[T]/\pi$.*

Proof. Solvability of $x^2 + c_1x + c_2 = 0$ in a field of characteristic 2 is equivalent to solvability of $x^2 + x + c_2/c_1^2 = 0$ in that field by the characteristic 2 analogue of completing the square. □

Theorem 2.4 is analogous to the solvability of $x^2 + ax + b \equiv 0 \bmod p$ being equivalent to $(\frac{a^2-4b}{p}) = 1$ when $a^2 - 4b \not\equiv 0 \bmod p$.

Now we will start working out properties of the symbol $[f, \pi)$ that will help us prove a reciprocity law for this symbol.

Lemma 2.5. *For irreducible π in $\mathbf{F}[T]$, half the elements of $\mathbf{F}[T]/\pi$ are $\wp$-values:*

$$|\{g^2 + g \bmod \pi\}| = \frac{q^{\deg \pi}}{2},$$

where $q = |\mathbf{F}|$.

Lemma 2.5 is analogous to the fact that $(\mathbf{Z}/p)^\times$ contains $(p-1)/2$ squares when $p \neq 2$. Since $\mathbf{F}[T]/\pi$ has size $q^{\deg \pi}$, which is even (q is a power of 2), $q^{\deg \pi}$ is analogous to the size of $(\mathbf{Z}/p)^\times$, which is $p - 1$.

Proof. For g and h in $\mathbf{F}[T]$,

$$\begin{aligned} g^2 + g \equiv h^2 + h \bmod \pi &\iff (g-h)^2 \equiv g - h \bmod \pi \\ &\iff g - h \equiv 0 \text{ or } 1 \bmod \pi \\ &\iff g \equiv h \text{ or } h + 1 \bmod \pi. \end{aligned}$$

Therefore the function $g \bmod \pi \mapsto g^2 + g \bmod \pi$ is 2-to-1, so the number of values is half the size of $\mathbf{F}[T]/\pi$. □

Lemma 2.5 is illustrated by Table 2, where 4 out of 8 values occur on the right side, and each value appearing occurs twice.

Theorem 2.6. *The symbol* $[f, \pi)$ *has the following properties:*

(1) *if* $f_1 \equiv f_2 \bmod \pi$ *then* $[f_1, \pi) = [f_2, \pi)$,
(2) $[f, \pi) \equiv f + f^2 + f^4 + f^8 + \cdots + f^{q^{\deg \pi}/2} \bmod \pi$, *where* $q = |\mathbf{F}|$,
(3) $[f_1 + f_2, \pi) = [f_1, \pi) + [f_2, \pi)$,
(4) $[f^2 + f, \pi) = 0$, *or equivalently* $[f^2, \pi) = [f, \pi)$.

The first property is the analogue of $(\frac{a}{p})$ only depending on a modulo p. The second property is an additive analogue of Euler's congruence $(\frac{a}{p}) \equiv a^{(p-1)/2} \bmod p$. The third property is analogous to multiplicativity of the Legendre symbol and the fourth property is analogous to $(\frac{a^2}{p}) = 1$ for $a \not\equiv 0 \bmod p$.

Proof. The first property is immediate from the definition of $[f, \pi)$.

To show the second property, let $g = f + f^2 + \cdots + f^{q^{\deg \pi}/2}$. Since $f^{q^{\deg \pi}} \equiv f \bmod \pi$,

$$g^2 = f^2 + f^4 + \cdots + f^{q^{\deg \pi}} \equiv g \bmod \pi.$$

Therefore $g \equiv 0$ or $1 \bmod \pi$. Writing g in terms of f again,

$$f + f^2 + f^4 + \cdots + f^{q^{\deg \pi}/2} \equiv 0 \text{ or } 1 \bmod \pi. \tag{2.1}$$

(This is analogous to $a^{(p-1)/2} \equiv \pm 1 \bmod p$ when $a \not\equiv 0 \bmod p$.) Let $S_\pi(x) = x + x^2 + x^4 + \cdots + x^{q^{\deg \pi}/2}$, so (2.1) says the values of $S_\pi(x)$ on $\mathbf{F}[T]/\pi$ are only 0 and 1. We want to show $S_\pi(f) \equiv 0 \bmod \pi$ exactly when f is a $\wp$-value modulo π.

The polynomials $S_\pi(x)$ and $\wp(x)$ commute in characteristic 2:

$$\begin{aligned} S_\pi(\wp(x)) &= \wp(x) + \wp(x)^2 + \cdots + \wp(x)^{q^{\deg \pi}/2} \\ &= \wp(x) + \wp(x^2) + \cdots + \wp(x^{q^{\deg \pi}/2}) \\ &= \wp(x + x^2 + \cdots + x^{q^{\deg \pi}/2}) \\ &= \wp(S_\pi(x)). \end{aligned}$$

Therefore, for $h \in \mathbf{F}[T]$ we have

$$S_\pi(\wp(h)) = \wp(S_\pi(h)) \equiv 0 \bmod \pi$$

since $S_\pi(h) \equiv 0$ or $1 \bmod \pi$ and $\wp$ vanishes at 0 and 1. This shows all $\wp$-values on $\mathbf{F}[T]/\pi$ are roots of $S_\pi(x)$. The polynomial $S_\pi(x)$ has degree $q^{\deg \pi}/2$, so it has at most $q^{\deg \pi}/2$ roots in a field. Since there are $q^{\deg \pi}/2$ $\wp$-values on $\mathbf{F}[T]/\pi$ by Lemma 2.5, the roots of $S_\pi(x)$ in $\mathbf{F}[T]/\pi$ are exactly the $\wp$-values. Therefore $S_\pi(f) \equiv 0 \bmod \pi$ if and only if $[f, \pi) = 0$. This settles the first property of the symbol.

To show $[f, \pi)$ is additive in f, we use additivity of $S_\pi(x)$:

$$\begin{aligned} [f_1 + f_2, \pi) &\equiv S_\pi(f_1 + f_2) \bmod \pi \\ &\equiv S_\pi(f_1) + S_\pi(f_2) \bmod \pi \\ &\equiv [f_1, \pi) + [f_2, \pi) \bmod \pi. \end{aligned}$$

Since $[f_1 + f_2, \pi)$ and $[f_1, \pi) + [f_2, \pi)$ are both in $\{0, 1\}$, their congruence modulo π implies their equality.

The final property of the symbol is immediate from its definition, and we can rewrite it as $[f^2, \pi) = [f, \pi)$ by additivity. $\square$

Example 2.7. We compute $[T^3+T, T^3+T^2+1)$ in $\mathbf{F}_2[T]$. Here $q=2$ and $\deg\pi=3$. Reducing the first component modulo the second, the symbol equals $[T^2+T+1, T^3+T^2+1)$, which is the same as $[1, T^3+T^2+1)$ since T^2+T has no effect in the left component (like a square factor in the numerator of a Legendre symbol). By the second property in Theorem 2.6 ("Euler's congruence"),

$$[1, T^3+T^2+1) \equiv 1+1^2+1^4 \bmod T^3+T^2+1,$$

so the symbol equals 1.

Since the Legendre symbol $(\frac{a}{p})$ is multiplicative in a, its evaluation is reduced to the cases when a is -1, 2, or an odd prime $q \neq p$. These cases are settled by the main law of quadratic reciprocity for $(\frac{q}{p})$ (first proved by Gauss) and the two supplementary laws for $(\frac{-1}{p})$ and $(\frac{2}{p})$. There is another formulation of the quadratic reciprocity law, in terms of periodicity in the denominator: for any nonzero integer a and positive primes p and q,

$$p \equiv q \bmod 4a \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right), \quad p \equiv -q \bmod 4a \Longrightarrow \left(\frac{a}{p}\right) = (\operatorname{sgn} a)\left(\frac{a}{q}\right),$$

where $\operatorname{sgn} a$ is the sign of a. We will call this periodicity Euler's reciprocity law, since it is in this form that Euler found the law. It is equivalent to the usual form of the quadratic reciprocity law (the main law and the two supplementary laws).

Euler's way of stating quadratic reciprocity for $\mathbf{Z}$ does not involve reciprocation, but it is the better way of thinking about quadratic reciprocity to understand the characteristic 2 situation. The reason is that the characteristic 2 quadratic residue symbol $[f,\pi)$ is additive in f, not multiplicative in f, so we can't reduce its calculation to the case of prime f and a reciprocation of terms. It turns out, however, that $[f,\pi)$ is essentially periodic in π. Taking Euler's point of view, this periodicity is reasonably called a reciprocity law.

To formulate the way in which $[f,\pi)$ is periodic in π, we use the following way of turning polynomials in $\mathbf{F}[T]$ into polynomials in $\mathbf{F}[1/T]$.

Definition 2.8. For nonzero $h = c_dT^d + c_{d-1}T^{d-1} + \cdots + c_1T + c_0$ in $\mathbf{F}[T]$ of degree d, define

$$h^* = \frac{h}{T^d} = c_d + \frac{c_{d-1}}{T} + \cdots + \frac{c_0}{T^d}.$$

Example 2.9. If $h = T^5+T+1$, then $h^* = 1 + 1/T^4 + 1/T^5$, *not* $1+1/T+1/T^5$.

Example 2.10. If $h = T^n$, then $h^* = 1$.

Viewing h^* as a polynomial in $\mathbf{F}[1/T]$, its degree in $1/T$ is at most the degree of h in T. There is equality if and only if $h(0) \neq 0$. For example, if h is any irreducible in $\mathbf{F}[T]$ other than a scalar multiple of T, then h and h^* have the same degree as polynomials (in T and $1/T$). Since $c_d \neq 0$, h^* has nonzero constant term. Thus, as a polynomial in $1/T$, any h^* is relatively prime to $1/T$ in $\mathbf{F}[1/T]$.

Here is a preliminary version of the main law of quadratic reciprocity in $\mathbf{F}[T]$.

Theorem 2.11. *Let $f \in \mathbf{F}[T]$ be nonconstant with degree $m \geq 1$ and assume $f(0) = 0$. Then the symbol $[f,\pi)$ depends on a congruence condition on π^*. More precisely, for irreducible π_1 and π_2 in $\mathbf{F}[T]$,*

$$\pi_1^* \equiv \pi_2^* \bmod 1/T^{m+1} \Longrightarrow [f,\pi_1) = [f,\pi_2).$$

The irreducibles π_1 and π_2 in Theorem 2.11 need not be monic.

The reciprocity law in Theorem 2.11 is not quite flexible enough to be used in a systematic calculation of $[f, \pi)$. For instance, it doesn't help us treat the case where $f(0) \neq 0$. To handle that, we will need a supplementary law. Moreover, it is better to define a Jacobi-like symbol $[f, g)$ where g is not necessarily irreducible. This will be carried out in Section 4.

3. Traces

The polynomial $S_\pi(x) = x + x^2 + x^4 + x^8 + \cdots + x^{q^{\deg \pi}/2}$ showed up in the proof of Theorem 2.6. It was computed on elements of the field $\mathbf{F}[T]/\pi$ and its values were in the subfield $\mathbf{F}_2 = \{0, 1\}$. There are similar polynomials defined relative to any extension of finite fields. We will define them in general, although our eventual application will only be to characteristic 2.

Definition 3.1. Let $\mathbf{F}' \supset \mathbf{F}$ be an extension of finite fields, with $r = |\mathbf{F}|$ and $r^d = |\mathbf{F}'|$. The *trace polynomial* from $\mathbf{F}'$ to $\mathbf{F}$ is

$$\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(x) = x + x^r + x^{r^2} + \cdots + x^{r^{d-1}}.$$

The terms in the trace polynomial are successive iterations of the r-th power map, where r is the size of the smaller field $\mathbf{F}$, and the total number of terms in the polynomial is d, where $d = [\mathbf{F}' : \mathbf{F}]$. (The trace can be defined for arbitrary finite extensions of fields, not necessarily finite fields, but it is not a polynomial function anymore.)

Example 3.2. If $c \in \mathbf{F}$ then $c^{r^i} = c$ for all i, so $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(c) = dc$.

Example 3.3. In the proof of Theorem 2.6, $S_\pi(x) = \mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_2}(x)$.

Theorem 3.4. *Viewing $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(x)$ as a function $\mathbf{F}' \to \mathbf{F}'$, it is $\mathbf{F}$-linear and its image is $\mathbf{F}$.*

Proof. Since the r-th power map is $\mathbf{F}$-linear on $\mathbf{F}'$, the trace polynomial is an $\mathbf{F}$-linear function on $\mathbf{F}'$.

For $c \in \mathbf{F}'$, $c^{r^d} = c$. Therefore $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(c)$ satisfies $x^r = x$. The solutions to this equation in $\mathbf{F}'$ are the elements of $\mathbf{F}$, so $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(c) \in \mathbf{F}$.

To show $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}$ takes on every value in $\mathbf{F}$, it suffices by $\mathbf{F}$-linearity to show $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}$ is not identically zero. Since it is a polynomial function of degree r^{d-1}, while $|\mathbf{F}'| > r^{d-1}$, it can't vanish on all of $\mathbf{F}'$. □

Theorem 3.5. *Let $\mathbf{F}'/\mathbf{F}$ be an extension of finite fields of degree d and let α be a field generator: $\mathbf{F}' = \mathbf{F}(\alpha)$. Then, for $c \in \mathbf{F}$ and any $n \geq 1$, $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(c\alpha^n)$ is c times the sum of the n-th powers of the roots of the monic minimal polyomial of α in $\mathbf{F}[T]$. In particular, writing this minimal polynomial as $T^d + c_{d-1}T^{d-1} + \cdots + c_0$, we have $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(\alpha) = -c_{d-1}$.*

Proof. Since α is a field generator for $\mathbf{F}'$ over $\mathbf{F}$, the different roots of its minimal polynomial in $\mathbf{F}[T]$ are $\alpha, \alpha^r, \alpha^{r^2}, \ldots, \alpha^{r^{d-1}}$, and the trace of $c\alpha^n$ is the sum of the powers $(c\alpha^n)^{r^i} = c(\alpha^{r^i})^n$ for $0 \leq i \leq d-1$. Factoring the monic minimal polynomial as

$$(T - \alpha)(T - \alpha^r) \cdots (T - \alpha^{r^{d-1}}),$$

the sum of the α^{r^i}'s is the negative of the coefficient of T^{d-1}. □

Theorem 3.6. *Let $\mathbf{F}'' \supset \mathbf{F}' \supset \mathbf{F}$ be extensions of finite fields. Then we have the polynomial identity*

$$\mathrm{Tr}_{\mathbf{F}''/\mathbf{F}}(x) = \mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(\mathrm{Tr}_{\mathbf{F}''/\mathbf{F}'}(x)).$$

This property is called transitivity of the trace.

Proof. Let $r = |\mathbf{F}|$, $m = [\mathbf{F}' : \mathbf{F}]$, and $n = [\mathbf{F}'' : \mathbf{F}']$. Then $\mathrm{Tr}_{\mathbf{F}''/\mathbf{F}}(x)$ is the sum of terms x^{r^i} for $0 \leq i \leq mn - 1$. That $\mathrm{Tr}_{\mathbf{F}'/\mathbf{F}}(\mathrm{Tr}_{\mathbf{F}''/\mathbf{F}'}(x))$ is the same sum is left to the reader. □

Corollary 3.7. *Let π be irreducible in $\mathbf{F}[T]$, where $\mathbf{F}$ has characteristic p. For $c \in \mathbf{F}$, $\mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_p}(c) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_p}(c) \deg \pi \bmod p$.*

Proof. Apply transitivity to the field extensions $\mathbf{F}[T]/\pi \supset \mathbf{F} \supset \mathbf{F}_p$, noting $c \in \mathbf{F}$:

$$\begin{aligned}
\mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_p}(c) &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_p}(\mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}}(c)) \\
&= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_p}([\mathbf{F}[T]/\pi : \mathbf{F}]c) \\
&= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_p}((\deg \pi)c) \\
&= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_p}(c) \deg \pi \bmod p.
\end{aligned}$$

□

The trace is connected to the quadratic residue symbol in characteristic 2 because $S_\pi(x)$ is a trace. The second property in Theorem 2.6, which involves $S_\pi(f)$, is equivalent to

$$[f, \pi) = \mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_2}(f \bmod \pi). \tag{3.1}$$

Using (3.1) and properties of the trace, we now evaluate $[f, \pi)$ when $\deg f \leq 1$.

Theorem 3.8. *For $c \in \mathbf{F}$, $[c, \pi) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c) \deg \pi \bmod 2$.*

Proof. Use (3.1) and Corollary 3.7. □

Example 3.9. Taking $\mathbf{F} = \mathbf{F}_2$, $[1, \pi) = \deg \pi \bmod 2$. For instance, $[1, T^3 + T + 1) = 3 \equiv 1 \bmod 2$. This is consistent with Table 2, where 1 does not occur in the second column.

Theorem 3.10. *Write the irreducible π in $\mathbf{F}[T]$ as $a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0$, with $a_d \neq 0$. Then, for $c \in \mathbf{F}$, $[cT, \pi) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c a_{d-1}/a_d)$.*

Proof. Both sides vanish when $c = 0$, so we may take $c \in \mathbf{F}^\times$.

In the field $\mathbf{F}[T]/\pi$, cT is a field generator over $\mathbf{F}$ and a minimal polynomial for $cT \bmod \pi$ over $\mathbf{F}$ is $\pi(X/c) = (a_d/c^d)X^d + (a_{d-1}/c^{d-1})X^{d-1} + \cdots + a_0$. Make this monic by division by a_d/c^d, giving $X^d + (c a_{d-1}/a_d)X^{d-1} + \cdots$. Then, by transitivity of the trace and Theorem 3.5, from (3.1) we get

$$\begin{aligned}
[cT, \pi) &= \mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_2}(cT) \\
&= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(\mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}}(cT)) \\
&= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(-c a_{d-1}/a_d).
\end{aligned}$$

Since we are in characteristic 2, $-1 = 1$. □

Example 3.11. In $\mathbf{F}_2[T]$, $[T, T^3 + T + 1) = 0$ since the coefficient of T^2 in $T^3 + T + 1$ is 0. This is consistent with Table 2, since $T \equiv \wp(T^2) \bmod T^3 + T + 1$.

Theorem 3.10 suggests the evaluation of $[f, \pi)$ is going to be more closely related to the top terms in π than to the bottom terms. So we don't expect $[f, \pi)$, for fixed f and varying π, to be determined by a congruence condition on π in $\mathbf{F}[T]$. To turn the top terms of π into bottom terms of a polynomial, we will work with π^* in $\mathbf{F}[1/T]$ (Definition 2.8).

Example 3.12. Fix a polynomial of degree at most one, $c_0 + c_1 T \in \mathbf{F}[T]$. For irreducible π,

$$[c_0 + c_1 T, \pi) = [c_0, \pi) + [c_1 T, \pi).$$

By Theorems 3.8 and 3.10, $[c_0 + c_1 T, \pi)$ is determined by $\deg \pi \bmod 2$ and $\pi^* \bmod 1/T^2$.

4. The quadratic reciprocity law for $\mathbf{F}[T]$

The best way to formulate the quadratic reciprocity law in characteristic 2 is not just in the form of Theorem 2.11 for $[f, \pi)$, but with a symbol allowing a composite second coordinate. We extend the second coordinate of our quadratic symbol $[\cdot, \cdot)$ multiplicatively (well, "logarithmically") to all nonzero elements of $\mathbf{F}[T]$: when $g = \pi_1 \cdots \pi_n$ with irreducible π_i (not necessarily monic or distinct), define

$$[f, g) := [f, \pi_1) + \cdots + [f, \pi_n).$$

This is well-defined in g.

As examples $[f, T^3 + 1) = [f, T + 1) + [f, T^2 + T + 1)$ and $[f, T^n) = 0$ if n is even. For instance, $[f, 1) = 0$.

The following properties of $[f, g)$ are immediate consequences of its definition or of properties of $[f, \pi)$:

- if $f_1 \equiv f_2 \bmod g$, then $[f_1, g) = [f_2, g)$,
- $[f_1 + f_2, g) = [f_1, g) + [f_2, g)$,
- $[f, g_1 g_2) = [f, g_1) + [f, g_2)$,
- $[\wp(f), g) = 0$.

Example 4.1. Write $g = a_d T^d + a_{d-1} T^{d-1} + \cdots$. Then

$$[c, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c)(\deg g) \bmod 2, \quad [cT, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\left(\frac{c a_{d-1}}{a_d}\right)$$

since Theorems 3.8 and 3.10 give these formulas when g is irreducible and both sides of the formulas are logarithmic in g.

To calculate $[cT^2, g)$, write $c = b^2$ for some $b \in \mathbf{F}$. Then $cT^2 = \wp(bT) + bT$, so $[cT^2, g) = [bT, g)$.

Here is the statement of quadratic reciprocity, which includes Theorem 2.11 and Example 4.1 as special cases. It is due to Hasse [2].

Theorem 4.2. *For fixed f in $\mathbf{F}[T]$, the symbol $[f, g)$ depends on $\deg g \bmod 2$ and a congruence condition on g^*. More precisely, we have the following.*

a) For $c \in \mathbf{F}$ and nonzero $g \in \mathbf{F}[T]$, $[c, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c) \deg g \bmod 2$.

b) Suppose f has degree $m \geq 1$ and $f(0) = 0$. For nonzero g_1 and g_2 in $\mathbf{F}[T]$,

$$g_1^* \equiv g_2^* \bmod 1/T^{m+1} \Longrightarrow [f, g_1) = [f, g_2).$$

In particular, $g^* \equiv 1 \bmod 1/T^{m+1} \Longrightarrow [f, g) = 0$.

When $\mathbf{F} = \mathbf{F}_2$, $\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}$ is the identity function and part a assumes the simpler form: $[c, g) = c \deg g \bmod 2$ with $c = 0$ or 1.

Before giving a proof of Theorem 4.2, we illustrate it by making calculations of three symbols $[f, \pi)$ on $\mathbf{F}_2[T]$. Pay attention to the way reductions in $\mathbf{F}_2[1/T]$ are used.

Example 4.3. Over $\mathbf{F}_2[T]$, we compute $[T^3, T^5 + T^3 + 1)$. (The polynomial $T^5 + T^3 + 1$ is irreducible in $\mathbf{F}_2[T]$.) Since T^3 has degree 3, Theorem 4.2b tells us to work modulo $1/T^4$:

$$\begin{aligned}(T^5 + T^3 + 1)^* &\equiv 1 + 1/T^2 \bmod 1/T^4 \\ &\equiv (T^2 + 1)^* \bmod 1/T^4.\end{aligned}$$

Thus

$$[T^3, T^5 + T^3 + 1) = [T^3, T^2 + 1) = [T^3, (T + 1)^2) = 0.$$

This means the congruence $x^2 + x \equiv T^3 \bmod T^5 + T^3 + 1$ has a solution in $\mathbf{F}_2[T]$. Searching by brute force, a solution is $T^3 + T^2 + T$.

Example 4.4. Over $\mathbf{F}_2[T]$, we compute $[T^5, \pi)$, where $\pi = T^7 + T^3 + T^2 + T + 1$. The reciprocity law tells us to look at π^* mod $1/T^6$:

$$\begin{aligned}\pi^* &\equiv 1 + 1/T^4 + 1/T^5 \bmod 1/T^6 \\ &\equiv (T^5 + T + 1)^* \bmod 1/T^6.\end{aligned}$$

Thus

$$[T^5, \pi) = [T^5, T^5 + T + 1) = [T + 1, T^5 + T + 1) = [T, T^5 + T + 1) + [1, T^5 + T + 1).$$

From Example 4.1 $[1, T^5 + T + 1) = 1$ and $[T, T^5 + T + 1) = 0$ since the coefficient of T^4 in T^5+T+1 is 0. Therefore $[T^5, \pi) = 1+0 = 1$. That means the congruence $x^2+x \equiv T^5 \bmod \pi$ has no solution in $\mathbf{F}_2[T]$.

It is worth noting that T^5+T+1 is reducible in $\mathbf{F}_2[T]$. It equals $(T^2+T+1)(T^3+T^2+1)$, so it was useful to have formulas for $[1, g)$ and $[T, g)$ when g is reducible in order to avoid having to factor the modulus and make the calculation longer.

Since $[T^5, \pi) = 1$ and $[1, \pi) = 1$ too, $[T^5 + 1, \pi) = 0$. Therefore $x^2 + x \equiv T^5 + 1 \bmod \pi$ must have solutions, and in fact a solution is $T^6 + T^5 + T^3$.

Now we prove Theorem 4.2.

Proof. Part a follows immediately from Theorem 3.8, the case of irreducible g, since both sides turn products into sums through the second coordinate.

For part b, by additivity we only have to treat the case of a monomial $f = cT^m$, where $m \geq 1$. We are going to show, for nonzero $g \in \mathbf{F}[T]$, that the symbol $[cT^m, g)$ is completely determined by knowledge of g^* mod $1/T^{m+1}$.

Suppose first that π is irreducible with distinct roots $\alpha_1, \ldots, \alpha_d$ in a splitting field over $\mathbf{F}$. (Note $d = \deg \pi$.) Then

$$\begin{aligned}[cT^m, \pi) &= \mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_2}(cT^m) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(\mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}}(cT^m)) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c(\alpha_1^m + \cdots + \alpha_d^m)).\end{aligned}$$

For any nonzero g, summing this formula over the irreducible factors of g gives

$$[cT^m, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c(\alpha_1^m + \cdots + \alpha_d^m)), \tag{4.1}$$

where $d = \deg g$ and $\alpha_1, \ldots, \alpha_d$ denote the roots of g counted with multiplicity. Therefore $[cT^m, g)$ is determined by the m-th power sum of the roots of g, counted with multiplicity. (If $g \in \mathbf{F}^\times$, then this power sum is 0 and $[cT^m, g) = 0$ as well.)

From Newton's formulas for power sums in terms of elementary symmetric functions, the m-th power sum p_m of the roots is an integral polynomial in the first m elementary symmetric functions $s_1, \ldots, s_m$. (For instance, $p_1 = s_1, p_2 = s_1^2 - 2s_2$, and $p_3 = s_1^3 - 3s_1s_2 +$

$3s_3$.) The first m elementary symmetric functions of the roots of g are determined by the top $m+1$ coefficients of g. All these coefficients can be read off from g^* mod $1/T^{m+1}$, so g^* mod $1/T^{m+1}$ determines $[cT^m, g)$. □

Example 4.5. We work out an explicit formula for $[cT^3, g)$ when $g = a_dT^d + a_{d-1}T^{d-1} + \cdots$ and $d \geq 3$:

$$\begin{aligned} [cT^3, g) &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(cp_3) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c(s_1^3 - 3s_1s_2 + 3s_3)) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\left(\frac{c}{a_d^3}\left(a_{d-1}^3 + a_{d-1}a_{d-2} + a_{d-3}\right)\right). \end{aligned}$$

For instance, when $\mathbf{F} = \mathbf{F}_2$, $[T^3, T^5 + T + 1) = 0$ since $d = 5$ and $a_{d-1} = a_{d-3} = 0$. This answer agrees with the calculation in Example 4.3.

Corollary 4.6. *Let $f(T) \in \mathbf{F}[T]$ have degree m. For nonzero g_1 and g_2 in $\mathbf{F}[T]$,*

$$g_1^* \equiv g_2^* \bmod 1/T^{m+1} \Longrightarrow [f, g_1) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0))(\deg g_1 - \deg g_2) + [f, g_2).$$

Proof. Write $f = f(0) + (f - f(0))$ and apply Theorem 4.2a to $c = f(0)$ and Theorem 4.2b to $f - f(0)$. □

5. Applications

We give characteristic 2 analogues of the following applications of quadratic reciprocity on $\mathbf{Z}$:

- decide if a particular quadratic equation modulo p has solutions,
- turn the condition $(\frac{a}{n}) = 1$, for a particular choice of a, into an explicit congruence condition on n when $n > 0$,
- find the minimal period of $(\frac{a}{p})$ as a function of p,
- show that, if a is not a square, then $(\frac{a}{p}) = -1$ for infinitely many p.

Example 5.1. Does the congruence $x^2 + (T+1)x + T^5 \equiv 0 \bmod T^6 + T + 1$ have solutions in $\mathbf{F}_2[T]$?

The modulus is irreducible. Denote it by π. Following the method of proof of Theorem 2.4, we have to decide if $x^2 + x + T^5/(T+1)^2 \equiv 0 \bmod \pi$ is solvable. The constant term here is $\equiv T^4 + T^3 + T^2 + T + 1$, so we must compute $[T^4 + T^3 + T^2 + T + 1, \pi)$. Since $\pi^* \equiv 1 \bmod 1/T^5$, $[T^i, \pi) = 0$ for $1 \leq i \leq 4$, so $[T^4 + T^3 + T^2 + T + 1, \pi) = [1, \pi)$, which vanishes since $\deg \pi$ is even. Thus, the original quadratic equation does have solutions. By a brute force search, the solutions are $T^4 + T^2$ and $T^4 + T^2 + T + 1$.

Example 5.2. On $\mathbf{F}_2[T]$, describe the condition $[T^3 + T, g) = 0$ in terms of congruences on g^* mod $1/T^4$.

In Table 3, we list the units in $\mathbf{F}_2[1/T]/(1/T^4)$, a polynomial g in $\mathbf{F}_2[T]$ whose $*$-value is each unit, and the corresponding value of the symbol. From quadratic reciprocity and Table 3, $[T^3+T, g) = 0$ if and only if $g^* \equiv 1, 1+1/T, 1+1/T^2$, or $1+1/T+1/T^2+1/T^3$ mod $1/T^4$.

When a is a squarefree integer, the minimal period of $(\frac{a}{p})$ as a function of p is $|a|$ if $a \equiv 1 \bmod 4$ and $4|a|$ if $a \not\equiv 2, 3 \bmod 4$. (When a has a square factor, of course the minimal period of $(\frac{a}{p})$ is smaller, *e.g.*, $(\frac{18}{p})$ has period 8.) The characteristic 2 analogue of this question is whether or not $m + 1 = \deg f + 1$ is the minimal exponent in Theorem 4.2b

g^*	g	$[T^3+T,g)$
1	1	0
$1+1/T$	$T+1$	0
$1+1/T^2$	T^2+1	0
$1+1/T+1/T^2$	T^2+T+1	1
$1+1/T^3$	T^3+1	1
$1+1/T+1/T^3$	T^3+T^2+1	1
$1+1/T^2+1/T^3$	T^3+T+1	1
$1+1/T+1/T^2+1/T^3$	T^3+T^2+T+1	0

TABLE 3. Computing $[T^3+T,g)$ in $\mathbf{F}_2[T]$

when $f(0)=0$. To answer this, we will use the following characteristic 2 analogue of writing an integer as a perfect square times either 1 or a squarefree integer.

Lemma 5.3. *For any $f \in \mathbf{F}[T]$, we can write $f = h^2+h+k$ where h and k are in $\mathbf{F}[T]$, $h(0)=0$, and k is constant or $\deg k$ is odd.*

Proof. If f is constant or has odd degree, use $h=0$ and $k=f$. Now suppose f has positive even degree, with leading term cT^{2n}. Since $\mathbf{F}$ is finite with characteristic 2, c is a perfect square in $\mathbf{F}^\times$, say $c=b^2$. Let $g=bT^n$, so $f-(g^2+g)$ has degree less than $2n$ and the same constant term as f. If the difference is constant or has odd degree we are done. If the difference has positive even degree, then by induction $f-(g^2+g)=h^2+h+k$ with $h(0)=0$ and k is constant or has odd degree. Then

$$f = (g+h)^2 - (g+h) + k.$$

□

In the notation of Lemma 5.3, $[f,g)=[k,g)$, so the study of the symbol $[f,\cdot)$ can always suppose f is constant or has odd degree. For example, $T^6+T = \wp(T^3)+T^3+T$, so

$$[T^6+T,g) = [T^3+T,g)$$

for all g. The h and k in Lemma 5.3 are uniquely determined by f, but we don't need this and omit the proof.

Theorem 5.4. *Let $f \in \mathbf{F}[T]$ have degree $m \geq 1$ and $f(0)=0$. If $\deg f$ is even, then $[f,g)$ is determined by $g^* \bmod 1/T^{d+1}$ for some $d<m$. If $\deg f$ is odd, then $[f,g)$ is determined by $g^* \bmod 1/T^{m+1}$ and $m+1$ is the smallest exponent possible.*

Proof. Assume $m>0$ is even. Write $f=h^2+h+k$ as in Lemma 5.3. Then $k(0)=f(0)=0$ and $[f,\cdot)=[k,\cdot)$. If $k=0$ then $[f,\cdot)$ is identically 0 and we are done. Otherwise k is nonconstant and Theorem 4.2b says $[f,g)=[k,g)$ is determined by $g^* \bmod 1/T^{d+1}$ where $d=\deg k<\deg f$.

Now assume m is odd. By Theorem 4.2b, $[f,g)$ is determined by $g^* \bmod 1/T^{m+1}$. To see $m+1$ is minimal, we will find $g \in \mathbf{F}[T]$ such that $g^* \equiv 1 \bmod 1/T^m$ and $[f,g)=1$.

Write $f=a_mT^m+\cdots+a_1T$. We will use $g=b+T^m$, with $b\in\mathbf{F}$ to be determined. Note $g^*\equiv 1 \bmod 1/T^m$. We will show

$$[f,b+T^m) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(a_mb). \tag{5.1}$$

Since $a_m b$ runs over $\mathbf{F}$ as b runs over $\mathbf{F}$, and $\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\colon \mathbf{F} \to \mathbf{F}_2$ is onto, $[f, b + T^m) = 1$ for some (nonzero) b and we'd be done.

To verify (5.1), we will check $[aT^m, b+T^m) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(ab)$ for $a \in \mathbf{F}$ while $[aT^n, b+T^m) = 0$ for $a \in \mathbf{F}$ and $1 \leq n < m$. Since m is odd, $b + T^m$ has distinct roots in a splitting field over $\mathbf{F}$. Write the roots as $\alpha_1, \ldots, \alpha_m$. Let ζ be a root of unity of order m, so we can take $\alpha_i = \alpha_1\zeta^{i-1}$ for $i = 1, 2, \ldots, m$. Then, for $a \in \mathbf{F}$ and $1 \leq n \leq m$, (4.1) gives us

$$\begin{aligned} [aT^n, b + T^m) &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(a(\alpha_1^n + \cdots + \alpha_m^n)) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(a\alpha_1^n(1 + \zeta^n + \cdots + \zeta^{(m-1)n})). \end{aligned}$$

If $1 \leq n < m$, then $\sum_{i=0}^{m-1} \zeta^{in} = 0$ so $[aT^n, b + T^m) = 0$. If $n = m$, then $\sum_{i=0}^{m-1} \zeta^{in} = m$ and $[aT^m, b+T^m) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(a\alpha_1^m m) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(abm)$. Since m is an odd integer, it can be taken out of the trace and then equals 1 in characteristic 2. $\square$

For any non-square $a \in \mathbf{Z}$, $(\frac{a}{p}) = -1$ for infinitely many primes p. That is, a non-square in $\mathbf{Z}$ will be detected as a non-square modulo many primes p. This is proved using Jacobi reciprocity in [3, Theorem 3, p. 57]. Now we give an analogue in characteristic 2 with a similar argument.

Theorem 5.5. *Let $f \in \mathbf{F}[T]$. If $f \neq h^2 + h$ for any $h \in \mathbf{F}[T]$, then $[f, \pi) = 1$ for infinitely many monic irreducible π.*

Proof. By our hypotheses and Lemma 5.3, $f = h^2 + h + k$ for some h and some k that is constant or of odd degree. Since $[f, \pi) = [k, \pi)$ for all π, we may suppose f is constant or of odd degree.

Case 1: $f = c$ is constant. Then for irreducible π, $[c, \pi) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c) \deg \pi \bmod 2$. If $\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c) = 0$, then $[c, T) = 0$, so $c \equiv a^2 + a \bmod T$ for some $a \in \mathbf{F}$. Then $c = a^2 + a$ in $\mathbf{F}$, which contradicts our hypothesis on f, so $\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(c) = 1$. Therefore $[c, \pi) \equiv \deg \pi \bmod 2$, and this is 1 infinitely often by letting π run through monic irreducibles with odd degree.

Case 2: f has odd degree, say m. Let the leading term of $f(T)$ be aT^m. Write

$$\begin{aligned} [f, g) &= [f(0), g) + [f - f(0), g) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0))(\deg g) + [f - f(0), g). \end{aligned}$$

For $g = b + T^m$ (where $m = \deg f$), we have by (5.1)

$$[f - f(0), b + T^m) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(ab).$$

Therefore

$$[f, b + T^m) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0))m + \mathrm{Tr}(ab) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0)) + \mathrm{Tr}(ab).$$

If $f(0)$ has trace 0, pick b so that ab has trace 1. If $f(0)$ has trace 1, use $b = 0$. In either case we have found a g such that $[f, g) = 1$, so $[f, \pi) = 1$ for one of the monic irreducible factors π of g.

Now assume we have monic irreducible $\pi_1, \ldots, \pi_r$ such that $[f, \pi_i) = 1$ for all i. For $b \in \mathbf{F}$, suppose we can find a $g \in \mathbf{F}[T]$ such that

$$\deg g \text{ is odd}, \quad g^* \equiv 1 + b/T^m \bmod 1/T^{m+1}, \quad (g, \pi_i) = 1 \text{ for all } i. \tag{5.2}$$

(We will explain how to find g later.) Since $g^* \equiv 1 \bmod 1/T^m$, $[cT^i, g) = 0$ for $1 \leq i \leq m-1$, so

$$[f, g) = [f(0), g) + [aT^m, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0))(\deg g) + [aT^m, g).$$

Since g has odd degree and $g^* \equiv (T^m + b)^* \bmod 1/T^{m+1}$,

$$[f, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0)) + [aT^m, T^m + b) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(f(0)) + \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(ab).$$

Depending on whether the trace of $f(0)$ is 0 or 1, b can be chosen so $[f, g) = 1$. Then $[f, \pi) = 1$ for some monic irreducible π dividing g. As g is relatively prime to the π_i's, this π is not equal to any of the π_i's by (5.2). Write π as π_{r+1} and repeat the argument again, so we get $[f, \pi) = 1$ for infinitely many monic irreducible π.

It remains to construct g satisfying (5.2). The idea is to turn all conditions on g in (5.2) into conditions on g^* and then apply results from the polynomial ring $\mathbf{F}[1/T]$.

The correspondence from polynomials $g \in \mathbf{F}[T]$ with $g(0) \neq 0$ to their images $g^* \in \mathbf{F}[1/T]$ is a bijection between polynomials with nonzero constant terms in $\mathbf{F}[T]$ and $\mathbf{F}[1/T]$. This correspondence preserves degrees (that is, the degree of g in T and the degree of g^* in $1/T$ are equal) and is multiplicative ($(g_1 g_2)^* = g_1^* g_2^*$). In particular, irreducible polynomials with nonzero constant terms in $\mathbf{F}[T]$ and $\mathbf{F}[1/T]$ correspond to each other under $g \mapsto g^*$. Letting $M = \pi_1 \pi_2 \cdots \pi_r$, if $g(0) \neq 0$ then $(g, M) = 1$ in $\mathbf{F}[T]$ if and only if $(g^*, M^*) = 1$ in $\mathbf{F}[1/T]$.

Thus, replace (5.2) with

$$\deg g^* \text{ is odd }, \quad g^* \equiv 1 + b/T^m \bmod 1/T^{m+1}, \quad (g^*, M^*) = 1 \text{ for all } i.$$

Since M^* has nonzero constant term in $\mathbf{F}[1/T]$, it is relatively prime to $1/T$. We therefore can solve

$$G \equiv 1 + b/T^m \bmod 1/T^{m+1}, \quad G \equiv 1 \bmod M^*$$

for some $G \in \mathbf{F}[1/T]$ by the Chinese remainder theorem in $\mathbf{F}[1/T]$. By adding a suitable multiple of $(1/T^{m+1})M^*$ to G, we can arrange that G has odd degree in $1/T$. Since $G = g^*$ for a polynomial $g \in \mathbf{F}[T]$ with nonzero constant term, this g satisfies (5.2). $\square$

6. A proof of Theorem 4.2b by residues

Theorem 4.2 is essentially the Artin reciprocity law for quadratic extensions of a rational function field in characteristic 2. The proof of the general Artin reciprocity law in characteristic p for abelian extensions of degree divisible by p uses residues of differential forms. Here is a proof of Theorem 4.2b from this point of view, assuming the reader is familiar with residues (in particular, the residue theorem on rational function fields).

Extend the operations $g \mapsto [f, g)$ and $g \mapsto g^*$ multiplicatively from nonzero g in $\mathbf{F}[T]$ to all g in $\mathbf{F}(T)^\times$. (But still we have $f \in \mathbf{F}[T]$.) We still have $[f, g) \in \{0, 1\}$, but now view g^* in $\mathbf{F}[[1/T]]^\times$. For instance, $(1/(1+T))^* = 1/(1+1/T) = 1 - 1/T + 1/T^2 - \cdots$.

For $f \in \mathbf{F}[T]$ and irreducible $\pi \in \mathbf{F}[T]$,

$$\begin{aligned} [f, \pi) &= \mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_2}(f \bmod \pi) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}(\mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}}(f \bmod \pi)) \\ &= \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\left(\mathrm{Res}_\pi\left(f\frac{\mathrm{d}\pi}{\pi}\right)\right). \end{aligned}$$

Since $f\mathrm{d}\pi/\pi$ has no poles away from π and ∞, the residue theorem gives

$$[f, \pi) = -\,\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\left(\mathrm{Res}_\infty\left(f\frac{\mathrm{d}\pi}{\pi}\right)\right) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\left(\mathrm{Res}_\infty\left(f\frac{\mathrm{d}\pi}{\pi}\right)\right).$$

Therefore, for any $f \in \mathbf{F}[T]$ and $g \in \mathbf{F}(T)^\times$,

$$[f, g) = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_2}\left(\mathrm{Res}_\infty\left(f\frac{\mathrm{d}g}{g}\right)\right). \tag{6.1}$$

We will prove Theorem 4.2b by showing, for $f \in \mathbf{F}[T]$ and $g \in \mathbf{F}(T)^\times$, that

$$f(0) = 0, \quad g^* \equiv 1 \bmod 1/T^{m+1} \Longrightarrow [f, g) = 0. \tag{6.2}$$

By additivity in f, we can focus on $f = cT^m$ with $m \geq 1$. Let's coordinatize everything at ∞. Set $w = 1/T$. Since $g^* = g/T^{\deg g}$, $\mathrm{d}g/g = \mathrm{d}g^*/g^* + (\deg g)\mathrm{d}T/T$. Then

$$cT^m\frac{\mathrm{d}g}{g} = \frac{c}{w^m}\left(\frac{\mathrm{d}g^*}{g^*} - \deg g\frac{\mathrm{d}w}{w}\right).$$

For $m \geq 1$, it follows that

$$\mathrm{Res}_\infty\left(cT^m\frac{\mathrm{d}g}{g}\right) = \mathrm{Res}_{w=0}\left(\frac{c}{w^m}\frac{\mathrm{d}g^*}{g^*}\right).$$

We want to show this residue is 0.

Write $g^* = 1 + w^{m+1}k(w)$, where $k(w) \in \mathbf{F}[[w]]$. Then

$$\frac{\mathrm{d}g^*}{w^m} = w\mathrm{d}k + (m+1)k\mathrm{d}w,$$

so

$$\frac{c}{w^m}\frac{\mathrm{d}g^*}{g^*} = \frac{c(wk'(w) + (m+1)k)\mathrm{d}w}{g^*}.$$

Since g^* has nonzero constant term in $\mathbf{F}[[w]]$, the right side has no pole at $w = 0$, so its residue at $w = 0$ is 0. This concludes the residue-based proof of Theorem 4.2.

By the way, the reader can check that (6.1) leads to a second proof of (5.1).

7. A p-power reciprocity law in characteristic p

Let $\mathbf{F} = \mathbf{F}_q$ be a finite field with characteristic p, and $\mathbf{F}_{p^s}$ be a subfield of $\mathbf{F}$. For irreducible π in $\mathbf{F}[T]$ and $f \in \mathbf{F}[T]$, consider the equation

$$x^{p^s} - x \equiv f \bmod \pi. \tag{7.1}$$

The polynomial $\wp(x) = x^{p^s} - x$ is additive in x and commutes with the p-th power map: $\wp(x)^p = \wp(x^p)$.

Define

$$[f, \pi)_{p^s} = \mathrm{Tr}_{(\mathbf{F}[T]/\pi)/\mathbf{F}_{p^s}}(f \bmod \pi) \in \mathbf{F}_{p^s}.$$

We will go through the properties of this symbol and the reciprocity law it satisfies, without details of proofs.

The symbol $[f, \pi)_{p^s}$ is additive in f, and (7.1) has a solution in $\mathbf{F}[T]$ if and only if $[f, \pi)_{p^s} = 0$. The reciprocity law for this symbol was first treated by Hasse [2, pp. 49–50], with $s = 1$, and it is where Hasse derivatives were first introduced. See the survey paper [4] (especially Section 7.1) for an historical discussion of this work.

Extend the symbol $[\cdot, \cdot)_{p^s}$ multiplicatively in the second coordinate to all nonzero polynomials. For $c \in \mathbf{F}$ and g of degree d,

$$[c, g)_{p^s} = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_{p^s}}(c)\deg g, \quad [cT, g)_{p^s} = -\,\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_{p^s}}(ca_{d-1}/a_d),$$

where $g = a_dT^d + a_{d-1}T^{d-1} + \cdots$. Since we are not necessarily in characteristic 2, the minus sign in the second formula is essential.

Set $m = \deg f$. When $f(0) = 0$, the basic reciprocity law is: $[f, g)_{p^s}$ only depends on g^* mod $1/T^{m+1}$. In case $f(0) \neq 0$, we write this as

$$g_1^* \equiv g_2^* \bmod 1/T^{m+1} \Longrightarrow [f, g_1)_{p^s} = \mathrm{Tr}_{\mathbf{F}/\mathbf{F}_{p^s}}(f(0))(\deg g_1 - \deg g_2) + [f, g_2)_{p^s}.$$

The proof is identical to the case $p = 2$ and $s = 1$ in Corollary 4.6. A proof using residues as in Section 6 requires the formula

$$[f, g)_{p^s} = -\,\mathrm{Tr}_{\mathbf{F}/\mathbf{F}_{p^s}}\left(\mathrm{Res}_\infty\left(f\frac{\mathrm{d}g}{g}\right)\right). \tag{7.2}$$

Note the minus sign.

We conclude this discussion by noting an alternate computational formula for $[f, g)_{p^s}$ when g is monic. First consider $p^s = q$. With $d = \deg g$, write

$$f(T)g'(T) \equiv b_0 + b_1T + \cdots + b_{d-1}T^{d-1} \bmod g, \tag{7.3}$$

where $b_j \in \mathbf{F}$. Then the formula is

$$[f, g)_q = b_{d-1}. \tag{7.4}$$

Example 7.1. Over $\mathbf{F}_2[T]$, we compute $[T^3, T^5 + T^3 + 1) = [T^3, T^5 + T^3 + 1)_2$. Since

$$T^3(T^5 + T^3 + 1)' \equiv T^2 \bmod T^5 + T^3 + 1,$$

the coefficient of T^4 on the right side is 0, so the symbol is 0. This agrees with Example 4.3.

Example 7.2. We compute $[T^5, \pi)_2$, where $\pi = T^7 + T^3 + T^2 + T + 1$. Since

$$T^5\pi'(T) \equiv T^6 + T^4 \bmod \pi,$$

where the coefficient of T^6 on the right side is 1, $[T^5, \pi) = 1$. This agrees with Example 4.4.

To extend (7.4) to $[f, g)_{p^s}$, write $\mathbf{F} \cong \mathbf{F}_{p^r}[x]/R(x)$, with $R \in \mathbf{F}_{p^r}[x]$ irreducible of degree $n = [\mathbf{F} : \mathbf{F}_{p^r}]$. Viewing b_{d-1} from (7.3) inside $\mathbf{F}_{p^s}[x]/R(x)$, write

$$b_{d-1}R'(x) \equiv a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \bmod R(x).$$

Then

$$[f, g)_{p^s} = a_{n-1}. \tag{7.5}$$

Formula (7.5) (and its special case (7.4)) is an easy consequence of (7.2). When $g = \pi$ is monic irreducible, (7.4) and (7.5) were proved by Carlitz [1, Theorems 11.4, 11.5] using his characteristic p exponential function.

References

[1] L. Carlitz, "On certain functions connected with polynomials in a Galois field," *Duke Math. J.* **1** (1935), 137–168.

[2] H. Hasse, "Theorie der relativ-zyklischen algebraischen Funktionenkörper insbesondere bei endlichem Konstantenkörper," *J. Reine Angew. Math.* **172** (1934), 37–54. (Math. Abh. Band 2, 133–150)

[3] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, New York, 1990.

[4] P. Roquette, Class field theory in characteristic p, its origin and development, pp. 549–631 of "Class field theory – its centenary and prospect," Math. Soc. Japan, Tokyo, 2001.