Mobius Functions, Legendre Symbols, and Discriminants

Zev Chonoles, Erick Knight, Tim Kunisky

1 Introduction

Over the integers, there are two key number-theoretic functions that take on values of 1, -1, and 0: the Mobius function and the Legendre symbol. While over $\mathbb{Z}$ there is no apparent connection between them, we will develop formulae connecting the two functions over finite fields.

Particularly, we will first relate the two over $\mathbb{Z}_p$ for p an odd prime, which is easily generalized to finite fields of characteristic p for odd primes. The case $p = 2$ will be a special case that requires modification of the formula as well as generalization of the method of proof. The formula in both cases looks like:

$$\mu(f) = (-1)^{\deg(f)} \left(\frac{\operatorname{disc}(f)}{p}\right)$$

where μ is the Mobius function, $\operatorname{disc}(f)$ is the discriminant, and the fraction notation is the Legendre symbol for odd primes p, generalized to the Kronecker symbol for the case of $p = 2$.

The discriminant will be the main tool we use to show the connection between the Legendre symbol and the Mobius function, so many intermediate propositions will involve its properties.

2 Definitions

Definition Let $f(T) \neq 0 \in \mathbb{F}[T]$ for some finite field $\mathbb{F}$. Then, the Mobius function $\mu(f(T))$ is defined in a similar manner as in $\mathbb{Z}$:

$$\mu(f(T)) = \begin{cases} 0 & \text{if } g(T)^2 \mid f(T) \text{ for some non-constant } g(T), \\ (-1)^r & \text{if } f(T) \text{ has } r \text{ distinct monic irreducible factors.} \end{cases}$$

Definition For monic $f(T) \in \mathbb{F}[T]$ for $\mathbb{F}$ a field, with roots α_k in an extension K of $\mathbb{F}$, $\operatorname{disc}(f)$ is the discriminant of f. If $\deg f < 2$, the discriminant is one. Otherwise, it is defined as

$$\operatorname{disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

This formula matches the familiar formulas for discriminants of degree two and three monic polynomials, which will be proven in Propositions 3.1 and 3.2. We will also find it useful to define another quantity, denoted $\delta(f)$, the square root of the discriminant:

$$\delta(f) = \prod_{i<j} (\alpha_i - \alpha_j).$$

Note that based on indexing of the roots, the value of this may vary up to sign, and therefore $\delta(f)$ is only well-defined up to sign. Finally, we define $\delta'(f)$ as a slightly different version of $\delta(f)$:

$$\delta'(f) = \prod_{i<j} (\alpha_i + \alpha_j).$$

Unlike $\delta(f)$, this is invariant under reindexing of the roots, so it is well-defined.

Definition For any $x \in \mathbb{Z}/8$, the Kronecker symbol (a generalization of the Legendre symbol) of x is defined as:

$$\left(\frac{x}{2}\right) = \begin{cases} 0 & \text{if } x \equiv 0, 2, 4, 6 \pmod 8, \\ 1 & \text{if } x \equiv 1, 7 \pmod 8, \\ -1 & \text{if } x \equiv 3, 5 \pmod 8. \end{cases}$$

3 Discriminant Properties and Examples

Proposition 3.1. (Monic Quadratic Discriminants) *If* $f(T) = T^2 + bT + c$, *then* $\operatorname{disc}(f) = b^2 - 4c$.

Proof. Let the roots of $f(T) = T^2 + bT + c$ be α_1 and α_2. Then, in an extension of $\mathbb{Z}/p$, $f(T) = (T - \alpha_1)(T - \alpha_2)$, so $\alpha_1 + \alpha_2 = -b$ and $\alpha_1\alpha_2 = c$. Thus

$$\operatorname{disc}(f) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c.$$

□

Proposition 3.2. (Monic Depressed Cubic Discriminants) *If* $f(T) = T^3 + aT + b$, *then* $\operatorname{disc}(f) = -4a^3 - 27b^2$.

Proof. Let $\alpha_0, \alpha_1, \alpha_2$ be the roots of $f(T) = T^3 + aT + b$. Then

$$(T - \alpha_0)(T - \alpha_1)(T - \alpha_2) = T^3 + aT + b.$$

Differentiating both sides with respect to T gives:

$$(T - \alpha_0)(T - \alpha_1) + (T - \alpha_0)(T - \alpha_2) + (T - \alpha_1)(T - \alpha_2) = 3T^2 + a,$$

and evaluating the equality at α_0, α_1, and α_2 yields:

$$(\alpha_0 - \alpha_1)(\alpha_0 - \alpha_2) = 3\alpha_0^2 + a,$$

$$(\alpha_1 - \alpha_0)(\alpha_1 - \alpha_2) = 3\alpha_1^2 + a,$$

$$(\alpha_2 - \alpha_0)(\alpha_2 - \alpha_1) = 3\alpha_2^2 + a.$$

Their product will give the negative of the discriminant of T:

$$-\text{disc}(f(T)) = (3\alpha_0^2 + a)(3\alpha_1^2 + a)(3\alpha_2^2 + a).$$

By manipulating the original polynomial, we can derive a polynomial with the roots $3\alpha_k^2 + a$:

$$t^3 + at = -b \Rightarrow t^6 + 2at^4 + a^2t^2 = b^2$$

Multiplying by -27:

$$(-3t^2)^3 - 6a(-3t^2)^2 + 9a^2(-3t^2) + 27b^2 = 0.$$

Letting $-3x^2 = a$ (with a change of sign) gives an expression for the discriminant:

$$a^3 - 6a^3 + 9a^3 + 27b^2 = 4a^3 + 27b^2 \Rightarrow \text{disc}(f(T)) = -4a^3 - 27b^2.$$

□

Proposition 3.3. *If f is a degree m monic polynomial with roots α_k in an extension of $\mathbb{Z}/p$, then*

$$\textit{disc}(f) = (-1)^{m(m-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Proof. Let f satisfy the hypotheses. Then

$$\begin{aligned}\operatorname{disc}(f) &= \prod_{i<j}(\alpha_i-\alpha_j)^2 = \prod_{i<j}(\alpha_i-\alpha_j)\prod_{i<j}(\alpha_i-\alpha_j)\\ &= \prod_{i<j}(\alpha_i-\alpha_j)\prod(\alpha_i-\alpha_j)(-1)^{m(m-1)/2}\\ &= (-1)^{m(m-1)/2}\prod_{i\neq j}(\alpha_i-\alpha_j),\end{aligned}$$

as we have $\frac{m(m-1)}{2}$ terms being negated. □

Example Some examples of discriminant evaluation:

$$\begin{aligned}\operatorname{disc}(T^3-T-1) &= -23,\\ \operatorname{disc}(T^3+3T-4) &= -540,\\ \operatorname{disc}(T^7+2T^3+9T-1) &= -235718099287,\\ \operatorname{disc}(T^{10}+8T^5+4T) &= 110357402604273664.\end{aligned}$$

4 Basic Results

Proposition 4.1. *Let p be an odd prime, and $f(T)=T^2+bT+c$ be a monic quadratic polynomial in $\mathbb{Z}/p$. Then $\mu(f(T))=(\frac{\operatorname{disc}(f(T))}{p})$, where μ is the Mobius function on $(\mathbb{Z}/p)[T]$ and $\operatorname{disc}f(T)=b^2-4c$.*

Proof. If $f(T+k)$ factors as $g(T)h(T)$ in $(\mathbb{Z}/p)[T]$, then $f(T)$ must factor as $g(T-k)h(T-k)$, so that adding a constant to the indeterminate T preserves the factorization of $f(T)$ and therefore the value of $\mu(f(T))$. Thus, $\mu(f(T))=\mu(f(T+k))$ for all k in $\mathbb{Z}/p$.

Since $\mathbb{Z}/p$ is a field, we have that $\frac{b}{2}\in\mathbb{Z}/p$ and therefore

$$\mu(f(T))=\mu\left(f\left(T-\frac{b}{2}\right)\right)=\mu\left(T^2-(b^2-4c)\right)$$

So:
(1) $f(T)$ is irreducible if and only if b^2-4c is a quadratic non-residue.
(2) $f(T)$ has a repeated root if and only if b^2-4c is 0.
(3) $f(T)$ has two distinct roots if and only if b^2-4c is a quadratic residue.

By the casework, $\mu(f(T))=(\frac{b^2-4c}{p})$. □

Proposition 4.2. (Viete's Formulas) *If $f(T) \in \mathbb{F}[T]$ is monic and splits in a field $\mathbb{E}$, $\mathbb{E} \supset \mathbb{F}$, where $f(T) = a_0 + a_1 T + \cdots + a_m T^m = (T - \alpha_1) \cdots (T - \alpha_m)$ in $\mathbb{E}[T]$, then*

$$a_k = (-1)^{m-k} \sum_{1 \le i_1 < \cdots < i_{m-k} \le m} \alpha_{i_1} \cdots \alpha_{i_{m-k}}.$$

Proof. Let $f(T) = (T - \alpha_1)(T - \alpha_2) \ldots (T - \alpha_m)$. In the expansion, every T^{m-1} term has coefficient of some α_k, and each α_k is multiplied by $m - 1$ factors of T. Therefore, the coefficient of T^{m-1} is the sum of all α_k:

$$-\alpha_1 - \alpha_2 - \cdots - \alpha_m = -(\alpha_1 + \alpha_2 + \cdots + \alpha_m) = a_{m-1}$$

The constant term of the polynomial is, up to sign, just the product of all α_k, which is:

$$(-\alpha_1)(-\alpha_2) \cdots (-\alpha_m) = (-1)^m (\alpha_1 \cdots \alpha_m) = a_0$$

In general, the coefficient of T^k is a_k. When the polynomial is expanded, each instance of T^k will have a coefficient of a different product of $m - k$ roots, and therefore the coefficient of T^k, up to sign, is the sum of all possible products of $m - k$ roots. Each term in the sum will also have a coefficient of $(-1)^{m-k}$, so we have the expression:

$$a_k = (-1)^{m-k} \sum_{1 \le i_1 < \cdots < i_{m-k} \le m} \alpha_{i_1} \cdots \alpha_{i_{m-k}}.$$

□

5 Deriving the Formula

Lemma 5.1. *For any monic $f \in (\mathbb{Z}/p)[T]$, $(\mathrm{disc}(f))^p = \mathrm{disc}(f)$, so $\mathrm{disc}(f) \in \mathbb{Z}/p$.*

Proof. Note that the discriminant is a symmetric polynomial in the roots, i.e. it is unchanged by any permutation of the roots. By Corollary 2.4,

$$\mathrm{disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \prod_{i<j} (\alpha_i^p - \alpha_j^p)^2.$$

But $x \mapsto x^p$ is an automorphism of any finite field with characteristic p. Thus

$$\mathrm{disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^{2p} = \mathrm{disc}(f)^p.$$

Consequently, $\mathrm{disc}(f)$ is in $\mathbb{Z}/p$ by Theorem 2.1. □

Lemma 5.2. *For degree m monic irreducible $\pi(T) \in (\mathbb{Z}/p)[T]$, $\delta(\pi)^p = (-1)^{m-1}\delta(\pi)$, where $\delta(\pi)$ is the square root of* $\mathrm{disc}\pi$ *as defined in Section 1. Furthermore, for $p \neq 2$*

$$\left(\frac{\mathrm{disc}\pi}{p}\right) = (-1)^{m-1}.$$

Proof. Let $\pi(T)$ be a monic irreducible polynomial of degree m over $(\mathbb{Z}/p)[T]$ with one root, α, in an appropriate extension field. Then the roots of $\pi(T)$ are $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$, so $\delta(\pi) = \prod_{0\leq i<j\leq m-1}(\alpha^{p^i} - \alpha^{p^j})$. Consequently,

$$\begin{aligned}
\delta(\pi)^p &= \prod_{0\leq i<j\leq m-1}(\alpha^{p^{i+1}} - \alpha^{p^{j+1}}) \\
&= \prod_{j=1}^{m}(\alpha^{p^j} - \alpha) \prod_{1\leq i<j\leq m-1}(\alpha^{p^i} - \alpha^{p^j}) \\
&= (-1)^{m-1} \prod_{0\leq i<j\leq m-1}(\alpha^{p^i} - \alpha^{p^j}) = (-1)^{m-1}\delta(\pi).
\end{aligned}$$

And, noting that

$$\left(\frac{\mathrm{disc}\pi}{p}\right) = 1 \Leftrightarrow \delta(\pi) \in \mathbb{Z}/p \Leftrightarrow \delta(\pi)^p = \delta(\pi) \Leftrightarrow (-1)^{m-1} = 1$$

yields the second result of $(\frac{\mathrm{disc}\pi}{p}) = (-1)^{m-1}$. □

Lemma 5.3. (Multiplicativity of Discriminant) *For monic $f(T), g(T) \in (\mathbb{Z}/p)[T]$, $disc(fg) = disc(f)disc(g)c_{f,g}^2$, where $c_{f,g}$ depends on f and g.*

Proof. Let f, g be polynomials in $(\mathbb{Z}/p)[T]$ of degree m, n, respectively. Let the roots of f be α_i and the roots of g be β_j. Then let $c_{f,g} = \prod_{i,j}(\alpha_i - \beta_j)$. Since the Frobenius automorphism permutes the roots of both f and g, and $c_{f,g}$ is symmetric in the roots of f and g, $c_{f,g}^p = \prod_{i,j}(\alpha_i^p - \beta_j^p) = \prod_{i,j}(\alpha_i - \beta_j) = c_{f,g}$, so $c_{f,g} \in \mathbb{Z}/p$. Therefore,

$$\mathrm{disc}(fg) = \prod_{i<j}(\alpha_i - \alpha_j)^2 \prod_{i<j}(\beta_i - \beta_j)^2 \prod_{i,j}(\alpha_i - \beta_j)^2 = \mathrm{disc}(f)\mathrm{disc}(g)c_{f,g}^2.$$

Note that, if f and g are relatively prime, then none of the α_i is a β_j because otherwise f and g share a factor of $(x - k)$ where k is the shared root, so $c_{f,g} \neq 0$. □

Theorem 5.4. (Mobius/Legendre Formula) *For monic* $f(T) \in (\mathbb{Z}/p)[T]$ *where* $p \neq 2$*,*

$$\mu(f(T)) = (-1)^{\deg f} \left(\frac{\mathrm{disc} f}{p}\right).$$

Proof. For relatively prime monic polynomials f and g in $(\mathbb{Z}/p)[T]$,

$$\left(\frac{\mathrm{disc}(fg)}{p}\right) = \left(\frac{(\mathrm{disc} f)(\mathrm{disc} g)c_{f,g}^2}{p}\right) = \left(\frac{\mathrm{disc} f}{p}\right)\left(\frac{\mathrm{disc} g}{p}\right).$$

Since $c_{f,g} \in \mathbb{Z}/p$ and $c_{f,g} \neq 0$. Therefore, the function $f(T) \mapsto (-1)^{\deg f}(\frac{\mathrm{disc} f}{p})$ is multiplicative on relatively prime polynomials in $(\mathbb{Z}/p)[T]$. And, by Problem 8, for any monic irreducible polynomial π of degree m,

$$(-1)^m \left(\frac{\mathrm{disc}(f)}{p}\right) = (-1)^m(-1)^{m-1} = -1 = \mu(\pi).$$

For irreducible π and $k \geq 2$,

$$\mu(\pi^k) = 0 \text{ and } (-1)^{\deg(\pi^k)} \left(\frac{\mathrm{disc}(\pi^k)}{p}\right) = 0.$$

Since $f(T) \mapsto \mu(f(T))$ and $f(T) \mapsto (-1)^{\deg f}(\frac{\mathrm{disc} f}{p})$ are multiplicative functions that agree on powers of irreducibles, they must be the same function. □

Remark The same proof applies in all finite fields of characteristic $p > 2$, if we replace the Legendre symbol with an appropriate quadratic character symbol (1 at quadratic residues, -1 at quadratic non-residues, and 0 at zero).

6 Quadratic Reciprocity

Theorem 6.1. (Law of Quadratic Reciprocity) *For primes* $p, q \neq 2$*,*

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

Proof. Let p, q be distinct odds primes. Viewing $T^q - 1$ as a polynomial in $(\mathbb{Z}/p)[T]$, we will compute $\mathrm{disc}(T^q - 1)$ in two different ways, first using the Mobius function, and then from the definition of the discriminant.

Let $f(T) = \frac{T^q-1}{T-1}$ viewed in $(\mathbb{Z}/p)[T]$. Let the order of p mod q be j and let α be a root of $f(T)$ in some extension of $\mathbb{Z}/p$. Then, by Theorem 2.9, we have that $\prod_{i=0}^{j-1}(T-\alpha^{p^i})$ divides $f(T)$. Since that polynomial is irreducible and all divisors of f are of that form, we have that f, which is of degree $q-1$, has all of its irreducible factors of degree j, and so the number of irreducible factors of f is $\frac{q-1}{j}$. Therefore, $\mu(f(T)) = (-1)^{\frac{q-1}{j}}$. Going into $\mathbb{Z}_q$, let x be a generator of U_q. Let $k = \gcd(\mathrm{Ind}_x(p), q-1)$. Then $(-1)^k = (\frac{p}{q})$ and $k = \frac{q-1}{j}$. Thus $\mathrm{disc}(T^q-1) = -(\frac{p}{q})$.

Now we evaluate the discriminant directly from its definition. First, we need to introduce some new notation. Let ζ be a primitive q^{th} root of unity in some extension of $\mathbb{Z}/p$. Then define

$$Q_i(T) = \frac{T^q-1}{T-\zeta^i} = \sum_{k=0}^{q-1} \zeta^{i(q-k)} T^k \qquad Q_i(\zeta^i) = \sum_{i=0}^{q-1} 1 = q.$$

We can then derive

$$\begin{aligned}
\mathrm{disc}(T^q-1) &= (-1)^{q(q-1)/2} \prod_{i=0}^{q-1} \prod_{j\neq i} (\zeta^i - \zeta^j) \\
&= (-1)^{q(q-1)/2} \prod_{i=0}^{q-1} Q_i(\zeta^i) \\
&= (-1)^{(q-1)/2} q^q.
\end{aligned}$$

To prove the law of quadratic reciprocity, we have

$$\begin{aligned}
-\left(\frac{p}{q}\right) &= \mathrm{disc}(T^q-1) \\
&= (-1)^q \left(\frac{\mathrm{disc}(T^q-1)}{p}\right) \\
&= -\left(\frac{(-1)^{(q-1)/2} q^q}{p}\right) \\
&= -\left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.
\end{aligned}$$

But all values of quadratic characters are one or negative one. Thus

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

□

7 Analogous Formula in $(\mathbb{Z}/2)[T]$

Remark Several times in this section, we will use the fact that certain expressions in the roots of an integral polynomial are always integers. More specifically, rational polynomial expressions that are symmetric in the roots. Polynomial expressions in the roots of an integral polynomial must be algebraic integers, since algebraic integers are closed under sum and product. And, expressions symmetric in the roots must be rational, because permutation of the roots fixes $\mathbb{Q}$. But, rational algebraic integers are rational integers, and therefore this class of expressions will always be integral.

Lemma 7.1. (Hensel's Lemma) *Let $f(T) \in \mathbb{Z}/p^n$, where $\overline{f}$ is irreducible over $\mathbb{Z}/p$. Let $R_n = \mathbb{Z}/p^n[T]/(f(T))$. Then, if $g \in R_n[x]$, $r \in R_1$, $\overline{g}(r) = 0$, $\overline{g}'(r) \neq 0$, then there exists a unique $s \in R_n$ such that $s \equiv r \bmod p$ and $g(r) = 0$.*

Remark Hensel's Lemma allows us to lift the roots of a polynomial over $\mathbb{Z}/2$ to any $\mathbb{Z}/2^k$, so initially it may seem that $\mathbb{Z}/4$ would satisfy our needs. However, we assert that $\text{disc} f \equiv 0, 1 \pmod 4$ for any $f \in \mathbb{Z}[T]$, and therefore $\mathbb{Z}/4$ provides us with no information different from that in $\mathbb{Z}/2$.

Proof. For some $f \in \mathbb{Z}[T]$ of degree n with roots α_k, consider $\delta(f)'^2 - \delta(f)^2$. First, we consider the relevant products as indexed from 1 to some k (irrelevant of the actual ordering, simply for convenience). We denote by

$$(\alpha_i^2 \pm 2\alpha_i\alpha_i' + \alpha_i'^2)$$

the relevant term in each product, when the square is expanded. This gives:

$$\delta(f)'^2 - \delta(f)^2 = \prod_{i=1}^{k} (\alpha_i^2 + 2\alpha_i\alpha_i' + \alpha_i'^2) - \prod_{i=1}^{k} (\alpha_i^2 - 2\alpha_i\alpha_i' + \alpha_i'^2)$$

Define the following products:

$$\begin{aligned} P_i &= \prod_{1 \leq j < i} (\alpha_j^2 - 2\alpha_j\alpha_j' + \alpha_j'^2) \\ Q_i &= \prod_{i < g \leq k} (\alpha_g^2 + 2\alpha_g\alpha_g' + \alpha_g'^2) \end{aligned}$$

Then,

$$\begin{aligned}\delta(f)'^2 - \delta(f)^2 &= \sum_{i=1}^{k} P_i \left((\alpha_i^2 + 2\alpha_i\alpha_i' + \alpha_i'^2) - (\alpha_i^2 - 2\alpha_i\alpha_i' + \alpha_i'^2) \right) Q_i \\ &= \sum_{i=1}^{k} P_i(4\alpha_i\alpha_i')Q_i = 4\sum_{i=1}^{k} P_i(\alpha_i\alpha_i')Q_i\end{aligned}$$

So, $4 \mid (\delta(f)'^2 - \delta(f)^2) \Rightarrow 4 \mid (\delta(f)'^2 - \mathrm{disc} f) \Rightarrow \mathrm{disc} f \equiv \delta(f)'^2 \pmod 4$. We already know $\delta(f)' \in \mathbb{Z}$, so the discriminant is a square modulo 4. But, the only squares modulo 4 are 0 and 1, so $\mathrm{disc} f \equiv 0, 1 \pmod 4$. □

Thus, our polynomial roots will be lifted to $\mathbb{Z}/8$ via Hensel's Lemma, where this problem does not occur.

Theorem 7.2. *For any monic $f(T) \in (\mathbb{Z}/8)[T]$ that is irreducible in $\mathbb{Z}/2$ of degree n, there exists an automorphism ϕ of $(\mathbb{Z}/8)[T]/(f(T))$ that acts as an n-cycle on the elements corresponding to roots of f and fixes precisely $\mathbb{Z}/8$.*

Proof. Let $f(T) \in (\mathbb{Z}/8)[T]$ satisify the hypotheses. Let α_i be the roots in $\mathbb{Z}/8[T]/(f(T))$ lifted from $\mathbb{Z}/2[T]/(f(T))$ with $\alpha_i \equiv T^{2^i} \bmod 2$, where $0 \leq i \leq n-1$. Define ϕ mapping $\mathbb{Z}/8[T]/(f(T))$ to itself by $\phi(1) = 1$ and $\phi(T) = \alpha_1$. Then ϕ is a well-defined homomorphism, as is its restriction to $\mathbb{Z}/2[T]/(f(T))$. Since it sends T to T^2, it is the Frobenius automorphism. And, since ϕ is a homomorphism, it sends roots of f to roots of f, and, as noted before, since it is the Frobenius automorphism, ϕ sends $\alpha_i \mapsto \alpha_{i+1}$ and $\alpha_{n-1} \mapsto \alpha_0$. So, ϕ acts as an n-cycle on the roots.

We know $\phi(1) = 1$, so ϕ must fix $\mathbb{Z}/8$. Suppose g_0 is fixed by ϕ. Then, the reduction of g_0 to $(\mathbb{Z}/2)[T]/(f(T))$ must be an integer in $\mathbb{Z}/2$, so there exists some $g_0' \in \mathbb{Z}/8$ where $2 \mid (g_0 - g_0')$. So, for some g_1, $2g_1 = (g - g')$, and g_1 is fixed by ϕ as well. Applying the same argument to g_2 shows that $g_1 - g_1'$ for some $g_1' \in \mathbb{Z}/8$ is equal to $2g_2$ for some g_2. Iterating again allows us to find a g_2' where $2g_3 = g_2 - g_2'$ for some g_3. So, we have that g_0 differs from an element of $\mathbb{Z}/8$ by a multiple of 8, and therefore $g_0 \in \mathbb{Z}/8$. □

Lemma 7.3. (Multiplicativity of discriminants) *If $f, g \in (\mathbb{Z}/8)[T]$ are monic, then*

$$\mathrm{disc}(fg) = \mathrm{disc}(f)\mathrm{disc}(g)c_{f,g}^2$$

where $c_{f,g} \in \mathbb{Z}/8$ depends on f and g. Moreover, $c_{f,g} = 0, 2, 4, 6$ iff f and g have a non-constant common divisor.

Proof. The proof goes along the same lines as in the previous case. Let f, g be polynomials in $(\mathbb{Z}/8)[T]$ of degree m, n, respectively. Let the roots of f be α_i and the roots of g be β_j. Then let $c_{f,g} = \prod_{i,j}(\alpha_i - \beta_j)$, just as in the previous proof. But, we now use the previously defined automorphism ϕ and apply it to $c_{f,g}$. The result is exactly the same since ϕ permutes the roots of both polynomials, therefore it must fix $c_{f,g}$ so we have $c_{f,g} \in \mathbb{Z}/8$. Note that:

$$\operatorname{disc}(fg) = \prod_{i<j}(\alpha_i - \alpha_j)^2 \prod_{i<j}(\beta_i - \beta_j)^2 \prod_{i,j}(\alpha_i - \beta_j)^2 = \operatorname{disc}(f)\operatorname{disc}(g)c_{f,g}^2$$

when f and g are relatively prime. If they are not, $c_{f,g} = c_{f,g}^2 = 0$, but the discriminant is zero if and only if f and g share a root, so the formula goes through in that case as well. □

Theorem 7.4. *We have an analogous but not identical formula in $\mathbb{Z}/2$:*

$$\mu(f(T)) = (-1)^{\deg f}\left(\frac{\operatorname{disc} f}{2}\right)$$

Where the Legendre symbol is just replaced with the Kronecker Symbol.

Proof. The proof for irreducibles and powers of irreducibles goes by the same exact argument that it did in the odd prime case. And, the Kronecker symbol is multiplicative in the same way that the Legendre symbol is, so the multiplicative argument holds here as well, so the new formula is correct. □

Remark The proof for general finite fields of characteristic 2 is not so simple as it was for characteristic $p > 2$. The entirety of the argument holds, except for a small detail in the proof of multiplicativity of discriminants. We must show that among the possible discriminants, the product of two non-squares is a square. This fails in general; for example, in $\mathbb{Z}/8$, $5 \cdot 7 = 3$, but none of 3, 5, or 7 are squares. So, we must exclude some number of terms and only look at those that can be discriminants.

Proposition 7.5. *Suppose we are looking at $F = \mathbb{F}_{2^n}$, where F is a finite field of degree n of characteristic 2. Let R_2 be the ring containing $\mathbb{Z}/4$ that is F lifted by Hensel's Lemma. And, let R_3 be the lifting of R_2 by Hensel's Lemma, containing $\mathbb{Z}/8$. Then, the subset P of R_3 composed of all elements that reduce to a square in R_3 (i.e. possible discriminants) contains an equal number of squares and non-squares.*

Proof. Since F has characteristic 2, all non-zero elements of F are squares. That is, there are $2^n - 1$ squares in F. Now, since $(x + 2y)^2 \equiv x^2 \bmod 4$, the number of squares in R_2 is the same as the number in F, namely $2^n - 1$. Thus, the number of possible discriminants in R_3 is equal to $2^{2n} - 2^n$. Now, if $x^2 = y^2$ in R_3, then $8 \mid (x^2 - y^2)$ or $8 \mid (x-y)(x+y)$ and then either $4 \mid (x-y)$ or $4 \mid (x+y)$. But each equivalence class under $x \equiv y \iff x^2 = y^2$ has size 2^{n+1}, so there are $2^{2n-1} - 2^{n-1}$ perfect squares in R_3. Thus, our collection contains all possible discriminants, and precisely half of the elements are perfect squares. □

So, within this collection the multiplicativity argument applies, so we can complete the proof as we did for $\mathbb{Z}/2$, and our formula holds for all fields of characteristic 2. Combining with our previous result, we have that our formula holds in all finite fields.