Extending the Legendre Symbol to the Rédei Symbol Using Milnor Numbers

Inseo Kim

Seoul National University

February 12, 2025

Table of Contents

Table of Contents

We can observe the following similarities between knots and prime numbers.

Knot side	Prime side
Links	Primes
Link group of L $G_L(M) = \pi_1(M \backslash L)$	Galois group with restricted ramification in S $G_S(k) = \pi_1\left(\mathrm{Spec}\left(\mathcal{O}_k\right) \backslash S\right)$
Linking number $\mathrm{lk}(L, K)$	Legendre symbol $\left(\frac{q}{p}\right)$
$\mathrm{lk}(L, K) = \mathrm{lk}(K, L)$	$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \quad (p, q \equiv 1 \bmod 4)$

Table of Contents

Let $S = \{p_1, \cdots, p_n\}$ be a finite set of primes.

We fix an embedding of $\mathbb{Q}$ into an algebraic closure of $\mathbb{Q}$, and a prime number l.

Let $\mathbb{Q}_{\bar{S}}(l)$ be the maximal l-extension of $\mathbb{Q}$ unramified outside $\bar{S}$.

The group $G_S(l)$ is defined by

$$G_S(l) := \mathrm{Gal}\left(\mathbb{Q}_{\bar{S}}(l)/\mathbb{Q}\right).$$

Proposition

$G_S(l)$ is a pro-l group.

(Proof omitted)

Koch's Theorem

Let l be a fixed prime number and let $S = \{p_1, \cdots, p_r\}$ be a set of r distinct prime numbers such that $p_i \equiv 1 \mod l (1 \le i \le r)$.

Let $e_S := \max\{e \mid p_i \equiv \ 1 \mod l^e (1 \le i \le r)\}$, $m = l^e \, (1 \le e \le e_S)$.

Choose an embedding of $\mathbb{Q}$ into $\bar{\mathbb{Q}}$.

Fix a primitive l-th root of unity, and define $\zeta_{l^n} \in \bar{\mathbb{Q}}$ by a primitive l^n-th root of unity such that $\zeta_{l^t}^{l^s} = \zeta_{l^{t-s}} \ (t \ge s)$.

Lemma

$G_S(l) = \mathrm{Gal}\left(\mathbb{Q}_{\bar{S}}(l)/\mathbb{Q}\right)$ is generated by the monodromy τ_i at p_i and the Frobenius automorphism σ_i at p_i, defined by

$$\begin{array}{ll} \tau_i\left(\zeta_{l^n}\right) = \zeta_{l^n}, & \tau_i\left(\sqrt[l^n]{p_i}\right) = \zeta_{l^n} \sqrt[l^n]{p_i}, \\ \sigma_i\left(\zeta_{l^n}\right) = \zeta_{l^n}^{p_i}, & \sigma_i\left(\sqrt[l^n]{p_i}\right) = \sqrt[l^n]{p_i} \end{array}.$$

(Proof omitted)

Koch's Theorem

Koch's theorem

(i) $G_S(l)$ has the following presentation:

$$G_S(l) \cong \left\langle x_1, \cdots, x_r \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 \right\rangle,$$

where x_i, y_i represent τ_i, σ_i, respectively.

That is, $G_S(l)$ is a quotient of $\hat{F}(l)$, the pro-l completion of the free group F on words $x_1, \cdots, x_r$.

Remark. The words y_i's can be expressed by x_i's.

Koch's Theorem(continued)

(ii) There exists $\mathrm{lk}\,(p_i, p_j) \in \mathbb{Z}_l$ for $i \neq j$ such that

$$\sigma_j \equiv \prod_{i \neq j} \tau_i^{\mathrm{lk}(p_i, p_j)} \bmod [G_S(l), G_S(l)].$$

(iii) Define $\mathrm{lk}_m\,(p_i, p_j) \in \mathbb{Z}/m\mathbb{Z}$ by $\mathrm{lk}\,(p_i, p_j) \bmod m$. Then

$$\zeta_m^{\mathrm{lk}_m(p_i, p_j)} = \left(\frac{p_j}{p_i}\right)_m$$

holds, where $\left(\frac{*}{p_i}\right)_m$ is the m-th power residue symbol in $\mathbb{Q}_{p_i}$.

(Proof omitted)

Table of Contents

Complete Group Algebra

Let $\mathfrak{R}$ be a compact complete local ring and $\mathfrak{G}$ be a pro-finite group.

$\mathfrak{R}[[\mathfrak{G}]]$ is the complete group algebra of $\mathfrak{G}$ over $\mathfrak{R}$.

A continuous homomorphism $f : \mathfrak{G} \to \mathfrak{H}$ of pro-finite groups induces a continuous homomorphism $f : \mathfrak{R}[[\mathfrak{G}]] \to \mathfrak{R}[[\mathfrak{H}]]$ of completed group algebras.

When $\mathfrak{H}$ is the trivial group $\{e\}$, the induced map denoted by

$$\epsilon_{\mathfrak{R}[[\mathfrak{G}]]} : \mathfrak{R}[[\mathfrak{G}]] \to \mathfrak{R},$$

is called *the augmentation map*.

We will discuss $\mathbb{Z}_l[[\hat{F}(l)]]$.

Magnus Isomorphism

Let $\mathbb{Z}_l \langle\langle X_1, \ldots, X_r \rangle\rangle$ be the algebra of non-commutative formal power series of variables $X_1, \ldots, X_r$ over $\mathbb{Z}_l$,

$$\left\{ \sum_{1 \le i_1, \ldots, i_n \le r} a_{i_1 \cdots i_n} X_{i_1} \cdots X_{i_n} \mid n \ge 0, a_{i_1 \cdots i_n} \in \mathbb{Z}_l \right\}.$$

Magnus Isomorphism

Let F be the free group on word $x_1, ..., x_r$, $\hat{F}(l)$ be a pro-l completion of F.

Define the homomorphism $M : F \to \mathbb{Z}_l \langle\langle X_1, \ldots, X_r \rangle\rangle^\times$ by

$$M(x_i) := 1 + X_i,$$

$$M\left(x_i^{-1}\right) := 1 - X_i + X_i^2 - \cdots \quad (1 \leq i \leq r).$$

Extending to $\mathbb{Z}_l[[\hat{F}(l)]]$, we obtain a continuous $\mathbb{Z}_l$-algebra homomorphism

$$\hat{M} : \mathbb{Z}_l[[\hat{F}(l)]] \longrightarrow \mathbb{Z}_l \langle\langle X_1, \ldots, X_r \rangle\rangle .$$

Proposition

$\hat{M}$ is an isomorphism of $\mathbb{Z}_l$-algebra, called the pro-l Magnus isomorphism.

(Proof omitted)

Magnus Expansion

Definition

Let α be an element in $\mathbb{Z}_l[[\hat{F}(l)]]$.

The pro-l Magnus expansion of α is defined by the image of the pro-l Magnus isomorphism

$$\hat{M}(\alpha) = \epsilon_{\mathbb{Z}_l[[\hat{F}(l)]]}(\alpha) + \sum_{\substack{I=(i_1\ldots i_n)\\ 1\le i_1,\ldots,i_n\le r}} \hat{\mu}(I;\alpha)X_I, \quad X_I := X_{i_1}\cdots X_{i_n}.$$

The coefficients $\hat{\mu}(I;\alpha)$ are called *the pro-l Magnus coefficients*.

Property of Magnus Coefficients

Lemma

Let α, β be elements in $\mathbb{Z}_l[[\hat{F}(l)]]$ and I be an index.
Then the following holds:

$$\hat{\mu}(I;\alpha\beta) = \sum_{I=JK} \hat{\mu}(J;\alpha)\hat{\mu}(K;\beta).$$

(Proof omitted)

Mod m Magnus Expansion

Fix $m = l^e (e \geq 1)$.

Applying mod m to the Magnus isomorphism, *the mod m Magnus isomorphism* is obtained:

$$M_m : \mathbb{Z}/m\mathbb{Z}[[\hat{F}(l)]] \longrightarrow \mathbb{Z}/m\mathbb{Z}\langle\langle X_1, \ldots, X_r \rangle\rangle .$$

Mod m Magnus Expansion

Definition

Let α be an element in $\mathbb{Z}_l[[\hat{F}(l)]]$.

The mod m Magnus expansion of α is defined by the image of the mod m Magnus isomorphism

$$M_m(\alpha) = \epsilon_{\mathbb{Z}/m\mathbb{Z}[[\hat{F}(l)]]}(\alpha) + \sum_{\substack{I=(i_1 \dots i_n) \\ 1 \leq i_1, \dots, i_n \leq r}} \mu_m(I;\alpha) X_I, \quad X_I := X_{i_1} \cdots X_{i_n}.$$

The coefficients $\mu_m(I;\alpha)$ are called *the mod m Magnus coefficients*.

Table of Contents

We keep the same conditions as in Koch's theorem.

Koch's theorem(Recap)

Let l be a fixed prime number and let $S = \{p_1, \cdots, p_r\}$ be a set of r distinct prime numbers such that $p_i \equiv 1 \bmod l (1 \leq i \leq r)$.
Let $e_S := \max\{e \mid p_i \equiv\ 1 \bmod l^e (1 \leq i \leq r)\}$ and fix $m = l^e\, (1 \leq e \leq e_S)$.

(i) $G_S(l)$ is a pro-l group and has the following presentation:

$$G_S(l) \cong \left\langle x_1, \cdots, x_r \mid x_1^{p_1 - 1}[x_1, y_1] = \cdots = x_r^{p_r - 1}[x_r, y_r] = 1 \right\rangle,$$

where x_i, y_i represent τ_i, σ_i, respectively.

Koch's Theorem(Recap)

(ii) There exists $\mathrm{lk}\,(p_i, p_j) \in \mathbb{Z}_l$ for $i \neq j$ such that

$$\sigma_j \equiv \prod_{i \neq j} \tau_i^{\mathrm{lk}(p_i,p_j)} \bmod [G_S(l), G_S(l)].$$

(iii) Define $\mathrm{lk}_m\,(p_i, p_j) \in \mathbb{Z}/m\mathbb{Z}$ by $\mathrm{lk}\,(p_i, p_j) \bmod m$. Then

$$\zeta_m^{\mathrm{lk}_m(p_i,p_j)} = \left(\frac{p_j}{p_i}\right)_m$$

holds, where $\left(\frac{*}{p_i}\right)_m$ is the m-th power residue symbol in $\mathbb{Q}_{p_i}$.

Milnor Number

Definition

Let

$$\hat{M}(y_i) = 1 + \sum \hat{\mu}(Ii) X_I,$$

be the pro-l Magnus expansion of y_i, where $\hat{\mu}(Ii) := \hat{\mu}(I; y_i)$.
The coefficient $\hat{\mu}(Ii)$ is called *the l-adic Milnor number*.

Let

$$M_m(y_i) = 1 + \sum \mu_m(Ii) X_I,$$

be the mod m Magnus expansion of y_i, where $\mu_m(Ii) := \mu_m(I; y_i)$.
The coefficient $\mu_m(Ii)$ is called *the mod m Milnor number*.

Milnor Number

Proposition

Let $\mu_m(ij)$ be the mod m Milnor number. Then

$$\zeta_m^{\mu_m(ij)} = \left(\frac{p_j}{p_i}\right)_m$$

holds, where ζ_m is given in the Koch's theorem.

Proof) In $G_S(l)$, each y_i represent σ_i.

By Koch's theorem (ii), $\sigma_j \equiv \prod_{i \neq j} \tau_i^{\mathrm{lk}(p_i, p_j)} \mod [G_S(l), G_S(l)]$.

Applying Magnus isomorphism, $\hat{M}(y_j) = 1 + \sum_{i \neq j} \mathrm{lk}(p_i, p_j) X_i + \dots$.

Therefore $\mathrm{lk}(p_i, p_j) = \mu(ij)$.

Applying this to Koch's theorem (iii), we get the result.

When $m = 2$, the equality is the case of the classical Legendre symbol:

$$(-1)^{\mu_2(ij)} = \left(\frac{p_j}{p_i}\right).$$

We can generalize this by extending 2-index to n-index.

Definition

Define *the n-tuple multiple Legendre symbol* for prime numbers $p_1, \ldots, p_n$ with each $p_i \equiv 1 \mod 4$ by

$$[p_1, \ldots, p_n] := (-1)^{\mu_2(1 \cdots n)}$$

under the assumption that all $\mu_2(I) = 0$ for $|I| < n$.

Rédei Symbol

Rédei suggested the Rédei symbol as follows.

We will show that the Rédei symbol is the 3-tuple multiple Legendre symbol.

Let $l = 2$ and let $S := \{p_1, p_2, p_3\}$ be a triple of distinct prime numbers such that

$$p_i \equiv 1 \bmod 4, \quad \left(\frac{p_j}{p_i}\right) = 1 \quad (1 \leq i \neq j \leq 3).$$

Note that this condition is equal to the one in the 3-tuple multiple Legendre symbol.

Set $k_i = \mathbb{Q}\left(\sqrt{p_i}\right)$ $(i = 1, 2)$.

Lemma

(i) There is $\alpha_2 \in \mathcal{O}_{k_1}$ such that the following conditions hold:
(1) $\mathrm{N}_{k_1/\mathbb{Q}}(\alpha_2) = p_2 z^2$ (z is a non-zero integer)
(2) $\mathrm{N}(d_{k_1(\sqrt{\alpha_2})/k_1}) = p_2$ ($d_{k_1(\sqrt{\alpha_2})/k_1}$ is the relative discriminant).

(ii) Let $\mathfrak{p}_3$ be a prime ideal of $\mathcal{O}_{k_1}$ over p_3. For such an α_2 in (i), one has the Frobenius automorphism $\sigma_{\mathfrak{p}_3} \in \mathrm{Gal}\left(k_1\left(\sqrt{\alpha_2}\right)/k_1\right)$, since $\mathfrak{p}_3$ is unramified in $k_1\left(\sqrt{\alpha_2}\right)/k_1$.

(iii) $\sigma_{\mathfrak{p}_3}$ is independent of the choices of α_2 and $\mathfrak{p}_3$.

(Proof omitted)

Rédei Symbol

Definition

With the notation of previous lemma, the Rédei Symbol is defined by

$$[p_1, p_2, p_3]_R = \begin{cases} 1 & \text{if } \sigma_{\mathfrak{p}_3} = \mathrm{id}_{k_1(\sqrt{\alpha_2})} \\ -1 & \text{otherwise} \end{cases}.$$

Rédei Symbol

Let $\alpha_1 := \alpha_2 + \bar{\alpha}_2 + 2\sqrt{p_2}z = \left(\sqrt{\alpha_2} + \sqrt{\bar{\alpha}_2}\right)^2 \in k_2$ and
$k := k_1k_2\left(\sqrt{\alpha_2}\right) = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{\alpha_2}\right)$.

Then $k/\mathbb{Q}$ is a Galois extension with Galois group as D_4 and it is unramified outside p_1, p_2, ∞.

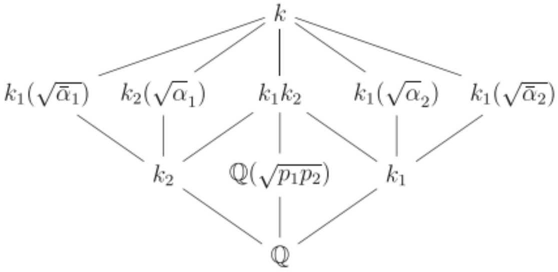

Figure: The intermediate fields of $k/\mathbb{Q}$

Rédei Symbol

Define $s, t \in \mathrm{Gal}(k/\mathbb{Q})$ by

$$s\left(\sqrt{p_1}\right) = \sqrt{p_1}, s\left(\sqrt{p_2}\right) = -\sqrt{p_2}, s\left(\sqrt{\alpha_2}\right) = \sqrt{\alpha_2}$$
$$t\left(\sqrt{p_1}\right) = -\sqrt{p_1}, t\left(\sqrt{p_2}\right) = -\sqrt{p_2}, t\left(\sqrt{\alpha_2}\right) = -\sqrt{\bar{\alpha}_2}.$$

The Galois group $\mathrm{Gal}(k/\mathbb{Q})$ is then generated by s, t and the relations are given by

$$s^2 = t^4 = 1, \quad sts^{-1} = t^{-1}$$

The subfields $k_1\left(\sqrt{\alpha_2}\right)$ and $\mathbb{Q}\left(\sqrt{p_1p_2}\right)$ correspond to $\langle s \rangle$ and $\langle t \rangle$ respectively, and the subfields $k_1k_2 = \mathbb{Q}\left(\sqrt{p_1}, \sqrt{p_2}\right)$ and $k_2\left(\sqrt{\alpha_1}\right)$ correspond to $\langle t^2 \rangle$ and $\langle st \rangle$ respectively.

Rédei Symbol

By the assumption, p_3 is completely decomposed in the extension $k_1k_2/\mathbb{Q}$. Let $\mathfrak{P}_3$ be a prime ideal in k_1k_2 over p_3.

Since $\mathfrak{P}_3$ is decomposed in k/k_1k_2 if and only if $\mathfrak{p}_3$ is decomposed in $k_1\left(\sqrt{\alpha_2}\right)/k_1$, we get from the definition

$$[p_1, p_2, p_3]_R = \begin{cases} 1 & \sigma_{\mathfrak{P}_3} = \mathrm{id}_k \\ -1 & \text{otherwise} \end{cases} .$$

Rédei Symbol

Since $k \subset \mathbb{Q}_{\bar{S}}(2)$, we have the canonical projection $\psi : G_S(2) \to \mathrm{Gal}(k/\mathbb{Q})$.

Let $\hat{F}(2)$ be the free pro-2 group on x_1, x_2, x_3 representing τ_1, τ_2, τ_3 and let $\pi : \hat{F}(2) \to G_S(2)$ be the canonical projection.

Define $\varphi : \hat{F}(2) \to \mathrm{Gal}(k/\mathbb{Q})$ by $\varphi := \psi \circ \pi$.

Rédei Symbol

Recall the definition of τ_i with $l = 2$:

$$\tau_i(-1) = -1, \quad \tau_i(\sqrt{p_i}) = -\sqrt{p_i}.$$

From this, we get

$$\varphi(x_1) = st, \quad \varphi(x_2) = s, \quad \varphi(x_3) = 1.$$

and

$$\varphi(x_1)^2 = \varphi(x_2)^2 = 1, \varphi(x_1 x_2)^4 = 1, \varphi(x_3) = 1.$$

Main Theorem

Theorem

Under the conditions so far, the equality holds:

$$(-1)^{\mu_2(123)} = [p_1, p_2, p_3]_R ,$$

which implies that

$$[p_1, p_2, p_3] = [p_1, p_2, p_3]_R .$$

Main Theorem

Proof) Recall that the definition of the Rédei Symbol is

$$[p_1, p_2, p_3]_R = \begin{cases} 1 & \sigma_{\mathfrak{P}_3} = \mathrm{id}_k \\ -1 & \text{otherwise} \end{cases}.$$

The Frobenius automorphism $\sigma_{\mathfrak{P}_3}$ at p_3 is represented by y_3 in $G_S(2)$.

Applying φ to each condition, we obtain

$$\varphi(y_3) = \begin{cases} 1 & [p_1, p_2, p_3]_R = 1 \\ t^2 = \varphi((x_1 x_2)^2) & [p_1, p_2, p_3]_R = -1 \end{cases}.$$

Main Theorem

Proof)(Continued) Since $\mathrm{Ker}(\varphi)$ is generated as a normal subgroup of $\hat{F}(2)$ by $x_1^2, x_2^2, (x_1x_2)^4, x_3$,

$$M_2\left(x_1^2\right) = (1+X_1)^2 = 1+X_1^2$$
$$M_2\left(x_2^2\right) = (1+X_2)^2 = 1+X_2^2,$$
$$M_2\left((x_1x_2)^4\right) = ((1+X_1)(1+X_2))^4 \equiv 1 \bmod \deg \geq 4,$$
$$M_2(x_3) = 1+X_3.$$

Therefore $\mu_2((1);*), \mu_2((2);*)$ and $\mu_2((12);*)$ take their values 0 on $\mathrm{Ker}(\varphi)$.

Proof)(Continued)
If $\varphi(y_3) = 1, \mu_2(123) = \mu_2((12); y_3) = 0$ by $y_3 \in \mathrm{Ker}(\varphi)$.

If $\varphi(y_3) = t^2 = \varphi\left((x_1x_2)^2\right)$, we can write $y_3 = (x_1x_2)^2 f, f \in \mathrm{Ker}(\varphi)$.

Then comparing the coefficients of X_1X_2 in

$$M_2(y_3) = M_2\left((x_1x_2)^2\right) M_2(f),$$

we have

$$\begin{aligned}\mu_2(123) &= \mu_2((12); y_3) \\ &= \mu_2\left((12); (x_1x_2)^2\right) + \mu_2((12); f) \\ &+ \mu_2\left((1); (x_1x_2)^2\right) \mu_2((2); f) \\ &= 1\end{aligned}$$