ABSTRACT

Title of dissertation: AN ALGORITHMIC APPROACH TO INVARIANT RATIONAL FUNCTIONS

Angela Marie Hennessy, Doctor of Philosophy, 2014

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

For any field K and group A acting on $K(x_0, x_1, \ldots, x_{n-1})$, the *fixed field* consists of the elements fixed under the action of A, and is denoted $K(x_0, x_1, \ldots, x_{n-1})^A$. Noether's problem seeks to answer whether $K(x_0, x_1, \ldots, x_{n-1})^A/K$ is a purely transcendental field extension.

Lenstra gave necessary and sufficient conditions for a purely transcendental extension when A is any finite abelian group, however his proof is often regarded as non-constructive. Masuda constructed generators of the fixed field when a certain ideal is principal in an integral group ring, and exhibited results when A is a cyclic group of order $n \leq 7$ and $n = 11$. We prove, however, that the ideal in question is not principal when $n = 13, 17, 19$ or 23, and thus Masuda's techniques cannot be used. We use Lenstra's proof as a basis of an algorithm which computes generators of the fixed field. We demonstrate this algorithm for groups of order $n = 3, 5, 7, 11, 13, 17, 19$ and 23.

Swan gave the first negative answer to Noether's problem for the cyclic group of order 47 over $\mathbb{Q}$. Leshin quantifies the degree to which a field extension fails to be purely transcendental by defining the *degree of irrationality*. We use the fact that the class group of the maximal real subfield $\mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$ is trivial to construct a field extension of degree 47 below the fixed field that is purely transcendental over K, thus providing a new bound for the degree of irrationality.

AN ALGORITHMIC APPROACH TO INVARIANT RATIONAL FUNCTIONS

by

Angela Marie Hennessy

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2014

Advisory Committee:
Professor Lawrence C. Washington, Chair/Advisor
Professor William Gasarch
Professor Niranjan Ramachandran
Professor James Schafer
Professor Harry Tamvakis

Acknowledgments

I would like to thank my PhD advisor Professor Lawrence Washington for his support, patience and countless suggestions over the last five years. I would also like to thank Professors William Gasarch, Niranjan Ramachandran, James Schafer and Harry Tamvakis for serving on my committee. I thank my friends, family and coworkers for their patience as I made my way through grad school. Special thanks to Finley for the numerous and valuable study sessions, and to Cathy and Reddy for their inspiration and perseverance.

Table of Contents

Chapter 1: Preliminaries

1.1 Introduction

Let K be any field, and A a subgroup of the permutation group S_n. Suppose A acts on the field $K(x_0, x_1, \ldots, x_{n-1})$ by permuting the variables. The elements of $K(x_0, x_1, \ldots, x_{n-1})$ that are fixed under the action of A define a subfield called the *fixed field*, which is denoted $K(x_0, x_1, \ldots, x_{n-1})^A$. Noether's problem asks under what circumstances the fixed field of $K(x_0, x_1, \ldots, x_{n-1})$ is a purely transcendental, or *rational*, extension of K. While this is an interesting problem in its own right, it also has applications to the inverse Galois problem and the study of generic polynomials. If A is the full symmetric group S_n, then as a result of the fundamental theorem of symmetric polynomials, the fixed field is generated by the elementary symmetric polynomials $e_1, e_2, \ldots, e_n$, that is,

$$K(x_0, \ldots, x_{n-1})^{S_n} = K(e_1, \ldots, e_n).$$

Fischer [2] showed that if A has exponent e and K contains the e-th roots of unity and is of characteristic prime to e, then $K(x_0, x_1, \ldots, x_{n-1})^A$ is rational over K. Swan and Voskresenskii independently gave the first negative answers to Noether's problem by proving that the fixed field when A is the cyclic group of order $p = 47, 113$, and 223 is not rational over $\mathbb{Q}$ [12, 14]. Lenstra gave a complete solution for finite abelian groups over any field [5] by showing that rationality is equivalent to the existence of a certain

principal ideal in the ring of integers of a cyclotomic field. However, Lenstra's proof is often regarded as not being constructive [4, p. 200].

Recently, Hoshi examined the case where A is a cyclic group of prime order and $K = \mathbb{Q}$ [3]. For primes $p < 20,000$, the only confirmed rational cases are $p \leq 43$ and $p = 61, 67, 71$. Under the generalized Riemann hypothesis, there are only 17 cases where the question of rationality has not been determined.

There have been limited results regarding algorithms to construct explicit generators of the fixed field. Masuda introduced techniques to construct generators of the fixed field when a certain ideal is principal in an integral group ring [7, 8], and exhibited results when A is a cyclic group of order $n \leq 7$ and $n = 11$. We prove, however, that the ideal in question is not principal when $n = 13, 17, 19$ or 23, and thus Masuda's techniques cannot be used. By Lenstra's result, however, the fixed field is rational over K. We use Lenstra's proof as a basis of an algorithm which, given a generator of the ideal in the ring of integers of the cyclotomic field, computes generators of the fixed field. We demonstrate this algorithm for cyclic groups of order $n = 3, 5, 7, 11, 13, 17, 19$ and 23. To the best of our knowledge, we are the first to exhibit explicit generators for $n = 13, 17, 19$ and 23.

When a field extension fails to be rational, we are interested in determining how "close" it is to a rational extension. Leshin defines the *degree of irrationality* [6] for a group A and field K as follows, where V_A denotes the regular representation $\langle x_a \rangle_{a \in A}$.

$$\mathrm{Irr}(K, A) = \min_{K \subseteq L \subseteq K(V_A)^A} \{ [K(V_A)^A : L] : L/K \text{ is rational } \}$$

If A is the cyclic group of order n, we can see that $\mathrm{Irr}(K, A) \leq (n-1)!$, as described in the diagram below.

$$
\begin{array}{c}
K(V_A) \\
\Big| \; n \\
K(V_A)^A \\
\Big| \; (n-1)! \\
K(V_A)^{S_n}
\end{array}
$$

When $A = \mathbb{Z}/p\mathbb{Z}$ is of prime order and $K = \mathbb{Q}$, Leshin proves

$$\mathrm{Irr}(K, A) \leq \frac{1}{p}\left(\frac{1}{2}\sqrt{p} + 1\right)^{\frac{p-1}{2}}.$$

When $A = \mathbb{Z}/47\mathbb{Z}$ and $K = \mathbb{Q}$, for example, we know that $K(V_A)^A/K$ is not rational, and therefore $\mathrm{Irr}(\mathbb{Q}, \mathbb{Z}/47\mathbb{Z}) \geq 2$, and the above bound gives

$$\mathrm{Irr}(\mathbb{Q}, \mathbb{Z}/47\mathbb{Z}) \leq \frac{1}{47}\left(\frac{1}{2}\sqrt{47} + 1\right)^{23} \approx 1.55 \times 10^{13}.$$

We use the fact that the class number of the maximal real subfield $\mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$ is 1 to construct a rational field extension of degree 47^2 below $K(V_A)$, and degree 47 below the fixed field $K(V_A)^A$. That is, we show that $\mathrm{Irr}(\mathbb{Q}, \mathbb{Z}/47\mathbb{Z}) \leq 47$. Similarly, $\mathrm{Irr}(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}) \leq p$ for $p = 59, 83, 107$, and 163, since the real cyclotomic fields of conductors 29, 41, 53, and 81 have class number 1 [13]. Under the generalized Riemann hypothesis, this extends to $p = 251$, since the class number of the 125-th real cyclotomic field has class number 1. The use of GRH could be eliminated if a calculation finds the principal generator of the relevant ideal.

1.2 Galois Descent Techniques

Many of the results regarding Noether's problem are based on the idea of Galois descent. We let K denote a field of characteristic zero, and $A = \langle \tau \rangle$ a cyclic group of prime order p, acting by permutation on the x_i, that is,

$$\tau(x_0) = x_1,\ \tau(x_1) = x_2,\ \cdots,\ \tau(x_{p-1}) = x_0.$$

Following [7,12], we define the *Lagrange resolvents* $y_0, \ldots, y_{p-1}$ as follows, where ζ denotes a primitive p-th root of unity.

$$y_i = \sum_{j=0}^{p-1} \zeta^{-ij} x_j$$

We can see that the y_i linearize the action of τ, since

$$\begin{aligned}
\tau(y_i) &= \tau(x_0 + \zeta^{-i}x_1 + \zeta^{-2i}x_2 + \cdots + \zeta^{-(p-1)i}x_{p-1}) \\
&= x_1 + \zeta^{-i}x_2 + \zeta^{-2i}x_3 + \cdots + \zeta^{-(p-1)i}x_0 \\
&= \zeta^i(x_0 + \zeta^{-i}x_1 + \zeta^{-2i}x_2 + \cdots + \zeta^{-(p-1)i}x_{p-1}) \\
&= \zeta^i y_i
\end{aligned}$$

Since the y_i are defined via an invertible Vandermonde matrix whose (i,j) entry is ζ^{-ij}, we have

$$K(\zeta, x_0, x_1, \ldots, x_{p-1}) = K(\zeta, y_0, y_1, \ldots, y_{p-1}).$$

The Galois group G of $K(\zeta)/K$ is cyclic of order d dividing $p-1$. We denote the generator by π and say it is determined by $\pi(\zeta) = \zeta^r$, where r has order d in $(\mathbb{Z}/p\mathbb{Z})^\times$.

$$G = \text{ Gal } (K(\zeta)/K) = \langle \pi \rangle.$$

We can see that π fixes the x_i and maps $\pi(y_i) = y_{ri}$. That is, y_0 is fixed, and $y_1, \ldots, y_{p-1}$ are permuted by π. We denote the multiplicative group generated by $y_1, \ldots, y_{p-1}$ as Y.

We define a group homomorphism $\alpha : Y \longrightarrow \langle \zeta \rangle$ via

$$\alpha(y_i) = \frac{\tau(y_i)}{y_i} = \zeta^i.$$

Clearly α is surjective, and its kernel consists of the elements of Y fixed by τ. We denote this kernel by I. We have the following generating set for I.

Lemma 1.1. *The elements* $y_1^p, \frac{y_2}{y_1^2}, \ldots, \frac{y_{p-1}}{y_1^{p-1}}$ *are a generating set for* I.

Proof. Since α is a surjection, we can see that $Y/I \cong \langle \zeta \rangle$, and therefore I has index p in Y. Clearly, $y_1^p, \frac{y_2}{y_1^2}, \ldots, \frac{y_{p-1}}{y_1^{p-1}} \in I$, and the quotient of Y by the subgroup generated by these elements is

$$\langle y_1, \ldots, y_{p-1} \ : \ y_1^p, \frac{y_2}{y_1^2}, \ldots, \frac{y_{p-1}}{y_1^{p-1}} \rangle \cong \langle y_1 \ : \ y_1^p \rangle.$$

Since $\langle y_1^p, \frac{y_2}{y_1^2}, \ldots, \frac{y_{p-1}}{y_1^{p-1}} \rangle \subseteq I$ has index p in Y, it must be a generating set for I. $\square$

We can now write the fixed field $K(x_0, x_1, \ldots, x_{p-1})^\tau$ in terms of I.

Proposition 1.1. *We have* $K(x_0, x_1, \ldots, x_{p-1})^\tau = K(\zeta, y_0, I)^\pi$.

Proof. Since I is fixed by τ, clearly $K(\zeta, y_0, I) \subseteq K(\zeta, y_0, y_1, \ldots, y_{p-1})^\tau$. Since the index

of I in Y is p, we have

$$[K(\zeta, y_0, y_1, \ldots, y_{p-1}) : K(\zeta, y_0, I)] = p,$$

and therefore

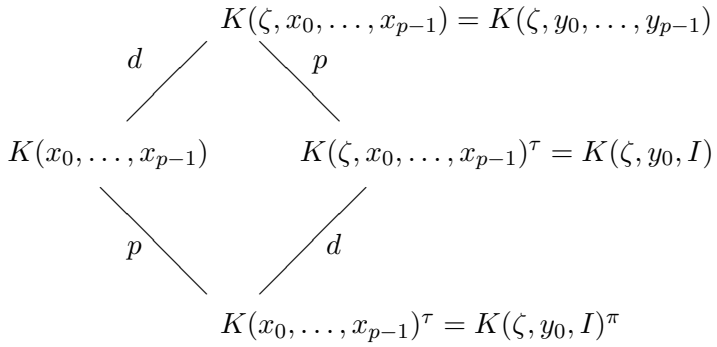
$$K(\zeta, y_0, y_1, \ldots, y_{p-1})^\tau = K(\zeta, y_0, I).$$

We see that the action of π and τ commute, and we have

$$\begin{aligned} K(x_0, x_1, \ldots, x_{p-1})^\tau &= (K(\zeta, x_0, \ldots, x_{p-1})^\pi)^\tau \\ &= (K(\zeta, y_0, \ldots, y_{p-1})^\pi)^\tau \\ &= (K(\zeta, y_0, \ldots, y_{p-1})^\tau)^\pi \\ &= K(\zeta, y_0, I)^\pi \end{aligned}$$

□

We summarize this in the following diagram.



We remark that if $\zeta \in K$, then the fixed field is rational and is generated by y_0 and I, as shown by Fischer [2].

1.2.1 Masuda's Results

Masuda made use of Galois descent techniques to find generators for the fixed field when A has prime order $p \leq 11$. We assume that $[K(\zeta) : K] = p-1$ and denote $L = K(\zeta)$. Since π permutes the Lagrange resolvents $y_1, \ldots, y_{p-1}$, we have a $\mathbb{Z}G$-module isomorphism

$$Y \cong \mathbb{Z}[t]/(t^{p-1} - 1) \text{ via } y_{r^i} \mapsto t^i,$$

where r has order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ and G acts by multiplication by t.

This is an example of a *permutation module*, that is, a $\mathbb{Z}$-free module with a $\mathbb{Z}$-basis permuted by $\mathbb{Z}G$. Under this isomorphism, the generators $y_1^p, \frac{y_r}{y_1^r}, \ldots, \frac{y_{r^{p-2}}}{y_1^{r^{p-2}}}$ of I correspond to

$$\{p, t-r, t^2-r^2, \ldots, t^{p-2}-r^{p-2}\}.$$

As a $\mathbb{Z}G$-module these are generated by p and $t-r$, so I is equal to the ideal $\langle p, t-r\rangle$. Masuda shows that principality of I is a sufficient condition for the rationality of $K(x_0, \ldots, x_{p-1})^\tau/K$.

Proposition 1.2 ([8, Lemma 2]). *The field extension $K(x_0, \ldots, x_{p-1})^\tau/K$ is rational if I is a principal ideal in $\mathbb{Z}G$.*

We note that I being a principal ideal is equivalent to being a permutation $\mathbb{Z}G$ module. Lenstra shows that any permutation module defines a rational extension.

Proposition 1.3 ([5, Proposition. 1.4]). *Suppose M is a finitely-generated permutation module over G. Then $L(M)^\pi$ is rational over K.*

For primes $p \leq 11$, Masuda finds generators of the ideal I [7, 8], therefore proving $K(x_0, \ldots, x_{p-1})^\tau/K$ is rational.

For example, for the case $p = 3$, the ideal $I = \langle 3, t-2\rangle$ is principal and generated by $t-2$. This corresponds to the element $\frac{y_2}{y_1^2}$ under the $\mathbb{Z}G$-module isomorphism $t^i \mapsto y_{2^i}$.

For the case $p = 5$, the ideal $I = \langle 5, t-2\rangle$ is principal and generated by $1 + t - t^3$. This corresponds to the element $\frac{y_1 y_2}{y_3}$ under the $\mathbb{Z}G$-module isomorphism $t^i \mapsto y_{2^i}$.

For the case $p = 7$, the ideal $I = \langle 7, t-3\rangle$ is principal and generated by $1 + t - t^4$. Under the map $t^i \mapsto y_{3^i}$ this corresponds to $\frac{y_1 y_3}{y_4}$.

For the case $p = 11$, the ideal $I = \langle 11, t-2\rangle$ is principal and generated by $1+t-t^8$. Under the map $t^i \mapsto y_{2^i}$ this corresponds to $\frac{y_1 y_2}{y_3}$.

Suppose I is principal and denote the generator by α, which we write multiplicatively, that is, $\alpha \in Y$. Then a $\mathbb{Z}$-basis of I is $\{\alpha, \pi(\alpha), \ldots, \pi^{p-2}(\alpha)\}$. Masuda then computes the generators of the fixed field $u_0, \ldots, u_{p-2}$ as follows. We define the $(p-1)\times(p-1)$ invertible matrix T whose (i,j)-th entry is $\zeta^{r^{i+j}}$, where r was defined via $\pi(\zeta) = \zeta^r$.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{p-2} \end{pmatrix} = T \cdot \begin{pmatrix} \alpha \\ \pi(\alpha) \\ \vdots \\ \pi^{p-2}(\alpha) \end{pmatrix} = \begin{pmatrix} \zeta & \pi(\zeta) & \cdots & \pi^{p-2}(\zeta) \\ \pi(\zeta) & \pi^2(\zeta) & \cdots & \zeta \\ \vdots & & & \vdots \\ \pi^{p-2}(\zeta) & \zeta & \cdots & \pi^{p-3}(\zeta) \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \pi(\alpha) \\ \vdots \\ \pi^{p-2}(\alpha) \end{pmatrix} \tag{1.1}$$

Clearly the u_i are fixed by π, and since T is an invertible matrix, we have

$$K(x_0, \ldots, x_{p-1})^\tau = K(y_0, u_0, \ldots, u_{p-2}).$$

For example, for the case $p = 3$, a $\mathbb{Z}$-basis of I is $\{\frac{y_2}{y_1^2}, \frac{y_1}{y_2^2}\}$, since π swaps the values y_1 and y_2. Then

$$K(x_0, x_1, x_2)^\tau = K(y_0, u_0, u_1),$$

where

$$u_0 = \zeta_3 \frac{y_2}{y_1^2} + \zeta_3^2 \frac{y_1}{y_2^2}$$
$$u_1 = \zeta_3^2 \frac{y_2}{y_1^2} + \zeta_3 \frac{y_1}{y_2^2}.$$

Using these techniques, Masuda gave generators of the fixed field for $p \leq 11$. For primes $p > 11$, however, it was not known if the ideal I is principal. We prove in the next chapter that I is not principal for $p = 13, 17, 19$ and 23. Therefore, Masuda's techniques cannot be used, and we will use Lenstra's techniques to compute the generators of the fixed field.

Chapter 2: Principality of the ideal I

We prove that the ideal I is not principal for the cases $p = 13, 17, 19$ and 23, and therefore we cannot use Masuda's techniques to compute generators of the fixed field. For the cases $p = 13, 17$ and 19, we use a similar method of proof. We search for a generator $f(t) \in \mathbb{Z}[t]/(t^{p-1} - 1)$ of I. If $f(t)$ is one such generator, $f(\zeta_{p-1})$ must generate the ideal

$$\langle p, \zeta_{p-1} - r \rangle \subseteq \mathbb{Z}[\zeta_{p-1}]$$

and $f(\zeta_d)$ is in the unit group $\mathcal{U}(\mathbb{Z}[\zeta_d])$ for every proper divisor d of $p - 1$.

Over the rationals the Chinese Remainder Theorem gives the following decomposition, since $t^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d(t)$ and the cyclotomic polynomials are relatively prime.

$$\mathbb{Q}[t]/(t^{p-1} - 1) \cong \overset{\oplus}{_{d \mid p-1}} \mathbb{Q}[t]/(\Phi_d(t)) = \overset{\oplus}{_{d \mid p-1}} \mathbb{Q}(\zeta_d)$$

This isomorphism is given by the map

$$\kappa : f(t) \mapsto (\overset{\oplus}{_{d \mid p-1}} f(\zeta_{p-1}^{\frac{p-1}{d}})).$$

Restricted to the integral group ring $\mathbb{Z}[t]/(t^{p-1} - 1)$, the map κ is no longer a surjection.

The image $\kappa(\mathbb{Z}[t]/(t^{p-1}-1))$ is contained in the unique maximal order

$$\overset{\oplus}{_{d \mid p-1}}\mathbb{Z}[\zeta_d] \subseteq \overset{\oplus}{_{d \mid p-1}}\mathbb{Q}(\zeta_d),$$

and the unit group $\mathcal{U}(\mathbb{Z}[t]/(t^{p-1}-1))$ maps into $\overset{\oplus}{_{d \mid p-1}}\mathcal{U}(\mathbb{Z}[\zeta_d])$. It has been shown that the image of the unit group has finite index in the unit group of the maximal order [9].

Since the value of $f(t)$ is unique up to multiplication by a unit of $\mathbb{Z}G$, we are interested in a set of coset representatives of $\overset{\oplus}{_{d \mid p-1}}\mathcal{U}(\mathbb{Z}[\zeta_d])$ modulo the image of $\mathcal{U}(\mathbb{Z}[t]/(t^{p-1}-1))$.

In general, however, it is very difficult to construct generators of the unit group of an integral group ring. For our purposes, it suffices to construct a subgroup of finite index of the unit group. Before we construct this subgroup, we review some results regarding units in integral group rings and rings of integers of cyclotomic fields.

2.1 Unit Groups of Integral Group Rings

If n is a prime power and ζ a primitive n-th root of unity, the *cyclotomic units* of $\mathbb{Q}(\zeta)$ are generated by $\pm\zeta$ and the units $\frac{1-\zeta^a}{1-\zeta}$, where $(a,n)=1$. We can restrict these to $1 < a < \lfloor \frac{n}{2} \rfloor$, since if $a > \lfloor \frac{n}{2} \rfloor$, we can rewrite it via

$$\frac{1-\zeta^a}{1-\zeta} = \frac{-\zeta^a(1-\zeta^{n-a})}{1-\zeta}.$$

The cyclotomic units generate a subgroup of $\mathcal{U}(\mathbb{Z}[\zeta])$ whose index is equal to the class number h_n^+ of the real subfield $\mathbb{Q}(\zeta)^+$ [15]. Therefore, the units in $\mathbb{Z}[\zeta_p]$ are the cyclotomic units for primes $p \leq 67$, or for $p < 163$ under the generalized Riemann hypothesis [13].

We have the following description of the unit group of $\mathbb{Z}G = \mathbb{Z}[t]/(t^n-1)$.

Lemma 2.1. *An element $u(t) \in \mathbb{Z}[t]/(t^n - 1)$ is a unit if and only if for each $d \mid n$, $u(\zeta^{\frac{n}{d}})$ is a unit in $\mathbb{Z}[\zeta_d]$.*

Proof. First, we suppose that $u(t) \in \mathcal{U}(\mathbb{Z}[t]/(t^n - 1))$ and let $v(t)$ be its inverse. Then for any $d \mid n$, we have $u(\zeta^{\frac{n}{d}}) \cdot v(\zeta^{\frac{n}{d}}) = 1$, and therefore $v(\zeta^{\frac{n}{d}}) = u(\zeta^{\frac{n}{d}})^{-1} \in \mathbb{Z}[\zeta_d]$.

Conversely, we suppose that $u(t) \in \mathcal{U}(\mathbb{Z}[t]/(t^n - 1))$ satisfies $u(\zeta^{\frac{n}{d}}) \in \mathcal{U}(\mathbb{Z}[\zeta_d])$ for all $d \mid n$. Clearly, the inverse in each factor $u(\zeta^{\frac{n}{d}})^{-1}$ lies in $\mathbb{Z}[\zeta_d]$ as well. Under the isomorphism between $\mathbb{Q}G$ and $\overset{\oplus}{_{d \mid n}} \mathbb{Q}[t]/(\Phi_d(t))$, the element $v \in \mathbb{Q}G$ that maps to each $u(\zeta^{\frac{n}{d}})^{-1}$ lies in the pull-back R of the maximal order $\overset{\oplus}{_{d \mid n}} \mathbb{Z}[\zeta_d]$. Therefore, v lies in the maximal order R of $\mathbb{Q}G$ that contains $\mathbb{Z}G$. Since R and $\mathbb{Z}G$ are of the same rank as $\mathbb{Z}$-modules, we see that v is integral over $\mathbb{Z}G$. Therefore, v satisfies an equation of the following form, where the $a_i \in \mathbb{Z}G$.

$$v^n + a_{n-1}v^{n-1} + \cdots + a_1 v + a_0 = 0$$

Multiplying by u^n, and using the fact that $uv = 1$, we have

$$1 + a_{n-1}u + a_{n-2}u^2 + \cdots + a_1 u^{n-1} + a_0 u^n = 0$$

and therefore

$$u^{-1} = -a_0 u^{n-1} - a_1 u^{n-2} - \cdots - a_{n-1}.$$

Since the a_i are in $\mathbb{Z}G$, we see that u^{-1} is also in $\mathbb{Z}G$. $\square$

2.2 Bass Cyclic Units

While we cannot find generators of $\mathcal{U}(\mathbb{Z}G)$ in general, we can construct elements that generate a subgroup of finite index in the unit group. This will allow us to compute a set that contains the coset representatives of $\overset{\oplus}{_{d \mid p-1}}\mathcal{U}(\mathbb{Z}[\zeta_d])$ modulo the image of $\mathcal{U}(\mathbb{Z}[t]/(t^{p-1}-1))$.

We construct a modified form of the *Bass cyclic units* of $\mathbb{Z}G$. We define

$$S_k(t) = 1 + t + \cdots + t^{k-1}$$

and choose $i, a \in [1, n-1]$ such that $\gcd(a, n) = 1$. Letting e be the smallest value satisfying

$$a^e \equiv \pm 1 \pmod{n},$$

and $k = a^e \pmod{n}$, we define

$$B(t^i, a, n) = S_a(t^i)^e + \left(\frac{1-ka^e}{n}\right) S_n(t^i) = (1+t^i+\cdots+t^{(a-1)i})^e + \left(\frac{1-ka^e}{n}\right)(1+t^i+\cdots+t^{(n-1)i})$$

The Bass units [1] use $\varphi(n)$ rather than e, and generate a subgroup of the modified Bass units.

Lemma 2.2. *The modified Bass cyclic units are units in* $\mathbb{Z}[t]/(t^n-1)$.

Proof. Since $\gcd(a, n) = 1$, we see that $S_a(t) = \frac{t^a-1}{t-1}$ is a unit when evaluated at any n-th root of unity other than $t = 1$. The second component $S_n(t^i)$ is a sum of the roots of

unity, and is zero except when $t = 1$. Therefore, when $t = \zeta^d$, where $d \mid n, d \neq n$, we have

$$B(\zeta^d, a, n) = \left(\frac{\zeta^{da} - 1}{\zeta^d - 1}\right)^e,$$

which is a unit in $\mathbb{Z}[\zeta^d]$.

At $t = 1$, we have

$$B(1, a, n) = a^e + \frac{1 - ka^e}{n}(n) = 1.$$

Therefore, $B(\zeta^{\frac{n}{d}}, a, n)$ is a unit in $\mathbb{Z}[\zeta_d]$ for every $d \mid n$, and by Lemma 2.1 it is a unit in $\mathbb{Z}G$. $\square$

It was shown [1] that for an abelian group G, the Bass cyclic units generate a subgroup of finite index in $\mathcal{U}(\mathbb{Z}G)$. Therefore, the image of the modified Bass units also generate a subgroup of finite index in $\overset{\oplus}{_{d \mid n}}\mathcal{U}(\mathbb{Z}[\zeta_d])$.

2.3 Showing I is not principal

To prove that the ideal I is not principal for the cases $p = 13, 17$ and 19, we first compute the image of the modified Bass units in $\overset{\oplus}{_{d \mid n}}\mathcal{U}(\mathbb{Z}[\zeta_d])$. This gives us a set containing the coset representatives of $\overset{\oplus}{_{d \mid p-1}}\mathcal{U}(\mathbb{Z}[\zeta_d])$ modulo the image of $\mathcal{U}(\mathbb{Z}G)$. Suppose that $f(t)$ is a principal generator of I. Then for any unit $u(t)$ in $\mathcal{U}(\mathbb{Z}G)$, $f(t)u(t)$ is another generator of I. For each proper divisor d of $p - 1$, we must have $f(\zeta_d) = u_d$, where $u_d \in \mathcal{U}(\mathbb{Z}[\zeta_d])$. If the ideal $\langle p, \zeta_{p-1} - r\rangle \subseteq \mathbb{Z}[\zeta_{p-1}]$ is generated by β, we must have $f(\zeta_{p-1}) = (\beta)(u_{p-1})$, where $u_{p-1} \in \mathcal{U}(\mathbb{Z}[\zeta_{p-1}])$. For each coset representative $(u_{p-1}, \ldots, u_d, \ldots)$ of $\left(\overset{\oplus}{_{d \mid p-1}}\mathcal{U}(\mathbb{Z}[\zeta_d])\right)/\mathcal{U}(\mathbb{Z}G)$, we use Lagrange interpolation to find the

unique $f(t)$ satisfying

$$f(\zeta_{p-1}) = (\beta)(u_{p-1}) \text{ and } f(\zeta_d) = u_d \text{ for each } d \mid p-1, d \neq p-1.$$

If $f(t)$ has integral coefficients, then it is a generator of I. If we do not find an $f(t)$ with integral coefficients, however, then I cannot be principal.

2.3.1 The Case $p = 13$

For the case $p = 13$, it is noted [10], without proof, that I is not principal. We prove that $I = \langle 13, t-2 \rangle$ is not principal in the group ring $\mathbb{Z}[t]/(t^{12}-1)$.

Theorem 2.1. *The ideal $I = \langle 13, t-2 \rangle \subseteq \mathbb{Z}[t]/(t^{12}-1)$ is not principal.*

Proof. We recall the map from the group ring to the maximal order $\overset{\oplus}{_{d \mid 12}}\mathbb{Z}(\zeta_d)$

$$\kappa : \mathbb{Z}[t]/(t^{12}-1) \longrightarrow \mathbb{Z}[\zeta_{12}] \oplus \mathbb{Z}[\zeta_6] \oplus \mathbb{Z}[\zeta_4] \oplus \mathbb{Z}[\zeta_3] \oplus \mathbb{Z} \oplus \mathbb{Z},$$

via

$$f(t) \mapsto (f(\zeta), f(\zeta^2), f(\zeta^3), f(\zeta^4), f(-1), f(1)),$$

where ζ denotes a primitive 12-th root of unity. If I is principal, the generator $f(t)$ must satisfy $f(\zeta_d) \in \mathcal{U}(\mathbb{Z}[\zeta_d])$ for every proper divisor d of 12. Since $I/\Phi_{12}(t)$ is principal and generated by $t^2 - t - 2$, at $t = \zeta$ we must have $f(\zeta) = u \cdot (\zeta^2 - \zeta - 2)$, where $u \in \mathcal{U}(\mathbb{Z}[\zeta])$.

We examine the image of the modified Bass units under the map κ. In $\mathcal{U}(\mathbb{Z}[\zeta])$, a fundamental unit is $\zeta - 1$. We compute the modified Bass unit

$$b(t) = B(t, 5, 12) = -2t^{11} - 2t^{10} - 2t^9 - t^8 + t^6 + 2t^5 + 3t^4 + 2t^3 + t^2 - 1$$

and we see that

$$b(t) \mapsto (\frac{-1}{(\zeta-1)^4}, -\zeta^2, 1, \zeta^4, 1, 1).$$

We note that $B(t,7,12) = t^2 B(t,5,12)$ and $B(t,11,12) = t^{10}$.

Therefore, the coset representatives of the quotient group $\overset{\oplus}{_{d \mid 12}}\mathcal{U}(\mathbb{Z}[\zeta^d])/\langle\kappa(b(t))\rangle$ are contained in the following set.

$$\{(\zeta-1)^i : 0 \leq i \leq 3\} \oplus \{\pm\zeta^2, \pm\zeta^4, \pm 1\} \oplus \{\pm\zeta^3, \pm 1\} \oplus \{\pm\zeta^2, \pm\zeta^4, \pm 1\} \oplus \{\pm 1\} \oplus \{\pm 1\} \subseteq$$
$$\mathcal{U}(\mathbb{Z}[\zeta]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^2]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^3]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^4]) \oplus \mathcal{U}(\mathbb{Z}) \oplus \mathcal{U}(\mathbb{Z})$$

Therefore, there are $4 \times 6 \times 4 \times 6 \times 2 \times 2 = 2,304$ possible values for f, and we see that all of them have non-integral coefficients. See Appendix A.1 for the relevant sage code. Therefore, no such f exists, and the ideal I is not principal. $\square$

2.3.2 The Case $p = 17$

Using a similar method of proof, we show that I is not principal when $p = 17$.

Theorem 2.2. *The ideal $I = \langle 17, t-3\rangle \subseteq \mathbb{Z}[t]/(t^{16}-1)$ is not principal.*

Proof. We recall the map from the group ring to the maximal order $\overset{\oplus}{_{d \mid 16}}\mathbb{Z}(\zeta_d)$

$$\kappa : \mathbb{Z}[t]/(t^{16}-1) \longrightarrow \mathbb{Z}[\zeta_{16}] \oplus \mathbb{Z}[\zeta_8] \oplus \mathbb{Z}[\zeta_4] \oplus \mathbb{Z} \oplus \mathbb{Z},$$

via

$$f(t) \mapsto (f(\zeta), f(\zeta^2), f(\zeta^4), f(-1), f(1)),$$

where ζ denotes a primitive 16-th root of unity. If I is principal, the generator $f(t)$ must

satisfy $f(\zeta_d) \in \mathcal{U}(\mathbb{Z}[\zeta_d])$ for every proper divisor d of 16. Since $I/\Phi_{16}(t)$ is principal and generated by t^5+t^4-1, at $t=\zeta$ we must have $f(\zeta) = u \cdot (\zeta^5+\zeta^4-1)$, where $u \in \mathcal{U}(\mathbb{Z}[\zeta])$.

We examine the image of the modified Bass units under the map κ. The unit group $\mathcal{U}(\mathbb{Z}[\zeta])$ is generated by the cyclotomic units $u_3 = \frac{\zeta^3-1}{\zeta-1}$, $u_5 = \frac{\zeta^5-1}{\zeta-1}$, $u_7 = \frac{\zeta^7-1}{\zeta-1}$ and the units of finite order. The unit group $\mathcal{U}(\mathbb{Z}[\zeta^2])$ is generated by the cyclotomic unit $v = \frac{(\zeta^2)^3-1}{(\zeta^2)-1}$ and the units of finite order. We compute the following modified Bass units

$$\begin{aligned}
b_1(t) = B(t,3,16) = &-5t^{15}-5t^{14}-5t^{13}-5t^{12}-5t^{11}-5t^{10}-5t^9-4t^8-t^7+5t^6+ \\
&11t^5+14t^4+11t^3+5t^2-t-4 \\
b_2(t) = B(t,5,16) = &-35t^{15}-29t^{14}-19t^{13}-4t^{12}+13t^{11}+29t^{10}+41t^9+46t^8+41t^7+ \\
&29t^6+13t^5-4t^4-19t^3-29t^2-35t-37 \\
b_3(t) = B(t,7,16) = &\,30t^{15}+56t^{14}+74t^{13}+81t^{12}+74t^{11}+56t^{10}+30t^9-30t^7-56t^6- \\
&74t^5-80t^4-74t^3-56t^2-30t \\
b_4(t) = B(t^2,3,16) = &-6t^{14}+6t^{10}+9t^8+6t^6-6t^2-8
\end{aligned}$$

and we see that

$$\begin{aligned}
b_1(t) &\mapsto (u_3^4, v^4, 1, 1, 1) \\
b_2(t) &\mapsto (u_5^4, -v^4, 1, 1, 1) \\
b_3(t) &\mapsto (u_7^4, -1, 1, 1, 1) \\
b_4(t) &\mapsto (-u_3^4 u_5^4 u_7^{-4}, 1, 1, 1, 1)
\end{aligned}$$

If we write these in terms of the generators u_3, u_5, u_7 and v, we have

$$\begin{pmatrix} 4 & 0 & 0 & 4 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 4 & 4 & -4 & 0 \end{pmatrix}$$

Row reducing this gives

$$\begin{pmatrix} 4 & 0 & 0 & 4 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix}$$

Therefore, the coset representatives of the quotient group

$$\overset{\oplus}{_{d \mid 16}}\mathcal{U}(\mathbb{Z}[\zeta^d])/\langle \kappa(b_1(t)), \kappa(b_2(t)), \kappa(b_3(t)), \kappa(b_4(t))\rangle,$$

are contained in the following set.

$$\{u_3^i u_5^j u_7^k : 0 \leq i,j,k \leq 3\} \oplus \{\zeta^i v^j : 0 \leq i \leq 15, 0 \leq j \leq 7\} \oplus \{\pm\zeta^4, \pm 1\} \oplus \{\pm 1\} \oplus \{\pm 1\} \subseteq$$
$$\mathcal{U}(\mathbb{Z}[\zeta]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^2]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^4]) \oplus \mathcal{U}(\mathbb{Z}) \oplus \mathcal{U}(\mathbb{Z})$$

Therefore, there are $512 \times 16 \times 4 \times 2 \times 2 = 131,072$ possible values for f, and we see that all of them have non-integral coefficients. See Appendix A.2 for the relevant sage code. Therefore, no such f exists, and the ideal I is not principal. $\square$

2.3.3 The Case $p = 19$

We prove that the ideal $I = \langle 19, t-2\rangle$ is not principal in the group ring $\mathbb{Z}[t]/(t^{18}-1)$.

Theorem 2.3. *The ideal $I = \langle 19, t-2\rangle \subseteq \mathbb{Z}[t]/(t^{18}-1)$ is not principal.*

Proof. We recall the map from the group ring to the maximal order $\bigoplus_{d \mid 18} \mathbb{Z}(\zeta_d)$

$$\kappa : \mathbb{Z}[t]/(t^{18}-1) \longrightarrow \mathbb{Z}[\zeta_{18}] \oplus \mathbb{Z}[\zeta_9] \oplus \mathbb{Z}[\zeta_6] \oplus \mathbb{Z}[\zeta_3] \oplus \mathbb{Z} \oplus \mathbb{Z}$$

via

$$f(t) \mapsto (f(\zeta), f(\zeta^2), f(\zeta^3), f(\zeta^6), f(-1), f(1)),$$

where ζ denotes a primitive 18-th root of unity. If I is principal, the generator $f(t)$ must satisfy $f(\zeta_d) \in \mathcal{U}(\mathbb{Z}[\zeta_d])$ for every proper divisor d of 18. Since $I/\Phi_{18}(t)$ is principal and generated by $t^5 - t^4 + t^3 - t^2 - 1$, at $t = \zeta$ we must have $f(\zeta) = u \cdot (\zeta^5 - \zeta^4 + \zeta^3 - \zeta^2 - 1)$, where $u \in \mathcal{U}(\mathbb{Z}[\zeta])$.

We examine the image of the modified Bass units under the map κ. The unit group $\mathcal{U}(\mathbb{Z}[\zeta]) = \mathcal{U}(\mathbb{Z}[\zeta_9])$ is generated by the cyclotomic units $u_2 = \frac{(-\zeta)^2-1}{-\zeta-1}$ and $u_4 = \frac{(-\zeta)^4-1}{-\zeta-1}$ and the units of finite order. We compute the following modified Bass units

$$\begin{aligned} b_1(t) = B(t,5,18) = &-7t^{17} - 7t^{16} - 7t^{15} - 7t^{14} - 7t^{13} - 6t^{12} - 4t^{11} - t^{10} + 3t^9 + 8t^8 + \\ &11t^7 + 12t^6 + 11t^5 + 8t^4 + 3t^3 - t^2 - 4t - 6 \end{aligned}$$

$$\begin{aligned} b_2(t) = B(t,7,18) = &-16t^{17} - 13t^{16} - 9t^{15} - 4t^{14} + 2t^{13} + 9t^{12} + 14t^{11} + 17t^{10} + 18t^9 + \\ &7t^8 + 14t^7 + 9t^6 + 2t^5 - 4t^4 - 9t^3 - 13t^2 - 16t - 17 \end{aligned}$$

$$b_3(t) = B(t^2,5,18) = t^{16} + 4t^{14} + 5t^{12} + 4t^{10} + t^8 - 3t^6 - 5t^4 - 5t^2 - 3$$

$$b_4(t) = B(t^2,7,18) = t^{16} + t^{14} - 2t^{10} - 2t^8 + t^4 + t^2 + 1$$

and we see that

$$b_1(t) \mapsto (\zeta^3 u_2^{-3} u_4^{-3}, u_2^{-3}, 1, -1, 1, -1)$$

$$b_2(t) \mapsto (-\zeta^3 u_2^{-6} u_4^3, \zeta^{15} u_2^{-3} u_4^3, 1, 1, 1, 1)$$

$$b_3(t) \mapsto (u_2^{-3}, u_2^3 u_4^{-3}, -1, -1, -1, -1)$$

$$b_4(t) \mapsto (\zeta^{15} u_2^{-3} u_4^3, u_4^{-3}, 1, 1, 1, 1)$$

If we write these in terms of the generators u_2 and u_4, we have

$$\begin{pmatrix} -3 & -3 & -3 & 0 \\ -6 & 3 & -3 & 3 \\ -3 & 0 & 3 & -3 \\ -3 & 3 & 0 & -3 \end{pmatrix}$$

Row reducing this gives

$$\begin{pmatrix} 3 & 0 & 0 & -12 \\ 0 & 3 & 0 & -36 \\ 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 21 \end{pmatrix}$$

Therefore, the coset representatives of the quotient group

$$\overset{\oplus}{_{d \mid 18}} \mathcal{U}(\mathbb{Z}[\zeta^d]) / \langle \kappa(b_1(t)), \kappa(b_2(t)), \kappa(b_3(t)), \kappa(b_4(t)) \rangle,$$

are contained in the following set.

$$\{u_2^i u_4^j : 0 \leq i, j \leq 2\} \oplus \{\zeta^i u_2^j u_4^k : 0 \leq i \leq 17, 0 \leq j \leq 2, 0 \leq k \leq 20\} \oplus \{\pm\zeta^3, \pm\zeta^6, \pm 1\} \oplus$$

$$\{\pm\zeta^3, \pm\zeta^6, \pm 1\} \oplus \{\pm 1\} \oplus \{\pm 1\} \subseteq \mathcal{U}(\mathbb{Z}[\zeta]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^2]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^3]) \oplus \mathcal{U}(\mathbb{Z}[\zeta^6]) \oplus \mathcal{U}(\mathbb{Z}) \oplus \mathcal{U}(\mathbb{Z})$$

Therefore, there are $9 \times 18 \times 63 \times 6 \times 6 \times 2 \times 2 = 1,469,664$ possible values for f, and we see that all of them have non-integral coefficients. See Appendix A.3 for the relevant sage code. Therefore, no such f exists, and the ideal I is not principal. $\square$

2.3.4 The Case $p = 23$

We prove that $I = \langle 23, t-5 \rangle$ is not principal in the group ring $\mathbb{Z}[t]/(t^{22}-1)$.

Theorem 2.4. *The ideal $I = \langle 23, t-5 \rangle \subseteq \mathbb{Z}[t]/(t^{22}-1)$ is not principal.*

Proof. Since $I/\Phi_{22}(t)$ is principal and generated by $t^8 - t^7 + 1$, a generator $f(t)$ of I must satisfy

$$f(\zeta) = v \cdot (\zeta^8 - \zeta^7 + 1),$$

where $v \in \mathcal{U}(\mathbb{Z}[\zeta])$ and ζ denotes a primitive 22-nd root of unity. Therefore, $f(t)$ would be of the following form, where $u(\zeta) \in \mathcal{U}(\mathbb{Z}[\zeta])$.

$$f(t) = u(t)(t^8 - t^7 + 1) + g(t)\Phi_{22}(t)$$

Since $-\zeta$ is a primitive 11-th root of unity, we must have $f(-\zeta) \in \mathcal{U}(\mathbb{Z}[-\zeta]) = \mathcal{U}(\mathbb{Z}[\zeta])$. We see that

$$f(-\zeta) = u(-\zeta)(\zeta^8 + \zeta^7 + 1) + g(-\zeta)(2\zeta^9 + 2\zeta^7 + 2\zeta^5 + 2\zeta^3 + 2\zeta).$$

Since $u(\zeta) \equiv u(-\zeta) \pmod 2$, we have

$$f(-\zeta) \equiv u(\zeta)(\zeta^8 + \zeta^7 + 1) \pmod 2.$$

Letting $w = f(-\zeta)u(\zeta)^{-1} \in \mathcal{U}(\mathbb{Z}[\zeta])$, we see that $w \equiv (\zeta^8 + \zeta^7 + 1) \pmod 2$. We show that

there is no such unit w in $\mathcal{U}(\mathbb{Z}[\zeta])$.

We define

$$u_2(t) = \frac{t^2-1}{t-1}, u_3(t) = \frac{t^3-1}{t-1}, u_4(t) = \frac{t^4-1}{t-1}, u_5(t) = \frac{t^5-1}{t-1}$$

and note that $\mathcal{U}(\mathbb{Z}[\zeta])$ is generated by $u_2(-\zeta)$, $u_3(-\zeta)$, $u_4(-\zeta)$, and $u_5(-\zeta)$, along with the units of finite order. We let M denote the matrix representing multiplication by ζ.

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

We see that

$$u_2(-M)^{2^{10}-1} = I \pmod 2,$$

and we note that each of the generators lies in the subgroup of index 3, that is,

$$u_2(-M)^{341} = u_3(-M)^{341} = u_4(-M)^{341} = u_5(-M)^{341} = I \pmod 2.$$

We can see that the matrix $M^8 + M^7 + I$ does not lie in the subgroup of index three, that is

$$(M^8 + M^7 + I)^{341} \not\equiv I \pmod 2.$$

Therefore, there is no unit in $\mathbb{Z}[\zeta]$ equivalent to $(\zeta^8 + \zeta^7 + 1)$ modulo 2, and I cannot be a principal ideal. $\square$

Chapter 3: Lenstra's Method

In the previous chapter, we showed that the ideal I is not principal for $p = 13, 17, 19$ and 23. Therefore, Masuda's techniques are insufficient for these cases. We will make use of Lenstra's result (adapted for our purposes), which gives necessary and sufficient conditions for the rationality of the fixed field. Recall that K is a field of characteristic zero such that $[K(\zeta_p) : K] = p - 1$, and r generates $(\mathbb{Z}/p\mathbb{Z})^\times$.

Theorem 3.1 ([5, Corollary 7.1]). *The fixed field $K(x_0, \ldots, x_{p-1})^\tau$ is rational over K if and only if the ideal $J = \langle p, \zeta_{p-1} - r \rangle$ is principal in $\mathbb{Z}[\zeta_{p-1}]$.*

The ideal J is principal if and only if the ring $\mathbb{Z}[\zeta_{p-1}]$ contains an element of norm p [5, Corollary 7.2]. In practice, this is a computationally difficult problem. Recently, Hoshi summarized the known results over $\mathbb{Q}$ for groups of order $p < 20,000$ [3]. The known rational cases are

$$R = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}.$$

The undetermined cases are

$$U = \{347, 587, 2459, 2819, 3299, 4547, 4787, 6659, 10667, 12227, 14281, 15299, 17027, 17681, 18059, 18481, 18947\}.$$

The cases that are not rational under the GRH are

$$X = \{83, 107, 163, 251, 487, 677, 727, 1187, 1459, 2663, 3779, 4259, 7523, 8837, 10883,$$

$$11699, 12659, 12899, 13043, 13183, 13523, 14243, 14387, 14723, 14867, 16547, 17939, 19379\}.$$

All other cases have been shown to be not rational. For the undetermined cases, our best guess is that they fail to be rational as well.

We describe an algorithm based on Lenstra's proof of Theorem 3.1 to compute generators of the fixed field, given a generator of J. First, however, we establish some preliminary results.

For any divisor d of $p-1$, we let G' denote the quotient group of G of order d. Following [6], we define a ring homomorphism ψ_d as the composition of the quotient map $\mathbb{Z}G \longrightarrow \mathbb{Z}G'$ with the map $\mathbb{Z}G' \longrightarrow \mathbb{Z}[\zeta_d]$ which sends a generator of G' to ζ_d.

$$\psi_d : \mathbb{Z}G \longrightarrow \mathbb{Z}G' \longrightarrow \mathbb{Z}[\zeta_d]$$

We also define a functor as in [5], from the category of G-modules to the category of torsion-free $\mathbb{Z}[\zeta_d]$-modules via

$$F_d(M) = (M \otimes_G \mathbb{Z}[\zeta_d])/\{ \text{ additive torsion } \}.$$

We note that F_d respects direct sums. Applying F_d to I gives

Proposition 3.1 ([5, Proposition 3.6]). *For any divisor $d \neq p-1$, we have $F_d(I) \cong \mathbb{Z}[\zeta_d]$, and if $d = p-1$, $F_d(I)$ is the ideal $\langle p, \zeta_{p-1} - r \rangle$ of $\mathbb{Z}[\zeta_{p-1}]$.*

Proof. For any $d \neq p-1$, we have $(\zeta_d - r) \mid \Phi_d(r) \in \mathbb{Z}$. Since r has order $p-1$ modulo p,

we see $\gcd(p, \Phi_d(r)) = 1$ and therefore $F_d(I) \cong \mathbb{Z}[\zeta_d]$. When $d = p-1$, we have $p \mid \Phi_{p-1}(r)$ and $\gcd(p, \Phi_{p-1}(r)) = p$ and therefore $F_{p-1}(I) \cong \langle p, \zeta_{p-1} - r \rangle$. $\square$

Suppose M is an abelian group, written multiplicatively, with a $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$. Then $L[M]$ denotes the group ring of M over L, that is

$$L[M] = L[b_1, \ldots, b_n, b_1^{-1}, \ldots, b_n^{-1}].$$

We let $L(M)$ denote the field of fractions of $L[M]$.

For example, when $M = Y$, we have $L(Y) = L(y_1, \ldots, y_{p-1})$. Lenstra proves we have an isomorphism of fixed fields when M is a *permutation-projective* $\mathbb{Z}G$-module, that is, a direct summand of a $\mathbb{Z}G$-permutation module.

Theorem 3.2 ([5, Theorem 2.4])**.** *Suppose M is a finitely generated permutation-projective $\mathbb{Z}G$-module. Then we have $L(M)^\pi \cong L(\overset{\oplus}{}_{d \mid p-1} F_d(M))^\pi$, where π acts on $F_d(M)$ via ψ_d.*

Applying this result to $M = \mathbb{Z}G$ gives

$$L(\mathbb{Z}G)^\pi \cong L(\overset{\oplus}{}_{d \mid p-1} \mathbb{Z}[\zeta_d])^\pi.$$

Since $\mathbb{Z}G$ is a permutation module, Proposition 1.3 shows $L(\mathbb{Z}G)^\pi$ is rational over $L^\pi = K$.

It is proved in [11, Proposition 7.1] that if the index of I in $\mathbb{Z}G$ is relatively prime to the order of G, then I is a permutation-projective $\mathbb{Z}G$ module. Applying Theorem 3.2 to I gives

$$L(I)^\pi \cong L(J \oplus \overset{\oplus}{}_{d \mid p-1, d \neq p-1} \mathbb{Z}[\zeta_d])^\pi.$$

If J is a principal ideal, then $J \cong \mathbb{Z}[\zeta_{p-1}]$, and $L(I)^\pi$ is rational over K.

The isomorphism in the previous theorem arises from the following proposition.

Proposition 3.2 ([5, Proposition 1.5]). *Suppose N is a permutation-projective $\mathbb{Z}G$ module, and we have the following exact sequence of finitely generated $\mathbb{Z}$-free $\mathbb{Z}G$-modules*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow N \longrightarrow 0.$$

Then $L(M_2)^\pi$ and $L(M_1 \oplus N)^\pi$ are isomorphic over L^π.

This isomorphism arises from the sequence

$$0 \longrightarrow L(M_1)^\times \longrightarrow L(M_1)^\times \cdot M_2 \xrightarrow{\rho} N \longrightarrow 0,$$

where ρ is defined via

$$\rho(\lambda \cdot m) = m \pmod{M_1} \in N, \text{ where } \lambda \in L(M_1)^\times, m \in M_2.$$

Lenstra proves that the above sequence splits, and we have

$$L(M_2) \cong L(M_1 \oplus N).$$

We note that this is actually a stronger result than the statement of the Proposition. It is shown that the isomorphism respects the action of π, and thus the fixed fields are also isomorphic.

3.1 Computing Generators using Lenstra's Method

We wish to compute generators of the fixed field $L(I)^\pi$ which, along with y_0, generate the fixed field $K(x_0, \ldots, x_{p-1})^\tau$. To do this, we first compute the isomorphism

$$L(\mathbb{Z}G) \cong L(\overset{\oplus}{}_{d \mid p-1} \mathbb{Z}[\zeta_d]).$$

This gives us

$$L(a_0, \ldots, a_{p-2}) = L(b_0, \ldots, b_{p-2}),$$

where G permutes the a_i, that is

$$a_0 \mapsto a_1 \mapsto \cdots \mapsto a_{p-2} \mapsto a_0.$$

The a_i are a renumbering of the Lagrange resolvents y_i to reflect the Galois action. The b_i are acted on via the cyclotomic polynomials $\Phi_d(t)$ for $d \mid p-1$.

We can write the a_i as L-rational functions of the b_i and also write the b_i as L-rational functions of the a_i. Suppose we have

$$a_0 = f_0(b_0, \ldots, b_{p-2}), \;\; a_1 = f_1(b_0, \ldots, b_{p-2}), \ldots, \;\; a_{p-2} = f_{p-2}(b_0, \ldots, b_{p-2}),$$

where the f_i are L-rational functions.

For example, when $|G| = 4$, we compute

$$L(a_0, \ldots, a_3) = L(b_0, \ldots, b_3).$$

Here G permutes the a_i and acts on the b_i via $\Phi_1(t)$, $\Phi_2(t)$ and $\Phi_4(t)$. That is, G acts on two elements via $t-1$ and $t+1$, i.e. b_0 is fixed and b_1 is inverted. The other two elements b_2 and b_3 are acted on via $\Phi_4(t) = t^2+1$, that is

$$G : b_2 \mapsto b_3 \mapsto b_2^{-1} \mapsto b_3^{-1} \mapsto b_2.$$

Since $\mathbb{Z}G$ is a permutation module, we can write generators of $L(\mathbb{Z}G)^\pi$ using Masuda's technique (1.1). That is, we define

$$u_i = \sum_{j=0}^{p-2} \zeta_p^{r^{i+j}} a_j, \quad \text{for } i = 0, \ldots, p-2.$$

Then we have

$$L(\mathbb{Z}G)^\pi = K(y_0, u_0, \ldots, u_{p-2}) = K(y_0, \sum_{j=0}^{p-2} \zeta_p^{r^j} a_j, \ldots, \sum_{j=0}^{p-2} \zeta_p^{r^{p-2+j}} a_j).$$

We can write this in terms of the b_i via

$$L(\mathbb{Z}G)^\pi = K(y_0, \sum_{j=0}^{p-2} \zeta_p^{r^j} f_j(b_0, \ldots, b_{p-2}), \ldots, \sum_{j=0}^{p-2} \zeta_p^{r^{p-2+j}} f_j(b_0, \ldots, b_{p-2})).$$

Next, we compute the isomorphism $L(I) \cong L(J \oplus \overset{\oplus}{}_{d \mid p-1, d \neq p-1} \mathbb{Z}[\zeta_d])$. This gives us

$$L(I) = L(c_0, c_1, \ldots, c_{p-2})$$

such that G acts on the c_i via the $\Phi_d(t)$. Then we substitute the c_i for the b_i in the functions f_j. Since the G-action on the c_i is the same as the b_i (namely the cyclotomic

polynomials), the resulting elements will be permuted by G, that is,

$$f_0(c_0, \ldots, c_{p-2}) \mapsto f_1(c_0, \ldots, c_{p-2}) \mapsto \ldots \mapsto f_{p-2}(c_0, \ldots, c_{p-2}) \mapsto f_0(c_0, \ldots, c_{p-2}).$$

Since this is an invertible operation, we have

$$L(I) = L(f_0(c_0, \ldots, c_{p-2}), f_1(c_0, \ldots, c_{p-2}), \ldots, f_{p-2}(c_0, \ldots, c_{p-2})).$$

We finally have a basis for I that is permuted by G, so we can use Masuda's technique to compute generators of $L(I)^\pi$. We define

$$v_i = \sum_{j=0}^{p-2} \zeta_p^{r^{i+j}} f_j(c_0, \ldots, c_{p-2}), \quad \text{for } i = 0, \ldots, p-2.$$

Then we have

$$L(I)^\pi = K(y_0, v_0, \ldots, v_{p-2}).$$

To compute the field isomorphisms, we use a sequence of short exact sequences and use Proposition 3.2 to decompose $L(M)$ into $L(\overset{\oplus}{}_{d \mid p-1} F_d(M))$. Each short exact sequence is of the form

$$0 \longrightarrow M/f(t) \longrightarrow M/f(t)(t^m - 1) \longrightarrow M/(t^m - 1) \longrightarrow 0,$$

where $M/(t^m - 1)$ is a permutation module. Lenstra shows that this sequence splits, and by explicitly computing the splitting homomorphism, we get an isomorphism

$$L(M/f(t)(t^m - 1)) \cong L(M/f(t) \oplus M/(t^m - 1)).$$

We next describe how we compute a sequence of equivalence relations, which give rise to the sequence of short exact sequences.

3.1.1 Explicit Construction of Field Isomorphisms

We compute a sequence of equivalence relations of the set $E(n) = \{d : d \mid n\}$, as in [5, Lemma 2.10]. Let $G(n)$ denote the set of all equivalence relations on $E(n)$, and let $[u]$ denote the set of non-empty equivalence classes of the equivalence relation u. Let $S(n) \subset G(n) \times G(n)$ denote pairs of equivalence relations $(u, v) \in G(n) \times G(n)$ such that

$$\exists d \in E(n) \text{ and } D \in [u] \text{ s.t. } E(d) \subsetneq D, [v] = \{E(d), D \setminus E(d), C : C \in [u], C \neq D\}. \quad (3.1)$$

Lenstra then proves

Proposition 3.3 ([5, Proposition 2.10])**.** *The graph* $(G(n), S(n))$ *is connected.*

This means that for any equivalence relations u, v on the set $E(n)$, there is a finite sequence $w_0, \ldots, w_r$ such that $w_0 = u$, $w_r = v$ and at each step in the sequence, either (w_i, w_{i+1}) or (w_{i+1}, w_i) is a pair of relations (u, v) satisfying (3.1). We begin with the equivalence relation defined by $[w_0] = \{\{d : d \mid p - 1\}\}$, and end with the relation defined by $[w_r] = \{\{d\} : d \mid p - 1\}$.

3.1.2 The case $p-1=2q$

If p is of the form $p-1=2q$, where q is an odd prime, then the following is a valid sequence.

$$\{\{1,2,q,2q\}\} \mapsto \{\{1,q\},\{2,2q\}\} \mapsto \{\{1\},\{q\},\{2,2q\}\} \mapsto \{\{1,2,2q\},\{q\}\} \mapsto$$
$$\{\{1,2\},\{q\},\{2q\}\} \mapsto \{\{1\},\{2\},\{q\},\{2q\}\}$$

We extend the functor F_m to the category of torsion-free $\mathbb{Z}[t]/f(t)$-modules, where $f(t)$ divides $t^{p-1}-1$ via

$$F'_{f(t)}(M) = (M \otimes_G (\mathbb{Z}[t]/f(t)))/\{ \text{ additive torsion } \}.$$

We note that $F'_{f(t)}$ still respects direct sums.

The sequence of equivalence relations gives rise to the following sequence of exact sequences, where we denote $F'_{f(t)}(M)$ as $M/f(t)$.

$$0 \longrightarrow M/\Phi_{2q}(t)\Phi_2(t) \longrightarrow M/(t^{2q}-1) \longrightarrow M/(t^q-1) \longrightarrow 0$$

$$0 \longrightarrow M/\Phi_q(t) \longrightarrow M/(t^q-1) \longrightarrow M/\Phi_1(t) \longrightarrow 0$$

$$0 \longrightarrow M/\Phi_{2q}(t)\Phi_2(t) \longrightarrow M/\Phi_{2q}(t)\Phi_2(t)\Phi_1(t) \longrightarrow M/\Phi_1(t) \longrightarrow 0$$

$$0 \longrightarrow M/\Phi_{2q}(t) \longrightarrow M/\Phi_{2q}(t)\Phi_2(t)\Phi_1(t) \longrightarrow M/(t^2-1) \longrightarrow 0$$

$$0 \longrightarrow M/\Phi_2(t) \longrightarrow M/(t^2-1) \longrightarrow M/\Phi_1(t) \longrightarrow 0$$

3.1.3 Computing the Splitting Homomorphism

We describe an algorithm for computing the splitting homomorphism. Suppose M is a finitely generated $\mathbb{Z}$-free permutation-projective $\mathbb{Z}G$ module, and suppose we have an exact sequence

$$0 \longrightarrow M/f(t) \longrightarrow M/f(t)(t^m - 1) \xrightarrow{\rho} M/(t^m - 1) \longrightarrow 0.$$

Suppose $f(t)$ is a degree $n - m$ polynomial, $a_0, \ldots, a_{n-1}$ is a $\mathbb{Z}$-basis of $M/f(t)(t^m - 1)$ (written multiplicatively), under the $\mathbb{Z}G$-module isomorphism $ct^i \mapsto a_i^c$, and the a_i are fixed by π^{nm}.

Then we have a $\mathbb{Z}G$-module isomorphism $M/f(t) \cong (t^m - 1)M/f(t)(t^m - 1)$, and the sequence from above gives rise to the exact sequence

$$0 \longrightarrow L((t^m - 1)M/f(t)(t^m - 1))^\times \longrightarrow L((t^m - 1)M/f(t)(t^m - 1))^\times \cdot \langle a_0, \ldots, a_{n-1} \rangle \xrightarrow{\rho} \langle b_0, \ldots, b_{m-1} \rangle \longrightarrow 0,$$

where $\rho : a_i \mapsto b_j$ such that $j \equiv i \pmod{m}$. The splitting homomorphism

$$\sigma : \langle b_0, \ldots b_{m-1} \rangle \longrightarrow L((t^m - 1)M/f(t)(t^m - 1))^\times \cdot \langle a_0, \ldots, a_{n-1} \rangle$$

must send b_0 to an element fixed by π^m.

Suppose we have an element $x \in \langle a_0, \ldots, a_{n-1} \rangle$ such that $\rho(x) = b_0$. We define

$$y = \frac{\pi^m(x)}{x}$$

and

$$\sigma(b_0) = x(1 + \frac{\pi^m(x)}{x} + \frac{\pi^m(x)}{x}\frac{\pi^{2m}(x)}{\pi^m(x)} + \frac{\pi^m(x)}{x}\frac{\pi^{2m}(x)}{\pi^m(x)} \cdots \frac{\pi^{(n-1)m}(x)}{\pi^{(n-2)m}(x)})$$
$$= x + \pi^m(x) + \cdots + \pi^{(n-1)m}(x).$$

We note that

$$\frac{\pi^m(x)}{x}, \ldots, \frac{\pi^{(n-1)m}(x)}{\pi^{(n-2)m}(x)} \in L((t^m - 1)M/f(t)(t^m - 1))^{\times}.$$

We can also see that $\sigma(b_0)$ is fixed by π^m, since

$$\pi^m(x + \pi^m(x) + \cdots + \pi^{(n-1)m}(x)) = \pi^m(x) + \pi^{2m}(x) + \cdots + \pi^{(n-2)m}(x) + x = \sigma(b_0).$$

Therefore, σ defines a valid splitting homomorphism for the sequence. A technique for finding the splitting homomorphism will be given in § 5 through § 10.

Chapter 4: Groups of Small Order

4.1 The case $A = \mathbb{Z}/3\mathbb{Z}$

We demonstrate Lenstra's techniques by computing generators of the fixed field for $p = 3$ and 5. Starting with the fixed field $K(x_0, x_1, x_2)^A$, where $A = \langle\tau\rangle \cong \mathbb{Z}/3\mathbb{Z}$, we recall that $K(x_0, x_1, x_2)^A = L(y_0, I)^\pi$. The Galois group $G = \langle\pi\rangle$ of L/K has order two and we have $I = \langle 3, t-2\rangle \subseteq \mathbb{Z}G$ and $J = \langle 3\rangle \subseteq \mathbb{Z}$.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^2-1)) \cong L(\mathbb{Z} \oplus \mathbb{Z}).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle y_1, y_2\rangle$, where π swaps y_1 and y_2. We note that the y_i are the same as the a_i from § 3.1. Using the exact sequence

$$0 \longrightarrow \mathbb{Z}[t]/(t+1) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0,$$

we have $\mathbb{Z}[t]/(t+1) \cong (t-1)\mathbb{Z}[t]/(t^2-1) = \langle\frac{y_2}{y_1}\rangle$. Therefore, we have the exact sequence

$$0 \longrightarrow L(\frac{y_2}{y_1})^\times \longrightarrow L(\frac{y_2}{y_1})^\times \cdot \langle y_1, y_2\rangle \xrightarrow{\rho} \langle z\rangle \longrightarrow 0,$$

where ρ sends the y_i to z.

We compute the splitting homomorphism from § 3.1.3

$$\sigma : \langle z \rangle \longrightarrow L(\frac{y_2}{y_1})^{\times} \cdot \langle y_1, y_2 \rangle.$$

Letting $x = y_1$, we can see that $\rho(x) = z$ and

$$\sigma(z) = (1 + \frac{\pi(x)}{x})x = (1 + \frac{y_2}{y_1})y_1 = y_1 + y_2,$$

which is fixed by π as required. Therefore, Proposition 3.2 gives

$$L(y_1, y_2) = L(\frac{y_2}{y_1}, y_1 + y_2) \tag{4.1}$$

We can see that this gives the isomorphism

$$L(\mathbb{Z}[t]/(t^2 - 1)) \cong L(\mathbb{Z}[t]/(t-1) \oplus \mathbb{Z}[t]/(t+1)) = L(\gamma_1, \gamma_2)$$

where π fixes $\gamma_1 = y_1 + y_2$ and inverts $\gamma_2 = \frac{y_2}{y_1}$. We note that the elements y_1 and y_2 are a basis for the permutation module $\mathbb{Z}G$. We write these in terms of the γ_i via

$$y_1 = \frac{\gamma_1}{1 + \gamma_2},\ y_2 = \frac{\gamma_1}{1 + \gamma_2^{-1}}.$$

We note that the γ_i are the same as the b_i from § 3.1.

Using Masuda's technique (1.1), we compute generators of the fixed field $L(\mathbb{Z}G)^{\pi} = K(u_0, u_1)$ via

$$\begin{pmatrix} u_0 \\ u_1 \end{pmatrix} = T \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \zeta_3 & \zeta_3^2 \\ \zeta_3^2 & \zeta_3 \end{pmatrix} \cdot \begin{pmatrix} \frac{\gamma_1}{1+\gamma_2} \\ \frac{\gamma_1}{1+\gamma_2^{-1}} \end{pmatrix}.$$

We next compute the isomorphism

$$L(I) \cong L(I/(t+1) \oplus I/(t-1)),$$

where $I = \langle 3, t-2 \rangle \subseteq \mathbb{Z}[t]/(t^2-1)$. Using the exact sequence

$$0 \longrightarrow I/(t+1) \longrightarrow I \longrightarrow I/(t-1) \longrightarrow 0,$$

we have $I/(t+1) \cong (t-1)I/(t^2-1) = \langle 3(t-1) \rangle = \langle \frac{y_2^3}{y_1^3} \rangle = \gamma_2^3$, and therefore

$$0 \longrightarrow L(\frac{y_2^3}{y_1^3})^\times \longrightarrow L(\frac{y_2^3}{y_1^3})^\times \cdot I \xrightarrow{\rho} \langle z \rangle \longrightarrow 0,$$

where ρ sends the y_i to z.

We compute the splitting homomorphism $\sigma : \langle z \rangle \longrightarrow L(\frac{y_2^3}{y_1^3})^\times \cdot I$. Letting $x = \frac{y_1^2}{y_2}$, we can see that $\rho(x) = z$ and

$$\sigma(z) = (1 + \frac{\pi(x)}{x})x = (1 + \frac{y_2^3}{y_1^3})\frac{y_1^2}{y_2} = \frac{y_1^2}{y_2} + \frac{y_2^2}{y_1},$$

which is again fixed by π. Therefore, Proposition 3.2 gives

$$L(I) = L(\delta_1, \delta_2),$$

where π fixes $\delta_1 = \frac{y_1^2}{y_2} + \frac{y_2^2}{y_1}$ and inverts $\delta_2 = \frac{y_2^3}{y_1^3}$. We note that the δ_i are the same as the c_i from § 3.1.

Therefore, we compute the fixed field $L(I)^\pi = K(v_0, v_1)$ via

$$\begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = T \cdot \begin{pmatrix} \frac{\delta_1}{1+\delta_2} \\ \frac{\delta_1}{1+\delta_2^{-1}} \end{pmatrix} = \begin{pmatrix} \zeta_3 & \zeta_3^2 \\ \zeta_3^2 & \zeta_3 \end{pmatrix} \cdot \begin{pmatrix} \frac{y_1^2}{y_2} \\ \frac{y_2^2}{y_1} \end{pmatrix}.$$

Thus we have $K(x_0, x_1, x_2)^\tau = K(y_0, v_0, v_1)$. We note that this is the same solution as [7].

4.2 The case $A = \mathbb{Z}/5\mathbb{Z}$

We next compute generators of the fixed field $L(x_0, \ldots, x_4)^A$, where $A = \mathbb{Z}/5\mathbb{Z}$. The Galois group $G = \langle \pi \rangle$ of L/K has order 4 and we have $I = \langle 5, t-2 \rangle \subseteq \mathbb{Z}G$ and $J = \langle 1 + 2i \rangle \subseteq \mathbb{Z}[i]$.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^4 - 1)) \cong L(\overset{\oplus}{}_{d \mid 4} \mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_3 \rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_3 \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action. We note that the a_i are the same as the a_i from § 3.1.

Using the exact sequence

$$0 \longrightarrow \mathbb{Z}[t]/(t^2+1) \longrightarrow \mathbb{Z}[t]/(t^4-1) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow 0,$$

we have $\mathbb{Z}[t]/(t^2+1) \cong (t^2-1)\mathbb{Z}[t]/(t^4-1) = \langle \frac{a_2}{a_0}, \frac{a_3}{a_1} \rangle$, and we have the exact sequence

$$0 \longrightarrow L(\frac{a_2}{a_0}, \frac{a_3}{a_1})^\times \longrightarrow L(\frac{a_2}{a_0}, \frac{a_3}{a_1}))^\times \cdot \langle a_0, a_1, a_2, a_3 \rangle \xrightarrow{\rho} \langle b_0, b_1 \rangle \longrightarrow 0,$$

where $\rho : a_{2i+j} \mapsto b_j$ for $0 \leq i, j \leq 1$.

We compute the splitting homomorphism $\sigma : \langle b_0, b_1 \rangle \longrightarrow L(\frac{a_2}{a_0}, \frac{a_3}{a_1})^{\times} \cdot \langle a_0, \ldots, a_3 \rangle$. Letting $x = a_0$, we can see that $\rho(x) = b_0$, $y = \frac{\pi^2(x)}{x} = \frac{a_2}{a_0}$, and

$$\sigma(b_0) = (1 + \frac{\pi^2(x)}{x})x = a_0 + a_2,$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(a_0, a_1, a_2, a_3) = L(\frac{a_2}{a_0}, \frac{a_3}{a_1}, a_0 + a_2, a_1 + a_3)$$

We see that the generators $a_0 + a_2$ and $a_1 + a_3$ are swapped by π, and therefore generate a module isomorphic to $\mathbb{Z}[t]/(t^2-1)$. We use the result from the previous section, namely

$$L(u, v) = L(\frac{v}{u}, u + v).$$

Therefore, we have an isomorphism

$$L(\mathbb{Z}[t]/(t^4 - 1)) \cong L(\gamma_1, \gamma_2, \gamma_{4,0}, \gamma_{4,1}), \tag{4.2}$$

where π fixes $\gamma_1 = a_0+a_1+a_2+a_3$, inverts $\gamma_2 = \frac{a_1+a_3}{a_0+a_2}$, and acts on $\gamma_{4,0} = \frac{a_2}{a_0}$ and $\gamma_{4,1} = \frac{a_3}{a_1}$ via $\Phi_4(t)$, that is,

$$\pi : \gamma_{4,0} \mapsto \gamma_{4,1} \mapsto \gamma_{4,0}^{-1} \mapsto \gamma_{4,1}^{-1} \mapsto \gamma_{4,0}.$$

We note that the a_i are a basis for the permutation module $\mathbb{Z}G$. We write these in terms

of the γ_i via

$$a_0 = \frac{\gamma_1}{(1+\gamma_2)(1+\gamma_{4,0})},\ a_1 = \frac{\gamma_1}{(1+\gamma_2^{-1})(1+\gamma_{4,1})},$$
$$a_2 = \frac{\gamma_1}{(1+\gamma_2)(1+\gamma_{4,0}^{-1})},\ a_3 = \frac{\gamma_1}{(1+\gamma_2^{-1})(1+\gamma_{4,1}^{-1})}.$$

We note that the γ_i are the same as the b_i from § 3.1.

Using Masuda's technique (1.1), we compute generators $u_0, \ldots, u_3$ of the fixed field $L(\mathbb{Z}G)^\pi$ via

$$\begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix} = T \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} \zeta & \zeta^2 & \zeta^4 & \zeta^3 \\ \zeta^2 & \zeta^4 & \zeta^3 & \zeta \\ \zeta^4 & \zeta^3 & \zeta & \zeta^2 \\ \zeta^3 & \zeta & \zeta^2 & \zeta^4 \end{pmatrix} \cdot \begin{pmatrix} \frac{\gamma_1}{(1+\gamma_2)(1+\gamma_{4,0})} \\ \frac{\gamma_1}{(1+\gamma_2^{-1})(1+\gamma_{4,1})} \\ \frac{\gamma_1}{(1+\gamma_2)(1+\gamma_{4,0}^{-1})} \\ \frac{\gamma_1}{(1+\gamma_2^{-1})(1+\gamma_{4,1}^{-1})} \end{pmatrix}$$

Therefore, we have $L(\mathbb{Z}G)^\pi = K(u_0, \ldots, u_3)$.

We next compute the isomorphism

$$L(I) \cong L(\overset{\oplus}{}_{d \mid 4} I/\Phi_d(t)),$$

where $I = \langle 5, t-2 \rangle$. Using the exact sequence

$$0 \longrightarrow I/(t^2+1) \longrightarrow I/(t^4-1) \longrightarrow I/(t^2-1) \longrightarrow 0,$$

and the fact that $I/(t^2+1)$ is generated by $1+2t$, we have

$$I/(t^2+1) \cong (t^2-1)I/(t^4-1) = \langle 2t^3 + t^2 - 2t - 1 \rangle.$$

Therefore, we have

$$0 \longrightarrow L(\frac{a_3^2 a_2}{a_0 a_1^2}, \frac{a_0^2 a_3}{a_1 a_2^2})^{\times} \longrightarrow L(\frac{a_3^2 a_2}{a_0 a_1^2}, \frac{a_0^2 a_3}{a_1 a_2^2})^{\times} \cdot I \xrightarrow{\rho} \langle b_0, b_1 \rangle \longrightarrow 0.$$

where $\rho : a_{2i+j} \mapsto b_j$ for $0 \leq i, j \leq 1$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1 \rangle \longrightarrow L(\frac{a_3^2 a_2}{a_0 a_1^2}, \frac{a_0^2 a_3}{a_1 a_2^2})^{\times} \cdot I.$$

Letting $x = \frac{a_0 a_1}{a_3}$, we can see that $x \in I$, $\rho(x) = b_0$ and

$$\sigma(b_0) = (1 + \frac{\pi^2(x)}{x})x = \frac{a_0 a_1}{a_3} + \frac{a_2 a_3}{a_1},$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(I) = L(\frac{a_3^2 a_2}{a_0 a_1^2}, \frac{a_0^2 a_3}{a_1 a_2^2}, \frac{a_0 a_1}{a_3} + \frac{a_2 a_3}{a_1}, \frac{a_1 a_2}{a_0} + \frac{a_0 a_3}{a_2}).$$

Since the last two generators are swapped by π, we use the result from the previous section. This gives the isomorphism

$$L(I) \cong L(\delta_1, \delta_2, \delta_{4,0}, \delta_{4,1})$$

where π fixes $\delta_1 = \frac{a_0 a_1}{a_3} + \frac{a_2 a_3}{a_1} + \frac{a_1 a_2}{a_0} + \frac{a_0 a_3}{a_2}$, inverts $\delta_2 = \frac{\frac{a_1 a_2}{a_0} + \frac{a_0 a_3}{a_2}}{\frac{a_0 a_1}{a_3} + \frac{a_2 a_3}{a_1}}$, and acts on $\delta_{4,0} = \frac{a_3^2 a_2}{a_0 a_1^2}$ and $\delta_{4,1} = \frac{a_0^2 a_3}{a_1 a_2^2}$ via $\Phi_4(t)$. We note that the δ_i are the same as the c_i from § 3.1.

Therefore, we compute the fixed field $L(I)^{\pi} = K(v_0, v_1, v_2, v_3)$ via

$$\begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = T \cdot \begin{pmatrix} \frac{\delta_1}{(1+\delta_2)(1+\delta_{4,0})} \\ \frac{\delta_1}{(1+\delta_2^{-1})(1+\delta_{4,1})} \\ \frac{\delta_1}{(1+\delta_2)(1+\delta_{4,0}^{-1})} \\ \frac{\delta_1}{(1+\delta_2^{-1})(1+\delta_{4,1}^{-1})} \end{pmatrix} = \begin{pmatrix} \zeta_5 & \zeta_5^2 & \zeta_5^4 & \zeta_5^3 \\ \zeta_5^2 & \zeta_5^4 & \zeta_5^3 & \zeta_5 \\ \zeta_5^4 & \zeta_5^3 & \zeta_5 & \zeta_5^2 \\ \zeta_5^3 & \zeta_5 & \zeta_5^2 & \zeta_5^4 \end{pmatrix} \cdot \begin{pmatrix} \frac{a_0 a_1}{a_3} \\ \frac{a_1 a_2}{a_0} \\ \frac{a_3 a_2}{a_1} \\ \frac{a_0 a_3}{a_2} \end{pmatrix}$$

Thus we have $K(x_0, \ldots, x_4)^\tau = K(y_0, v_0, \ldots, v_3)$. Again, we produce the same solution as [7].

Chapter 5: The case $A = \mathbb{Z}/7\mathbb{Z}$

We next compute generators for the fixed field $K(x_0, \ldots, x_6)^A$, where $A = \langle \tau \rangle$. The Galois group $G = \langle \pi \rangle$ of L/K has order six and we have $I = \langle 7, t-3 \rangle \subseteq \mathbb{Z}G$ and $J = \langle 7, \zeta - 3 \rangle = \langle \zeta - 3 \rangle \subseteq \mathbb{Z}[\zeta]$, where ζ denotes a primitive sixth root of unity.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^6 - 1)) \cong L(\overset{\oplus}{}_{d \mid 6} \mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_5 \rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_5 \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action.

We first compute the sequence of equivalence relations of $p - 1 = 6$; from (3.1.2) we have the following.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^6 - 1) \longrightarrow \mathbb{Z}[t]/(t^3 - 1) \longrightarrow 0 \tag{5.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_3(t) \longrightarrow \mathbb{Z}[t]/(t^3 - 1) \longrightarrow \mathbb{Z}[t]/(t - 1) \longrightarrow 0 \tag{5.2}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t) \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t - 1) \longrightarrow 0 \tag{5.3}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_6(t) \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^2 - 1) \longrightarrow 0 \tag{5.4}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^2 - 1) \longrightarrow \mathbb{Z}[t]/(t - 1) \longrightarrow 0 \tag{5.5}$$

Starting with (5.1), we have

$$\mathbb{Z}[t]/(t^3+1) \cong (t^3-1)\mathbb{Z}[t]/(t^6-1) = \langle \frac{a_3}{a_0}, \frac{a_4}{a_1}, \frac{a_5}{a_2} \rangle.$$

Therefore, we have the exact sequence

$$0 \longrightarrow L(\frac{a_3}{a_0}, \frac{a_4}{a_1}, \frac{a_5}{a_2})^\times \longrightarrow L(\frac{a_3}{a_0}, \frac{a_4}{a_1}, \frac{a_5}{a_2})^\times \cdot \langle a_0, \ldots, a_5 \rangle \xrightarrow{\rho} \langle b_0, b_1, b_2 \rangle \longrightarrow 0,$$

where ρ maps $a_{3i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, 1, 2$.

We compute the splitting homomorphism from (3.1.3)

$$\sigma : \langle b_0, b_1, b_2 \rangle \longrightarrow L(\frac{a_3}{a_0}, \frac{a_4}{a_1}, \frac{a_5}{a_2})^\times \cdot \langle a_0, \ldots, a_5 \rangle.$$

Letting $x = a_0$, we can see that $\rho(x) = b_0$, $y = \frac{\pi^3(x)}{x} = \frac{a_3}{a_0}$, and

$$\sigma(b_0) = (1 + \frac{\pi^3(x)}{x})x = a_0 + a_3 \in L(\frac{a_3}{a_0}, \frac{a_4}{a_1}, \frac{a_5}{a_2})^\times \cdot \langle a_0, \ldots, a_5 \rangle.$$

We see $\sigma(b_0)$ is fixed by π^3, and thus we have a valid splitting homomorphism.

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^6-1)) \cong L(a_0, \ldots, a_5) = L(\frac{a_3}{a_0}, \frac{a_4}{a_1}, \frac{a_5}{a_2}, a_0 + a_3, a_1 + a_4, a_2 + a_5). \tag{5.6}$$

We see this explicitly if we let

$$c_0 = a_0 + a_3,\ c_1 = a_1 + a_4,\ c_2 = a_2 + a_5,\ d_0 = \frac{a_3}{a_0},\ d_1 = \frac{a_4}{a_1},\ d_2 = \frac{a_5}{a_2}.$$

Then we have

$$a_0 = \frac{c_0}{1+d_0},\ \ldots, a_3 = \frac{c_0}{1+d_0^{-1}},\ \ldots, a_5 = \frac{c_2}{1+d_2^{-1}}.$$

We can see that c_0, c_1 and c_2 are permuted cyclically by π and generate a module isomorphic to $\mathbb{Z}[t]/(t^3-1)$. Using these in sequence (5.2), we have

$$\mathbb{Z}[t]/\Phi_3(t) \cong (t-1)\mathbb{Z}[t]/(t^3-1) = \langle \frac{c_1}{c_0}, \frac{c_2}{c_1} \rangle.$$

Writing $\mathbb{Z}[t]/(t-1) = \langle \omega \rangle$, we have the exact sequence

$$0 \longrightarrow L(\frac{c_1}{c_0}, \frac{c_2}{c_1})^\times \longrightarrow L(\frac{c_1}{c_0}, \frac{c_2}{c_1})^\times \cdot \langle c_0, c_1, c_2 \rangle \xrightarrow{\rho} \langle \omega \rangle \longrightarrow 0,$$

where ρ maps the c_i to ω.

We compute the splitting homomorphism $\sigma : \langle \omega \rangle \longrightarrow L(\frac{c_1}{c_0}, \frac{c_2}{c_1})^\times \cdot \langle c_0, c_1, c_2 \rangle$. Letting $x = c_0$ and $y = \frac{\pi(x)}{x} = \frac{c_1}{c_0}$, we define σ via

$$\sigma(\omega) = (1 + \frac{\pi(x)}{x} + \frac{\pi(x)}{x}\frac{\pi^2(x)}{\pi(x)})x = c_0 + c_1 + c_2,$$

which is fixed by π as required.

Therefore, Proposition 3.2 gives

$$L(c_0, c_1, c_2) = L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, c_0 + c_1 + c_2). \tag{5.7}$$

We define

$$\gamma_{3,0} = \frac{c_1}{c_0},\ \gamma_{3,1} = \frac{c_2}{c_1},\ \gamma_1 = c_0 + c_1 + c_2.$$

We can see explicitly that $L(c_0, c_1, c_2) = L(\gamma_{3,0}, \gamma_{3,1}, \gamma_1)$, since

$$c_0 = \frac{\gamma_1}{1 + \gamma_{3,0} + \gamma_{3,0}\gamma_{3,1}}, \ \ldots, c_2 = \frac{\gamma_1}{1 + \gamma_{3,0}^{-1}\gamma_{3,1}^{-1} + \gamma_{3,1}^{-1}}. \tag{5.8}$$

We note that π acts on $\gamma_{3,0}$ and $\gamma_{3,1}$ via $\Phi_3(t)$, and fixes γ_1, that is,

$$\pi : \gamma_{3,0} \mapsto \gamma_{3,1} \mapsto \gamma_{3,0}^{-1}\gamma_{3,1}^{-1}$$

Combining this result with (5.6), we have

$$L(\mathbb{Z}[t]/(t^6 - 1)) \cong L(d_0, d_1, d_2, \gamma_{3,0}, \gamma_{3,1}, \gamma_1) \tag{5.9}$$

Next, we compute generators of $L(\mathbb{Z}[t]/(t^3+1))$ that π acts on via Φ_6 and Φ_2. From (5.5) we have

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^2 - 1) \longrightarrow \mathbb{Z}[t]/(t - 1) \longrightarrow 0.$$

Writing $\mathbb{Z}[t]/(t^2 - 1) = \langle u, v \rangle$, from (4.1) we have

$$L(u, v) = L(\frac{v}{u}, u + v),$$

where π fixes $u + v$ and inverts $\frac{v}{u}$.

We use this result in sequence (5.4), where we had

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_6(t) \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^2 - 1) \longrightarrow 0.$$

Since $\Phi_6(t)\Phi_2(t)\Phi_1(t) = t^4 - t^3 + t - 1$, we have a $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t)$ and the multiplicative group $\langle e_0, e_1, e_2, e_3\rangle$ via $t^i \mapsto e_i$, where π acts via

$$e_0 \mapsto e_1 \mapsto \cdots \mapsto e_3 \mapsto \frac{e_3e_0}{e_1} \mapsto \frac{e_3e_0}{e_2} \mapsto e_0.$$

Therefore, we have

$$\mathbb{Z}[t]/\Phi_6(t) \cong (t^2-1)\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) = \langle \frac{e_2}{e_0}, \frac{e_3}{e_1}\rangle$$

and

$$0 \longrightarrow L(\frac{e_2}{e_0}, \frac{e_3}{e_1})^\times \longrightarrow L(\frac{e_2}{e_0}, \frac{e_3}{e_1})^\times \cdot \langle e_0, \ldots, e_3\rangle \xrightarrow{\rho} \langle f_0, f_1\rangle \longrightarrow 0,$$

where $\rho(e_{2i+j}) = f_j$, for $0 \le i, j \le 1$.

We compute the splitting homomorphism $\sigma : \langle f_0, f_1\rangle \longrightarrow L(\frac{e_2}{e_0}, \frac{e_3}{e_1})^\times \cdot \langle e_0, \ldots, e_3\rangle$. Letting $x = e_0$ and $y = \frac{\pi^2(x)}{x} = \frac{e_2}{e_0}$, we define σ via

$$\sigma(f_0) = (1 + \frac{\pi^2(x)}{x} + \frac{\pi^2(x)}{x}\frac{\pi^4(x)}{\pi^2(x)})x = e_0 + e_2 + \frac{e_3e_0}{e_1},$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{e_2}{e_0}, \frac{e_3}{e_1}, e_0 + e_2 + \frac{e_3e_0}{e_1}, e_1 + e_3 + \frac{e_3e_0}{e_2}).$$

We combine this with the previous result, since the last two generators are swapped by π.

$$L(\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{e_2}{e_0}, \frac{e_3}{e_1}, \frac{e_1 + e_3 + \frac{e_3e_0}{e_2}}{e_0 + e_2 + \frac{e_3e_0}{e_1}}, e_0 + e_1 + \ldots + \frac{e_3e_0}{e_2}) \qquad (5.10)$$

From sequence (5.3) we had the following.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t) \longrightarrow \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0$$

In this sequence, we have a description of the field corresponding to the middle component and the right component. We use these to find a description of $L(\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t))$. We have

$$\mathbb{Z}[t]/(t^3+1) \cong (t-1)\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \cong \langle \frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2} \rangle.$$

Writing $\mathbb{Z}[t]/\Phi_1(t) = \langle \omega \rangle$, we have

$$0 \longrightarrow L(\frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2})^\times \longrightarrow L(\frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2})^\times \cdot \langle e_0, \ldots, e_3 \rangle \xrightarrow{\rho} \langle \omega \rangle \longrightarrow 0.$$

We compute the splitting homomorphism $\sigma : \langle \omega \rangle \longrightarrow L(\frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2})^\times \cdot \langle e_0, \ldots, e_3 \rangle$. Since we already have the generator $e_0 + e_1 + \ldots + \frac{e_3 e_0}{e_2}$ fixed by π, we define $x = e_0$ and $y = \frac{\pi(x)}{x} = \frac{e_1}{e_0}$, and we have

$$\sigma(\omega) := (1 + \frac{e_1}{e_0} + \frac{e_1}{e_0}\frac{e_2}{e_1} + \cdots + \frac{e_1}{e_0}\frac{e_2}{e_1}\cdots\frac{e_1}{e_2})e_0 = e_0 + e_1 + \ldots + \frac{e_3 e_0}{e_2}.$$

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2}, e_0 + e_1 + \ldots + \frac{e_3 e_0}{e_2}).$$

We define

$$\gamma_{6,0} = \frac{e_2}{e_0},\ \gamma_{6,1} = \frac{e_3}{e_1},\ \gamma_2 = \frac{e_1 + e_3 + \frac{e_3 e_0}{e_2}}{e_0 + e_2 + \frac{e_3 e_0}{e_1}},$$

and combine the result with (5.10) to obtain

$$L(\frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2}, e_0 + e_1 + \ldots + \frac{e_3 e_0}{e_2}) \cong L(\gamma_{6,0}, \gamma_{6,1}, \gamma_2, e_0 + e_1 + \ldots + \frac{e_3 e_0}{e_2}).$$

Therefore, we have a description of $L(\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)) = L(\mathbb{Z}[t]/(t^3+1))$.

$$L(\mathbb{Z}[t]/(t^3+1)) \cong L(\frac{e_1}{e_0}, \frac{e_2}{e_1}, \frac{e_3}{e_2}) = L(\gamma_{6,0}, \gamma_{6,1}, \gamma_2) \tag{5.11}$$

We note that π inverts γ_2, and acts on the $\gamma_{6,j}$ via Φ_6, that is

$$\pi : \gamma_{6,0} \mapsto \gamma_{6,1} \mapsto \gamma_{6,1}\gamma_{6,0}^{-1}.$$

We see that the following isomorphism is multiplication by $\Phi_3(t)$

$$\langle e_0, \ldots e_3 \rangle \cong \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \cong \Phi_3(t)\mathbb{Z}[t]/(t^6-1).$$

Therefore,

$$e_0 = a_0a_1a_2,\ e_1 = a_1a_2a_3,\ \ldots,\ e_3 = a_3a_4a_5$$

and we have

$$\frac{e_1}{e_0} = \frac{a_3}{a_0} = d_0,\ \frac{e_2}{e_1} = \frac{a_4}{a_1} = d_1,\ \frac{e_3}{e_2} = \frac{a_5}{a_2} = d_2.$$

We can see $L(d_0, d_1, d_2) = L(\gamma_{6,0}, \gamma_{6,1}, \gamma_2)$ explicitly, since

$$\gamma_{6,0} = d_0d_1,\ \gamma_{6,1} = d_1d_2,\ \gamma_2 = d_0\left(\frac{1 + \gamma_{6,1} + \gamma_{6,1}\pi^2(\gamma_{6,1})}{1 + \gamma_{6,0} + \gamma_{6,0}\pi^2(\gamma_{6,0})}\right)$$

and

$$d_0 = \gamma_2\left(\frac{1+\gamma_{6,0}+\gamma_{6,0}\pi^2(\gamma_{6,0})}{1+\gamma_{6,1}+\gamma_{6,1}\pi^2(\gamma_{6,1})}\right),\ \ldots, d_2 = \gamma_2\left(\frac{1+\pi^2(\gamma_{6,0})+\pi^2(\gamma_{6,0})\pi^4(\gamma_{6,0})}{1+\pi^2(\gamma_{6,1})+\pi^2(\gamma_{6,1})\pi^4(\gamma_{6,1})}\right) \quad (5.12)$$

We combine (5.11) with (5.9) to obtain the isomorphism

$$L(\mathbb{Z}[t]/(t^6-1)) \cong L(\overset{\oplus}{}_{d\mid 6}\mathbb{Z}[t]/\Phi_d(t)) = L(\gamma_1,\gamma_2,\gamma_{3,0},\gamma_{3,1},\gamma_{6,0},\gamma_{6,1}).$$

We can also write this in terms of the a_i

$$L(\mathbb{Z}[t]/(t^6-1)) \cong L(a_0+a_1+\cdots+a_5, \frac{a_1a_2a_3+a_0a_1a_5+a_3a_4a_5}{a_0a_1a_2+a_2a_3a_4+a_0a_4a_5}, \frac{a_1+a_4}{a_0+a_3}, \frac{a_2+a_5}{a_1+a_4}, \frac{a_3a_4}{a_0a_1}, \frac{a_4a_5}{a_1a_2}). \quad (5.13)$$

We note that a_0 and its π-conjugates, namely $a_0,\ldots,a_5$, are a permutation basis of $\mathbb{Z}G$. We write the permutation basis in terms of the γ_i; it suffices to express a_0 in terms of the γ_i. From (5.8) and (5.12) we have

$$c_0 = \frac{\gamma_1}{1+\gamma_{3,0}+\gamma_{3,0}\gamma_{3,1}},\ d_0 = \frac{\gamma_2(1+\gamma_{6,0}+\gamma_{6,0}\pi^2(\gamma_{6,0}))}{1+\gamma_{6,1}+\gamma_{6,1}\pi^2(\gamma_{6,1})}$$

Finally, we can write a_0 via

$$a_0 = \frac{c_0}{1+d_0}.$$

5.1 Computing the fixed field of I

We next compute the isomorphism

$$L(I) \cong L(J \oplus \overset{\oplus}{}_{d \mid 6, d \neq 6} \mathbb{Z}[\zeta_d]),$$

where $I = \langle 7, t-3 \rangle$. From (3.1.2) we have the following.

$$0 \longrightarrow I/\Phi_6(t)\Phi_2(t) \longrightarrow I/(t^6-1) \longrightarrow I/(t^3-1) \longrightarrow 0 \tag{5.14}$$

$$0 \longrightarrow I/\Phi_3(t) \longrightarrow I/(t^3-1) \longrightarrow I/(t-1) \longrightarrow 0 \tag{5.15}$$

$$0 \longrightarrow I/\Phi_6(t)\Phi_2(t) \longrightarrow I/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t-1) \longrightarrow 0 \tag{5.16}$$

$$0 \longrightarrow I/\Phi_6(t) \longrightarrow I/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^2-1) \longrightarrow 0 \tag{5.17}$$

$$0 \longrightarrow I/\Phi_2(t) \longrightarrow I/(t^2-1) \longrightarrow I/(t-1) \longrightarrow 0 \tag{5.18}$$

Again using the $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^6-1)$ and the multiplicative group $\langle a_0, a_1, \ldots, a_5 \rangle$ via $t^i \mapsto a_i$, (5.14) gives

$$0 \longrightarrow L((t^3-1)I/(t^6-1))^\times \longrightarrow L((t^3-1)I/(t^6-1))^\times \cdot I/(t^6-1) \xrightarrow{\rho} \langle b_0, b_1, b_2 \rangle \longrightarrow 0,$$

where ρ maps $a_{3i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, 1, 2$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, b_2 \rangle \longrightarrow L((t^3-1)I/(t^6-1))^\times \cdot I/(t^6-1).$$

Since $I = \langle 7, t-3 \rangle$, we have the following generating set for I.

$$I = \langle a_0^7, a_1^7, \ldots, a_5^7, \frac{a_1}{a_0^3}, \frac{a_2}{a_1^3}, \ldots, \frac{a_5}{a_4^3}, \frac{a_0}{a_5^3} \rangle$$

The image of this set under ρ is

$$\langle a_0^7, a_1^7, \ldots, a_5^7, \frac{a_1}{a_0^3}, \frac{a_2}{a_1^3}, \ldots, \frac{a_5}{a_4^3}, \frac{a_0}{a_5^3} \rangle \mapsto \langle b_0^7, b_1^7, \ldots, b_2^7, \frac{b_1}{b_0^3}, \frac{b_2}{b_1^3}, \ldots, \frac{b_0}{b_2^3} \rangle,$$

and therefore in order to find x with $\rho(x) = b_0$, we need to solve

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}^{\mathsf{T}} \cdot \begin{pmatrix} -3 & 1 & 0 \\ 0 & -3 & 1 \\ 1 & 0 & -3 \\ 7 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

The solution $(x_1, x_2, x_3, x_4, x_5, x_6) = (1, 5, 4, 0, 2, 1)$ yields

$$x = \frac{a_1}{a_0^3} \left(\frac{a_2}{a_1^3} \right)^5 \left(\frac{a_3}{a_2^3} \right)^4 (a_1^7)^2 (a_2^7) = \frac{a_3^4}{a_0^3}.$$

We see that $\rho(x) = b_0$, and define σ via

$$\sigma(b_0) = (1 + \frac{\pi^3(x)}{x})x = \frac{a_3^4}{a_0^3} + \frac{a_0^4}{a_3^3},$$

which is fixed by π^3 as required. Therefore, Proposition 3.2 gives

$$L(I/(t^6 - 1)) \cong L(I/(t^3 + 1) \oplus \langle \frac{a_3^4}{a_0^3} + \frac{a_0^4}{a_3^3}, \frac{a_4^4}{a_1^3} + \frac{a_1^4}{a_4^3}, \frac{a_5^4}{a_2^3} + \frac{a_2^4}{a_5^3} \rangle)$$

We define

$$c_0 = \frac{a_3^4}{a_0^3} + \frac{a_0^4}{a_3^3},\ c_1 = \frac{a_4^4}{a_1^3} + \frac{a_1^4}{a_4^3},\ c_2 = \frac{a_5^4}{a_2^3} + \frac{a_2^4}{a_5^3}$$

We see that π acts via $c_0 \mapsto c_1 \mapsto c_2 \mapsto c_0$ and use the result from the previous section, namely

$$L(c_0, c_1, c_2) \cong L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, c_0 + c_1 + c_2).$$

We label $\frac{c_1}{c_0}$ and $\frac{c_2}{c_1}$ as $\gamma_{3,0}$ and $\gamma_{3,1}$, and note that π acts on them via $\Phi_3(t)$.

$$\gamma_{3,0} = \frac{c_1}{c_0} = \frac{\frac{a_4^4}{a_1^3} + \frac{a_1^4}{a_4^3}}{\frac{a_3^4}{a_0^3} + \frac{a_0^4}{a_3^3}},\ \gamma_{3,1} = \frac{c_2}{c_1} = \frac{\frac{a_5^4}{a_2^3} + \frac{a_2^4}{a_5^3}}{\frac{a_4^4}{a_1^3} + \frac{a_1^4}{a_4^3}}$$

We label $\gamma_1 = c_0 + c_1 + c_2$ and note that it is fixed by π. Therefore, we have

$$L(I/(t^6 - 1)) \cong L(I/(t^3 + 1) \oplus \langle \gamma_{3,0}, \gamma_{3,1}, \gamma_1 \rangle) \tag{5.19}$$

Next, we compute generators of $L(I/(t^3 + 1))$ that π acts on via Φ_6 and Φ_2. From (5.18) we have

$$0 \longrightarrow I/\Phi_2(t) \longrightarrow I/(t^2 - 1) \longrightarrow I/(t - 1) \longrightarrow 0.$$

We use the result from (4.1), namely $L(u, v) = L(\frac{v}{u}, u + v)$. We use this result in sequence (5.17)

$$0 \longrightarrow I/\Phi_6(t) \longrightarrow I/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^2 - 1) \longrightarrow 0.$$

Writing $\mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t)$ multiplicatively as $\langle e_0, e_1, e_2, e_3 \rangle$ via $t^i \mapsto e_i$, π acts via

$$e_0 \mapsto e_1 \mapsto \cdots \mapsto e_3 \mapsto \frac{e_3 e_0}{e_1} \mapsto \frac{e_3 e_0}{e_2} \mapsto e_0.$$

The ideal $I/\Phi_6(t)$ is principal and generated by $3-t$, which gives a $\mathbb{Z}G$-module isomorphism

$$I/\Phi_6(t) \cong (t^2-1)I/\Phi_6(t)\Phi_2(t)\Phi_1(t) = \langle -t^3+3t^2+t-3\rangle = \langle \frac{e_1e_2^3}{e_0^3e_3}, \frac{e_2e_3^2}{e_0e_1^2}\rangle$$

and we have

$$0 \longrightarrow L(\frac{e_1e_2^3}{e_0^3e_3}, \frac{e_2e_3^2}{e_0e_1^2})^\times \longrightarrow L(\frac{e_1e_2^3}{e_0^3e_3}, \frac{e_2e_3^2}{e_0e_1^2})^\times \cdot I/\Phi_6(t)\Phi_2(t)\Phi_1(t) \xrightarrow{\rho} \langle f_0, f_1\rangle \longrightarrow 0,$$

where ρ sends $e_{2i+j} \mapsto f_j$, for $i,j = 0,1$.

We compute the splitting homomorphism

$$\sigma : \langle f_0, f_1\rangle \longrightarrow L(\frac{e_1e_2^3}{e_0^3e_3}, \frac{e_2e_3^2}{e_0e_1^2})^\times \cdot I/\Phi_6(t)\Phi_2(t)\Phi_1(t).$$

We have the following generating set for $I/\Phi_6(t)\Phi_2(t)\Phi_1(t)$.

$$I/\Phi_6(t)\Phi_2(t)\Phi_1(t) = \langle e_0^7, \ldots, e_3^7, \frac{e_1}{e_0^3}, \frac{e_2}{e_1^3}, \frac{e_3}{e_2^3}, \frac{e_0}{e_1e_3^2}\rangle$$

The image of this set under ρ is

$$\langle e_0^7, \ldots, e_3^7, \frac{e_1}{e_0^3}, \frac{e_2}{e_1^3}, \frac{e_3}{e_2^3}, \frac{e_0}{e_1e_3^2}\rangle \mapsto \langle f_0^7, \ldots, f_1^7, \frac{f_1}{f_0^3}, \frac{f_0}{f_1^3}, \frac{f_1}{f_0^3}, \frac{f_0}{f_1^3}\rangle,$$

and therefore we need to solve

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_8 \end{pmatrix}^{\mathsf{T}} \cdot \begin{pmatrix} -3 & 1 & 0 & 0 \\ 0 & -3 & 1 & 0 \\ 0 & 0 & -3 & 1 \\ 1 & -1 & 0 & 2 \\ 7 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$$

The solution $(x_1, x_2, \ldots, x_8) = (11, 6, 7, 7, 4, 2, 2, 1)$ yields

$$x = \left(\frac{e_1}{e_0^3}\right)^{11} \left(\frac{e_2}{e_1^3}\right)^{6} \left(\frac{e_3}{e_2^3}\right)^{7} \left(\frac{e_0}{e_1 e_3^2}\right)^{7} (e_0^7)^4 (e_1^7)^2 (e_2^7)^2 (e_3^7) = \frac{e_0^2}{e_2}.$$

We see that $\rho(x) = f_0$, and we define σ via

$$\sigma(f_0) = \frac{e_0^2}{e_2} + \frac{e_1 e_2^2}{e_0 e_3} + \frac{e_0 e_3^2}{e_1^2}$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(I/\Phi_6(t)\Phi_2(t)\Phi_1(t)) = L(\frac{e_1 e_2^3}{e_0^3 e_3}, \frac{e_2 e_3^2}{e_0 e_1^2}, \frac{e_0^2}{e_2} + \frac{e_1 e_2^2}{e_0 e_3} + \frac{e_0 e_3^2}{e_1^2}, \frac{e_1^2}{e_3} + \frac{e_2 e_3}{e_0} + \frac{e_0^2 e_3^2}{e_1 e_2^2})$$

We combine this with the previous result, since the last two generators are swapped by π.

$$L(I/\Phi_6(t)\Phi_2(t)\Phi_1(t)) = L(\frac{e_1 e_2^3}{e_0^3 e_3}, \frac{e_2 e_3^2}{e_0 e_1^2}, \frac{\frac{e_1^2}{e_3} + \frac{e_2 e_3}{e_0} + \frac{e_0^2 e_3^2}{e_1 e_2^2}}{\frac{e_0^2}{e_2} + \frac{e_1 e_2^2}{e_0 e_3} + \frac{e_0 e_3^2}{e_1^2}}, \frac{e_0^2}{e_2} + \frac{e_1^2}{e_3} + \cdots + \frac{e_0^2 e_3^2}{e_1 e_2^2})$$

From (5.16) we have

$$0 \longrightarrow I/\Phi_6(t)\Phi_2(t) \longrightarrow I/\Phi_6(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t-1) \longrightarrow 0.$$

In this sequence, we have a description of the field corresponding to the middle component

and the right component. We use these to find a description of $L(I/\Phi_6(t)\Phi_2(t))$.

We compute the splitting homomorphism

$$\sigma : \langle\omega\rangle \longrightarrow L((t-1)I/\Phi_6(t)\Phi_2(t)\Phi_1(t))^{\times} \cdot I/\Phi_6(t)\Phi_2(t)\Phi_1(t).$$

Since we already have the generator $\frac{e_0^2}{e_2} + \frac{e_1^2}{e_3} + \cdots + \frac{e_0^2 e_3^2}{e_1 e_2^2}$ fixed by π, we define $x = \frac{e_0^2}{e_2}$ and $y = \frac{\pi(x)}{x} = \frac{e_1^2 e_2}{e_0^2 e_3}$, which leads to

$$\sigma(\omega) := x + \pi(x) + \pi^2(x) + \cdots + \pi^5(x) = \frac{e_0^2}{e_2} + \frac{e_1^2}{e_3} + \cdots + \frac{e_0^2 e_3^2}{e_1 e_2^2}.$$

Therefore, we have a description of $L(I/(t^3+1))$

$$L(I/(t^3+1)) = L(\frac{e_1 e_2^3}{e_0^3 e_3}, \frac{e_2 e_3^2}{e_0 e_1^2}, \frac{\frac{e_1^2}{e_3} + \frac{e_2 e_3}{e_0} + \frac{e_0^2 e_3^2}{e_1 e_2^2}}{\frac{e_0^2}{e_2} + \frac{e_1 e_2^2}{e_0 e_3} + \frac{e_0 e_3^2}{e_1^2}}) \tag{5.20}$$

We note that the following isomorphism is multiplication by $\Phi_3(t)$

$$\langle e_0, \ldots e_3\rangle \cong \mathbb{Z}[t]/\Phi_6(t)\Phi_2(t)\Phi_1(t) \cong \Phi_3(t)\mathbb{Z}[t]/(t^6-1).$$

Therefore,

$$e_0 = a_0a_1a_2,\ e_1 = a_1a_2a_3,\ \ldots,\ e_3 = a_3a_4a_5.$$

We define

$$\gamma_{6,0} = \frac{e_1 e_2^3}{e_0^3 e_3},\ \gamma_{6,1} = \frac{e_2 e_3^2}{e_0 e_1^2},\ \gamma_2 = \frac{\frac{e_1^2}{e_3} + \frac{e_2 e_3}{e_0} + \frac{e_0^2 e_3^2}{e_1 e_2^2}}{\frac{e_0^2}{e_2} + \frac{e_1 e_2^2}{e_0 e_3} + \frac{e_0 e_3^2}{e_1^2}}$$

We note that π inverts γ_2 and acts on the $\gamma_{6,j}$ via Φ_6. Combining this with (5.9) gives

$$L(I/(t^6-1)) \cong L(\overset{\oplus}{_{d\,|\,6}} I/\Phi_d(t)) = L(\gamma_1, \gamma_2, \gamma_{3,0}, \gamma_{3,1}, \gamma_{6,0}, \gamma_{6,1}).$$

Finally, we write the generator of the permutation basis in terms of the γ_i. We write c_0 in terms of the γ_i.

$$c_0 = \frac{\gamma_1}{1 + \gamma_{3,0} + \gamma_{3,0}\gamma_{3,1}} = \frac{a_0^4}{a_3^3} + \frac{a_3^4}{a_0^3}$$

Next, we compute the element d_0 that corresponded to $\frac{a_3}{a_0}$ from the previous section.

$$d_0 = \frac{\gamma_2(1 + \gamma_{6,0} + \gamma_{6,0}\pi^2(\gamma_{6,0}))}{1 + \gamma_{6,1} + \gamma_{6,1}\pi^2(\gamma_{6,1})} = \frac{e_1^2 e_2}{e_0^2 e_3} = \frac{a_2 a_3^2}{a_0^2 a_5}$$

Finally, we compute the generator α of the permutation basis (which was a_0 in the previous section) in terms of c_0 and d_0.

$$\alpha = \frac{c_0}{1 + d_0} = \frac{a_0^7 a_5 + a_3^7 a_5}{a_0 a_2 a_3^5 + a_0^3 a_3^3 a_5}$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$. We define the 6×6 matrix T whose (i,j)-th entry is $\zeta^{3^{i+j}}$ and compute the generators $u_0, \ldots, u_5$ as follows, where ζ denotes a primitive seventh root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_5 \end{pmatrix} = T \cdot \begin{pmatrix} \alpha \\ \pi(\alpha) \\ \vdots \\ \pi^5(\alpha) \end{pmatrix} = \begin{pmatrix} \zeta\alpha + \zeta^3\pi(\alpha) + \zeta^2\pi^2(\alpha) + \zeta^6\pi^3(\alpha) + \zeta^4\pi^4(\alpha) + \zeta^5\pi^5(\alpha) \\ \zeta^3\alpha + \zeta^2\pi(\alpha) + \zeta^6\pi^2(\alpha) + \zeta^4\pi^3(\alpha) + \zeta^5\pi^4(\alpha) + \zeta\pi^5(\alpha) \\ \zeta^2\alpha + \zeta^6\pi(\alpha) + \zeta^4\pi^2(\alpha) + \zeta^5\pi^3(\alpha) + \zeta\pi^4(\alpha) + \zeta^3\pi^5(\alpha) \\ \zeta^6\alpha + \zeta^4\pi(\alpha) + \zeta^5\pi^2(\alpha) + \zeta\pi^3(\alpha) + \zeta^3\pi^4(\alpha) + \zeta^2\pi^5(\alpha) \\ \zeta^4\alpha + \zeta^5\pi(\alpha) + \zeta\pi^2(\alpha) + \zeta^3\pi^3(\alpha) + \zeta^2\pi^4(\alpha) + \zeta^6\pi^5(\alpha) \\ \zeta^5\alpha + \zeta\pi(\alpha) + \zeta^3\pi^2(\alpha) + \zeta^2\pi^3(\alpha) + \zeta^6\pi^4(\alpha) + \zeta^4\pi^5(\alpha) \end{pmatrix}$$

Therefore, we have $K(x_0, \ldots, x_6)^\tau = K(y_0, u_0, u_1, \ldots, u_5)$.

Chapter 6: The case $A = \mathbb{Z}/11\mathbb{Z}$

We next compute generators of the fixed field $K(x_0, \ldots, x_{10})^A$, where $A = \langle\tau\rangle$. The Galois group $G = \langle\pi\rangle$ of L/K has order 10 and we have $I = \langle 11, t-2\rangle \subseteq \mathbb{Z}G$ and $J = \langle 11, \zeta - 2\rangle = \langle \zeta^9 - \zeta^7 + 1\rangle \subseteq \mathbb{Z}[\zeta]$, where ζ denotes a primitive tenth root of unity.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^{10}-1)) \cong L(\overset{\oplus}{}_{d \mid 10}\mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_9\rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_9 \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action.

We first compute the sequence of equivalence relations of $p - 1 = 10$; from (3.1.2) we have the following.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^{10}-1) \longrightarrow \mathbb{Z}[t]/(t^5-1) \longrightarrow 0 \tag{6.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_5(t) \longrightarrow \mathbb{Z}[t]/(t^5-1) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0 \tag{6.2}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t) \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0 \tag{6.3}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow 0 \tag{6.4}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0 \tag{6.5}$$

Starting with (6.1), we have

$$\mathbb{Z}[t]/(t^5+1) \cong (t^5-1)\mathbb{Z}[t]/(t^{10}-1) = \langle \frac{a_5}{a_0}, \frac{a_6}{a_1}, \ldots, \frac{a_9}{a_4} \rangle.$$

Therefore, we have the exact sequence

$$0 \longrightarrow L(\frac{a_5}{a_0}, \frac{a_6}{a_1}, \ldots, \frac{a_9}{a_4})^\times \longrightarrow L(\frac{a_5}{a_0}, \frac{a_6}{a_1}, \ldots, \frac{a_9}{a_4})^\times \cdot \langle a_0, a_1, \ldots, a_9 \rangle \xrightarrow{\rho} \langle b_0, b_1, b_2, b_3, b_4 \rangle \longrightarrow 0,$$

where ρ maps $a_{5i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 4$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, b_2, b_3, b_4 \rangle \longrightarrow L(\frac{a_5}{a_0}, \frac{a_6}{a_1}, \ldots, \frac{a_9}{a_4})^\times \cdot \langle a_0, a_1, \ldots, a_9 \rangle.$$

Letting $x = a_0$ and $y = \frac{\pi^5(x)}{x} = \frac{a_5}{a_0}$, we define σ via

$$\sigma(b_0) = (1 + \frac{\pi^5(x)}{x})x = a_0 + a_5,$$

which is fixed by π^5 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^{10}-1)) \cong L(a_0, \ldots, a_9) = L(\frac{a_5}{a_0}, \frac{a_6}{a_1}, \ldots, \frac{a_9}{a_4}, a_0 + a_5, \ldots, a_4 + a_9). \tag{6.6}$$

We see this explicitly since

$$a_0 = \frac{a_0 + a_5}{1 + \frac{a_5}{a_0}}, \ \ldots, a_9 = \frac{a_4 + a_9}{1 + \frac{a_4}{a_9}}.$$

We define

$$c_0 = a_0 + a_5,\ c_1 = a_1 + a_6,\ \ldots,\ c_4 = a_4 + a_9.$$

We can see that $c_0, \ldots, c_4$ are permuted cyclically by π and generate a module isomorphic to $\mathbb{Z}[t]/(t^5 - 1)$. Using these in (6.2), we have

$$\mathbb{Z}[t]/\Phi_5(t) \cong (t-1)\mathbb{Z}[t]/(t^5-1) = \langle \frac{c_1}{c_0}, \frac{c_2}{c_1}, \frac{c_3}{c_2}, \frac{c_4}{c_3} \rangle.$$

Writing $\mathbb{Z}[t]/\Phi_1(t) = \langle \omega \rangle$, we have the exact sequence

$$0 \longrightarrow L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, \frac{c_3}{c_2}, \frac{c_4}{c_3})^\times \longrightarrow L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, \frac{c_3}{c_2}, \frac{c_4}{c_3})^\times \cdot \langle c_0, c_1, c_2, c_3, c_4 \rangle \xrightarrow{\rho} \langle \omega \rangle \longrightarrow 0,$$

where ρ maps the c_i to ω.

We compute the splitting homomorphism $\sigma : \langle \omega \rangle \longrightarrow L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, \frac{c_3}{c_2}, \frac{c_4}{c_3})^\times \cdot \langle c_0, c_1, c_2, c_3, c_4 \rangle$. Letting $x = c_0$ and $y = \frac{\pi(x)}{x} = \frac{c_1}{c_0}$, we define σ via

$$\sigma(\omega) = (1 + \frac{\pi(x)}{x} + \cdots + \frac{\pi(x)}{x} \cdots \frac{\pi^4(x)}{\pi^3(x)})x = c_0 + c_1 + \cdots + c_4,$$

which is fixed by π as required.

Therefore, Proposition 3.2 gives

$$L(c_0, c_1, c_2, c_3, c_4) = L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, \frac{c_3}{c_2}, \frac{c_4}{c_3}, c_0 + c_1 + c_2 + c_3 + c_4).$$

We define

$$\gamma_{5,0} = \frac{c_1}{c_0},\ \ldots,\ \gamma_{5,3} = \frac{c_4}{c_3},\ \gamma_1 = c_0 + c_1 + c_2 + c_3 + c_4.$$

We can see explicitly that $L(c_0, c_1, c_2, c_3, c_4) = L(\gamma_{5,0}, \ldots, \gamma_{5,3}, \gamma_1)$, since

$$c_0 = \frac{\gamma_1}{1 + \gamma_{5,0} + \gamma_{5,0}\gamma_{5,1} + \cdots + \gamma_{5,0}\cdots\gamma_{5,3}}, \ \ldots, \tag{6.7}$$

$$c_4 = \frac{\gamma_1}{1 + \gamma_{5,3}^{-1} + \gamma_{5,3}^{-1}\gamma_{5,2}^{-1} + \cdots + \gamma_{5,3}^{-1}\cdots\gamma_{5,0}^{-1}}$$

We note that π acts on the $\gamma_{5,i}$ via $\Phi_5(t)$, and fixes γ_1, that is,

$$\pi : \gamma_{5,0} \mapsto \gamma_{5,1} \mapsto \cdots \mapsto \gamma_{5,3} \mapsto \gamma_{5,0}^{-1}\cdots\gamma_{5,3}^{-1}$$

Combining this result (6.6), we have

$$L(\mathbb{Z}[t]/(t^{10} - 1)) \cong L(\frac{a_5}{a_0}, \ldots, \frac{a_9}{a_4}, \gamma_{5,0}, \ldots, \gamma_{5,3}, \gamma_1) \tag{6.8}$$

Next, we compute generators of $L(\mathbb{Z}[t]/(t^5 + 1))$ that π acts on via Φ_{10} and Φ_2. From (6.5) we have

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^2 - 1) \longrightarrow \mathbb{Z}[t]/(t - 1) \longrightarrow 0$$

We use the result from (4.1), namely $L(u, v) = L(\frac{v}{u}, u+v)$. We use this result in sequence (6.4)

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_2(t)\Phi_1(t) \longrightarrow 0.$$

Since $\Phi_{10}(t)\Phi_2(t)\Phi_1(t) = t^6 - t^5 + t - 1$, we have a $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)$ and the multiplicative group $\langle d_0, d_1, d_2, \ldots, d_5\rangle$ via $t^i \mapsto d_i$, where π acts via

$$d_0 \mapsto d_1 \mapsto \cdots \mapsto d_5 \mapsto \frac{d_5 d_0}{d_1} \mapsto \frac{d_5 d_0}{d_2} \mapsto \cdots \mapsto \frac{d_5 d_0}{d_4} \mapsto d_0.$$

Therefore, we have

$$\mathbb{Z}[t]/\Phi_{10}(t) \cong (t^2-1)\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) = \langle \frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3} \rangle$$

and

$$0 \longrightarrow L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3})^\times \longrightarrow L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3})^\times \cdot \langle d_0, d_1, d_2, \ldots, d_5 \rangle \xrightarrow{\rho} \langle e_0, e_1 \rangle \longrightarrow 0,$$

where $\rho(d_{2i}) = e_0$, and $\rho(d_{2i+1}) = e_1$, for $i = 0, 1, 2$.

We compute the splitting homomorphism

$$\sigma : \langle e_0, e_1 \rangle \longrightarrow L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3})^\times \cdot \langle d_0, d_1, d_2, \ldots, d_5 \rangle.$$

Letting $x = d_0$ and $y = \frac{\pi^2(x)}{x} = \frac{d_2}{d_0}$, we define σ via

$$\sigma(e_0) = d_0 + d_2 + d_4 + \frac{d_5 d_0}{d_1} + \frac{d_5 d_0}{d_3},$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3}, d_0 + d_2 + d_4 + \frac{d_5 d_0}{d_1} + \frac{d_5 d_0}{d_3}, \\ d_1 + d_3 + d_5 + \frac{d_5 d_0}{d_2} + \frac{d_5 d_0}{d_4}).$$

We combine this with the previous result, since the last two generators are swapped by π.

$$L(\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3}, \frac{d_1+d_3+d_5+\frac{d_5d_0}{d_2}+\frac{d_5d_0}{d_4}}{d_0+d_2+d_4+\frac{d_5d_0}{d_1}+\frac{d_5d_0}{d_3}},$$
$$d_0+d_1+\cdots+d_5+\frac{d_5d_0}{d_1}+\cdots+\frac{d_5d_0}{d_4})$$

From sequence (6.3) we had the following.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t) \longrightarrow \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0$$

In this sequence, we have a description of the field corresponding to the middle component and the right component. We use these to find a description of $L(\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t))$. We have

$$\mathbb{Z}[t]/(t^5+1) \cong (t-1)\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \cong \langle \frac{d_1}{d_0}, \frac{d_2}{d_1}, \frac{d_3}{d_2}, \frac{d_4}{d_3}, \frac{d_5}{d_4} \rangle.$$

Letting $f_0 = \frac{d_1}{d_0}, f_1 = \frac{d_2}{d_1}, \ldots, f_4 = \frac{d_5}{d_4}$ and $\mathbb{Z}[t]/(t-1) = \langle \omega \rangle$, we have

$$0 \longrightarrow L(f_0, f_1, \ldots, f_4)^\times \longrightarrow L(f_0, f_1, \ldots, f_4)^\times \cdot \langle d_0, d_1, d_2, \ldots, d_5 \rangle \xrightarrow{\rho} \langle \omega \rangle \longrightarrow 0.$$

We compute the splitting homomorphism

$$\sigma : \langle \omega \rangle \longrightarrow L(f_0, f_1, \ldots, f_4)^\times \cdot \langle d_0, d_1, d_2, \ldots, d_5 \rangle.$$

Since we already have the generator $d_0 + d_1 + \cdots + d_5 + \frac{d_5d_0}{d_1} + \cdots + \frac{d_5d_0}{d_4}$ fixed by π, we define $x = d_0$ and $y = \frac{\pi(x)}{x} = \frac{d_1}{d_0}$, and we have

$$\sigma(\omega) := (1 + f_0 + f_0f_1 + \cdots + f_0 \cdots f_4)d_0 = d_0 + d_1 + d_2 + \cdots + \frac{d_5d_0}{d_4}.$$

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)) \cong L(f_0, f_1, \ldots, f_4, d_0 + d_1 + d_2 + \cdots + \frac{d_5 d_0}{d_4}).$$

This gives us the following.

$$L(f_0, f_1, \ldots, f_4, d_0 + d_1 + \cdots + \frac{d_5 d_0}{d_4}) \cong L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3}, \frac{d_1 + d_3 + d_5 + \frac{d_5 d_0}{d_2} + \frac{d_5 d_0}{d_4}}{d_0 + d_2 + d_4 + \frac{d_5 d_0}{d_1} + \frac{d_5 d_0}{d_3}}, d_0 + d_1 + \cdots + d_5 + \frac{d_5 d_0}{d_1} + \cdots + \frac{d_5 d_0}{d_4})$$

Therefore, we have a description of $L(\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)) = L(\mathbb{Z}[t]/(t^5+1))$.

$$L(\mathbb{Z}[t]/(t^5+1)) \cong L(\frac{d_2}{d_0}, \frac{d_3}{d_1}, \frac{d_4}{d_2}, \frac{d_5}{d_3}, \frac{d_1 + d_3 + d_5 + \frac{d_5 d_0}{d_2} + \frac{d_5 d_0}{d_4}}{d_0 + d_2 + d_4 + \frac{d_5 d_0}{d_1} + \frac{d_5 d_0}{d_3}}) \tag{6.9}$$

We see that the following isomorphism is multiplication by $\Phi_5(t)$

$$\langle d_0, \ldots d_5 \rangle \cong \mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \cong \Phi_5(t)\mathbb{Z}[t]/(t^{10}-1).$$

Therefore, we have

$$d_0 = a_0a_1a_2a_3a_4,\ d_1 = a_1a_2a_3a_4a_5,\ \ldots,\ d_5 = a_5a_6a_7a_8a_9.$$

We define

$$\gamma_{10,0} = \frac{d_2}{d_0},\ \gamma_{10,1} = \frac{d_3}{d_1},\ \gamma_{10,2} = \frac{d_4}{d_2},\ \gamma_{10,3} = \frac{d_5}{d_3},\ \gamma_2 = \frac{d_1 + d_3 + d_5 + \frac{d_5 d_0}{d_2} + \frac{d_5 d_0}{d_4}}{d_0 + d_2 + d_4 + \frac{d_5 d_0}{d_1} + \frac{d_5 d_0}{d_3}}$$

We note that π inverts γ_2, and acts on the $\gamma_{10,j}$ via Φ_{10}, that is

$$\pi : \gamma_{10,0} \mapsto \gamma_{10,1} \mapsto \gamma_{10,2} \mapsto \gamma_{10,3} \mapsto \gamma_{10,3}\gamma_{10,2}^{-1}\gamma_{10,1}\gamma_{10,0}^{-1}.$$

We can see $L(f_0, f_1, \cdots, f_4) = L(\gamma_{10,0}, \ldots, \gamma_{10,3}, \gamma_2)$ explicitly, since

$$\gamma_{10,0} = f_0 f_1, \ \ldots, \gamma_{10,3} = f_3 f_4$$

and

$$f_0 = \gamma_2 \left(\frac{1 + \gamma_{10,0} + \gamma_{10,0}\pi^2(\gamma_{10,0}) + \gamma_{10,0}\pi^2(\gamma_{10,0})\pi^4(\gamma_{10,0}) + \gamma_{10,0}\pi^2(\gamma_{10,0})\pi^4(\gamma_{10,0})\pi^6(\gamma_{10,0})}{1 + \gamma_{10,1} + \gamma_{10,1}\pi^2(\gamma_{10,1}) + \gamma_{10,1}\pi^2(\gamma_{10,1})\pi^4(\gamma_{10,1}) + \gamma_{10,1}\pi^2(\gamma_{10,1})\pi^4(\gamma_{10,1})\pi^6(\gamma_{10,1})} \right) \tag{6.10}$$

Combining this with (6.8), we obtain the isomorphism

$$L(\mathbb{Z}[t]/(t^{10} - 1)) \cong L(\overset{\oplus}{}_{d \mid 10} \mathbb{Z}[t]/(\Phi_d(t))) = L(\gamma_1, \gamma_2, \gamma_{5,0}, \ldots, \gamma_{5,3}, \gamma_{10,0}, \ldots, \gamma_{10,3}).$$

We note that a_0 and its π-conjugates, namely $a_0, \ldots, a_9$, are a permutation basis of $\mathbb{Z}G$. We write the permutation basis in terms of the γ_i; it suffices to express a_0 in terms of the γ_i. From (6.7) we have

$$c_0 = \frac{\gamma_1}{1 + \gamma_{5,0} + \gamma_{5,0}\gamma_{5,1} + \gamma_{5,0}\gamma_{5,1}\gamma_{5,2} + \gamma_{5,0}\gamma_{5,1}\gamma_{5,2}\gamma_{5,3}}$$

From (6.10) we have

$$f_0 = \frac{\gamma_2(1 + \gamma_{10,0} + \gamma_{10,0}\pi^2(\gamma_{10,0}) + \gamma_{10,0}\pi^2(\gamma_{10,0})\pi^4(\gamma_{10,0}) + \gamma_{10,0}\pi^2(\gamma_{10,0})\pi^4(\gamma_{10,0})\pi^6(\gamma_{10,0}))}{1 + \gamma_{10,1} + \gamma_{10,1}\pi^2(\gamma_{10,1}) + \gamma_{10,1}\pi^2(\gamma_{10,1})\pi^4(\gamma_{10,1}) + \gamma_{10,1}\pi^2(\gamma_{10,1})\pi^4(\gamma_{10,1})\pi^6(\gamma_{10,1})}$$

Finally, we can write a_0 in terms of c_0 and f_0.

$$a_0 = \frac{c_0}{1 + f_0}$$

6.1 Computing the fixed field of I

We next compute the isomorphism

$$L(I) \cong L(J \oplus \overset{\oplus}{}_{d \mid 10, d \neq 10} \mathbb{Z}[\zeta_d]),$$

where $I = \langle 11, t-2 \rangle$. From (3.1.2) we have the following.

$$0 \longrightarrow I/\Phi_{10}(t)\Phi_2(t) \longrightarrow I/(t^{10}-1) \longrightarrow I/(t^5-1) \longrightarrow 0 \tag{6.11}$$

$$0 \longrightarrow I/\Phi_5(t) \longrightarrow I/(t^5-1) \longrightarrow I/(t-1) \longrightarrow 0 \tag{6.12}$$

$$0 \longrightarrow I/\Phi_{10}(t)\Phi_2(t) \longrightarrow I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t-1) \longrightarrow 0 \tag{6.13}$$

$$0 \longrightarrow I/\Phi_{10}(t) \longrightarrow I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^2-1) \longrightarrow 0 \tag{6.14}$$

$$0 \longrightarrow I/\Phi_2(t) \longrightarrow I/(t^2-1) \longrightarrow I/(t-1) \longrightarrow 0 \tag{6.15}$$

Again using the $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^{10}-1)$ and the multiplicative group $\langle a_0, a_1, \ldots, a_9 \rangle$ via $t^i \mapsto a_i$, (6.11) gives

$$0 \longrightarrow L((t^5-1)I/(t^{10}-1))^\times \longrightarrow L((t^5-1)I/(t^{10}-1))^\times \cdot I/(t^{10}-1) \xrightarrow{\rho} \langle b_0, b_1, b_2, b_3, b_4 \rangle \longrightarrow 0,$$

where ρ maps $a_{5i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 4$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, b_2, b_3, b_4 \rangle \longrightarrow L((t^5-1)I/(t^{10}-1))^{\times} \cdot I/(t^{10}-1).$$

Since $I = \langle 11, t-2 \rangle$, we have the following generating set for I.

$$I = \langle a_0^{11}, a_1^{11}, \ldots, a_9^{11}, \frac{a_1}{a_0^2}, \frac{a_2}{a_1^2}, \ldots, \frac{a_9}{a_8^2}, \frac{a_0}{a_9^2} \rangle$$

The image of this set under ρ is

$$\langle a_0^{11}, a_1^{11}, \ldots, a_9^{11}, \frac{a_1}{a_0^2}, \frac{a_2}{a_1^2}, \ldots, \frac{a_9}{a_8^2}, \frac{a_0}{a_9^2} \rangle \mapsto \langle b_0^{11}, b_1^{11}, \ldots, b_4^{11}, \frac{b_1}{b_0^2}, \frac{b_2}{b_1^2}, \ldots, \frac{b_0}{b_4^2}, \rangle$$

and therefore we need to solve

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \end{pmatrix}^{\intercal} \cdot \begin{pmatrix} -2 & 1 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & -2 & 1 \\ 1 & 0 & 0 & 0 & -2 \\ 11 & 0 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 & 0 \\ 0 & 0 & 11 & 0 & 0 \\ 0 & 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 0 & 11 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}^{\intercal}$$

The solution $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}) = (8, 4, 2, 1, 6, 1, 0, 0, 0, 1)$ yields

$$x = \left(\frac{a_1}{a_0^2}\right)^8 \left(\frac{a_2}{a_1^2}\right)^4 \left(\frac{a_3}{a_2^2}\right)^2 \left(\frac{a_4}{a_3^2}\right) \left(\frac{a_5}{a_4^2}\right)^6 (a_0^{11})(a_4^{11}) = \frac{a_5^6}{a_0^5}.$$

We see that $\rho(x) = b_0$, and define σ via

$$\sigma(b_0) = (1 + \frac{\pi^5(x)}{x})x = \frac{a_5^6}{a_0^5} + \frac{a_0^6}{a_5^5},$$

which is fixed by π^5 as required. Therefore, Proposition 3.2 gives

$$L(I/(t^{10}-1)) \cong L(I/(t^5+1) \oplus \langle \frac{a_5^6}{a_0^5} + \frac{a_0^6}{a_5^5}, \frac{a_6^6}{a_1^5} + \frac{a_1^6}{a_6^5}, \frac{a_7^6}{a_2^5} + \frac{a_2^6}{a_7^5}, \frac{a_8^6}{a_3^5} + \frac{a_3^6}{a_8^5}, \frac{a_9^6}{a_4^5} + \frac{a_4^6}{a_9^5} \rangle)$$

We define

$$c_0 = \frac{a_5^6}{a_0^5} + \frac{a_0^6}{a_5^5},\ c_1 = \frac{a_6^6}{a_1^5} + \frac{a_1^6}{a_6^5},\ \ldots,\ c_4 = \frac{a_9^6}{a_4^5} + \frac{a_4^6}{a_9^5}$$

We see that π acts via $c_0 \mapsto c_1 \mapsto \cdots \mapsto c_4 \mapsto c_0$ and use the result from the previous section, namely

$$L(c_0, c_1, c_2, c_3, c_4) \cong L(\frac{c_1}{c_0}, \frac{c_2}{c_1}, \frac{c_3}{c_2}, \frac{c_4}{c_3}, c_0 + c_1 + c_2 + c_3 + c_4).$$

We label $\frac{c_1}{c_0}, \ldots, \frac{c_4}{c_3}$ as $\gamma_{5,0}, \ldots, \gamma_{5,3}$, and note that π acts on them via $\Phi_5(t)$.

$$\gamma_{5,0} = \frac{c_1}{c_0} = \frac{\frac{a_6^6}{a_1^5} + \frac{a_1^6}{a_6^5}}{\frac{a_5^6}{a_0^5} + \frac{a_0^6}{a_5^5}},\ \ldots,\ \gamma_{5,3} = \frac{c_4}{c_3} = \frac{\frac{a_9^6}{a_4^5} + \frac{a_4^6}{a_9^5}}{\frac{a_8^6}{a_3^5} + \frac{a_3^6}{a_8^5}}$$

We label $\gamma_1 = c_0 + c_1 + c_2 + c_3 + c_4$ and see it is fixed by π. Therefore, we have

$$L(I/(t^{10}-1)) \cong L(I/(t^5+1) \oplus \langle \gamma_{5,0}, \gamma_{5,1}, \gamma_{5,2}, \gamma_{5,3}, \gamma_1 \rangle) \tag{6.16}$$

Next, we compute generators of $L(I/(t^5+1))$ that π acts on via Φ_{10} and Φ_2. We use the result (4.1), namely $L(u,v) = L(\frac{v}{u}, u+v)$. We use this result in sequence (6.14)

$$0 \longrightarrow I/\Phi_{10}(t) \longrightarrow I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/\Phi_2(t)\Phi_1(t) \longrightarrow 0.$$

Writing $\mathbb{Z}[t]/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)$ multiplicatively as $\langle d_0, d_1, \ldots, d_5 \rangle$ via $t^i \mapsto d_i$, π acts

via

$$d_0 \mapsto d_1 \mapsto \cdots \mapsto d_5 \mapsto \frac{d_5 d_0}{d_1} \mapsto \frac{d_5 d_0}{d_2} \mapsto \cdots \mapsto \frac{d_5 d_0}{d_4} \mapsto d_0.$$

The ideal $I/\Phi_{10}(t)$ is principal and generated by $t^9 - t^7 + 1$, and gives a $\mathbb{Z}G$-module isomorphism

$$I/\Phi_{10}(t) \cong (t^2-1)I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) = \langle -t^5+2t^4+t-2 \rangle = \langle \frac{d_1 d_4^2}{d_0^2 d_5}, \frac{d_2 d_5}{d_0 d_1}, \frac{d_0 d_3 d_5}{d_1^2 d_2}, \frac{d_0 d_4 d_5}{d_2^2 d_3} \rangle$$

and we have

$$0 \longrightarrow L(\frac{d_1 d_4^2}{d_0^2 d_5}, \ldots, \frac{d_0 d_4 d_5}{d_2^2 d_3})^\times \longrightarrow L(\frac{d_1 d_4^2}{d_0^2 d_5}, \ldots, \frac{d_0 d_4 d_5}{d_2^2 d_3})^\times \cdot I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \xrightarrow{\rho}$$

$$\langle e_0, e_1 \rangle \longrightarrow 0,$$

where ρ sends $d_{2i+j} \mapsto e_j$, for $i = 0, 1, 2$ and $j = 0, 1$.

We compute the splitting homomorphism

$$\sigma : \langle e_0, e_1 \rangle \longrightarrow L(\frac{d_1 d_4^2}{d_0^2 d_5}, \ldots, \frac{d_0 d_4 d_5}{d_2^2 d_3})^\times \cdot I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t).$$

We have the following generating set for $I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)$.

$$I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) = \langle d_0^{11}, d_1^{11}, \ldots, d_5^{11}, \frac{d_1}{d_0^2}, \frac{d_2}{d_1^2}, \ldots, \frac{d_5}{d_4^2}, \frac{d_0}{d_1 d_5} \rangle$$

The image of this set under ρ is

$$\langle d_0^{11}, d_1^{11}, \ldots, d_5^{11}, \frac{d_1}{d_0^2}, \frac{d_2}{d_1^2}, \ldots, \frac{d_5}{d_4^2}, \frac{d_0}{d_1 d_5} \rangle \mapsto \langle e_0^{11}, e_1^{11}, \ldots, e_1^{11}, \frac{e_1}{e_0^2}, \frac{e_0}{e_1^2}, \ldots, \frac{e_1}{e_0^2}, \frac{e_0}{e_1^2} \rangle$$

and therefore we need to solve

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \end{pmatrix}^{\intercal} \cdot \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 \\ 1 & -1 & 0 & 0 & 0 & -1 \\ 11 & 0 & 0 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 & 0 & 0 \\ 0 & 0 & 11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 11 & 0 & 0 \\ 0 & 0 & 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 & 11 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}^{\intercal}$$

The solution

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}) = (-6, -3, -2, -1, 0, 0, -1, 0, 0, 0, 0, 0)$$

yields

$$x = \left(\frac{d_1}{d_0^2}\right)^{-6} \left(\frac{d_2}{d_1^2}\right)^{-3} \left(\frac{d_3}{d_2^2}\right)^{-2} \left(\frac{d_4}{d_3^2}\right)^{-1} (d_0^{11})^{-1} = \frac{d_0 d_2}{d_4}.$$

We see that $\rho(x) = e_0$, and we define σ via

$$\sigma(e_0) = \left(1 + \frac{d_1 d_4^2}{d_0^2 d_5} + \frac{d_3 d_4^2}{d_0 d_1 d_2} + \frac{d_4 d_5^2}{d_1 d_2 d_3} + \frac{d_0 d_4 d_5}{d_2^2 d_3}\right) \frac{d_0 d_2}{d_4} = \frac{d_0 d_2}{d_4} + \frac{d_1 d_2 d_4}{d_0 d_5} + \frac{d_3 d_4}{d_1} + \frac{d_0 d_5^2}{d_1 d_3} + \frac{d_0^2 d_5}{d_2 d_3}.$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$\begin{aligned} L(I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)) = L(&\frac{d_1 d_4^2}{d_0^2 d_5}, \frac{d_2 d_5}{d_0 d_1}, \frac{d_0 d_3 d_5}{d_1^2 d_2}, \frac{d_0 d_4 d_5}{d_2^2 d_3}, \\ &\frac{d_0 d_2}{d_4} + \frac{d_1 d_2 d_4}{d_0 d_5} + \frac{d_3 d_4}{d_1} + \frac{d_0 d_5^2}{d_1 d_3} + \frac{d_0^2 d_5}{d_2 d_3}, \frac{d_1 d_3}{d_5} + \frac{d_2 d_3}{d_0} + \frac{d_4 d_5}{d_2} + \frac{d_0^2 d_5^2}{d_1 d_2 d_4} + \frac{d_0 d_1 d_5}{d_3 d_4}) \end{aligned}$$

We combine this with the previous result, since the last two generators are swapped

by π.

$$L(I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t)) = L(\frac{d_1d_4^2}{d_0^2d_5}, \frac{d_2d_5}{d_0d_1}, \frac{d_0d_3d_5}{d_1^2d_2}, \frac{d_0d_4d_5}{d_2^2d_3}, \\ \frac{\frac{d_1d_3}{d_5} + \frac{d_2d_3}{d_0} + \frac{d_4d_5}{d_2} + \frac{d_0^2d_5^2}{d_1d_2d_4} + \frac{d_0d_1d_5}{d_3d_4}}{\frac{d_0d_2}{d_4} + \frac{d_1d_2d_4}{d_0d_5} + \frac{d_3d_4}{d_1} + \frac{d_0d_5^2}{d_1d_3} + \frac{d_0^2d_5}{d_2d_3}}, \frac{d_0d_2}{d_4} + \frac{d_1d_3}{d_5} + \cdots + \frac{d_0^2d_5}{d_2d_3} + \frac{d_0d_1d_5}{d_3d_4})$$

From (6.13) we have

$$0 \longrightarrow I/\Phi_{10}(t)\Phi_2(t) \longrightarrow I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t-1) \longrightarrow 0.$$

We have a description of the field corresponding to the middle component and the right component. We use these to find a description of $L(I/\Phi_{10}(t)\Phi_2(t))$.

We compute the splitting homomorphism

$$\sigma : \langle\omega\rangle \longrightarrow L((t-1)I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t))^\times \cdot I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t).$$

Since we already have a generator fixed by π, we define $x = \frac{d_0d_2}{d_4}$, which satisfies $\rho(x) = \omega$ and leads to

$$\sigma(\omega) = x + \pi(x) + \pi^2(x) + \cdots + \pi^9(x) = \frac{d_0d_2}{d_4} + \frac{d_1d_3}{d_5} + \cdots + \frac{d_0d_1d_5}{d_3d_4}.$$

Therefore, we have a description of $L(I/(t^5+1))$

$$L(I/(t^5+1)) = L(\frac{d_1d_4^2}{d_0^2d_5}, \frac{d_2d_5}{d_0d_1}, \frac{d_0d_3d_5}{d_1^2d_2}, \frac{d_0d_4d_5}{d_2^2d_3}, \frac{\frac{d_1d_3}{d_5} + \frac{d_2d_3}{d_0} + \frac{d_4d_5}{d_2} + \frac{d_0^2d_5^2}{d_1d_2d_4} + \frac{d_0d_1d_5}{d_3d_4}}{\frac{d_0d_2}{d_4} + \frac{d_1d_2d_4}{d_0d_5} + \frac{d_3d_4}{d_1} + \frac{d_0d_5^2}{d_1d_3} + \frac{d_0^2d_5}{d_2d_3}}) \tag{6.17}$$

We note that the following isomorphism is multiplication by $\Phi_5(t)$

$$\langle d_0, \dots d_5 \rangle \cong I/\Phi_{10}(t)\Phi_2(t)\Phi_1(t) \cong \Phi_5(t)I/(t^{10}-1).$$

Therefore, we see

$$d_0 = a_0a_1a_2a_3a_4,\ d_1 = a_1a_2a_3a_4a_5,\ \dots,\ d_5 = a_5a_6a_7a_8a_9.$$

We define

$$\gamma_{10,0} = \frac{d_1d_4^2}{d_0^2d_5},\ \gamma_{10,1} = \frac{d_2d_5}{d_0d_1},\ \gamma_{10,2} = \frac{d_0d_3d_5}{d_1^2d_2},\ \gamma_{10,3} = \frac{d_0d_4d_5}{d_2^2d_3}$$

$$\gamma_2 = \frac{\frac{d_1d_3}{d_5} + \frac{d_2d_3}{d_0} + \frac{d_4d_5}{d_2} + \frac{d_0^2d_5^2}{d_1d_2d_4} + \frac{d_0d_1d_5}{d_3d_4}}{\frac{d_0d_2}{d_4} + \frac{d_1d_2d_4}{d_0d_5} + \frac{d_3d_4}{d_1} + \frac{d_0d_5^2}{d_1d_3} + \frac{d_0^2d_5}{d_2d_3}}$$

We note that π inverts γ_2 and acts on the $\gamma_{10,j}$ via Φ_{10}. Combining this with (6.16) gives

$$L(I/(t^{10}-1)) \cong L(\overset{\oplus}{}_{d\,|\,10} I/(\Phi_d(t))) = L(\gamma_1, \gamma_2, \gamma_{5,0}, \dots, \gamma_{5,3}, \gamma_{10,0}, \dots, \gamma_{10,3}).$$

Finally, we use the results from the previous section to write the permutation basis in terms of the γ_i. We write c_0 in terms of the γ_i.

$$c_0 = \frac{\gamma_1}{1 + \gamma_{5,0} + \gamma_{5,0}\gamma_{5,1} + \gamma_{5,0}\gamma_{5,1}\gamma_{5,2} + \gamma_{5,0}\gamma_{5,1}\gamma_{5,2}\gamma_{5,3}} = \frac{a_5^6}{a_0^5} + \frac{a_0^6}{a_5^5}$$

Next, we compute the element α that corresponded to $\frac{a_5}{a_0}$ from the previous section.

$$\alpha = \frac{\gamma_2(1+\gamma_{10,0}+\gamma_{10,0}\pi^2(\gamma_{10,0})+\cdots+\gamma_{10,0}\cdots\pi^6(\gamma_{10,0}))}{1+\gamma_{10,1}+\gamma_{10,1}\pi^2(\gamma_{10,1})+\cdots+\gamma_{10,1}\cdots\pi^6(\gamma_{10,1})} = \frac{d_1d_3d_4}{d_0d_2d_5} = \frac{a_4a_5a_7}{a_0a_2a_9}$$

Finally, we compute the generator β of the permutation basis (which was a_0 in the previous section) in terms of c_0 and α.

$$\beta = \frac{c_0}{1+\alpha} = \frac{\frac{a_5^6}{a_0^5}+\frac{a_0^6}{a_5^5}}{1+\frac{a_4a_5a_7}{a_0a_2a_9}} = \frac{a_0^{11}a_2a_9+a_2a_5^{11}a_9}{a_0^4a_4a_5^6a_7+a_0^5a_2a_5^5a_9}$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$. We define the 10×10 matrix T whose (i,j)-th entry is $\zeta^{2^{i+j}}$ and compute the generators $u_0,\ldots,u_9$ as follows, where ζ denotes a primitive eleventh root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_9 \end{pmatrix} = T \cdot \begin{pmatrix} \beta \\ \pi(\beta) \\ \pi^2(\beta) \\ \vdots \\ \pi^9(\beta) \end{pmatrix}$$

Therefore, we have $K(x_0,\ldots,x_{10})^\tau = K(y_0,u_0,u_1,\ldots,u_9)$.

Chapter 7: The case $A = \mathbb{Z}/13\mathbb{Z}$

We next compute generators of the fixed field $K(x_0, \ldots, x_{12})^A$, where $A = \langle \tau \rangle$. The Galois group $G = \langle \pi \rangle$ of L/K has order 12 and we have $I = \langle 13, t-2 \rangle \subseteq \mathbb{Z}G$ and $J = \langle 13, \zeta - 2 \rangle = \langle \zeta^2 - \zeta - 2 \rangle \subseteq \mathbb{Z}[\zeta]$, where ζ denotes a primitive twelfth root of unity.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^{12}-1)) \cong L(\bigoplus_{d \mid 12} \mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_{11} \rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_{11} \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action. We compute the sequence of equivalence relations for $p - 1 = 12$ as in (3.1.1).

$$\{\{1,2,3,4,6,12\}\} \mapsto \{\{1,2,3,6\},\{4,12\}\} \mapsto \{\{1,3\},\{2,6\},\{4,12\}\} \mapsto$$

$$\{\{1\},\{3\},\{2,6\},\{4,12\}\} \mapsto \{\{1,2,6\},\{3\},\{4,12\}\} \mapsto \{\{1,2\},\{3\},\{6\},\{4,12\}\} \mapsto$$

$$\{\{1,2,4,12\},\{3\},\{6\}\} \mapsto \{\{1,2,4\},\{3\},\{6\},\{12\}\} \mapsto \{\{1,2\},\{4\},\{3\},\{6\},\{12\}\} \mapsto$$

$$\{\{1\},\{2\},\{3\},\{4\},\{6\},\{12\}\}$$

This gives rise to the following exact sequences, which we use along with results

from § 5.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t) \longrightarrow \mathbb{Z}[t]/(t^{12}-1) \longrightarrow \mathbb{Z}[t]/(t^6-1) \longrightarrow 0 \tag{7.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t) \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow 0 \tag{7.2}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^4-1) \longrightarrow 0 \tag{7.3}$$

$$0 \longrightarrow \mathbb{Z}[t]/(t^2+1) \longrightarrow \mathbb{Z}[t]/(t^4-1) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow 0 \tag{7.4}$$

Starting with (7.1), we have

$$\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t) \cong (t^6-1)\mathbb{Z}[t]/(t^{12}-1) = \langle \frac{a_6}{a_0}, \frac{a_7}{a_1}, \ldots, \frac{a_{11}}{a_5} \rangle.$$

Therefore, we have the exact sequence

$$0 \longrightarrow L(\frac{a_6}{a_0}, \ldots, \frac{a_{11}}{a_5})^\times \longrightarrow L(\frac{a_6}{a_0}, \ldots, \frac{a_{11}}{a_5})^\times \cdot \langle a_0, \ldots, a_{11} \rangle \xrightarrow{\rho} \langle b_0, b_1, \ldots, b_5 \rangle \longrightarrow 0,$$

where ρ maps $a_{6i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 5$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, \ldots, b_5 \rangle \longrightarrow L(\frac{a_6}{a_0}, \ldots, \frac{a_{11}}{a_5})^\times \cdot \langle a_0, \ldots, a_{11} \rangle.$$

Letting $x = a_0$, we define σ via

$$\sigma(b_0) = (1 + \frac{\pi^6(x)}{x})x = a_0 + a_6,$$

which is fixed by π^6 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^{12}-1)) \cong L(a_0,\ldots,a_{11}) = L(\frac{a_6}{a_0},\frac{a_7}{a_1},\ldots,\frac{a_{11}}{a_5},a_0+a_6,a_1+a_7\ldots,a_5+a_{11}). \quad (7.5)$$

We see this explicitly since

$$a_0 = \frac{a_0+a_6}{1+\frac{a_6}{a_0}},\ \ldots, a_{11} = \frac{a_5+a_{11}}{1+\frac{a_5}{a_{11}}}.$$

We note that the last 6 generators are permuted cyclically by π; we denote these via

$$c_0 := a_0+a_6,\ c_1 := a_1+a_7,\ \ldots,\ c_5 := a_5+a_{11}.$$

Using the results from (5.13), we have

$$L(\mathbb{Z}[t]/(t^6-1)) \cong L(\overset{\oplus}{_{d\mid 6}}\mathbb{Z}[t]/\Phi_d(t)) = L(\gamma_1,\gamma_2,\gamma_{3,0},\gamma_{3,1},\gamma_{6,0},\gamma_{6,1}),$$

where

$$\gamma_{6,0} = \frac{c_3c_4}{c_0c_1},\ \gamma_{6,1} = \frac{c_4c_5}{c_1c_2},\ \gamma_{3,0} = \frac{c_1+c_4}{c_0+c_3},\ \gamma_{3,1} = \frac{c_2+c_5}{c_1+c_4},\ \gamma_2 = \frac{c_1c_2c_3+c_0c_1c_5+c_3c_4c_5}{c_0c_1c_2+c_2c_3c_4+c_0c_4c_5},$$

$$\gamma_1 = c_0+c_1+\cdots+c_5.$$

Combining this with (7.5) gives

$$L(\mathbb{Z}[t]/(t^{12}-1)) \cong L(\frac{a_6}{a_0},\frac{a_7}{a_1},\ldots,\frac{a_{11}}{a_5},\gamma_1,\gamma_2,\gamma_{3,0},\gamma_{3,1},\gamma_{6,0},\gamma_{6,1}). \quad (7.6)$$

Next, we compute generators of $L(\mathbb{Z}[t]/(t^6+1))$ that π acts on via Φ_{12} and Φ_4.

From (7.3) we have

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^4-1) \longrightarrow 0.$$

Since $\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) = t^8 - t^6 + t^2 - 1$, we have a $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)$ and the multiplicative group $\langle d_0, d_1, d_2, \ldots, d_7\rangle$ via $t^i \mapsto d_i$, where π acts via

$$d_0 \mapsto d_1 \mapsto \cdots \mapsto d_7 \mapsto \frac{d_0 d_6}{d_2} \mapsto \cdots \mapsto \frac{d_1 d_7}{d_5} \mapsto d_0.$$

Therefore, we have

$$\mathbb{Z}[t]/\Phi_{12}(t) \cong (t^4-1)\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) = \langle \frac{d_4}{d_0}, \ldots, \frac{d_7}{d_3}\rangle$$

and

$$0 \longrightarrow L(\frac{d_4}{d_0}, \ldots, \frac{d_7}{d_3})^\times \longrightarrow L(\frac{d_4}{d_0}, \ldots, \frac{d_7}{d_3})^\times \cdot \langle d_0, \ldots, d_7\rangle \xrightarrow{\rho} \langle e_0, e_1 \ldots, e_3\rangle \longrightarrow 0,$$

where ρ maps $d_{4i+j} \mapsto e_j$ for $i = 0, 1$, and $j = 0, \ldots, 3$.

We compute the splitting homomorphism

$$\sigma : \langle e_0, \ldots, e_3\rangle \longrightarrow L(\frac{d_4}{d_0}, \ldots, \frac{d_7}{d_3})^\times \cdot \langle d_0, \ldots, d_7\rangle.$$

Letting $x = d_0$ and $y = \frac{\pi^4(x)}{x} = \frac{d_4}{d_0}$, we define σ via

$$\sigma(e_0) = (1 + \frac{\pi^4(x)}{x} + \frac{\pi^4(x)}{x}\frac{\pi^8(x)}{\pi^4(x)})x = d_0 + d_4 + \frac{d_0 d_6}{d_2},$$

which is fixed by π^4 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{d_4}{d_0},\ldots,\frac{d_7}{d_3},d_0+d_4+\frac{d_0d_6}{d_2},d_1+d_5+\frac{a_1a_7}{a_3},$$
$$d_2+d_6+\frac{d_0d_6}{d_4},d_3+d_7+\frac{d_1d_7}{d_5}).$$

We define

$$f_0 = d_0+d_4+\frac{d_0d_6}{d_2},\ \ldots,\ f_3 = d_3+d_7+\frac{d_1d_7}{d_5}$$

and note they are permuted cyclically by π. From (7.4) we have

$$0 \longrightarrow L(\frac{f_2}{f_0},\frac{f_3}{f_1})^\times \longrightarrow L(\frac{f_2}{f_0},\frac{f_3}{f_1})^\times \cdot \langle f_0,\ldots,f_3\rangle \xrightarrow{\rho} \langle g_0,g_1\rangle \longrightarrow 0.$$

The splitting $\sigma(g_0) = f_0+f_2$ yields

$$L(f_0,f_1,f_2,f_3) = L(\frac{f_2}{f_0},\frac{f_3}{f_1},f_0+f_2,f_1+f_3).$$

Letting

$$\gamma_{12,0}=\frac{d_4}{d_0},\ \gamma_{12,1}=\frac{d_5}{d_1},\ \gamma_{12,2}=\frac{d_6}{d_2},\ \gamma_{12,3}=\frac{d_7}{d_3},$$
$$\gamma_{4,0}=\frac{f_2}{f_0}=\frac{d_2+d_6+\frac{d_0d_6}{d_4}}{d_0+d_4+\frac{d_0d_6}{d_2}},\ \gamma_{4,1}=\frac{f_3}{f_1}=\frac{d_3+d_7+\frac{d_1d_7}{d_5}}{d_1+d_5+\frac{d_1d_7}{d_3}},$$

we note that π acts on the $\gamma_{12,i}$ and $\gamma_{4,j}$ via Φ_{12} and Φ_4.

$$\pi : \gamma_{12,0} \mapsto \gamma_{12,1} \mapsto \cdots \mapsto \gamma_{12,3} \mapsto \gamma_{12,0}^{-1}\gamma_{12,2}$$

$$\pi : \gamma_{4,0} \mapsto \gamma_{4,1} \mapsto \gamma_{4,0}^{-1}$$

We then have

$$L(\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)) \cong L(\gamma_{12,0},\ldots,\gamma_{12,3},\gamma_{4,0},\gamma_{4,1},f_0+f_2,f_1+f_3). \qquad (7.7)$$

Finally, we use (7.2)

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t) \longrightarrow \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow 0.$$

We have

$$\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t) \cong (t^2-1)\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) = \langle \frac{d_2}{d_0},\frac{d_3}{d_1},\ldots,\frac{d_7}{d_5}\rangle,$$

and therefore

$$0 \longrightarrow L(\frac{d_2}{d_0},\ldots,\frac{d_7}{d_5})^\times \longrightarrow L(\frac{d_2}{d_0},\ldots,\frac{d_7}{d_5})^\times \cdot \langle d_0,\ldots,d_7\rangle \xrightarrow{\rho} \langle h_0,h_1\rangle \longrightarrow 0,$$

where ρ maps $d_{2i+j} \mapsto h_j$ for $i = 0,\ldots,3$, and $j = 0,1$. We compute the splitting homomorphism $\sigma : \langle h_0,h_1\rangle \longrightarrow L(\frac{d_2}{d_0},\ldots,\frac{d_7}{d_5})^\times \cdot \langle d_0,\ldots,d_7\rangle$. Letting $x = d_0$, we define σ via

$$\sigma(h_0) := d_0 + d_2 + \cdots + \frac{d_0 d_6}{d_4},$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{d_2}{d_0},\ldots,\frac{d_7}{d_5},d_0+d_2+\cdots+\frac{d_0d_6}{d_4},d_1+d_3+\cdots+\frac{d_1d_7}{d_5}).$$

We define

$$k_0 = \frac{d_2}{d_0},\ k_1 = \frac{d_3}{d_1},\ \ldots, k_5 = \frac{d_7}{d_5},$$

and

Combining this with (7.7) gives

$$L(\gamma_{12,0}, \ldots, \gamma_{12,3}, \gamma_{4,0}, \gamma_{4,1}, f_0 + f_2, f_1 + f_3) \cong L(k_0, \ldots, k_5, f_0 + f_2, f_1 + f_3).$$

Therefore, we have

$$L(\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)) \cong L(\gamma_{12,0}, \ldots, \gamma_{12,3}, \gamma_{4,0}, \gamma_{4,1}). \tag{7.8}$$

We can see $L(k_0, k_1, \cdots, k_5) = L(\gamma_{12,0}, \ldots, \gamma_{12,3}, \gamma_{4,0}, \gamma_{4,1})$ explicitly, since

$$\gamma_{12,0} = k_0 k_2,\ \ldots, \gamma_{12,3} = k_3 k_5,$$

$$\gamma_{4,0} = k_0\left(\frac{1 + \gamma_{12,2} + \pi^2(\gamma_{12,2})}{1 + \gamma_{12,0} + \gamma_{12,2}}\right),\ \gamma_{4,1} = k_1\left(\frac{1 + \gamma_{12,3} + \pi^2(\gamma_{12,3})}{1 + \gamma_{12,1} + \gamma_{12,3}}\right),$$

and

$$k_0 = \gamma_{4,0}\left(\frac{1 + \gamma_{12,0} + \gamma_{12,2}}{1 + \gamma_{12,2} + \pi^2(\gamma_{12,2})}\right),\ \ldots, k_5 = \gamma_{4,1}\left(\frac{1 + \pi^2(\gamma_{12,3}) + \pi^4(\gamma_{12,3})}{1 + \pi^4(\gamma_{12,3}) + \pi^6(\gamma_{12,3})}\right)$$

We note that the following isomorphism is multiplication by $\Phi_3(t)\Phi_6(t) = t^4 + t^2 + 1$.

$$\langle d_0, \ldots d_7 \rangle \cong \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \cong \Phi_3(t)\Phi_6(t)\mathbb{Z}[t]/(t^{12} - 1)$$

Therefore,

$$d_0 = a_0a_2a_4,\ d_1 = a_1a_3a_5,\ \ldots,\ d_7 = a_7a_9a_{11}.$$

Combining (7.6) and (7.8), we obtain

$$L(\mathbb{Z}[t]/(t^{12}-1)) \cong L(\overset{\oplus}{}_{d\mid 12}\mathbb{Z}[t]/\Phi_d(t)) = L(\gamma_1, \gamma_2, \gamma_{3,0}, \gamma_{3,1}, \gamma_{4,0}, \gamma_{4,1}, \gamma_{6,0}, \gamma_{6,1}, \gamma_{12,0}, \ldots, \gamma_{12,3}).$$

We note that a_0 and its π-conjugates, namely $a_0, \ldots, a_{11}$, are a permutation basis of $\mathbb{Z}G$. We write the permutation basis in terms of the γ_i; it suffices to express a_0 in terms of the γ_i. From (5) we have

$$c_0 = \frac{\gamma_1}{(1+\gamma_{3,0}+\gamma_{3,0}\gamma_{3,1})(1+\gamma_2(\frac{1+\gamma_{6,0}+\gamma_{6,0}\pi^2(\gamma_{6,0})}{1+\gamma_{6,1}+\gamma_{6,1}\pi^2(\gamma_{6,1})}))},\ k_0 = \frac{a_6}{a_0} = \frac{\gamma_{4,0}(1+\gamma_{12,0}+\gamma_{12,2}))}{1+\gamma_{12,2}+\pi^2(\gamma_{12,2})}$$

Finally, we can express a_0 via

$$a_0 = \frac{c_0}{1+k_0}.$$

7.1 Computing the fixed field of I

We next compute the isomorphism

$$L(I) \cong L(J \oplus \overset{\oplus}{}_{d\mid 12, d\neq 12}\mathbb{Z}[\zeta_d]),$$

where $I = \langle 13, t-2 \rangle$. Using the same sequence as the previous section, we have

$$0 \longrightarrow I/\Phi_{12}(t)\Phi_4(t) \longrightarrow I/(t^{12}-1) \longrightarrow I/(t^6-1) \longrightarrow 0 \tag{7.9}$$

$$0 \longrightarrow I/\Phi_{12}(t)\Phi_4(t) \longrightarrow I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^2-1) \longrightarrow 0 \tag{7.10}$$

$$0 \longrightarrow I/\Phi_{12}(t) \longrightarrow I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^4-1) \longrightarrow 0 \tag{7.11}$$

$$0 \longrightarrow I/(t^2+1) \longrightarrow I/(t^4-1) \longrightarrow I/(t^2-1) \longrightarrow 0 \tag{7.12}$$

Again using the $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^{12}-1)$ and the multiplicative group $\langle a_0, a_1, \ldots, a_{11} \rangle$ via $t^i \mapsto a_i$, (7.9) gives

$$0 \longrightarrow L((t^6-1)I/(t^{12}-1))^\times \longrightarrow L((t^6-1)I/(t^{12}-1))^\times \cdot I/(t^{12}-1) \xrightarrow{\rho} \langle b_0, b_1, \ldots, b_5 \rangle \longrightarrow 0,$$

where ρ maps $a_{6i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 5$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, \ldots, b_5 \rangle \longrightarrow L((t^6-1)I/(t^{12}-1))^\times \cdot I/(t^{12}-1).$$

We have the following generating set for I.

$$I = \langle a_0^{13}, a_1^{13}, \ldots, a_{11}^{13}, \frac{a_1}{a_0^2}, \frac{a_2}{a_1^2}, \ldots, \frac{a_{11}}{a_{10}^2}, \frac{a_0}{a_{11}^2} \rangle$$

The image of this set under ρ is

$$\langle a_0^{13}, a_1^{13}, \ldots, a_{11}^{13}, \frac{a_1}{a_0^2}, \frac{a_2}{a_1^2}, \ldots, \frac{a_{11}}{a_{10}^2}, \frac{a_0}{a_{11}^2} \rangle \mapsto \langle b_0^{13}, b_1^{13}, \ldots, b_5^{13}, \frac{b_1}{b_0^2}, \frac{b_2}{b_1^2}, \ldots, \frac{b_5}{b_4^2}, \frac{b_0}{b_5^2} \rangle,$$

and therefore we need to solve

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{12} \end{pmatrix}^{\intercal} \cdot \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 \\ 1 & 0 & 0 & 0 & 0 & -2 \\ 13 & 0 & 0 & 0 & 0 & 0 \\ 0 & 13 & 0 & 0 & 0 & 0 \\ 0 & 0 & 13 & 0 & 0 & 0 \\ 0 & 0 & 0 & 13 & 0 & 0 \\ 0 & 0 & 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 & 0 & 13 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^{\intercal}$$

The solution $(x_1, x_2, \ldots, x_{12}) = (3, 8, 4, 2, 1, 7, 0, 1, 0, 0, 0, 1)$ yields

$$x = \left(\frac{a_1}{a_0^2}\right)^3 \left(\frac{a_2}{a_1^2}\right)^8 \left(\frac{a_3}{a_2^2}\right)^4 \left(\frac{a_4}{a_3^2}\right)^2 \left(\frac{a_5}{a_4^2}\right) \left(\frac{a_6}{a_5^2}\right)^7 a_1^{13} a_5^{13} = \frac{a_6^7}{a_0^6}.$$

We see that $\rho(x) = b_0$, and define σ via

$$\sigma(b_0) = (1 + \frac{\pi^6(x)}{x})x = \frac{a_6^7}{a_0^6} + \frac{a_0^7}{a_6^6},$$

which is fixed by π^6 as required. Therefore, Proposition 3.2 gives

$$L(I/(t^{12} - 1)) \cong L(I/(t^6 + 1) \oplus \langle \frac{a_6^7}{a_0^6} + \frac{a_0^7}{a_6^6}, \frac{a_7^7}{a_1^6} + \frac{a_1^7}{a_7^6}, \ldots, \frac{a_{11}^7}{a_5^6} + \frac{a_5^7}{a_{11}^6} \rangle) \tag{7.13}$$

We define

$$c_0 = \frac{a_6^7}{a_0^6} + \frac{a_0^7}{a_6^6},\ c_1 = \frac{a_7^7}{a_1^6} + \frac{a_1^7}{a_7^6},\ \ldots,\ c_5 = \frac{a_{11}^7}{a_5^6} + \frac{a_5^7}{a_{11}^6}$$

and see that π permutes them cyclically. Using (5.13), we have

$$L(I/(t^6 - 1)) \cong L(\overset{\oplus}{_{d \mid 6}} \mathbb{Z}[t]/\Phi_d(t)) = L(\gamma_1, \gamma_2, \gamma_{3,0}, \gamma_{3,1}, \gamma_{6,0}, \gamma_{6,1}),$$

where

$$\gamma_{6,0} = \frac{c_3c_4}{c_0c_1},\ \gamma_{6,1} = \frac{c_4c_5}{c_1c_2},\ \gamma_{3,0} = \frac{c_1+c_4}{c_0+c_3},\ \gamma_{3,1} = \frac{c_2+c_5}{c_1+c_4},$$

$$\gamma_2 = \frac{c_1c_2c_3 + c_0c_1c_5 + c_3c_4c_5}{c_0c_1c_2 + c_2c_3c_4 + c_0c_4c_5},\ \gamma_1 = c_0 + c_1 + \cdots + c_5$$

Combining this with (7.13) gives

$$L(I/(t^{12}-1)) \cong L(I/(t^6+1) \oplus \langle \gamma_1, \gamma_2, \gamma_{3,0}, \gamma_{3,1}, \gamma_{6,0}, \gamma_{6,1} \rangle). \tag{7.14}$$

Next, we compute generators of $L(I/(t^6+1))$ that π acts on via Φ_{12} and Φ_4. From (7.11), we have

$$0 \longrightarrow I/\Phi_{12}(t) \longrightarrow I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^4-1) \longrightarrow 0.$$

Writing $\mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)$ multiplicatively as $\langle d_0, d_1, \ldots, d_7 \rangle$ via $t^i \mapsto d_i$, and since the ideal $I/\Phi_{12}(t)$ is generated by $t^3 - t^2 - 2t$, we have

$$I/\Phi_{12}(t) \cong \langle t^7 - t^6 - 2t^5 - t^3 + t^2 + 2t \rangle \cong \langle \frac{d_1^2d_2d_7}{d_3d_5^2d_6}, \frac{d_0d_2d_3}{d_4d_6d_7}, \frac{d_1d_2d_3d_4}{d_0d_5d_6d_7}, \frac{d_2^2d_3d_4d_5}{d_0d_1d_6^2d_7} \rangle,$$

and we have

$$0 \longrightarrow L(\frac{d_1^2d_2d_7}{d_3d_5^2d_6}, \ldots, \frac{d_2^2d_3d_4d_5}{d_0d_1d_6^2d_7})^\times \longrightarrow L(\frac{d_1^2d_2d_7}{d_3d_5^2d_6}, \ldots, \frac{d_2^2d_3d_4d_5}{d_0d_1d_6^2d_7})^\times \cdot \langle I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \rangle$$
$$\xrightarrow{\rho} \langle e_0, \ldots, e_3 \rangle \longrightarrow 0,$$

where ρ maps $d_{4i+j} \mapsto e_j$ for $i = 0, 1$, and $j = 0, \ldots, 3$. We compute the splitting

homomorphism

$$\sigma : \langle e_0, \ldots, e_3 \rangle \longrightarrow L(\frac{d_1^2 d_2 d_7}{d_3 d_5^2 d_6}, \ldots, \frac{d_2^2 d_3 d_4 d_5}{d_0 d_1 d_6^2 d_7})^{\times} \cdot I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t).$$

We have the following generating set for $I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)$.

$$I = \langle d_0^{13}, d_1^{13}, \ldots, d_7^{13}, \frac{d_1}{d_0^2}, \frac{d_2}{d_1^2}, \ldots, \frac{d_7}{d_6^2}, \frac{d_0 d_6}{d_2 d_7^2} \rangle\rangle$$

The image of this set under ρ is the following.

$$\langle d_0^{13}, d_1^{13}, \ldots, d_7^{13}, \frac{d_1}{d_0^2}, \frac{d_2}{d_1^2}, \ldots, \frac{d_7}{d_6^2}, \frac{d_0 d_6}{d_2 d_7^2} \rangle \mapsto \langle e_0^{13}, e_1^{13}, \ldots, e_3^{13}, \frac{e_1}{e_0^2}, \frac{e_2}{e_1^2}, \frac{e_3}{e_2^2}, \frac{e_0}{e_3^2} \rangle,$$

and therefore we need to solve

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{16} \end{pmatrix}^{\intercal} \cdot \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 1 & -2 \\ 13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 13 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 13 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 13 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 13 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 13 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 13 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^{\intercal}$$

The solution $(x_1, x_2, \ldots, x_{16}) = (0, -6, -3, -8, -4, 4, 15, 1, 0, -1, 0, 1, 0, 1, 2, -1)$ yields

$$x = \left(\frac{d_2}{d_1^2}\right)^{-6}\left(\frac{d_3}{d_2^2}\right)^{-3}\left(\frac{d_4}{d_3^2}\right)^{-8}\left(\frac{d_5}{d_4^2}\right)^{-4}\left(\frac{d_6}{d_5^2}\right)^{4}\left(\frac{d_7}{d_6^2}\right)^{15}\left(\frac{d_0 d_6}{d_2 d_7^2}\right)(d_1^{13})^{-1}(d_3^{13})(d_5^{13})(d_6^{13})^2(d_7^{13})^{-1}$$
$$= \frac{d_0 d_5 d_6}{d_1 d_2}.$$

We see that $\rho(x) = e_0$, and we define σ via

$$\sigma(e_0) = \frac{d_0 d_5 d_6}{d_1 d_2} + \frac{d_0 d_1 d_7}{d_3 d_5} + \frac{d_3 d_4}{d_7},$$

which is fixed by π^4 as required. Therefore, Proposition 3.2 gives

$$L(I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{d_1^2 d_2 d_7}{d_3 d_5^2 d_6}, \ldots, \frac{d_2^2 d_3 d_4 d_5}{d_0 d_1 d_6^2 d_7}, \frac{d_0 d_5 d_6}{d_1 d_2} + \frac{d_0 d_1 d_7}{d_3 d_5} + \frac{d_3 d_4}{d_7},$$
$$\frac{d_1 d_6 d_7}{d_2 d_3} + \frac{d_0 d_1}{d_4} + \frac{d_2 d_4 d_5}{d_0 d_6}, \frac{d_0 d_6 d_7}{d_3 d_4} + \frac{d_1 d_2}{d_5} + \frac{d_3 d_5 d_6}{d_1 d_7}, \frac{d_0 d_1 d_6 d_7}{d_2 d_4 d_5} + \frac{d_2 d_3}{d_6} + \frac{d_4 d_7}{d_0})$$

Noting that the last 4 generators are permuted cyclically by π, using the result from the previous section, we have

$$L(w_0, w_1, w_2, w_3) = L(\frac{w_2}{w_0}, \frac{w_3}{w_1}, w_0 + w_2, w_1 + w_3),$$

and therefore

$$L(I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)) \cong L(\frac{d_1^2 d_2 d_7}{d_3 d_5^2 d_6}, \ldots, \frac{d_2^2 d_3 d_4 d_5}{d_0 d_1 d_6^2 d_7}, \frac{\frac{d_0 d_6 d_7}{d_3 d_4} + \frac{d_1 d_2}{d_5} + \frac{d_3 d_5 d_6}{d_1 d_7}}{\frac{d_0 d_5 d_6}{d_1 d_2} + \frac{d_0 d_1 d_7}{d_3 d_5} + \frac{d_3 d_4}{d_7}},$$
$$\frac{\frac{d_0 d_1 d_6 d_7}{d_2 d_4 d_5} + \frac{d_2 d_3}{d_6} + \frac{d_4 d_7}{d_0}}{\frac{d_1 d_6 d_7}{d_2 d_3} + \frac{d_0 d_1}{d_4} + \frac{d_2 d_4 d_5}{d_0 d_6}}, \frac{d_0 d_5 d_6}{d_1 d_2} + \frac{d_0 d_6 d_7}{d_3 d_4} + \cdots + \frac{d_3 d_5 d_6}{d_1 d_7}, \frac{d_1 d_6 d_7}{d_2 d_3} + \frac{d_0 d_1 d_6 d_7}{d_2 d_4 d_5} + \cdots + \frac{d_4 d_7}{d_0}). \tag{7.15}$$

From (7.10) we have

$$0 \longrightarrow I/\Phi_{12}(t)\Phi_4(t) \longrightarrow I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \longrightarrow I/(t^2-1) \longrightarrow 0,$$

giving a $\mathbb{Z}G$-module isomorphism $I/\Phi_{12}(t)\Phi_4(t) \cong (t^2-1)I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t)$. We compute the splitting homomorphism

$$\sigma : \langle h_0, h_1 \rangle \longrightarrow L((t^2-1)I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t))^{\times} \cdot I/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t).$$

Since the last two generators from (7.15) are swapped by π, we define $x := \frac{d_0d_5d_6}{d_1d_2}$ and

$$\sigma(h_0) := x + \pi^2(x) + \cdots + \pi^{10}(x) = \frac{d_0d_5d_6}{d_1d_2} + \frac{d_0d_6d_7}{d_3d_4} + \cdots + \frac{d_3d_5d_6}{d_1d_7}.$$

Therefore we have a description of $L(I/\Phi_{12}(t)\Phi_4(t))$.

$$L(I/\Phi_{12}(t))\Phi_4(t)) \cong L(\frac{d_1^2d_2d_7}{d_3d_5^2d_6}, \ldots, \frac{d_2^2d_3d_4d_5}{d_0d_1d_6^2d_7}, \frac{\frac{d_0d_6d_7}{d_3d_4} + \frac{d_1d_2}{d_5} + \frac{d_3d_5d_6}{d_1d_7}}{\frac{d_0d_5d_6}{d_1d_2} + \frac{d_0d_1d_7}{d_3d_5} + \frac{d_3d_4}{d_7}}, \frac{\frac{d_0d_1d_6d_7}{d_2d_4d_5} + \frac{d_2d_3}{d_6} + \frac{d_4d_7}{d_0}}{\frac{d_1d_6d_7}{d_2d_3} + \frac{d_0d_1}{d_4} + \frac{d_2d_4d_5}{d_0d_6}}). \quad (7.16)$$

We note that the following isomorphism is multiplication by $\Phi_3(t)\Phi_6(t) = t^4+t^2+1$

$$\langle d_0, \ldots d_7 \rangle \cong \mathbb{Z}[t]/\Phi_{12}(t)\Phi_4(t)\Phi_2(t)\Phi_1(t) \cong \Phi_3(t)\Phi_6(t)\mathbb{Z}[t]/(t^{12}-1).$$

Therefore,

$$d_0 = a_0a_2a_4,\ d_1 = a_1a_3a_5,\ \ldots,\ d_7 = a_7a_9a_{11}$$

We define

$$\gamma_{12,0} = \frac{d_1^2 d_2 d_7}{d_3 d_5^2 d_6}\ \gamma_{12,1} = \frac{d_0 d_2 d_3}{d_4 d_6 d_7},\ \gamma_{12,2} = \frac{d_1 d_2 d_3 d_4}{d_0 d_5 d_6 d_7},\ \gamma_{12,3} = \frac{d_2^2 d_3 d_4 d_5}{d_0 d_1 d_6^2 d_7},$$

$$\gamma_{4,0} = \frac{\frac{d_0 d_6 d_7}{d_3 d_4} + \frac{d_1 d_2}{d_5} + \frac{d_3 d_5 d_6}{d_1 d_7}}{\frac{d_0 d_5 d_6}{d_1 d_2} + \frac{d_0 d_1 d_7}{d_3 d_5} + \frac{d_3 d_4}{d_7}},\ \gamma_{4,1} = \frac{\frac{d_0 d_1 d_6 d_7}{d_2 d_4 d_5} + \frac{d_2 d_3}{d_6} + \frac{d_4 d_7}{d_0}}{\frac{d_1 d_6 d_7}{d_2 d_3} + \frac{d_0 d_1}{d_4} + \frac{d_2 d_4 d_5}{d_0 d_6}}$$

Combining (7.14) and (7.16), we obtain the isomorphism

$$L(I/(t^{12}-1)) \cong L(\overset{\oplus}{_{d \mid 12}} I/\Phi_d(t)) = L(\gamma_1, \gamma_2, \gamma_{3,0}, \gamma_{3,1}, \gamma_{4,0}, \gamma_{4,1}, \gamma_{6,0}, \gamma_{6,1}, \gamma_{12,0}, \ldots, \gamma_{12,3}).$$

To compute a generator of the permutation basis, we compute $c_0 = \frac{a_6^7}{a_0^6} + \frac{a_0^7}{a_6^6}$ and α, which corresponds to $\frac{a_6}{a_0}$ from the previous section.

$$\alpha = \frac{\gamma_{4,0}(1 + \gamma_{12,0} + \gamma_{12,2}))}{1 + \gamma_{12,2} + \pi^2(\gamma_{12,2})} = \frac{d_1 d_2 d_7}{d_3 d_4 d_5} = \frac{a_1 a_2 a_{11}}{a_5 a_7 a_8}$$

Finally, we compute a generator β of the permutation basis.

$$\beta = \frac{c_0}{1+\alpha} = \frac{a_0^{13} a_5 a_7 a_8 + a_5 a_6^{13} a_7 a_8}{a_0^6 a_5 a_6^6 a_7 a_8 + a_0^6 a_1 a_2 a_6^6 a_{11}}$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$. We define the 12×12 matrix T whose (i,j)-th entry is $\zeta^{2^{i+j}}$ and compute the generators $u_0, \ldots, u_{11}$ as follows, where ζ denotes a primitive 13-th root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{11} \end{pmatrix} = T \cdot \begin{pmatrix} \beta \\ \pi(\beta) \\ \vdots \\ \pi^{11}(\beta) \end{pmatrix}$$

Therefore, we have $K(x_0, \ldots, x_{12})^\tau = K(y_0, u_0, u_1, \ldots, u_{11})$.

Chapter 8: The case $A = \mathbb{Z}/17\mathbb{Z}$

We next compute generators of the fixed field $K(x_0, \ldots, x_{16})^A$, where $A = \langle \tau \rangle$. The Galois group $G = \langle \pi \rangle$ of L/K has order 16 and we have $I = \langle 17, t-3 \rangle \subseteq \mathbb{Z}G$ and $J = \langle 17, \zeta - 3 \rangle = \langle \zeta^5 + \zeta^4 - 1 \rangle \subseteq \mathbb{Z}[\zeta]$, where ζ denotes a primitive 16-th root of unity.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^{16}-1)) \cong L(\overset{\oplus}{}_{d \mid 16} \mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_{15} \rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_{15} \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action.

We first compute the sequence of equivalence relations of $p - 1 = 16$ as in (3.1.1).

$$\{\{1,2,4,8,16\}\} \mapsto \{\{1,2,4,8\},\{16\}\} \mapsto \{\{1,2,4\},\{8\},\{16\}\} \mapsto \{\{1,2\},\{4\},\{8\},\{16\}\} \mapsto$$
$$\{\{1\},\{2\},\{4\},\{8\},\{16\}\}$$

This gives rise to the following exact sequences

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{16}(t) \longrightarrow \mathbb{Z}[t]/(t^{16}-1) \longrightarrow \mathbb{Z}[t]/(t^8-1) \longrightarrow 0 \tag{8.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{8}(t) \longrightarrow \mathbb{Z}[t]/(t^{8}-1) \longrightarrow \mathbb{Z}[t]/(t^4-1) \longrightarrow 0 \tag{8.2}$$

Starting with (8.1), we have

$$\mathbb{Z}[t]/\Phi_{16}(t) \cong (t^8-1)\mathbb{Z}[t]/(t^{16}-1) = \langle \frac{a_8}{a_0}, \frac{a_9}{a_1}, \ldots, \frac{a_{15}}{a_7} \rangle.$$

Therefore, we have the exact sequence

$$0 \longrightarrow L(\frac{a_8}{a_0}, \ldots, \frac{a_{15}}{a_7})^\times \longrightarrow L(\frac{a_8}{a_0}, \ldots, \frac{a_{15}}{a_7})^\times \cdot \langle a_0, \ldots, a_{15} \rangle \xrightarrow{\rho} \langle b_0, b_1, \ldots, b_7 \rangle \longrightarrow 0,$$

where ρ maps $a_{8i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 7$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, \ldots, b_7 \rangle \longrightarrow L(\frac{a_8}{a_0}, \ldots, \frac{a_{15}}{a_7})^\times \cdot \langle a_0, \ldots, a_{15} \rangle$$

by letting $x = a_0$ and defining

$$\sigma(b_0) = (1 + \frac{a_8}{a_0})a_0 = a_0 + a_8,$$

which is fixed by π^8 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^{16}-1)) \cong L(a_0, \ldots, a_{15}) = L(\frac{a_8}{a_0}, \frac{a_9}{a_1}, \ldots, \frac{a_{15}}{a_7}, a_0+a_8, a_1+a_9 \ldots, a_7+a_{15}). \quad (8.3)$$

We see this explicitly since

$$a_0 = \frac{a_0 + a_8}{1 + \frac{a_8}{a_0}}, \ \ldots, a_{15} = \frac{a_7 + a_{15}}{1 + \frac{a_7}{a_{15}}}.$$

We define

$$\gamma_{16,0} = \frac{a_8}{a_0},\ \gamma_{16,1} = \frac{a_9}{a_1},\ \ldots,\ \gamma_{16,7} = \frac{a_{15}}{a_7}$$

and note that π acts on the $\gamma_{16,i}$ via Φ_{16}, that is

$$\pi : \gamma_{16,0} \mapsto \gamma_{16,1} \mapsto \cdots \mapsto \gamma_{16,7} \mapsto \gamma_{16,0}^{-1}$$

We note that the last 8 generators are permuted cyclically by π; we denote these via

$$c_0 = a_0 + a_8,\ c_1 = a_1 + a_9,\ \ldots,\ c_7 = a_7 + a_{15}.$$

From (8.2) we have

$$\mathbb{Z}[t]/\Phi_8(t) \cong (t^4 - 1)\mathbb{Z}[t]/(t^8 - 1) = \langle \frac{c_4}{c_0}, \frac{c_5}{a_1}, \ldots, \frac{c_7}{c_3} \rangle.$$

which yields the sequence

$$0 \longrightarrow L(\frac{c_4}{c_0}, \ldots, \frac{c_7}{c_3})^\times \longrightarrow L(\frac{c_4}{c_0}, \ldots, \frac{c_7}{c_3})^\times \cdot \langle c_0, \ldots, c_7 \rangle \xrightarrow{\rho} \langle d_0, \ldots, d_3 \rangle \longrightarrow 0,$$

where ρ maps $c_{4i+j} \mapsto d_j$, for $i = 0, 1$ and $j = 0, \ldots, 3$.

The splitting homomorphism $\sigma : \langle d_0, \ldots, d_3 \rangle \longrightarrow L(\frac{c_4}{c_0}, \ldots, \frac{c_7}{c_3})^\times \cdot \langle c_0, \ldots, c_7 \rangle$ is defined via $x = c_0$ and

$$\sigma(d_0) = (1 + \frac{c_4}{c_0})c_0 = c_0 + c_4,$$

which is fixed by π^4 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^8 - 1)) \cong L(c_0, \ldots, c_7) = L(\frac{c_4}{c_0}, \ldots, \frac{c_7}{c_3}, c_0 + c_4, \ldots, c_3 + c_7). \tag{8.4}$$

We see this explicitly since

$$c_0 = \frac{c_0 + c_4}{1 + \frac{c_4}{c_0}}, \ \ldots, c_7 = \frac{c_3 + c_7}{1 + \frac{c_7}{c_3}}.$$

We define

$$\gamma_{8,0} = \frac{c_4}{c_0}, \ \ldots, \ \gamma_{8,3} = \frac{c_7}{c_3}$$

and see that π acts on the $\gamma_{8,i}$ via Φ_8, that is

$$\pi : \gamma_{8,0} \mapsto \cdots \mapsto \gamma_{8,3} \mapsto \gamma_{8,0}^{-1}$$

We note that the last 4 generators are permuted cyclically by π; we denote these via

$$e_0 = c_0 + c_4, \ \ldots, \ e_3 = c_3 + c_7.$$

From (4.2), we have

$$L(e_0, e_1, e_2, e_3) = L(\gamma_{4,0}, \gamma_{4,1}, \gamma_2, \gamma_1)$$

where π fixes $\gamma_1 = e_0 + e_1 + e_2 + e_3$, inverts $\gamma_2 = \frac{e_1+e_3}{e_0+e_2}$, and acts on $\gamma_{4,0} = \frac{e_2}{e_0}$ and $\gamma_{4,1} = \frac{e_3}{e_1}$ via $\Phi_2(t)$.

Combining (8.3) and (9.6) gives

$$L(\mathbb{Z}[t]/(t^{16} - 1)) \cong L(\bigoplus_{d \mid 16} \mathbb{Z}[t]/(\Phi_d(t))) = L(\gamma_1, \gamma_2, \gamma_{4,0}, \gamma_{4,1}, \gamma_{8,0}, \ldots, \gamma_{8,3}, \gamma_{16,0}, \ldots, \gamma_{16,7}).$$

We note that a_0 and its π-conjugates, namely $a_0, \ldots, a_{15}$, are a permutation basis

of $\mathbb{Z}G$. We write the permutation basis in terms of the γ_i; it suffices to express a_0 in terms of the γ_i. We can see that

$$a_0 = \frac{c_0}{1+\gamma_{16,0}},\ c_0 = \frac{e_0}{1+\gamma_{8,0}},\ e_0 = \frac{\frac{\gamma_1}{1+\gamma_2}}{1+\gamma_{4,0}}.$$

8.1 Computing the fixed field of I

We next compute the isomorphism

$$L(I) \cong L(J \oplus \overset{\oplus}{}_{d \mid 16, d \neq 16} \mathbb{Z}[\zeta_d]),$$

where $I = \langle 17, t-3 \rangle$. Using the same sequence as the previous section, we have

$$0 \longrightarrow I/\Phi_{16}(t) \longrightarrow I/(t^{16}-1) \longrightarrow I/(t^8-1) \longrightarrow 0 \tag{8.5}$$

$$0 \longrightarrow I/\Phi_8(t) \longrightarrow I/(t^8-1) \longrightarrow I/(t^4-1) \longrightarrow 0 \tag{8.6}$$

Since $I/\Phi_{16}(t)$ is principal and generated by t^5+t^4-1, (8.5) gives

$$I/\Phi_{16}(t) \cong (t^8-1)I/(t^{16}-1) = \langle t^{13}+t^{12}-t^8-t^5-t^4+1 \rangle = \langle \frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8}, \ldots, \frac{a_7 a_{19} a_{20}}{a_{11} a_{12} a_{15}} \rangle,$$

and

$$0 \longrightarrow L(\frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8}, \ldots, \frac{a_7 a_{19} a_{20}}{a_{11} a_{12} a_{15}})^{\times} \longrightarrow L(\frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8}, \ldots, \frac{a_7 a_{19} a_{20}}{a_{11} a_{12} a_{15}})^{\times} \cdot I/(t^{16}-1)$$
$$\xrightarrow{\rho} \langle b_0, \ldots, b_7 \rangle \longrightarrow 0,$$

where ρ maps $a_{8i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 7$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, \ldots, b_7 \rangle \longrightarrow L(\frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8}, \ldots, \frac{a_7 a_{19} a_{20}}{a_{11} a_{12} a_{15}})^{\times} \cdot I/(t^{16} - 1).$$

We have the following generating set for I.

$$I = \langle a_0^{17}, a_1^{17}, \ldots, a_{15}^{17}, \frac{a_1}{a_0^3}, \frac{a_2}{a_1^3}, \ldots, \frac{a_{15}}{a_{14}^3}, \frac{a_0}{a_{15}^3} \rangle$$

The image of this set under ρ is

$$\langle a_0^{17}, \ldots, a_{15}^{17}, \frac{a_1}{a_0^3}, \ldots, \frac{a_{15}}{a_{14}^3}, \frac{a_0}{a_{15}^3} \rangle \mapsto \langle b_0^{17}, \ldots, b_7^{17}, \frac{b_1}{b_0^3}, \ldots, \frac{b_7}{b_6^3}, \frac{b_0}{b_7^3} \rangle.$$

We find an element $x \in I/(t^{16} - 1)$ such that $\rho(x) = b_0$ via

$$x = \left(\frac{a_1}{a_0^3}\right)^{14} \left(\frac{a_2}{a_1^3}\right)^{16} \left(\frac{a_3}{a_2^3}\right)^{11} \left(\frac{a_4}{a_3^3}\right)^{15} \left(\frac{a_5}{a_4^3}\right)^{5} \left(\frac{a_6}{a_5^3}\right)^{13} \left(\frac{a_7}{a_6^3}\right)^{10} \left(\frac{a_8}{a_7^3}\right)^{9} (a_0^{17})^2 (a_1^{17})^2 (a_2^{17})$$
$$(a_3^{17})^2 (a_5^{17})^2 (a_6^{17}) (a_7^{17}) = \frac{a_8^9}{a_0^8},$$

which gives us

$$\sigma(b_0) = (1 + \frac{\pi^8(x)}{x})x = \frac{a_8^9}{a_0^8} + \frac{a_0^9}{a_8^8}.$$

Therefore, Proposition 3.2 gives

$$L(I/(t^{16} - 1)) \cong L(\frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8}, \ldots, \frac{a_7 a_{19} a_{20}}{a_{11} a_{12} a_{15}}, \frac{a_8^9}{a_0^8} + \frac{a_0^9}{a_8^8}, \frac{a_9^9}{a_1^8} + \frac{a_1^9}{a_9^8}, \ldots, \frac{a_{15}^9}{a_7^8} + \frac{a_7^9}{a_{15}^8}) \qquad (8.7)$$

We define

$$\gamma_{16,0} = \frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8},\ \gamma_{16,1} = \frac{a_1 a_{13} a_{14}}{a_5 a_6 a_9},\ \ldots,\ \gamma_{16,7} = \frac{a_7 a_{19} a_{20}}{a_{11} a_{12} a_{15}}$$

and note that the last 8 generators are permuted cyclically by π; we define the following and use the results from the previous section.

$$c_0 = \frac{a_8^9}{a_0^8} + \frac{a_0^9}{a_8^8},\ c_1 = \frac{a_9^9}{a_1^8} + \frac{a_1^9}{a_9^8},\ \ldots,\ c_7 = \frac{a_{15}^9}{a_7^8} + \frac{a_7^9}{a_{15}^8}$$

$$e_0 = c_0 + c_4,\ \ldots,\ e_3 = c_3 + c_7.$$

$$\gamma_{8,0} = \frac{c_4}{c_0},\ \ldots,\ \gamma_{8,3} = \frac{c_7}{c_3}$$

$$\gamma_1 = e_0 + e_1 + e_2 + e_3,\ \gamma_2 = \frac{e_1 + e_3}{e_0 + e_2},\ \gamma_{4,0} = \frac{e_2}{e_0},\ \gamma_{4,1} = \frac{e_3}{e_1}$$

We then have

$$L(c_0, \ldots, c_7) = L(\frac{c_4}{c_0}, \ldots, \frac{c_7}{c_3}, \gamma_{4,0}, \gamma_{4,1}, \gamma_2, \gamma_1).$$

Combining this with (8.7) gives

$$L(I/(t^{16}-1)) \cong L(\overset{\oplus}{}_{d\,|\,16} I/(\Phi_d(t))) = L(\gamma_1, \gamma_2, \gamma_{4,0}, \gamma_{4,1}, \gamma_{8,0}, \ldots, \gamma_{8,3}, \gamma_{16,0}, \ldots, \gamma_{16,7}).$$

We compute a generator α of the permutation basis, which corresponds to a_0 from the previous section.

$$\alpha = \frac{c_0}{1 + \gamma_{16,0}} = \frac{\frac{a_8^9}{a_0^8} + \frac{a_0^9}{a_8^8}}{1 + \frac{a_0 a_{12} a_{13}}{a_4 a_5 a_8}}$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$.

We define the 16×16 matrix T whose (i, j)-th entry is $\zeta^{3^{i+j}}$ and compute the generators $u_0, \ldots, u_{15}$ as follows, where ζ denotes a primitive 17-th root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{15} \end{pmatrix} = T \cdot \begin{pmatrix} \alpha \\ \pi(\alpha) \\ \vdots \\ \pi^{15}(\alpha) \end{pmatrix}$$

Therefore, we have $K(x_0, \ldots, x_{16})^\tau = K(y_0, u_0, u_1, \ldots, u_{15})$.

Chapter 9: The case $A = \mathbb{Z}/19\mathbb{Z}$

We next compute generators of the fixed field $K(x_0, \ldots, x_{18})^A$, where $A = \langle \tau \rangle$. The Galois group $G = \langle \pi \rangle$ of L/K has order 18 and we have $I = \langle 19, t-2 \rangle \subseteq \mathbb{Z}G$ and $J = \langle 19, \zeta - 2 \rangle = \langle \zeta^5 - \zeta^4 + \zeta^3 - \zeta^2 - 1 \rangle \subseteq \mathbb{Z}[\zeta]$, where ζ denotes a primitive 18-th root of unity.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^{18}-1)) \cong L(\overset{\oplus}{}_{d \mid 18} \mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_{17} \rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_{17} \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action.

We compute the sequence of equivalence relations for $p - 1 = 18$ as in (3.1.1).

$$\{\{1,2,3,6,9,18\}\} \mapsto \{\{1,3,9\},\{2,6,18\}\} \mapsto \{\{1,3\},\{9\},\{2,6,18\}\} \mapsto \{\{1,2,3,6,18\},\{9\}\} \mapsto$$

$$\{\{1,2,3,6\},\{9\},\{18\}\} \mapsto \{\{1,3\},\{2,6\},\{9\},\{18\}\} \mapsto \{\{1\},\{3\},\{2,6\},\{9\},\{18\}\} \mapsto$$

$$\{\{1,2,6\},\{3\},\{9\},\{18\}\} \mapsto \{\{1,2\},\{3\},\{6\},\{9\},\{18\}\} \mapsto \{\{1\},\{2\},\{3\},\{6\},\{9\},\{18\}\}$$

This gives rise to the following exact sequences, which we use along with results

from (5)

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^{18}-1) \longrightarrow \mathbb{Z}[t]/(t^9-1) \longrightarrow 0 \tag{9.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_9(t) \longrightarrow \mathbb{Z}[t]/(t^9-1) \longrightarrow \mathbb{Z}[t]/(t^3-1) \longrightarrow 0 \tag{9.2}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^6-1)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^3-1) \longrightarrow 0 \tag{9.3}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^6-1)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^6-1) \longrightarrow 0 \tag{9.4}$$

Starting with (9.1), we have

$$\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \cong (t^9-1)\mathbb{Z}[t]/(t^{18}-1) = \langle \frac{a_9}{a_0}, \frac{a_{10}}{a_1}, \ldots, \frac{a_{17}}{a_8} \rangle.$$

Therefore, we have the exact sequence

$$0 \longrightarrow L(\frac{a_9}{a_0}, \ldots, \frac{a_{17}}{a_8})^\times \longrightarrow L(\frac{a_9}{a_0}, \ldots, \frac{a_{17}}{a_8})^\times \cdot \langle a_0, \ldots, a_{17} \rangle \xrightarrow{\rho} \langle b_0, b_1, \ldots, b_8 \rangle \longrightarrow 0,$$

where ρ maps $a_{9i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 8$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1, \ldots, b_8 \rangle \longrightarrow L(\frac{a_9}{a_0}, \ldots, \frac{a_{17}}{a_8})^\times \cdot \langle a_0, \ldots, a_{17} \rangle.$$

Letting $x = a_0$, we define σ via

$$\sigma(b_0) = (1 + \frac{\pi^9(x)}{x})x = a_0 + a_9,$$

which is fixed by π^9 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^{18}-1)) \cong L(a_0,\ldots,a_{17}) = L(\frac{a_9}{a_0},\ldots,\frac{a_{17}}{a_8}, a_0+a_9, a_1+a_{10}\ldots,a_8+a_{17}). \quad (9.5)$$

We see this explicitly since

$$a_0 = \frac{a_0+a_9}{1+\frac{a_9}{a_0}},\ \ldots, a_{17} = \frac{a_8+a_{17}}{1+\frac{a_8}{a_{17}}}.$$

We note that the last 9 generators are permuted cyclically by π; we denote these via

$$c_0 = a_0+a_9,\ c_1 = a_1+a_{10},\ \ldots,\ c_8 = a_8+a_{17}.$$

From sequence (9.2), we have

$$\mathbb{Z}[t]/\Phi_9(t) \cong (t^3-1)\mathbb{Z}[t]/(t^9-1) = \langle \frac{c_3}{c_0}, \frac{c_4}{a_1}, \ldots, \frac{c_8}{c_5}\rangle.$$

and

$$0 \longrightarrow L(\frac{c_3}{c_0},\ldots,\frac{c_8}{c_5})^\times \longrightarrow L(\frac{c_3}{c_0},\ldots,\frac{c_8}{c_5})^\times \cdot \langle c_0,\ldots,c_8\rangle \xrightarrow{\rho} \langle d_0,d_1,d_2\rangle \longrightarrow 0,$$

where ρ maps $c_{3i+j} \mapsto d_j$, for $i = 0,1,2$ and $j = 0,1,2$. We compute the splitting homomorphism

$$\sigma : \langle d_0,d_1,d_2\rangle \longrightarrow L(\frac{c_3}{c_0},\ldots,\frac{c_8}{c_5})^\times \cdot \langle c_0,\ldots,c_8\rangle$$

by letting $x = c_0$ and defining σ via

$$\sigma(d_0) = (1+\frac{\pi^3(x)}{x}+\frac{\pi^3(x)}{x}\frac{\pi^6(x)}{\pi^3(x)})x = c_0+c_3+c_6.$$

Therefore, we have

$$L(\mathbb{Z}[t]/(t^9-1)) \cong L(c_0,\ldots,c_8) = L(\frac{c_3}{c_0},\ldots,\frac{c_8}{c_5}, c_0+c_3+c_6, c_1+c_4+c_7, c_2+c_5+c_8). \quad (9.6)$$

We see this explicitly since

$$c_0 = \frac{c_0+c_3+c_6}{1+\frac{c_3}{c_0}+\frac{c_3}{c_0}\frac{c_6}{c_3}}, \ \ldots, c_8 = \frac{c_2+c_5+c_8}{1+\frac{c_5}{c_8}+\frac{c_2}{c_5}\frac{c_5}{c_8}}.$$

We define

$$\gamma_{9,0} = \frac{c_3}{c_0}, \ \ldots, \ \gamma_{9,5} = \frac{c_8}{c_5}$$

and note that π acts on the $\gamma_{9,i}$ via Φ_9, that is

$$\pi : \gamma_{9,0} \mapsto \cdots \mapsto \gamma_{9,5} \mapsto \gamma_{9,0}^{-1}\gamma_{9,3}^{-1}$$

We see that $c_0+c_3+c_6$, $c_1+c_4+c_7$, and $c_2+c_5+c_8$ are permuted by π. Using (5.7), we have

$$L(u_0,u_1,u_2) = L(\frac{u_1}{u_0}, \frac{u_2}{u_1}, u_0+u_1+u_2)$$

and therefore

$$L(c_0+c_3+c_6, c_1+c_4+c_7, c_2+c_5+c_8) = L(\frac{c_1+c_4+c_7}{c_0+c_3+c_6}, \frac{c_2+c_5+c_8}{c_1+c_4+c_7}, c_0+c_1+\cdots+c_8).$$

We define

$$\gamma_{3,0} = \frac{c_1+c_4+c_7}{c_0+c_3+c_6}, \ \gamma_{3,1} = \frac{c_2+c_5+c_8}{c_1+c_4+c_7}, \ \gamma_1 = c_0+c_1+\cdots+c_8.$$

Combining this with (9.6) and (9.5)s gives

$$L(\mathbb{Z}[t]/(t^{18}-1)) \cong L(\frac{a_9}{a_0}, \ldots, \frac{a_{17}}{a_8}, \gamma_{9,0}, \ldots, \gamma_{9,5}, \gamma_{3,0}, \gamma_{3,1}, \gamma_1). \tag{9.7}$$

Next, we compute generators of $L(\mathbb{Z}[t]/(t^{18}+1))$ that π acts on via $\Phi_2(t)$, $\Phi_6(t)$, and $\Phi_{18}(t)$. From (9.4) we have

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^6-1)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^6-1) \longrightarrow 0.$$

Since $(t^6-1)\Phi_{18}(t)$ is a degree 12 polynomial, we have a $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^6-1)\Phi_{18}(t)$ and the multiplicative group $\langle e_0, e_1, \ldots, e_{11}\rangle$ via $t^i \mapsto e_i$, where π acts via

$$e_0 \mapsto e_1 \mapsto \cdots \mapsto e_{11} \mapsto \frac{e_0 e_9}{e_3} \mapsto \cdots \mapsto \frac{e_2 e_{11}}{e_8} \mapsto e_0.$$

Therefore, we have

$$\mathbb{Z}[t]/\Phi_{18}(t) \cong (t^6-1)\mathbb{Z}[t]/(t^6-1)\Phi_{18}(t) = \langle \frac{e_6}{e_0}, \frac{e_7}{e_1}, \ldots, \frac{e_{11}}{e_5}\rangle$$

and the exact sequence

$$0 \longrightarrow L(\frac{e_6}{e_0}, \ldots, \frac{e_{11}}{e_5})^\times \longrightarrow L(\frac{e_6}{e_0}, \ldots, \frac{e_{11}}{e_5})^\times \cdot \langle e_0, \ldots, e_{11}\rangle \xrightarrow{\rho} \langle f_0, f_1, \ldots, f_5\rangle \longrightarrow 0,$$

where ρ sends $e_0 \mapsto f_0, \ldots, e_5 \mapsto f_5, e_6 \mapsto f_0, e_7 \mapsto f_1, \ldots, e_{11} \mapsto f_5$.

We compute the splitting homomorphism

$$\sigma : \langle f_0, \ldots, f_5\rangle \longrightarrow L(\frac{e_6}{e_0}, \ldots, \frac{e_{11}}{e_5})^\times \cdot \langle e_0, \ldots, e_{11}\rangle$$

by letting $x = e_0$ and defining

$$\sigma(f_0) = (1 + \frac{\pi^6(x)}{x} + \frac{\pi^6(x)}{x}\frac{\pi^1 2(x)}{\pi^6(x)})x = e_0 + e_6 + \frac{e_0 e_9}{e_3},$$

which is fixed by π^6 as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^6 - 1)\Phi_{18}(t)) \;\cong\; L(\frac{e_6}{e_0}, \ldots, \frac{e_{11}}{e_5}, e_0 + e_6 + \frac{e_0 e_9}{e_3}, \ldots, e_5 + e_{11} + \frac{e_2 e_{11}}{e_8}). \quad (9.8)$$

We define

$$\gamma_{18,0} = \frac{e_6}{e_0},\ \gamma_{18,1} = \frac{e_7}{e_1},\ \ldots,\ \gamma_{18,5} = \frac{e_{11}}{e_5}$$

and we note that π acts on the $\gamma_{18,i}$ via $\Phi_{18}(t)$, that is

$$\gamma_{18,0} \mapsto \gamma_{18,1} \mapsto \cdots \mapsto \gamma_{18,5} \mapsto \gamma_{18,0}^{-1}\gamma_{18,3}.$$

Therefore we have

$$L(\mathbb{Z}[t]/(t^6 - 1)\Phi_{18}(t)) \cong L(\gamma_{18,0}, \gamma_{18,1}, \ldots, \gamma_{18,5}, e_0 + e_6 + \frac{e_0 e_9}{e_3}, \ldots, e_5 + e_{11} + \frac{e_2 e_{11}}{e_8}). \quad (9.9)$$

We see that the last 6 generators are permuted cyclically by π. We define

$$g_0 = e_0 + e_6 + \frac{e_0 e_9}{e_3},\ g_1 = e_1 = e_7 + \frac{e_1 e_{10}}{e_4},\ \ldots,\ g_5 = e_5 + e_{11} + \frac{e_2 e_{11}}{e_8}.$$

From (5.13) we have

$$L(\mathbb{Z}[t]/(t^6 - 1) \cong L(g_0 + g_3, g_1 + g_4, g_2 + g_5, \gamma_2, \gamma_{6,0}, \gamma_{6,1}),$$

where

$$\gamma_2 = \frac{g_1g_2g_3 + g_0g_1g_5 + g_3g_4g_5}{g_0g_1g_2 + g_2g_3g_4 + g_0g_4g_5},\ \gamma_{6,0} = \frac{g_3g_4}{g_0g_1},\ \gamma_{6,1} = \frac{g_4g_5}{g_1g_2}.$$

We note that $g_0 + g_3$, $g_1 + g_4$, and $g_2 + g_5$ generate a module isomorphic to $\mathbb{Z}[t]/(t^3 - 1)$.

Combining this with (9.9) gives

$$L(\mathbb{Z}[t]/(t^6-1)\Phi_{18}(t)) \cong L(g_0+g_3, g_1+g_4, g_2+g_5, \gamma_2, \gamma_{6,0}, \gamma_{6,1}, \gamma_{18,0}, \gamma_{18,1}, \ldots, \gamma_{18,5}). \quad (9.10)$$

From sequence (9.3) we had

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^6 - 1)\Phi_{18}(t) \longrightarrow \mathbb{Z}[t]/(t^3 - 1) \longrightarrow 0$$

In this sequence, we have descriptions of the fields corresponding to the middle and right components. We use these to find a description of $L(\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t))$.

Since $\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \cong (t^3 - 1)\mathbb{Z}[t]/(t^6 - 1)\Phi_{18}(t)$, we have

$$\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \cong \langle \frac{e_3}{e_0}, \frac{e_4}{e_1}, \ldots, \frac{e_{11}}{e_8} \rangle.$$

We define

$$h_0 = \frac{e_3}{e_0},\ h_1 = \frac{e_4}{e_1},\ \ldots,\ h_8 = \frac{e_{11}}{e_8}.$$

We then have

$$0 \longrightarrow L(h_0, \ldots, h_8)^\times \longrightarrow L(h_0, \ldots, h_8)^\times \cdot \langle e_0, \ldots, e_{11} \rangle \xrightarrow{\rho} \langle k_0, k_1, k_2 \rangle \longrightarrow 0,$$

where ρ sends $e_0 \mapsto k_0, \ldots, e_3 \mapsto k_0, \ldots, e_{11} \mapsto k_2$.

We compute the splitting homomorphism

$$\sigma : \langle k_0, k_1, k_2 \rangle \longrightarrow L(h_0, \ldots, h_8)^{\times} \cdot \langle e_0, \ldots, e_{11} \rangle.$$

Since we already have the generator $g_0 + g_3$ fixed by π^3, we let $x = e_0$ and define σ via

$$\sigma(k_0) := (1 + h_0 + h_0h_3 + h_0h_3h_6 + h_3h_6 + h_6)e_0 = e_0 + e_3 + e_6 + e_9 + \frac{e_0e_9}{e_3} + \frac{e_0e_9}{e_6} = g_0 + g_3.$$

Therefore, we have

$$L(\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t)) \cong L(h_0, \ldots, h_8, g_0 + g_3, g_1 + g_4, g_2 + g_5).$$

Therefore, we have a description of $L(\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t))$.

$$L(\mathbb{Z}[t]/\Phi_2(t)\Phi_6(t)\Phi_{18}(t)) \cong L(\gamma_2, \gamma_{6,0}, \gamma_{6,1}, \gamma_{18,0}, \gamma_{18,1}, \ldots, \gamma_{18,5}) \tag{9.11}$$

We combine this with (9.7)

$$L(Z[t]/(t^{18} - 1)) \cong L(\gamma_2, \gamma_{6,0}, \gamma_{6,1}, \gamma_{18,0}, \ldots, \gamma_{18,5}, \gamma_{9,0}, \ldots, \gamma_{9,5}, \gamma_{3,0}, \gamma_{3,1}, \gamma_1). \tag{9.12}$$

The following isomorphism is multiplication by $\Phi_9(t)$, that is,

$$\langle e_0, \ldots e_{11} \rangle \cong \mathbb{Z}[t]/(t^6 - 1)\Phi_{18}(t) \cong \Phi_9(t)\mathbb{Z}[t]/(t^{18} - 1).$$

Therefore,

$$e_0 = a_0a_3a_6,\ e_1 = a_1a_4a_7,\ \ldots,\ e_{11} = a_{11}a_{14}a_{17}$$

We note that a_0 and its π-conjugates are a permutation basis of $\mathbb{Z}G$. We write the permutation basis in terms of the γ_i; it suffices to express a_0 in terms of the γ_i. We see that

$$a_0 = \frac{c_0}{1+h_0},\ c_0 = \frac{\gamma_1}{(1+\gamma_{3,0}+\gamma_{3,0}\gamma_{3,1})(1+\gamma_{9,0}+\gamma_{9,0}\gamma_{9,3})}$$

and

$$h_0 = \left(\frac{g_3}{g_0}\right)\left(\frac{1+\gamma_{18,0}+\gamma_{18,3}}{1+\gamma_{18,3}+\pi(\gamma_{18,5})}\right),$$

where

$$\frac{g_3}{g_0} = \frac{\gamma_2(1+\gamma_{6,0}+\gamma_{6,0}\pi^2(\gamma_{6,0}))}{1+\gamma_{6,1}+\gamma_{6,1}\pi^2(\gamma_{6,1})}.$$

9.1 Computing the fixed field of I

We next compute the isomorphism

$$L(I) \cong L(J \oplus \overset{\oplus}{}_{d \mid 18, d \neq 18} \mathbb{Z}[\zeta_d]),$$

where $I = \langle 19, t-2 \rangle$. Using the same sequence as the previous section, we have

$$0 \longrightarrow I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \longrightarrow I/(t^{18}-1) \longrightarrow I/(t^9-1) \longrightarrow 0 \tag{9.13}$$

$$0 \longrightarrow I/\Phi_9(t) \longrightarrow I/(t^9-1) \longrightarrow I/(t^3-1) \longrightarrow 0 \tag{9.14}$$

$$0 \longrightarrow I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \longrightarrow I/(t^6-1)\Phi_{18}(t) \longrightarrow I/(t^3-1) \longrightarrow 0 \tag{9.15}$$

$$0 \longrightarrow I/\Phi_{18}(t) \longrightarrow I/(t^6-1)\Phi_{18}(t) \longrightarrow I/(t^6-1) \longrightarrow 0 \tag{9.16}$$

Again using the $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^{18}-1)$ and the multiplica-

tive group $\langle a_0, a_1, \ldots, a_{17}\rangle$ via $t^i \mapsto a_i$, (9.13) gives

$$0 \longrightarrow L((t^9-1)I/(t^{18}-1))^\times \longrightarrow L((t^9-1)I/(t^{18}-1))^\times \cdot I/(t^{18}-1) \xrightarrow{\rho} \langle b_0, b_1, \ldots, b_8\rangle \longrightarrow 0,$$

where ρ maps $a_{9i+j} \mapsto b_j$, for $i = 0, 1$ and $j = 0, \ldots, 8$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, \ldots, b_8\rangle \longrightarrow L((t^9-1)I/(t^{18}-1))^\times \cdot I/(t^{18}-1).$$

We have the following generating set for I.

$$I = \langle a_0^{19}, a_1^{19}, \ldots, a_{17}^{17}, \frac{a_1}{a_0^2}, \frac{a_2}{a_1^2}, \ldots, \frac{a_{17}}{a_{16}^2}, \frac{a_0}{a_{17}^2}\rangle$$

The image of this set under ρ is

$$\langle a_0^{19}, a_1^{19}, \ldots, a_{17}^{19}, \frac{a_1}{a_0^2}, \frac{a_2}{a_1^2}, \ldots, \frac{a_{17}}{a_{16}^2}, \frac{a_0}{a_{17}^2}\rangle \mapsto \langle b_0^{19}, \ldots, b_8^{19}, \frac{b_1}{b_0^2}, \ldots, \frac{b_8}{a_7^2}, \frac{b_0}{b_8^2}\rangle.$$

We find an element $x \in I/(t^{18}-1)$ such that $\rho(x) = b_0$ via

$$\begin{aligned} x &= \left(\frac{a_1}{a_0^2}\right)^{14}\left(\frac{a_2}{a_1^2}\right)^{7}\left(\frac{a_3}{a_2^2}\right)^{13}\left(\frac{a_4}{a_3^2}\right)^{16}\left(\frac{a_5}{a_4^2}\right)^{8}\left(\frac{a_6}{a_5^2}\right)^{4}\left(\frac{a_7}{a_6^2}\right)^{2}\left(\frac{a_8}{a_7^2}\right)\left(\frac{a_9}{a_8^2}\right)^{10} a_0^{19}a_2^{19}a_3^{19}a_8^{19} \\ &= \frac{a_9^{10}}{a_0^9}. \end{aligned}$$

Therefore, we have

$$\sigma(b_0) = (1 + \frac{\pi^9(x)}{x})x = \frac{a_9^{10}}{a_0^9} + \frac{a_0^{10}}{a_9^9},$$

which is fixed by π^9 as required. Therefore, Proposition 3.2 gives

$$L(I/(t^{18}-1)) \cong L(I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \oplus \langle \frac{a_9^{10}}{a_0^9} + \frac{a_0^{10}}{a_9^9}, \frac{a_{10}^{10}}{a_1^9} + \frac{a_1^{10}}{a_{10}^9}, \ldots, \frac{a_{17}^{10}}{a_8^9} + \frac{a_8^{10}}{a_{17}^9} \rangle) \quad (9.17)$$

We note that the last 9 generators are permuted cyclically by π; we denote these via

$$c_0 = \frac{a_9^{10}}{a_0^9} + \frac{a_0^{10}}{a_9^9}, \ \ldots, \ c_8 = \frac{a_{17}^{10}}{a_8^9} + \frac{a_8^{10}}{a_{17}^9}.$$

We use the result from the previous section, namely

$$L(c_0, \ldots, c_8) = L(\frac{c_3}{c_0}, \ldots, \frac{c_8}{c_5}, \frac{c_1 + c_4 + c_7}{c_0 + c_3 + c_6}, \frac{c_2 + c_5 + c_8}{c_1 + c_4 + c_7}, c_0 + c_1 + \cdots + c_8)$$

and define

$$\gamma_{9,0} = \frac{c_3}{c_0}, \ \ldots, \ \gamma_{9,5} = \frac{c_8}{c_5}$$

$$\gamma_{3,0} = \frac{c_1 + c_4 + c_7}{c_0 + c_3 + c_6}, \ \gamma_{3,1} = \frac{c_2 + c_5 + c_8}{c_1 + c_4 + c_7}, \ \gamma_1 = c_0 + c_1 + \cdots + c_8.$$

Combining this with (9.17) gives

$$L(I/(t^{18}-1)) \cong L(I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \oplus \langle \gamma_{9,0}, \ldots, \gamma_{9,5}, \gamma_{3,0}, \gamma_{3,1}, \gamma_1 \rangle) \quad (9.18)$$

From (9.16) we have

$$0 \longrightarrow I/\Phi_{18}(t) \longrightarrow I/(t^6-1)\Phi_{18}(t) \longrightarrow I/(t^6-1) \longrightarrow 0$$

Writing $\mathbb{Z}[t]/(t^6-1)\Phi_{18}(t)$ multiplicatively as $\langle e_0, e_1, \ldots, e_{11} \rangle$, and using the generator

$t^5 - t^4 + t^3 - t^2 - 1$ of the principal ideal $I/\Phi_{18}(t)$, we have

$$I/\Phi_{18}(t) \cong (t^6-1)I/(t^6-1)\Phi_{18}(t) = \langle \frac{e_0e_2e_4e_9e_{11}}{e_3e_5e_6e_8e_{10}}, \ldots, \frac{e_2e_4e_6}{e_0e_8e_{10}} \rangle.$$

We have the exact sequence

$$0 \longrightarrow L(\frac{e_0e_2e_4e_9e_{11}}{e_3e_5e_6e_8e_{10}}, \ldots, \frac{e_2e_4e_6}{e_0e_8e_{10}})^\times \longrightarrow L(\frac{e_0e_2e_4e_9e_{11}}{e_3e_5e_6e_8e_{10}}, \ldots, \frac{e_2e_4e_6}{e_0e_8e_{10}})^\times \cdot I/(t^6-1)\Phi_{18}(t)$$
$$\xrightarrow{\rho} \langle f_0, f_1, \ldots, f_5 \rangle \longrightarrow 0,$$

where ρ sends $e_{6i+j} \mapsto f_j$, for $i = 0, 1$ and $j = 0, \ldots, 5$.

We compute the splitting homomorphism

$$\sigma : \langle f_0, \ldots, f_5 \rangle \longrightarrow L(\frac{e_0e_2e_4e_9e_{11}}{e_3e_5e_6e_8e_{10}}, \ldots, \frac{e_2e_4e_6}{e_0e_8e_{10}})^\times \cdot I/(t^6-1)\Phi_{18}(t).$$

The image of the generating set for $I/(t^6-1)\Phi_{18}(t)$ under ρ is the following.

$$\langle e_0^{19}, e_1^{19}, \ldots, e_{17}^{19}, \frac{e_1}{e_0^2}, \frac{e_2}{e_1^2}, \ldots, \frac{e_{17}}{e_{16}^2}, \frac{e_0}{e_{17}^2} \rangle \mapsto \langle f_0^{19}, \ldots, f_5^{19}, \frac{f_1}{f_0^2}, \ldots, \frac{f_5}{f_4^2}, \frac{f_0}{f_5^2} \rangle.$$

We find an element $x \in I/(t^6-1)\Phi_{18}(t)$ such that $\rho(x) = f_0$ via

$$x = \left(\frac{e_1}{e_0^2}\right)\left(\frac{e_2}{e_1^2}\right)^{10}\left(\frac{e_3}{e_2^2}\right)^{5}\left(\frac{e_4}{e_3^2}\right)^{12}\left(\frac{e_5}{e_4^2}\right)^{6}\left(\frac{e_6}{e_5^2}\right)^{3} e_1^{19}a_3^{19} = \frac{a_9^{10}}{a_0^9} = \frac{e_6^3}{e_0^2}$$

We then have

$$\sigma(f_0) = \frac{e_6^3}{e_0^2} + \frac{e_0^3e_9^3}{e_3^3e_6^2} + \frac{e_0e_2^3}{e_9^2},$$

which is fixed by π^6 as required. Therefore, Proposition 3.2 gives

$$L(I/(t^6-1)\Phi_{18}(t)) \cong L(\frac{e_0e_2e_4e_9e_{11}}{e_3e_5e_6e_8e_{10}}, \ldots, \frac{e_2e_4e_6}{e_0e_8e_{10}}, \frac{e_6^3}{e_0^2} + \frac{e_0^3e_9^3}{e_3^3e_6^2} + \frac{e_0e_2^3}{e_9^2}, \ldots, \frac{e_{11}^3}{e_5^2} + \frac{e_2^3e_{11}}{e_8^3} + \frac{e_5^3e_7^3}{e_2^2e_{11}^2}). \quad (9.19)$$

We define

$$\gamma_{18,0} = \frac{e_0e_2e_4e_9e_{11}}{e_3e_5e_6e_8e_{10}},\ \gamma_{18,1} = \frac{e_0e_1e_5e_{10}}{e_4e_6e_7e_{11}},\ \ldots,\ \gamma_{18,5} = \frac{e_2e_4e_6}{e_0e_8e_{10}}.$$

Therefore, we have

$$L(I/(t^6-1)\Phi_{18}(t)) \cong L(\gamma_{18,0}, \gamma_{18,1}, \ldots, \gamma_{18,5}, \frac{e_6^3}{e_0^2} + \frac{e_0^3e_9^3}{e_3^3e_6^2} + \frac{e_0e_2^3}{e_9^2}, \ldots, \frac{e_{11}^3}{e_5^2} + \frac{e_2^3e_{11}}{e_8^3} + \frac{e_5^3e_7^3}{e_2^2e_{11}^2}). \quad (9.20)$$

We can see that the last 6 generators are permuted cyclically by π. We define

$$g_0 = \frac{e_6^3}{e_0^2} + \frac{e_0^3e_9^3}{e_3^3e_6^2} + \frac{e_0e_2^3}{e_9^2},\ g_1 = \frac{e_7^3}{e_1^2} + \frac{e_1^3e_{10}^3}{e_4^3e_7^2} + \frac{e_1e_3^3}{e_{10}^2},\ \ldots,\ g_5 = \frac{e_{11}^3}{e_5^2} + \frac{e_2^3e_{11}}{e_8^3} + \frac{e_5^3e_7^3}{e_2^2e_{11}^2}.$$

Using (5.13), we have

$$L(\mathbb{Z}[t]/(t^6-1)) \cong L(g_0+g_3, g_1+g_4, g_2+g_5, \gamma_2, \gamma_{6,0}, \gamma_{6,1}).$$

where

$$\gamma_2 = \frac{g_1g_2g_3 + g_0g_1g_5 + g_3g_4g_5}{g_0g_1g_2 + g_2g_3g_4 + g_0g_4g_5},\ \gamma_{6,0} = \frac{g_3g_4}{g_0g_1},\ \gamma_{6,1} = \frac{g_4g_5}{g_1g_2}.$$

We recall that g_0+g_3, g_1+g_4, and g_2+g_5 generate a module isomorphic to $\mathbb{Z}[t]/(t^3-1)$.

Combining this with (9.20) gives

$$L(I/(t^6-1)\Phi_{18}(t)) \cong L(g_0+g_3, g_1+g_4, g_2+g_5, \gamma_2, \gamma_{6,0}, \gamma_{6,1}, \gamma_{18,0}, \gamma_{18,1}, \ldots, \gamma_{18,5}). \quad (9.21)$$

We combine this with sequence (9.15).

$$0 \longrightarrow I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t) \longrightarrow I/(t^6-1)\Phi_{18}(t) \longrightarrow I/(t^3-1) \longrightarrow 0$$

In this sequence, we have descriptions of the fields corresponding to the middle and right components. We use these to find a description of $L(I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t))$.

We have

$$0 \longrightarrow L((t^3-1)I/(t^6-1)\Phi_{18}(t))^\times \longrightarrow L((t^3-1)I/(t^6-1)\Phi_{18}(t))^\times \cdot I/(t^6-1)\Phi_{18}(t)$$
$$\xrightarrow{\rho} \langle k_0, k_1, k_2\rangle \longrightarrow 0,$$

where ρ sends $e_0 \mapsto k_0, \ldots, e_3 \mapsto k_0, \ldots, e_{11} \mapsto k_2$. We compute the splitting homomorphism

$$\sigma : \langle k_0, k_1, k_2\rangle \longrightarrow L((t^3-1)I/(t^6-1)\Phi_{18}(t))^\times \cdot I/(t^6-1)\Phi_{18}(t)\rangle.$$

Since we already have the generator g_0+g_3 fixed by π^3, we let $x = \frac{e_6^3}{e_0^2}$ and define

$$\sigma(k_0) = (1 + \frac{\pi^3(x)}{x} + \cdots + \frac{\pi^3(x)}{x}\frac{\pi^6(x)}{\pi^3(x)}\cdots\frac{\pi^{15}(x)}{\pi^{12}(x)})x = \frac{e_6^3}{e_0^2} + \frac{e_9^3}{e_3^2} + \cdots + \frac{e_3^3e_5^3}{e_0^2e_9^2} = g_0+g_3.$$

Therefore, we have a description of $L(I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t))$.

$$L(I/\Phi_2(t)\Phi_6(t)\Phi_{18}(t)) \cong L(\gamma_2, \gamma_{6,0}, \gamma_{6,1}, \gamma_{18,0}, \gamma_{18,1}, \ldots, \gamma_{18,5}) \quad (9.22)$$

Combining this with (9.18) gives

$$L(I) \cong L(\gamma_2, \gamma_{6,0}, \gamma_{6,1}, \gamma_{18,0}, \ldots, \gamma_{18,5}, \gamma_{9,0}, \ldots, \gamma_{9,5}, \gamma_{3,0}, \gamma_{3,1}, \gamma_1). \tag{9.23}$$

The following isomorphism is multiplication by $\Phi_9(t)$, that is,

$$\langle e_0, \ldots e_{11} \rangle \cong \mathbb{Z}[t]/(t^6 - 1)\Phi_{18}(t) \cong \Phi_9(t)\mathbb{Z}[t]/(t^{18} - 1).$$

Therefore,

$$e_0 = a_0a_3a_6,\ e_1 = a_1a_4a_7,\ \ldots,\ e_{11} = a_{11}a_{14}a_{17}$$

The generator α of the permutation basis, which corresponds to a_0 from the previous section, can be expressed via $\alpha = \frac{c_0}{1+h_0}$, where

$$c_0 = \frac{\gamma_1}{(1 + \gamma_{3,0} + \gamma_{3,0}\gamma_{3,1})(1 + \gamma_{9,0} + \gamma_{9,0}\gamma_{9,3})}$$

$$h_0 = \frac{\gamma_2(1 + \gamma_{6,0} + \gamma_{6,0}\pi^2(\gamma_{6,0}))(1 + \gamma_{18,0} + \gamma_{18,3})}{(1 + \gamma_{6,1} + \gamma_{6,1}\pi^2(\gamma_{6,1}))(1 + \gamma_{18,3} + \pi(\gamma_{18,5}))}.$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$. We define the 18×18 matrix T whose (i, j)-th entry is $\zeta^{2^{i+j}}$ and compute the generators $u_0, \ldots, u_{17}$ as follows, where ζ denotes a primitive 19-th root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{17} \end{pmatrix} = T \cdot \begin{pmatrix} \beta \\ \pi(\beta) \\ \vdots \\ \pi^{17}(\beta) \end{pmatrix}$$

Therefore, we have $K(x_0, \ldots, x_{18})^\tau = K(y_0, u_0, u_1, \ldots, u_{17})$.

Chapter 10: The case $A = \mathbb{Z}/23\mathbb{Z}$

We next compute generators of the fixed field $K(x_0, \ldots, x_{22})^A$, where $A = \langle\tau\rangle$. The Galois group $G = \langle\pi\rangle$ of L/K has order 22 and we have $I = \langle 23, t-5\rangle \subseteq \mathbb{Z}G$ and $J = \langle 23, \zeta - 5\rangle = \langle -\zeta^8 + \zeta^7 - 1\rangle \subseteq \mathbb{Z}[\zeta]$, where ζ denotes a primitive 22-nd root of unity.

We first compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^{22}-1)) \cong L(\overset{\oplus}{}_{d \mid 22}\mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_{21}\rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_{21} \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action. We first compute the sequence of equivalence relations of $p - 1 = 22$; from (3.1.2) we have the following.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t) \longrightarrow \mathbb{Z}[t]/(t^{22}-1) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow 0 \tag{10.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0 \tag{10.2}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0 \tag{10.3}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/(t^{11}-1) \tag{10.4}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{11}(t) \longrightarrow \mathbb{Z}[t]/(t^{11}-1) \longrightarrow \mathbb{Z}[t]/(t-1) \longrightarrow 0 \tag{10.5}$$

Starting with (10.1), we have

$$\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t) \cong (t^2-1)\mathbb{Z}[t]/(t^{22}-1) = \langle \frac{a_2}{a_0}, \frac{a_3}{a_1}, \ldots, \frac{a_{21}}{a_{19}} \rangle.$$

We define

$$c_0 = \frac{a_2}{a_0},\ c_1 = \frac{a_3}{a_1},\ \ldots,\ c_{19} = \frac{a_{21}}{a_{19}}$$

Then we have the exact sequence

$$0 \longrightarrow L(c_0, \ldots, c_{19})^\times \longrightarrow L(c_0, \ldots, c_{19})^\times \cdot \langle a_0, \ldots, a_{21} \rangle \xrightarrow{\rho} \langle b_0, b_1 \rangle \longrightarrow 0,$$

where ρ maps $a_{2i+j} \mapsto b_j$, for $i = 0, \ldots, 10$ and $j = 0, 1$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1 \rangle \longrightarrow L(c_0, \ldots, c_{19})^\times \cdot \langle a_0, \ldots, a_{21} \rangle.$$

Letting $x = a_0$, we define σ via

$$\sigma(b_0) = a_0 + a_2 + \cdots + a_{20},$$

which is fixed by π^2 as required. Letting $d_0 = a_0 + a_2 + \cdots + a_{20}$ and $d_1 = a_1 + a_3 + \cdots + a_{21}$, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^{22}-1)) \cong L(a_0, a_1, \ldots, a_{21}) = L(c_0, \ldots, c_{19}, d_0, d_1).$$

We can see this explicitly since

$$a_0 = \frac{d_0}{1 + c_0 + c_0c_2 + \cdots + c_0 \cdots c_{18}}, \ \ldots, a_{19} = \frac{d_1}{1 + c_{19}^{-1} + c_{19}^{-1}c_{17}^{-1} + \cdots + c_{19}^{-1} \cdots c_1^{-1}} \tag{10.6}$$

Noting that the last two generators are swapped by π, using (4.1), we have

$$L(Z[t]/(t^{22} - 1)) \cong L(a_0, a_1, \ldots, a_{21}) = L(c_0, \ldots, c_{19}, \frac{d_1}{d_0}, d_0 + d_1). \tag{10.7}$$

We let $\gamma_2 = \frac{d_1}{d_0}$ and $\gamma_1 = d_0 + d_1$, which are inverted and fixed by π.

Next, we compute generators of $L(\mathbb{Z}[t]/(t^{22} - 1))$ that π acts on via Φ_{22} and Φ_{11}. From (10.4), we have a $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)$ and the multiplicative group $\langle e_0, e_1, \ldots, e_{20}\rangle$ via $t^i \mapsto e_i$. Therefore, we have

$$\mathbb{Z}[t]/\Phi_{22}(t) \cong (t^{11} - 1)\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) = \langle \frac{e_{11}}{e_0}, \frac{e_{12}}{e_1}, \ldots, \frac{e_{20}}{e_9}\rangle.$$

and

$$0 \longrightarrow L(\frac{e_{11}}{e_0}, \ldots, \frac{e_{20}}{e_9})^\times \longrightarrow L(\frac{e_{11}}{e_0}, \ldots, \frac{e_{20}}{e_9})^\times \cdot \langle e_0, \ldots, e_{20}\rangle \xrightarrow{\rho} \langle f_0, f_1, \ldots, f_{10}\rangle \longrightarrow 0,$$

where ρ maps $e_{11i+j} \mapsto f_j$, for $i = 0, 1$ and $j = 0, \ldots, 10$.

We define

$$\gamma_{22,0} = \frac{e_{11}}{e_0}, \ \gamma_{22,1} = \frac{e_{12}}{e_1}, \ \ldots, \ \gamma_{22,9} = \frac{e_{20}}{e_9}$$

and note that π acts on the $\gamma_{22,i}$ via $\Phi_{22}(t)$, that is

$$\pi(\gamma_{22,9}) = \gamma_{22,9}\gamma_{22,8}^{-1}\gamma_{22,7} \cdots \gamma_{22,0}^{-1}.$$

We compute the splitting homomorphism

$$\sigma : \langle f_0, \ldots, f_{10} \rangle \longrightarrow L(\frac{e_{11}}{e_0}, \ldots, \frac{e_{20}}{e_9})^{\times} \cdot \langle e_0, \ldots, e_{20} \rangle,$$

letting $x = e_0$ we define σ via

$$\sigma(f_0) = (1 + \frac{\pi^{11}(x)}{x})x = e_0 + e_{11}.$$

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(\gamma_{22,0}, \gamma_{22,1}, \ldots, \gamma_{22,9}, e_0 + e_{11}, e_1 + e_{12}, \ldots, e_9 + e_{20}, e_{10} + \frac{e_{20}e_{18}\cdots e_2 e_0}{e_{19}e_{17}\cdots e_3 e_1}). \quad (10.8)$$

We can see that the last 11 generators are permuted cyclically by π. Using these in sequence (10.5), we define

$$g_0 = e_0 + e_{11},\ g_1 = e_1 + e_{12}, \ldots,\ g_{10} = e_{10} + \frac{e_{20}e_{18}\cdots e_2 e_0}{e_{19}e_{17}\cdots e_3 e_1}.$$

We then have

$$\mathbb{Z}[t]/\Phi_{11}(t) \cong (t-1)\mathbb{Z}[t]/(t^{11} - 1) = \langle \frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{10}}{g_9} \rangle$$

and

$$0 \longrightarrow L(\frac{g_1}{g_0}, \ldots, \frac{g_{10}}{g_9})^{\times} \longrightarrow L(\frac{g_1}{g_0}, \ldots, \frac{g_{10}}{g_9})^{\times} \cdot \langle g_0, \ldots, g_{10} \rangle \xrightarrow{\rho} \langle \omega \rangle \longrightarrow 0,$$

where ρ sends the g_i to ω. We compute the splitting homomorphism

$$\sigma : \langle \omega \rangle \longrightarrow L(\frac{g_1}{g_0}, \ldots, \frac{g_{10}}{g_9})^{\times} \cdot \langle g_0, \ldots, g_{10} \rangle,$$

letting $x = g_0$ we define σ via

$$\sigma(\omega) = g_0 + g_1 + \cdots + g_{10}.$$

Therefore, we have

$$L(\mathbb{Z}[t]/(t^{11} - 1)) \cong L(g_0, \ldots, g_{10}) = L(\frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{10}}{g_9}, g_0 + g_1 + \cdots + g_{10}).$$

We define

$$\gamma_{11,0} = \frac{g_1}{g_0},\ \gamma_{11,1} = \frac{g_2}{g_1},\ \ldots \gamma_{11,8} = \frac{g_9}{g_8},\ \gamma_{11,9} = \frac{g_{10}}{g_9}.$$

We note that π acts on the $\gamma_{11,i}$ via $\Phi_{11}(t)$, that is

$$\pi : \gamma_{11,0} \mapsto \gamma_{11,1} \mapsto \cdots \mapsto \gamma_{11,9} \mapsto \gamma_{11,9}^{-1}\gamma_{11,8}^{-1} \cdots \gamma_{11,0}^{-1}.$$

We also note that the $\gamma_{11,i}$ satisfy

$$\gamma_{11,0} = \frac{e_1 + e_{12}}{e_0 + e_{11}} = \left(\frac{e_1}{e_0}\right)\left(\frac{1 + \gamma_{22,1}}{1 + \gamma_{22,0}}\right). \tag{10.9}$$

Combining this with (10.8) gives

$$L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(\gamma_{22,0}, \gamma_{22,1}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \gamma_{11,1}, \ldots, \gamma_{11,9}, g_0 + \cdots + g_{10}). \tag{10.10}$$

From (10.3), we had

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0$$

In this sequence, we have a description of the field corresponding to the middle component, and the right component is just the multiplicative group $\langle\omega\rangle$. We use these to find a description of $L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t))$.

Since $\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t) \cong (t-1)\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)$, we have

$$\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t) \cong \langle \frac{e_1}{e_0}, \frac{e_2}{e_1}, \ldots, \frac{e_{20}}{e_{19}} \rangle.$$

Defining

$$h_0 = \frac{e_1}{e_0},\ h_1 = \frac{e_2}{e_1},\ \ldots,\ h_{19} = \frac{e_{20}}{e_{19}},$$

we have

$$0 \longrightarrow L(h_0, \ldots, h_{19})^\times \longrightarrow L(h_0, \ldots, h_{19})^\times \cdot \langle e_0, \ldots, e_{20} \rangle \xrightarrow{\rho} \langle\omega\rangle \longrightarrow 0,$$

where ρ sends the e_i to ω.

We compute the splitting homomorphism $\sigma : \langle\omega\rangle \longrightarrow L(h_0, \ldots, h_{19})^\times \cdot \langle e_0, \ldots, e_{20} \rangle$. Since we already have the generator $g_0 + g_1 + \cdots + g_{10}$ fixed by π, we define $x = e_0$, and

we have

$$\sigma(\omega) := (1 + h_0 + h_0h_1 + \cdots + h_0 \cdots h_{19} + h_1h_3 \cdots h_{19})e_0 = g_0 + \cdots + g_{10}.$$

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(h_0, \ldots, h_{19}, e_0 + \cdots + \frac{e_{20}e_{18} \cdots e_2e_0}{e_{19}e_{17} \cdots e_3e_1}).$$

Combining this with (10.10) gives

$$L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(h_0, \ldots, h_{19}, e_0 + \cdots + \frac{e_{20}e_{18} \cdots e_2e_0}{e_{19}e_{17} \cdots e_3e_1}) \cong$$
$$L(\gamma_{22,0}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \gamma_{11,1}, \ldots, \gamma_{11,9}, e_0 + \cdots + \frac{e_{20}e_{18} \cdots e_2e_0}{e_{19}e_{17} \cdots e_3e_1}).$$

Therefore, we have a description of $L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t))$.

$$L(\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)) \cong L(\gamma_{22,0}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \gamma_{11,1}, \ldots, \gamma_{11,9}). \tag{10.11}$$

We can see $L(h_0, \ldots, h_{19}) = L(\gamma_{22,0}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \ldots, \gamma_{11,9})$ explicitly, since

$$\gamma_{22,0} = h_0h_1 \cdots h_{10}, \ \ldots, \gamma_{22,9} = h_9h_{10} \cdots h_{19},$$

$$\gamma_{11,0} = h_0\left(\frac{1 + \gamma_{22,1}}{1 + \gamma_{22,0}}\right), \ \ldots, \gamma_{11,9} = h_9\left(\frac{1 + \pi(\gamma_{22,9})}{1 + \gamma_{22,9}}\right),$$

and

$$h_0 = \gamma_{11,0}\left(\frac{1 + \gamma_{22,0}}{1 + \gamma_{22,1}}\right), \ \ldots, h_{19} = \pi^{10}(\gamma_{11,9})\left(\frac{1 + \pi^{10}(\gamma_{22,9})}{1 + \pi^{11}(\gamma_{22,9})}\right).$$

We note that the following isomorphism is multiplication by $\Phi_2(t) = t + 1$, that is,

$$\langle e_0, \ldots e_{20} \rangle \cong \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \cong (t+1)\mathbb{Z}[t]/(t^{22}-1).$$

Therefore, we have

$$e_0 = a_0a_1,\ e_1 = a_1a_2,\ \ldots,\ e_{20} = a_{20}a_{21}$$

We combine this with (10.7) to obtain

$$L(Z[t]/(t^{22}-1)) \cong L(\overset{\oplus}{}_{d \mid 22}\mathbb{Z}[t]/(\Phi_d(t))) \cong L(\gamma_{22,0}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \ldots, \gamma_{11,9}, \gamma_2, \gamma_1).$$

We note that a_0 generates the permutation basis, which we write in terms of the γ_i. From (11.9) we have

$$a_0 = \frac{\gamma_1}{(1+\gamma_2)(1 + h_0 + h_0\pi^2(h_0) + \cdots + h_0\pi^2(h_0)\cdots\pi^{18}(h_0))}. \tag{10.12}$$

and from (10.9) we have

$$h_0 = \frac{a_2}{a_0} = \frac{\gamma_{11,0}(1+\gamma_{22,0})}{1+\gamma_{22,1}} \tag{10.13}$$

10.1 Computing the fixed field of I

We next compute the isomorphism

$$L(I) \cong L(J \oplus \overset{\oplus}{}_{d \mid 22, d \neq 22}\mathbb{Z}[\zeta_d]),$$

where $I = \langle 23, t-5 \rangle$. From (3.1.2) we have the following.

$$0 \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t) \longrightarrow I/(t^{22}-1) \longrightarrow I/\Phi_2(t)\Phi_1(t) \longrightarrow 0 \tag{10.14}$$

$$0 \longrightarrow I/\Phi_2(t) \longrightarrow I/(t^2-1) \longrightarrow I/\Phi_1(t) \longrightarrow 0 \tag{10.15}$$

$$0 \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t) \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow I/\Phi_1(t) \longrightarrow 0 \tag{10.16}$$

$$0 \longrightarrow I/\Phi_{22}(t) \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow I/\Phi_{11}(t)\Phi_1(t) \longrightarrow 0 \tag{10.17}$$

$$0 \longrightarrow I/\Phi_{11}(t) \longrightarrow I/\Phi_{11}(t)\Phi_1(t) \longrightarrow I/\Phi_1(t) \longrightarrow 0 \tag{10.18}$$

Again using the $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^{22}-1)$ and the multiplicative group $\langle a_0, a_1, \ldots, a_{21} \rangle$ via $t^i \mapsto a_i$, (10.14) gives

$$0 \longrightarrow L((t^2-1)I/(t^{22}-1))^\times \longrightarrow L((t^2-1)I/(t^{22}-1))^\times \cdot I/(t^{22}-1) \xrightarrow{\rho} \langle b_0, b_1 \rangle \longrightarrow 0,$$

where ρ maps $a_{2i+j} \mapsto b_j$, for $i = 0, \ldots, 10$ and $j = 0, 1$.

We compute the splitting homomorphism $\sigma : \langle b_0, b_1 \rangle \longrightarrow L((t^2-1)I/(t^{22}-1))^\times \cdot I$. We have the following generating set for I.

$$I/(t^{22}-1) = \langle a_0^{23}, a_1^{23}, \ldots, a_{20}^{23}, \frac{a_1}{a_0^5}, \frac{a_2}{a_1^5}, \ldots, \frac{a_{21}}{a_{20}^5} \rangle$$

The image of this set under ρ is

$$\langle a_0^{23}, a_1^{23}, \ldots, a_{20}^{23}, \frac{a_1}{a_0^5}, \frac{a_2}{a_1^5} \ldots, \frac{a_{21}}{a_{20}^5} \rangle \mapsto \langle b_0^{23}, b_1^{23}, \ldots, b_0^{23}, \frac{b_1}{b_0^5}, \frac{b_0}{b_1^5}, \ldots, \frac{b_1}{b_0^5} \rangle$$

and therefore in order to find x with $\rho(x) = b_0$, we need to solve

$$x \cdot \begin{pmatrix} -5 & 1 \\ 1 & -5 \\ 23 & 0 \\ 0 & 23 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

The solution $x = (18, 22, 3, 4)$ yields

$$x = \left(\frac{a_1}{a_0^5}\right)^{18} \left(\frac{a_2}{a_1^5}\right)^{22} (a_0^{23})^3 (a_1^{23})^4 = \frac{a_2^{22}}{a_0^{21}}.$$

Therefore, we define σ via

$$\sigma(b_0) = (1 + \frac{\pi^2(x)}{x} + \frac{\pi^2(x)}{x}\frac{\pi^4(x)}{\pi^2(x)} + \cdots + \frac{\pi^2(x)}{x}\frac{\pi^4(x)}{\pi^2(x)} \cdots \frac{\pi^{20}(x)}{\pi^{18}(x)})x = \frac{a_2^{22}}{a_0^{21}} + \frac{a_4^{22}}{a_2^{21}} + \cdots + \frac{a_0^{22}}{a_{20}^{21}},$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(I) \cong L(I/\Phi_{22}(t)\Phi_{11}(t) \oplus \langle \frac{a_2^{22}}{a_0^{21}} + \frac{a_4^{22}}{a_2^{21}} + \cdots + \frac{a_0^{22}}{a_{20}^{21}}, \frac{a_3^{22}}{a_1^{21}} + \frac{a_5^{22}}{a_3^{21}} + \cdots + \frac{a_1^{22}}{a_{21}^{21}} \rangle)$$

Noting that the last two generators are swapped by π, using (4.1), we have

$$L(I) \cong L(I/\Phi_{22}(t)\Phi_{11}(t) \oplus \langle \frac{\frac{a_3^{22}}{a_1^{21}} + \frac{a_5^{22}}{a_3^{21}} + \cdots + \frac{a_1^{22}}{a_{21}^{21}}}{\frac{a_2^{22}}{a_0^{21}} + \frac{a_4^{22}}{a_2^{21}} + \cdots + \frac{a_0^{22}}{a_{20}^{21}}}, \frac{a_2^{22}}{a_0^{21}} + \frac{a_3^{22}}{a_1^{21}} + \cdots + \frac{a_1^{22}}{a_{21}^{21}} \rangle) \tag{10.19}$$

We label the last two generators γ_2 and γ_1.

$$\gamma_2 = \frac{\frac{a_3^{22}}{a_1^{21}} + \frac{a_5^{22}}{a_3^{21}} + \cdots + \frac{a_1^{22}}{a_{21}^{21}}}{\frac{a_2^{22}}{a_0^{21}} + \frac{a_4^{22}}{a_2^{21}} + \cdots + \frac{a_0^{22}}{a_{20}^{21}}}, \ \gamma_1 = \frac{a_2^{22}}{a_0^{21}} + \frac{a_3^{22}}{a_1^{21}} + \cdots + \frac{a_1^{22}}{a_{21}^{21}}$$

Next, we compute generators of $L(I)$ that π acts on via Φ_{22} and Φ_{11}. From (10.17) we have

$$0 \longrightarrow I/\Phi_{22}(t) \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow I/\Phi_{11}(t)\Phi_1(t) \longrightarrow 0.$$

We write $\mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)$ multiplicatively as $\langle e_0, e_1, \ldots, e_{20}\rangle$, via $t^i \mapsto e_i$. Using the fact that $I/\Phi_{22}(t)$ is principal and generated by $-t^8 + t^7 - 1$, we have

$$\begin{aligned} I/\Phi_{22}(t) &\cong (t^{11}-1)I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) = \langle -t^{19} + t^{18} - t^{11} + t^8 - t^7 + 1\rangle \\ &= \langle \frac{e_0e_8e_{18}}{e_7e_{11}e_{19}}, \frac{e_1e_9e_{19}}{e_8e_{12}e_{20}}, \ldots, \frac{e_5e_9e_{17}}{e_6e_{16}e_{20}}\rangle \end{aligned}$$

and

$$0 \longrightarrow L(\frac{e_0e_8e_{18}}{e_7e_{11}e_{19}}, \ldots, \frac{e_5e_9e_{17}}{e_6e_{16}e_{20}})^\times \longrightarrow L(\frac{e_0e_8e_{18}}{e_7e_{11}e_{19}}, \ldots, \frac{e_5e_9e_{17}}{e_6e_{16}e_{20}})^\times \cdot I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \xrightarrow{\rho}$$
$$\langle f_0, \ldots, f_{10}\rangle \longrightarrow 0,$$

where ρ maps $e_{11i+j} \mapsto f_j$, for $i = 0, 1$ and $j = 0, \ldots, 10$.

We compute the splitting homomorphism

$$\sigma : \langle f_0, f_1, \ldots, f_{10}\rangle \longrightarrow L(\frac{e_0e_8e_{18}}{e_7e_{11}e_{19}}, \ldots, \frac{e_5e_9e_{17}}{e_6e_{16}e_{20}})^\times \cdot I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t).$$

We have the following generating set for $I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)$.

$$I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) = \langle e_0^{23}, e_1^{23}, \ldots, e_{20}^{23}, \frac{e_1}{e_0^5}, \frac{e_{20}}{e_{19}^5}\rangle$$

The image of this set under ρ is the following.

$$\langle e_0^{23}, e_1^{23}, \ldots, e_{20}^{23}, \frac{e_1}{e_0^5}, \frac{e_{20}}{e_{19}^5}\rangle \mapsto \langle f_0^{23}, f_1^{23}, \ldots, f_{10}^{23}, \frac{f_1}{f_0^5}, \ldots, \frac{f_{10}}{f_9^5}, \frac{f_0}{f_{10}^5}\rangle$$

and therefore to find an x with $\rho(x) = f_0$ we need to solve

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \\ x_{16} \\ x_{17} \\ x_{18} \\ x_{19} \\ x_{20} \\ x_{21} \end{pmatrix}^{\intercal} \cdot \begin{pmatrix} -5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -5 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -5 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -5 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -5 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -5 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -5 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -5 \\ 23 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 23 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 23 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 23 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}^{\intercal}$$

The solution

$$x = (16, 17, 8, 20, 4, 10, 2, 5, 1, 14, 12, 3, 3, 1, 4, 0, 2, 0, 1, 0, 3, 2).$$

yields

$$x = \left(\frac{e_1}{e_0^5}\right)^{16} \left(\frac{e_2}{e_1^5}\right)^{17} \left(\frac{e_3}{e_2^5}\right)^{8} \left(\frac{e_4}{e_3^5}\right)^{20} \left(\frac{e_5}{e_4^5}\right)^{4} \left(\frac{e_6}{e_5^5}\right)^{10} \left(\frac{e_7}{e_6^5}\right)^{2} \left(\frac{e_8}{e_7^5}\right)^{5} \left(\frac{e_9}{e_8^5}\right) \left(\frac{e_{10}}{e_9^5}\right)^{14} \left(\frac{e_{11}}{e_{10}^5}\right)^{12} (e_0^{23})^3 (e_1^{23})^3 (e_2^{23}) (e_3^{23})^4 (e_5^{23})^2 (e_7^{23}) (e_9^{23})^2 (e_{10}^{23})^2 = \frac{e_{11}^{12}}{e_0^{11}}.$$

Therefore, we have

$$\sigma(f_0) = (1 + \frac{\pi^{11}(x)}{x})x = \frac{e_{11}^{12}}{e_0^{11}} \left(1 + \frac{e_0^{23}}{e_{11}^{23}}\right) = \frac{e_{11}^{12}}{e_0^{11}} + \frac{e_0^{12}}{e_{11}^{11}},$$

and

$$L(I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(\frac{e_0e_8e_{18}}{e_7e_{11}e_{19}}, \frac{e_1e_9e_{19}}{e_8e_{12}e_{20}}, \ldots, \frac{e_5e_9e_{17}}{e_6e_{16}e_{20}}, \frac{e_{11}^{12}}{e_0^{11}} + \frac{e_0^{12}}{e_{11}^{11}},$$
$$\frac{e_{12}^{12}}{e_1^{11}} + \frac{e_1^{12}}{e_{12}^{11}}, \ldots, \frac{e_{20}^{12}}{e_9^{11}} + \frac{e_9^{12}}{e_{20}^{11}}, \frac{e_{20}^{12}e_{18}^{12}\cdots e_{12}^{12}e_{10}e_8^{12}\cdots e_0^{12}}{e_{19}^{12}e_{17}^{12}\cdots e_1^{12}} + \frac{e_{19}^{11}e_{17}^{11}\cdots e_1^{11}e_{10}}{e_{20}^{11}e_{18}^{11}\cdots e_{12}^{11}e_8^{11}\cdots e_0^{11}}).$$

We define

$$\gamma_{22,0} = \frac{e_0e_8e_{18}}{e_7e_{11}e_{19}},\ \gamma_{22,1} = \frac{e_1e_9e_{19}}{e_8e_{12}e_{20}},\ \ldots,\ \gamma_{22,9} = \frac{e_5e_9e_{17}}{e_6e_{16}e_{20}}$$

and note that π acts on the $\gamma_{22,i}$ via $\Phi_{22}(t)$. Therefore we have

$$L(I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(\gamma_{22,0}, \gamma_{22,1}, \ldots, \gamma_{22,9}, \frac{e_{11}^{12}}{e_0^{11}} + \frac{e_0^{12}}{e_{11}^{11}},$$
$$\frac{e_{12}^{12}}{e_1^{11}} + \frac{e_1^{12}}{e_{12}^{11}}, \ldots, \frac{e_{20}^{12}}{e_9^{11}} + \frac{e_9^{12}}{e_{20}^{11}}, \frac{e_{20}^{12}e_{18}^{12}\cdots e_{12}^{12}e_{10}e_8^{12}\cdots e_0^{12}}{e_{19}^{12}e_{17}^{12}\cdots e_1^{12}} + \frac{e_{19}^{11}e_{17}^{11}\cdots e_1^{11}e_{10}}{e_{20}^{11}e_{18}^{11}\cdots e_{12}^{11}e_8^{11}\cdots e_0^{11}}) \quad (10.20)$$

We can see that the last 11 generators are permuted cyclically by π. We use these in sequence (10.18), in which we had

$$0 \longrightarrow I/\Phi_{11}(t) \longrightarrow I/\Phi_{11}(t)\Phi_1(t) \longrightarrow I/\Phi_1(t) \longrightarrow 0.$$

We define

$$g_0 = \frac{e_{11}^{12}}{e_0^{11}} + \frac{e_0^{12}}{e_{11}^{11}},\ g_1 = \frac{e_{12}^{12}}{e_1^{11}} + \frac{e_1^{12}}{e_{12}^{11}}, \ldots,\ g_9 = \frac{e_{20}^{12}}{e_9^{11}} + \frac{e_9^{12}}{e_{20}^{11}},$$

$$g_{10} = \frac{e_{20}^{12}e_{18}^{12}\cdots e_{12}^{12}e_{10}e_8^{12}\cdots e_0^{12}}{e_{19}^{12}e_{17}^{12}\cdots e_1^{12}} + \frac{e_{19}^{11}e_{17}^{11}\cdots e_1^{11}e_{10}}{e_{20}^{11}e_{18}^{11}\cdots e_{12}^{11}e_8^{11}\cdots e_0^{11}}$$

and we use the result from the previous section, namely

$$L(g_0, g_1, \ldots, g_{10}) = L(\frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{10}}{g_9}, g_0 + g_1 + \cdots + g_{10}).$$

Combining this with (10.20) gives

$$L(I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t)) \cong L(\gamma_{22,0}, \gamma_{22,1}, \ldots, \gamma_{22,9}, \frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{10}}{g_9}, g_0 + g_1 + \cdots + g_{10}) \tag{10.21}$$

We define

$$\gamma_{11,0} = \frac{g_1}{g_0},\ \gamma_{11,1} = \frac{g_2}{g_1},\ \ldots \gamma_{11,8} = \frac{g_9}{g_8},\ \gamma_{11,9} = \frac{g_{10}}{g_9}$$

From (10.16) we had

$$0 \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t) \longrightarrow I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \longrightarrow I/\Phi_1(t) \longrightarrow 0$$

In this sequence, we have a description of the field corresponding to the middle component, and the right component is just the multiplicative group $\langle\omega\rangle$. We use these to find a description of $L(I/\Phi_{22}(t)\Phi_{11}(t))$.

We compute the splitting homomorphism

$$\sigma : \langle\omega\rangle \longrightarrow L(\langle t-1\rangle I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t))^{\times} \cdot I/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t).$$

Since we already have the generator $g_0 + g_1 + \cdots + g_{10}$ fixed by π, we define $x = \frac{e_0^{12}}{e_{11}^{11}}$ which

gives

$$\sigma(\omega) := x + \pi(x) + \cdots + \pi^{21}(x) = \frac{e_{11}^{12}}{e_0^{11}} + \frac{e_0^{12}}{e_{11}^{11}} + \cdots + \frac{e_{20}^{12}e_{18}^{12}\cdots e_{12}^{12}e_{10}e_8^{12}\cdots e_0^{12}}{e_{19}^{12}e_{17}^{12}\cdots e_1^{12}} + \frac{e_{19}^{11}e_{17}^{11}\cdots e_1^{11}e_{10}}{e_{20}^{11}e_{18}^{11}\cdots e_{12}^{11}e_8^{11}\cdots e_0^{11}} = g_0 + g_1 + \cdots + g_{10}$$

Therefore, we have a description of $L(I/\Phi_{22}(t)\Phi_{11}(t))$.

$$L(I/\Phi_{22}(t)\Phi_{11}(t)) \cong L(\gamma_{22,0}, \gamma_{22,1}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \ldots, \gamma_{11,9}) \tag{10.22}$$

We note that the following isomorphism is multiplication by $\Phi_2(t) = t + 1$, that is,

$$\langle e_0, \ldots e_{20} \rangle \cong \mathbb{Z}[t]/\Phi_{22}(t)\Phi_{11}(t)\Phi_1(t) \cong (t+1)\mathbb{Z}[t]/(t^{22} - 1).$$

Therefore, we have

$$e_0 = a_0a_1,\ e_1 = a_1a_2,\ \ldots,\ e_{20} = a_{20}a_{21}$$

We combine this with (10.19) to obtain

$$L(I/(t^{22}-1)) \cong L(\overset{\oplus}{_{d\,|\,22}} I/(\Phi_d(t))) \cong L(\gamma_{22,0}, \ldots, \gamma_{22,9}, \gamma_{11,0}, \gamma_{11,1}, \ldots, \gamma_{11,9}, \gamma_2, \gamma_1).$$

We use the results from the previous section to compute the generator of the permutation basis from the γ_i. From (10.13), we compute the element α that corresponded to $h_0 = \frac{a_2}{a_0}$ from the previous section

$$\alpha = \frac{\gamma_{11,0}(1 + \gamma_{22,0})}{1 + \gamma_{22,1}}.$$

From (10.12) we write the generator β of the permutation basis

$$\beta = \frac{\gamma_1}{(1+\gamma_2)(1+\alpha+\alpha\pi^2(\alpha)+\cdots+\alpha\pi^2(\alpha)\cdots\pi^{18}(\alpha))}.$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$. We define the 22×22 matrix T whose (i,j)-th entry is $\zeta^{5^{i+j}}$ and compute the generators $u_0,\ldots,u_{21}$ as follows, where ζ denotes a primitive 23-rd root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{21} \end{pmatrix} = T \cdot \begin{pmatrix} \beta \\ \pi(\beta) \\ \vdots \\ \pi^{21}(\beta) \end{pmatrix}$$

Therefore, we have $K(x_0,\ldots,x_{22})^\tau = K(y_0,u_0,u_1,\ldots,u_{21})$.

Chapter 11: The case $A = \mathbb{Z}/47\mathbb{Z}$

Swan [12] showed that the ideal $I/\Phi_{46}(t)$ in $\mathbb{Z}[t]/\Phi_{46}(t)$ is not principal, and therefore the field extension $K(x_0, x_1, \ldots, x_{46})^\tau/K$ is not a rational one. We use the fact that the class number of the real subfield $\mathbb{Q}(\zeta_{23}+\zeta_{23}^{-1})$ is 1 to construct a principal ideal in $\mathbb{Z}[\zeta_{46}]$ above 47 of norm 47^2. We then use this ideal to construct a rational field extension of degree 47^2 below $K(x_0, x_1, \ldots, x_{46})$, and degree 47 below the fixed field $K(x_0, x_1, \ldots, x_{46})^\tau$.

First, we compute the isomorphism

$$L(\mathbb{Z}G) = L(\mathbb{Z}[t]/(t^{46}-1)) \cong L(\,{}_{d\,|\,46}^{\oplus}\mathbb{Z}[\zeta_d]).$$

We write $\mathbb{Z}G$ multiplicatively as $\langle a_0, \ldots, a_{45}\rangle$, where π acts via $a_0 \mapsto \cdots \mapsto a_{45} \mapsto a_0$. The a_i are a renumbering of the y_i to reflect the Galois action. We compute the sequence of equivalence relations of $p-1 = 46$; from (3.1.2) we have the following.

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t) \longrightarrow \mathbb{Z}[t]/(t^{46}-1) \longrightarrow \mathbb{Z}[t]/\Phi_2(t)\Phi_1(t) \longrightarrow 0 \tag{11.1}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_2(t) \longrightarrow \mathbb{Z}[t]/(t^2-1) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0 \tag{11.2}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0 \tag{11.3}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_{23}(t)\Phi_1(t) \longrightarrow 0 \tag{11.4}$$

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{23}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{23}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0 \tag{11.5}$$

Starting with (11.1), we have

$$\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t) \cong (t^2-1)\mathbb{Z}[t]/(t^{46}-1) = \langle \frac{a_2}{a_0}, \frac{a_3}{a_1}, \ldots, \frac{a_{45}}{a_{43}} \rangle.$$

We define

$$c_0 = \frac{a_2}{a_0},\ c_1 = \frac{a_3}{a_1},\ \ldots,\ c_{43} = \frac{a_{45}}{a_{43}}$$

and write $\mathbb{Z}[t]/(t^2-1)$ multiplicatively as $\langle b_0, b_1 \rangle$. Then we have

$$0 \longrightarrow L(c_0, \ldots, c_{43})^\times \longrightarrow L(c_0, \ldots, c_{43})^\times \cdot \langle a_0, \ldots, a_{45} \rangle \xrightarrow{\rho} \langle b_0, b_1 \rangle \longrightarrow 0,$$

where ρ maps $a_{2i+j} \mapsto b_j$, for $i = 0, \ldots, 22$ and $j = 0, 1$.

We compute the splitting homomorphism $\sigma : \langle b_0, b_1 \rangle \longrightarrow L(c_0, \ldots, c_{43})^\times \cdot \langle a_0, \ldots, a_{45} \rangle$, letting $x = a_0$ we define σ via $\sigma(b_0) = a_0 + a_2 + \cdots + a_{44}$, which is fixed by π^2 as required. Letting $d_0 = a_0 + a_2 + \cdots + a_{44}$ and $d_1 = a_1 + a_3 + \cdots + a_{45}$, we have

$$L(\mathbb{Z}[t]/(t^{46}-1)) \cong L(a_0, a_1, \ldots, a_{45}) = L(c_0, \ldots, c_{43}, d_0, d_1).$$

We can see this explicitly since

$$a_0 = \frac{d_0}{1 + c_0 + c_0c_2 + \cdots + c_0c_2\cdots c_{42}},\ \ldots, a_{45} = \frac{d_1}{1 + c_{43}^{-1} + c_{43}^{-1}c_{41}^{-1} + \cdots + c_{43}^{-1}c_{41}^{-1}\cdots c_1^{-1}} \tag{11.6}$$

Noting that d_0 and d_1 are swapped by π, using (4.1), we have

$$L(\mathbb{Z}[t]/(t^{46}-1)) \cong L(a_0, a_1, \ldots, a_{45}) = L(c_0, \ldots, c_{43}, \frac{d_1}{d_0}, d_0 + d_1). \tag{11.7}$$

We label the last two generators γ_2 and γ_1 and note that π fixes γ_1 and inverts γ_2 .

$$\gamma_2 = \frac{d_1}{d_0},\ \gamma_1 = d_0 + d_1$$

Next, we find generators of $L(\mathbb{Z}[t]/(t^{46}-1))$ that π acts on via Φ_{46} and Φ_{23}. From (11.4), we had

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_{23}(t)\Phi_1(t) \longrightarrow 0.$$

We have a $\mathbb{Z}G$-module isomorphism $\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \cong \langle e_0, e_1, \ldots, e_{44}\rangle$ via $t^i \mapsto e_i$. Therefore, we have

$$\mathbb{Z}[t]/\Phi_{46}(t) \cong (t^{23}-1)\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) = \langle \frac{e_{23}}{e_0}, \frac{e_{24}}{e_1}, \ldots, \frac{e_{44}}{e_{21}}\rangle$$

and we have the exact sequence

$$0 \longrightarrow L(\frac{e_{23}}{e_0}, \ldots, \frac{e_{44}}{e_{21}})^\times \longrightarrow L(\frac{e_{23}}{e_0}, \ldots, \frac{e_{44}}{e_{21}})^\times \cdot \langle e_0, \ldots, e_{44}\rangle \xrightarrow{\rho} \langle f_0, f_1, \ldots, f_{22}\rangle \longrightarrow 0,$$

where ρ maps $e_{22i+j} \mapsto f_j$, for $i = 0, 1$ and $j = 0, \ldots, 11$.

We compute the splitting homomorphism

$$\sigma : \langle f_0, \ldots, f_{22}\rangle \longrightarrow L(\frac{e_{23}}{e_0}, \ldots, \frac{e_{44}}{e_{21}})^\times \cdot \langle e_0, \ldots, e_{44}\rangle.$$

Letting $x = e_0$, we define σ via

$$\sigma(f_0) = (1 + \frac{\pi^{23}(x)}{x})x = e_0 + e_{23}.$$

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(e_0, e_1, \ldots, e_{44}) = L(\frac{e_{23}}{e_0}, \ldots, \frac{e_{44}}{e_{21}}, e_0 + e_{23}, e_1 + e_{24}, \ldots, e_{21} + e_{44}, e_{22} + \frac{e_{44}e_{42}\cdots e_2e_0}{e_{43}e_{41}\cdots e_3e_1}).$$

We define

$$\gamma_{46,0} = \frac{e_{23}}{e_0},\ \gamma_{46,1} = \frac{e_{24}}{e_1},\ \ldots,\ \gamma_{46,21} = \frac{e_{44}}{e_{21}}$$

and we note that π acts on the $\gamma_{46,i}$ via $\Phi_{46}(t)$, that is

$$\pi(\gamma_{46,21}) = \gamma_{46,21}\gamma_{46,20}^{-1}\gamma_{46,19}\cdots\gamma_{46,0}^{-1}.$$

Therefore we have

$$L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(e_0, e_1, \ldots, e_{44}) = L(\gamma_{46,0}, \gamma_{46,1}, \ldots, \gamma_{46,21}, e_0 + e_{23}, e_1 + e_{24}, \ldots, e_{21} + e_{44}, e_{22} + \frac{e_{44}e_{42}\cdots e_2e_0}{e_{43}e_{41}\cdots e_3e_1}). \quad (11.8)$$

We can see that the last 23 generators are permuted cyclically by π. We use these in sequence (11.5), where we had

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{23}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{23}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0.$$

Defining

$$g_0 = e_0 + e_{23},\ g_1 = e_1 + e_{24}, \ldots,\ g_{22} = e_{22} + \frac{e_{44}e_{42}\cdots e_2e_0}{e_{43}e_{41}\cdots e_3e_1},$$

we have

$$\mathbb{Z}[t]/\Phi_{23}(t) \cong (t-1)\mathbb{Z}[t]/(t^{23}-1) = \langle \frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{22}}{g_{21}} \rangle$$

and

$$0 \longrightarrow L(\frac{g_1}{g_0}, \ldots, \frac{g_{22}}{g_{21}})^{\times} \longrightarrow L(\frac{g_1}{g_0}, \ldots, \frac{g_{22}}{g_{21}})^{\times} \cdot \langle g_0, \ldots, g_{22} \rangle \xrightarrow{\rho} \langle \omega \rangle \longrightarrow 0,$$

where ρ sends the g_i to ω. We compute the splitting homomorphism

$$\sigma : \langle \omega \rangle \longrightarrow L(\frac{g_1}{g_0}, \ldots, \frac{g_{22}}{g_{21}})^{\times} \cdot \langle g_0, \ldots, g_{22} \rangle,$$

letting $x = g_0$ we define σ via

$$\sigma(\omega) = g_0 + g_1 + \cdots + g_{22}.$$

Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/(t^{23}-1)) \cong L(g_0, \ldots, g_{22}) = L(\frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{22}}{g_{21}}, g_0 + g_1 + \cdots + g_{22}).$$

We define

$$\gamma_{23,0} = \frac{g_1}{g_0},\ \gamma_{23,1} = \frac{g_2}{g_1},\ \ldots \gamma_{23,20} = \frac{g_{21}}{g_{20}},\ \gamma_{23,21} = \frac{g_{22}}{g_{21}}$$

We note that π acts on the $\gamma_{23,i}$ via $\Phi_{23}(t)$, that is

$$\pi : \gamma_{23,0} \mapsto \gamma_{23,1} \mapsto \cdots \mapsto \gamma_{23,21} \mapsto = \gamma_{23,21}^{-1}\gamma_{23,20}^{-1} \cdots \gamma_{23,0}^{-1}$$

We also note that the $\gamma_{23,i}$ satisfy

$$\gamma_{23,0} = \frac{e_1 + e_{24}}{e_0 + e_{23}} = \left(\frac{e_1}{e_0}\right)\left(\frac{1+\gamma_{46,1}}{1+\gamma_{46,0}}\right). \tag{11.9}$$

Combining this with (11.8) gives

$$L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(e_0, e_1, \ldots, e_{44}) = L(\gamma_{46,0}, \gamma_{46,1}, \ldots, \gamma_{46,21},$$
$$\gamma_{23,0}, \gamma_{23,1}, \ldots, \gamma_{23,21}, g_0 + \cdots + g_{22}). \tag{11.10}$$

From (11.3) we had

$$0 \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t) \longrightarrow \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow \mathbb{Z}[t]/\Phi_1(t) \longrightarrow 0$$

In this sequence, we have a description of the field corresponding to the middle component, and the right component is $\langle\omega\rangle$. We use these to find a description of $L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t))$.

Since $\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t) \cong (t-1)\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)$, we have

$$\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t) \cong \langle\frac{e_1}{e_0}, \frac{e_2}{e_1}, \ldots, \frac{e_{44}}{e_{43}}\rangle.$$

Letting

$$h_0 = \frac{e_1}{e_0},\ h_1 = \frac{e_2}{e_1},\ \ldots,\ h_{43} = \frac{e_{44}}{e_{43}},$$

we then have

$$0 \longrightarrow L(h_0, \ldots, h_{43})^\times \longrightarrow L(h_0, \ldots, h_{43})^\times \cdot \langle e_0, \ldots, e_{44}\rangle \xrightarrow{\rho} \langle\omega\rangle \longrightarrow 0,$$

where ρ sends the e_i to ω.

We compute the splitting homomorphism

$$\sigma : \langle \omega \rangle \longrightarrow L(h_0, \ldots, h_{43})^{\times} \cdot \langle e_0, \ldots, e_{44} \rangle.$$

Since we already have the generator $g_0 + g_1 + \cdots + g_{22}$ that is fixed by π, we let $x = e_0$ and define

$$\sigma(\omega) = (1 + h_0 + h_0h_1 + \cdots + h_0 \cdots h_{43} + h_1h_3 \cdots h_{41}h_{43})e_0 = g_0 + \cdots + g_{22},$$

which is fixed by π as required. Therefore, Proposition 3.2 gives

$$L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(h_0, \ldots, h_{43}, e_0 + \cdots + \frac{e_{44}e_{42} \cdots e_2e_0}{e_{43}e_{41} \cdots e_3e_1}).$$

Combining this with (11.10) gives

$$L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(h_0, \ldots, h_{19}, e_0 + \cdots + \frac{e_{44}e_{42} \cdots e_2e_0}{e_{43}e_{41} \cdots e_3e_1}) \cong$$
$$L(\gamma_{46,0}, \ldots, \gamma_{46,21}, \gamma_{23,0}, \gamma_{23,1}, \ldots, \gamma_{23,21}, e_0 + \cdots + \frac{e_{44}e_{42} \cdots e_2e_0}{e_{43}e_{41} \cdots e_3e_1}).$$

Therefore, we have a description of $L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t))$.

$$L(\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)) \cong L(\gamma_{46,0}, \ldots, \gamma_{46,21}, \gamma_{23,0}, \gamma_{23,1}, \ldots, \gamma_{23,21}). \tag{11.11}$$

We can see $L(h_0, \ldots, h_{43}) = L(\gamma_{46,0}, \ldots, \gamma_{46,21}, \gamma_{23,0}, \gamma_{23,1}, \ldots, \gamma_{23,21})$ explicitly, since

$$\gamma_{46,0} = h_0h_1 \cdots h_{22}, \ \ldots, \gamma_{46,21} = h_{21}h_{22} \cdots h_{43},$$

$$\gamma_{23,0} = h_0\left(\frac{1+\gamma_{46,1}}{1+\gamma_{46,0}}\right),\ \ldots, \gamma_{23,21} = h_{21}\left(\frac{1+\pi(\gamma_{46,21})}{1+\gamma_{46,21}}\right),$$

and

$$h_0 = \gamma_{23,0}\left(\frac{1+\gamma_{46,0}}{1+\gamma_{46,1}}\right),\ \ldots, h_{43} = \pi^{22}(\gamma_{23,21})\left(\frac{1+\pi^{22}(\gamma_{46,21})}{1+\pi^{23}(\gamma_{46,21})}\right).$$

Noting that the isomorphism $\langle e_0, \ldots e_{44}\rangle \cong \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)$ is multiplication by $\Phi_2(t) = t+1$, we see that

$$e_0 = a_0a_1,\ e_1 = a_1a_2,\ \ldots,\ e_{44} = a_{44}a_{45}.$$

Combining this with (11.7), we obtain

$$L(\mathbb{Z}[t]/(t^{46}-1)) \cong L(\overset{\oplus}{_{d\mid 46}}\mathbb{Z}[t]/(\Phi_d(t))) \cong L(\gamma_{46,0},\ldots,\gamma_{46,21},\gamma_{23,0},\ldots,\gamma_{23,21},\gamma_2,\gamma_1).$$

Since a_0 generates a permutation basis, we express it in terms of the γ_i. From (11.6) we have

$$a_0 = \frac{\gamma_1}{(1+\gamma_2)(1+\frac{a_2}{a_0}+\frac{a_2}{a_0}\pi^2(\frac{a_2}{a_0})+\cdots+\frac{a_2}{a_0}\pi^2(\frac{a_2}{a_0})\cdots\pi^{42}(\frac{a_2}{a_0}))}. \tag{11.12}$$

And from (11.9) we have

$$\frac{a_2}{a_0} = \gamma_{23,0}\left(\frac{1+\gamma_{46,0}}{1+\gamma_{46,1}}\right). \tag{11.13}$$

11.1 Computing the fixed field of I

We know that the field extension $K(x_0, x_1, \ldots, x_{46})^\tau/K$ is not rational. However, since the class number of the real subfield $\mathbb{Q}(\zeta_{23}+\zeta_{23}^{-1})$ is 1 we have the following principal

ideal J_0 in $\mathbb{Z}[\zeta_{46}] = \mathbb{Z}[\zeta_{23}]$

$$J_0 = \langle 47, \zeta_{46} - 5\rangle \cdot \langle 47, \zeta_{46} - 19\rangle = \langle \zeta_{46}^{17} + \zeta_{46}^{13} - \zeta_{46}^{10} - \zeta_{46}^{6} - 1\rangle.$$

We see that J_0 lies above 47 and has norm $47^2 = 2209$.

We let I_0 be the ideal $\langle 47, t-5\rangle \cdot \langle 47, t-19\rangle \subseteq \mathbb{Z}[t]/(t^{46}-1)$. We see that

$$I_0 = \langle 47^2, 47(t-5), 47(t-19), t^2 - 24t + 95\rangle = \langle 47, t^2 - 24t + 95\rangle,$$

since $3 \cdot 47^2 - 470(t-5) + 470(t-19) = 47$, and therefore I_0 has index 47^2 in $\mathbb{Z}G$.

By the same argument as in (3.1), for any proper divisor $m \mid 46$, we have $F_m(I_0) \cong \mathbb{Z}[\zeta_m]$, and $F_{46}(I_0) = J_0$. We also note that [11, Proposition 7.1] implies I_0 is a permutation-projective $\mathbb{Z}G$ module. Therefore, we can use Lenstra's techniques to construct a rational field extension of degree 47 below the fixed field $K(x_0, x_1, \ldots, x_{46})^\tau$.

From (3.1.2) we again have the following.

$$0 \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t) \longrightarrow I_0/(t^{46}-1) \longrightarrow I_0/(t^2-1) \longrightarrow 0 \tag{11.14}$$

$$0 \longrightarrow I_0/\Phi_2(t) \longrightarrow I_0/(t^2-1) \longrightarrow I_0/\Phi_1(t) \longrightarrow 0 \tag{11.15}$$

$$0 \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t) \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow I_0/\Phi_1(t) \longrightarrow 0 \tag{11.16}$$

$$0 \longrightarrow I_0/\Phi_{46}(t) \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow I_0/\Phi_{23}(t)\Phi_1(t) \longrightarrow 0 \tag{11.17}$$

$$0 \longrightarrow I_0/\Phi_{23}(t) \longrightarrow I_0/\Phi_{23}(t)\Phi_1(t) \longrightarrow I_0/\Phi_1(t) \longrightarrow 0 \tag{11.18}$$

Again using the $\mathbb{Z}G$-module isomorphism between $\mathbb{Z}[t]/(t^{46}-1)$ and the multiplica-

tive group $\langle a_0, a_1, \ldots, a_{45}\rangle$, (11.14) gives

$$0 \longrightarrow L((t^2-1)I_0/(t^{46}-1))^\times \longrightarrow L((t^2-1)I_0/(t^{46}-1))^\times \cdot I_0/(t^{46}-1) \xrightarrow{\rho} \langle b_0, b_1\rangle \longrightarrow 0,$$

where ρ maps $a_{2i+j} \mapsto b_j$, for $i = 0, \ldots, 22$ and $j = 0, 1$.

We compute the splitting homomorphism

$$\sigma : \langle b_0, b_1\rangle \longrightarrow L((t^2-1)I_0/(t^{46}-1))^\times \cdot I_0/(t^{46}-1).$$

Since $I_0/(t^2-1) = \langle 47, -24t+96\rangle$, we must solve the following to find an x with $\rho(x) = b_0$.

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \cdot \begin{pmatrix} 96 & -24 \\ -24 & 96 \\ 47 & 0 \\ 0 & 47 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

The solution $x = (35, 44, -49, -72)$ yields $x = \frac{a_0^{1022}a_3^{44}}{a_1^{44}a_2^{1021}}$. Therefore, we have

$$\sigma(b_0) = \frac{a_0^{1022}a_3^{44}}{a_1^{44}a_2^{1021}} + \frac{a_2^{1022}a_5^{44}}{a_3^{44}a_4^{1021}} + \cdots + \frac{a_{44}^{1022}a_1^{44}}{a_{45}^{44}a_0^{1021}},$$

which is fixed by π^2 as required. Therefore, Proposition 3.2 gives

$$L(I_0) \cong L(I_0/\Phi_{22}(t)\Phi_{11}(t) \oplus \langle \frac{a_0^{1022}a_3^{44}}{a_1^{44}a_2^{1021}} + \frac{a_2^{1022}a_5^{44}}{a_3^{44}a_4^{1021}} + \cdots + \frac{a_{44}^{1022}a_1^{44}}{a_{45}^{44}a_0^{1021}}, \\ \frac{a_1^{1022}a_4^{44}}{a_2^{44}a_3^{1021}} + \frac{a_3^{1022}a_6^{44}}{a_4^{44}a_5^{1021}} + \cdots + \frac{a_{45}^{1022}a_2^{44}}{a_0^{44}a_1^{1021}}\rangle).$$

Noting that the last two generators are swapped by π, using (4.1), we define

$$\gamma_2 = \frac{\frac{a_1^{1022}a_4^{44}}{a_2^{44}a_3^{1021}} + \frac{a_3^{1022}a_6^{44}}{a_4^{44}a_5^{1021}} + \cdots + \frac{a_{45}^{1022}a_2^{44}}{a_0^{44}a_1^{1021}}}{\frac{a_0^{1022}a_3^{44}}{a_1^{44}a_2^{1021}} + \frac{a_2^{1022}a_5^{44}}{a_3^{44}a_4^{1021}} + \cdots + \frac{a_{44}^{1022}a_1^{44}}{a_{45}^{44}a_0^{1021}}}, \ \gamma_1 = \frac{a_0^{1022}a_3^{44}}{a_1^{44}a_2^{1021}} + \frac{a_1^{1022}a_4^{44}}{a_2^{44}a_3^{1021}} + \cdots + \frac{a_{45}^{1022}a_2^{44}}{a_0^{44}a_1^{1021}}.$$

We then have

$$L(I_0) \cong L(I_0/\Phi_{46}(t)\Phi_{23}(t) \oplus \langle \gamma_1, \gamma_2 \rangle) \tag{11.19}$$

From (11.17), we have

$$0 \longrightarrow I_0/\Phi_{46}(t) \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow I_0/(t^{23}-1) \longrightarrow 0$$

We write $\mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)$ multiplicatively as $\langle e_0, e_1, \ldots, e_{44} \rangle$ via $t^i \mapsto e_i$. Since $I_0/\Phi_{46}(t) = \langle t^{17} + t^{13} - t^{10} - t^6 - 1 \rangle$ is principal, we have

$$I_0/\Phi_{46}(t) \cong (t^{23}-1)I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) = \langle \frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}, \ldots, \pi^{21}\left(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}\right) \rangle$$

and we have the exact sequence

$$0 \longrightarrow L(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}, \ldots, \pi^{21}\left(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}\right))^{\times} \longrightarrow L(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}, \ldots,$$
$$\pi^{21}\left(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}\right))^{\times} \cdot I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \xrightarrow{\rho} \langle f_0, \ldots, f_{22} \rangle \longrightarrow 0,$$

where ρ maps $e_{22i+j} \mapsto f_j$, for $i = 0, 1$ and $j = 0, \ldots, 11$.

We compute the splitting homomorphism

$$\sigma : \langle f_0, \ldots, f_{22} \rangle \longrightarrow L(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}, \ldots, \pi^{21}\left(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}\right))^{\times} \cdot I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t).$$

Since we have $I_0 = \langle 47, t^2 - 24t + 95 \rangle$, we see that

$$x = (t^2-24t+95)(24+12t+29t^2+26t^3+31t^4+13t^5+46t^6+10t^7+6t^8+40t^9+14t^{10}+14t^{11}+$$
$$40t^{12} + 6t^{13} + 10t^{14} + 46t^{15} + 13t^{16} + 31t^{17} + 26t^{18} + 29t^{19} + 12t^{20} + 24t^{21})+$$
$$47(-49 - 12t - 53t^2 - 38t^3 - 50t^4 - 11t^5 - 87t^6 + 3t^7 - 8t^8 - 78t^9 - 8t^{10} - 22t^{11} - 74t^{12}+$$
$$8t^{13} - 18t^{14} - 88t^{15} - 3t^{16} - 57t^{17} - 37t^{18} - 46t^{19} - 10t^{20} - 43t^{21} + 12t^{22}) = 24t^{23} - 23$$

or written multiplicatively,

$$x = \frac{e_{23}^{24}}{e_0^{23}}.$$

We see that $\rho(x) = f_0$, and we define σ via

$$\sigma(f_0) = (1 + \frac{\pi^{23}(x)}{x})x = \frac{e_{23}^{24}}{e_0^{23}} + \frac{e_0^{24}}{e_{23}^{23}},$$

which is fixed by π^{23} as required. We define

$$\gamma_{46,0} = \frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}, \ \ldots, \ \gamma_{46,21} = \pi^{21}\left(\frac{e_0e_6e_{10}e_{36}e_{40}}{e_{13}e_{17}e_{23}e_{29}e_{33}}\right)$$

Proposition 3.2 then gives

$$L(I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(\gamma_{46,0}, \ldots, \gamma_{46,21}, \frac{e_{23}^{24}}{e_0^{23}} + \frac{e_0^{24}}{e_{23}^{23}}, \frac{e_{24}^{24}}{e_1^{23}} + \frac{e_1^{24}}{e_{24}^{23}}, \ldots, \pi^{22}\left(\frac{e_{23}^{24}}{e_0^{23}} + \frac{e_0^{24}}{e_{23}^{23}}\right)) \tag{11.20}$$

We can see that the last 23 generators are permuted cyclically by π. We use these

in sequence (11.18), where we had

$$0 \longrightarrow I_0/\Phi_{23}(t) \longrightarrow I_0/\Phi_{23}(t)\Phi_1(t) \longrightarrow I_0/(t-1) \longrightarrow 0$$

We define

$$g_0 = \frac{e_{23}^{24}}{e_0^{23}} + \frac{e_0^{24}}{e_{23}^{23}},\ g_1 = \frac{e_{24}^{24}}{e_1^{23}} + \frac{e_1^{24}}{e_{24}^{23}}, \ldots,\ g_{21} = \frac{e_{44}^{24}}{e_{21}^{23}} + \frac{e_{21}^{24}}{e_{44}^{23}},$$

$$g_{22} = \frac{e_0^{24}e_2^{24}\cdots e_{44}^{24}}{e_1^{24}e_3^{24}\cdots e_{43}^{24}} + \frac{e_1^{23}e_3^{23}\cdots e_{21}^{23}e_{22}e_{23}^{23}\cdots e_{43}^{23}}{e_0^{23}e_2^{23}\cdots e_{20}^{23}e_{24}^{23}e_{26}^{23}\cdots e_{44}^{23}}$$

We use the result from the previous section, namely

$$L(g_0, \ldots, g_{22}) = L(\frac{g_1}{g_0}, \frac{g_2}{g_1}, \ldots, \frac{g_{22}}{g_{21}}, g_0 + g_1 + \cdots + g_{22}).$$

We define

$$\gamma_{23,0} = \frac{g_1}{g_0},\ \gamma_{23,1} = \frac{g_2}{g_1},\ \ldots \gamma_{23,20} = \frac{g_{21}}{g_{20}},\ \gamma_{23,21} = \frac{g_{22}}{g_{21}},$$

which π acts on via $\Phi_{23}(t)$. Combining this with (11.20) gives

$$L(I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t)) \cong L(\gamma_{46,0}, \gamma_{46,1}, \ldots, \gamma_{46,21}, \gamma_{23,0}, \gamma_{23,1}, \ldots, \gamma_{23,21}, g_0 + \cdots + g_{22}).$$

From (11.16) we had

$$0 \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t) \longrightarrow I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \longrightarrow I_0/(t-1) \longrightarrow 0$$

In this sequence, we have a description of the field corresponding to the middle component, and the right component is $\langle\omega\rangle$. We use these to find a description of $L(I_0/\Phi_{46}(t)\Phi_{23}(t))$.

We have the exact sequence

$$0 \longrightarrow L((t-1)I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t))^\times \longrightarrow L((t-1)I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t))^\times \cdot$$
$$I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \xrightarrow{\rho} \langle\omega\rangle \longrightarrow 0,$$

where ρ sends the e_i to ω. We compute the splitting homomorphism

$$\sigma : \langle\omega\rangle \longrightarrow L((t-1)I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t))^\times \cdot I_0/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t).$$

Since we already have the generator $g_0 + g_1 + \cdots + g_{22}$ that is fixed by π, we let $x = g_0$ and define

$$\sigma(\omega) = g_0 + \cdots + g_{22}.$$

Therefore, we have a description of $L(I_0/\Phi_{46}(t)\Phi_{23}(t))$

$$L(I_0/\Phi_{46}(t)\Phi_{23}(t)) \cong L(\gamma_{46,0}, \ldots, \gamma_{46,21}, \gamma_{23,0}, \gamma_{23,1}, \ldots, \gamma_{23,21}). \tag{11.21}$$

Noting that the following isomorphism is multiplication by $\Phi_2(t) = t + 1$, that is,

$$\langle e_0, \ldots e_{44}\rangle \cong \mathbb{Z}[t]/\Phi_{46}(t)\Phi_{23}(t)\Phi_1(t) \cong (t+1)\mathbb{Z}[t]/(t^{46}-1),$$

we then have

$$e_0 = a_0a_1,\ e_1 = a_1a_2,\ \ldots,\ e_{44} = a_{44}a_{45}$$

We combine this with (11.19) to obtain

$$L(I_0) \cong L(\gamma_{46,0}, \ldots, \gamma_{46,21}, \gamma_{23,0}, \ldots, \gamma_{23,21}, \gamma_2, \gamma_1). \tag{11.22}$$

Now we can write the generator of the permutation basis from the previous section in terms of the γ_i. From (11.13), we compute the element α that corresponded to $\frac{a_2}{a_0} = \frac{e_1}{e_0}$ from the previous section.

$$\alpha = \gamma_{23,0}\left(\frac{1+\gamma_{46,0}}{1+\gamma_{46,1}}\right)$$

Finally, from (11.12) we write the generator β of the permutation basis in terms of α, γ_1 and γ_2.

$$\beta = \frac{\gamma_1}{(1+\gamma_2)(1+\alpha+\alpha\pi^2(\alpha)+\cdots+\alpha\pi^2(\alpha)\cdots\pi^{42}(\alpha))}.$$

We use Masuda's method (1.2.1) to compute generators of the fixed field $L(I)^\pi$. We define the 46×46 matrix T whose (i,j)-th entry is $\zeta^{5^{i+j}}$ and compute the generators $u_0,\ldots,u_{45}$ as follows, where ζ denotes a primitive 47-th root of unity.

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{45} \end{pmatrix} = T \cdot \begin{pmatrix} \beta \\ \pi(\beta) \\ \vdots \\ \pi^{45}(\beta) \end{pmatrix}$$

Therefore, we have generators of $L(y_0,I_0)^\pi = K(y_0,u_0,u_1,\ldots,u_{45})$, which is a degree 47 subfield of $K(x_0,\ldots,x_{46})^\tau$. That is, we have shown that $\mathrm{Irr}(\mathbb{Q},\mathbb{Z}/47\mathbb{Z}) \leq 47$. Similarly, $\mathrm{Irr}(\mathbb{Q},\mathbb{Z}/p\mathbb{Z}) \leq p$ for $p = 59, 83, 107$, and 163, since the real cyclotomic fields of conductors 29, 41, 53, and 81 have class number 1 [13]. Under the generalized Riemann hypothesis, this extends to $p = 251$, since the 125-th real cyclotomic field has class number 1. The use of GRH could be eliminated if a calculation finds the principal generator of the relevant ideal.

Chapter A: Lagrange Interpolation Sage Code

A.1 The $p = 13$ Case

```
sage: K.<z> = CyclotomicField(12)
sage: R.<t> = PolynomialRing(K)
sage: for i in [0..3]:
....:   k = (t-1)^i*(t^2 - t - 2)
....:   for a0 in [-1,1]:
....:     for a1 in [-1,1]:
....:       for a2 in [1,-1,z^2,-z^2,z^4,-z^4]:
....:         for a3 in [1,-1,z^3,-z^3]:
....:           for a4 in [1,-1,z^2,-z^2,z^4,-z^4]:
....:             pts = [(1,a0), (-1,a1), (z^2,a2),
(z^(10),a2.conjugate()), (z^3,a3), (z^9,a3.conjugate()),
(z^4,a3), (z^8,a3.conjugate()), (z,k(z)), (z^(11),
k(z).conjugate()), (z^5,k(z^5)), (z^7,k(z^5).conjugate())]
....:             f = R.lagrange_polynomial(pts); print f;
....:
-1/6*t^11 - t^10 + 1/6*t^9 - 1/6*t^8 + 1/3*t^7 + 1/2*t^6 +
1/6*t^5 + 1/3*t^4 - 1/6*t^3 - 1/2*t^2 - 1/3*t - 1/6
-1/6*t^11 - t^10 + 1/6*t^9 - 1/6*t^8 + 1/3*t^7 + 1/2*t^6 +
1/6*t^5 + 1/3*t^4 - 1/6*t^3 - 1/2*t^2 - 1/3*t - 1/6
-1/6*t^11 - t^10 + 1/6*t^9 - 1/6*t^8 + 1/3*t^7 + 1/2*t^6 +
1/6*t^5 + 1/3*t^4 - 1/6*t^3 - 1/2*t^2 - 1/3*t - 1/6
-1/6*t^11 - t^10 + 1/6*t^9 - 1/6*t^8 + 1/3*t^7 + 1/2*t^6 +
1/6*t^5 + 1/3*t^4 - 1/6*t^3 - 1/2*t^2 - 1/3*t - 1/6
-1/6*t^11 - t^10 + 1/6*t^9 - 1/6*t^8 + 1/3*t^7 + 1/2*t^6 +
1/6*t^5 + 1/3*t^4 - 1/6*t^3 - 1/2*t^2 - 1/3*t - 1/6
-1/6*t^11 - t^10 + 1/6*t^9 - 1/6*t^8 + 1/3*t^7 + 1/2*t^6 +
1/6*t^5 + 1/3*t^4 - 1/6*t^3 - 1/2*t^2 - 1/3*t - 1/6
-1/2*t^10 - 1/6*t^9 - 1/3*t^8 + 1/2*t^7 + 1/2*t^6 +
1/3*t^5 + 1/6*t^4 - 1/2*t^3 - 1/6*t - 5/6
-1/2*t^10 - 1/6*t^9 - 1/3*t^8 + 1/2*t^7 + 1/2*t^6 +
1/3*t^5 + 1/6*t^4 - 1/2*t^3 - 1/6*t - 5/6
-1/2*t^10 - 1/6*t^9 - 1/3*t^8 + 1/2*t^7 + 1/2*t^6 +
1/3*t^5 + 1/6*t^4 - 1/2*t^3 - 1/6*t - 5/6
-1/2*t^10 - 1/6*t^9 - 1/3*t^8 + 1/2*t^7 + 1/2*t^6 +
1/3*t^5 + 1/6*t^4 - 1/2*t^3 - 1/6*t - 5/6
-1/2*t^10 - 1/6*t^9 - 1/3*t^8 + 1/2*t^7 + 1/2*t^6 +
1/3*t^5 + 1/6*t^4 - 1/2*t^3 - 1/6*t - 5/6
-1/2*t^10 - 1/6*t^9 - 1/3*t^8 + 1/2*t^7 + 1/2*t^6 +
1/3*t^5 + 1/6*t^4 - 1/2*t^3 - 1/6*t - 5/6
(1/12*z^3 - 1/6*z - 1/4)*t^11 + (-1/12*z^3 + 1/6*z - 3/4)*t^10 +
1/6*t^9 + (1/12*z^3 - 1/6*z - 1/4)*t^8 + (-1/12*z^3 + 1/6*z +
1/4)*t^7 + 1/2*t^6 + (1/12*z^3 - 1/6*z + 5/12)*t^5 + (-1/12*z^3 +
1/6*z + 1/4)*t^4 - 1/2*t^3 + (1/12*z^3 - 1/6*z - 1/4)*t^2 +
(-1/12*z^3 + 1/6*z - 1/12)*t - 1/2
```

⋮

A.2 The $p = 17$ Case

```
sage: K.<z> = CyclotomicField(16)
sage: R.<t> = PolynomialRing(K)
sage: Q.<t> = ZZ[t]
sage: u3 = (z^3-1)/(z-1)
sage: u5 = (z^5-1)/(z-1)
sage: u7 = (z^7-1)/(z-1)
sage: v = (z^6-1)/(z^2-1)
sage: h = K.hom([z^3])
sage: cosets_U16 = []
sage: for i in [0..3]:
....:   for j in [0..3]:
....:     for k in [0..3]:
....:       cosets_U16.append(u3^i*u5^j*u7^k)
....:
sage: cosets_U8 = []
sage: for i in [0..15]:
....:   for j in [0..7]:
....:     cosets_U8.append(z^i*v^j)
....:
sage: for a0 in [-1,1]:
....:   for a1 in [-1,1]:
....:     for a2 in cosets_U16:
....:       g = a2*(t^5 + t^4 - 1)
....:       for a3 in cosets_U8:
....:         for a4 in [1,-1,z^4,-z^4]:
....:           pts = [(-1,a0), (1,a1), (z,g(z)), (h(z),h(g(z))),
(h(h(z)),h(h(g(z)))), (h(h(h(z))),h(h(h(g(z))))), (z.conjugate(),
g(z).conjugate()), (h(z.conjugate()),h(g(z).conjugate())),
(h(h(z.conjugate())),h(h(g(z).conjugate()))),
(h(h(h(z.conjugate()))),h(h(h(g(z).conjugate())))), (z^2,a3),
(h(z^2),h(a3)), (z^(14),a3.conjugate()), (h(z^(14)),
h(a3.conjugate())), (z^4,a4), (z^(12),h(a4))]
....:           f = R.lagrange_polynomial(pts)
....:           if f in Q:
....:             print f;
....:
```

A.3 The $p = 19$ Case

```
sage: K.<z> = CyclotomicField(18)
sage: R.<t> = PolynomialRing(K)
sage: Q.<t> = ZZ[t]
sage: u2 = -z + 1
sage: u4 = -z^3 + z^2 - z + 1
sage: h = K.hom([z^5])
sage:
sage: cosets_U18 = []
sage: for i in [0..2]:
....:       for j in [0..2]:
....:         cosets_U18.append(u2^i*u4^j)
....:
sage: cosets_U9 = []
sage: for i in [0..2]:
....:       for j in [0..20]:
....:         cosets_U9.append(u2^i*u4^j)
....:
sage: for a0 in cosets_U18:
....:   g = a0*(t^5 - t^4 + t^3 - t^2 - 1)
....:   for a1 in cosets_U9:
....:     for a2 in [0..17]:
....:       k = a1*z^a2
....:       for a3 in [1,-1,z^3,-z^3,z^6,-z^6]:
....:         for a4 in [1,-1,z^3,-z^3,z^6,-z^6]:
....:           for a5 in [-1,1]:
....:             for a6 in [-1,1]:
....:               pts = [(z,g(z)), (h(z),h(g(z))), (h(h(z)),
h(h(g(z)))), (h(h(h(z))),h(h(h(g(z))))), (h(h(h(h(z)))),
h(h(h(h(g(z)))))), (h(h(h(h(h(z))))),h(h(h(h(h(g(z)))))),
(z^2,k), (h(z^2),h(k)), (h(h(z^2)),h(h(k))), (h(h(h(z^2))),
h(h(h(k)))), (h(h(h(h(z^2)))),h(h(h(h(k))))), (h(h(h(h(h(z^2))))),
h(h(h(h(h(k))))), (z^3,a3), (h(z^3),h(a3)), (z^6,a4),
(h(z^6),h(a4)), (-1,a5), (1,a6)]
....:               f = R.lagrange_polynomial(pts)
....:               if f in Q:
....:                 print f;
```

Bibliography

[1] H. Bass. The Dirichlet unit theorem, induced characters, and whitehead groups of finite groups. *Topology*, 4(4):391–410, 1966.

[2] E. Fischer. Die isomorphie der invariantenkörper der endlichen abelschen gruppen lineaerer transformatioen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1915:77–80, 1915.

[3] A. Hoshi. On Noether's problem for cyclic groups of prime order. *arXiv preprint arXiv:1402.3678*, 2014.

[4] C. U. Jensen, A. Ledet, and N. Yui. *Generic polynomials: constructive aspects of the inverse Galois problem*, volume 45. Cambridge University Press, 2002.

[5] H. Lenstra. Rational functions invariant under a finite abelian group. *Inventiones Mathematicae*, 25(3):299–325, 1974.

[6] J. Leshin. On the degree of irrationality in Noethers problem. Available at `http://www.math.brown.edu/~jleshin/Noether_Irr.pdf`.

[7] K. Masuda. On a problem of Chevalley. *Nagoya Mathematical Journal*, 8:59–63, 1955.

[8] K. Masuda. Application of the theory of the group of classes of projective modules to the existence problem of independent parameters of invariant. *Journal of the Mathematical Society of Japan*, 20(1-2):223–232, 1968.

[9] S. Sehgal. Units in integral group rings, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 69, 1993.

[10] E. Shizuo, T. Miyata, et al. Invariants of finite abelian groups. *Journal of the Mathematical Society of Japan*, 25(1):7–26, 1973.

[11] R. G. Swan. Induced representations and projective modules. *The Annals of Mathematics*, 71(3):552–578, 1960.

[12] R. G. Swan. Invariant rational functions and a problem of Steenrod. *Inventiones Mathematicae*, 7(2):148–158, 1969.

[13] F. van der Linden. Class number computations of real abelian number fields. *Mathematics of Computation*, 39(160):693–707, 1982.

[14] V. E. Voskresenskii. On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field \mathbbfq(x_1,,x_n). *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 34(2):366–375, 1970.

[15] L. C. Washington. *Introduction to cyclotomic fields*, volume 83. Springer, 1997.