Parametrizing extensions with fixed Galois group

Fabian Gundlach

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the Department of
Mathematics
Adviser: Manjul Bhargava

June 2019

Abstract

We study the problem of parametrizing Galois extensions of fields with a fixed Galois group G. Similar problems have recently received much attention, as they are often a useful first step to finding the asymptotic number of such Galois extensions with bounded invariants. For example, Davenport and Heilbronn used a parametrization due to Levi of rings of rank three to count cubic field extensions of $\mathbb{Q}$. Bhargava discovered and then used parametrizations of rings of ranks four and five to count quartic and quintic field extensions of $\mathbb{Q}$. The approach taken by Levi and Bhargava can roughly be summarized as follows: Choose a basis of the field or ring extension R under consideration, and then write down the coefficients in the multiplication table of R with respect to this basis. To keep the multiplication table simple, one needs to choose a suitable basis of R, which has previously been accomplished in special cases using ad-hoc methods. In this thesis, we explain how the representation theory of G provides a convenient choice of basis in general.

This recovers many of the known parametrizations. We study cyclic groups $G = \mathbb{Z}/n\mathbb{Z}$ in some detail and for example obtain a new parametrization for the cyclic group of order five. We also obtain a new parametrization for the quaternion group $G = \{\pm 1, \pm i, \pm j, \pm k\}$. This allows us to count quaternionic extensions of $\mathbb{Q}$ by conductor.

Acknowledgements

First and foremost, I am deeply grateful to my advisor Manjul Bhargava for his enthusiastic support and insight. I would also like to thank my fantastic parents, who have introduced me to the wonders of mathematics and selflessly supported me in all aspects of my life. This work would not have been possible without everyone who discussed mathematics with me and/or at times distracted me from it. I've been lucky to have had interesting mathematical conversations with Levent Alpoge, Amitesh Datta, Evan O'Dorney, Dan Fess, Kiran Kedlaya, Shilin Lai, Sophie Morel, Junho Peter Whang, Melanie Matchett Wood, Ziquan Zhuang, and others. I am also grateful to my wonderful brother Manuel and my amazing friends, who have made the past five years a great time. In particular, I would like to mention Amina Abdurrahman, Eric Chen, Amitesh Datta, Daniel Kriz, Shilin Lai, Nikita Lvov, Thomas Massoni, Akash Sengupta, Antoine Song, Daniel Stern, Ziquan Zhuang, and Jonathan Zung. The Department of Mathematics at Princeton has provided the perfect environment for the creation of this thesis.

Contents

Chapter 1

Introduction

Fix some finite group G and some field K. The goal of this thesis is to parametrize *G-extensions of K*: K-algebras R together with a left action of G that makes K isomorphic to the group ring $K[G]$ as a left $K[G]$-module. The motivating and main examples of G-extensions of K are Galois extensions L of K with Galois group G: By the Normal Basis Theorem, the field extension $L|K$ has a basis of the form $(g\alpha)_{g\in G}$ with $\alpha \in L$. Then, the K-linear map $K[G] \to L$ sending g to $g\alpha$ is an isomorphism of left $K[G]$-modules.

By a *parametrization* of G-extensions, we mean (for the purpose of this thesis) an explicit bijection

$$\{G\text{-extension } R \text{ of } K\} \longleftrightarrow \mathcal{G}(K)\backslash X(K),$$

where the right-hand side denotes the set of orbits of an appropriate algebraic group $\mathcal{G}(K)$ acting on a variety $X(K)$. The left-hand side is understood modulo isomorphism. Often, it will be convenient to only consider *nondegenerate* G-extensions (extensions with nonzero discriminant). Invariants of the G-extension R should correspond naturally to invariants of the group action. See for example [11] for an introduction to parametrizations of field extensions.

Traditionally, this problem has been approached using *Galois cohomology*: First, observe that nondegenerate G-extensions of K are in bijection with continuous group homomorphisms

$$\mathrm{Gal}(K^{\mathrm{sep}}|K) \longrightarrow G$$

from the absolute Galois group of K to G, up to conjugation by elements of G. (The G-extension is essentially the field fixed by the homomorphism's kernel.) It then follows from a short computation (see for example [33, section 5]) that it suffices to find an algebraic group $\mathcal{G}$ acting transitively (over the separable closure K^{sep}) on a variety X with a point $x \in X(K)$ satisfying the following properties: $H^1(K, \mathcal{G}) = 1$ and $G \cong \mathrm{Stab}_{\mathcal{G}(K^{\mathrm{sep}})}(x) \subseteq \mathcal{G}(K)$ (the stabilizer of $x \in X(K)$ is isomorphic to G and all its points are defined over K).

The most famous example of this approach is *Kummer theory*: if G is the cyclic group of order n and K contains n distinct n-th roots of unity (in particular, $\mathrm{char}(K) \nmid n$), we can let $\mathcal{G} = \mathbb{G}_m$ and $X = \mathbb{G}_m$ be the multiplicative group, with the action given by $g.x = g^n x$. Hilbert's Theorem 90 says that $H^1(K, \mathbb{G}_m) = 1$. The stabilizer of any number $x \in X(K) = K^\times$ is the (cyclic) group of n-th roots of unity. It is isomorphic to G, and contained in $\mathcal{G}(K) = K^\times$. Therefore, nondegenerate G-extensions of K are in bijection with elements of $K^{\times n}\backslash K^\times$.

Later, the theory and classification of prehomogeneous vector spaces have led to several other useful examples of parametrizations: A *prehomogeneous vector space* is a representation V of a group $\mathcal{G}$ possessing a dense orbit X. Sato and Kimura [26] completely classified *irreducible* prehomogeneous vector spaces where $\mathcal{G}$ is a reductive complex Lie group. Wright and Yukie [33] then realized that some of those representations (lifted to a field K of appropriate characteristic) satisfy exactly the

requirements specified above (for some finite group G): For example, nondegenerate S_3-extensions of K are in bijection with orbits of $\mathrm{GL}_2(K)$ acting on $X \subset V = \mathrm{Sym}^3(K^2)$ (via $g.f = \frac{1}{\det(g)} f \circ g$).[1] Nondegenerate S_4-extensions of K are in bijection with orbits of $\mathcal{G} \subseteq \mathrm{GL}_2(K) \times \mathrm{GL}_3(K)$ acting on $X \subset K^2 \otimes \mathrm{Sym}^2(K^3)$. Nondegenerate S_5-extensions of K are in bijection with orbits of $\mathcal{G} \subseteq \mathrm{GL}_4(K) \times \mathrm{GL}_5(K)$ acting on $X \subset K^4 \otimes \mathrm{Alt}^2(K^5)$. Unfortunately, this is where we run out of examples coming from [26]. Sporadically, other parametrizations were discovered. For example, Bhargava and Shnidman [7] constructed a *reducible* prehomogeneous vector space for the cyclic group of order three.

In his PhD thesis and subsequent work, Bhargava [3, 4, 6] managed to extend the parametrizations of extensions of *fields* K given by Wright and Yukie to parametrizations of extensions of *rings* S (in particular $S = \mathbb{Z}$). Melanie Wood [31] further generalized his work to extensions of *schemes* and also parametrized for example quartic extensions with quadratic subrings or cubic quotients.

Parametrizations of extensions of rings have proven particularly useful in solving *asymptotic counting problems*: For example, how many number fields are there of degree n and discriminant between $-X$ and X, for large X? How many Galois extensions of $\mathbb{Q}$ are there with Galois group G and discriminant between $-X$ and X, for large X? (The discriminant of a number field is really a property of its *ring* of integers!)

Malle [23, 24] formulated precise conjectures on those asymptotics. Looking at Hilbert class fields, these questions also turn out to be closely related to the Cohen–Lenstra heuristics concerning the average behaviour of ideal class groups (see [21]).

This thesis proposes a framework yielding parametrizations of ring extensions. It does not rely on any classification of prehomogeneous vector spaces, and can in fact produce more general parametrizations.

The work is organized as follows: In Chapter 2, we explain the theory for general groups G. In subsequent chapters, we explore certain examples in more detail.

We start by constructing for any group G a *preliminary parametrization* of G-extensions of a field K with $\mathcal{G}(K) = K[G]^\times$ and $X(K) \subseteq K[G] \otimes_K K[G]$. We give two independent proofs of this parametrization: a cohomological proof resembling arguments of Wright and Yukie, and an elementary proof resembling the arguments of Levi, Delone–Faddeev, and Bhargava.

The idea of the latter proof is that, after fixing a normal basis of a G-extension L of K, and hence an isomorphism $L \cong K[G]$ of left $K[G]$-modules, the multiplication map can be encoded as an element of $\mathrm{Hom}_{K[G]}(K[G] \otimes_K K[G] \to K[G]) \cong K[G] \otimes_K K[G]$. The normal basis (or, equivalently, the isomorphism $L \cong K[G]$) is unique exactly up to an action of the group $K[G]^\times$.

This can be generalized to ring extensions: A G-extension R of a Dedekind domain S (see Definition 2.5) might not have a normal integral basis; it might not be isomorphic to $S[G]$ as a left $S[G]$-module. However, we can provide a parametrization for any *fixed* left $S[G]$-module structure I (the *type*) of R. Under favorable circumstances, only finitely many different types can occur.

The preliminary parametrization has the unfortunate property that the dimension $|G|$ of the group $\mathcal{G}$, and thus the orbit X, is far smaller than the dimension $|G|^2$ of the ambient space $K[G] \otimes_K K[G]$. In general, this makes counting points (or orbits) in $X(K)$, and therefore counting G-extensions of K, difficult.

Luckily, the preliminary parametrization can often be *simplified*, by projecting to suitable subspaces of $K[G] \otimes_K K[G]$. This recovers the spaces studied by Levi, Delone–Faddeev, Wright–Yukie, and Bhargava. Assume that the characteristic of K does not divide the order of G. The underlying idea is that the multiplication table of a G-extension L of K in terms of a normal basis $(g\alpha)_{g \in G}$ possesses a lot of symmetry: If for any $g_1, g_2 \in G$, we write $(g_1\alpha)(g_2\alpha) = \sum_{h \in G} t_{g_1,g_2,h}(h\alpha)$ with $t_{g_1,g_2,h} \in K$, then $t_{ig_1,ig_2,ih} = t_{g_1,g_2,h}$ for any $i, g_1, g_2, h \in G$. This symmetry can be exploited by considering a more convenient basis coming from the representation theory of G: Consider the Artin–Wedderburn decomposition $K[G] \cong \prod_i M_{n_i}(D_i)$. Fix a K-basis of each division ring D_i. This gives rise to a

[1] This particular parametrization had earlier been discovered by Levi [22] using an ad-hoc method.

basis of each $M_{n_i}(D_i)$ and therefore a basis of $K[G] \cong L$. Many coefficients in the multiplication table with respect to this basis tend to be zero.[2] The action of $K[G]^\times$ on the remaining coefficients is also easier to understand.

Example 1.1. Let $G = \{e, \tau\}$ be the cyclic group of order two. Then, the most convenient basis for a Galois extension L of K with Galois group G is clearly a basis of the form $(1, \sqrt{x})$ with $x \in K$. How can we construct it from a normal basis $(\alpha, \tau\alpha)$? The element $\alpha + \tau\alpha$ is G-invariant and therefore lies in K. After rescaling, we can assume $\alpha + \tau\alpha = 1$. We can then construct the convenient basis as $(1, \sqrt{x}) = (\alpha + \tau\alpha, \alpha - \tau\alpha) = (\mathrm{triv}(\alpha), \mathrm{sgn}(\alpha))$ where triv and sgn are the trivial and nontrivial onedimensional representations of G, respectively. Note that for any $\rho, \sigma \in \{\mathrm{triv}, \mathrm{sgn}\}$, the product $\rho(\alpha)\cdot\sigma(\alpha)$ lies in $K\cdot((\rho\otimes\sigma)(\alpha))$. (For example, $\mathrm{sgn}(\alpha)^2 = x \in K = K\cdot\mathrm{triv}(\alpha) = K\cdot((\mathrm{sgn}\otimes\mathrm{sgn})(\alpha))$.)

$\otimes$	triv	sgn
triv	triv	sgn
sgn	sgn	triv

$\cdot$	$\mathrm{triv}(\alpha) = 1$	$\mathrm{sgn}(\alpha) = \sqrt{x}$
$\mathrm{triv}(\alpha) = 1$	$1 \cdot \mathrm{triv}(\alpha)$	$1 \cdot \mathrm{sgn}(\alpha)$
$\mathrm{sgn}(\alpha) = \sqrt{x}$	$1 \cdot \mathrm{sgn}(\alpha)$	$x \cdot \mathrm{triv}(\alpha)$

Remark 1.2. The trick of choosing a convenient basis has been used ad hoc in the special cases mentioned above by Levi, Delone–Faddeev and Bhargava.

We will illustrate the strategy for obtaining parametrizations on a few small groups G.

For the cyclic group of order two, we recover the well-known parametrization:

Theorem 1.3. *Let G be the cylic group of order two. Then, G-extensions of $\mathbb{Z}$ are in bijection with elements v of $(1 + 4\mathbb{Z}) \cup 4\mathbb{Z}$. (Elements of $1 + 4\mathbb{Z}$ correspond to G-extensions of one type I_1; elements of $4\mathbb{Z}$ correspond to G-extensions of another type I_2.) The discriminant of the G-extension is v. The G-extension is nonmaximal if and only if v is divisible by the square of an odd prime or $v \in (4 + 16\mathbb{Z}) \cup 16\mathbb{Z}$.*

For the cyclic group of order three, we obtain a parametrization equivalent to the one discovered by Bhargava and Shnidman [7]:

Theorem 1.4. *Let G be the cyclic group of order three. Then, G-extensions of $\mathbb{Z}$ are in bijection with elements v of $(\{\pm 1\}+3\mathbb{Z}[\zeta_3])\cup 3\mathbb{Z}[\zeta_3]$, modulo multiplication by ± 1. (Elements of $\{\pm 1\}+3\mathbb{Z}[\zeta_3]$ correspond to G-extensions of type I_1; elements of $3\mathbb{Z}[\zeta_3]$ correspond to G-extensions of type I_2.) The discriminant of the G-extension is $N_{\mathbb{Q}(\zeta_3)|\mathbb{Q}}(v)^2$. The G-extension is nonmaximal if and only if $N_{\mathbb{Q}(\zeta_3)|\mathbb{Q}}(v)$ is divisible by q^2 for any prime $q \neq 3$ or $v \in 3(\{\pm 1\} + 3\mathbb{Z}[\zeta_3]) \cup 3(\zeta_3 - 1)\mathbb{Z}[\zeta_3]$.*

Remark 1.5. This corresponds to the parametrization given in [7, Theorem 14] by identifying an element $b\zeta_3 + c\zeta_3^2$ of $(\{\pm 1\} + 3\mathbb{Z}[\zeta_3]) \cup 3\mathbb{Z}[\zeta_3]$ with (in their notation) the vector $(b, c)^t$ in the lattice L.

For the cyclic group of order five, we obtain a parametrization that in this form appears to be new. It can easily be exploited to count G-extensions of $\mathbb{Z}$ by discriminant. The asymptotic number of maximal extensions was known before. In fact, Mäki [25] managed to count maximal G-extensions of $\mathbb{Z}$ for *any* abelian group G! Wright [32] later generalized this to extensions of arbitrary number fields, but did not compute the asymptotic constant. Cohen, Diaz y Diaz, and Olivier [12] computed the asymptotic constant for cyclic extensions of prime degree of arbitrary number fields. The asymptotic number of nondegenerate (not necessarily maximal) extensions seems to be new. To keep this introduction simple, we only write down the parametrization of maximal nondegenerate extensions, here.

[2] For any i, let $V_i = D_i^{n_i}$ be the representation of G corresponding to the i-th factor in the Artin–Wedderburn decomposition. Then, in particular, the product of a basis element in $M_{n_i}(D_i)$ and a basis element in $M_{n_j}(D_j)$ is always a linear combination of basis elements in just those $M_{n_k}(D_k)$ for which the representation $V_i \otimes V_j$ of G contains V_k as a subrepresentation.

Theorem 1.6. *Let G be the cyclic group of order five. For $i = 1, 2, 3, 4$, denote by σ_i the automorphism of $\mathbb{Q}(\zeta_5)$ sending ζ_5 to ζ_5^i. Let X be the set of elements v of $\mathbb{Q}(\zeta_5)^\times$ satisfying the following local requirements:*

a) For all primes $q \equiv 2, 3, 4 \mod 5$: $N_{\mathbb{Q}(\zeta_5)|\mathbb{Q}}(v) \not\equiv 0 \mod q$. In other words, the q-part of v should be the ideal (1).

b) For all primes $q \equiv 1 \mod 5$: Let $\mathfrak{q}_1$ be a prime ideal of $\mathbb{Z}[\zeta_5]$ above q. Hence, q splits as $(q) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$, where $\mathfrak{q}_i = \sigma_i(\mathfrak{q}_1)$. The q-part of v should be one of the ideals (1), $\mathfrak{q}_1\mathfrak{q}_2$, $\mathfrak{q}_2\mathfrak{q}_4$, $\mathfrak{q}_3\mathfrak{q}_1$, $\mathfrak{q}_4\mathfrak{q}_3$.

c)
$$v \in (\{1, 2, 3, 4\} + (\zeta_5 - 1)^2\mathbb{Z}[\zeta_5]) \cup 5\mathbb{Z}[\zeta_5],$$
but
$$v \notin 5(\{1, 2, 3, 4\} + (\zeta_5 - 1)^2\mathbb{Z}[\zeta_5]) \cup 5(\zeta_5 - 1)\mathbb{Z}[\zeta_5].$$

Then, maximal G-extensions of $\mathbb{Z}$ are in bijection with elements of X, modulo multiplication by elements of the group $\langle -1, \zeta_5 + \zeta_5^{-1}\rangle$. (Elements of $\{1, 2, 3, 4\} + (\zeta_5 - 1)^2\mathbb{Z}[\zeta_5]$ correspond to G-extensions of type I_1; elements of $5\mathbb{Z}[\zeta_5]$ correspond to G-extensions of type I_2.) The discriminant of the G-extension is $N_{\mathbb{Q}(\zeta_5)|\mathbb{Q}}(v)^2$.

The Dirichlet series
$$D^{\max}(s) = \sum_{R \text{ maximal } G\text{-ext. of } \mathbb{Z}} \operatorname{disc}(R)^{-s}$$
of maximal extensions is
$$D^{\max}(s) = \left(1 + 4 \cdot 5^{-8s}\right) \prod_{q \equiv 1 \mod 5} \left(1 + 4q^{-4s}\right),$$

The Dirichlet series
$$D^{\text{nondeg}}(s) = \sum_{R \text{ nondeg. } G\text{-ext. of } \mathbb{Z}} \operatorname{disc}(R)^{-s}$$
of nondegenerate extensions is
$$D^{\text{nondeg}}(s) = \left(1 + 5 \cdot \frac{5^{-8s}}{1 - 5^{-2s}}\right) \prod_{q \neq 5} f_q^{\text{nondeg}}(q^{-s}),$$

where for any prime $q \neq 5$, we put
$$f_q^{\text{nondeg}}(x) = \begin{cases} \dfrac{1 + 2x^4 + 2x^6 + 2x^8 + x^{12}}{(1 - x^4)^2 (1 - x^6)^2}, & q \equiv 1 \mod 5, \\ \dfrac{1 - x^4 + x^8}{(1 - x^4)(1 - x^{12})}, & q \equiv 4 \mod 5, \\ \dfrac{1}{1 - x^8}, & q \equiv 2, 3 \mod 5. \end{cases}$$

In particular,
$$\#\{R \text{ maximal } G\text{-extension of } \mathbb{Z} \text{ with } \operatorname{disc}(R) \leqslant X\} \sim C_{\max} X^{1/4}$$
and
$$\#\{R \text{ nondegenerate } G\text{-extension of } \mathbb{Z} \text{ with } \operatorname{disc}(R) \leqslant X\} \sim C_{\text{nondeg}} X^{1/4}$$
for constants $C_{\max}, C_{\text{nondeg}} > 0$.

Using the same methods, very similar parametrizations can be obtained for the cyclic groups of orders 4, 6, and 7.

For the quaternion group, we obtain another new parametrization:

Theorem 1.7. *Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order eight. Consider the set X of tuples (d, v_1, v_2, v_3) in $\mathbb{Q} \times \mathbb{Q}^3 \times \mathbb{Q}^3 \times \mathbb{Q}^3$ such that $d \neq 0$ and $v_1, v_2, v_3 \neq 0$ are pairwise orthogonal vectors. Let $\mathbb{H}(\mathbb{Q})$ be the ring of Hamilton quaternions with rational coordinates. Let $\mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{H}(\mathbb{Q})^\times$ act on X as follows:*

$$(\lambda_1, \lambda_2, \lambda_3, h).(d, v_1, v_2, v_3) = (N(h)d, \lambda_1 r(h)v_1, \lambda_2 r(h)v_2, \lambda_3 r(h)v_3)$$

where $N(h) = a^2 + b^2 + c^2 + d^2$ denotes the norm of a Hamilton quaternion $h = a + bi + cj + dk$ and $r(h)$ denotes the orthogonal matrix

$$r(h) = \frac{1}{N(h)} \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2bc - 2ad & 2bd + 2ac \\ 2bc + 2ad & a^2 - b^2 + c^2 - d^2 & 2cd - 2ab \\ 2bd - 2ac & 2cd + 2ab & a^2 - b^2 - c^2 + d^2 \end{pmatrix}.$$

Then, nondegenerate G-extensions of $\mathbb{Q}$ are in bijection with $\mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{H}(\mathbb{Q})^\times$-orbits in X.

The multiplication table for the G-extension corresponding to (d, v_1, v_2, v_3) can be found on page 55.

We are then able to use the corresponding parametrization of ring extensions to count maximal quaternionic extensions of $\mathbb{Z}$ by conductor. (See Section 4.6 for a more detailed introduction to counting quaternionic extensions.)

Theorem 1.8. *Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order eight. For any G-extension R of $\mathbb{Z}$, define the conductor*

$$\operatorname{cond}(R) = \frac{\operatorname{disc}(R)}{\operatorname{disc}(R^{\{\pm 1\}})}$$

as the quotient of the discriminant of R and the discriminant of the subring fixed by $\{\pm 1\} \subsetneq G$. Then,

$$\#\{\text{max. } G\text{-extension } R \text{ of } \mathbb{Z} \text{ with } |\operatorname{cond}(R)|^{1/4} \leqslant X\} = C_{\text{cond}} \cdot X(\log X)^3 + o(X(\log X)^3).$$

where

$$\begin{aligned} C_{\text{cond}} &= \frac{1}{2^8} \cdot \prod_{p \neq 2} (1 + 4p^{-1})(1 - p^{-1})^4 \\ &\approx 0.00085271440732599. \end{aligned}$$

Chapter 2

General theory

Fix a finite group G. We write $e \in G$ for the identity element.

2.1 Parametrizing field extensions via Galois cohomology

For motivational purposes, we start with a short cohomological proof of a parametrization of field extensions. We will later meet the same parametrization space again, when we show that it can also be used to parametrize ring extensions.

Let K be any field. Consider the group ring $K[G]$. The tensor product $K[G] \otimes_K K[G]$ naturally becomes a K-algebra.

Let $\Delta : K[G] \to K[G] \otimes_K K[G]$ be the diagonal embedding of K-algebras given by $g \mapsto g \otimes g$ for $g \in G$.

Warning 2.1. Note that in general $\Delta(\lambda) \neq \lambda \otimes \lambda$: For example, if $\lambda = ae$ with $a \in K$, then $\Delta(\lambda) = a(e \otimes e)$, but $\lambda \otimes \lambda = a^2(e \otimes e)$.

Define an action of $K[G]^\times$ on $K[G] \otimes_K K[G]$ as follows: an element $\lambda \in K[G]^\times$ sends $T \in K[G] \otimes_K K[G]$ to $(\lambda \otimes \lambda) \cdot T \cdot \Delta(\lambda)^{-1}$.

Let K^{sep} be the separable closure of K and let $X \subseteq K^{\mathrm{sep}}[G] \otimes_{K^{\mathrm{sep}}} K^{\mathrm{sep}}[G]$ be the $K^{\mathrm{sep}}[G]^\times$-orbit containing $e \otimes e$. We will later specify polynomial equalities (unit, symmetric, associativity conditions) and inequalities (nonzero discriminant) cutting out the orbit X.

Lemma 2.2. *In $K^{\mathrm{sep}}[G]^\times$, the stabilizer of $e \otimes e \in K[G] \otimes_K K[G]$ is the finite group $G \subseteq K[G]^\times$.*

Proof. Clearly, $(g \otimes g) \cdot (e \otimes e) \cdot \Delta(g)^{-1} = e \otimes e$ for any $g \in G$. We therefore only have to show that any element $\lambda \in K^{\mathrm{sep}}[G]^\times$ satisfying $(\lambda \otimes \lambda) \cdot (e \otimes e) \cdot \Delta(\lambda)^{-1} = e \otimes e$ lies in G. This equation is equivalent to

$$\lambda \otimes \lambda = \Delta(\lambda).$$

If we let $\lambda = \sum_{g \in G} \lambda_g g$, we obtain

$$\sum_{g_1, g_2} \lambda_{g_1} \lambda_{g_2}\ g_1 \otimes g_2 = \sum_{g \in G} \lambda_g\ g \otimes g.$$

This means that $\lambda_{g_1} \lambda_{g_2} = 0$ if $g_1 \neq g_2$ and that $\lambda_g^2 = \lambda_g$ for all g. In other words, there can be at most one nonzero λ_g, which has to be 1. Since $\lambda \neq 0$, we conclude that exactly one λ_g is 1, so λ indeed lies in G. □

Using that $H^1(K, K^{\mathrm{sep}}[G]^\times) = 1$, a cohomological argument (see [33, section 5]) then implies the following theorem.

Theorem 2.3. *There is a bijection between the set of G-conjugacy classes of continuous group homomorphisms $\mathrm{Gal}(K^{\mathrm{sep}}|K) \to G$ and the set of $K[G]^\times$-orbits of points in $X \cap K[G] \otimes_K K[G]$.*

Remark 2.4. Clearly, the action of $K[G]^\times$ on $K[G] \otimes_K K[G]$ restricts to an action on the "slightly simplified" space $\mathrm{Sym}^2 K[G] \subseteq K[G] \otimes_K K[G]$. We could therefore alternatively have stated the above theorem with $K[G] \otimes_K K[G]$ replaced by $\mathrm{Sym}^2 K[G]$. We will later see how to restrict to even smaller subrepresentations.

2.2 Parametrizing ring extensions

Let S be a Dedekind domain (an integrally closed Noetherian domain in which every nonzero prime ideal is maximal, for example a field or the ring of integers of a number field) with field of fractions K.

Definition 2.5. We call a (commutative) S-algebra R together with a left action of G on the S-algebra R a *G-extension of S* if

i) the ring R is a finitely generated torsion-free S-module, and

ii) there is an isomorphism $R \otimes_S K \cong K[G]$ of left $K[G]$-modules.[1]

By an isomorphism of G-extensions of S, we mean a G-invariant isomorphism of S-algebras between them.

Lemma 2.6. *Let $L|K$ be a Galois extension with Galois group G. Then, L is a G-extension of K and the integral closure R of S in L is a G-extension of S. The automorphism groups of both of these G-extensions is the center $Z(G)$ of G.*

Proof. Let us first show property i). L is a finite-dimensional vector space over K, and therefore a finitely generated torsion-free K-module, showing property i) for $L|K$. This also implies that $R \subseteq L$ is a torsion-free S-module.

To show that is R a finitely generated S-module, first note that R is contained in a finitely generated S-module (see [2, Chapter 5, Prop. 5.17]). Since S is Noetherian, R must also be finitely generated.

For the G-extension L of K, property ii) follows from the Normal Basis Theorem for Galois extensions. This implies property ii) for the G-extension R of S, since $R \otimes_S K \cong L$.

The automorphisms of the field extension $L|K$ correspond to elements of the group. Each of them restricts to an automorphism of R. The automorphism corresponding to $g \in G$ is G-invariant if and only if g commutes with every element h of G. □

Remark 2.7. The automorphisms of the left $K[G]$-module $K[G]$ are exactly the functions of the form $x \mapsto x\lambda$ with $\lambda \in K[G]^\times$. Thus, the isomorphism $R \otimes_S K \cong K[G]$ is unique up to multiplication by elements of $K[G]^\times$ on the right.

Definition 2.8. We call a left $S[G]$-submodule I of $K[G]$ a *full ideal* of $S[G]$ if I is a finitely generated S-module and $I \otimes_S K = K[G]$ (meaning $k_1 \cdot S[G] \subseteq I \subseteq k_2 \cdot S[G]$ for some $k_1, k_2 \in K^\times$). Two full ideals I, I' are called *equivalent* if $I' = I\lambda$ for some $\lambda \in K[G]^\times$. Write $\mathrm{Aut}(I)$ for the group of all $\lambda \in K[G]^\times$ such that $I = I\lambda$.

We further call a full ideal I *unitary* if $\{s \in K \mid s \cdot \sum_{g \in G} g \in I\} = S$. (In other words, $I^G = S[G]^G = S$.) Write $K[G]_1^\times$ for the group of elements $\sum \lambda_g g$ of $K[G]^\times$ such that $\sum_g \lambda_g = 1$. They correspond

[1] The left G-action on R of course gives R the structure of a left $S[G]$-module, and hence $R \otimes_S K$ the structure of a left $K[G]$-module.

exactly to the automorphisms of $K[G]$ that fix $\sum_g g$. Furthermore, let $S[G]_1^\times = S[G]^\times \cap K[G]_1^\times$ and $\mathrm{Aut}_1(I) = \mathrm{Aut}(I) \cap K[G]_1^\times$.

Note that two full ideals I, I' are equivalent if and only if they are isomorphic left $S[G]$-modules.

Example 2.9. The module $S[G]$ is a unitary full ideal, with $\mathrm{Aut}(S[G]) = S[G]^\times$. If S is a field ($S = K$), then $S[G]$ is the only full ideal up to equivalence.

Lemma 2.10. *Let R be a G-extension of S. Then, there is an isomorphism $\varphi : R \to I$ of left $S[G]$-modules such that I is a unitary full ideal and $1 \in R$ is sent to $\sum_{g\in G} g \in I$.*

Proof. Since R is a torsion-free S-module, the map $R \to R \otimes_S K \cong K[G]$ is injective. We thus obtain an $S[G]$-module isomorphism between R and some full ideal I of $S[G]$. Since $1 \in R$ is fixed by the action of any element of G, the image $u \in K[G]$ of $1 \in R$ must satisfy $gu = u$ for all $g \in G$. This means that $u = l \cdot \sum_{g\in G} g$ for some $l \in K^\times$. After dividing the isomorphism $R \otimes_S K \xrightarrow{\sim} K[G]$ by l, we can assume that $l = 1$. We hence have $S \cdot \sum_g g \subseteq I$. Now, take any $x = \frac{a}{b} \in K$ (with $a, b \in S$) such that $x \cdot \sum_g g \in I$. Let $r \in R$ be its preimage. By definition, we have $br = a$ in R, so in fact $r = \frac{a}{b} = x$ in K. Since R is a finitely generated S-module, $r = x$ must be a root of some monic polynomial with coefficients in S. We assumed that S is an integrally closed domain, so $x \in S$. Therefore, I is a unitary full ideal. □

Definition 2.11. The *type* of a G-extension R of S is the equivalence class of this full ideal I.

Remark 2.12. One says that a G-extension R *has a normal integral basis* if it is of type $S[G]$.

We are now ready to construct a preliminary parametrization for G-extensions of R of type I. The idea is that, fixing the type I and the isomorphism $R \cong I$ of left $S[G]$-modules, to determine the G-extension R, it only remains to specify the multiplication map $R \times R \to R$. The multiplication map translates to a map $m : I \times I \to I$.

Clearly, K-bilinear (left) G-invariant[2] maps $m : K[G] \times K[G] \to K[G]$ are in bijection with K-linear (left) G-invariant maps $K[G] \otimes_K K[G] \to K[G]$. Write $\mathcal{H} = \mathcal{H}(K) = \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$ for this space of K-linear (left) G-invariant maps. Let $\lambda \in K[G]^\times$ act on $m \in \mathcal{H}$ as follows:

$$(\lambda.m)(x \otimes y) = m(x\lambda \otimes y\lambda)\lambda^{-1}.$$

Theorem 2.13. *Let I be a unitary full ideal. Let $\mathcal{P}_I(S)$ be the set of elements m of $\mathcal{H} = \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$ satisfying the following four conditions:*
The unit condition

$$m\Big(\sum_{g\in G} g \otimes x\Big) = x \qquad \text{for all } x \in K[G], \tag{Cu}$$

the symmetry condition

$$m(x \otimes y) = m(y \otimes x) \qquad \text{for all } x, y \in K[G], \tag{Cs}$$

the associativity condition

$$m(m(x \otimes y) \otimes z) = m(x \otimes m(y \otimes z)) \qquad \text{for all } x, y, z \in K[G], \tag{Ca}$$

and the closedness condition

$$m(x \otimes y) \in I \qquad \text{for all } x, y \in I. \tag{Cc}$$

Then, the G-extensions R of S of type I are in bijection with the elements m of $\mathcal{P}_I(S)$ modulo the action of $\mathrm{Aut}_1(I) \subseteq K[G]_1^\times$.

The stabilizer $\mathrm{Stab}_{\mathrm{Aut}_1(I)}(m)$ is isomorphic to the automorphism group of the corresponding G-extension of S.

[2] A map $m : K[G] \times K[G] \to K[G]$ is *(left) G-invariant* if $m(gx, gy) = gm(x, y)$ for all $x, y \in K[G]$.

Proof. A G-extension R of S of type I with a fixed isomorphism $\varphi : R \to I$ sending $1 \in R$ to $u = \sum_{g\in G} g \in I$ is determined by the multiplication operation on R. (The S-module structure and the action of G are determined by the isomorphism!) The multiplication operation on R translates to a bilinear G-invariant map $I \times I \to I$, which we can extend to a bilinear map $K[G] \times K[G] \to K[G]$, i.e. a K-linear G-invariant map $m : K[G] \otimes K[G] \to K[G]$.

When we compose φ with an automorphism $x \mapsto x\lambda^{-1}$ of I, the map m becomes m' with $m'(x\otimes y) = m(x\lambda \otimes y\lambda)\lambda^{-1}$, so $m' = \lambda.m$. The unit $u = \sum_{g\in G} g \in I$ is fixed by λ if and only if λ lies in $K[G]_1^\times$.

Clearly, an automorphism of the G-extension R corresponds exactly to a (left) $S[G]$-module automorphism of I fixing the unit and preserving the multiplication map m, i.e., an element of $\mathrm{Aut}_1(I)$ that stabilizes m.

Now let us list the additional properties the map $m : K[G] \otimes K[G] \to K[G]$ needs to satisfy to produce an S-algebra:

(Cu) The element $u = \sum_{g\in G} g \in I \subseteq K[G]$ needs to be a (left) unit. In other words, $m(\sum_{g\in G} g\otimes x) = x$ for all $x \in I$ and hence for all $x \in K[G]$.

(Cs) Multiplication must be symmetric/commutative, i.e. $m(x \otimes y) = m(y \otimes x)$ for all $x, y \in I$ and hence for all $x, y \in K[G]$.

(Ca) Multiplication must be associative, i.e. $m(m(x \otimes y) \otimes z) = m(x \otimes m(y \otimes z))$ for all $x, y, z \in I$ and hence for all $x, y, z \in K[G]$.

(Cc) The set I must be closed under multiplication, i.e. $m(x \otimes y) \in I$ for all $x, y \in I$. □

Remark 2.14. Condition (Ca) says that the left and right associative compositions $K[G]\otimes K[G]\otimes K[G] \to K[G]$ of $m : K[G]\otimes K[G] \to K[G]$ coincide, where we define the *left associative composition* by $x\otimes y\otimes z \mapsto m(m(x\otimes y)\otimes z)$ and the *right associative composition* by $x\otimes y\otimes z \mapsto m(x\otimes m(y\otimes z))$.

Definition 2.15. Let $\pi : K[G]\otimes K[G] \to K[G]$ be the K-linear map sending $g\otimes g$ to g and $g_1\otimes g_2$ to 0 for $g_1 \neq g_2$. It is easy to verify that $\pi \in \mathcal{P}_{S[G]}(S)$. We call the corresponding G-extension R of type $S[G]$ the *trivial G-extension* of S. As an S-algebra, it is isomorphic to $\prod_{g\in G} S$. The action of G simply permutes the factors as $g'.(x_g)_{g\in G} = (x_{g'^{-1}g})_{g\in G}$. The automorphism group of the trivial G-extension R is G: The automorphism corresponding to $g' \in G$ sends $(x_g)_g$ to $(x_{gg'})_g$.

Question 2.16. Is $\mathcal{P}_I(S) \neq \varnothing$ for every unitary full ideal I? I.e., does every unitary full ideal occur as the type of some G-extension of S?

Remark 2.17. Clearly, conditions (Cu), (Cs), and (Ca) only need to be checked for x, y, z in a K-basis of $K[G]$, for example $x, y, z \in G$. Condition (Cc) only needs to be checked for x, y in a set of generators of the S-module I.

Remark 2.18. Notice the different characters of those four conditions:

- (Cu) and (Cs) cut out affine linear subspaces of $\mathcal{H}$.
- (Ca) cuts out a subvariety of $\mathcal{H}$ defined by a set of homogeneous equations of degree two.
- (Cc) describes a lattice inside $\mathcal{H}$. If $k_1 \cdot S[G] \subseteq I \subseteq k_2 \cdot S[G]$, then

$$\frac{k_1}{k_2^2} \cdot \mathcal{H}(S) \subseteq \{m \in \mathcal{H}(K) \text{ satisfying (Cc)}\} \subseteq \frac{k_2}{k_1^2} \cdot \mathcal{H}(S),$$

  where $\mathcal{H}(S) = \mathrm{Hom}_G(S[G] \otimes S[G] \to S[G]) \subseteq \mathcal{H}(K)$.

If S is a field, then all full ideals are equivalent and condition (Cc) is automatically satisfied, so we will just write $\mathcal{P}$ instead of $\mathcal{P}_I$. An element of $\mathcal{P}(K)$ lies in $\mathcal{P}_I(S)$ if and only if it satisfies condition (Cc).

Remark 2.19. If I is a unitary full ideal and $I\lambda$ is an equivalent unitary ideal with $\lambda \in K[G]_1^\times$, then $\mathcal{P}_{I\lambda}(S) = \lambda^{-1}.\mathcal{P}_I(S)$.

Remark 2.20. Note that the representation $K[G] \otimes K[G]$ of $K[G]^\times$ defined in Section 2.1 is isomorphic to the representation $\mathcal{H}$ of $K[G]^\times$ defined in this section: There is an isomorphism

$$K[G] \otimes K[G] \longleftrightarrow \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$$

sending $T \in K[G] \otimes K[G]$ to the map m defined by $m(x \otimes y) = \pi((x \otimes y) \cdot T)$. In particular, note that $\mathcal{H}$ is a $|G|^2$-dimensional vector space over K. The element $e \otimes e$ corresponds to π. Hence, the stabilizer of π in $K[G]^\times$ is $G \subseteq K[G]_1^\times$.

Remark 2.21. The parametrization is functorial in the base ring S under injective maps: if $S \subseteq S'$ are Dedekind domains and $m \in \mathcal{P}_I(S)$ corresponds to the G-extension R of S, then $m \in \mathcal{P}_{I \otimes_S S'}(S')$ corresponds to the G-extension $R \otimes_S S'$ of S'.

Lemma 2.22. *If $I = S[G]$, then $\mathcal{P}_I$ is represented by an affine scheme, which we will denote by $\mathcal{P}$: There is a closed subscheme $\mathcal{P}$ of $\mathbb{A}_{\mathbb{Z}}^{|G|^2}$ such that $\mathcal{P}_{S[G]}(S) = \mathcal{P}(S)$ for all rings S.*

Proof. As in Remark 2.20, G-invariant S-linear maps $m : S[G] \otimes_S S[G] \to S[G]$ can be described by $|G|^2$ elements of S. According to Remark 2.17, conditions (Cu), (Cs), and (Ca) are all equivalent to some (fixed) polynomial conditions in these elements. □

Warning 2.23. In general, if I is a unitary full ideal of $\mathbb{Z}[G]$, then $I \otimes_{\mathbb{Z}} S$ need not be a unitary ideal of $S[G]$. For example, if $G = \{e, \tau\}$ is the cyclic group of order two, then

$$I = (e + \tau)\mathbb{Z} \oplus \frac{e - \tau}{2}\mathbb{Z}$$

is a unitary full ideal of $\mathbb{Z}[G]$, but the left $\mathbb{F}_2[G]$-module $I \otimes_{\mathbb{Z}} \mathbb{F}_2$ cannot even be embedded into $\mathbb{F}_2[G]$. (All four elements of $I \otimes_{\mathbb{Z}} \mathbb{F}_2$ are left G-invariant.) In particular, if R is a G-extension of $\mathbb{Z}$, then $R \otimes_{\mathbb{Z}} \mathbb{F}_p$ might not always be a G-extension of $\mathbb{F}_p$. To solve this issue, one could broaden the definition of G-extensions to allow $S[G]$-modules not contained in $K[G]$. In addition to the $S[G]$-isomorphism class of I, one should then remember to fix the element $u \in I$ corresponding to the unit in R. As we have seen, there may be many elements fixed by G.

2.3 Nondegenerate extensions

Definition 2.24. An *extension* R of K is a finite-dimensional K-algebra. As usual, if we denote a basis of R by $(\alpha_1, \ldots, \alpha_n)$, we define the *discriminant* of R to be $\mathrm{disc}(R) = \det(M)$ where M is the trace matrix $(\mathrm{Tr}(\alpha_i\alpha_j))_{i,j}$. Modulo multiplication by elements of $K^{\times 2}$, the discriminant is independent of the choice of basis. We call R a *nondegenerate* extension if $\mathrm{disc}(R) \neq 0$.

Remark 2.25. Nondegenerate extensions are also called *étale algebras*.

Definition 2.26. Let $\mathcal{P}^{\mathrm{nondeg}}(K)$ be the set of points in $\mathcal{P}(K)$ that correspond to nondegenerate G-extensions of K. For any unitary full ideal I, let $\mathcal{P}_I^{\mathrm{nondeg}}(S) = \mathcal{P}_I(S) \cap \mathcal{P}^{\mathrm{nondeg}}(K)$.

Example 2.27. Any finite-dimensional field extension $L|K$ is nondegenerate.

Let us now prove some well-known facts about extensions of a field K.

Lemma 2.28. *For any two extensions R_1, R_2 of K,*

$$\mathrm{disc}(R_1 \times R_2) = \mathrm{disc}(R_1) \cdot \mathrm{disc}(R_2).$$

Proof. The trace in $R_1 \times R_2$ of any $\alpha \in R_i$ equals its trace in R_i. Choosing bases for R_1 and R_2, we obtain a basis for $R_1 \times R_2$ whose trace matrix is a block diagonal matrix consisting of the trace matrices for R_1 and R_2. □

Lemma 2.29. *If R is a nondegenerate extension of K, it contains no nonzero nilpotent elements: if $x^k = 0$ for some $x \in R$ and $k \geqslant 1$, then $x = 0$.*

Proof. Let us first show that $\mathrm{Tr}(x) = 0$ for any $x \in R$ with $x^k = 0$: multiplication by x sends each element of $x^i R$ to $x^{i+1}R$. Since

$$R = x^0 R \supseteq x^1 R \supseteq \cdots \supseteq x^k R = 0,$$

it follows that $\mathrm{Tr}(x) = 0$. (With respect to a particular basis, the multiplication by x map is represented by a strictly upper triangular matrix.)

Now, assume there exists some $x \in R$ such that $x^k = 0$ but $x \neq 0$. Find a basis $\alpha_1, \ldots, \alpha_n$ of R with $\alpha_1 = x$. The first row $(\mathrm{Tr}(x\alpha_j))_j$ of the trace matrix consists of traces of nilpotent elements, which we have shown to be zero. Hence, $\mathrm{disc}(R) = 0$. □

Lemma 2.30. *Let K be a field and R a nondegenerate extension of K. Then, $R \cong L_1 \times \cdots \times L_r$ for some field extensions $L_i | K$.*

Proof. Assume R is a nondegenerate extension. We will show the claim using induction over the dimension of R as a K-vector space. The claim is clear for $R = 0$. Assume $\dim(R) \geqslant 1$.

For any $x \in R$, the multiplication by x map $\times_x : R \to R$ is a linear endomorphism of the finite-dimensional K-vector space R. Thus, the map is either surjective (so x is invertible in R) or not injective (so x is a zero divisor). If all $x \neq 0$ are invertible, then R is a field extension of K. Otherwise, choose $x \neq 0$ so that the image $R' = xR$ has minimal dimension. Correspondingly, the kernel $R'' = \{y \in R \mid xy = 0\}$ has maximal dimension. Clearly, R' and R'' are extensions of K with $\dim(R') + \dim(R'') = \dim(R)$ and $0 \subsetneq R' \subsetneq R$ and $R' \cdot R'' = 0$.

Assume $R' \cap R'' \neq 0$, say $0 \neq xz \in R''$. This means that $x^2 z = 0$. Then, $\{z' \in R \mid xz' = 0\} \subsetneq \{z' \in R \mid x^2 z' = 0\}$, so $\dim(xR) > \dim(x^2 R)$. Since we chose $x \neq 0$ so that xR has minimal dimension, this can only happen if $x^2 = 0$, contradicting Lemma 2.29.

We therefore have $R' \cap R'' = 0$. It follows that $R = R' \times R''$. Finally, $0 \neq \mathrm{disc}(R) = \mathrm{disc}(R') \cdot \mathrm{disc}(R'')$ and $\dim(R'), \dim(R'') < \dim(R)$, so we can apply the induction hypothesis to R' and R''. □

Lemma 2.31. *Let $L_1, \ldots, L_r$ be field extensions of K. Let f be any K-linear ring automorphism of $R = L_1 \times \cdots \times L_r$. Then, there exists a unique permutation $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ so that for any i, the function f sends elements of $L_i \subseteq R$ to elements of $L_{\sigma(i)} \subseteq R$ via an isomorphism $L_i \xrightarrow{\sim} L_{\sigma(i)}$ of field extensions of K.*

Proof. Write π_i for the i-th projection map $R \twoheadrightarrow L_i$. For any $1 \leqslant i \leqslant r$, let $P_i = \{1 \leqslant j \leqslant r \mid \exists x \in L_i : \pi_j(f(x)) \neq 0\}$. Clearly, $P_i \neq \varnothing$ because f is injective. For any $i \neq i'$ with $x_i \in L_i$ and $x_{i'} \in L_{i'}$ and any j, we have

$$\pi_j(f(x_i))\pi_j(f(x_{i'})) = \pi_j(f(x_i x_{i'})) = \pi_j(f(0)) = 0,$$

which means that $\pi_j(f(x_i)) = 0$ or $\pi_j(f(x_{i'})) = 0$. In other words, $P_i \cap P_{i'} = \varnothing$ whenever $i \neq i'$.

The disjoint nonempty sets $P_1, \ldots, P_r \subseteq \{1, \ldots, r\}$ must then each have exactly one distinct element: $P_i = \{\sigma(i)\}$ for some permutation σ of $\{1, \ldots, r\}$. Therefore, $f(x_i) \in L_{\sigma(i)}$ for each $x_i \in L_i$. □

Lemma 2.32. *Let G be a finite group. Then, any nondegenerate G-extension R of K is of the form*

$$R \cong \left\{ (x_g)_g \in \prod_{g \in G} L \mid \forall g \in G, h \in H : x_{gh} = h^{-1} x_g \right\} \cong L^{[G:H]}$$

where $L|K$ is a Galois extension with Galois group $H \subseteq G$ and the action of G on R is given by $g'.(x_g)_g = (x_{g'^{-1}g})_g$.
This is unique up to conjugation of $H \subseteq G$ and simulateneously of the action of H on $L|K$ by elements of G.

Proof. According to Lemma 2.30, we can write $R = L_1 \times \cdots \times L_r$ for some field extensions $L_i|K$. We will use two properties following from the fact that R is isomorphic to $K[G]$ as a left $K[G]$-module:

(a) The dimension of R as a K-vector space is $|G|$.

(b) The vector space of elements of R fixed by G is onedimensional.

Apply Lemma 2.31 to the action of elements $g \in G$ on R. It follows that there is an action of G on the set $\{1, \ldots, r\}$, so that the action of $g \in G$ on R sends elements of $L_i \subseteq R$ to elements of $L_{gi} \subseteq R$:

$$\varphi_{g,i} : L_i \xrightarrow{g} L_{gi}$$

These maps are all isomorphisms of field extensions of K.

By property (b), the action of G on $\{1, \ldots, r\}$ must be transitive: if $X \subseteq \{1, \ldots, r\}$ is any set invariant under G, then the element $(\mathbb{1}_{i \in X})_i$ of $R = L_1 \times \cdots \times L_r$ is fixed by G.

It follows that the field extensions $L_i|K$ are all isomorphic. We can furthermore identify $\{1, \ldots, r\}$ with G/H where $H \subseteq G$ denotes the stabilizer of 1. In particular, $r = [G : H]$. Choose representatives $t_1, \ldots, t_r$ of G/H so that $t_i 1 = i$. Note that H acts on L_1.

Let $x \in L_1$ be an element fixed by all $h \in H$. For each $1 \leqslant i \leqslant r$, let $y_i = t_i x \in L_i$. For any $g \in G$ and any $1 \leqslant i \leqslant r$, write $gt_i = t_j h$ with $1 \leqslant j \leqslant r$ and $h \in H$. The action of g on y_i is then given by

$$gy_i = t_j h t_i^{-1} y_i = t_j h x = t_j x = y_j.$$

For the element $y = (y_i)_i$ of $R = L_1 \times \cdots \times L_r$, it follows that $gy = y$. By property (b), all y constructed in this manner from elements x of L_1^H (for example, $x = 1$) are proportional. This means that y must be of the form $(k, \ldots, k) \in L_1 \times \cdots \times L_r$ for some $k \in K$. But then $k = y_i = t_i x$, so since $L_1 \xrightarrow{t_i} L_i$ is an isomorphism fixing K, it follows that $x \in K$.

Thus, the subfield of L_1 fixed by all elements of H is exactly K. In particular, $L_1|K$ must be a Galois extension, with a surjection $H \twoheadrightarrow \mathrm{Gal}(L_1|K)$. Since

$$\begin{aligned} |G| &= \dim_K(R) = \dim_K(L_1) + \cdots + \dim_K(L_r) = r \dim_K(L_1) \\ &= [G : H] \dim_K(L_1), \end{aligned}$$

so $\dim_K(L_1) = |H|$, we can in fact conclude that $L_1|K$ is a Galois extension with Galois group H.

Let $L = L_1$. Construct an isomorphism

$$R \longrightarrow \left\{ (x_g)_g \in \prod_{g \in G} L \mid \forall g \in G, h \in H : x_{gh} = h^{-1} x_g \right\}$$

by sending an element $(y_i)_i$ to the tuple $(x_g)_g$ defined by $x_{t_i h} = h^{-1} \varphi_{t_i,1}^{-1}(y_i)$ for all $1 \leqslant i \leqslant r$ and $h \in H$. It can easily be verified that the actions of G on the two sides coincide.

Uniqueness is also easy to show. □

Example 2.33. If $H = G$, we have $R \cong L$ for some Galois extension $L|K$ with Galois group G.

Example 2.34. If $H = 1$, we have the trivial G-extension $R \cong \prod_{g \in G} K$.

As a very important consequence, we conclude that all nondegenerate G-extensions lie in the same orbit over the separable closure of K:

Corollary 2.35. *If K is separably closed, the trivial G-extension is the only nondegenerate G-extension of K. It follows that $K[G]_1^\times$ acts transitively on $\mathcal{P}^{\mathrm{nondeg}}(K)$ if K is separably closed:*

$$\mathcal{P}^{\mathrm{nondeg}}(K) = K[G]_1^\times.\pi.$$

For general fields K, we therefore obtain

$$\mathcal{P}^{\mathrm{nondeg}}(K) = K^{\mathrm{sep}}[G]_1^\times.\pi \cap \mathcal{H}(K),$$

so we can write any $m \in \mathcal{P}^{\mathrm{nondeg}}(K)$ as $m = \alpha.\pi$ for some $\alpha \in K^{\mathrm{sep}}[G]_1^\times$.

The corollary has the following useful application: If W is a representation of $K[G]_1^\times$ and $f : \mathcal{H} \to W$ is any $K[G]_1^\times$-invariant linear map, then for any $m \in \mathcal{P}^{\mathrm{nondeg}}(K)$, we have $f(m) = 0$ if and only if $f(\pi) = 0$. This way, after decomposing $\mathcal{H}$ into irreducible representations of $K[G]_1^\times$, we can often eliminate some summands (on which π projects to 0)!

Warning 2.36. As we will see in Remark 4.10, we might nevertheless have $f(m) \neq 0$ and $f(\pi) = 0$ for some *degenerate* extensions!

Remark 2.37. Lemma 2.32 also implies that nondegenerate G-extensions of a field K are in bijection with continuous homomorphisms

$$f : \mathrm{Gal}(K^{\mathrm{sep}}|K) \to G$$

modulo conjugation by elements of G. The automorphisms of such a G-extension are in bijection with elements of the centralizer $Z(\mathrm{im}(f)) \subseteq G$ of the image of f.

Corollary 2.38. *If $K = \mathbb{F}_q$ is a finite field, the number of nondegenerate $\mathbb{F}_q$-points on $\mathcal{P}$ is*

$$|\mathcal{P}^{\mathrm{nondeg}}(\mathbb{F}_q)| = |\mathbb{F}_q[G]_1^\times|.$$

Proof. Nondegenerate G-extensions of $\mathbb{F}_q$ are in bijection with $\mathbb{F}_q[G]_1^\times$-orbits in $\mathcal{P}^{\mathrm{nondeg}}(\mathbb{F}_q)$. By Burnside's Lemma, and because continuous maps $\mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q) \to G$ are exactly determined by the image of the Frobenius automorphism of $\overline{\mathbb{F}_q}|\mathbb{F}_q$, we have

$$\begin{aligned}
|\mathcal{P}^{\mathrm{nondeg}}(\mathbb{F}_q)| &= \sum_{\substack{f:\mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)\to G \\ \text{modulo conjugation}}} \frac{|\mathbb{F}_q[G]_1^\times|}{Z(\mathrm{im}(f))} \\
&= \#\{f : \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q) \to G\} \cdot \frac{|\mathbb{F}_q[G]_1^\times|}{|G|} \\
&= |\mathbb{F}_q[G]_1^\times|.
\end{aligned}$$

□

Using Artin–Wedderburn's Theorem, the number $|\mathbb{F}_q[G]_1^\times|$ can easily be deduced from the representation theory of G over $\mathbb{F}_q$.

We have thus constructed a (potentially complicated) quasi-projective variety $\mathcal{P}^{\mathrm{nondeg}}$ with a known number of $\mathbb{F}_q$-points for all q.

2.4 Localizations

The closedness condition (Cc) can of course be verified locally:

Lemma 2.39. *Condition (Cc) holds for $m \in \mathcal{H}$ with type I over the ring S if and only if for all maximal ideals $\mathfrak{p}$ of S, condition (Cc) holds for m with type $I \otimes_S S_\mathfrak{p}$ over the ring $S_\mathfrak{p}$.*

Proof. The claim follows from the fact that

$$I = \{x \in K[G] \mid \forall \mathfrak{p} : x \in I \otimes_S S_\mathfrak{p}\}.$$

□

Definition 2.40. We call a nondegenerate G-extension of S *maximal* if it doesn't properly contain another G-extension of S. Let $\mathcal{P}_I^{\max}(S)$ be the set of points in $\mathcal{P}_I^{\text{nondeg}}(S)$ corresponding to maximal extensions.

Example 2.41. The integral closure constructed in Lemma 2.6 is a maximal G-extension. More generally, the integral closure of S in a nondegenerate extension of K as in Lemma 2.32 is a maximal G-extension.

Lemma 2.42. *A G-extension corresponding to $m \in \mathcal{P}_I(S)$ is maximal if and only if there exists no larger unitary ideal $J \supsetneq I$ such that $m \in \mathcal{P}_J(S)$.*

In particular, if all full ideals of $S[G]$ are equivalent, then the G-extension corresponding to $m \in \mathcal{P}_{S[G]}^{\text{nondeg}}(S)$ is maximal if and only if there exists no $\lambda \in S[G] \cap K[G]_1^\times \backslash S[G]_1^\times$ such that $\lambda^{-1}.m \in \mathcal{P}_{S[G]}(S)$.

Proof. The first claim follows directly from the construction of m. For the second claim, notice that for any $\lambda \in K[G]_1^\times$, we have $S[G]\lambda^{-1} \supsetneq S[G]$ if and only if λ lies in $S[G]$, but not in $\mathrm{Aut}_1(S[G]) = S[G]_1^\times$. Also, recall that $\mathcal{P}_{S[G]\lambda^{-1}}(S) = \lambda.\mathcal{P}_{S[G]}(S)$. □

It is a well-known fact that maximality is a local condition:

Lemma 2.43. *A G-extension R of S is maximal if and only if the G-extension $R \otimes_S S_\mathfrak{p}$ of $S_\mathfrak{p}$ is maximal for every maximal ideal $\mathfrak{p}$ of S.*

Proof. $\Rightarrow$ If $R' \supsetneq R$ is a larger G-extension, then $R' \otimes_S S_\mathfrak{p} \supsetneq R \otimes_S S_\mathfrak{p}$ for some maximal ideal $\mathfrak{p}$.

$\Leftarrow$ Assume that for some $\mathfrak{p}$, there is a larger G-extension $R'_\mathfrak{p} \supsetneq R \otimes_S S_\mathfrak{p}$. Interpret $R \otimes_S S_\mathfrak{q}$ and $R'_\mathfrak{p}$ as subsets of $R \otimes_S K$. Let $R' = R'_\mathfrak{p} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} R \otimes_S S_\mathfrak{q}$. It follows that $R' \otimes_S S_\mathfrak{p} = R'_\mathfrak{p}$ (Take any $x \in R'_\mathfrak{p}$ and again consider the ideal $0 \neq J_x = \{z \in S \mid xz \in S\} \subseteq S$. Let $J_x = \mathfrak{p}^k J'$ where $J' \subseteq S$ is an ideal coprime to $\mathfrak{p}$. Pick $b \in J' \backslash \mathfrak{p}$ and let $a = xb$. Then, $J_a \supseteq \mathfrak{p}^k$, so $J_a \backslash \mathfrak{q} \neq \varnothing$ for any maximal ideal $\mathfrak{q} \neq \mathfrak{p}$. Therefore, $a \in R'_\mathfrak{p} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} R \otimes_S S_\mathfrak{q} = R'$. Since $b \in S \backslash \mathfrak{p}$, it follows that $x = \frac{a}{b} \in R' \otimes_S S_\mathfrak{p}$.) and $R' \otimes_S S_\mathfrak{q} = R \otimes_S S_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$. Then, you can show that $R' \supsetneq R$ is again a G-extension. □

You can furthermore show that closedness and maximality hold over a local ring $\mathbb{Z}_{(p)}$ if and only if they hold over its completion $\mathbb{Z}_p$.

2.5 Decomposition of $\mathcal{H}$

To simplify the parametrization in Theorem 2.13 for nondegenerate extensions, we will use the following simple idea: Find a projection $f : \mathcal{H} \to W$ to a lower-dimensional $K[G]_1^\times$-representation so that its restriction to the orbit $\mathcal{P}^{\text{nondeg}}(K^{\text{sep}})$ is injective. Checking injectivity is (in principle) easy: It is equivalent to the assumption that the stabilizer in $K^{\text{sep}}[G]_1^\times$ of $f(\pi) \in W$ equals the stabilizer G of $\pi \in \mathcal{H}$.

We will now facilitate finding a good projection W by decomposing $\mathcal{H}$ into smaller $K[G]_1^\times$-representations.

Throughout this section, we assume that the characteristic of K does not divide the order of G, so that every representation of G defined over K is semisimple.

In the appendix, you can find the list of irreducible summands of the $K[G]_1^\times$-subrepresentation of $\mathcal{H}$ generated by $\mathcal{P}^{\text{nondeg}}(K)$, for certain finite groups G.

Let $\mathcal{C} = \mathcal{C}(K)$ be the set of irreducible representations of G over K (up to isomorphism). We denote the trivial onedimensional representation by $\mathrm{triv} \in \mathcal{C}$.

For any irreducible representation $V \in \mathcal{C}$, let $D(V)$ be the division ring such that $V \cong D(V)^{\deg(V)}$ and let $\mathrm{End}(V) \cong M_{\deg(V)}(D(V))$ be the ring of right $D(V)$-linear maps $V \to V$. The Artin–Wedderburn Theorem states that $K[G]$ is the product of these matrix algebras:

$$K[G] \cong \prod_{V \in \mathcal{C}} \mathrm{End}(V)$$

The action of the finite group G on V factors through the canonical left action of the matrix group $\mathrm{Aut}(V) = \mathrm{End}(V)^\times = \mathrm{GL}_{\deg(V)}(D(V))$:

$$G \hookrightarrow K[G]^\times \twoheadrightarrow \mathrm{Aut}(V) \circlearrowright V$$

We will often consider V a representation of not only the finite group G, but also of the group $K[G]^\times$.

Warning 2.44. Let $K = \mathbb{Q}$ and $G = \{e, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$. We then have an isomorphism $K[G] \cong K \times K$ where the first factor corresponds to the trivial representation triv and the second factor corresponds to the nontrivial representation sgn. The action of $(a, b) \in K^\times \times K^\times = K[G]^\times$ on triv is given by $(a, b).x = ax$ and the action on sgn is given by $(a, b).x = bx$. Note that $\mathrm{sgn} \otimes \mathrm{sgn} \ncong \mathrm{triv}$ as representations of $K[G]^\times$: the action on $\mathrm{sgn} \otimes \mathrm{sgn}$ is given by $(a, b).x = b^2 x$.

The subgroup $K[G]_1^\times$ consists of those elements of $K[G]^\times$ that project to $1 \in K^\times \cong \mathrm{Aut}(\mathrm{triv})$.

Now, clearly

$$\begin{aligned} \mathcal{H} &= \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G]) \\ &\cong \bigoplus_{V_1, V_2, W \in \mathcal{C}} \mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)). \end{aligned}$$

For any three irreducible representations V_1, V_2, W of G, write

$$m(V_1 \otimes V_2 \leftrightarrows W)$$

for the projection of $m \in \mathcal{H}$ to

$$\mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)).$$

We will now describe how to further decompose each of these summands.

2.5.1 Over sufficiently large base fields

Let us first assume that the division rings are $D(V) = K$ for all $V \in \mathcal{C}$, so $\mathrm{End}(V) = M_{\deg(V)}(K)$ and $V = K^{\deg(V)}$. (In other words, all irreducible representations of G over K stay irreducible over $\overline{K}$.)

Now, the space $\mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W))$ can be interpreted as the tensor product of the space of G-invariant K-linear maps $V_1 \otimes V_2 \to W$ and the space of (not necessarily G-invariant) K-linear maps $W \to V_1 \otimes V_2$. The idea is that the space of K-linear maps is

$$\begin{aligned} &\mathrm{Hom}_K(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)) \\ \cong\ &\mathrm{End}(V_1)^* \otimes \mathrm{End}(V_2)^* \otimes \mathrm{End}(W) \\ \cong\ &(V_1 \otimes V_1^*) \otimes (V_2 \otimes V_2^*) \otimes (W^* \otimes W) \\ \cong\ &(V_1^* \otimes V_2^* \otimes W) \otimes (W^* \otimes V_1 \otimes V_2) \\ \cong\ &\mathrm{Hom}_K(V_1 \otimes V_2 \to W) \otimes \mathrm{Hom}_K(W \to V_1 \otimes V_2). \end{aligned}$$

Now, recall that we are interested in *left* G-invariant maps $\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)$. They correspond to tensors in which the *first* tensor factor $V_1 \otimes V_2 \to W$ is G-invariant.

On the other hand, we considered the *right* action of $K[G]^\times$ on $K[G]$ (and hence $\mathrm{End}(V_1)$, $\mathrm{End}(V_2)$, and $\mathrm{End}(W)$). This means that it translates to an action on the *second* tensor factor $W \to V_1 \otimes V_2$.

When explicitly writing down a convenient isomorphism, we will make use of the following small lemma.

Lemma 2.45. *If the characteristic of K doesn't divide the order of G, then the characteristic of K doesn't divide the degree of any irreducible representation V of G over K.*

Remark 2.46. The lemma immediately follows from the fact that the degree of V divides the order of G: This is true in characteristic zero according to [29, Section 6.5, Corollary 2] and then translates to any characteristic not dividing $|G|$ by [29, Section 15.5].

However, we don't need these strong statements. Here is an easier proof:

Proof. Assume that $\mathrm{char}(K) \mid \deg(V)$, so the image of $\deg(V)$ in K is zero.

Now, let us recall the following well-known application of Schur's Lemma: If $f : G \to K$ is any class function, then the G-invariant map $V \to V$ given by $v \mapsto \sum_{g \in G} f(g)gv$ must be some multiple of the identity, say $\lambda \cdot \mathrm{id}_V$ for $\lambda \in K$. Computing the trace, we conclude that

$$\sum_{g \in G} f(g)\chi_V(g) = \lambda \cdot \deg(V) = 0 \text{ in } K,$$

where $\chi_V : G \to K$ is the character of the representation V. On the other hand, we have

$$\sum_{g \in G} \chi_V(g^{-1})\chi_V(g) = |G| \neq 0 \text{ in } K,$$

since V is irreducible. □

Theorem 2.47. *For any $V_1, V_2, W \in \mathcal{C}$, the map*

$$\begin{array}{c} \mathrm{Hom}_G(V_1 \otimes V_2 \to W) \otimes \mathrm{Hom}_K(W \to V_1 \otimes V_2) \\ \big\downarrow \varphi \\ \mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)) \end{array}$$

given by

$$\begin{array}{c} p \otimes t \\ \big\downarrow \\ A_1 \otimes A_2 \mapsto \frac{\deg(V_1)\deg(V_2)}{\deg(W)|G|} \cdot p \circ (A_1 \otimes A_2) \circ t \end{array}$$

is an isomorphism of K-vector spaces. (Here, we wrote $\frac{\deg(V_1)\deg(V_2)}{\deg(W)|G|} \cdot p \circ (A_1 \otimes A_2) \circ t$ for the map in $\mathrm{End}(W)$ that sends $w \in W$ to $\frac{\deg(V_1)\deg(V_2)}{\deg(W)|G|} \cdot p((A_1 \otimes A_2)t(w)) \in W$.)

$$V_1 \otimes V_2 \underset{K\text{-linear map } t}{\overset{K[G]\text{-linear map } p}{\rightleftarrows}} W$$

The action of $K[G]^\times$ is given by

$$\lambda.(p \otimes t) = p \otimes ((\lambda \otimes \lambda) \circ t \circ \lambda^{-1}),$$

where we interpret $\lambda \in K[G]^\times$ as an element of $\mathrm{Aut}(V_1)$, $\mathrm{Aut}(V_2)$, and $\mathrm{Aut}(W)$.

Remark 2.48. The dimension h of the K-vector space $\mathrm{Hom}_G(V_1 \otimes V_2 \to W)$ is the multiplicity with which the irreducible representation W of G occurs in $V_1 \otimes V_2$. Fix a basis $p_1, \ldots, p_h$ of $\mathrm{Hom}_G(V_1 \otimes V_2 \to W)$. The lemma then means that elements of $\mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W))$ are in bijection with tuples $(t_1, \ldots, t_h)$ of elements of $\mathrm{Hom}_K(W \to V_1 \otimes V_2)$:

$$\mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)) \cong \mathrm{Hom}_K(W \to V_1 \otimes V_2)^{\oplus h}$$

The group $K[G]^\times$ acts on each summand $\mathrm{Hom}_K(W \to V_1 \otimes V_2)$ in the canonical way:

$$\lambda.t_i = (\lambda \otimes \lambda) \circ t_i \circ \lambda^{-1}.$$

If $h = 1$ and we have fixed the projection map $p = p_1$, we will often identify $\mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W))$ with $\mathrm{Hom}_K(W \to V_1 \otimes V_2)$. If $V_1 = \mathrm{triv}$ and $V_2 = W$, we will use the canonical isomorphism $p : V_1 \otimes V_2 \to W$. (Similarly, if $V_2 = \mathrm{triv}$ and $V_1 = W$.)

Remark 2.49. The representation $\mathrm{Hom}_K(W \to V_1 \otimes V_2)$ of $K[G]^\times$ is in general not irreducible: For example, if $V_1 = V_2 = V$ and $\dim(V) \geqslant 2$, we can decompose it as $\mathrm{Hom}_K(W \to \mathrm{Sym}^2(V)) \oplus \mathrm{Hom}_K(W \to \mathrm{Alt}^2(V))$. However, since each factor $\mathrm{Aut}(V) \cong \mathrm{GL}_{\deg(V)}(K)$ of $K[G]^\times$ is a matrix group over K, the theory of irreducible representations of Lie algebras presents an easy way of completely decomposing into irreducible representations of $K[G]^\times$.

Proof of the lemma. It is clear that the map is well-defined: the composition $p \circ (A_1 \otimes A_2) \circ t$ is K-linear and the map $\varphi(p \otimes t)$ is G-invariant:

$$\begin{aligned} p \circ (gA_1 \otimes gA_2) \circ t &= p \circ (g \otimes g) \circ (A_1 \otimes A_2) \circ t \\ &= g \circ p \circ (A_1 \otimes A_2) \circ t \end{aligned}$$

because p is G-invariant.

Next, let us construct the inverse map. Pick a basis $(e_{1,r_1})_{r_1}$ of V_1, a basis $(e_{2,r_2})_{r_2}$ of V_2, and a basis $(f_s)_s$ of W. Let $(e^*_{1,r_1})_{r_1}$, $(e^*_{2,r_2})_{r_2}$, $(f^*_s)_s$ be the respective dual bases of V_1^*, V_2^*, W^*.

Now, let $T : \mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)$ be a K-linear G-invariant map.

For any r_1, r_2, s, let $t_{r_1 r_2 s} = (e_{1,r_1} \otimes e_{2,r_2}) f^*_s \in \mathrm{Hom}_K(W \to V_1 \otimes V_2)$ and define $p_{r_1 r_2 s} \in \mathrm{Hom}_G(V_1 \otimes V_2 \to W)$ by

$$p_{r_1 r_2 s}(v_1 \otimes v_2) = \frac{\deg(W)|G|}{\deg(V_1)\deg(V_2)} \cdot T(v_1 e^*_{1,r_1} \otimes v_2 e^*_{2,r_2}) f_s$$

for $v_1 \otimes v_2 \in V_1 \otimes V_2$. Then, $p_{r_1 r_2 s}$ is K-linear and G-invariant because T is.

You can then show that $\widetilde{\varphi}(T) = \sum_{r_1, r_2, s} p_{r_1 r_2 s} \otimes t_{r_1 r_2 s}$ defines the inverse $\widetilde{\varphi}$ of φ. □

The isomorphisms given above combine to an isomorphism

$$\mathcal{H} \cong \bigoplus_{V_1, V_2, W \in \mathcal{C}} \mathrm{Hom}_G(V_1 \otimes V_2 \to W) \otimes \mathrm{Hom}_K(W \to V_1 \otimes V_2).$$

The following lemma explains what element of $\mathrm{Hom}_G(V_1 \otimes V_2 \to W) \otimes \mathrm{Hom}_K(W \to V_1 \otimes V_2)$ the trivial map $\pi \in \mathcal{H}$ projects to.

Lemma 2.50. *For any $V_1, V_2 \in \mathcal{C}$, fix a decomposition $V_1 \otimes V_2 \cong \bigoplus_{s \in S(V_1, V_2)} W_s$ into irreducible G-representations $W_s \in \mathcal{C}$ with projection maps $p_s : V_1 \otimes V_2 \twoheadrightarrow W_s$ and inclusion maps $\iota_s : W_s \hookrightarrow V_1 \otimes V_2$. Then, the element $\sum_{V_1, V_2 \in \mathcal{C}} \sum_{s \in S(V_1, V_2)} p_s \otimes \iota_s$ corresponds to the trivial element π of $\mathcal{H}$.*

Proof. The decomposition of $V_1 \otimes V_2$ gives rise to a decomposition of

$$\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \cong V_1^{\deg(V_1)} \otimes V_2^{\deg(V_2)} \cong (V_1 \otimes V_2)^{\deg(V_1)\deg(V_2)}.$$

(Separately decompose each pair of column spaces of the matrix rings $\mathrm{End}(V_1)$ and $\mathrm{End}(V_2)$.) Each pair of projection and inclusion maps $p_s, \iota_s : V_1 \otimes V_2 \rightleftarrows W_s$ corresponds to $\deg(V_1)\deg(V_2)$ projection and inclusion maps $\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \rightleftarrows W_s$. The element of $\mathcal{H}$ can be computed from the resulting maps $K[G] \otimes K[G] \rightleftarrows W_s$ and the following lemma then shows the claim. □

Lemma 2.51. *Fix a decomposition of G-representations $K[G] \otimes K[G] \cong \bigoplus_{s\in S} W_s$ with projection maps $p_s : K[G] \otimes K[G] \twoheadrightarrow W_s$ and inclusion maps $\iota_s : W_s \hookrightarrow K[G] \otimes K[G]$.*

For any $s \in S$, consider the element

$$f_s = \left[x \otimes y \mapsto \frac{1}{\deg(W_s)|G|} \cdot p_s \circ (x \otimes y) \circ \iota_s \right]$$

of $\mathrm{Hom}_G(K[G] \otimes K[G] \to \mathrm{End}(W_s))$. Then, the sum

$$F = \sum_{s\in S} f_s \in \bigoplus_{W\in\mathcal{C}} \mathrm{Hom}_G(K[G] \otimes K[G] \to \mathrm{End}(W)) \cong \mathcal{H}$$

is the trivial map $\pi \in \mathcal{H}$.

Proof. The crucial idea is to note that the sum is independent of the choice of decomposition $K[G] \otimes K[G] \cong \bigoplus_{s\in S} W_s$. We can therefore assume that each of the irreducible summands $\iota_s(W_s)$ is contained in one of the $|G|$ summands in $K[G] \otimes K[G] = \bigoplus_{h\in G} \Delta(K[G])(e \otimes h)$.

Since the element F of $\mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$ is G-invariant, it suffices to check that it sends $e \otimes e$ to e and $e \otimes g$ to 0 for $g \neq e$.

Firstly, putting $x = y = e$, the composition $p_s \circ \iota_s$ is always the identity, so $f_s(e \otimes e) = \frac{1}{\deg(W_s)|G|} \cdot \mathrm{id} \in \mathrm{End}(W_s)$. Any irreducible representation W occurs as a summand in $K[G]$ exactly $\deg(W)$ times and therefore $\deg(W)|G|$ times in $K[G] \otimes K[G] \cong \bigoplus_{h\in G} \Delta(K[G])(e \otimes h)$. Thus, $F(e \otimes e)$ maps to $\mathrm{id} \in \mathrm{End}(W)$ and hence $F(e \otimes e) = e \in K[G]$.

On the other hand, putting $x = e$ and $y = g \neq e$, observe that the intersection

$$\Delta(K[G])(e \otimes h) \cap (e \otimes g)\Delta(K[G])(e \otimes h)$$

is trivial for any $h \in G$. Thus, for each summand $U = \iota_s(W_s)$ in our decomposition of $K[G] \otimes K[G]$, the intersection $U \cap ((e \otimes g) \cdot U)$ is trivial. This means that the composition $p_s \circ (e \otimes g) \circ \iota_s$ must be zero for each of the projection/inclusion pairs (p_s, ι_s). Therefore, we indeed have $F(e \otimes g) = 0$. □

The unit, symmetry, and associativity conditions have convenient descriptions in terms of our decomposition.

As representations of G, we clearly have a canonical isomorphism $\mathrm{triv} \otimes V = V$. The unit condition (Cu) fixes the corresponding K-linear map $V \to \mathrm{triv} \otimes V = V$:

Lemma 2.52. *For $m \in \mathcal{H}$, the unit condition (Cu) is equivalent to*

$$\pi(\mathrm{triv} \otimes V \rightleftarrows V) = \mathrm{id} \otimes \mathrm{id} \qquad \textit{for all } V \in \mathcal{C}. \tag{Cu}$$

Proof. The image of $\sum_g g$ in $\mathrm{End}(V)$ is $|G| \cdot \mathrm{id}$ if $V = \mathrm{triv}$ and 0 otherwise. Therefore, the only summands contributing to $m(\sum_g g \otimes x)$ are those with $V_1 = \mathrm{triv}$ and $V_2 = W$. As $\mathrm{Hom}_G(\mathrm{triv} \otimes V \to V)$ is generated by the identity map, we can write $m(\mathrm{triv} \otimes V \rightleftarrows V) = \mathrm{id} \otimes t$ for some $t \in \mathrm{Hom}_K(V \to \mathrm{triv} \otimes V) = \mathrm{Hom}_K(V \to V)$. This corresponds to the map

$$A_1 \otimes A_2 \mapsto \frac{1}{|G|}(A_1 \otimes A_2) \circ t \in \mathrm{End}(V),$$

which sends $\sum_g g \otimes x$ to $x \circ t$. Hence, (Cu) is equivalent to $t = \mathrm{id}$. □

Lemma 2.53. *For $m \in \mathcal{H}$, the symmetry condition (Cs) is equivalent to*

$$m(V_1 \otimes V_2 \rightleftarrows W) = \mathrm{swap}(m(V_2 \otimes V_1 \rightleftarrows W)) \qquad \text{for all } V_1, V_2, W \in \mathcal{C}, \tag{Cs}$$

where swap *interchanges the two tensor factors corresponding to V_1 and V_2.*

To describe the associativity condition, we refer to Remark 2.14, which says that left and right associative compositions

$$K[G] \otimes K[G] \otimes K[G] \to K[G]$$

should coincide. We first decompose the space

$$\mathrm{Hom}_G(K[G] \otimes K[G] \otimes K[G] \to K[G]) = \bigoplus_{V_1, V_2, V_3, W} \mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \otimes \mathrm{End}(V_3) \to \mathrm{End}(W))$$

as before, and use the analogue of Theorem 2.47:

Lemma 2.54. *The map*

$$\begin{array}{c} \mathrm{Hom}_G(V_1 \otimes V_2 \otimes V_3 \to W) \otimes \mathrm{Hom}_K(W \to V_1 \otimes V_2 \otimes V_3) \\ \big\downarrow \\ \mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \otimes \mathrm{End}(V_3) \to \mathrm{End}(W)) \end{array}$$

given by

$$\begin{array}{c} p \otimes t \\ \big\downarrow \\ A_1 \otimes A_2 \otimes A_3 \mapsto \frac{\deg(V_1)\deg(V_2)\deg(V_3)}{\deg(W)|G|^2} \cdot p \circ (A_1 \otimes A_2 \otimes A_3) \circ t \end{array}$$

is an isomorphism of K-vector spaces.

$$V_1 \otimes V_2 \otimes V_3 \underset{K\text{-linear map } t}{\overset{K[G]\text{-linear map } p}{\rightleftarrows}} W$$

The action of $K[G]^\times$ is defined by

$$\lambda.(p \otimes t) = p \otimes ((\lambda \otimes \lambda \otimes \lambda) \circ t \circ \lambda^{-1}).$$

Then, the left associative composition can be computed as follows:

Lemma 2.55. *The left associative composition*

$$\text{left-ass}(m) \in \mathrm{Hom}_G(K[G] \otimes K[G] \otimes K[G] \to K[G])$$

of any $m \in \mathcal{H}$ is defined by

$$\text{left-ass}(m)(V_1 \otimes V_2 \otimes V_3 \leftrightarrows W) = \sum_{U \in \mathcal{C}} \text{left-ass}(m(V_1 \otimes V_2 \leftrightarrows U), m(U \otimes V_3 \leftrightarrows W)),$$

where the left associative composition of

$$p \otimes t \in \mathrm{Hom}_G(V_1 \otimes V_2 \to U) \otimes \mathrm{Hom}_K(U \to V_1 \otimes V_2)$$

and

$$p' \otimes t' \in \mathrm{Hom}_G(U \otimes V_3 \to W) \otimes \mathrm{Hom}_K(W \to U \otimes V_3)$$

is

$$\text{left-ass}(p \otimes t, p' \otimes t') = p'' \otimes t'' \in \mathrm{Hom}_G(V_1 \otimes V_2 \otimes V_3 \to W) \otimes \mathrm{Hom}_K(W \to V_1 \otimes V_2 \otimes V_3)$$

with

$$p'' = p' \circ (p \otimes \mathrm{id}_{V_3})$$

and

$$t'' = (t \otimes \mathrm{id}_{V_3}) \circ t'.$$

$$V_1 \otimes V_2 \otimes V_3 \underset{t \otimes \mathrm{id}_{V_3}}{\overset{p \otimes \mathrm{id}_{V_3}}{\rightleftarrows}} U \otimes V_3 \underset{t'}{\overset{p'}{\rightleftarrows}} W$$

The right associative composition is defined similarly.

2.5.2 Galois descent

In the previous section, we have described how to decompose $\mathcal{H}$ if K is sufficiently large for all irreducible representations of G over K to stay irreducible over $\overline{K}$. To decompose $\mathcal{H} = \mathcal{H}(K)$ for arbitrary base fields K (with $\mathrm{char}(K) \nmid |G|$), you can for example use the method of Galois descent. It is often not difficult to guess and then prove the correct decomposition without explicitly referring to Galois descent, though. In fact that is the path we will be taking in the later examples. This section is mostly included as a general reference.

The elements of $\mathcal{H}(K)$ are exactly the elements of $\mathcal{H}(\overline{K})$ fixed by $\mathrm{Gal}(\overline{K}|K)$.

If $V \in \mathcal{C}(\overline{K})$ are the irreducible representations of G over $\overline{K}$, let us first describe the action of $\mathrm{Gal}(\overline{K}|K)$ on $\overline{K}[G]$ and on $\mathcal{H}(\overline{K})$. The canonical action on $\overline{K}[G]$ often does not correspond to the canonical (factor-wise) action on $\prod_{V \in \mathcal{C}(\overline{K})} \mathrm{End}(V)$ and $\bigoplus_{V_1,V_2,W \in \mathcal{C}(\overline{K})} \mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W))$:

In general, the Galois group $\mathrm{Gal}(\overline{K}|K)$ permutes rows of the character table of G. Consider the corresponding action of $\mathrm{Gal}(\overline{K}|K)$ on $\mathcal{C}(\overline{K})$. For any $\sigma \in \mathrm{Gal}(\overline{K}|K)$, we can then find a corresponding isomorphism $P_{\sigma,V} : \sigma V \to V$ of vector spaces over $\overline{K}$ such that $P_{\sigma,V} g P_{\sigma,V}^{-1} = \sigma g \sigma^{-1}$ for each $g \in G$. This isomorphism is unique up to scaling.

Then, σ sends an element $A \in \mathrm{End}(V) \subseteq \overline{K}[G]$ to $\sigma.A = P_{\sigma,V}^{-1} \sigma(A) P_{\sigma,V} \in \mathrm{End}(\sigma V) \subseteq \overline{K}[G]$.

Similarly, σ sends an element $t \in \mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(W)) \subseteq \mathcal{H}(\overline{K})$ to $\sigma.t \in \mathrm{Hom}_G(\mathrm{End}(\sigma V_1) \otimes \mathrm{End}(\sigma V_2) \to \mathrm{End}(\sigma W)) \subseteq \mathcal{H}(\overline{K})$ given by

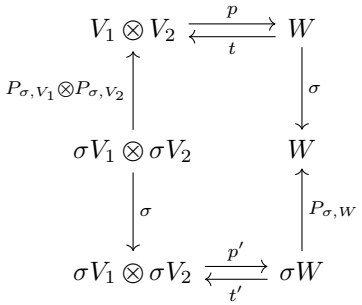
$$(\sigma.t)(A_1 \otimes A_2) = P_{\sigma,W}^{-1} \sigma \left[t \left[(P_{\sigma,V_1} \sigma^{-1}(A_1) P_{\sigma,V_1}^{-1}) \otimes (P_{\sigma,V_2} \sigma^{-1}(A_2) P_{\sigma,V_2}^{-1}) \right] \right] P_{\sigma,W}.$$

Under the isomorphism in Theorem 2.47, this means that

$$\sigma.(p \otimes t) = p' \otimes t'$$

where

$$p' = P_{\sigma,W}^{-1} \circ \sigma(p \circ (P_{\sigma,V_1} \otimes P_{\sigma,V_2})),$$
$$t' = \sigma((P_{\sigma,V_1}^{-1} \otimes P_{\sigma,V_2}^{-1}) \circ t) \circ P_{\sigma,W}.$$



Example 2.56. Let $G = C_n$ be the cyclic group of order n, generated by τ. Then, the (one-dimensional) irreducible representations of G over $\overline{K}$ are the spaces $V_0, \dots, V_{n-1}$ with $V_i = \overline{K}$ and the action of G given by $\tau.v = \zeta_n^i v$ for $v \in V_i$.

The action of $\mathrm{Gal}(\overline{K}|K)$ on $V_0, \dots, V_{n-1}$ is given by $\sigma V_i = V_{ri}$ when $\sigma(\zeta_n) = \zeta_n^r$. For $P_{\sigma,V}$, we can without loss of generality pick the identity map $\overline{K} \to \overline{K}$. Then, σ sends an element $\lambda_i \in \mathrm{End}(V_i) = \overline{K}$ to $\sigma.\lambda_i = \sigma(\lambda_i) \in \mathrm{End}(\sigma V_i) = \overline{K}$.

An element $(\lambda_i)_i$ of $\overline{K}[G] \cong \prod_i \overline{K}$ therefore turns out to be fixed by $\mathrm{Gal}(\overline{K}|K)$ if and only if $\lambda_0, \dots, \lambda_{n-1} \in K(\zeta_n)$ and $\lambda_{ri} = \sigma(\lambda_i)$ for each $\sigma \in \mathrm{Gal}(K(\zeta_n)|K)$ with $\sigma(\zeta_n) = \zeta_n^r$. For example, if $K = \mathbb{Q}$, this corresponds to the natural decomposition $\mathbb{Q}[G] \cong \prod_{d|n} \mathbb{Q}(\zeta_d)$.

For any i, j, we have $V_i \otimes V_j \cong V_{i+j}$ (the obvious identity map $\overline{K} \otimes \overline{K} \cong \overline{K}$ is an isomorphism). Let $V_{i,j} = \mathrm{Hom}_{\overline{K}}(V_{i+j} \to V_i \otimes V_j) \cong \overline{K}$. We therefore have

$$\mathcal{H}(\overline{K}) \cong \bigoplus_{i,j} V_{i,j}.$$

Any $\sigma \in \mathrm{Gal}(\overline{K}|K)$ sends $v \in V_{i,j} = \overline{K}$ to $\sigma.v = \sigma(v) \in V_{ri,rj} = \overline{K}$ where $\sigma(\zeta_n) = \zeta_n^r$ as above.

An element $(v_{i,j})_{i,j}$ of $\mathcal{H}(\overline{K}) \cong \bigoplus_{i,j} V_{i,j}$ is therefore fixed by $\mathrm{Gal}(\overline{K}|K)$ if and only if $v_{i,j} \in K(\zeta_n)$ and $v_{ri,rj} = \sigma(v_{i,j})$ for all i, j and all $\sigma \in \mathrm{Gal}(K(\zeta_n)|K)$ with $\sigma(\zeta_n) = \zeta_n^r$.

An element $(\lambda_i)_i \in K[G]^\times$ acts on $(v_{i,j})_{i,j} \in \mathcal{H}(K)$ as $(\lambda_i)_i.(v_{ij})_{i,j} = (\frac{\lambda_i \lambda_j}{\lambda_{i+j}} \cdot v_{i,j})_{i,j}$.

2.6 Discriminants

Our goal in this section is to compute the discriminant of a G-extension R of S in terms of the corresponding element m of $\mathcal{P}_I(S)$. Let $\mathrm{triv} : K[G] \to K$ be the map $\sum_g a_g g \mapsto \sum_g a_g$. We will show that this corresponds to the trace map $R \otimes_S K \to K$.

Definition 2.57. For any $m \in \mathcal{P}(K)$, we call

$$\mathrm{disc}(m) = \det((\mathrm{triv} \circ m(a \otimes b))_{a,b \in G})$$

the *discriminant of* m.

We define discriminants and indices as usual:

Let R be a G-extension of S. If S is a principal ideal domain, then R is a free S-module. Let $\alpha_1, \dots, \alpha_n$ be a basis. The *discriminant of* R is then

$$\mathrm{disc}(R) = \det((\mathrm{Tr}(\alpha_i \alpha_j))_{1 \leqslant i,j \leqslant n}).$$

This is well-defined up to multiplication by elements of $S^{\times 2}$. If S is an arbitrary Dedekind domain, the discriminant of R is the ideal of S generated by the determinants of matrices $\det((\mathrm{Tr}(\alpha_i \alpha_j))_{i,j})$ where $\alpha_1, \dots, \alpha_n \in R$.

Let I be a full ideal of $S[G]$. If S is a principal ideal domain, we define the *index* $[S[G] : I]$ as the

determinant of any matrix sending a basis of $S[G]$ to a basis of I. (This index is well-defined up to multiplication by elements of $S^\times$.) If S is an arbitrary Dedekind domain, we define the index $[S[G] : I]$ to be the fractional ideal of S generated by determinants of matrices sending a basis of $S[G]$ to elements of I.

For any unitary full ideal I and any $m \in \mathcal{P}(K)$, we call

$$\mathrm{disc}_I(m) = [S[G] : I]^2 \cdot \mathrm{disc}(m)$$

the *discriminant of m with respect to I*.

Of course, $\mathrm{disc}(m) = \mathrm{disc}_{S[G]}(m)$.

Lemma 2.58. *Let R be the G-extension of S corresponding to $m \in \mathcal{P}_I(S)$. Then, the discriminant of R is*

$$\mathrm{disc}(R) = \mathrm{disc}_I(m).$$

Proof. The trace map $\mathrm{Tr} = \mathrm{Tr}_R : R \otimes_S K \to K$ corresponds to a map $\mathrm{Tr}_{K[G]} : K[G] \to K$.

For any $a, b \in G$, write $m(a \otimes b) = \sum_{c \in G} t_{a,b,c} c$. The G-invariance of m means that $t_{ga,gb,gc} = t_{a,b,c}$ for all $g, a, b, c \in G$. Now, the unit condition (Cu) implies that $\sum_{a \in G} t_{a,e,e} = 1$. Then,

$$\mathrm{Tr}_{K[G]}(h) = \sum_{g \in G} t_{h,g,g} = \sum_{g \in G} t_{g^{-1}h,e,e} = 1 \qquad \text{for all } h \in G.$$

Hence, $\mathrm{Tr}_{K[G]}(a) = \mathrm{triv}(a)$ for all $a \in K[G]$. The claim then follows by performing a change of basis from $K[G]$ to I, since by definition

$$\mathrm{disc}(R) = [S[G] : I]^2 \cdot \det((\mathrm{Tr}_{K[G]}(m(a \otimes b)))_{a,b \in G}) = \mathrm{disc}_I(m). \qquad \square$$

Assuming that $\mathrm{char}(K) \nmid |G|$, we can also express the discriminant in terms of the decomposition of $\mathcal{H}$ given in section 2.5. For any irreducible representation V of G over $\overline{K}$, identify elements of $V \otimes V^*$ with endomorphisms of V. Denote by $\mathrm{tr} : V \otimes V^* \to \overline{K} = \mathrm{triv}$ and $\det : V \otimes V^* \to \overline{K}$ the trace and determinant maps. Up to scaling, tr is the only G-invariant linear map $V \otimes V^* \to \mathrm{triv}$. We can therefore write any element f of $\mathrm{Hom}_G(\mathrm{End}(V) \otimes \mathrm{End}(V^*) \to \mathrm{End}(\mathrm{triv})) \cong \mathrm{Hom}_G(V \otimes V^* \to \mathrm{triv}) \otimes \mathrm{Hom}_{\overline{K}}(\mathrm{triv} \to V \otimes V^*)$ as $f = \frac{\mathrm{tr}}{\dim(V)} \otimes t$ for some $t \in \mathrm{Hom}_{\overline{K}}(\mathrm{triv} \to V \otimes V^*) \cong V \otimes V^*$. Then, let $\det(f) = \det(t)$.

Theorem 2.59. *If the characteristic of K does not divide the order of G, then*

$$\mathrm{disc}(m) = \prod_{V \in \mathcal{C}(\overline{K})} \det(m(V \otimes V^* \leftrightarrows \mathrm{triv}))^{\dim(V)}$$

for any $m \in \mathcal{P}(K)$.

Proof. First, note that the function $\mathrm{triv} \circ m : K[G] \otimes K[G] \to K$ can be interpreted as

$$\mathrm{triv} \circ m = \sum_{V_1, V_2 \in \mathcal{C}(\overline{K})} m(V_1 \otimes V_2 \rightleftarrows \mathrm{triv}).$$

Now, a summand

$$\mathrm{Hom}_G(\mathrm{End}(V_1) \otimes \mathrm{End}(V_2) \to \mathrm{End}(\mathrm{triv})) \cong \mathrm{Hom}_G(V_1 \otimes V_2 \to \mathrm{triv}) \otimes \mathrm{Hom}_{\overline{K}}(\mathrm{triv} \to V_1 \otimes V_2)$$

of $\mathcal{H}(\overline{K})$ is nonzero if and only if triv occurs as a summand in $V_1 \otimes V_2$. This means the representations

V_1 and V_2 of G are dual: $V_1 \cong V_2^*$. Hence,

$$\mathrm{triv} \circ m = \sum_{V \in \mathcal{C}(\overline{K})} m(V \otimes V^* \rightleftarrows \mathrm{triv}).$$

For each $V \in \mathcal{C}(\overline{K})$, fix a basis of V and the corresponding dual basis of V^*. This induces the basis $(E^V_{r,s})_{1 \leqslant r,s \leqslant \dim(V)}$ of $\mathrm{End}(V)$ of elementary matrices and a dual basis $(E^{V^*}_{r',s'})_{r',s'}$ of $\mathrm{End}(V^*)$. Note that

$$K[G] \cong \bigoplus_{V \in \mathcal{C}(\overline{K})} \mathrm{End}(V) \cong \bigoplus_{V \in \mathcal{C}(\overline{K})} \mathrm{End}(V^*).$$

Write $m(V \otimes V^* \rightleftarrows \mathrm{triv}) = \frac{\mathrm{tr}}{\dim(V)} \otimes t^V$ with $t^V \in V \otimes V^* \cong \mathrm{End}(V)$. According to the construction of our decomposition of $\mathcal{H}(\overline{K})$, we get

$$\mathrm{triv} \circ m(E^V_{r,s} \otimes E^{V^*}_{r',s'}) = \frac{\dim(V)}{|G|} \cdot \mathrm{tr}(E^V_{r,s} t^V E^V_{s',r'}) = \begin{cases} \frac{\dim(V)}{|G|} \cdot t^V_{s,s'}, & r = r', \\ 0, & r \neq r'. \end{cases}$$

Therefore, the $|G| \times |G|$-matrix $(\mathrm{triv} \circ m(E^V_{r,s} \otimes E^{V^*}_{r',s'}))_{V,r,s,r',s'}$ is a block diagonal matrix in which the block $\frac{\dim(V)}{|G|} t^V$ occurs $\dim(V)$ times for each $V \in \mathcal{C}(\overline{K})$. Its determinant is therefore

$$\prod_{V \in \mathcal{C}(\overline{K})} \det\left(\frac{\dim(V)}{|G|} t^V\right)^{\dim(V)}.$$

We have performed changes of basis of $K[G]$ (independent of m) that transformed the matrix $(\mathrm{triv} \circ m(a \otimes b))_{a,b \in G}$ into the matrix $(\mathrm{triv} \circ m(E^V_{r,s} \otimes E^{V^*}_{r',s'}))_{V,r,s,r',s'}$. This shows that the identity

$$\mathrm{disc}(m) = \prod_{V \in \mathcal{C}(\overline{K})} \det(m(V \otimes V^* \leftrightarrows \mathrm{triv}))^{\dim(V)}$$

is true up to some multiplicative constant. It therefore suffices to show that both sides agree for $m = \pi$. We then have $\mathrm{disc}(m) = 1$ and $t^V = \mathrm{id}_V$ for all V, since $\frac{\mathrm{tr}}{\dim(V)}$ and id_V are corresponding projection and inclusion maps $V \otimes V^* \rightleftarrows \mathrm{triv}$. □

More generally, consider a subgroup $H \subseteq G$. A basis of the S-module $S[G]^H$ is $(\sum_{h \in H} hg)_{[g] \in H \backslash G}$.

Definition 2.60. For any $m \in \mathcal{P}(K)$, we call

$$\mathrm{disc}^H(m) = \det\big(\big(\sum_{h \in H} \mathrm{triv} \circ m(a \otimes hb)\big)_{[a],[b] \in H \backslash G}\big)$$

the *H-discriminant of m*.

For any unitary full ideal I and any $m \in \mathcal{P}(K)$, we call

$$\mathrm{disc}^H_I(m) = \big[S[G]^H : I^H\big]^2 \cdot \mathrm{disc}^H(m)$$

the *H-discriminant of m with respect to I*.

Computations similar to the above then show the following two results.

Lemma 2.61. *Let R be the G-extension of S corresponding to $m \in \mathcal{P}_I(S)$. Then, the discriminant of the subring fixed by a subgroup $H \subseteq G$ is*

$$\mathrm{disc}(R^H) = \mathrm{disc}^H_I(m).$$

Proof. Let $\mathrm{Tr}_R : R \otimes_S K \to K$ be the trace map in R and $\mathrm{Tr}_{R^H} : R^H \otimes_S K \to K$ be the trace map in R^H. For any $r \in R$, we have

$$\mathrm{Tr}_{R^H}\big(\sum_{h\in H} hr\big) = \mathrm{Tr}_R(r).$$

Let $\mathrm{Tr}_{K[G]} : K[G] \to K$ and $\mathrm{Tr}_{K[G]^H} : K[G]^H \to K$ be the corresponding trace maps in $K[G]$ and $K[G]^H$. We conclude that

$$\begin{aligned}\mathrm{Tr}_{K[G]^H}\big(m\big(\sum_{h_a\in H} h_a a \otimes \sum_{h_b\in H} h_b b\big)\big) &= \mathrm{Tr}_{K[G]^H}\big(\sum_{h_a\in H} h_a m\big(a \otimes \sum_{h_b\in H} h_b b\big)\big)\\ &= \mathrm{Tr}_{K[G]}\big(m\big(a \otimes \sum_{h\in H} hb\big)\big)\\ &= \mathrm{triv} \circ m\big(a \otimes \sum_{h\in H} hb\big).\end{aligned}$$

The result again follows by performing a change of basis from $K[G]^H$ to I^H. □

Theorem 2.62. *If the characteristic of K does not divide the order of G, then*

$$\mathrm{disc}^H(m) = \prod_{V\in\mathcal{C}(\overline{K})} \det(m(V \otimes V^* \leftrightarrows \mathrm{triv}))^{\dim(V^H)}$$

for any $m \in \mathcal{P}(K)$.

Proof. This follows from a computation similar to the proof of Theorem 2.59. □

We can also describe the effect of the action of $K[G]_1^\times$ on discriminants. Denote by $\mathbb{I}_H^G = \mathrm{Ind}_H^G \mathrm{triv}$ the result of lifting the trivial representation of H to G via induction. This is the permutation representation for right cosets of H in G. For example, $\mathbb{I}_1^G$ is the regular representation reg of G. Then, $\langle \mathbb{I}_H^G, V\rangle = \dim(V^H)$ is the multiplicity with which V occurs in $\mathbb{I}_H^G$.

Lemma 2.63. *For any $m \in \mathcal{P}(K)$ and any $\lambda \in K[G]_1^\times$, we have*

$$\mathrm{disc}(\lambda.m) = \det(\mathrm{reg}(\lambda))^2 \cdot \mathrm{disc}(m)$$

and for all subgroups $H \subseteq G$, we have

$$\mathrm{disc}^H(\lambda.m) = \det(\mathbb{I}_H^G(\lambda))^2 \cdot \mathrm{disc}^H(m).$$

Proof. These facts are immediate consequences of the definition of $\mathrm{disc}(m)$ and $\mathrm{disc}^H(m)$. □

2.7 Ideal classes

Fix a Dedekind domain S with field of fractions K.

Let A be some (not necessarily commutative) S-algebra. Assume that A is a finitely generated torsion-free S-module. Write $A_K = A \otimes_S K$.

Definition 2.64. We call a left A-submodule I of A_K a *full ideal* of A (over S) if I is a finitely generated S-module and $I \otimes_S K = A_K$ (meaning $k_1 \cdot A \subseteq I \subseteq k_2 \cdot A$ for some $k_1, k_2 \in K^\times$). Two full ideals I, I' are called *equivalent* if $I' = I\lambda$ for some $\lambda \in A_K^\times$. For any full ideal I, we denote the set of $\lambda \in A_K^\times$ such that $I = I\lambda$ by $\mathrm{Aut}(I)$.

Let $\mathrm{Cl}(A) = \mathrm{Cl}_S(A)$ be the set of equivalence classes of full ideals of A.

We call A a *principal ideal ring* (over S) if all full ideals of A are equivalent.

Example 2.65. If A a Dedekind domain, then the full ideals of A are exactly the nonzero fractional ideals of A. Hence, $\mathrm{Cl}(A)$ is the class group of A.

For any finite group G, the Jordan–Zassenhaus Theorem (see [34]) implies that $\mathrm{Cl}_{\mathbb{Z}}(\mathbb{Z}[G])$ is finite.

For computing $\mathrm{Cl}(\mathbb{Z}[G])$ in specific examples, we roughly follow the proof in [34]. The following simple lemmas are sufficient for the groups studied in this thesis.

Lemma 2.66. *Let $A_1, \ldots, A_n$ be S-algebras as above. Then, the map*

$$\begin{aligned} \mathrm{Cl}(A_1) \times \cdots \times \mathrm{Cl}(A_n) &\longrightarrow \mathrm{Cl}(A_1 \times \cdots \times A_n) \\ (I_1, \cdots, I_n) &\longmapsto I_1 \times \cdots \times I_n \end{aligned}$$

is a bijection.

Lemma 2.67 (Similar to [34, pages 282f.])**.** *If A is a principal ideal ring, then the matrix ring $M_n(A)$ is also a principal ideal ring.*

Proof. Let I be a full ideal of $M_n(A)$. Consider the set $V \subseteq A_K^n$ of rows of elements of I. The fact that I is a left $M_n(A)$-module shows that V is a left A-module, and that I is the set of matrices whose elements lie in V. Our goal is now to construct some $\lambda \in \mathrm{GL}_n(A_K)$ such that $V\lambda = A^n$, so $I\lambda = M_n(A)$.

For $1 \leqslant i \leqslant n$, let $\iota_i : A_K \to A_K^n$ be the i-th inclusion map and let $p_i : A_K^n \to A_K$ be the i-th projection map. We will now inductively construct upper triangular matrices $\lambda_k \in \mathrm{GL}_n(A_K)$ for $0 \leqslant k \leqslant n$ such that $p_i(V\lambda_k) = A$ and $\iota_i(A) \subseteq V\lambda_k$ for all $1 \leqslant i \leqslant k$. For $k = 0$, we can of course take the identity matrix $\lambda_0 = I_n$. Assume we have constructed λ_{k-1} for some $1 \leqslant k \leqslant n$. The assumption that $I \subseteq M_n(A_K)$ is a full ideal of $M_n(A)$ implies that $p_k(V\lambda_{k-1}) \subseteq A_K$ is a full ideal of A. Since A is a principal ideal ring, there exists some $x_k \in A_K^\times$ with $p_k(V\lambda_{k-1}) = Ax_k$. Now, let $x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n \in A_K$ such that $(x_1, \ldots, x_n) \in V\lambda_{k-1}$. By the induction hypothesis, we have $(x_1, \ldots, x_{k-1}, 0, \ldots, 0) \in V\lambda_{k-1}$. Hence, $(0, \ldots, 0, x_k, \ldots, x_n) \in V\lambda_{k-1}$. We can then put $\lambda_k = \lambda_{k-1}\mu_k$ where $\mu_k \in \mathrm{GL}_n(A_K)$ is the identity matrix with the k-th row replaced by $(0, \ldots, 0, \frac{1}{x_k}, -\frac{x_{k+1}}{x_k}, \ldots, -\frac{x_n}{x_k})$, finishing the induction.

For $k = n$, we obtain $V\lambda_n = A^n$ and therefore $I\lambda_n = M_n(A)$. □

Assume we have computed $\mathrm{Cl}(B)$ for some ring B and want to compute $\mathrm{Cl}(A)$ for a subring of finite index. The following lemma explains how this can be achieved.

Lemma 2.68. *Let $A \subseteq B$ be S-algebras as above such that $kB \subseteq A$ for some non-zero-divisor $k \in S$. Define the set W of pairs (J, T) where J is a full ideal of B and T is a left A-submodule of J/kJ with $BT = J/kJ$. Call two such pairs (J, T) and (J', T') equivalent if there is an element $\lambda \in A_K^\times = B_K^\times$ such that $J\lambda = J'$ and $T\lambda = T'$.*

Then, we obtain a bijection between $\mathrm{Cl}(A)$ and the set of equivalence classes of elements $(J, T) \in W$. A full ideal I of A corresponds to the pair $(BI, I/kBI)$. Conversely, a pair (J, T) corresponds to the preimage of T under the projection map $J \to J/kJ$. The automorphism groups satisfy $\mathrm{Aut}(I) \subseteq \mathrm{Aut}(J)$.

Proof. This is a direct consequence of the fact that $kBI \subseteq AI = I$ for any $I \in \mathrm{Cl}(A)$. □

Remark 2.69. Fixing representatives $(J_i)_{i \in \mathcal{I}}$ of the equivalence classes of full ideals of B, we see that any element of W is equivalent to one of the form (J_i, T), and that two pairs (J_i, T) and $(J_{i'}, T')$ are equivalent if and only if $i = i'$ and $T\lambda = T'$ for some $\lambda \in \mathrm{Aut}(J_i)$.

Corollary 2.70. *Assume $\mathrm{Cl}(B)$ is finite and the ideal kS has finite index in S. Then, $\mathrm{Cl}(A)$ is finite and $\mathrm{Aut}(I)$ is a subgroup of finite index of $\mathrm{Aut}(J)$ for all $I \in \mathrm{Cl}(A)$ as above with $BI = J$.*

Proof. For any $J \in \mathrm{Cl}(B)$, the finite set $J/kJ \cong J \otimes_S (S/kS)$ has only finitely many left A-submodules T. The group $\mathrm{Aut}(J)$ acts on this finite set of submodules T of J/kJ. For any $I \in \mathrm{Cl}(A)$ with $BI = J$, the automorphism group $\mathrm{Aut}(I)$ is exactly the stabilizer of I. □

Example 2.71. Let $G = C_2 = \{e, \tau\}$ be the cyclic group of order two and let $S = \mathbb{Z}$. Then, the image of the canonical embedding $\mathbb{Z}[G] \subseteq \mathbb{Z} \times \mathbb{Z}$ is the set of pairs (a, b) such that $a \equiv b \mod 2$. The ring $\mathbb{Z}$ and hence the ring $\mathbb{Z} \times \mathbb{Z}$ is a principal ideal ring. We have $2(\mathbb{Z} \times \mathbb{Z}) \subseteq \mathbb{Z}[G]$, so each full ideal of $\mathbb{Z}[G]$ corresponds to a left $\mathbb{Z}[G]$-submodule T of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ such that $(\mathbb{Z} \times \mathbb{Z}) \cdot T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (in other words, T projects surjectively onto both factors), modulo the action of $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}) = \{\pm 1\} \times \{\pm 1\}$. There are exactly two (equivalence classes of) such modules:

- The module $\{(0,0), (1,0), (0,1), (1,1)\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ corresponding to the full ideal $\mathbb{Z} \times \mathbb{Z}$ of $\mathbb{Z}[G]$.
- The module $\{(0,0), (1,1)\} \subsetneq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ corresponding to the full ideal $\mathbb{Z}[G] = \{(a, b) \mid a \equiv b \mod 2\} \subsetneq \mathbb{Z} \times \mathbb{Z}$ of $\mathbb{Z}[G]$.

Remark 2.72. In Dirichlet domains, class groups are a purely global phenomenon: the localizations are always principal ideal domains. This is not the case in our more general situation: for example, the ring $\mathbb{Z}_2[C_2]$ still has two equivalence classes of full ideals.

2.8 Toy example: the cyclic group of order two

As a toy example, let us look at the cyclic group $G = C_2 = \{e, \tau\}$ of order two over the ring $S = \mathbb{Z}$ of integers. It is recommended to compare this example with the more general treatment of cyclic groups in Chapter 3.

Artin–Wedderburn decomposition of $\mathbb{Q}[G]$. We have an isomorphism $\mathbb{Q}[G] \cong \mathbb{Q} \times \mathbb{Q}$ sending e to $(1, 1)$ and τ to $(1, -1)$. Identify any element of $\mathbb{Q}[G]$ with the corresponding element of $\mathbb{Q} \times \mathbb{Q}$. The first factor corresponds to the trivial representation, the second factor corresponds to the sign representation.

The image of the embedding $\mathbb{Z}[G] \subseteq \mathbb{Z} \times \mathbb{Z}$ is the set of pairs $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $a \equiv b \mod 2$. There are two equivalence classes of unitary full ideals of $\mathbb{Z}[G]$: one represented by the ideal

$$I_1 = \mathbb{Z}[C_2] = e\mathbb{Z} \oplus \tau\mathbb{Z} \cong \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \mod 2\}$$

and another represented by the ideal

$$I_2 = (e + \tau)\mathbb{Z} \oplus \frac{e - \tau}{2}\mathbb{Z} \cong 2\mathbb{Z} \times \mathbb{Z}.$$

Both ideals $I = I_1, I_2$ have index $[\mathbb{Z}[G] : I] = 1$.

Decomposition of $\mathcal{H}$. The tensor products of the irreducible representations of G are as follows:

$\otimes$	triv	sgn
triv	triv	sgn
sgn	sgn	triv

As we saw in Section 2.5, $\mathcal{H}$ is isomorphic to the direct sum of the following representations of $\mathbb{Q}[G]^\times$:

- $\mathrm{Hom}_{\mathbb{Q}}(\mathrm{triv} \to \mathrm{triv} \otimes \mathrm{triv})$
- $\mathrm{Hom}_{\mathbb{Q}}(\mathrm{sgn} \to \mathrm{triv} \otimes \mathrm{sgn})$
- $\mathrm{Hom}_{\mathbb{Q}}(\mathrm{sgn} \to \mathrm{sgn} \otimes \mathrm{triv})$
- $\mathrm{Hom}_{\mathbb{Q}}(\mathrm{triv} \to \mathrm{sgn} \otimes \mathrm{sgn})$

Of course, each of those representations is one-dimensional and comes with a canonical identification with $\mathbb{Q}$. For an element $m \in \mathcal{H}$, let us denote the corresponding elements of $\mathbb{Q}$ by $v_{00}, v_{01}, v_{10}, v_{11}$, respectively.

The map $m : \mathbb{Q}[G] \otimes \mathbb{Q}[G] \to \mathbb{Q}[G]$ is defined as follows:

$$m((a,b) \otimes (a',b')) = \left(\frac{v_{00}aa' + v_{11}bb'}{2}, \frac{v_{01}ab' + v_{10}a'b}{2} \right).$$

The trivial extension corresponds to $v_{00} = v_{01} = v_{10} = v_{11} = 1$.

Conditions (Cu) and (Cs) are equivalent to $v_{00} = v_{01} = v_{10} = 1$. Condition (Ca) is automatically satisfied. Therefore,

$$\mathcal{P}(\mathbb{Q}) = \{(1,1,1,v_{11}) \mid v_{11} \in \mathbb{Q}\} \cong \mathbb{Q}.$$

The action of $\mathbb{Q}[G]_1^\times = 1 \times \mathbb{Q}^\times \cong \mathbb{Q}^\times$ on $\mathcal{P}(\mathbb{Q})$ is given by $\lambda.v_{11} = \lambda^2 v_{11}$. Thus, G-extensions of $\mathbb{Q}$ are in bijection with elements of $\mathbb{Q}$, modulo multiplication by elements of $\mathbb{Q}^{\times 2}$.

The discriminant of a G-extension of $\mathbb{Z}$ corresponding to v_{11} is v_{11}.

The closedness condition (Cc) is equivalent to $v \in 1 + 4\mathbb{Z}$ for type I_1 and equivalent to $v \in 4\mathbb{Z}$ for type I_2. Therefore,

$$\mathcal{P}_{I_1}(\mathbb{Z}) \cong 1 + 4\mathbb{Z}, \qquad \mathcal{P}_{I_2}(\mathbb{Z}) \cong 4\mathbb{Z}.$$

Furthermore, $\mathrm{Aut}_1(I_1) = \mathrm{Aut}_1(I_2) = 1 \times \mathbb{Z}^\times \cong \{\pm 1\}$ acts trivially on v_{11}.

The extension corresponding to $m \in \mathcal{P}_{I_1}(\mathbb{Z})$ or $m \in \mathcal{P}_{I_2}(\mathbb{Z})$ is nonmaximal if and only if there exists some nonzero $\lambda \in \mathbb{Z} \backslash \mathbb{Z}^\times$ such that $\lambda^{-1}.v = \frac{v}{\lambda^2} \in \mathcal{P}_{I_1}(\mathbb{Z}) \cup \mathcal{P}_{I_2}(\mathbb{Z})$.

We have thus recovered the well-known Theorem 1.3.

Chapter 3

Cyclic groups

Assume $G = C_n$ is a cyclic group of order n generated by τ. Let S be a Dedekind domain whose field of fractions K has characteristic not dividing n.

3.1 Decomposition

For any positive integer d and any ring T, let $T[\zeta_d] = \mathbb{Z}[\zeta_d] \otimes_{\mathbb{Z}} T$. (Note that this is often not an integral domain! For example, if $T = \mathbb{Z}_q$ is a local ring, it might be a product of local rings.) If T is a field, we alternatively write $T(\zeta_d)$.

Artin–Wedderburn decomposition of $K[G]$. We have an isomorphism $K[G] \cong \prod_{d|n} K(\zeta_d)$ sending τ to the tuple $(\zeta_d)_{d|n}$.

For $i \in \mathbb{Z}/n\mathbb{Z}$, denote by ρ_i the homomorphism $K[G] \to K(\zeta_n)$ sending τ to ζ_n^i.

For $r \in (\mathbb{Z}/n\mathbb{Z})^\times$, denote by σ_r the automorphism of $K(\zeta_n)$ sending ζ_n to ζ_n^r.

The maps $\rho_i : K[G] \to K(\zeta_n)$ combine to an isomorphism

$$K[G] \cong \prod_{i \in \mathbb{Z}/n\mathbb{Z}}{}' K(\zeta_n)$$

where the right-hand side is the set of tuples $(x_i)_i \in \prod_i K(\zeta_n)$ such that for all $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ and all $i \in \mathbb{Z}/n\mathbb{Z}$, we have $x_{ri} = \sigma_r(x_i)$. Note that this implies that $x_i \in K(\zeta_d)$ where we denote by d the size of the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by i.

The inverse map is

$$(x_i)_i \longmapsto \frac{1}{n} \sum_i \left(\sum_j x_j \zeta_n^{-ij} \right) \tau^i. \tag{3.1}$$

Decomposition of $\mathcal{H}$. For $i, j \in \mathbb{Z}/n\mathbb{Z}$, let $\lambda \in K[G]^\times$ act on the space $V_{i,j} := K(\zeta_n)$ by multiplication by $\frac{\rho_i(\lambda)\rho_j(\lambda)}{\rho_{i+j}(\lambda)}$.

Let $\bigoplus'_{i,j} V_{i,j}$ be the set of tuples $(v_{i,j})_{i,j}$ in $\bigoplus_{i,j} V_{i,j}$ such that $v_{ri,rj} = \sigma_r(v_{i,j})$ for all $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ and all $i, j \in \mathbb{Z}/n\mathbb{Z}$. Note that this condition implies that $v_{i,j} \in K(\zeta_d)$ where we denote by d the size of the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by i and j.

We can now construct a $K[G]^\times$-invariant isomorphism

$$\bigoplus_{i,j}{}' V_{i,j} \xrightarrow{\sim} \mathcal{H} = \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$$

as follows: send $(v_{i,j})_{i,j}$ to the G-invariant homomorphism m defined by

$$\rho_u(m(x \otimes y)) = \frac{1}{n} \sum_{\substack{i,j: \\ i+j=u}} \rho_i(x)\rho_j(y)v_{i,j} \in K(\zeta_n) \qquad \text{for all } u \text{ and all } x, y \in K[G]. \tag{3.2}$$

The inverse map $\mathcal{H} \to \bigoplus_{i,j}{}' V_{i,j}$ sends m to $(v_{i,j})_{i,j}$ with

$$\begin{aligned} v_{i,j} &= \sum_k \zeta_n^{-ik} \rho_{i+j}(m(\tau^k \otimes e)) \\ &= \frac{1}{n} \sum_{k,l} \zeta_n^{-ik-jl} \rho_{i+j}\left(m\left(\tau^k \otimes \tau^l\right)\right) \\ &= \frac{1}{n} \sum_{k,l} \zeta_n^{-ik-jl} \sum_u \rho_u\left(m\left(\tau^k \otimes \tau^l\right)\right). \end{aligned} \tag{3.3}$$

We will in the following identify elements $m \in \mathcal{H}$ with tuples $v = (v_{i,j})_{i,j} \in \bigoplus_{i,j}{}' V_{i,j}$.

Remark 3.1. The trivial map $\pi \in \mathcal{H}$ corresponds to the tuple $(1)_{i,j} \in \bigoplus_{i,j}{}' V_{i,j}$. Let $v = (v_{i,j})_{i,j} \in \mathcal{P}^{\mathrm{nondeg}}(K)$. According to Corollary 2.35, there exists some $\alpha \in K^{\mathrm{sep}}[G]_1^\times$ such that $v = \alpha.\pi$, so

$$v_{i,j} = \frac{\rho_i(\alpha)\rho_j(\alpha)}{\rho_{i+j}(\alpha)} \qquad \text{for all } i, j.$$

The numbers $v_{i,j} \in K(\zeta_n)$ are therefore all invertible for nondegenerate extensions.

For any i,

$$\rho_i(\alpha^n) = \prod_j \frac{\rho_i(\alpha)\rho_j(\alpha)}{\rho_{i+j}(\alpha)} = \prod_j v_{i,j} \in K(\zeta_n)^\times,$$

which means that $\beta := \alpha^n$ lies in $K[G]_1^\times$ and is independent of the choice of α. Note that

$$v_{i,j}^n = \frac{\rho_i(\beta)\rho_j(\beta)}{\rho_{i+j}(\beta)}.$$

3.2 Equations

The unit, symmetry, and associativity conditions for $v = (v_{i,j})_{i,j} \in \mathcal{H}$ (see Theorem 2.13) are as follows:

$$v_{0,i} = 1 \qquad \text{for all } i, \tag{Cu}$$

$$v_{j,i} = v_{i,j} \qquad \text{for all } i, j, \tag{Cs}$$

$$v_{i,j}v_{i+j,k} = v_{j,k}v_{i,j+k} \qquad \text{for all } i, j, k. \tag{Ca}$$

Remark 3.2. Assuming (Cu) and (Cs), it suffices to check (Ca) only for $1 \leqslant i < k \leqslant n-1$ and $j \neq 0$. Due to the condition that $\sigma_r(v_{i,j}) = v_{ri,rj}$, you in fact only need to check it for one such tuple $(i, j, k) \in (\mathbb{Z}/n\mathbb{Z})^3$ in each orbit of the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Remark 3.3. For any tuple $(v_{i,j})_{i,j} \in \bigoplus'_{i,j} V_{i,j}$ satisfying (Cu) and (Cs), we have

$$v_{i,j} \in \begin{cases} \{1\}, & \text{if } i \text{ or } j = 0, \\ K(\zeta_d + \zeta_d^{-1}), & \text{if } i = -j, \\ K(\zeta_d), & \text{always.} \end{cases}$$

where d is the size of the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by i and j.

Proof. We have already seen that $v_{i,j} \in K(\zeta_d)$. If $i = 0$ or $j = 0$, then $v_{i,j} = 1$ clearly follows from (Cu) and (Cs). If $i = -j$, then $\sigma_{-1}(v_{i,j}) = v_{j,i} = v_{i,j}$ implies that $v_{i,j} \in K(\zeta_d + \zeta_d^{-1})$. □

The discriminant of $m = (v_{i,j})_{i,j} \in \mathcal{P}(K)$ is (use Theorem 2.59 over the separable closure of K or directly compute the discriminant by hand)

$$\operatorname{disc}(m) = \prod_i v_{i,-i}. \tag{3.4}$$

More generally, if $H = \langle \tau^h \rangle \subseteq G$, the H-discriminant of $m = (v_{i,j})_{i,j} \in \mathcal{P}(K)$ is

$$\operatorname{disc}^H(m) = \prod_{\substack{i: \\ ih \equiv 0 \bmod n}} v_{i,-i}.$$

The simple (purely multiplicative) structure of the variety $\mathcal{P}^{\text{nondeg}}$ allows us to understand its points. Let us first show some examples where $\mathcal{P}^{\text{nondeg}}$ can be described in particularly simple form.

Example 3.4 ($n = 2$)**.** The only variable $v_{i,j}$ not fixed by (Cu) and (Cs) is $v_{11} \in K(\zeta_2) = K$. The associativity equation (Ca) is then automatically satisfied.

$v_{i,j}$	0	1
0	1	1
1	1	v_{11}

We hence have a bijection $\mathcal{P}(K) \cong K$ sending v to v_{11}. It restricts to a bijection $\mathcal{P}^{\text{nondeg}}(K) \cong K^\times$. The discriminant is

$$\operatorname{disc}(m) = v_{11}.$$

Example 3.5 ($n = 3$)**.** The variables $v_{i,j}$ can be computed from $v_{11} \in K(\zeta_3)$ as follows:

$v_{i,j}$	0	1	2
0	1	1	1
1	1	v_{11}	$v_{11}\sigma_2(v_{11})$
2	1	$v_{11}\sigma_2(v_{11})$	$\sigma_2(v_{11})$

We have a bijection $\mathcal{P}(K) \cong K(\zeta_3)$ sending v to v_{11}. It restricts to a bijection $\mathcal{P}^{\text{nondeg}}(K) \cong K(\zeta_3)^\times$. The discriminant is

$$\operatorname{disc}(m) = v_{12}v_{21} = N_{K(\zeta_3)|K}(v_{11})^2.$$

Example 3.6 ($n = 4$)**.** If $v \in \mathcal{P}(K)$ is nondegenerate, the variables can be computed from $v_{13} \in K^\times$ and $v_{12} \in K(i)^\times$ as follows:

$v_{i,j}$	0	1	2	3
0	1	1	1	1
1	1	$v_{13}/\sigma_3(v_{12})$	v_{12}	v_{13}
2	1	v_{12}	$v_{12}\sigma_3(v_{12})$	$\sigma_3(v_{12})$
3	1	v_{13}	$\sigma_3(v_{12})$	v_{13}/v_{12}

We have a bijection $\mathcal{P}^{\mathrm{nondeg}}(K) \cong K^\times \times K(i)^\times$ sending v to (v_{13}, v_{12}).

The discriminant is

$$\mathrm{disc}(m) = v_{13}v_{22}v_{31} = v_{13}^2 N_{K(i)|K}(v_{12}).$$

The H-discriminant for $H = \langle \tau^2 \rangle$ is

$$\mathrm{disc}^H(m) = v_{22} = N_{K(i)|K}(v_{12}).$$

Example 3.7 ($n = 5$)**.** If $v \in \mathcal{P}(K)$ is nondegenerate, the variables can be computed from $v_{12} \in K(\zeta_5)^\times$ as follows:[1]

$v_{i,j}$	0	1	2	3	4
0	1	1	1	1	1
1	1	$v_{12}^{\sigma_1+\sigma_4-\sigma_2}$	$v_{12}^{\sigma_1}$	$v_{12}^{\sigma_3}$	$v_{12}^{\sigma_1+\sigma_4}$
2	1	$v_{12}^{\sigma_1}$	$v_{12}^{\sigma_2+\sigma_3-\sigma_4}$	$v_{12}^{\sigma_2+\sigma_3}$	$v_{12}^{\sigma_2}$
3	1	$v_{12}^{\sigma_3}$	$v_{12}^{\sigma_2+\sigma_3}$	$v_{12}^{\sigma_2+\sigma_3-\sigma_1}$	$v_{12}^{\sigma_4}$
4	1	$v_{12}^{\sigma_1+\sigma_4}$	$v_{12}^{\sigma_2}$	$v_{12}^{\sigma_4}$	$v_{12}^{\sigma_1+\sigma_4-\sigma_3}$

We have a bijection $\mathcal{P}^{\mathrm{nondeg}}(K) \cong K(\zeta_5)^\times$ sending v to v_{12}.

The discriminant is

$$\mathrm{disc}(m) = v_{14}v_{23}v_{32}v_{41} = N_{K(\zeta_5)|K}(v_{12})^2.$$

Example 3.8 ($n = 6$)**.** If $v \in \mathcal{P}(K)$ is nondegenerate, the variables can be computed from $v_{11} \in K(\zeta_3)^\times$, $v_{12} \in K(\zeta_3)^\times$, and $v_{15} \in K^\times$.

We have a bijection $\mathcal{P}^{\mathrm{nondeg}}(K) \cong K(\zeta_3)^\times \times K(\zeta_3)^\times \times K^\times$ sending v to (v_{11}, v_{12}, v_{15}).

Example 3.9 ($n = 7$)**.** If $v \in \mathcal{P}(K)$ is nondegenerate, the variables can be computed from $v_{13} \in K(\zeta_7)^\times$.

We have a bijection $\mathcal{P}^{\mathrm{nondeg}}(K) \cong K(\zeta_7)^\times$ sending v to v_{13}.

3.3 Integral structure, full ideals

To compute $\mathrm{Cl}(S[G])$, we first need to understand the ring $S[G] \subseteq \prod'_i S[\zeta_n]$:

Lemma 3.10. *The image of $S[G]$ in $\prod'_i S[\zeta_n]$ is the set of tuples $(x_i)_i$ such that $\sum_i x_i \zeta_n^{-ij} \equiv 0 \mod n$ for all j. The image in $\prod_{d|n} S[\zeta_d]$ is the set of tuples $(y_d)_d$ such that $\sum_{d|n} \mathrm{Tr}_{K(\zeta_d)|K}(y_d \zeta_d^{-j}) \equiv 0 \mod n$ for all j.*

Proof. According to (3.1), an element $(x_i)_i$ of $\prod'_i S[\zeta_n]$ lies in the image if and only if

$$\sum_i x_i \zeta_n^{-ij} \equiv 0 \mod n \qquad \text{for all } j.$$

An element $(x_i)_i$ of $\prod'_i S[\zeta_n]$ corresponds to $(y_d)_d \in \prod_{d|n} S[\zeta_d]$ given by $y_d = x_{n/d}$. As $x_{ri} = \sigma_r(x_i)$ for $r \in (\mathbb{Z}/n\mathbb{Z})^\times$, the left-hand side is

$$\sum_i x_i \zeta_n^{-ij} = \sum_{d|n} \sum_{r \in (\mathbb{Z}/d\mathbb{Z})^\times} x_{rn/d} \zeta_d^{-rj} = \sum_{d|n} \sum_{r \in (\mathbb{Z}/d\mathbb{Z})^\times} \sigma_r(x_{n/d} \zeta_d^{-j}) = \sum_{d|n} \mathrm{Tr}_{K(\zeta_d)|K}(y_d \zeta_d^{-j}). \qquad \square$$

[1] We use exponential notation: for example, $v_{12}^{\sigma_4+\sigma_1-\sigma_2}$ is $\sigma_4(v_{12})\sigma_1(v_{12})/\sigma_2(v_{12})$.

Example 3.11. If $n = p$ is prime, the image in $S \times S[\zeta_p]$ is

$$\begin{aligned}&\{(a,b) \in S \times S[\zeta_p] \mid a + \mathrm{Tr}_{K(\zeta_p)|K}(b) \equiv 0 \mod p\}\\ =\ &\{(a,b) \in S \times S[\zeta_p] \mid a \equiv b \mod (\zeta_p - 1)\}.\end{aligned}$$

The image in $\prod\!\!\!\!\!\!\prod_i' S[\zeta_p]$ is the set of tuples $(x_i)_i$ such that $\sum_i x_i \equiv 0 \mod \zeta_p - 1$.

Example 3.12. If $n = 4$, the image is the set of $(a, b, c + id) \in S \times S \times S[i]$ such that

$$a + b + 2c \equiv 0 \mod 4 \quad \text{and} \quad b + c + d \equiv 0 \mod 2.$$

We will now study the case $S = \mathbb{Z}$.

Lemma 3.13. *Let $n = p$ be prime and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be representatives of the h ideal classes in $\mathbb{Z}[\zeta_p]$. For each i, let f_i be a $\mathbb{Z}$-linear isomorphism $\mathfrak{a}_i/((\zeta_p - 1)\mathfrak{a}_i) \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$ of $\mathbb{Z}$-modules. (Such an isomorphism exists because $(\zeta_p - 1)$ is an ideal of norm p.) The $2h$ equivalence classes of full ideals of $\mathbb{Z}[G]$ are as follows: for each $1 \leqslant i \leqslant h$, there are the two full ideal classes represented by the unitary full ideals*

$$I_{1,i} = \{(x, y) \in \mathbb{Z} \times \mathfrak{a}_i \mid x \equiv f_i(y) \mod p\}$$

and

$$I_{2,i} = p\mathbb{Z} \times \mathfrak{a}_i.$$

The indices of $I_{1,i}$ and $I_{2,i}$ in $\mathbb{Z}[G]$ are both equal to the index $[\mathbb{Z}[\zeta_p] : \mathfrak{a}_i]$.

Proof. First of all $\mathrm{Cl}(\mathbb{Z}) = \{\mathbb{Z}\}$ and $\mathrm{Cl}(\mathbb{Z}[\zeta_p]) = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$. Therefore, Lemma 2.66 implies that $\mathrm{Cl}(\mathbb{Z} \times \mathbb{Z}[\zeta_p]) = \{\mathbb{Z} \times \mathfrak{a}_1, \ldots, \mathbb{Z} \times \mathfrak{a}_h\}$. Since $p(\mathbb{Z} \times \mathbb{Z}[\zeta_p]) \subseteq \mathbb{Z}[G]$, Lemma 2.68 implies that elements of $\mathrm{Cl}(\mathbb{Z}[G])$ are in bijection with equivalence classes of pairs $(\mathbb{Z} \times \mathfrak{a}_i, T)$ where $1 \leqslant i \leqslant h$ and T is a $\mathbb{Z}[G]$-submodule of $\mathbb{Z}/p\mathbb{Z} \times \mathfrak{a}_i/p\mathfrak{a}_i$ that projects surjectively onto both factors. Two such pairs $(\mathbb{Z} \times \mathfrak{a}_i, T)$ and $(\mathbb{Z} \times \mathfrak{a}_{i'}, T')$ are equivalent if and only if $i = i'$ and there exists some $\lambda \in \mathrm{Aut}(\mathbb{Z} \times \mathfrak{a}_i) = \mathbb{Z}^\times \times \mathbb{Z}[\zeta_p]^\times$ such that $T\lambda = T'$. It is not hard to see that we either have $T = \mathbb{Z} \times \mathfrak{a}_i$, corresponding to the ideal $\mathbb{Z} \times \mathfrak{a}_i = I_{2,i}(\frac{1}{p}, 1) \cong I_{2,i}$, or we have $T = \{(x, y) \in \mathbb{Z} \times \mathfrak{a}_i \mid x \equiv g(y) \mod p\}$ for some surjective $\mathbb{Z}$-linear map $g : \mathfrak{a}_i/p\mathfrak{a}_i \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$. As T is closed under multiplication by $(1, \zeta_p) \in \mathbb{Z}[G]$, we must have $g(\zeta_p y) = g(y)$ for all $y \in \mathfrak{a}_i$. The kernel of g must therefore be a $\mathbb{Z}[\zeta_p]$-ideal of index p in $\mathfrak{a}_i$. Since $(\zeta_p - 1)$ is the only ideal of index p, the kernel has to be $(\zeta_p - 1)\mathfrak{a}_i$. Then, $g = \mu f_i$ for some $\mu \in (\mathbb{Z}/p\mathbb{Z})^\times$. Multiplying T by the unit $\lambda = (1, \frac{\zeta_p^\mu - 1}{\zeta_p - 1}) \in \mathbb{Z}^\times \times \mathbb{Z}[\zeta_p]^\times$ satisfying $\frac{\zeta_p^\mu - 1}{\zeta_p - 1} \equiv \mu \mod (\zeta_p - 1)$, we see that this case only produces one additional ideal class: $I_{1,i}$. □

Corollary 3.14. *Assume $\mathbb{Z}[\zeta_p]$ is a principal ideal domain. (This is the case if and only if $p \leqslant 19$.) We then have $h = 1$ and can choose $\mathfrak{a}_1 = \mathbb{Z}[\zeta_p]$. The two types are then*

$$I_1 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}[\zeta_p] \mid x \equiv y \mod (\zeta_p - 1)\} = \mathbb{Z}[G]$$

and

$$I_2 = p\mathbb{Z} \times \mathbb{Z}[\zeta_p].$$

The indices of I_1 and I_2 in $\mathbb{Z}[G]$ are both 1.

Example 3.15. If $n = 4$, the seven equivalence classes of full ideals are represented by the following

unitary full ideals:

$$\begin{aligned}
I_1 &= \langle (4,0,0),(0,2,0),(0,0,1),(0,0,i)\rangle \\
I_2 &= \langle (2,2,0),(0,4,0),(0,0,1),(0,0,i)\rangle \\
I_3 &= \langle (2,0,i),(0,2,0),(0,0,1+i),(0,0,2i)\rangle \\
I_4 &= \langle (4,0,0),(0,1,i),(0,0,1+i),(0,0,2i)\rangle \\
I_5 &= \langle (2,0,i),(0,2,i),(0,0,1+i),(0,0,2i)\rangle \\
I_6 &= \langle (2,1,i),(0,2,0),(0,0,1+i),(0,0,2i)\rangle \\
I_7 &= \langle (1,1,i),(0,2,1+i),(0,0,2),(0,0,2i)\rangle
\end{aligned}$$

Again, let $H = \langle \tau^2 \rangle$ be the index 2 subgroup of G. For convenience, we have chosen these full ideals so that $[\mathbb{Z}[G] : I_i] = [\mathbb{Z}[G]^H : I_i^H] = 1$ for each of our full ideals I_i.

3.4 Good primes

Let us study G-extensions of $S = \mathbb{Z}_q$ for any prime q not dividing n.

Lemma 3.16. *If q is a prime not dividing n, then $\mathbb{Z}_q[G] = \prod'_i \mathbb{Z}_q[\zeta_n] = \prod_{d|n} \mathbb{Z}_q[\zeta_d]$.*

Proof. This follows immediately from Lemma 3.10. □

In particular, as each $\mathbb{Z}_q[\zeta_d]$ and therefore $\mathbb{Z}_q[G]$ is a product of principal ideal domains, all full ideals of $\mathbb{Z}_q[G]$ are equivalent to $\mathbb{Z}_q[G]$. Assume $I = \mathbb{Z}_q[G]$ throughout this section.

Lemma 3.17. *Let $m = (v_{i,j})_{i,j} \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$. If q is a prime not dividing n, then $(v_{i,j})_{i,j}$ satisfies the closedness condition (Cc), i.e. $(v_{i,j})_{i,j} \in \mathcal{P}_I^{\mathrm{nondeg}}(\mathbb{Z}_p)$, if and only if $v_{i,j} \in \mathbb{Z}_q[\zeta_n]$ for all i, j.*

Proof. The closedness condition (Cc) is equivalent to $m(\mathbb{Z}_q[G] \otimes \mathbb{Z}_q[G]) \subseteq \mathbb{Z}_q[G] = \prod'_i \mathbb{Z}_q[\zeta_n]$, so $\rho_u(m(\mathbb{Z}_q[G] \otimes \mathbb{Z}_q[G])) \subseteq \mathbb{Z}_q[\zeta_n]$ for all u. By (3.2), this is equivalent to

$$\frac{1}{n} \sum_{\substack{i,j: \\ i+j=u}} \rho_i(\tau^r)\rho_j(\tau^s)v_{i,j} \in \mathbb{Z}_q[\zeta_n] \qquad \text{for all } u, r, s,$$

which simply means that

$$\frac{1}{n} \sum_{\substack{i,j: \\ i+j=u}} \zeta_n^{ir+js} v_{i,j} \in \mathbb{Z}_q[\zeta_n] \qquad \text{for all } u, r, s.$$

Note that $n \in \mathbb{Z}_q^\times$, so this condition holds whenever all $v_{i,j}$ lie in $\mathbb{Z}_q[\zeta_n]$.

Conversely, if $\rho_u(m(\mathbb{Z}_q[G] \otimes \mathbb{Z}_q[G])) \subseteq \mathbb{Z}_q[\zeta_n]$ for all u, then (3.3) implies that

$$v_{i,j} = \sum_k \zeta_n^{-ik} \rho_{i+j}(m(\tau^k \otimes e)) \in \mathbb{Z}_q[\zeta_n].$$ □

Let us now recall that q is unramified in $\mathbb{Z}[\zeta_n]$. The decomposition group is generated by the q-th power map, corresponding to the element σ_q of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$. If we denote any prime factor of q in $\mathbb{Z}[\zeta_n]$ by $\mathfrak{q}_1$, then the prime factors of q are exactly the ideals $\mathfrak{q}_i = \sigma_i(\mathfrak{q}_1)$ for $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. Two such ideals $\mathfrak{q}_i$ and $\mathfrak{q}_j$ are identical if and only if $j = q^t i$ for some integer t.

Let $(\mathbb{Z}/n\mathbb{Z})[q-1] = \frac{n}{\gcd(n,q-1)}\mathbb{Z}/n\mathbb{Z}$ be the set of $f \in \mathbb{Z}/n\mathbb{Z}$ such that $f(q-1) \equiv 0 \mod n$. Let B_q be the set of tuples $(b_i)_{i\in\mathbb{Z}/n\mathbb{Z}}$ of integers such that $b_0 = 0$ and such that $b_{qi} = b_i$ for all i and such that there exists some (unique) $f \in (\mathbb{Z}/n\mathbb{Z})[q-1]$ with $b_i \equiv fi \mod n$ for all i.

Remark 3.18. The set $B_q \subseteq \mathbb{Z}^n$ is a lattice of rank $\sum_{d|n,\ d\geqslant 2} \frac{\varphi(d)}{\operatorname{ord}_d(q)}$ where $\varphi(d) = \#(\mathbb{Z}/d\mathbb{Z})^\times$ is the Euler phi function and $\operatorname{ord}_d(q)$ is the multiplicative order of q modulo d.

We will now construct a map

$$\mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p) \to B_q$$

using the following lemma.

Lemma 3.19. *Let $(v_{i,j})_{i,j} = \alpha.\pi \in \mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$ with $\alpha \in \overline{\mathbb{Q}_p}[G]_1^\times$ and $\beta = \alpha^n \in \mathbb{Q}_p[G]_1^\times$ as in Remark 3.1. For each $i \in \mathbb{Z}/n\mathbb{Z}$, let b_i be the $\mathfrak{q}_1$-valuation of $\rho_i(\beta)$. Then, the tuple $(b_i)_i$ lies in B_q.*

Proof. Since $v_{i,j}^n = \frac{\rho_i(\beta)\rho_j(\beta)}{\rho_{i+j}(\beta)}$, we must have

$$b_i + b_j - b_{i+j} \equiv 0 \mod n \qquad \text{for all } i,j.$$

This implies that there exists some $f \in \mathbb{Z}/n\mathbb{Z}$ such that $b_i \equiv fi \mod n$ for all i. Since $\sigma_q(\mathfrak{q}_1) = \mathfrak{q}_1$, we have $b_{qi} = b_i$ for all i. In particular, it follows that $f(q-1) \equiv 0 \mod n$. □

Remark 3.20. The map $\mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p) \to B_q$ is clearly $\mathbb{Z}_q[G]_1^\times$-invariant.

We can compute the q-valuation of the discriminant of $(v_{i,j})_{i,j} \in \mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$ in terms of its image $(b_i)_i$ in B_q: Since $v_{i,-i}^p = \frac{\rho_i(\beta)\rho_{-i}(\beta)}{\rho_0(\beta)} = \rho_i(\beta)\rho_{-i}(\beta)$, it is $\operatorname{vdisc}(b) = \frac{1}{n}\sum_i (b_i + b_{-i}) = \frac{2}{n}\sum_i b_i$.

The closedness condition from Lemma 3.17 can also be rephrased in terms of the image $(b_i)_i$ in B_q: It holds if and only if

$$b_i + b_j - b_{i+j} \geqslant 0 \qquad \text{for all } i,j. \tag{3.5}$$

Taking b_j to be the smallest among the numbers $b_0, \dots, b_{n-1}$, we see that in particular $b_i \geqslant b_i + b_j - b_{i+j} \geqslant 0$ for all i.

Given that the closedness condition and the discriminant only depend on the tuple $b = (b_i)_i$, it makes sense to define the following series (the *local factor at q*):

$$f_q^{\text{nondeg}}(x) = \sum_{b\in B_q \text{ satisfying (3.5)}} x^{\operatorname{vdisc}(b)}.$$

Note that the closedness condition (3.5) cuts out a polyhedron in the lattice $B_q \subseteq \mathbb{Z}^n$. The series $f_q^{\text{nondeg}}(x)$ can therefore be interpreted as an Ehrhart series (see [15] for the definition and a proof that the series is a rational function). For $n = 2, 3$, the series can easily be computed by hand. We used the Normaliz software [9, 10] for $n = 4, 5$:

Example 3.21 ($n = 2$)**.** The local factor at $q \neq 2$ is

$$f_q^{\text{nondeg}}(x) = \frac{1}{1-x}.$$

Example 3.22 ($n = 3$)**.** The local factor at $q \neq 3$ is

$$f_q^{\text{nondeg}}(x) = \begin{cases} \dfrac{1}{(1-x^2)^2}, & q \equiv 1 \mod 3, \\ \dfrac{1}{1-x^4}, & q \equiv 2 \mod 3. \end{cases}$$

Example 3.23 ($n = 4$)**.** The local factor at $q \neq 2$ is

$$f_q^{\mathrm{nondeg}}(x) = \begin{cases} \dfrac{1 - x + x^2}{(1-x)\,(1-x^3)\,(1-x^4)}, & q \equiv 1 \mod 4, \\ \dfrac{1}{(1-x^2)\,(1-x^4)}, & q \equiv 3 \mod 4. \end{cases}$$

Example 3.24 ($n = 5$)**.** The local factor at $q \neq 5$ is

$$f_q^{\mathrm{nondeg}}(x) = \begin{cases} \dfrac{1 + 2x^4 + 2x^6 + 2x^8 + x^{12}}{(1-x^4)^2\,(1-x^6)^2}, & q \equiv 1 \mod 5, \\ \dfrac{1 - x^4 + x^8}{(1-x^4)\,(1-x^{12})}, & q \equiv 4 \mod 5, \\ \dfrac{1}{1-x^8}, & q \equiv 2, 3 \mod 5. \end{cases}$$

The maximality condition can be expressed in terms of the image $(b_i)_i \in B_q$ as follows:

Lemma 3.25. *We have $(v_{i,j})_{i,j} \in \mathcal{P}_I^{\max}(\mathbb{Z}_q)$ if and only if (3.5) holds and*

$$0 \leqslant b_i < n \qquad \text{for all } i. \tag{3.6}$$

Proof. Since $\mathbb{Z}_q[G]$ is the only full ideal up to equivalence, the G-extension of $\mathbb{Z}_q$ is nonmaximal if and only if there exists some $\lambda \in \mathbb{Z}_q[G] \cap \mathbb{Q}_q[G]_1^\times \backslash \mathbb{Z}_q[G]_1^\times$ such that $\lambda^{-1}.v = (\lambda^{-1}\alpha).\pi$ still satisfies the closedness condition. The $\mathfrak{q}_1$-valuation $l_i \geqslant 0$ of $\rho_i(\lambda)$ then has to be positive for some i. On the other hand, the $\mathfrak{q}_1$-valuation $b_i - nl_i$ of $\rho_i(\lambda^{-n}\beta) = \rho_i((\lambda^{-1}\alpha)^n)$ must still be nonnegative, which means that $b_i \geqslant n$.

Conversely, assume $L := \max_i b_i \geqslant n$. To show that the G-extension of $\mathbb{Z}_q$ is nonmaximal, construct $\lambda \in \mathbb{Z}_q[G] \cap \mathbb{Q}_q[G]_1^\times$ so that the $\mathfrak{q}_1$-valuation of $\rho_i(\lambda)$ is $l_i = 1$ when $b_i = M$ and is $l_i = 0$ when $b_i < M$. It then follows that

$$(b_i - nl_i) + (b_j - nl_j) - (b_{i+j} - nl_{i+j}) \geqslant 0,$$

so $\lambda^{-1}.v$ still satisfies the closedness condition: since the left-hand side is divisible by n, it suffices to show that it is greater than $-n$. If $(l_i, l_j, l_{i+j}) = (1, 0, 0)$, then the left-hand side is $b_i + b_j - b_{i+j} - n > M + b_j - M - n \geqslant -n$. If $(l_i, l_j, l_{i+j}) = (1, 1, 0)$, then the left-hand side is $b_i + b_j - b_{i+j} - 2n > M + M - M - 2n \geqslant -n$. If $(l_i, l_j, l_{i+j}) = (1, 1, 1)$, then the left-hand side is $b_i + b_j - b_{i+j} - n = M + M - M - n \geqslant 0$. The remaining cases are all similarly easy. □

For maximal rings, we therefore obtain one potential tuple $(b_0, \ldots, b_{n-1}) \in B_q$ for each

$$f \in (\mathbb{Z}/n\mathbb{Z})[q-1] = \frac{n}{\gcd(n, q-1)}\mathbb{Z}/n\mathbb{Z}.$$

The numbers $0 \leqslant b_i < n$ are determined by $b_i \equiv fi \mod n$.

The q-valuation of the discriminant is then

$$\frac{2}{n}\sum_i b_i = \frac{2}{n} \cdot g(f) \cdot \sum_{t=0}^{n/g(f)-1} tg(f) = \frac{2g(f)^2 \cdot (n/g(f) - 1)(n/g(f))}{n \cdot 2} = n - g(f)$$

with $g(f) = \gcd(f, n)$.

As before, we define the local factor

$$f_q^{\max}(x) = \sum_{b \in B \text{ satisfying (3.5) and (3.6)}} x^{\mathrm{vdisc}(b)}.$$

We have shown that

$$\begin{aligned} f_q^{\max}(x) &= \sum_{f \in \frac{n}{\gcd(n,q-1)}\mathbb{Z}/n\mathbb{Z}} x^{n-\gcd(f,n)} \\ &= \sum_{\frac{n}{\gcd(n,q-1)} | g | n} \varphi\left(\frac{n}{g}\right) x^{n-g} \\ &= \sum_{d | \gcd(n,q-1)} \varphi(d) x^{n\left(1-\frac{1}{d}\right)} \end{aligned}$$

where φ denotes the Euler phi function.

Example 3.26. If $n = p$ is prime, the local factor at $q \neq p$ is

$$f_q^{\max}(x) = \begin{cases} 1, & q \not\equiv 1 \mod p, \\ 1 + (p-1)x^{p-1}, & q \equiv 1 \mod p. \end{cases}$$

Example 3.27. More generally, if $n = p^k$ is a prime power with $\gcd(p^k, q-1) = p^e$, the local factor at $q \neq p$ is

$$f_q^{\max}(x) = 1 + \sum_{t=1}^{e} (p-1) p^{t-1} x^{p^k - p^{k-t}}.$$

Example 3.28. For $n = 4$, the local factor at $q \neq 2$ is

$$f_q^{\max}(x) = \begin{cases} 1 + x^2, & q \equiv 3 \mod 4, \\ 1 + x^2 + 2x^3, & q \equiv 1 \mod 4. \end{cases}$$

Remark 3.29. For $q \nmid n$, any G-extension of $\mathbb{Q}_q$ is tame. We could also have computed the series $f_q^{\max}(s)$ using the fact that the maximal tame quotient of the absolute Galois group of $\mathbb{Q}_q$ is topologically generated by (a lift of) the Frobenius φ and a map τ sending $q^{1/k}$ to $\zeta_k q^{1/k}$, subject to the relation $\varphi \circ \tau \circ \varphi^{-1} = \tau^q$. In [18, section 5] used this approach to study "mass formulas" for tame extensions of $\mathbb{Q}_q$ with arbitrary prescribed Galois group.

3.5 Bad primes

It remains to treat the closedness and maximality conditions for primes q dividing n. We only cover the case that $n = p$ is prime (and $q = p$). For other specific values of n, one could carry out a similar analysis, or refer to a database of local fields (see [17]) for a list of all G-extensions of $\mathbb{Q}_q$.

Let $n = p$ be prime. Recall that p ramifies completely in $\mathbb{Z}_p[\zeta_p]$: We have $(p) = (\zeta_p - 1)^{p-1}$. We will repeatedly make use of the congruence

$$\frac{\zeta_p^i - 1}{\zeta_p - 1} \equiv \zeta_p^{i-1} + \cdots + 1 \equiv i \mod \zeta_p - 1$$

for $i \in \mathbb{Z}/n\mathbb{Z}$.

Since $\mathbb{Z}_p[\zeta_p]$ is a principal ideal domain, an argument as in the proof of Lemma 3.13 shows that, up to equivalence, $\mathbb{Z}_p[G]$ has exactly two unitary full ideals: the ideal $I_1 = \mathbb{Z}_p[G]$ and the ideal

$I_2 = p\mathbb{Z}_p \times \mathbb{Z}_p[\zeta_p]$. We will now analyze the closedness conditions for each of these two possible types.

3.5.1 Closedness in type I_1

Before we can simplify the closedness condition, we need to solve a linear functional equation:

Lemma 3.30. *Let $f : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a function such that*

$$f(i,j) + f(i+j,k) \equiv f(j,k) + f(i,j+k) \mod n \qquad \text{for all } i,j,k. \tag{3.7}$$

Then, there exists some function $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n^2\mathbb{Z}$ such that g is linear modulo n (meaning that $g(i+j) \equiv g(i) + g(j) \mod n$ for all i, j) and

$$f(i,j) \equiv \frac{g(i) + g(j) - g(i+j)}{n} \mod n \qquad \text{for all } i,j. \tag{3.8}$$

Proof. Define the function g as follows:

$$g(a) \equiv a \sum_{b=0}^{n-1} f(1,b) + nf(1,0) - n \sum_{b=0}^{a-1} f(1,b) \mod n^2 \qquad \text{for } a \geqslant 0.$$

First of all, note that this function is indeed well-defined: $g(a+n) \equiv g(a)$ for all $a \geqslant 0$. It is also clearly linear modulo n.

Next, we will show (3.8) for integers $i \geqslant 1$ and j via induction over i.

For $i = 1$, this follows directly from the definition. Assume now that we have shown (3.8) for some i and all j. Then, (3.7) implies that

$$f(1,i) + f(1+i,j) \equiv f(i,j) + f(1,i+j) \mod n,$$

so

$$f(1+i,j) \equiv f(i,j) + f(1,i+j) - f(1,i) \mod n.$$

According to the induction hypothesis, this is

$$f(1+i,j) \equiv \frac{g(1+i) + g(j) - g(1+i+j)}{n}.$$ □

Lemma 3.31. *Let $n = p$ be prime and $1 \leqslant e \leqslant p-1$ and let $f : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be a function satisfying (3.7) and*

$$f(ri, rj) \equiv r^e f(i,j) \mod p \qquad \text{for all } r,i,j.$$

Then, there exists some constant $c \in \mathbb{Z}/p\mathbb{Z}$ such that modulo p,

$$f(i,j) \equiv \begin{cases} c \cdot \frac{i^p + j^p - (i+j)^p}{p}, & e = 1, \\ c \cdot (i^e + j^e - (i+j)^e), & e \geqslant 2. \end{cases}$$

Proof. Let g be a function as in Lemma 3.30. First, note that we can find some $b \in \mathbb{Z}$ such that $g'(i) = g(i) - b \cdot i^p$ is divisible by p for all i. Then, the function $\frac{1}{p}g'$ from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ can be represented by a polynomial of degree at most p. We can therefore write

$$g(i) = \sum_{k=0}^{p} a_k \cdot i^k$$

where the coefficients $a_0, \ldots, a_{p-1}$ are divisible by p. Replacing $g(i)$ by $g(i) - a_1 i$ doesn't change $g(i) + g(j) - g(i+j)$, so we can assume without loss of generality that $a_1 = 0$.

Now, the requirement that $f(ri, rj) \equiv r^e f(i,j) \mod p$ means that

$$\frac{1}{p}\sum_{k=0}^{p} a_k(r^k - r^e)(i^k + j^k - (i+j)^k) \equiv 0 \mod p \qquad \text{for all } r,i,j.$$

The left-hand side is a polynomial of degree at most p in r. To be zero for all r, it must be a multiple of $r^p - r$. Its r^p-coefficient is $a_p \cdot \frac{i^p+j^p-(i+j)^p}{p}$.

If $e \neq 1$, the r-coefficient is $\frac{1}{p}a_1(i+j-(i+j)) = 0$, so we must have $a_p \cdot \frac{i^p+j^p-(i+j)^p}{p} \equiv 0 \mod p$ for all i,j. For $j=1$, the term $\frac{i^p+j^p-(i+j)^p}{p}$ is a polynomial of degree $p-1$ in i and hence cannot always be zero. Therefore, $a_p = 0$.

For any $0 \leqslant k \leqslant p-1$ with $k \neq e$, the r^k-coefficient is $\frac{a_k}{p} \cdot (i^k + j^k - (i+j)^k)$. If $k \geqslant 2$ and $j = 1$, the term $i^k + j^k - (i+j)^k$ is a polynomial of degree $k-1 \leqslant p-2$ in i and hence cannot always be zero. The term is 1 for $k = 0$. Therefore, $a_k = 0$ whenever $k \neq 1, p, e$.

We have thus shown that if $e = 1$, all coefficients a_k except a_p must be zero, and that if $e \neq 1$, all coefficients a_k except a_e must be zero (and a_e must be divisible by p). This finishes the proof. □

Lemma 3.32. *Let $n = p$ be prime and assume $m = (v_{i,j})_{i,j} \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$. Let $e \geqslant 1$ so that $v_{i,j} = 1 + (\zeta_p - 1)^e w_{i,j}$ with $w_{i,j} \in \mathbb{Z}_p[\zeta_p]$ for all i,j. Then, there is a constant $c \in \mathbb{Z}$ such that modulo $\zeta_p - 1$,*

$$w_{i,j} \equiv \begin{cases} c \cdot \frac{i^p+j^p-(i+j)^p}{p}, & e = 1, \\ c \cdot (i^e + j^e - (i+j)^e), & e \geqslant 2. \end{cases}$$

Proof. Modulo $(\zeta_p - 1)^{e+1}$, the associativity condition (Ca) becomes

$$w_{i,j} + w_{i+j,k} \equiv w_{j,k} + w_{i,j+k} \mod \zeta_p - 1.$$

The condition $v_{ri,rj} = \sigma_r(v_{i,j})$ means that $(\zeta_p - 1)^e w_{ri,rj} = (\zeta_p^r - 1)^e \sigma_r(w_{i,j})$, so

$$\begin{aligned} w_{ri,rj} &\equiv \left(\frac{\zeta_p^r - 1}{\zeta_p - 1}\right)^e \sigma_r(w_{i,j}) \\ &\equiv r^e w_{i,j} \mod (\zeta_p - 1) \qquad \text{for all } i,j,r. \end{aligned}$$

(Note that this conclusion holds even if $r = 0$, as $v_{0,0} = 1$.)

The claim then follows from Lemma 3.31 (just pick $f(i,j) \equiv w_{i,j} \mod \zeta_p - 1$). □

Lemma 3.33. *Let $n = p$ be prime and assume $m = (v_{i,j})_{i,j} \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$. Let $2 \leqslant e \leqslant p-1$ so that $v_{i,j} \in 1 + (\zeta_p - 1)^e \mathbb{Z}_p[\zeta_p]$ for all i,j. Then, there exists some $\lambda \in \mathbb{Z}_p[G]_1^\times$ such that $v'_{i,j} \in 1 + (\zeta_p - 1)^{e+1}\mathbb{Z}_p[\zeta_p]$, where $m' = \lambda.m = (v'_{i,j})_{i,j} \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$.*

Proof. Writing $v_{i,j} = 1 + (\zeta_p - 1)^e w_{i,j}$, Lemma 3.32 shows that there is a constant $c \in \mathbb{Z}$ such that

$$w_{i,j} \equiv c \cdot (i^e + j^e - (i+j)^e) \mod \zeta_p - 1 \qquad \text{for all } i,j.$$

Take $\lambda = 1 - c \cdot (\tau - 1)^e \in \mathbb{Z}_p[G]_1^\times$. Then, modulo $(\zeta_p - 1)^{e+1}$, we get

$$\begin{aligned} v'_{i,j} &\equiv \frac{\rho_i(\lambda)\rho_j(\lambda)}{\rho_{i+j}(\lambda)} \cdot v_{i,j} \\ &\equiv \frac{(1 - c \cdot (\zeta_p^i - 1)^e)(1 - c \cdot (\zeta_p^j - 1)^e)}{(1 - c \cdot (\zeta_p^{i+j} - 1)^e)} \cdot (1 + c \cdot (i^e + j^e - (i+j)^e)(\zeta_p - 1)^e) \\ &\equiv 1. \end{aligned}$$

We again used that $(\zeta_p^i - 1)^e \equiv i^e(\zeta_p - 1)^e \mod (\zeta_p - 1)^{e+1}$. □

Lemma 3.34. *Let $n = p$ be prime. For type $I_1 = \mathbb{Z}_p[G]$, the closedness condition (Cc) is equivalent to the conditions that $v_{i,j} \in \mathbb{Z}_p[\zeta_p]$ and*

$$\sum_{\substack{i,j:\\ i+j=u}} v_{i,j}\zeta_p^{ir+js} \equiv 0 \mod p \qquad \text{for all } r, s, u$$

and

$$\sum_{i,j} v_{i,j}\zeta_p^{ir+js} \equiv 0 \mod p^2 \qquad \text{for all } r, s.$$

Proof. Recall that $I_1 = \mathbb{Z}_p[G] = \{(x_i)_i \in \prod_i{}' \mathbb{Z}_p[\zeta_p] \mid \sum_i x_i \equiv 0 \mod \zeta_p - 1\}$. Hence, we have $m(I_1 \otimes I_1) \subseteq I_1$ if and only if $\rho_u(m(\tau^r \otimes \tau^s)) \in \mathbb{Z}_p[\zeta_p]$ for all u and $\sum_u \rho_u(m(\tau^r \otimes \tau^s)) \in p\mathbb{Z}_p[\zeta_p]$. The claim then follows from (3.2). □

Lemma 3.35. *Let $n = p$ be prime and assume $m \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$, i.e., commutativity and associativity are satisfied. For type $I_1 = \mathbb{Z}_p[G]$, the closedness condition (Cc) is then equivalent to the condition that*

$$v_{i,j} \in 1 + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \qquad \text{for all } i, j.$$

Proof. Assume $v_{i,j} \in 1 + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p]$ for all i, j. Repeatedly applying Lemma 3.33 and using the fact that $\mathcal{P}^{\mathrm{nondeg}}_{I_1}(\mathbb{Z}_p)$ is invariant under $\mathrm{Aut}_1(I_1) = \mathbb{Z}_p[G]_1^\times$, we can in fact assume that $v_{i,j} \in 1 + (\zeta_p - 1)^p\mathbb{Z}_p[\zeta_p]$.

Let $v_{i,j} = 1 + (\zeta_p - 1)^p w_{i,j}$. Then, we have

$$\sum_{\substack{i,j:\\ i+j=u}} v_{i,j}\zeta_p^{ir+js} \equiv \sum_{\substack{i,j:\\ i+j=u}} (1 + (\zeta_p - 1)^p w_{i,j})\zeta_p^{ir+js} \equiv 0 \mod p \qquad \text{for all } r, s, u.$$

so it only remains to show that

$$\sum_{i,j} v_{i,j}\zeta_p^{ir+js} \equiv 0 \mod p^2.$$

Since the left-hand side is an integer, we only need to verify that it is congruent to 0 modulo $(p)(\zeta_p - 1) = (\zeta_p - 1)^p$, which is again obvious:

$$\sum_{i,j} v_{i,j}\zeta_p^{ir+js} \equiv \sum_{i,j}(1 + (\zeta_p - 1)^p w_{i,j})\zeta_p^{ir+js} \equiv 0 \mod (\zeta_p - 1)^p.$$

Conversely, let us show that $v_{i,j} \in 1 + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p]$ is necessary. Assume the closedness condition is satisfied.

We know that $v_{i,j} \in \mathbb{Z}_p[\zeta_p]$ and that

$$0 \equiv \sum_{\substack{i,j:\\ i+j=u}} v_{i,j} \mod p \qquad \text{for all } u. \tag{3.9}$$

With $u = 0$, we get

$$0 \equiv v_{0,0} + \sum_{i \neq 0} \sigma_i(v_{1,-1}) \equiv 1 + (p-1)v_{1,-1} \equiv 1 - v_{1,-1} \mod (\zeta_p - 1),$$

so $v_{1,-1} \equiv 1 \mod (\zeta_p - 1)$ and hence $v_{i,-i} \equiv 1 \mod (\zeta_p - 1)$ for all i. Then, the associativity condition (Ca) with $i = b$, $j = a$, $k = -a - b$ proves that

$$v_{b,a}v_{a+b,-a-b} = v_{a,-a-b}v_{b,-b},$$

so

$$v_{a,b} \equiv v_{b,a} \equiv v_{a,-a-b} \mod (\zeta_p - 1).$$

The associativity condition with $i = -a$, $j = a$, $k = b$ proves that

$$v_{-a,a}v_{0,b} = v_{a,b}v_{-a,a+b} = v_{a,b}\sigma_{-1}(v_{a,-a-b}),$$

so

$$1 \equiv v_{a,b}v_{a,-a-b} \equiv v_{a,b}^2 \mod (\zeta_p - 1).$$

Since $(\zeta_p - 1)$ is a prime ideal in $\mathbb{Z}_p[\zeta_p]$, it follows that

$$v_{a,b} \equiv \pm 1 \mod (\zeta_p - 1) \qquad \text{for all } a, b.$$

Now, the right-hand side of (3.9) consists of p summands, each of which is ± 1 modulo $(\zeta_p - 1)$. As $(\zeta_p - 1) \cap \mathbb{Z} = p\mathbb{Z}$, the summands must all have the same sign modulo $(\zeta_p - 1)$. One of the summands is $v_{0,u} = 1$, so we must have $v_{i,j} \equiv 1 \mod (\zeta_p - 1)$ for all i, j.

Writing $v_{i,j} = 1 + (\zeta_p - 1)w_{i,j}$, Lemma 3.32 shows that there is a constant $c \in \mathbb{Z}$ such that

$$w_{i,j} \equiv c \cdot \frac{i^p + j^p - (i+j)^p}{p} \mod (\zeta_p - 1) \qquad \text{for all } i, j.$$

For odd p, set $u = 1$ in (3.9). We get that

$$0 \equiv c \cdot \frac{1}{p}\left(2\sum_i i^p - p\right) \equiv c \cdot \frac{1}{p}\left(\sum_i (i^p + (-i)^p) - p\right) \equiv -c \mod (\zeta_p - 1),$$

which implies that $c \equiv 0 \mod (\zeta_p - 1)$, so $w_{i,j} \equiv 0 \mod (\zeta_p - 1)$ and indeed $v_{i,j} \in 1 + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p]$.

For $p = 2$, use that

$$0 \equiv \sum_{i,j} v_{i,j} \equiv 3 + v_{11} \mod 4.$$

□

3.5.2 Closedness in type I_2

Lemma 3.36. *Let $n = p$ be prime. For type $I_2 = p\mathbb{Z}_p \times \mathbb{Z}_p[\zeta_p]$, the closedness condition (Cc) is equivalent to the conditions that $v_{i,j} \in \mathbb{Z}_p[\zeta_p]$ and*

$$\sum_{\substack{i,j \neq 0: \\ i+j=u}} v_{i,j}\zeta_p^{ir+js} \equiv 0 \mod p \qquad \text{for all } r, s, u \tag{3.10}$$

and

$$\sum_{i \neq 0} v_{i,-i}\zeta_p^{i(r-s)} \equiv 0 \mod p^2 \qquad \text{for all } r, s. \tag{3.11}$$

Proof. Note that $I_2 = p\mathbb{Z}_p \times \mathbb{Z}_p[\zeta_p] = \{(x_i)_i \in \prod_i{}' \mathbb{Z}_p[\zeta_p] \mid x_0 \equiv 0 \mod p\}$. Hence, we have $m(I_2 \otimes I_2) \subseteq I_2$ if and only if $\rho_u(m(\tau^r \otimes \tau^s)) \in \mathbb{Z}_p[\zeta_p]$ for all u and $\rho_0(m(\tau^r \otimes \tau^s)) \in p\mathbb{Z}_p[\zeta_p]$. The claim then follows from (3.2). □

Lemma 3.37. *Let $n = p$ be prime and assume $m \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$. For type $I_2 = p\mathbb{Z}_p \times \mathbb{Z}_p[\zeta_p]$, the closedness condition (Cc) is then equivalent to the conditions that*

$$v_{i,j} \in p\mathbb{Z}_p[\zeta_p] \qquad \text{for all } i, j \neq 0$$

and

$$v_{i,-i} \in p^2\mathbb{Z}_p[\zeta_p] \qquad \textit{for all } i \neq 0.$$

Proof. The conditions clearly imply closedness according to the previous lemma.

Conversely, assume that the closedness condition is satisfied. First, let us show that $v_{1,-1} \equiv 0 \mod (\zeta_p - 1)^p$: write $v_{1,-1} = \sum_k a_k \zeta_p^k$ with $a_k \in \mathbb{Z}$. Without loss of generality, $a_{p-1} = 0$. We have, $v_{i,-i} = \sigma_i(v_{1,-1}) = \sum_k a_k \zeta_p^{ik}$. Then, (3.11) with $r = 0$ implies

$$0 \equiv \sum_{i\neq 0}\sum_k a_k \zeta_p^{i(k-s)} \equiv \sum_k a_k \sum_i \zeta_p^{i(k-s)} - \sum_k a_k \equiv pa_s - \sum_k a_k \mod p^2 \qquad \text{for all } s.$$

Hence, $a_0 \equiv a_1 \equiv \cdots \equiv a_{p-1} \equiv 0 \mod p$. Let $a_k = pb_k$. Then, we obtain

$$0 \equiv p^2 b_s - \sum_k pb_k \equiv -p\sum_k b_k \mod p^2 \qquad \text{for all } s,$$

so $\sum_k b_k \equiv 0 \mod k$. This implies that $\sum_k b_k \zeta_p^k \equiv 0 \mod \zeta_p - 1$, so $v_{1,-1}$ is divisible by $(p)(\zeta_p - 1) = (\zeta_p - 1)^p$.

Now, define $\beta \in \mathbb{Q}_p[G]_1^\times$ as in Remark 3.1, so that

$$v_{i,j}^p = \frac{\rho_i(\beta)\rho_j(\beta)}{\rho_{i+j}(\beta)} \qquad \text{for all } i, j.$$

By definition of $\mathbb{Q}_p[G]_1^\times$, we have $\rho_0(\beta) = 1$. Write $\rho_1(\beta) = (\zeta_p - 1)^e t$ with $t \in \mathbb{Z}_p[\zeta_p]^\times$. Then,

$$v_{1,-1}^p = \rho_1(\beta)\rho_{-1}(\beta) = \rho_1(\beta)\sigma_{-1}(\rho_1(\beta))$$

is divisible by $\zeta_p - 1$ exactly $2e$ times. We have seen that the left-hand side is divisible by $(\zeta_p - 1)^{p^2}$, so $e/p \geqslant \frac{p}{2}$. Now, for any $i, j \neq 0$ with $i + j \neq 0$,

$$v_{i,j}^p = \frac{\rho_i(\beta)\rho_j(\beta)}{\rho_{i+j}(\beta)} = \frac{\sigma_i(\rho_1(\beta))\sigma_j(\rho_1(\beta))}{\sigma_{i+j}(\rho_1(\beta))}$$

is divisible by $\zeta_p - 1$ exactly e times. In particular, e is divisible by p. Our goal is to show that $e/p \geqslant p - 1$, since this implies that $v_{i,-i}$ is divisible by $\zeta_p - 1$ exactly $\frac{2e}{p} \geqslant 2(p-1)$ times and $v_{i,j}$ is divisible by $\zeta_p - 1$ exactly $\frac{e}{p} \geqslant p - 1$ times, as claimed. Assume $e/p \leqslant p - 2$. Let $\lambda = (1, \zeta_p - 1) \in \mathbb{Z}^\times \times \mathbb{Z}_p[\zeta_p]^\times = \mathrm{Aut}_1(I_2)$. Then, consider $w = \lambda^{-e/p}.v \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$. If $i, j, i + j \neq 0$, we get

$$w_{i,j}^p = \frac{\sigma_i(t)\sigma_j(t)}{\sigma_{i+j}(t)}.$$

Letting $t \equiv c \mod \zeta_p - 1$ for some $0 \neq c \in \mathbb{Z}/p\mathbb{Z}$, we conclude that $w_{i,j}^p \equiv c \mod \zeta_p - 1$, so $w_{i,j} \equiv c \equiv t \mod \zeta_p - 1$. Then, as $v = \lambda^{e/p}.w$,

$$v_{i,j} \equiv \frac{(\zeta_p^i - 1)^{e/p}(\zeta_p^j - 1)^{e/p}}{(\zeta_p^{i+j} - 1)^{e/p}} \cdot t \equiv (\zeta_p - 1)^{e/p} \cdot \left(\frac{ij}{i+j}\right)^{e/p} \cdot t \mod (\zeta_p - 1)^{e/p+1}.$$

Now, (3.10) implies that

$$\sum_{\substack{i,j\neq 0:\\ i+j=1}} v_{i,j} \equiv (\zeta_p - 1)^{e/p} \cdot \sum_{\substack{i,j\neq 0:\\ i+j=1}} (ij)^{e/p} \cdot t \mod (\zeta_p - 1)^{e/p+1}.$$

However, since $\frac{p}{2} \leqslant \frac{e}{p} \leqslant p-2$, we have

$$\sum_{\substack{i,j\neq 0:\\ i+j=1}} (ij)^{e/p} \equiv \sum_i (i(1-i))^{e/p} \equiv \sum_i \sum_{r=0}^{e/p} \binom{e/p}{r} \cdot (-1)^r \cdot i^{e/p+r}$$

$$\equiv \binom{e/p}{p-1-e/p} \cdot (-1)^{p-1-e/p} \cdot (-1) \not\equiv 0 \mod p,$$

so $t \equiv 0 \mod \zeta_p - 1$, contradicting our assumption that $t \in \mathbb{Z}_p[\zeta_p]^\times$. □

3.5.3 Maximality

Lemma 3.38. *Let $n = p$ be prime. Then, any $m \in \mathcal{P}_{I_1}^{\text{nondeg}}(\mathbb{Z}_p)$ is maximal.*

Proof. We know that m is nonmaximal if and only if there exists some unitary full ideal $J \supsetneq I_1$ such that $m \in \mathcal{P}_J(\mathbb{Z}_p)$. Now, there are two cases:

i) The full ideal is of the form $J = I_1\lambda^{-1}$ (so $\mathcal{P}_J(\mathbb{Z}_p) = \lambda.\mathcal{P}_{I_1}(\mathbb{Z}_p)$) for some $\lambda \in \mathbb{Q}_p[G]_1^\times \cong \mathbb{Q}_p[\zeta_p]^\times$ with $\lambda \in (\zeta_p - 1)\mathbb{Z}_p[\zeta_p]$.

ii) The full ideal is of the form $J = I_2\lambda^{-1}$ (so $\mathcal{P}_J(\mathbb{Z}_p) = \lambda.\mathcal{P}_{I_2}(\mathbb{Z}_p)$) for some $\lambda \in \mathbb{Q}_p[G]_1^\times \cong \mathbb{Q}_p[\zeta_p]^\times$ with $\lambda \in (\zeta_p - 1)\mathbb{Z}_p[\zeta_p]$.

In either case, you can see that $v_{1,-1} \notin \lambda\sigma_{-1}(\lambda)\mathbb{Z}_p[\zeta_p]$, so $m \notin \lambda.\mathcal{P}_J(\mathbb{Z}_p)$. □

Lemma 3.39. *Let $n = p$ be prime and assume $m \in \mathcal{P}_{I_2}^{\text{nondeg}}(\mathbb{Z}_p)$. Then, m is nonmaximal if and only if one of the following two conditions holds:*

a) We have

$$\frac{1}{p} v_{i,j} \in (\zeta_p - 1)\mathbb{Z}_p[\zeta_p] \qquad \text{for all } i, j \neq 0 \text{ with } i \neq j$$

and

$$\frac{1}{p^2} v_{i,-i} \in (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \qquad \text{for all } i \neq 0.$$

b) There exists some $a \in \{1, \ldots, p-1\}$ such that

$$\frac{1}{p} v_{i,j} \in a + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \qquad \text{for all } i, j \neq 0 \text{ with } i \neq j$$

and

$$\frac{1}{p^2} v_{i,-i} \in a^2 + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \qquad \text{for all } i \neq 0.$$

Proof. We know that m is nonmaximal if and only if there exists some unitary full ideal $J \supsetneq I_2$ such that $m \in \mathcal{P}_J(\mathbb{Z}_p)$. Now, there are two cases:

i) The full ideal is of the form $J = I_1\lambda^{-1}$ (so $\mathcal{P}_J(\mathbb{Z}_p) = \lambda.\mathcal{P}_{I_1}(\mathbb{Z}_p)$) for some $\lambda \in \mathbb{Q}_p[G]_1^\times \cong \mathbb{Q}_p[\zeta_p]^\times$ with $\lambda \in (\zeta_p - 1)\mathbb{Z}_p[\zeta_p]$.

ii) The full ideal is of the form $J = I_2\lambda^{-1}$ (so $\mathcal{P}_J(\mathbb{Z}_p) = \lambda.\mathcal{P}_{I_2}(\mathbb{Z}_p)$) for some $\lambda \in \mathbb{Q}_p[G]_1^\times \cong \mathbb{Q}_p[\zeta_p]^\times$ with $\lambda \in (\zeta_p - 1)\mathbb{Z}_p[\zeta_p]$.

In case ii), you can see that $m \in \mathcal{P}_J(\mathbb{Z}_p)$ for some λ is equivalent to a).

Now assume we're not in case a). In case i), you can see that $m \in \mathcal{P}_J(\mathbb{Z}_p)$ can only happen when $\lambda \in p\mathbb{Z}_p[\zeta_p]^\times$. Write $\frac{1}{p}\lambda \equiv a + b(\zeta_p - 1) \mod (\zeta_p - 1)^2$ with $a, b \in \{0, \dots, p-1\}$ and $a \neq 0$. Then, $m \in \mathcal{P}_J(\mathbb{Z}_p)$ is equivalent to

$$\begin{aligned}\frac{1}{p}v_{i,j} &\in \frac{(a + b(\zeta_p^i - 1))(a + b(\zeta_p^j - 1))}{a + b(\zeta_p^{i+j} - 1)} + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \\ &= a + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \qquad \text{for } i, j \neq 0 \text{ with } i + j \neq 0,\end{aligned}$$

and

$$\begin{aligned}\frac{1}{p^2}v_{i,-i} &\in (a + b(\zeta_p^i - 1))(a + b(\zeta_p^{-i} - 1)) + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \\ &= a^2 + (\zeta_p - 1)^2\mathbb{Z}_p[\zeta_p] \text{ for } i \neq 0.\end{aligned}$$

□

3.6 Summary

By combining the descriptions of $\mathcal{P}(\mathbb{Q})$ in Examples 3.4, 3.5 and 3.7 with the local analysis performed in Sections 3.4 and 3.5, we obtain the following parametrizations.

Lemma 3.40. *Let $n = 2$. The projection $\mathcal{P}(\mathbb{Q}) \to V_{11} \cong \mathbb{Q}$ is bijective. The two full ideals of $\mathbb{Z}[G]$ are $I_1 = \mathbb{Z}[G] = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \mod 2\}$ and $I_2 = 2\mathbb{Z} \times \mathbb{Z}$. The image of the injective map $\mathcal{P}_I(\mathbb{Z}) \to V_{11} \cong \mathbb{Q}$ is*

$$\begin{cases} 1 + 4\mathbb{Z}, & I = I_1, \\ 4\mathbb{Z}, & I = I_2. \end{cases}$$

The discriminant of the ring corresponding to $m \in \mathcal{P}_I(\mathbb{Z})$ is v_{11} in both cases. We have $\mathrm{Aut}_1(I) = \{\pm 1\}$ and hence $\mathrm{Aut}_1(I)^{\sigma_1+\sigma_2} = 1$ in both cases.

For any prime q and any $m \in \mathcal{P}_{I\otimes\mathbb{Z}_q}(\mathbb{Z}_q)$, we have $m \in \mathcal{P}^{\max}_{I\otimes\mathbb{Z}_q}(\mathbb{Z}_q)$ if and only if

$$\begin{cases} v_{11} \notin q^2\mathbb{Z}, & q \neq 2,\ I = I_1 \text{ or } I_2, \\ \text{always}, & q = 2,\ I = I_1, \\ \frac{1}{4}v_{11} \notin 4\mathbb{Z} \cup (1 + 4\mathbb{Z}), & q = 2,\ I = I_2. \end{cases}$$

Theorem 1.3 follows easily.

Lemma 3.41. *Let $n = 3$. The projection $\mathcal{P}(\mathbb{Q}) \to V_{11} \cong \mathbb{Q}(\zeta_3)$ is bijective. The two full ideals of $\mathbb{Z}[G]$ are $I_1 = \mathbb{Z}[G] = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}[\zeta_3] \mid a \equiv b \mod (\zeta_3 - 1)\}$ and $I_2 = 3\mathbb{Z} \times \mathbb{Z}[\zeta_3]$. The image of the injective map $\mathcal{P}_I(\mathbb{Z}) \to V_{11} \cong \mathbb{Q}(\zeta_3)$ is*

$$\begin{cases} 1 + 3\mathbb{Z}[\zeta_3], & I = I_1, \\ 3\mathbb{Z}[\zeta_3], & I = I_2. \end{cases}$$

The discriminant of the ring corresponding to $m \in \mathcal{P}_I(\mathbb{Z})$ is $N_{\mathbb{Q}(\zeta_3)|\mathbb{Q}}(v_{11})^2$ in both cases. We have

$$\mathrm{Aut}_1(I) = \begin{cases} \{1, \zeta_3, \zeta_3^2\}, & I = I_1, \\ \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}, & I = I_2, \end{cases}$$

and hence

$$\mathrm{Aut}_1(I)^{\sigma_1+\sigma_1-\sigma_2} = \begin{cases} \{1\}, & I = I_1, \\ \{\pm 1\}, & I = I_2. \end{cases}$$

For any prime q and any $m \in \mathcal{P}_I(\mathbb{Z})$, we have $m \in \mathcal{P}^{\max}_{I\otimes\mathbb{Z}_q}(\mathbb{Z}_q)$ if and only if

$$\begin{cases} v_{11}\mathbb{Z}_q[\zeta_3] \in \{(1),(q_1),(q_2)\}, & q \equiv 1 \mod 3,\ q = q_1q_2 \text{ in } \mathbb{Z}[\zeta_3],\ I = I_1 \text{ or } I_2, \\ v_{11} \in \mathbb{Z}_q[\zeta_3]^\times, & q \equiv 2 \mod 3,\ I = I_1 \text{ or } I_2, \\ \text{always}, & q = 3,\ I = I_1, \\ \frac{1}{3}v_{11} \notin (\zeta_3-1)\mathbb{Z}[\zeta_3] \cup (\{\pm 1\} + 3\mathbb{Z}[\zeta_3]), & q = 3,\ I = I_2. \end{cases}$$

Theorem 1.4 follows easily.

Lemma 3.42. *Let $n = 5$. The projection $\mathcal{P}^{\text{nondeg}}(\mathbb{Q}) \to V_{12}^\times \cong \mathbb{Q}(\zeta_5)^\times$ is bijective. The two full ideals of $\mathbb{Z}[G]$ are $I_1 = \mathbb{Z}[G] = \{(a,b) \in \mathbb{Z} \times \mathbb{Z}[\zeta_5] \mid a \equiv b \mod (\zeta_5 - 1)\}$ and $I_2 = 5\mathbb{Z} \times \mathbb{Z}[\zeta_5]$. For any prime q and any $m \in \mathcal{P}^{\text{nondeg}}(\mathbb{Q})$, we have $m \in \mathcal{P}^{\max}_{I\otimes\mathbb{Z}_q}(\mathbb{Z}_q)$ if and only if:*

If $q \equiv 1 \mod 5$ with decomposition $q = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$ in $\mathbb{Z}[\zeta_5]$ such that $\mathfrak{q}_i = \sigma_i(\mathfrak{q}_1)$,

$$v_{12}\mathbb{Z}_q[\zeta_5] \in \{(1), \mathfrak{q}_1\mathfrak{q}_2, \mathfrak{q}_2\mathfrak{q}_4, \mathfrak{q}_3\mathfrak{q}_1, \mathfrak{q}_4\mathfrak{q}_3\}.$$

If $q \equiv 2,3,4 \mod 5$,

$$v_{12} \in \mathbb{Z}_q[\zeta_5]^\times.$$

If $q = 5$ and $I = I_1$,

$$v_{12} \in 1 + (\zeta_5 - 1)^2\mathbb{Z}[\zeta_5].$$

If $q = 5$ and $I = I_2$,

$$v_{12} \in 5\mathbb{Z}[\zeta_5], \text{ but } \frac{1}{5}v_{12} \notin (\zeta_5-1)\mathbb{Z}[\zeta_5] \cup (\{1,2,3,4\} + (\zeta_5-1)^2\mathbb{Z}[\zeta_5]).$$

The discriminant of the ring corresponding to $m \in \mathcal{P}_I(\mathbb{Z})$ is $N_{\mathbb{Q}(\zeta_5)|\mathbb{Q}}(v_{12})^2$ in both cases. We have

$$\mathrm{Aut}_1(I) = \begin{cases} \langle \zeta_5, -(1+\zeta_5)^2 \rangle, & I = I_1, \\ \langle -\zeta_5, 1+\zeta_5 \rangle, & I = I_2, \end{cases}$$

and hence

$$\mathrm{Aut}_1(I)^{\sigma_1+\sigma_2-\sigma_3} = \begin{cases} \langle -(\zeta_5 + \zeta_5^{-1})^2 \rangle, & I = I_1, \\ \langle -1, \zeta_5 + \zeta_5^{-1} \rangle, & I = I_2. \end{cases}$$

Theorem 1.6 follows easily, noting that the elements of $\mathrm{Aut}_1(I_2)^{\sigma_1+\sigma_2-\sigma_3}/\mathrm{Aut}_1(I_1)^{\sigma_1+\sigma_2-\sigma_3}$ are represented by $1, -1, (\zeta_5 + \zeta_5^{-1}), -(\zeta_5 + \zeta_5^{-1})$, which reduce to $1,4,2,3$ modulo $(\zeta_5-1)^2$.

To show that the Dirichlet series

$$D^{\max}(s) = \sum_{R \text{ maximal } G\text{-ext. of } \mathbb{Z}} \mathrm{disc}(R)^{-s}$$

is

$$D^{\max}(s) = \left(1 + 4 \cdot 5^{-8s}\right) \prod_{q \equiv 1 \mod 5} \left(1 + 4q^{-4s}\right),$$

it only remains to make use of the fact that the canonical map

$$\mathbb{Z}[\zeta_5]^\times \to (\mathbb{Z}[\zeta_5]/(\zeta_5-1)^2)^\times/\{1,2,3,4\}$$

is injective with kernel $\langle -1, \zeta_5 + \zeta_5^{-1} \rangle$. Hence, for any $t \in \mathbb{Z}[\zeta_5]$ with $t \not\equiv 0 \mod (\zeta_5 - 1)$, there is exactly one $[r] \in \mathbb{Z}[\zeta_5]^\times/\langle -1, \zeta_5 + \zeta_5^{-1} \rangle$ such that rt satisfies condition c) in Theorem 1.6. For any $t \in 5\mathbb{Z}[\zeta_5] \backslash 5(\zeta_5-1)\mathbb{Z}[\zeta_5]$, there are exactly four such $[r]$.

One can similarly show that the Dirichlet series

$$D^{\mathrm{nondeg}}(s) = \sum_{R \text{ nondeg. } G\text{-ext. of } \mathbb{Z}} \mathrm{disc}(R)^{-s}$$

is

$$\begin{aligned} D^{\mathrm{nondeg}}(s) &= \left(1 + 5 \cdot \sum_{a=4}^{\infty} 5^{-2as}\right) \prod_{q \neq 5} f_q^{\mathrm{nondeg}}(q^{-s}) \\ &= \left(1 + 5 \cdot \frac{5^{-8s}}{1 - 5^{-2s}}\right) \prod_{q \neq 5} f_q^{\mathrm{nondeg}}(q^{-s}) \end{aligned}$$

where the local factors $f_q^{\mathrm{nondeg}}(x)$ are as in Example 3.24.

Chapter 4

The quaternion group

Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group and let K be a field of characteristic different from 2.

First, recall the subgroup structure and the representation theory of G. The subgroups of G are

$$1, \{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}, G.$$

They are normal subgroups of G with respective quotients

$$G, (\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 1.$$

In addition to the discriminant $\mathrm{disc}(R)$ of a nondegenerate G-extension R, we will also look at its *conductor*

$$\mathrm{cond}(R) = \frac{\mathrm{disc}(R)}{\mathrm{disc}(R^{\{\pm 1\}})}.$$

We similarly define $\mathrm{cond}(m) = \frac{\mathrm{disc}(m)}{\mathrm{disc}^{\{\pm 1\}}(m)}$ and $\mathrm{cond}_I(m) = \frac{\mathrm{disc}_I(m)}{\mathrm{disc}_I^{\{\pm 1\}}(m)}$.

We write the elements of $(\mathbb{Z}/2\mathbb{Z})^2$ as $00, 01, 10, 11$. The quotient $G/\{\pm 1\}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ via

$$1 \mapsto 00, \quad i \mapsto 01, \quad j \mapsto 10, \quad k \mapsto 11.$$

Let us fix preimages

$$\varphi_{00} = 1, \quad \varphi_{01} = -i, \quad \varphi_{10} = -j, \quad \varphi_{11} = -k.$$

The four irreducible representations of $(\mathbb{Z}/2\mathbb{Z})^2$ produce four irreducible representations of G over K:

$$\mathrm{triv} = \mathrm{sgn}_{00}, \quad \mathrm{sgn}_i = \mathrm{sgn}_{01}, \quad \mathrm{sgn}_j = \mathrm{sgn}_{10}, \quad \mathrm{sgn}_k = \mathrm{sgn}_{11}$$

given by

$$\begin{array}{cccc}
\mathrm{triv}(\pm 1) = +1 & \mathrm{triv}(\pm i) = +1 & \mathrm{triv}(\pm j) = +1 & \mathrm{triv}(\pm k) = +1 \\
\mathrm{sgn}_i(\pm 1) = +1 & \mathrm{sgn}_i(\pm i) = +1 & \mathrm{sgn}_i(\pm j) = -1 & \mathrm{sgn}_i(\pm k) = -1 \\
\mathrm{sgn}_j(\pm 1) = +1 & \mathrm{sgn}_j(\pm i) = -1 & \mathrm{sgn}_j(\pm j) = +1 & \mathrm{sgn}_j(\pm k) = -1 \\
\mathrm{sgn}_k(\pm 1) = +1 & \mathrm{sgn}_k(\pm i) = -1 & \mathrm{sgn}_k(\pm j) = -1 & \mathrm{sgn}_k(\pm k) = +1
\end{array}$$

We shall also consider the standard four-dimensional representation $\mathrm{std} : G \to \mathbb{H}(K)$ where $\mathbb{H}(K) = \{a + bi + cj + dk \mid a, b, c, d \in K\}$ is the ring of Hamilton quaternions over K.

We obtain the Artin–Wedderburn decomposition

$$K[G] \cong K \times K \times K \times K \times \mathbb{H}(K)$$

corresponding to the representations $\mathrm{triv}, \mathrm{sgn}_i, \mathrm{sgn}_j, \mathrm{sgn}_k, \mathrm{std}$.

Let us fix some notation regarding the ring of quaternions.

Definition 4.1. For any $h = a + bi + cj + dk \in \mathbb{H}(K)$, define its *real part* $\Re(h) = h^{\Re} = a$ and its *imaginary part* $\Im(h) = h^{\Im} = bi + cj + dk$. An element h is called *real* if $h = \Re(h)$ and *purely imaginary* if $h = \Im(h)$. Denote the set of purely imaginary quaternions by $\mathbb{H}^{\Im}(K)$. We further define the *conjugate* $h^* = a - bi - cj - dk$ and the *norm* $N(h) = a^2 + b^2 + c^2 + d^2$. An element $h \in \mathbb{H}(K)$ is invertible if and only if $N(h) \neq 0$. We then have $h^{-1} = \frac{1}{N(h)} h^*$. Also note that $(h_1 h_2)^* = h_2^* h_1^*$ and $\Re(h_1 h_2) = \Re(h_2 h_1)$ for all $h_1, h_2 \in \mathbb{H}(K)$.

Remark 4.2. The standard representation is irreducible over K (and $\mathbb{H}(K)$ is a division ring) if and only if $a^2 + b^2 + c^2 + d^2 = 0$ has no nontrivial solution over K. Otherwise, it splits as $\mathrm{std} \cong \mathrm{std}' \oplus \mathrm{std}'$ for an irreducible two-dimensional representation std'. Then, $\mathbb{H}(K)$ is isomorphic to $M_2(K)$. Assume there is such an isomorphism $f : \mathbb{H}(K) \to M_2(K)$ of K-algebras. Let $h \in \mathbb{H}(K)$. Then, the real part is $\Re(h) = \frac{1}{2}\operatorname{Tr}(f(h))$. The imaginary part corresponds to $f(\Im(h)) = f(h) - \frac{1}{2}\operatorname{Tr}(f(h))I_2$. Real quaterions correspond to multiples of the identity matrix. Purely imaginary quaternions correspond to trace-free matrices (elements of $\mathfrak{sl}_2(K) \subset M_2(K)$). The conjugate corresponds to $f(h^*) = \operatorname{Tr}(f(h))I_2 - f(h) = \operatorname{adj}(f(h))$, the adjugate matrix of $f(h)$. The norm is $N(h) = \det(f(h))$. The tensor products of irreducible representations of G decompose as follows:

$\otimes$	triv	sgn_i	sgn_j	sgn_k	std'
triv	triv	sgn_i	sgn_j	sgn_k	std'
sgn_i	sgn_i	triv	sgn_k	sgn_j	std'
sgn_j	sgn_j	sgn_k	triv	sgn_i	std'
sgn_k	sgn_k	sgn_j	sgn_i	triv	std'
std'	std'	std'	std'	std'	$\mathrm{triv} \oplus \mathrm{sgn}_i \oplus \mathrm{sgn}_j \oplus \mathrm{sgn}_k$

This decomposition reflects the shape of the multiplication table of a G-extension (see Table 4.1).

Now, let us decompose $\mathcal{H} \cong \bigoplus_{V_1, V_2, W} \operatorname{Hom}_G(\operatorname{End}(V_1) \otimes \operatorname{End}(V_2) \to \operatorname{End}(W))$ into irreducible representations of $K[G]^\times$. Note that, as representations of G, we have $\operatorname{End}(\mathrm{sgn}_a) \cong \mathrm{sgn}_a [\cong K]$ for all a and $\operatorname{End}(\mathrm{std}) \cong \mathrm{std} [\cong \mathbb{H}(K)]$.

Lemma 4.3. *The following is a description of the elements of all nonzero spaces* $\operatorname{Hom}_G(\operatorname{End}(V_1) \otimes \operatorname{End}(V_2) \to \operatorname{End}(W))$ *where the representations* V_1, V_2, W *of* G *are among the representations* triv, sgn_i, sgn_j, sgn_k, std *defined above. We also give a formula for the action of*

$$\lambda = (\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11}, \lambda_{\mathrm{std}}) \in K^\times \times K^\times \times K^\times \times K^\times \times \mathbb{H}(K)^\times = K[G]^\times$$

on each such space.

- *For all* $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$, *elements* t *of*

$$\operatorname{Hom}_G(\operatorname{End}(\mathrm{sgn}_a) \otimes \operatorname{End}(\mathrm{sgn}_b) \to \operatorname{End}(\mathrm{sgn}_{a+b}))$$

  are in bijection with numbers $u_{a,b} \in K$ *via*

$$t(x \otimes y) = \frac{1}{8} u_{a,b} x y.$$

The action is given by

$$\lambda.u_{a,b} = \frac{\lambda_a\lambda_b}{\lambda_{a+b}} \cdot u_{a,b}.$$

- *For all $a \in (\mathbb{Z}/2\mathbb{Z})^2$, elements t of*

$$\mathrm{Hom}_G(\mathrm{End}(\mathrm{sgn}_a) \otimes \mathrm{End}(\mathrm{std}) \to \mathrm{End}(\mathrm{std}))$$

are in bijection with quaternions $v_a \in \mathbb{H}(K)$ via

$$t(x \otimes y) = \frac{1}{8} x\varphi_a y v_a.$$

The action is given by

$$\lambda.v_a = \lambda_a \cdot \lambda_{\mathrm{std}} v_a \lambda_{\mathrm{std}}^{-1}.$$

We can further decompose $v_a = v_a^{\Re} + v_a^{\Im}$. The action on these two summands is given by

$$\lambda.v_a^{\Re} = \lambda_a \cdot v_a^{\Re}$$

and

$$\lambda.v_a^{\Im} = \lambda_a \cdot \lambda_{\mathrm{std}} v_a^{\Im} \lambda_{\mathrm{std}}^{-1}.$$

- *Similarly, for all $a \in (\mathbb{Z}/2\mathbb{Z})^2$, elements t of*

$$\mathrm{Hom}_G(\mathrm{End}(\mathrm{std}) \otimes \mathrm{End}(\mathrm{sgn}_a) \to \mathrm{End}(\mathrm{std}))$$

are in bijection with quaternions $v'_a \in \mathbb{H}(K)$ via

$$t(x \otimes y) = \frac{1}{8} \varphi_a x v'_a y.$$

The action on v'_a is defined exactly like the action on v_a.

- *For all $a \in (\mathbb{Z}/2\mathbb{Z})^2$, elements t of*

$$\mathrm{Hom}_G(\mathrm{End}(\mathrm{std}) \otimes \mathrm{End}(\mathrm{std}) \to \mathrm{End}(\mathrm{sgn}_a))$$

are in bijection with quaternions $w_a \in \mathbb{H}(K)$ via

$$t(x \otimes y) = \frac{1}{2} \Re(\varphi_a x w_a y^*).$$

The action is given by

$$\lambda.w_a = \frac{1}{\lambda_a} \cdot \lambda_{\mathrm{std}} w_a \lambda_{\mathrm{std}}^*.$$

Again, decompose $w_a = w_a^{\Re} + w_a^{\Im}$. The action on these two summands is given by

$$\lambda.w_a^{\Re} = \frac{N(\lambda_{\mathrm{std}})}{\lambda_a} \cdot w_a^{\Re}$$

and

$$\lambda.w_a^{\Im} = \frac{1}{\lambda_a} \cdot \lambda_{\mathrm{std}} w_a^{\Im} \lambda_{\mathrm{std}}^*.$$

Therefore elements m of $\mathcal{H}$ exactly correspond to tuples

$$((u_{a,b})_{a,b}, (v_a^{\Re})_a, (v_a^{\Im})_a, (v_a'^{\Re})_a, (v_a'^{\Im})_a, (w_a^{\Re})_a, (w_a^{\Im})_a)$$

and we obtain a corresponding decomposition

$$\begin{aligned}\mathcal{H}(K) &\cong \bigoplus_{a,b} U_{a,b} \oplus \bigoplus_a V_a^{\Re} \oplus \bigoplus_a V_a^{\Im} \oplus \bigoplus_a V_a'^{\Re} \oplus \bigoplus_a V_a'^{\Im} \oplus \bigoplus_a W_a^{\Re} \oplus \bigoplus_a W_a^{\Im} \\ &\cong \bigoplus_{a,b} K \oplus \bigoplus_a K \oplus \bigoplus_a \mathbb{H}^{\Im}(K) \oplus \bigoplus_a K \oplus \bigoplus_a \mathbb{H}^{\Im}(K) \oplus \bigoplus_a K \oplus \bigoplus_a \mathbb{H}^{\Im}(K)\end{aligned}$$

of $\mathcal{H}(K)$ into irreducible $K[G]^\times$-representations.

The trivial map $\pi \in \mathcal{H}(K)$ corresponds to the tuple with $u_{a,b} = 1$ and $v_a = v_a' = w_a = \varphi_a^{-1}$ for all a, b.

Proof. You can verify that $\varphi_a \mathrm{std}(g) \varphi_a^{-1} = \mathrm{sgn}_a(g)\mathrm{std}(g)$ for all $a \in (\mathbb{Z}/2\mathbb{Z})^2$ and $g \in G$. It is then easy to see that all of the elements t defined above are indeed G-invariant and to translate the action of $K[G]^\times$ on $\mathcal{H}(K) = \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$ to an action on the summands $u_{a,b}, v_a, v_a', w_a$. In total, we have constructed a space of G-invariant maps of dimension

$$\sum_{a,b \in (\mathbb{Z}/2\mathbb{Z})^2} 1 + \sum_{a \in (\mathbb{Z}/2\mathbb{Z})^2} 4 + \sum_{a \in (\mathbb{Z}/2\mathbb{Z})^2} 4 + \sum_{a \in (\mathbb{Z}/2\mathbb{Z})^2} 4 = 64.$$

On the other hand, according to Remark 2.20, the dimension of $\mathcal{H}(K) = \mathrm{Hom}_G(K[G] \otimes K[G] \to K[G])$ is also $|G|^2 = 64$, so we have indeed constructed all G-invariant maps. You can check by hand that the element m of $\mathcal{H}(K)$ with $u_{a,b} = 1$ and $v_a = v_a' = w_a = \varphi_a^{-1}$ for all a indeed satisfies $m(e \otimes e) = e$ and $m(e \otimes g) = 0$ for all $e \neq g \in G$. Then, G-invariance proves that $m = \pi$. □

For reference, we now state the unit, symmetry and associativity conditions in terms of the parameters given above. We skip the straightforward proofs of the following lemmas, as they are not necessary for showing the parametrization of nondegenerate extensions in Theorem $4.11_{\mathbb{H}^{\Im}(K)}$.

Lemma 4.4. *For an element $((u_{a,b})_{a,b}, (v_a^{\Re})_a, (v_a^{\Im})_a, (v_a'^{\Re})_a, (v_a'^{\Im})_a, (w_a^{\Re})_a, (w_a^{\Im})_a)$ of $\mathcal{H}(K)$, the unit condition (Cu) is equivalent to the following equations:*

- $u_{00,a} = 1$ *for all* $a \in (\mathbb{Z}/2\mathbb{Z})^2$.
- $v_{00} = 1$.

Lemma 4.5. *The symmetry condition (Cs) is equivalent to the following equations:*

- $u_{a,b} = u_{b,a}$ *for all* $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$.
- $v_a = v_a'$ *for all* $a \in (\mathbb{Z}/2\mathbb{Z})^2$.
- $w_{00}^{\Im} = 0$.
- $w_a^{\Re} = 0$ *for all nonzero* $a \in (\mathbb{Z}/2\mathbb{Z})^2$.

Lemma 4.6. *Assuming (Cs), the associativity condition (Ca) is equivalent to the following equations:*

- $u_{a,b}u_{a+b,c} = u_{b,c}u_{a,b+c}$ *for all* $a, b, c \in (\mathbb{Z}/2\mathbb{Z})^2$.
- $\varphi_{a+b} \cdot u_{a,b}v_{a+b} = \varphi_a\varphi_b \cdot v_b v_a$ *for all* $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$. *Note that always* $\varphi_{a+b} = \pm\varphi_a\varphi_b$.
- $\varphi_b\varphi_a \cdot v_a v_b = \varphi_a\varphi_b \cdot v_b v_a$ *for all* $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$. *Note that always* $\varphi_b\varphi_a = \pm\varphi_a\varphi_b$.
- $\varphi_b\varphi_a \cdot v_a w_b = \varphi_{a+b} \cdot u_{a,a+b}w_{a+b}$.
- $\varphi_b\varphi_a \cdot v_a w_b = \varphi_a^*\varphi_b \cdot w_b v_a^*$. *Note that* $\varphi_b\varphi_a = \pm\varphi_a^*\varphi_b$.
- $\sum_a \Re(\varphi_a x w_a y^*)\varphi_a z v_a = \sum_a \varphi_a x v_a \Re(\varphi_a y w_a z^*)$ *for all* $x, y, z \in \mathbb{H}(K)$.

Lemma 4.7. *The H-discriminants and conductor of an element $m \in \mathcal{P}(K)$ can be computed as follows:*

$$\begin{aligned}
\operatorname{disc}(m) &= u_{01,01}u_{10,10}u_{11,11}w_{00}^4 \\
\operatorname{disc}^{\{\pm 1\}}(m) &= u_{01,01}u_{10,10}u_{11,11} \\
\operatorname{disc}^{\{\pm 1,\pm i\}}(m) &= u_{01,01} \\
\operatorname{disc}^{\{\pm 1,\pm j\}}(m) &= u_{10,10} \\
\operatorname{disc}^{\{\pm 1,\pm k\}}(m) &= u_{11,11} \\
\operatorname{cond}(m) &= w_{00}^4
\end{aligned}$$

Proof. To show this, you can either use Theorem 2.59 over a field in which std splits, or directly compute the discriminants by hand. □

4.1 Nondegenerate extensions

Lemma 4.8. *If the G-extension is nondegenerate, then $v_{00}^{\Im} = v_{00}'^{\Im} = w_{00}^{\Im} = 0$ and $v_a^{\Re} = v_a'^{\Re} = w_a^{\Re} = 0$ for all $a \neq 00$. On the other hand, the remeaining summands $u_{a,b} \in K$, $v_{00}^{\Re} \in K$, $v_a^{\Im} = v_a'^{\Im} \in \mathbb{H}^{\Im}(K)$ (for $a \neq 00$), $w_{00}^{\Re} \in K$, $w_a^{\Im} \in \mathbb{H}^{\Im}(K)$ (for $a \neq 00$) are all invertible in K, respectively $\mathbb{H}(K)$.*

Proof. The statement clearly holds for the trivial element π of $\mathcal{P}^{\mathrm{nondeg}}(K)$. Since the points in $\mathcal{P}^{\mathrm{nondeg}}$ all lie on the same $K^{\mathrm{sep}}[G]_1^{\times}$-orbit (see Corollary 2.35), it therefore holds for any element of $\mathcal{P}^{\mathrm{nondeg}}(K)$. □

Remark 4.9. Therefore, the subspace of $\mathcal{H}(K)$ spanned by $\mathcal{P}^{\mathrm{nondeg}}(K)$ can be written as

$$\bigoplus_{a,b} U_{a,b} \oplus V_{00}^{\Re} \oplus \bigoplus_{a \neq 00} V_a^{\Im} \oplus W_{00}^{\Re} \bigoplus_{a \neq 00} W_a^{\Im}.$$

For $K = \mathbb{C}$, this corresponds to the decomposition of the subspace of $\mathcal{H}(K)$ spanned by $\mathcal{P}^{\mathrm{nondeg}}(K)$ given in section 6.6: For example, $u_{01,01}$ corresponds to an element of $\mathrm{Sym}^2(\mathrm{sgni})$ and $u_{01,10}$ corresponds to an element of $\frac{\mathrm{stdi}\cdot\mathrm{stdj}}{\mathrm{stdk}}$ and $w_{00}^{\Re}$ corresponds to an element of $\mathrm{Alt}^2(\mathrm{std})$ and $v_{01}^{\Im}$ corresponds to an element of $\mathfrak{sl}(\mathrm{std}) \cdot \mathrm{sgni}$ and $w_{01}^{\Im}$ corresponds to an element of $\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{sgni}}$.

Remark 4.10. There are degenerate elements of $\mathcal{P}(K)$ with $v_{01}^{\Re} \neq 0$. The space $\mathcal{P}$ parametrizing G-extensions is therefore not irreducible! The corresponding degenerate G-extensions cannot be approximated by nondegenerate G-extensions.

To construct an example, take $v_{00} = v_{01} = 1$ and $v_{10} = v_{11} = 0$ and $w_{00} = w_{01} = w_{10} = w_{11} = 0$ and $u_{a,b}$ according to the following table:

$u_{a,b}$	00	01	10	11
00	1	1	1	1
01	1	−1	−1	1
10	1	−1	0	0
11	1	1	0	0

The corresponding degenerate G-extension of K has a basis $1, x_1, x_2, x_3, y_1, y_i, y_j, y_k$ with the following multiplication table:

$\cdot$	1	x_1	x_2	x_3	y_1	y_i	y_j	y_k
1	1	x_1	x_2	x_3	y_1	y_i	y_j	y_k
x_1	x_1	-1	$-x_3$	x_2	$-y_i$	y_1	y_k	$-y_j$
x_2	x_2	$-x_3$	0	0	0	0	0	0
x_3	x_3	x_2	0	0	0	0	0	0
y_1	y_1	$-y_i$	0	0	0	0	0	0
y_i	y_i	y_1	0	0	0	0	0	0
y_j	y_j	y_k	0	0	0	0	0	0
y_k	y_k	$-y_j$	0	0	0	0	0	0

4.1.1 Parametrization in terms of purely imaginary quaternions

Theorem 4.11$_{\mathbb{H}^{\Im}(K)}$**.** *Elements of $\mathcal{P}^{\mathrm{nondeg}}(K)$ are in bijection with tuples $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ such that $d \in K^\times$, $v_i \in \mathbb{H}^{\Im}(K)^\times$, $e_i \in K^\times$ satisfy the equations*

$$e_1 v_1 = v_2 v_3, \qquad e_2 v_2 = v_3 v_1, \qquad e_3 v_3 = v_1 v_2. \tag{4.1$_{\mathbb{H}^{\Im}(K)}$}$$

An element $(\lambda_1, \lambda_2, \lambda_3, \lambda_H)$ of $K[G]_1^\times$ acts on the tuple $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ in $\mathcal{P}^{\mathrm{nondeg}}(K)$ as follows:

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_H).(d, v_1, v_2, v_3, e_1, e_2, e_3) = (d', v_1', v_2', v_3', e_1', e_2', e_3'),$$

where

$$\begin{aligned} d' &= N(\lambda_H) \cdot d, \\ v_i' &= \lambda_i \cdot \lambda_H v_i \lambda_H^{-1}, \\ e_i' &= \frac{\lambda_1 \lambda_2 \lambda_3}{\lambda_i^2} \cdot e_i. \end{aligned}$$

The trivial element $\pi \in \mathcal{P}^{\mathrm{nondeg}}(K)$ corresponds to the tuple $(1, i, j, k, 1, 1, 1)$.

The bijection is given by

$$\begin{gathered} u_{00,00} = u_{00,01} = u_{00,10} = u_{00,11} = u_{01,00} = u_{10,00} = u_{11,00} = 1, \\ u_{01,01} = N(v_1), \qquad u_{10,10} = N(v_2), \qquad u_{11,11} = N(v_3), \\ u_{11,10} = u_{10,11} = e_1, \qquad u_{01,11} = u_{11,01} = e_2, \qquad u_{10,01} = u_{01,10} = e_3, \\ v_{00} = v_{00}' = 1, \qquad v_{01} = v_{01}' = v_1, \qquad v_{10} = v_{10}' = v_2, \qquad v_{11} = v_{11}' = v_3, \\ w_{00} = d, \qquad w_{01} = \frac{d}{N(v_1)} \cdot v_1, \qquad w_{10} = \frac{d}{N(v_2)} \cdot v_2, \qquad w_{11} = \frac{d}{N(v_3)} \cdot v_3. \end{gathered}$$

The H-discriminants and conductor of $m = (d, v_1, v_2, v_3, e_1, e_2, e_3) \in \mathcal{P}^{\mathrm{nondeg}}(K)$ can be computed as follows:

$$\begin{aligned} \mathrm{disc}(m) &= N(v_1)N(v_2)N(v_3)d^4 \\ \mathrm{disc}^{\{\pm 1\}}(m) &= N(v_1)N(v_2)N(v_3) \\ \mathrm{disc}^{\{\pm 1, \pm i\}}(m) &= N(v_1) \\ \mathrm{disc}^{\{\pm 1, \pm j\}}(m) &= N(v_2) \\ \mathrm{disc}^{\{\pm 1, \pm k\}}(m) &= N(v_3) \\ \mathrm{cond}(m) &= d^4 \end{aligned}$$

Proof. You can easily verify that $\pi \in \mathcal{P}^{\mathrm{nondeg}}(K)$ corresponds to the tuple $(1, i, j, k, 1, 1, 1)$. The equations (4.1$_{\mathbb{H}^{\Im}(K)}$) and the equations defining the bijection are all $K^{\mathrm{sep}}[G]_1^\times$-invariant. Furthermore, the space of tuples with $d \in (K^{\mathrm{sep}})^\times$, $v_i \in \mathbb{H}^{\Im}(K^{\mathrm{sep}})^\times$, $e_i \in (K^{\mathrm{sep}})^\times$ satisfying the equa-

tions ($4.1_{\mathbb{H}^{\Im}(K)}$) defines an irreducible seven-dimensional variety (see Remark $4.14_{\mathbb{H}^{\Im}(K)}$ below). Since $K^{\mathrm{sep}}[G]_1^\times$ also defines a seven-dimensional variety, and $K^{\mathrm{sep}}[G]_1^\times.\pi = \mathcal{P}^{\mathrm{nondeg}}(K)$, the map $m \mapsto (d, v_1, v_2, v_3, e_1, e_2, e_3)$ must be surjective. (Alternatively, you could explicitly check the unit, symmetry, and associativity conditions.) □

We will procrastinate proving the following remarks until we have an equivalent, but slightly more intuitive description of $\mathcal{P}^{\mathrm{nondeg}}(K)$ in the next section.

Remark $4.12_{\mathbb{H}^{\Im}(K)}$. Note that ($4.1_{\mathbb{H}^{\Im}(K)}$) implies that

$$N(v_i) = \frac{e_1 e_2 e_3}{e_i}.$$

Remark $4.13_{H^{\Im}(K)}$. The map $(d, v_1, v_2, v_3, e_1, e_2, e_3) \mapsto (d, v_1, v_2, v_3)$ is injective. Its image is the set of tuples such that $d \in K^\times$, $v_i \in \mathbb{H}^{\Im}(K)^\times$ and

$$\Re(v_2 v_3) = \Re(v_3 v_1) = \Re(v_1 v_2) = 0.$$

Remark $4.14_{\mathbb{H}^{\Im}(K)}$. The map $(d, v_1, v_2, v_3, e_1, e_2, e_3) \mapsto (d, e_3, v_1, v_2)$ is injective. Its image is the set of tuples such that $d \in K^\times$, $e_3 \in K^\times$, $v_1, v_2 \in \mathbb{H}^{\Im}(K)^\times$ and

$$\Re(v_1 v_2) = 0.$$

4.1.2 Parametrization in terms of vectors

For any vector v, denote its length by $|v|$. We can identify the space K^3 with the space $\mathbb{H}^{\Im}(K)$ of purely imaginary quaternions via the map $f : K^3 \to \mathbb{H}^{\Im}(K)$ sending (b, c, d) to $bi + cj + dk$. Note that for any $v_1 = (b_1, c_1, d_1)$ and $v_2 = (b_2, c_2, d_2)$, we get

$$\begin{aligned} f(v_1)f(v_2) &= (b_1 i + c_1 j + d_1 k)(b_2 i + c_2 j + d_2 k) \\ &= (-b_1 b_2 - c_1 c_2 - d_1 d_2) \\ &\quad + (c_1 d_2 - d_1 c_2)i + (d_1 b_2 - b_1 d_2)j + (b_1 c_2 - c_1 b_2)k \\ &= -v_1 \cdot v_2 + f(v_1 \times v_2), \end{aligned}$$

where $\cdot$ denotes the standard inner product and $\times$ denotes the cross product in K^3. In particular,

$$N(f(v)) = -f(v)^2 = |v|^2$$

for all $v \in K^3$. For any $h = a + bi + cj + dk \in \mathbb{H}(K)$ and $v \in K^3$, we have

$$hf(v)h^{-1} = f(r(h)v),$$

where $r(h) \in \mathrm{SO}_3(K)$ is the orthogonal matrix

$$r(h) = \frac{1}{N(h)} \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2bc - 2ad & 2bd + 2ac \\ 2bc + 2ad & a^2 - b^2 + c^2 - d^2 & 2cd - 2ab \\ 2bd - 2ac & 2cd + 2ab & a^2 - b^2 - c^2 + d^2 \end{pmatrix}.$$

Then, our parametrization in Theorem $4.11_{\mathbb{H}^{\Im}(K)}$ translates to the following:

Theorem 4.11_{K^3}. *Elements of $\mathcal{P}^{\mathrm{nondeg}}(K)$ are in bijection with tuples $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ such that $d \in K^\times$, $v_i \in K^3$ with $|v_i|^2 \neq 0$, $e_i \in K^\times$ satisfy the equations*

$$e_1 v_1 = v_2 \times v_3, \qquad e_2 v_2 = v_3 \times v_1, \qquad e_3 v_3 = v_1 \times v_2. \tag{4.1_{K^3}}$$

An element $(\lambda_1, \lambda_2, \lambda_3, \lambda_H)$ *of* $K[G]_1^\times$ *acts on the tuple* $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ *in* $\mathcal{P}^{\mathrm{nondeg}}(K)$ *as follows:*

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_H).(d, v_1, v_2, v_3, e_1, e_2, e_3) = (d', v_1', v_2', v_3', e_1', e_2', e_3'),$$

where

$$\begin{aligned} d' &= N(\lambda_H) \cdot d, \\ v_i' &= \lambda_i \cdot r(\lambda_H) v_i, \\ e_i' &= \frac{\lambda_1\lambda_2\lambda_3}{\lambda_i^2} \cdot e_i. \end{aligned}$$

The trivial element $\pi \in \mathcal{P}^{\mathrm{nondeg}}(K)$ *corresponds to the tuple* $(1, (1,0,0), (0,1,0), (0,0,1), 1, 1, 1)$. *The bijection is given by*

$$\begin{gathered} u_{00,00} = u_{00,01} = u_{00,10} = u_{00,11} = u_{01,00} = u_{10,00} = u_{11,00} = 1, \\ u_{01,01} = |v_1|^2, \qquad u_{10,10} = |v_2|^2, \qquad u_{11,11} = |v_3|^2, \\ u_{11,10} = u_{10,11} = e_1, \qquad u_{01,11} = u_{11,01} = e_2, \qquad u_{10,01} = u_{01,10} = e_3, \\ v_{00} = v_{00}' = 1, \qquad v_{01} = v_{01}' = f(v_1), \qquad v_{10} = v_{10}' = f(v_2), \qquad v_{11} = v_{11}' = f(v_3), \\ w_{00} = d, \qquad w_{01} = \frac{d}{|v_1|^2} f(v_1), \qquad w_{10} = \frac{d}{|v_2|^2} f(v_2), \qquad w_{11} = \frac{d}{|v_3|^2} f(v_3). \end{gathered}$$

The H*-discriminants of* $m = (d, v_1, v_2, v_3, e_1, e_2, e_3) \in \mathcal{P}^{\mathrm{nondeg}}(K)$ *can be computed as follows:*

$$\begin{aligned} \mathrm{disc}(m) &= |v_1|^2 |v_2|^2 |v_3|^2 d^4 \\ \mathrm{disc}^{\{\pm 1\}}(m) &= |v_1|^2 |v_2|^2 |v_3|^2 \\ \mathrm{disc}^{\{\pm 1, \pm i\}}(m) &= |v_1|^2 \\ \mathrm{disc}^{\{\pm 1, \pm j\}}(m) &= |v_2|^2 \\ \mathrm{disc}^{\{\pm 1, \pm k\}}(m) &= |v_3|^2 \\ \mathrm{cond}(m) &= d^4 \end{aligned}$$

Remark 4.12$_{K^3}$**.** Note that (4.1_{K^3}) implies that

$$|v_i|^2 = \frac{e_1 e_2 e_3}{e_i},$$

and in particular $(|v_1||v_2||v_3|)^2 = (e_1 e_2 e_3)^2$.

Proof. First, note that (4.1_{K^3}) implies that v_1 and v_2 are orthogonal. Hence,

$$e_2 e_3 v_3 = v_1 \times e_2 v_2 = v_1 \times (v_3 \times v_1) = |v_1|^2 \cdot v_3,$$

so $e_2 e_3 = |v_1|^2$. The other two equations $e_1 e_3 = |v_2|^2$ and $e_1 e_2 = |v_3|^2$ can be proved similarly. □

Remark 4.13$_{K^3}$**.** The map $(d, v_1, v_2, v_3, e_1, e_2, e_3) \mapsto (d, v_1, v_2, v_3)$ is injective. Its image is the set of tuples such that $d \in K^\times$, $v_i \in K^3$ with $|v_i|^2 \neq 0$ and the vectors v_1, v_2, v_3 are pairwise orthogonal:

$$v_2 \cdot v_3 = v_3 \cdot v_1 = v_1 \cdot v_2 = 0.$$

Proof. The fact that v_1, v_2, v_3 are pairwise orthogonal clearly follows from (4.1_{K^3}). On the other hand, if v_1, v_2 are orthogonal vectors of nonzero length, then the vectors orthogonal to both v_1 and v_2 are exactly the multiples of the cross product $v_1 \times v_2$. Hence, as the length of v_3 is also nonzero, there exists some unique number $e_3 \in K^\times$ such that $e_3 v_3 = v_1 \times v_2$. You can similarly construct e_1 and e_2. □

Remark 4.14$_{K^3}$**.** The map $(d, v_1, v_2, v_3, e_1, e_2, e_3) \mapsto (d, e_3, v_1, v_2)$ is injective. Its image is the set of tuples such that $d \in K^\times$, $e_3 \in K^\times$, and $v_1, v_2 \in K^3$ with $|v_1|^2, |v_2|^2 \neq 0$ are orthogonal:

$$v_1 \cdot v_2 = 0.$$

Proof. The remaining parameters v_3, e_1, e_2 can be computed as follows:

$$v_3 = \frac{v_1 \times v_2}{e_3}, \qquad e_1 = \frac{|v_2|^2}{e_3}, \qquad e_2 = \frac{|v_1|^2}{e_3}.$$

Then,

$$v_2 \times v_3 = \frac{v_2 \times (v_1 \times v_2)}{e_3} = \frac{|v_2|^2}{e_3} \cdot v_1 = e_1 v_1$$

and similarly $v_3 \times v_1 = e_2 v_2$. □

Remark 4.15. Consider a tuple $(d, v_1, v_2, v_3, e_1, e_2, e_3) \in \mathcal{P}^{\text{nondeg}}(K)$, corresponding to a G-extension L of K with a fixed isomorphism $L \cong K[G]$ of left $K[G]$-modules. Write $v_i = (v_{i1}, v_{i2}, v_{i3})$. Table 4.1 gives the explicit multiplication table of L with respect to the basis

$$\begin{aligned} 1 &= (8,0,0,0,0),\\ x_1 &= (0,8,0,0,0),\\ x_2 &= (0,0,8,0,0),\\ x_3 &= (0,0,0,8,0),\\ y_1 &= (0,0,0,0,4),\\ y_i &= (0,0,0,0,4i),\\ y_j &= (0,0,0,0,4j),\\ y_k &= (0,0,0,0,4k), \end{aligned}$$

of $L \cong K[G] \cong K \times K \times K \times K \times \mathbb{H}(K)$.

We have

$$L \cong K[x_1, x_2, y_1]/(x_1^2 - |v_1|^2, x_2^2 - |v_2|^2, y_1^2 x_1 x_2 - d(x_1 x_2 + v_{11} x_2 + v_{22} x_1 + v_{33} e_3)).$$

Interpreted carefully, we can write

$$L \cong K\left[\sqrt{d\left(1 + \frac{v_{11}}{\sqrt{|v_1|^2}} + \frac{v_{22}}{\sqrt{|v_2|^2}} + \frac{v_{33}}{\sqrt{|v_3|^2}}\right)}\right].$$

The subfields are

$$L^{\{\pm 1\}} \cong K[x_1, x_2]/(x_1^2 - |v_1|^2, x_2^2 - |v_2|^2) \cong K\left[\sqrt{|v_1|^2}, \sqrt{|v_2|^2}\right] = K\left[\sqrt{|v_1|^2}, \sqrt{|v_2|^2}, \sqrt{|v_3|^2}\right],$$

$$L^{\{\pm 1, \pm i\}} \cong K[x_1]/(x_1^2 - |v_1|^2) \cong K\left[\sqrt{|v_1|^2}\right],$$

$$L^{\{\pm 1, \pm j\}} \cong K[x_2]/(x_2^2 - |v_2|^2) \cong K\left[\sqrt{|v_2|^2}\right],$$

$$L^{\{\pm 1, \pm k\}} \cong K[x_3]/(x_3^2 - |v_3|^2) \cong K\left[\sqrt{|v_3|^2}\right].$$

Table 4.1: Multiplication table of a G-extension L

$\cdot$	1	x_1	x_2	x_3	y_1	y_i	y_j	y_k
1	1	x_1	x_2	x_3	y_1	y_i	y_j	y_k
x_1	$\cdots$	e_2e_3	e_3x_3	e_2x_2	$v_{11}y_1 - v_{12}y_k + v_{13}y_j$	$v_{11}y_i + v_{12}y_j + v_{13}y_k$	$-v_{11}y_j + v_{12}y_i + v_{13}y_1$	$-v_{11}y_k - v_{12}y_1 + v_{13}y_i$
x_2	$\cdots$	$\cdots$	e_1e_3	e_1x_1	$v_{21}y_k + v_{22}y_1 - v_{23}y_i$	$v_{21}y_j - v_{22}y_i - v_{23}y_1$	$v_{21}y_i + v_{22}y_j + v_{23}y_k$	$v_{21}y_1 - v_{22}y_k + v_{23}y_j$
x_3	$\cdots$	$\cdots$	$\cdots$	e_1e_2	$-v_{31}y_j + v_{32}y_i + v_{33}y_1$	$v_{31}y_k + v_{32}y_1 - v_{33}y_i$	$-v_{31}y_1 + v_{32}y_k - v_{33}y_j$	$v_{31}y_i + v_{32}y_j + v_{33}y_k$
y_1	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$d(1 + \frac{v_{11}}{e_2e_3}x_1 + \frac{v_{22}}{e_1e_3}x_2 + \frac{v_{33}}{e_1e_2}x_3)$	$d(\frac{v_{32}}{e_1e_2}x_3 - \frac{v_{23}}{e_1e_3}x_2)$	$d(\frac{v_{13}}{e_2e_3}x_1 - \frac{v_{31}}{e_1e_2}x_3)$	$d(\frac{v_{21}}{e_1e_3}v_j - \frac{v_{12}}{e_2e_3}x_1)$
y_i	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$d(1 + \frac{v_{11}}{e_2e_3}x_1 - \frac{v_{22}}{e_1e_3}x_2 - \frac{v_{33}}{e_1e_2}x_3)$	$d(\frac{v_{12}}{e_2e_3}x_1 + \frac{v_{21}}{e_1e_3}x_2)$	$d(\frac{v_{13}}{e_2e_3}x_1 + \frac{v_{31}}{e_1e_2}x_3)$
y_j	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$d(1 - \frac{v_{11}}{e_2e_3}x_1 + \frac{v_{22}}{e_1e_3}x_2 - \frac{v_{33}}{e_1e_2}x_3)$	$d(\frac{v_{23}}{e_1e_3}x_2 + \frac{v_{32}}{e_1e_2}x_3)$
y_k	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$d(1 - \frac{v_{11}}{e_2e_3}x_1 - \frac{v_{22}}{e_1e_3}x_2 + \frac{v_{33}}{e_1e_2}x_3)$

Remark 4.16. In [19, Theorem 4], Kiming used Galois cohomology to show that a field extension $K(\sqrt{a},\sqrt{b})$ of K of degree four is contained in a Galois extension L of K with Galois group G if and only if there exist orthogonal vectors $v_1, v_2 \in K^3$ such that $|v_1|^2 = a$ and $|v_2|^2 = b$. This is a direct consequence of the parametrization given above.

4.1.3 Parametrization in terms of trace-free matrices

Recall Remark 4.2: If $a^2 + b^2 + c^2 + d^2 = 0$ has a nontrivial solution in K, then there is an isomorphism $f : M_2(K) \to \mathbb{H}(K)$. Purely imaginary quaternions correspond exactly to trace-free matrices. The norm of a quaternion corresponds to the determinant of the corresponding matrix. Our parametrization can then be rewritten as follows:

Theorem 4.11$_{\mathfrak{sl}_2(K)}$. *Elements of $\mathcal{P}^{\text{nondeg}}(K)$ are in bijection with tuples $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ such that $d \in K^\times$, $v_i \in \mathfrak{sl}_2(K)$ with $\det(v_i) \neq 0$, $e_i \in K^\times$ satisfy the equations*

$$e_1 v_1 = v_2 v_3, \qquad e_2 v_2 = v_3 v_1, \qquad e_3 v_3 = v_1 v_2. \tag{$4.1_{\mathfrak{sl}_2(K)}$}$$

An element $(\lambda_1, \lambda_2, \lambda_3, \lambda_H)$ of the group $K^\times \times K^\times \times K^\times \times \mathrm{GL}_2(K) \cong K[G]_1^\times$ acts on the tuple $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ in $\mathcal{P}^{\text{nondeg}}(K)$ as follows:

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_H).(d, v_1, v_2, v_3, e_1, e_2, e_3) = (d', v_1', v_2', v_3', e_1', e_2', e_3'),$$

where

$$\begin{aligned} d' &= \det(\lambda_H) \cdot d, \\ v_i' &= \lambda_i \cdot \lambda_H v_i \lambda_H^{-1}, \\ e_i' &= \frac{\lambda_1\lambda_2\lambda_3}{\lambda_i^2} \cdot e_i. \end{aligned}$$

The bijection is given by

$$\begin{gathered} u_{00,00} = u_{00,01} = u_{00,10} = u_{00,11} = u_{01,00} = u_{10,00} = u_{11,00} = 1, \\ u_{01,01} = \det(v_1), \qquad u_{10,10} = \det(v_2), \qquad u_{11,11} = \det(v_3), \\ u_{11,10} = u_{10,11} = e_1, \qquad u_{01,11} = u_{11,01} = e_2, \qquad u_{10,01} = u_{01,10} = e_3, \\ v_{00} = v_{00}' = 1, \qquad v_{01} = v_{01}' = f(v_1), \qquad v_{10} = v_{10}' = f(v_2), \qquad v_{11} = v_{11}' = f(v_3), \\ w_{00} = d, \qquad w_{01} = \frac{d}{\det(v_1)} \cdot f(v_1), \qquad w_{10} = \frac{d}{\det(v_2)} \cdot f(v_2), \qquad w_{11} = \frac{d}{\det(v_3)} \cdot f(v_3). \end{gathered}$$

The H-discriminants and conductor of $m = (d, v_1, v_2, v_3, e_1, e_2, e_3) \in \mathcal{P}^{\text{nondeg}}(K)$ can be computed as follows:

$$\begin{aligned} \mathrm{disc}(m) &= \det(v_1)\det(v_2)\det(v_3)d^4 \\ \mathrm{disc}^{\{\pm 1\}}(m) &= \det(v_1)\det(v_2)\det(v_3) \\ \mathrm{disc}^{\{\pm 1, \pm i\}}(m) &= \det(v_1) \\ \mathrm{disc}^{\{\pm 1, \pm j\}}(m) &= \det(v_2) \\ \mathrm{disc}^{\{\pm 1, \pm k\}}(m) &= \det(v_3) \\ \mathrm{cond}(m) &= d^4 \end{aligned}$$

Remark 4.12$_{\mathfrak{sl}_2(K)}$. Note that $(4.1_{\mathfrak{sl}_2(K)})$ implies that

$$\det(v_i) = \frac{e_1 e_2 e_3}{e_i}.$$

Remark 4.13$_{\mathfrak{sl}_2(K)}$**.** The map $(d, v_1, v_2, v_3, e_1, e_2, e_3) \mapsto (d, v_1, v_2, v_3)$ is injective. Its image is the set of tuples such that $d \in K^\times$, $v_i \in \mathfrak{sl}_2(K)$ with $\det(v_i) \neq 0$ and

$$\mathrm{Tr}(v_2 v_3) = \mathrm{Tr}(v_3 v_1) = \mathrm{Tr}(v_1 v_2) = 0.$$

Remark 4.14$_{\mathfrak{sl}_2(K)}$**.** The map $(d, v_1, v_2, v_3, e_1, e_2, e_3) \mapsto (d, e_3, v_1, v_2)$ is injective. Its image is the set of tuples such that $d \in K^\times$, $e_3 \in K^\times$, $v_1, v_2 \in \mathfrak{sl}_2(K)$ with $\det(v_1), \det(v_2) \neq 0$ and

$$\mathrm{Tr}(v_1 v_2) = 0.$$

The parametrization in terms of trace-free matrices is particularly useful when $K = \mathbb{Q}_p$ for some odd prime p, as it will allow us to more easily understand the maximality conditions. We can in fact construct an isomorphism $\mathbb{H}(\mathbb{Q}_p) \cong M_2(\mathbb{Q}_p)$ preserving integrality and will always use such an isomorphism in the following:

Lemma 4.17. *Let $p \neq 2$ be an odd prime. Then, there is an isomorphism $\mathbb{H}(\mathbb{Q}_p) \cong M_2(\mathbb{Q}_p)$ that restricts to an isomorphism $\mathbb{H}(\mathbb{Z}_p) \cong M_2(\mathbb{Z}_p)$, where $\mathbb{H}(\mathbb{Z}_p)$ denotes the ring of Hamilton quaternions $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}_p$.*

Proof. By the pigeon-hole principle, there exists a solution $(\alpha, \beta) \in \mathbb{F}_p^2$ to $\alpha^2 + \beta^2 + 1 = 0$. Since p is odd, we can use Hensel's Lemma to lift it to a solution $(\alpha, \beta) \in \mathbb{Z}_p^2$. Then, we obtain an isomorphism $\mathbb{H}(\mathbb{Q}_p) \to M_2(\mathbb{Q}_p)$ given by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} -\beta & -\alpha \\ -\alpha & \beta \end{pmatrix}, \qquad k \mapsto \begin{pmatrix} \alpha & -\beta \\ -\beta & -\alpha \end{pmatrix}.$$

The inverse map is given by

$$1 + \beta j - \alpha k \leftarrow\!\shortmid \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \qquad 1 - \beta j + \alpha k \leftarrow\!\shortmid \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix},$$
$$-i + \alpha j + \beta k \leftarrow\!\shortmid \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \qquad i + \alpha j + \beta k \leftarrow\!\shortmid \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}. \qquad \square$$

4.2 Integral structure, full ideals

Let S be a Dedekind domain whose field of fractions K has characteristic different from 2.

Definition 4.18. The ring $\mathbb{H}'(S)$ of *Lipschitz quaternions* is the ring of quaternions $a + bi + cj + dk$ with $a, b, c, d \in S$.

The ring $\mathbb{H}(S) \subseteq \mathbb{H}'(S[\frac{1}{2}])$ of *Hurwitz quaternions* is the ring of quaternions $a + bi + cj + dk$ such that either a, b, c, d all lie in S or a, b, c, d all lie in $\frac{1}{2} + S$.

Remark 4.19. If 2 is invertible in S, then $\mathbb{H}(S) = \mathbb{H}'(S)$.

Unlike the ring of Lipschitz quaternions, the ring $\mathbb{H}(\mathbb{Z})$ of Hurwitz quaternions over $\mathbb{Z}$ is a principal ideal ring:

Theorem 4.20. *All ideals of $\mathbb{H}(\mathbb{Z})$ are principal.*

Proof. See [13, Section 5.1] for a proof that one can perform Euclidean division in $\mathbb{H}(\mathbb{Z})$. $\square$

Given the isomorphism

$$K[G] \xrightarrow{\sim} K \times K \times K \times K \times \mathbb{H}(K),$$

it is natural to consider its restriction

$$S[G] \hookrightarrow S \times S \times S \times S \times \mathbb{H}(S).$$

Its image contains

$$8S \times 8S \times 8S \times 8S \times 2\mathbb{H}'(S).$$

In particular, if we let

$$\overline{S[G]} = S \times S \times S \times S \times \mathbb{H}(S),$$

we have $8\overline{S[G]} \subseteq S[G] \subseteq \overline{S[G]}$. If 2 is invertible in S, then $S[G] = \overline{S[G]}$. We will also write

$$\overline{S[G]}_1^\times = S^\times \times S^\times \times S^\times \times \mathbb{H}(S)^\times \supseteq S[G]_1^\times$$

and note that if 2 is invertible in S, then $S[G]_1^\times = \overline{S[G]}_1^\times$.

Given that $8\overline{\mathbb{Z}[G]} \subseteq \mathbb{Z}[G] \subseteq \overline{\mathbb{Z}[G]}$ and that $\overline{\mathbb{Z}[G]}$ is a principal ideal ring, one can use Lemma 2.68 and a simple computer program to enumerate all 701 equivalence classes of full ideals I of $\mathbb{Z}[G]$.

For any odd prime p, we have

$$\mathbb{Z}_p[G] = \overline{\mathbb{Z}_p[G]} \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times M_2(\mathbb{Z}_p).$$

Lemma 2.67 therefore shows that $\mathbb{Z}_p[G]$ is also a principal ideal ring for any odd prime p.

For counting G-extensions, we will later need the following lemma relating unitary full ideal classes of $\mathbb{Z}[G]$ and unitary full ideal classes of $\mathbb{Z}_2[G]$.

Lemma 4.21. *For any unitary full ideal J_2 of $\mathbb{Z}_2[G]$, we have*

$$\sum_{\substack{\text{unitary full} \\ \text{ideal class } I \text{ of } \mathbb{Z}[G] \\ \text{with } I \otimes \mathbb{Z}_2 \cong J_2}} [\overline{\mathbb{Z}[G]}_1^\times : \mathrm{Aut}_1(I)] = [\overline{\mathbb{Z}_2[G]}_1^\times : \mathrm{Aut}_1(J_2)].$$

Remark 4.22. Corollary 2.70 implies that $\mathrm{Aut}_1(I)$ and $\mathrm{Aut}_1(J_2)$ have finite index in $\overline{\mathbb{Z}[G]}_1^\times$ and $\overline{\mathbb{Z}_2[G]}_1^\times$, respectively.

Proof. We describe the relation between full ideals of $\mathbb{Z}[G]$ and full ideals of $\mathbb{Z}_p[G]$ via the ring of adeles of $\mathbb{Q}$. This is motivated by work of Borel [8].

Let $\mathbb{A}_{\mathrm{fin}} = \prod_p' \mathbb{Q}_p$ be the finite part of the adele ring over $\mathbb{Q}$ and let $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. We make use of the fact that full ideals I of $\mathbb{Z}$ (resp. $\mathbb{H}(\mathbb{Z})$, $\mathbb{Z}[G]$) can be written as $U = \bigcap_p T_p$, where $T_p = U \otimes \mathbb{Z}_p$ is a full ideal of $\mathbb{Z}_p$ (resp. $\mathbb{H}(\mathbb{Z}_p)$, $\mathbb{Z}_p[G]$) for all primes p, and $T_p = \mathbb{Z}_p$ (resp. $\mathbb{H}(\mathbb{Z}_p)$, $\mathbb{Z}_p[G]$) for almost all primes p.

The facts that $\mathbb{Z}$ and $\mathbb{H}(\mathbb{Z})$ are principal ideal rings imply that $\mathbb{Q}^\times$ acts transitively on $\hat{\mathbb{Z}} \backslash \mathbb{A}_{\mathrm{fin}}^\times$ by right multiplication and that $\mathbb{H}(\mathbb{Q})^\times$ acts transitively on $\mathbb{H}(\hat{\mathbb{Z}})^\times \backslash \mathbb{H}(\mathbb{A}_{\mathrm{fin}})^\times$ by right multiplication. Hence, $\mathbb{Q}[G]_1^\times$ acts transitively on $\overline{\hat{\mathbb{Z}}[G]}_1^\times \backslash \mathbb{A}_{\mathrm{fin}}[G]_1^\times$ by right multiplication.

For any odd prime p, there is (up to equivalence) only one unitary full ideal of $\mathbb{Z}_p[G]$: the ideal $J_p = \mathbb{Z}_p[G]$. Any unitary full ideal I of $\mathbb{Z}[G]$ such that $I \otimes \mathbb{Z}_2 \cong J_2$ is therefore equivalent to one of the form $\bigcap_p J_p \lambda_p$, where $\lambda_p \in \mathrm{Aut}_1(J_p) \backslash \overline{\mathbb{Q}_p[G]}_1^\times$ for all primes p. Using that $\mathbb{Q}[G]_1^\times$ acts transitively on $\overline{\hat{\mathbb{Z}}[G]}_1^\times \backslash \mathbb{A}_{\mathrm{fin}}[G]_1^\times$, we can assume that $\lambda_p \in \mathrm{Aut}_1(J_p) \backslash \overline{\mathbb{Z}_p[G]}_1^\times$. Note that $\mathrm{Aut}_1(J_2)$ is a subgroup of $\overline{\mathbb{Z}_2[G]}_1^\times$ of finite index and $\overline{\mathbb{Z}_p[G]}_1^\times = \mathbb{Z}_p[G]_1^\times = \mathrm{Aut}_1(J_p)$ for all odd primes p. The group $\overline{\mathbb{Z}[G]}_1^\times$ acts on $\prod_p \mathrm{Aut}_1(J_p) \backslash \overline{\mathbb{Z}_p[G]}_1^\times$ by right multiplication. The orbits correspond to equivalence classes of unitary full ideals I satisfying $I \otimes \mathbb{Z}_2 \cong J_2$, and the stabilizer of I is $\mathrm{Aut}_1(I)$. □

4.3 Good primes

Let $p \neq 2$ be an odd prime. As we have seen earlier, $I = \mathbb{Z}_p[G]$ is the only unitary full ideal up to equivalence.

We will now compute the subset $\mathcal{P}^{\text{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p) \subseteq \mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$, first in terms of the parametrization given in Theorem 4.11_{K^3}, then in terms of the parametrization given in Theorem $4.11_{\mathfrak{sl}_2(K)}$.

Lemma 4.23_{K^3}. *Let $p \neq 2$ be an odd prime. An element $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ of $\mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$ as in Theorem 4.11_{K^3} lies in $\mathcal{P}^{\text{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$ (i.e., satisfies the closedness condition (Cc)) if and only if $d \in \mathbb{Z}_p$, $v_i \in \mathbb{Z}_p^3$, $e_i \in \mathbb{Z}_p$, and $\frac{d}{|v_i|^2} \cdot v_i \in \mathbb{Z}_p^3$ for all i.*

Proof. This follows directly from the decomposition of $\mathcal{H}$ given in Lemma 4.3 and the definition of the bijection constructed in Theorem 4.11_{K^3}. It is also obvious from the explicit multiplication table given in Remark 4.15 and Table 4.1. □

Lemma $4.23_{\mathfrak{sl}_2(K)}$. *Let $p \neq 2$ be an odd prime. An element $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ of $\mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$ as in Theorem $4.11_{\mathfrak{sl}_2(K)}$ (employing the isomorphism $\mathbb{H}(\mathbb{Q}_p) \cong M_2(\mathbb{Q}_p)$ constructed in Lemma 4.17) lies in $\mathcal{P}^{\text{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$ (i.e., satisfies the closedness condition (Cc)) if and only if $d \in \mathbb{Z}_p$, $v_i \in \mathfrak{sl}_2(\mathbb{Z}_p)$, $e_i \in \mathbb{Z}_p$, and $\frac{d}{\det(v_i)} \cdot v_i \in \mathfrak{sl}_2(\mathbb{Z}_p)$ for all i.*

Lemma 4.24. *An element $m = (d, v_1, v_2, v_3, e_1, e_2, e_3)$ of $\mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$ as in Theorem $4.11_{\mathfrak{sl}_2(K)}$ lies in $\mathcal{P}^{\max}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$ if and only if $\frac{d}{e_1e_2e_3} \in \mathbb{Z}_p$, $v_i \in \mathfrak{sl}_2(\mathbb{Z}_p)$, $e_i \in \mathbb{Z}_p$, and $d \in \mathbb{Z}_p$ is squarefree.*

Proof. "⇐" Assume $d \in \mathbb{Z}_p$ is squarefree and $v_1, v_2, v_3 \in \mathfrak{sl}_2(\mathbb{Z}_p)$ and $e_1, e_2, e_3 \in \mathbb{Z}_p$ and $e_1e_2e_3 \mid d$. As $\det(v_i) = \frac{e_1e_2e_3}{e_i^2}$, these conditions clearly imply that $m \in \mathcal{P}^{\text{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$. Assume the extension is nonmaximal. Recall that this means that there exists some $\lambda \in \mathbb{Z}_p[G] \cap \mathbb{Q}_p[G]_1^\times \setminus \mathbb{Z}_p[G]_1^\times$ such that $m' = \lambda^{-1}.m \in \mathcal{P}^{\text{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$. Write $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_H)$ and $m' = (d', v_1', v_2', v_3', e_1', e_2', e_3')$. We have $\mathbb{Z}_p \ni e_2'e_3' = \lambda_1^{-2}e_2e_3$. Since $e_2e_3 \mid d$ and d is squarefree, this implies that $\lambda_1 \in \mathbb{Z}_p^\times$. Similarly, $\lambda_2, \lambda_3 \in \mathbb{Z}_p^\times$. Furthermore, $\mathbb{Z}_p \ni d' = \det(\lambda_H)^{-1}d$. Since d is squarefree, this implies that either $\det(\lambda_H) \in \mathbb{Z}_p^\times$ (so $\lambda_H \in \mathrm{GL}_2(\mathbb{Z}_p)$ and therefore $\lambda \in \mathbb{Z}_p[G]_1^\times$), or $\det(\lambda_H) \in p\mathbb{Z}_p^\times$ and $d' \in \mathbb{Z}_p^\times$. In the latter case, note that $\mathbb{Z}_p \ni \det(\frac{d'}{\det(v_3')} \cdot v_3') = \frac{d'^2}{e_1'e_2'}$, so we must have $e_1', e_2' \in \mathbb{Z}_p^\times$. Similarly, $e_3' \in \mathbb{Z}_p^\times$. Since $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_p^\times$, it follows that $e_1, e_2, e_3 \in \mathbb{Z}_p^\times$. Multiplying λ_H on the left and right by appropriate elements of $\mathrm{GL}_2(\mathbb{Z}_p) \subset \mathbb{Z}_p[G]_1^\times$, we can assume that λ_H is in Smith Normal Form, so

$$\lambda_H = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Then, writing

$$v_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & -a_1 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & -a_2 \end{pmatrix}, \qquad v_3 = \begin{pmatrix} a_3 & b_3 \\ c_3 & -a_3 \end{pmatrix},$$

we get

$$\mathfrak{sl}_2(\mathbb{Z}_p) \ni v_1' = \lambda_1^{-1}\lambda_H^{-1}v_1\lambda_H = \lambda_1^{-1}\begin{pmatrix} a_1 & b_1/p \\ c_1p & -a_1 \end{pmatrix}.$$

We must therefore have $b_1 \equiv 0 \mod p$. Similarly, $b_2 \equiv 0 \mod p$ and $b_3 \equiv 0 \mod p$. Remember that $0 \equiv \mathrm{Tr}(v_1v_2) \equiv 2a_1a_2 \mod p$, so one of the numbers a_1 and a_2 must be divisible by p, say $a_1 \equiv 0 \mod p$. Hence, $p \mid \det(v_1) = e_2e_3$, contradicting our earlier conclusion that $e_2, e_3 \in \mathbb{Z}_p^\times$.

"⇒" Assume $m \in \mathcal{P}^{\max}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$. We must in particular have $d \in \mathbb{Z}_p$, $v_i \in \mathfrak{sl}_2(\mathbb{Z}_p)$, $e_i \in \mathbb{Z}_p$, and $\frac{d}{\det(v_i)} \cdot v_i \in \mathfrak{sl}_2(\mathbb{Z}_p)$. Assume for contradiction that $p^2 \mid d$ or $e_1e_2e_3 \nmid d$. Without loss of generality, $e_1 \mid e_2$ and $e_2 \mid e_3$.

Remember that $\det(v_1)$ is the discriminant of the degree two extension of $\mathbb{Z}_p$ fixed by $\{\pm 1, \pm i\}$. Discriminants of degree two extensions of $\mathbb{Z}_p$ (with p odd) are always squarefree, so e_2e_3, and similarly e_1e_2 and e_1e_3 must be squarefree. Hence, $e_1, e_2 \in \mathbb{Z}_p^\times$ and either $e_3 \in \mathbb{Z}_p^\times$ or $e_3 \in p\mathbb{Z}_p^\times$. In particular, none of the three matrices v_1, v_2, v_3 with determinants e_2e_3, e_1e_3, e_1e_2 can be divisible by p. Then, $\frac{d}{\det(v_1)} \cdot v_1$ implies that $e_2e_3 = \det(v_1) \mid d$. In fact, $e_1e_2e_3 \mid d$, since $e_1 \in \mathbb{Z}_p^\times$.

If $p^2 \mid d$, let us explicitly construct some $\lambda \in \mathbb{Z}_p[G] \cap \mathbb{Q}_p[G]_1^\times \backslash \mathbb{Z}_p[G]_1^\times$ such that $m' = \lambda^{-1}.m \in \mathcal{P}^{\mathrm{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$. There are two cases: If $p^2e_1e_2e_3 \mid d$, then we can take $\lambda = (1, 1, 1, \left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right))$ and get $m' = \lambda^{-1}.m \in \mathcal{P}^{\mathrm{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$. If $p \mid e_3$ and $pe_1e_2e_3 \mid d$, then applying an element of $\mathrm{GL}_2(\mathbb{Z}_p) \subset \mathbb{Z}_p[G]_1^\times$ to m, we can turn v_1 into Frobenius Normal Form modulo p: either $v_1 \equiv \left(\begin{smallmatrix} a_1 & 0 \\ 0 & -a_1 \end{smallmatrix}\right) \mod p$ for some $a_1 \in \mathbb{Z}_p$, or $v_1 \equiv \left(\begin{smallmatrix} 0 & b_1 \\ 1 & 0 \end{smallmatrix}\right) \mod p$ for some $b_1 \in \mathbb{Z}_p$. As $\det(v_1) \equiv 0 \mod p$, but $v_1 \not\equiv 0 \mod p$, the only possibility that remains is $v_1 \equiv \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \mod p$. Since $\mathrm{Tr}(v_1v_2) = \mathrm{Tr}(v_1v_3) = 0$, the matrices v_2 and v_3 must be of the form $\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)$ modulo p. We can then take $\lambda = (1, 1, 1, \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right))$ and get $m' = \lambda^{-1}.m \in \mathcal{P}^{\mathrm{nondeg}}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$. □

Corollary 4.25. *Let $p \neq 2$ be an odd prime. An element $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ of $\mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$ as in Theorem 4.11$_{K^3}$ lies in $\mathcal{P}^{\max}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$ if and only if $\frac{d}{e_1e_2e_3} \in \mathbb{Z}_p$, $v_i \in \mathbb{Z}_p^3$, $e_i \in \mathbb{Z}_p$, and $d \in \mathbb{Z}_p$ is squarefree. (In particular, the vectors v_1, v_2, v_3 cannot be divisible by p.)*

Let us also rewrite the maximality condition in terms of the parameters e_3, v_1, v_2, d:

Corollary 4.26. *Let $p \neq 2$ be an odd prime. An element $(d, v_1, v_2, v_3, e_1, e_2, e_3)$ of $\mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$ as in Theorem 4.11$_{K^3}$ lies in $\mathcal{P}^{\max}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p)$ if and only if the following conditions hold: The number e_3 lies in $\mathbb{Z}_p$. The vectors v_1, v_2 lie in $\mathbb{Z}_p^3$. Furthermore, $|v_1|^2$ is squarefree and divisible by e_3 and the vector $v_1 \times v_2$ is also divisible by e_3. Finally, $d \in \mathbb{Z}_p$ is squarefree and divisible by $\frac{|v_1|^2|v_2|^2}{e_3}$.*

Proof. Recall that $v_3 = \frac{v_1 \times v_2}{e_3}$ and $e_2 = \frac{|v_1|^2}{e_3}$ and $e_1 = \frac{|v_2|^2}{e_3}$. Hence, $e_1e_2e_3 = \frac{|v_1|^2|v_2|^2}{e_3}$.
The squarefreeness of $|v_1|^2$ is necessary since $|v_1|^2 = e_2e_3$ divides d. Furthermore, note that $|v_3|^2 = \frac{|v_1|^2|v_2|^2}{e_3^2}$. Hence, if $v_3 \in \mathbb{Z}_p^3$ and $|v_1|^2 \in \mathbb{Z}_p$ is squarefree, then $|v_2|^2$ is also divisible by e_3. □

For counting maximal G-extensions of $\mathbb{Z}$, we will need to know how many maximal G-extensions $\mathbb{Z}_p$ has, weighted by the inverse of the number of automorphisms.

Lemma 4.27. *For any odd prime p, we have*

$$\sum_{R \text{ maximal } G\text{-extension of } \mathbb{Z}_p} \frac{|\operatorname{cond}(R)|_p^{1/4}}{\#\operatorname{Aut}(R)} = 1 + 4p^{-1}.$$

Proof. Remember that nondegenerate G-extensions of $\mathbb{Q}_p$ correspond to continuous homomorphisms $f : \mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p) \to G$, modulo conjugation by elements of G. Automorphisms of G-extensions correspond to centralizers of the image. As in Corollary 2.38, we can therefore write

$$\sum_{R \text{ maximal } G\text{-extension of } \mathbb{Z}_p} \frac{|\operatorname{cond}(R)|_p^{1/4}}{\#\operatorname{Aut}(R)} = \frac{1}{\#G} \sum_{f:\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)\to G} |\operatorname{cond}(f)|_p^{1/4}.$$

Now, use the description of the Galois group of the maximal tame extension of $\mathbb{Q}_p$ (see [18, section 5]): the group is topologically generated by (a lift of) the Frobenius φ and a map τ sending $p^{1/k}$ to $\zeta_k p^{1/k}$, subject to the relation $\varphi \circ \tau \circ \varphi^{-1} = \tau^p$. If $f(\tau) = +1$, there are 8 possible values of $f(\varphi)$, and $\operatorname{cond}(f) = 1$. If $f(\tau) = -1$, there are 8 possible values of $f(\varphi)$, and $\operatorname{cond}(f) = p^4$. If $f(\tau) = \pm i$ (or, similarly, $f(\tau) = \pm j$ or $f(\tau) = \pm k$), there are 4 possible values of $f(\varphi)$ (namely $\pm 1, \pm i$ if $p \equiv 1 \mod 4$ and $\pm j, \pm k$ if $p \equiv 3 \mod 4$), and $\operatorname{cond}(f) = p^4$. □

4.4 Bad prime

For counting maximal G-extensions of $\mathbb{Z}$ by conductor, we won't need an explicit description of $\mathcal{P}_I^{\max}(\mathbb{Z}_2)$ similar to Lemma 4.24. It suffices to count maximal G-extensions of $\mathbb{Z}_2$ as in Lemma 4.27.

Lemma 4.28. *We have*

$$\sum_{R \text{ maximal } G\text{-extension of } \mathbb{Z}_2} \frac{|\operatorname{cond}(R)|_p^{1/4}}{\#\operatorname{Aut}(R)} = 3.$$

Proof. Again,

$$\sum_{R \text{ maximal } G\text{-extension of } \mathbb{Z}_2} \frac{|\operatorname{cond}(R)|_p^{1/4}}{\#\operatorname{Aut}(R)} = \frac{1}{\#G} \sum_{f:\operatorname{Gal}(\overline{\mathbb{Q}}_2|\mathbb{Q}_2)\to G} |\operatorname{cond}(f)|_p^{1/4}.$$

We use the database of local fields described in [17] and also accessible at [30]. Separately study each possible isomorphism class of the image of f in G.

Up to automorphisms of G, there are six surjective homomorphisms $\operatorname{Gal}(\overline{\mathbb{Q}}_2|\mathbb{Q}_2) \to G$ (there are six Galois extensions of $\mathbb{Q}_2$ with Galois group G). They all have conductor 2^{16}. The group G has 24 automorphisms.

Up to automorphisms of $\mathbb{Z}/4\mathbb{Z}$, there are twelve surjective homomorphisms $\operatorname{Gal}(\overline{\mathbb{Q}}_2|\mathbb{Q}_2) \to \mathbb{Z}/4\mathbb{Z}$. There are 6 embeddings $\mathbb{Z}/4\mathbb{Z} \hookrightarrow G$ and the conductor of the composition $\operatorname{Gal}(\overline{\mathbb{Q}}_2|\mathbb{Q}_2) \to \mathbb{Z}/4\mathbb{Z} \hookrightarrow G$ doesn't depend on the embedding. Modulo the embedding, one homomorphism has conductor 1, one has conductor 2^8, two have conductor 2^{12}, eight have conductor 2^{16}.

There are seven surjective homomorphisms $\operatorname{Gal}(\overline{\mathbb{Q}}_2|\mathbb{Q}_2) \to \mathbb{Z}/2\mathbb{Z}$. There is a unique embedding $\mathbb{Z}/2\mathbb{Z} \hookrightarrow G$. One map has conductor 1, two have conductor 2^8, four have conductor 2^{12}.

Finally, there is one trivial map $\operatorname{Gal}(\overline{\mathbb{Q}}_2|\mathbb{Q}_2) \to 1 \hookrightarrow G$. Therefore, the sum is

$$\frac{1}{8}(6 \cdot 24 \cdot 2^{-4} + (1 \cdot 1 + 1 \cdot 2^{-2} + 2 \cdot 2^{-3} + 8 \cdot 2^{-4}) \cdot 6 + (1 \cdot 1 + 2 \cdot 2^{-2} + 4 \cdot 2^{-3}) \cdot 1 + 1) = 3. \quad \square$$

4.5 Measures

Let $K = \mathbb{Q}_p$ for some prime p, or $K = \mathbb{R}$. We denote the usual absolute value on K by $|\cdot|_K$. For any vector $v \in K^3$, we write $|v|_K = ||v||_K$ for the valuation of the length of v. If $K = \mathbb{Q}_p$, we will alternatively write $|\cdot|_p$. If $K = \mathbb{R}$, we simply write $|\cdot|$.

For counting maximal G-extensions of bounded conductor, it will be useful to define a Haar measure on the group $K[G]_1^\times$ and a $K[G]_1^\times$-invariant measure on $\mathcal{P}^{\text{nondeg}}(K)$. The technique of defining invariant measures has been used extensively. (See for example [5].) The sets $\mathcal{P}_I^{\max}(\mathbb{Z}_p) \subset \mathcal{P}^{\text{nondeg}}(\mathbb{Q}_p)$ may contain infinitely many elements, but still have finite volume.

Let us endow K and $\mathbb{H}(K)$ with the standard (additive) Haar measure $\mathrm{d}g$ (normalized so that $\operatorname{vol}(\mathbb{Z}_p) = \operatorname{vol}(\mathbb{H}'(\mathbb{Z}_p)) = 1$). We can use it to construct a (multiplicative) Haar measure $d^\times g$ on $K^\times$ by $\mathrm{d}^\times x = |x|_K^{-1}\mathrm{d}x$ and a (multiplicative) Haar measure $\mathrm{d}^\times x$ on $\mathbb{H}(K)^\times$ by $\mathrm{d}^\times x = |N(x)|_K^{-2}\mathrm{d}x$. They combine to a (multiplicative) Haar measure $\mathrm{d}^\times\lambda$ on $K[G]_1^\times = K^\times \times K^\times \times K^\times \times \mathbb{H}(K)^\times$.

As before, we identify $\mathcal{P}^{\text{nondeg}}(K)$ with the space of tuples (e_3, v_1, v_2, d) where $e_3, d \in K^\times$ and $v_1, v_2 \in K^3$ with $|v_1|^2, |v_2|^2 \neq 0$ are orthogonal. Recall that the other parameters v_3, e_1, e_2 can be computed as

$$v_3 = \frac{v_1 \times v_2}{e_3}, \qquad e_1 = \frac{|v_2|^2}{e_3}, \qquad e_2 = \frac{|v_1|^2}{e_3}$$

and that the conductor is given by

$$\operatorname{cond}(m) = d^4.$$

We define a $K[G]_1^\times$-invariant measure $\mathrm{d}m$ on $\mathcal{P}^{\mathrm{nondeg}}(K)$ by

$$\int_{\mathcal{P}^{\mathrm{nondeg}}(K)} \mathrm{d}m \cdot r(m) = \int_{K^\times} \frac{\mathrm{d}e_3}{|e_3|_K} \int_{K^3\setminus\{|\cdot|^2=0\}} \frac{\mathrm{d}v_1}{|v_1|_K^3} \int_{\langle v_1\rangle^\perp\setminus\{|\cdot|^2=0\}} \frac{\mathrm{d}v_2}{|v_2|_K^2} \int_{K^\times} \frac{\mathrm{d}d}{|d|_K} \cdot r(e_3, v_1, v_2, d),$$

where $\mathrm{d}v_1$ is the standard Haar measure on K^3, and $\mathrm{d}v_2$ is the standard area measure on the plane $\langle v_1\rangle^\perp \subsetneq K^3$ perpendicular to v_1. It will also be convenient to consider the measure $\mathrm{d}'m = \mathrm{d}m \cdot |\operatorname{cond}(m)|_K^{1/4} = \mathrm{d}m \cdot |d|_K$ on $\mathcal{P}^{\mathrm{nondeg}}(K)$:

$$\begin{aligned}
&\int_{\mathcal{P}^{\mathrm{nondeg}}(K)} \mathrm{d}'m \cdot r(m) \\
&= \int_{K^\times} \frac{\mathrm{d}e_3}{|e_3|_K} \int_{K^3\setminus\{|\cdot|^2=0\}} \frac{\mathrm{d}v_1}{|v_1|_K^3} \int_{\langle v_1\rangle^\perp\setminus\{|\cdot|^2=0\}} \frac{\mathrm{d}v_2}{|v_2|_K^2} \int_{K^\times} \mathrm{d}d \cdot r(e_3, v_1, v_2, d) \\
&= \int_{K^\times} \mathrm{d}e_3 \int_{K^3\setminus\{|\cdot|^2=0\}} \frac{\mathrm{d}v_1}{|e_3|_K} \int_{\langle v_1\rangle^\perp\setminus\{|\cdot|^2=0\}} \frac{\mathrm{d}v_2}{|v_1|_K|e_3|_K} \int_{K^\times} \frac{\mathrm{d}d}{|v_1|_K^2|v_2|_K^2/|e_3|_K} \cdot r(e_3, v_1, v_2, d).
\end{aligned}$$

The Jacobi matrix for the map $\mathbb{Q}_p[G]_1^\times \to \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$ given by $\lambda \mapsto \lambda.\pi$ at $\lambda = 1$ with respect to the basis $(\mathrm{d}\lambda_1, \mathrm{d}\lambda_2, \mathrm{d}\lambda_3, \mathrm{d}a, \mathrm{d}b, \mathrm{d}c, \mathrm{d}d)$ of the cotangent space $T_1^*\mathbb{Q}_p[G]_1^\times$ and the basis $(\mathrm{d}e_3, \mathrm{d}v_{11}, \mathrm{d}v_{12}, \mathrm{d}v_{13}, \mathrm{d}v_{22}, \mathrm{d}v_{23}, \mathrm{d}d)$ of the cotangent space $T_\pi^*\mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q}_p)$ is

$$\begin{pmatrix}
1 & 1 & -1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & -2 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 \\
0 & 0 & 0 & 2 & 0 & 0 & 0
\end{pmatrix}.$$

Its determinant is 16. Therefore, if $A \subseteq K[G]_1^\times$ is a subgroup of finite measure and if $m_0 \in \mathcal{P}^{\mathrm{nondeg}}(K)$ has finite stabilizer $\mathrm{Stab}_A(m_0)$, then

$$\int_{A.m_0} \mathrm{d}m = |16|_K \cdot \frac{1}{\#\operatorname{Stab}_A(m_0)} \cdot \int_A \mathrm{d}^\times\lambda$$

and, because $\operatorname{cond}(\lambda.m_0)^{1/4} = N(\lambda_H)\operatorname{cond}(m_0)^{1/4}$,

$$\int_{A.m_0} \mathrm{d}m \cdot |\operatorname{cond}_I(m)|_K^{1/4} = |16|_K \cdot \frac{|\operatorname{cond}_I(m_0)|_K^{1/4}}{\#\operatorname{Stab}_A(m_0)} \cdot \int_A \mathrm{d}^\times\lambda \cdot |N(\lambda_H)|_K.$$

For any prime p and any unitary full ideal I of $\mathbb{Z}_p[G]$, consider the local "volume"

$$\mu_{I,p} = \int_{\mathcal{P}_I^{\max}(\mathbb{Z}_p)} \mathrm{d}m \cdot |\operatorname{cond}_I(m)|_p^{1/4}.$$

Remark 4.29. Note that the $K[G]_1^\times$-invariance of $\mathrm{d}m$ together with Remark 2.19 implies that $\mu_{I,p}$ depends only on the equivalence class of the unitary full ideal I.

We can now compute the local "volume" $\mu_{I,p}$ for any odd prime p:

Lemma 4.30. *For any odd prime p and any unitary full ideal I of $\mathbb{Z}_p[G]$, we have*

$$\mu_{I,p} = (1 + 4p^{-1})(1 - p^{-1})^4(1 - p^{-2}).$$

Proof. We have seen above that

$$\mu_{I,p} = \sum_{[m]\in \mathrm{Aut}_1(I)\backslash \mathcal{P}_I^{\max}(\mathbb{Z}_p)} |16|_p \cdot \frac{|\operatorname{cond}_I(m)|_p^{1/4}}{\#\operatorname{Stab}_{\mathrm{Aut}_1(I)}(m)} \cdot \int_{\mathrm{Aut}_1(I)} \mathrm{d}^\times\lambda \cdot |N(\lambda_H)|_p.$$

Remember that $I \cong \mathbb{Z}_p[G]$, so $\mathrm{Aut}_1(I) \cong \mathbb{Z}_p[G]_1^\times \cong \overline{\mathbb{Z}_p[G]_1^\times}$. Therefore,

$$\begin{aligned}\int_{\mathrm{Aut}_1(I)} \mathrm{d}^\times\lambda \cdot |N(\lambda_H)|_p &= \mathrm{vol}(\mathrm{Aut}_1(I)) = \mathrm{vol}(\overline{\mathbb{Z}_p[G]_1^\times}) = \mathrm{vol}(\mathbb{Z}_p^\times)^3 \cdot \mathrm{vol}(\mathrm{GL}_2(\mathbb{Z}_p)) \\ &= (1-p^{-1})^3 \cdot (1-p^{-2})(1-p^{-1}) = (1-p^{-1})^4(1-p^{-2}).\end{aligned}$$

Each orbit $[m] \in \mathrm{Aut}_1(I)\backslash\mathcal{P}_I^{\max}(\mathbb{Z}_p)$ corresponds to exactly one maximal G-extension of $\mathbb{Z}_p$ and the stabilizer of m in $\mathrm{Aut}_1(I)$ is isomorphic to $\mathrm{Aut}(R)$. Hence, using Lemma 4.27, we obtain

$$\begin{aligned}\mu_{I,p} &= \sum_{R \text{ maximal } G\text{-extension of } \mathbb{Z}_p} \frac{|\operatorname{cond}(R)|_p^{1/4}}{\#\operatorname{Aut}(R)} \cdot (1-p^{-1})^4(1-p^{-2}) \\ &= (1+4p^{-1})(1-p^{-1})^4(1-p^{-2}).\end{aligned}$$

□

Similarly, we can compute an appropriate weighted sum of the local "volumes" $\mu_{I,2}$:

Lemma 4.31. *We have*

$$\sum_{\text{unitary full ideal class } I \text{ of } \mathbb{Z}_2[G]} \frac{\mu_{I,2}}{\mathrm{vol}(\mathrm{Aut}_1(I))} = \frac{3}{2^4}.$$

Proof. Again,

$$\mu_{I,2} = \sum_{[m]\in \mathrm{Aut}_1(I)\backslash \mathcal{P}_I^{\max}(\mathbb{Z}_2)} |16|_2 \cdot \frac{|\operatorname{cond}_I(m)|_2^{1/4}}{\#\operatorname{Stab}_{\mathrm{Aut}_1(I)}(m)} \cdot \mathrm{vol}(\mathrm{Aut}_1(I)).$$

The result then follows from Lemma 4.28 as before. □

Corollary 4.32. *Summing over ideal classes of $\mathbb{Z}[G]$, we get*

$$\sum_{\text{unitary full ideal class } I \text{ of } \mathbb{Z}[G]} \frac{\mu_{I\otimes\mathbb{Z}_2,2}}{\#\operatorname{Aut}_1(I)} = \frac{3}{2^{14}}.$$

Proof. Combine the previous lemma and Lemma 4.21 and use that

$$\#\overline{\mathbb{Z}[G]_1^\times} = (\#\mathbb{Z}^\times)^3 \cdot \#\mathbb{H}(\mathbb{Z})^\times = 2\cdot 2\cdot 2\cdot 24 = 3\cdot 2^6$$

and

$$\mathrm{vol}(\overline{\mathbb{Z}_2[G]_1^\times}) = \mathrm{vol}(\mathbb{Z}_2^\times)^3 \cdot \mathrm{vol}(\mathbb{H}(\mathbb{Z}_2)^\times) = (1/2)^3 \cdot (3/2) = 3\cdot 2^{-4}.$$

□

4.6 Counting

We discuss two different ways of counting maximal G-extensions R of $\mathbb{Z}$:

a) by discriminant $\mathrm{disc}(R)$

b) by conductor $\mathrm{cond}(R) = \frac{\mathrm{disc}(R)}{\mathrm{disc}(R^{\{\pm 1\}})}$

Remark 4.33. The conductor $\mathrm{cond}(R)$ is a fourth power for any maximal G-extension R of $\mathbb{Z}$.

Klüners [20, Korollar 7.1] has counted Galois extensions of $\mathbb{Q}$ with Galois group G by discriminant:[1]

Theorem 4.34. *There exists a constant $C_{\mathrm{disc}} > 0$ such that*

$$\#\{\text{max. } G\text{-extension } R \text{ of } \mathbb{Z} \text{ with } |\operatorname{disc}(R)|^{1/4} \leqslant X\} = C_{\mathrm{disc}} \cdot X + o(X).$$

We will show how to use our parametrization to count by conductor:

Theorem 4.35 (See Theorem 1.8)**.** *We have*

$$\#\{\text{max. } G\text{-extension } R \text{ of } \mathbb{Z} \text{ with } |\operatorname{cond}(R)|^{1/4} \leqslant X\} = C_{\mathrm{cond}} \cdot X(\log X)^3 + o(X(\log X)^3).$$

where

$$\begin{aligned} C_{\mathrm{cond}} &= \frac{\pi^2}{2^{11}} \cdot \prod_{p \neq 2} (1 + 4p^{-1})(1 - p^{-1})^4(1 - p^{-2}) \\ &= \frac{1}{2^8} \cdot \prod_{p \neq 2} (1 + 4p^{-1})(1 - p^{-1})^4 \\ &\approx 0.00085271440732599. \end{aligned}$$

There is a fundamental difference between counting by discriminant and counting by conductor: To any G-extension L of $\mathbb{Q}$, associate the subextension $L^{\{\pm 1\}}$ fixed by $\{\pm 1\} \subset G$. It is a $(\mathbb{Z}/2\mathbb{Z})^2$-extension of $\mathbb{Q}$. When ordering G-extensions L of $\mathbb{Q}$ by discriminant, a positive proportion of them have the same associated subextension $L^{\{\pm 1\}}$. (In fact, in terms of our parametrization, a positive proportion of G-extensions have the same vectors v_1, v_2, v_3.) When ordering by conductor, any $(\mathbb{Z}/2\mathbb{Z})^2$-extension occurs in 0% of G-extensions. (In fact, any vector v_1 and any number e_1 occurs in 0% of G-extensions.)

This difference has several consequences:

- It is an obstruction for Klüners's proof to work when counting by conductor: For any $(\mathbb{Z}/2\mathbb{Z})^2$-extension L' of $\mathbb{Q}$, he studies the number of $\mathbb{Z}/2\mathbb{Z}$-extensions L of L' that are Galois over $\mathbb{Q}$ with Galois group G. The $\mathbb{Z}/2\mathbb{Z}$-extensions of a fixed number field L' can be counted using Dirichlet series, but the error bound depends on the field L'. To have a chance of controlling the total number of G-extensions, we want most of the contribution to come from few "small" fields L'.

- It seems to be an obstruction to C_{disc} having a good representation as an Euler product: The constant C_{disc} is largely influenced by the behavior of small $(\mathbb{Z}/2\mathbb{Z})^2$-extensions. In fact, we can write $C_{\mathrm{disc}} = \sum_{L'} f(L')$ for some natural values $f(L')$. Unless the values $f(L')$ exhibit some multiplicative structure, one would not expect prime factors of the discriminant to behave independently.

  On the other hand, no particular L' contributes a positive amount to the constant C_{cond}, so one could hope different primes behave independently by virtue of the Chinese Remainder Theorem. This is why we can express C_{cond} in a natural way as an Euler product.

- When counting by conductor, almost all G-extensions have exactly two automorphisms. When counting by discriminant, a positive proportion have more than two automorphisms. Instead of simply counting G-extensions, one might find it more natural to count G-extensions L weighted by $1/\#\operatorname{Aut}(L)$, or to exclude those G-extensions of $\mathbb{Q}$ that are not fields, which would change the constant C_{disc}.

[1] In fact, he counted extensions of arbitrary number fields!

Remark 4.36. Counting D_4-extensions of $\mathbb{Q}$, a similar phenomenon (different behaviors when counting by discriminant versus conductor) has been observed by Altuğ, Shankar, Varma, and Wilson in [1].

4.6.1 Overview

We first give an overview of the counting process. Our goal is to approximate the sum

$$\begin{aligned} N(X) &= \sum_{\substack{R \text{ maximal } G\text{-extension of } \mathbb{Z}, \\ |\operatorname{cond}(R)|^{1/4} \leqslant X}} \frac{1}{\operatorname{Aut}(R)} \\ &= \sum_{\substack{I \text{ unitary full ideal} \\ \text{class of } \mathbb{Z}[G]}} \sum_{\substack{m \in \operatorname{Aut}_1(I) \backslash \mathcal{P}_I^{\max}(\mathbb{Z}), \\ |\operatorname{cond}_I(m)|^{1/4} \leqslant X}} \frac{1}{\operatorname{Stab}_{\operatorname{Aut}_1(I)}(m)} \\ &= \sum_{\substack{I \text{ unitary full ideal} \\ \text{class of } \mathbb{Z}[G]}} \frac{\#\{m \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}_I(m)|^{1/4} \leqslant X\}}{\#\operatorname{Aut}_1(I)} \end{aligned}$$

for large X.

For any unitary full ideal I of $\mathbb{Z}[G]$, let

$$M_I(X) = \{m \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}_I(m)|^{1/4} \leqslant X\}.$$

In the following, we write $f = \mathcal{O}(g)$ if there exists some constant C (possibly depending on I, but not on X or any other variable) such that $|f| \leqslant C|g|$. We write $f = o(g)$ if for each $\varepsilon > 0$, there exists some N (possibly depending on I and ε, but not on any other variable) such that $|f| \leqslant \varepsilon|g|$ for all $X \geqslant N$. We write $\mathcal{O}_P(g)$ and $o_P(g)$ to signify that the constants C or N may depend on P.

The main difficulty lies in showing the following theorem.

Theorem 4.37.

$$\#M_I(X) = \frac{4\pi^2}{3} \cdot \prod_p \mu_{I \otimes \mathbb{Z}_p, p} \cdot X(\log X)^3 + o(X(\log X)^3).$$

Summing over all unitary full ideals I of $\mathbb{Z}[G]$, we conclude:

Corollary 4.38.

$$N(X) = \frac{4\pi^2}{3} \cdot \sum_I \frac{\prod_p \mu_{I \otimes \mathbb{Z}_p, p}}{\#\operatorname{Aut}_1(I)} \cdot X(\log X)^3 + o(X(\log X)^3).$$

For some purposes, the following estimate will be useful. It can easily be proved with the same methods as Theorem 4.37.

Theorem 4.39. *For any vector $u \in \mathbb{Q}^3$, let*

$$M_I^u(X) = \{m = (v_1, v_2, v_3, d) \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}_I(m)|^{1/4} \leqslant X,\ v_1 = u\}.$$

Then,

$$\#M_I^u(X) = o(X(\log X)^3).$$

Corollary 4.40. *When counting by conductor, almost all G-extensions have an automorphism group of size two:*

$$\#\{R \text{ maximal } G\text{-extension of } \mathbb{Z} \mid |\operatorname{cond}(R)|^{1/4} \leqslant X \text{ and } \#\operatorname{Aut}(R) \neq 2\} = o(X(\log X)^3).$$

Proof. For any $m \in \mathcal{P}_I^{\max}(\mathbb{Z})$, the elements $+1$ and -1 of $Z(G) \subseteq \mathrm{Aut}_1(I)$ (corresponding to $\lambda = (1,1,1,\pm 1) \in \mathrm{Aut}_1(I)$) stabilize m. On the other hand, they are usually the only two elements of $\mathrm{Aut}_1(I)$ stabilizing m: Say $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_H) \in \mathbb{Q}[G]_1^\times$ stabilizes $m = (v_1, v_2, v_3, d) \in \mathcal{P}^{\mathrm{nondeg}}(\mathbb{Q})$. This means that $N(\lambda_H) = 1$ and that v_1, v_2, v_3 is an eigenbasis of the orthogonal matrix $r(\lambda_H) \in \mathrm{SO}_3(\mathbb{Q})$ with corresponding eigenvalues $\lambda_1^{-1}, \lambda_2^{-1}, \lambda_3^{-1}$. The only possible rational eigenvalues of an orthogonal matrix are ± 1. Hence, the eigenvalues must be $1, 1, 1$ or (some permutation of) $1, -1, -1$. In the former case, $r(\lambda_H)$ is the identity matrix, so $\lambda_H = \pm 1$. In the latter case, $r(\lambda_H)$ is a rotation by angle π around one of the vectors v_1, v_2, v_3. Now, $\mathrm{Aut}_1(I)$ is a finite group, so there are only finitely many possible rotation axes. The following lemma then shows that there are only finitely many possible vectors v_1, v_2, or v_3. The result then follows from Theorem 4.39. □

Lemma 4.41. *For any unitary full ideal I and any line $l \subseteq \mathbb{Q}^3$ through the origin, there are only $\mathcal{O}(1)$ vectors $u \in l$ such that there exists some $m = (v_1, v_2, v_3, d) \in \mathcal{P}_I^{\max}(\mathbb{Z})$ with $v_1 = u$.*

Proof. Replacing I by $I\lambda$ for some $\lambda \in \mathbb{Q}_p[G]_1^\times$, we can assume that $v_1 \in \mathbb{Z}^3$ for all $m = (v_1, v_2, v_3, d) \in \mathcal{P}_I^{\mathrm{nondeg}}(\mathbb{Z})$.

There exists a number $P \geqslant 3$ such that for all primes $p > P$, we have $I \otimes \mathbb{Z}_p = \mathbb{Z}_p[G]$. As we have seen in Corollary 4.25, the vector v_1 cannot be divisible by any such prime $p > P$.

On the other hand, for any small prime $p \leqslant P$, there are of course only finitely many maximal G-extensions of $\mathbb{Z}_p$. The valuation $|v_1|_p^2$ is invariant under the action of $\overline{\mathbb{Z}_p[G]_1^\times} \supseteq \mathrm{Aut}_1(I)$ and can therefore only assume finitely many different values.

Therefore, $v_1 \in \mathbb{Z}^3$ can only be some bounded multiple of a primitive vector spanning the line l. □

Lemma 4.42. *When counting $m = (d, v_1, v_2, v_3, e_1, e_2, e_3) \in \mathcal{P}_I^{\max}(\mathbb{Z})$ by conductor, almost always $|e_1| \neq |e_2|$ (and similarly $|e_1| \neq |e_3|$ and $|e_2| \neq |e_3|$):*

$$\#\{m = (d, v_1, v_2, v_3, e_1, e_2, e_3) \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}(m)|^{1/4} = |d| \leqslant X,\ |e_1| = |e_2|\} = o(X(\log X)^3).$$

Proof. If $|e_1| = |e_2|$, then $\mathrm{disc}^{\{\pm 1, \pm k\}}(m) = e_1 e_2 = e_1^2$. The discriminant of a maximal extension of $\mathbb{Z}$ of degree 2 cannot be divisible by a square other than 4. Hence, the number $|e_1| = |e_2|$ can only attain finitely many different values. Then, $|v_3|^2 = e_1 e_2$ implies that there are only finitely many possible vectors v_3 and we can apply Theorem 4.39. □

Together with the volume computations in Lemma 4.30 and Corollary 4.32, we obtain our main counting theorem: Theorem 4.35.

To express $\mathrm{cond}_I(m)$ in terms of the more convenient invariant $\mathrm{cond}(m)$, define

$$\tau_I = \frac{[\mathbb{Z}[G] : I]^2}{[\mathbb{Z}[G]^{\{\pm 1\}} : I^{\{\pm 1\}}]^2},$$

so that

$$\mathrm{cond}_I(m) = \tau_I \cdot \mathrm{cond}(m).$$

For any prime p, letting

$$\mu'_{I,p} = \int_{\mathcal{P}_I^{\max}(\mathbb{Z}_p)} \mathrm{d}'m = \int_{\mathcal{P}_I^{\max}(\mathbb{Z}_p)} \mathrm{d}m \cdot |\operatorname{cond}(m)|_p^{1/4},$$

we therefore get

$$\mu_{I,p} = |\tau_I|_p^{1/4} \cdot \mu'_{I,p}.$$

It follows from the product formula for valuations that Theorem 4.37 is equivalent to the following

theorem concerning the set

$$\begin{aligned} M_I'(X) &= \{m \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}(m)|^{1/4} \leqslant X\} \\ &= M_I(|\tau_I|^{1/4}X). \end{aligned}$$

Theorem 4.37'.

$$\#M_I'(X) = \frac{4\pi^2}{3} \cdot \prod_p \mu'_{I\otimes\mathbb{Z}_p,p} \cdot X(\log X)^3 + o(X(\log X)^3).$$

4.6.2 Strategy

To count elements of the sets

$$M_I'(X) = \{m \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}(m)|^{1/4} \leqslant X\},$$

first note that by symmetry, it suffices to count elements of sets we denote by abuse of notation by $\frac{1}{6}M_I'(X)$:

$$\begin{aligned} \tfrac{1}{6}M_I'(X) &= \{m = (v_1, v_2, v_3, e_1, e_2, e_3, d) \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |\operatorname{cond}(m)|^{1/4} \leqslant X \text{ and } |e_1| \geqslant |e_2| \geqslant |e_3|\} \\ &= \{m = (e_3, v_1, v_2, d) \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |d| \leqslant X \text{ and } |v_2| \geqslant |v_1| \geqslant |e_3|\}. \end{aligned}$$

To count elements of $\frac{1}{6}M_I'(X)$, we construct the tuples $(e_3, v_1, v_2, d) \in \frac{1}{6}M_I'(X)$ step by step:

1) Pick e_3: Very roughly, the allowed values are those $e_3 \in \mathbb{Z}$ such that $|e_3|^3 \leqslant X$.

2) Pick v_1: Very roughly, the allowed vectors are those $v_1 \in \mathbb{Z}^3$ such that $|v_1|^2 \equiv 0 \mod e_3$ and $|e_3| \leqslant |v_1| \leqslant X^{1/4}|e_3|^{1/4}$. (You expect them to have a density of $\frac{1}{e_3}$. See Theorem 4.50 below.)

3) Pick v_2: Very roughly, the allowed vectors are those $v_2 \in \mathbb{Z}^3$ that are orthogonal to v_1 and such that $v_1 \times v_2 \equiv 0 \mod e_3$ and $|v_1| \leqslant |v_2| \leqslant X^{1/2}|e_3|^{1/2}/|v_1|$. (You pick v_2 from a lattice that usually has covolume $|v_1| \cdot |e_3|$. See Corollary 4.59 and Lemma 4.62 below.)

4) Pick d: Very roughly, the allowed values are those $d \in \mathbb{Z}$ such that $d \equiv 0 \mod \frac{|v_1|^2|v_2|^2}{e_3}$ and $|d| \leqslant X$. (You pick d from a lattice of covolume $\frac{|v_1|^2|v_2|^2}{e_3}$.)

We use a sieve to control the behavior of the element $m = (e_3, v_1, v_2, d) \in \mathcal{P}_I^{\max}(\mathbb{Z})$ at small primes $p \leqslant P$.

Our goal is now to prove the following lemma.

Lemma 4.43. *For sufficiently large $P \geqslant 2$, the number of elements of $\frac{1}{6}M_I'(X)$ is*

$$\begin{aligned} \#\tfrac{1}{6}M_I'(X) = \frac{2\pi^2}{9} \cdot \prod_{p\leqslant P} \mu'_{I\otimes\mathbb{Z}_p,p} \cdot X(\log X)^3 \\ + X(\log X)^3(o_P(1) + \mathcal{O}(P^{-1})). \end{aligned}$$

Since the infinite product $\prod_p \mu'_{I\otimes\mathbb{Z}_p,p}$ converges to a positive real number, letting P and X go to infinity, it follows that

$$\#\tfrac{1}{6}M_I'(X) = \frac{2\pi^2}{9} \cdot \prod_p \mu'_{I\otimes\mathbb{Z}_p,p} \cdot X(\log X)^3 + o(X(\log X)^3).$$

Using symmetry and Lemma 4.42, we obtain Theorem 4.37':

$$\#M_I'(X) = \frac{4\pi^2}{3} \cdot \prod_p \mu'_{I\otimes\mathbb{Z}_p,p} \cdot X(\log X)^3 + o(X(\log X)^3).$$

4.6.3 Integration by parts

To reduce summation problems to counting problems, we will frequently make use of integration by parts in the form of the following lemma.

Lemma 4.44. *Let $n : \mathbb{R}_{\geqslant 1} \to \mathbb{R}$ be a function such that for all $L > 0$, there are only finitely many $x \leqslant L$ with $n(x) \neq 0$. Furthermore, let $a_r \geqslant 0$ for $r \geqslant 0$ with $a_r = 0$ for all but finitely many r. Let $k \geqslant 1$. Assume that for all $L \geqslant 1$,*

$$N(L) = \sum_{x\leqslant L} n(x) = a_0 L^k + \sum_{r>0} \mathcal{O}(a_r L^{k-r}).$$

Then, for all $1 \leqslant L_1 \leqslant L_2$, we have

$$\sum_{L_1\leqslant x\leqslant L_2} n(x) \cdot \frac{(\log x)^h}{x^k} = \frac{k}{h+1} \cdot a_0 \cdot ((\log L_2)^{h+1} - (\log L_1)^{h+1}) + \sum_{r\geqslant 0} \mathcal{O}_{k,r,h}\left(a_r \cdot \frac{(\log L_2)^h + 1}{L_1^r}\right).$$

for any integer $h \geqslant 0$. The same statement holds when replacing a_0 by $\mathcal{O}(a_0)$ everywhere.

Proof. Using integration by parts, we see that

$$\begin{aligned}\sum_{L_1\leqslant x\leqslant L_2} n(x) \cdot \frac{(\log x)^h}{x^k} &= (a_0 L_2^k + \sum_{r>0} \mathcal{O}(a_r L_2^{k-r})) \cdot \frac{(\log L_2)^h}{L_2^k} - (a_0 L_1^k + \sum_{r>0} \mathcal{O}(a_r L_1^{k-r})) \cdot \frac{(\log L_1)^h}{L_1^k} \\ &\quad + \int_{L_1}^{L_2} \mathrm{d}t (a_0 t^k + \sum_{r>0} \mathcal{O}(a_r t^{k-r})) \cdot \frac{k(\log t)^h - h(\log t)^{h-1}}{t^{k+1}}.\end{aligned}$$

The first two summands are

$$\sum_{r\geqslant 0} \mathcal{O}\left(a_r \frac{(\log L_2)^h}{L_1^r}\right).$$

The main term in the integral summand is

$$\int_{L_1}^{L_2} \mathrm{d}t a_0 \cdot \frac{k(\log t)^h - h(\log t)^{h-1}}{t} = \frac{k}{h+1} \cdot a_0 \cdot ((\log L_2)^{h+1} - (\log L_1)^{h+1}) + \mathcal{O}_h(a_0(\log L_2)^h).$$

The error term in the integral summand is

$$\sum_{r>0} \mathcal{O}\left(\int_{L_1}^{L_2} \mathrm{d}t a_r \cdot \frac{k(\log t)^h + h(\log t)^{h-1}}{t^{r+1}}\right) = \sum_{r>0} \mathcal{O}_{k,r,h}\left(a_r \cdot \frac{(\log L_2)^h + 1}{L_1^r}\right).$$

□

4.6.4 A few well-known estimates

We will also repeatedly use the following well-known facts:

Lemma 4.45 (Mertens' Theorem)**.** *For all $Y \geqslant 1$, we have*

$$\sum_{p\leqslant Y \text{ prime}} p^{-1} = \log\log\max(Y, 10) + \mathcal{O}(1).$$

Lemma 4.46. *For all integers $n \geqslant 1$, we have*

$$\prod_{p|n \text{ prime}} (1 + p^{-1}) = \mathcal{O}(\log\log\max(n, 10)).$$

Proof. We can assume without loss of generality that $n \geqslant 100$ and that $n = p_1 \cdots p_k$ is squarefree. Denote the sequence of prime numbers by $q_1 \leqslant q_2 \leqslant \cdots$. We of course have $q_1 \cdots q_k \leqslant n$. The prime number theorem implies that $q_k = \mathcal{O}(\log n)$. Then, Mertens' Theorem implies that

$$\begin{aligned}\log \prod_{i=1}^{k}(1 + p_i^{-1}) &\leqslant \log \prod_{i=1}^{k}(1 + q_i^{-1}) = -\sum_{i=1}^{k}\sum_{j=1}^{\infty}\frac{(-1)^j q_i^{-j}}{j} = \sum_{i=1}^{k} q_i^{-1} + \mathcal{O}(1) = \log\log q_k + \mathcal{O}(1)\\ &\leqslant \log\log\log n + \mathcal{O}(1).\end{aligned}$$

□

4.6.5 Counting lattice points

We will need to count points of bounded length in certain shifted lattices of ranks two and three. Consider a lattice $\Lambda \subseteq \mathbb{R}^n$ of rank r and covolume V. For large L, we expect the number of vectors $v \in \Lambda$ of length $|v| \leqslant L$ to be roughly $\mathrm{vol}(B_r(L))/V$, where $B_r(L)$ is an r-dimensional ball of radius L. The main obstacle when trying to get good error bounds is that the lattice might be very degenerate. For example, it might contain a nonzero vector of length far smaller than $V^{1/r}$. To circumvent this problem in rank two, we will exclude all vectors on the line through the shortest nonzero vector of Λ. In rank three, our specific lattices happen to be sufficiently nondegenerate.

Lemma 4.47. *Let $\Lambda \subset \mathbb{Z}^3$ be a rank two lattice of covolume V. Let $b_1 \in \Lambda$ be a nonzero vector of minimal length. Furthermore, let $t \in \Lambda$ and let $M \geqslant 1$ be an integer and $L \geqslant 1$ a real number. Then, the number $N(L)$ of vectors $v \in (M\Lambda + t)\backslash b_1\mathbb{Z}$ of length $|v| \leqslant L$ satisfies*

$$N(L) = \pi \cdot \frac{L^2}{M^2 V} + \mathcal{O}(L)$$

and

$$N(L) = \mathcal{O}\left(\frac{L^2}{V}\right).$$

In particular, if $L \ll V^{1/2}$, then $N(L) = 0$.

Proof. It is well-known that the number of nonzero vectors $v \in M\Lambda + t$ of length $|v| \leqslant L$ is $\pi \cdot \frac{L^2}{M^2 V} + \mathcal{O}(L)$. The number of nonzero vectors $v \in b_1\mathbb{Z}$ of length $|v| \leqslant L$ is clearly $\mathcal{O}(L)$.

By considering a reduced basis of Λ, one can easily show the second estimate: The number of vectors $v \in \Lambda \subseteq M\Lambda + t$ that don't lie on the line $b_1\mathbb{Z}$ is $\mathcal{O}(L^2/V)$. □

Corollary 4.48. *Let Λ, V, t, M, b_1 be as in the previous lemma. Then, for all $1 \leqslant L_1 \leqslant L_2$,*

$$\sum_{\substack{v \in (M\Lambda + t)\backslash b_1\mathbb{Z}\\ L_1 \leqslant |v| \leqslant L_2}} \frac{1}{|v|^2} = \begin{cases} \pi \cdot \frac{\log(L_2^2/L_1^2)}{M^2 V} + \mathcal{O}(\frac{1}{V}), & L_1 \gg V^{1/2},\\ 0, & L_2 \ll V^{1/2}.\end{cases}$$

Proof. Apply integration by parts (Lemma 4.44) to the first estimate for $N(L)$ when $L > V$ and the second estimate when $L \leqslant V$. □

When counting vectors in a shifted lattice of rank three, we will use a lower bound on the length of the lattice's shortest vector. The following lemma is also well-known.

Lemma 4.49. *Let Λ be a lattice of rank three and covolume V. Assume every nonzero vector in Λ has length at least B. Let $t \in \Lambda$ and let $M \geqslant 1$ be an integer and $L \geqslant 1$ a real number. Then, the number of nonzero vectors v in the shifted lattice $M\Lambda + t$ of length $|v| \leqslant L$ is*

$$\frac{4\pi}{3} \cdot \frac{L^3}{M^3 V} + \mathcal{O}(\frac{L^2}{B^2}).$$

4.6.6 Counting vectors v_1

The number of nonzero vectors $v \in \mathbb{Z}^3$ of length $|v| \leqslant L$ is $\frac{4\pi}{3} \cdot L^3 + \mathcal{O}(L^2)$. For any prime number p, exactly p^2 of the p^3 vectors $\overline{v}$ in $\mathbb{F}_p^3$ satisfy $|\overline{v}|^2 \equiv 0 \mod p$. For a nonzero squarefree integer e, we therefore expect roughly $\frac{4\pi}{3} \cdot \frac{L^3}{|e|}$ of the vectors $v \in \mathbb{Z}^3$ of length $|v| \leqslant L$ to satisfy $|v|^2 \equiv 0 \mod e$. The following theorem gives a concrete error bound and also allows for congruence conditions at small primes.

Theorem 4.50. *Let $P \geqslant 2$. For any $p \leqslant P$, let $\Lambda_p \subseteq \mathbb{Z}_p^3$ be a shifted $\mathbb{Z}_p$-lattice of rank three and covolume V_p. Let $e \in \mathbb{Z}$ be a cubefree nonzero integer. For any $p > P$, let*

$$S_p(e) = \{v \in \mathbb{Z}_p^3 \mid |v|^2 \equiv 0 \mod e\}.$$

Define

$$S(e) = \bigcap_{p \leqslant P} \Lambda_p \cap \bigcap_{p > P} S_p(e) \subseteq \mathbb{Z}^3.$$

Then, for any $L \geqslant 1$, the number of nonzero vectors $v \in S(e)$ of length $|v| \leqslant L$ is

$$\frac{4\pi}{3} \cdot \prod_{p \leqslant P} \frac{V_p}{|e|_p} \cdot \frac{L^3}{|e|} \cdot \prod_{\substack{p > P, \\ p^2 | e}} (1 + p^{-1} - p^{-2}) + \mathcal{O}\Bigg(L^2 \cdot \prod_{\substack{p > P, \\ p | e, \\ p^2 \nmid e}} (1 + 2p^{-1}) \cdot \prod_{\substack{p > P, \\ p^2 | e}} (2p^{-1} + 3p^{-2}) \Bigg).$$

Remark 4.51. One could easily replace the error bound by $\mathcal{O}(L^2 + |e|^2)$, which is weaker for small L, but slightly better than the one given in the lemma for large L. We won't need this alternative error bound. Also note that all nonzero vectors $v \in S(e)$ have length at least $\prod_{p>P} |e|_p^{-1/2}$ because $|v|^2 \equiv 0 \mod \prod_{p>P} |e|_p^{-1}$.

Remark 4.52. According to Lemma 4.46, we have

$$\prod_{p|e} (1 + 2p^{-1}) \leqslant \prod_{p|e} (1 + p^{-1})^2 = \mathcal{O}((\log\log\max(|e|, 10))^2).$$

Therefore, if e is divisible by p^2 for only a bounded number of primes $p > P$, then the error bound in Theorem 4.50 is at most

$$\mathcal{O}(L^2 \cdot (\log\log\max(|e|, 10))^2).$$

Remark 4.53. For the number of vectors $v \in \mathbb{Z}^3$ of length $|v| \leqslant L$, the trivial estimate is $\frac{4\pi}{3} \cdot L^3 + \mathcal{O}(L^2)$. However, the error bound has been improved to $\mathcal{O}(L^{21/16+\varepsilon})$ by Heath-Brown. See [16, Section 2] for a survey of this problem.

The idea of the proof of Theorem 4.50 is to write the characteristic function of the set $S(e) \subseteq \mathbb{Z}^3$ as a linear combination of characteristic functions of lattices. We then separately count vectors in each of the lattices, using divisibility relations of the form $|v|^2 \equiv 0 \mod l$ to show that all vectors v in a lattice have length at least $l^{1/2}$. First, let us decompose characteristic functions locally: We write $S_p(e)$ as a linear combination of $p+1$ lattices if e is divisible by p exactly once, and as a linear combination of $2p+3$ lattices if e is divisible by p exactly twice:

Lemma 4.54. *Let $p \neq 2$ be an odd prime and assume $e \in \mathbb{Z}_p$ is divisible by p exactly $k_p \in \{1,2\}$ times. Define $S_p(e)$ as in Theorem 4.50. Then, we can write the characteristic function of $S_p(e) \subseteq \mathbb{Z}_p^3$ as*

$$\mathbb{1}_{S_p(e)} = \sum_{s \in \Sigma_p} \mathrm{coeff}_p(s) \cdot \mathbb{1}_{\Lambda_{p,s}}.$$

Here, we used the sets of "symbols"

$$\Sigma_p = \begin{cases} \{1, \ldots, p+1, \cap\}, & k_p = 1, \\ \{1, \ldots, p+1, 1 \cap \theta, \ldots, p+1 \cap \theta, \theta\}, & k_p = 2. \end{cases}$$

The corresponding coefficients are

$$\mathrm{coeff}_p(s) = \begin{cases} +1, & s \in \{1, \ldots, p+1, \theta\}, \\ -p, & s = \cap, \\ -1, & s = i \cap \theta \text{ with } i \in \{1, \ldots, p+1\}. \end{cases}$$

The lattices $\Lambda_{p,s} \subseteq \mathbb{Z}_p^3$ have covolume $V_{p,s}$ (index $V_{p,s}^{-1}$), where

$$V_{p,s} = \begin{cases} p^{-k_p-1}, & s \in \{1, \ldots, p+1, \theta\}, \\ p^{-3}, & s = \cap, \\ p^{-4}, & s = i \cap \theta \text{ with } i \in \{1, \ldots, p+1\}. \end{cases}$$

Furthermore, for each vector $v \in \Lambda_{p,s}$, we have $|v|_p \leqslant \mathrm{len}_p(s)$ (so $|v|^2 \equiv 0 \mod \mathrm{len}_p(s)^{-2}$), where

$$\mathrm{len}_p(s) = \begin{cases} p^{-k_p/2}, & s \neq \cap, \\ p^{-1}, & s = \cap. \end{cases}$$

Proof. The conic $V_p = \{w \in \mathbb{P}^2_{\mathbb{F}_p} : |w|^2 = 0\} \subseteq \mathbb{P}^2_{\mathbb{F}_p}$ is isomorphic to $\mathbb{P}^1_{\mathbb{F}_p}$ and therefore has exactly $p+1$ points $[w_1], \ldots, [w_{p+1}] \in \mathbb{P}^2_{\mathbb{F}_p}$ over $\mathbb{F}_p$. Using Hensel's lemma, we can lift representatives $w_i \in \mathbb{F}_p^3$ to points $w_i \in (\mathbb{Z}/p^{k_p}\mathbb{Z})^3$ such that $|w_i|^2 \equiv 0 \mod p^{k_p}$.

If $k_p = 1$, then the vectors $\tilde{v} \in (\mathbb{Z}/p\mathbb{Z})^3$ satisfying $0 \equiv |\tilde{v}|^2 \mod p$ therefore form the union of $p+1$ subgroups (lines) $\Lambda_{p,1}, \cdots, \Lambda_{p,p+1}$ of $(\mathbb{Z}/p\mathbb{Z})^3$ of order p (and index p^2). The intersection of any two of the subgroups is the trivial subgroup $\Lambda_{p,\cap} = (p\mathbb{Z}/p\mathbb{Z})^3 = 0$ of order 1 (and index p^3). Lift these subgroups of $(\mathbb{Z}/p\mathbb{Z})^3$ to $\mathbb{Z}^3$. Then,

$$\mathbb{1}_{S_p(e)} = \sum_{i=1}^{p+1} \mathbb{1}_{\Lambda_{p,i}} - p \cdot \mathbb{1}_{\Lambda_{p,\cap}}.$$

Any vector v in $\Lambda_{p,i}$ has $|v|^2 \equiv 0 \mod p$. Any vector v in $\Lambda_{p,\cap} = p\mathbb{Z}^3$ has $|v|^2 \equiv 0 \mod p^2$.

If $k_p = 2$, then the vectors $\tilde{v} \in (\mathbb{Z}/p^2\mathbb{Z})^3$ satisfying $0 \equiv |\tilde{v}|^2 \mod p^2$ form the union of $p+2$ subgroups $\Lambda_{p,1}, \cdots, \Lambda_{p,p+1}, \Lambda_{p,\theta}$ of $(\mathbb{Z}/p^2\mathbb{Z})^3$: Here, the subgroups $\Lambda_{p,i} = w_i \cdot (\mathbb{Z}/p^2\mathbb{Z}) + p \cdot \langle w_i \rangle^\perp$ for $i = 1, \ldots, p+1$ are of order p^3 (and index p^3), and the subgroup $\Lambda_{p,\theta} = (p\mathbb{Z}/p^2\mathbb{Z})^3$ also has order p^3 (and index p^3). The intersection $\Lambda_{p,i} \cap \Lambda_{p,j}$ of any two of the lattices ($i \neq j$) is contained in $\Lambda_{p,\theta}$. The intersections $\Lambda_{p,i\cap\theta} = \Lambda_{p,i} \cap \Lambda_{p,\theta} = p \cdot \langle w_i \rangle^\perp$ have order p^2 (and index p^4). Again, lift these subgroups of $(\mathbb{Z}/p^2\mathbb{Z})^3$ to $\mathbb{Z}^3$ so that

$$\mathbb{1}_{S_p(e)} = \sum_{i=1}^{p+1} (\mathbb{1}_{\Lambda_{p,i}} - \mathbb{1}_{\Lambda_{p,i\cap\theta}}) + \mathbb{1}_{\Lambda_{p,\theta}}.$$

Any vector v in $\Lambda_{p,i}$ or $\Lambda_{p,i\cap\theta}$ or $\Lambda_{p,\theta}$ has $|v|^2 \equiv 0 \mod p^2$. □

Proof of Theorem 4.50. We can assume without loss of generality that e is not divisible by any prime $p \leqslant P$. (Dividing e by such a prime changes neither the set $S(e)$ nor our expression for the number of vectors.)

For any $p > P$, let e be divisible by p exactly $k_p \in \{0, 1, 2\}$ times. For any prime p dividing e, write the characteristic function of $S_p(e) \subseteq \mathbb{Z}_p^3$ as a linear combination as above. Hence, the characteristic function of the set $S \subseteq \mathbb{Z}^3$ is

$$\mathbb{1}_S = \prod_{p \leqslant P} \mathbb{1}_{\Lambda_p} \cdot \prod_{p|e} \mathbb{1}_{S_p(e)} = \prod_{p \leqslant P} \mathbb{1}_{\Lambda_p} \cdot \prod_{p|e} \sum_{s \in \Sigma_p} \operatorname{coeff}_p(s) \cdot \mathbb{1}_{\Lambda_{p,s}}.$$

Expanding the product, we obtain

$$\mathbb{1}_S = \sum_f \prod_{p \leqslant P} \mathbb{1}_{\Lambda_p} \cdot \prod_{p|e} \operatorname{coeff}_p(f(p)) \cdot \mathbb{1}_{\Lambda_{p,f(p)}} = \sum_f \operatorname{coeff}(f) \cdot \mathbb{1}_{\Lambda(f)},$$

where we sum over all tuples $(f(p))_{p|e}$ such that $f(p) \in \Sigma_p$, and where we used the notation

$$\operatorname{coeff}(f) = \prod_{p|e} \operatorname{coeff}_p(f(p))$$

and

$$\Lambda_f = \bigcap_{p \leqslant P} \Lambda_p \cap \bigcap_{p|e} \Lambda_{p,f(p)} \subseteq \mathbb{Z}^3.$$

For each summand, we will use Lemma 4.49 to find the sum over all $v \in \mathbb{Z}^3$ with $|v| \leqslant L$. The shifted lattice $\Lambda_f \subseteq \mathbb{Z}^3$ has rank three. By the product formula for valuations, its covolume is

$$V(f) = \prod_{p \leqslant P} V_p^{-1} \cdot \prod_{p|e} V_{p,f(p)}^{-1}.$$

Therefore, the main term in $\sum_{v \in \mathbb{Z}^3,\ |v| \leqslant L} \mathbb{1}_S(v)$ coming from Lemma 4.49 is

$$\begin{aligned} \text{main term} &= \sum_f \operatorname{coeff}(f) \cdot \frac{4\pi}{3} \cdot \frac{L^3}{V(f)} \\ &= \frac{4\pi}{3} \cdot \prod_{p \leqslant P} V_p \cdot L^3 \cdot \sum_f \prod_{p|e} \operatorname{coeff}_p(f(p)) V_{p,f(p)}. \end{aligned}$$

The main term can thus be factored as

$$\begin{aligned} \text{main term} &= \frac{4\pi}{3} \cdot \prod_{p \leqslant P} V_p \cdot L^3 \cdot \prod_{p|e} \sum_{s \in \Sigma_p} \operatorname{coeff}_p(s) V_{p,s} \\ &= \frac{4\pi}{3} \cdot \prod_{p \leqslant P} V_p \cdot L^3 \cdot \prod_{p:\ k_p = 1} \left(\frac{p+1}{p^2} - \frac{p}{p^3} \right) \cdot \prod_{p:\ k_p = 2} \left(\frac{p+1}{p^3} - \frac{p+1}{p^4} + \frac{1}{p^3} \right) \\ &= \frac{4\pi}{3} \cdot \prod_{p \leqslant P} V_p \cdot \frac{L^3}{|e|} \cdot \prod_{p:\ k_p = 2} (1 + p^{-1} - p^{-2}). \end{aligned}$$

For the error term, note that (by the product formula for valuations) all nonzero vectors in the lattice $\bigcap_{p|e} \Lambda_{p,f(p)}$ have length at least

$$\operatorname{len}(f) = \prod_{p|e} \operatorname{len}_p(f(p))^{-1}.$$

The error term in $\sum_{v\in\mathbb{Z}^3,\ |v|\leqslant L} \mathbb{1}_S(v)$ coming from Lemma 4.49 is therefore

$$\begin{aligned}
\text{error term} &= \mathcal{O}\bigg(\sum_f |\operatorname{coeff}(f)| \cdot \frac{L^2}{\operatorname{len}(f)^2}\bigg) \\
&= \mathcal{O}\bigg(L^2 \cdot \sum_f \prod_{p|e} |\operatorname{coeff}_p(f(p))| \operatorname{len}_p(f(p))^2\bigg) \\
&= \mathcal{O}\bigg(L^2 \cdot \sum_f \prod_{p|e} p^{-k_p}\bigg) \\
&= \mathcal{O}\bigg(L^2 \cdot \prod_{p:\ k_p=1} \frac{p+2}{p} \cdot \prod_{p:\ k_p=2} \frac{2p+3}{p^2}\bigg) \\
&= \mathcal{O}\bigg(L^2 \cdot \prod_{p:\ k_p=1} (1+2p^{-1}) \cdot \prod_{p:\ k_p=2} (2p^{-1}+3p^{-2})\bigg).
\end{aligned}$$

□

4.6.7 Counting vectors v_2

Over a field, the cross product of two vectors is zero if and only if the vectors are colinear. A similar statement holds modulo any integer e:

Lemma 4.55. *Let $v \in \mathbb{Z}^3$ be a primitive vector, let $w \in \mathbb{Z}^3$ be any vector, and let e be a nonzero integer. Then, we have $v \times w \equiv 0 \mod e$ if and only if $w \equiv \lambda v \mod e$ for some $\lambda \in \mathbb{Z}/e\mathbb{Z}$.*

Proof. By the Chinese Remainder Theorem, we may assume that $e = p^k$ is a prime power. Let $v = (x, y, z)$ and $w = (x', y', z')$. Since v is primitive, we can assume without loss of generality that $p \nmid z$. Then, $0 \equiv v \times w \equiv (yz' - zy', zx' - xz', xy' - yx') \mod p^k$ implies that $x' \equiv z'z^{-1}x \mod p^k$ and $y' \equiv z'z^{-1}y \mod p^k$, so indeed $w \equiv z'z^{-1}v \mod p^k$. □

Corollary 4.56. *Let $v, w \in \mathbb{Z}^3$ be primitive orthogonal vectors and let e be a nonzero integer such that $v \times w \equiv 0 \mod e$. Then, both $|v|^2$ and $|w|^2$ are divisible by e.*

Proof. We must have $w \equiv \lambda v \mod e$ for some integer λ. Since w is a primitive vector, λ and e must be relatively prime. On the other hand, $0 \equiv v \cdot w \equiv \lambda |v|^2 \mod e$, which implies that $|v|^2$ (and similarly $|w|^2$) must be divisible by e. □

Lemma 4.57. *Let $v \in (\mathbb{Z}/e\mathbb{Z})^3$ be a primitive vector and let e be a nonzero integer dividing $|v|^2$. Let $\langle v\rangle^\perp \subseteq (\mathbb{Z}/e\mathbb{Z})^3$ be set of vectors perpendicular to v. Consider the linear map $f : \langle v\rangle^\perp \to \langle v\rangle^\perp$ sending w to $v \times w$. Its kernel and image are both the span $\langle v\rangle \subseteq \langle v\rangle^\perp$ of v.*

Proof. The statement on the kernel follows directly from Lemma 4.55. Furthermore, $v \times (v \times w) \equiv -|v|^2 \cdot w \equiv 0 \mod e$, so the image is contained in the kernel. Since v is primitive, the kernel $\langle v\rangle$ has size e and the domain $\langle v\rangle^\perp$ has size e^2. Hence, the image also has to have size e and therefore has to coincide with the kernel. □

See [27, Corollary in Section 2] for a more general form of the following lemma.

Lemma 4.58. *Let $v \in \mathbb{Z}^3$ be a primitive vector. Then, the vectors $w \in \mathbb{Z}^3$ which are orthogonal to v form a lattice Λ of rank two and covolume $|v|$.*

Proof. The lattice $\Lambda + \mathbb{Z} \cdot v$ is the kernel of the linear map $\mathbb{Z}^3 \to \mathbb{Z}/|v|^2\mathbb{Z}$ sending w to $v \cdot w$. Since v is primitive, the map is surjective. Hence, $\Lambda + \mathbb{Z} \cdot v$ has index $|v|^2$ in $\mathbb{Z}^3$. Since Λ and $\mathbb{Z} \cdot v$ are orthogonal, the covolume $|v|^2$ of $\Lambda + \mathbb{Z} \cdot v$ is the product of the covolume of Λ and the covolume $|v|$ of $\mathbb{Z} \cdot v$. □

Corollary 4.59. *Let $v \in \mathbb{Z}^3$ be a primitive vector and let e be a nonzero integer dividing $|v|^2$. Then, the vectors $w \in \mathbb{Z}^3$ which are orthogonal to v and such that $v \times w$ is divisible by e form a lattice Λ of rank two and covolume $|v| \cdot |e|$.*

Proof. Since v is primitive, the lattice $\langle v \rangle^\perp \subseteq \mathbb{Z}^3$ of vectors perpendicular to $v \in \mathbb{Z}^3$ surjects onto the lattice $\langle \overline{v} \rangle^\perp \subseteq (\mathbb{Z}/e\mathbb{Z})^3$ of vectors perpendicular to the reduction $\overline{v} \in (\mathbb{Z}/e\mathbb{Z})^3$ of v modulo e. The set of vectors $\overline{w} \in \langle \overline{v} \rangle^\perp$ such that $v \times \overline{w} \equiv 0 \mod e$ has index e in $\langle \overline{v} \rangle^\perp$ according to Lemma 4.57. □

Lemma 4.60. *Let $p \neq 2$ be an odd prime and let $\Lambda \subsetneq \mathbb{Z}_p^3$ be a primitive $\mathbb{Z}_p$-lattice of rank two. Then, the set*

$$\{v \in \Lambda \mid |v|^2 \equiv 0 \mod p\}$$

is the union of $\mathcal{O}(1)$ sublattices Γ of Λ of index at least p.

Proof. Since Λ is a primitive lattice of rank two, its image V in $\mathbb{F}_p^3$ is a two-dimensional vector space. Consider the variety X of points $v \in \mathbb{P}^2_{\mathbb{F}_p}$ such that $|v|^2 = 0$. Since the variety X is smooth and of degree two, it cannot contain the line V in $\mathbb{P}^2_{\mathbb{F}_p}$. Therefore, the intersection $X \cap V$ consists of at most two points. Each point corresponds to a line in $V \subseteq \mathbb{F}_p^3$, which corresponds to a sublattice of Λ of index p. If $X \cap V$ is empty, then only the vectors in the sublattice $\Lambda \cap p\mathbb{Z}_p^3$ of index p^2 satisfy $|v|^2 \equiv 0 \mod p$. □

Lemma 4.61. *Let $p \neq 2$ be an odd prime and let $\Lambda \subsetneq \mathbb{Z}_p^3$ be a primitive $\mathbb{Z}_p$-lattice of rank two. Then, the set*

$$\{v \in \Lambda \mid |v|^2 \equiv 0 \mod p^2\}$$

is the union of $\mathcal{O}(1)$ sublattices Γ of Λ of covolume at most p^{-2}.

Proof. We can use Hensel's Lemma to lift the $\mathcal{O}(1)$ sublattices with $|v|^2 \equiv 0 \mod p$ to $\mathcal{O}(1)$ sublattices with $|v|^2 \equiv 0 \mod p^2$. It only remains to show that every $\mathbb{Z}_p$-lattice $\Gamma \subsetneq \mathbb{Z}_p^3$ of rank two such that $|v|^2 \equiv 0 \mod p^2$ for all $v \in \Gamma$ has covolume at most p^{-2}. Let (v, w) be a basis of Γ. Then, $|xv + yw|^2 \equiv 0 \mod p^2$ for all $x, y \in \mathbb{Z}_p$ implies that $|v|^2 \equiv |w|^2 \equiv v \cdot w \equiv 0 \mod p^2$. Hence, the covolume

$$\left| \det \begin{pmatrix} |v|^2 & v \cdot w \\ v \cdot w & |w|^2 \end{pmatrix} \right|_p^{1/2}$$

of Γ is indeed at most p^{-2}. □

Lemma 4.62. *Let $p \neq 2$ be an odd prime and $v \in \mathbb{Z}_p^3$ a nonzero vector such that $|v|^2$ is squarefree. Write $|v|^2 = ee'$ for some $e, e' \in \mathbb{Z}_p$.*

Then, the set

$$S_p(e, v) = \{w \in \mathbb{Z}_p^3 \mid v \cdot w = 0 \text{ and } v \times w \equiv 0 \mod e\} \subseteq \langle v \rangle^\perp \cap \mathbb{Z}_p^3 \subsetneq \mathbb{Z}_p^3.$$

is a lattice of rank two and covolume $|v|_p |e|_p$.

The subset

$$S'_p(e, v) = \{w \in S_p(e, v) \mid |w|^2 \equiv 0 \mod ep\} \subseteq \langle v \rangle^\perp \cap \mathbb{Z}_p^3 \subsetneq \mathbb{Z}_p^3.$$

is the union of $\mathcal{O}(1)$ lattices of rank two and covolume at most $|v|_p |e|_p p^{-1}$.

If $p \nmid |v|^2$ (and therefore $p \nmid e$), the subset

$$S''_p(e, v) = \{w \in S_p(e, v) \mid |w|^2 \equiv 0 \mod p^2\} \subseteq \langle v \rangle^\perp \cap \mathbb{Z}_p^3 \subsetneq \mathbb{Z}_p^3.$$

is the union of $\mathcal{O}(1)$ lattices of rank two and covolume at most $|v|_p |e|_p p^{-2} = p^{-2}$.

Proof. The first statement follows from the proof of Corollary 4.59.

If $p \nmid e$, then $S_p(e,v) = S_p(1,v) = \langle v \rangle^\perp \cap \mathbb{Z}_p^3 \subsetneq \mathbb{Z}_p^3$ is a primitive lattice of covolume $|v|_p$, so the remaining statements follow from Lemmas 4.60 and 4.61.

It only remains to show the second statement if $p \mid e$. The lattice $S_p(e,v)$ contains a vector $v' \equiv v \mod e$. Since $v \cdot v' = 0$ and ee' is squarefree, we get

$$|v'|^2 \equiv |v - v'|^2 - |v|^2 \equiv -|v|^2 \equiv -ee' \not\equiv 0 \mod p^2.$$

Therefore, $S_p(e,v)$ isn't contained in any of the $\mathcal{O}(1)$ sublattices Γ of $S_p(1,v)$ of vectors w with $|w|^2 \equiv 0 \mod p^2$. The $\mathcal{O}(1)$ intersections $S_p(e,v) \cap \Gamma \subsetneq S_p(e,v)$ must then all have index at least p in $S_p(e,v)$. □

4.6.8 Conclusion of the proof

As before, let I be a unitary full ideal of $\mathbb{Z}[G]$.

By replacing I by $I\lambda$ for some appropriate $\lambda \in \mathbb{Q}[G]_1^\times$, we can assume without loss of generality that for all primes p and all $(e_3, v_1, v_2, d) \in \mathcal{P}^{\max}_{I \otimes \mathbb{Z}_p}(\mathbb{Z}_p)$, we have $e_3, d \in \mathbb{Z}_p$ and $v_1, v_2 \in \mathbb{Z}_p^3$ and $\frac{|v_1|^2|v_2|^2}{e_3} \mid d$ and $e_3 \mid v_1 \times v_2$.

Let $P \geqslant 2$ so that $I \otimes \mathbb{Z}_p = \mathbb{Z}_p[G]$ for all primes $p > P$.

The preparations in the previous sections now reduce the proof of Lemma 4.43 (and therefore Theorem 4.35) to a straightforward but lengthy computation, which we will sketch in this section. Recall the definition of $\frac{1}{6}M_I'(X)$:

$$\tfrac{1}{6}M_I'(X) = \{m = (e_3, v_1, v_2, d) \in \mathcal{P}_I^{\max}(\mathbb{Z}) \mid |d| \leqslant X \text{ and } |v_2| \geqslant |v_1| \geqslant |e_3|\}.$$

For primes $p \leqslant P$, we use the local "volumes" $\mu'_{I,p}$ to count points in $\mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)$. For primes $p > P$, we use the criterion given in Corollary 4.26 to describe points in $\mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)$.

Lemma 4.63. *Let $e_3 \in \mathbb{Z}$ be nonzero and let $v_1, v_2 \in \mathbb{Z}^3$ be nonzero orthogonal vectors such that $e_3 \mid |v_1|^2$ and $e_3 \mid v_1 \times v_2$ and the following local conditions hold:*

- *For all $p > P$, we have $p^2 \nmid |v_1|^2$ and $p^2 \nmid \frac{|v_1|^2|v_2|^2}{e_3}$.*
- *We have $|e_3| \leqslant |v_1| \leqslant |v_2|$ and $\frac{|v_1|^2|v_2|^2}{|e_3|} \leqslant X$.*

Then, the number of d such that $(e_3, v_1, v_2, d) \in \frac{1}{6}M_I'(X)$ is

$$\begin{aligned}\sum_d 1 = &\prod_{p \leqslant P} \mu'_{I,p}(e_3, v_1, v_2) \cdot 2 \cdot \frac{X|e_3|}{|v_1|^2|v_2|^2} + \mathcal{O}_P(1) \\ &+ \frac{X|e_3|}{|v_1|^2|v_2|^2} \cdot \left(\mathcal{O}(P^{-1}) + \mathcal{O}\Big(\sum_{\substack{p>P,\\ p \mid \frac{|v_1|^2|v_2|^2}{e_3}}} p^{-1}\Big)\right)\end{aligned}$$

where

$$\mu'_{I,p}(e_3, v_1, v_2) = \int_{d:(e_3,v_1,v_2,d)\in\mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)} \frac{\mathrm{d}d}{|v_1|_p^2|v_2|_p^2/|e_3|_p}.$$

If one of the local conditions doesn't hold, there is no such number d.

Proof. For each $p \leqslant P$, we can write the set of possible $d \in \mathbb{Z}_p$ (such that $(e_3, v_1, v_2, d) \in \mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)$) as the disjoint union of $\mathcal{O}_P(1)$ shifted lattices of rank one in $\mathbb{Z}_p$.

For $p > P$, the set of possible $d \in \mathbb{Z}_p$ (such that $\frac{|v_1|^2|v_2|^2}{e_3} \mid d$ and $p^2 \nmid d$) is

$$\left(\frac{|v_1|^2|v_2|^2}{e_3} \cdot \mathbb{Z}_p\right) \backslash p^2\mathbb{Z}_p \subseteq \mathbb{Z}_p.$$

The set of possible $d \in \mathbb{R}$ (such that $|\operatorname{cond}|^{1/4} = |d| \leqslant X$) is

$$[-X, X] \subseteq \mathbb{R}.$$

Hence,

$$\begin{aligned}\sum_d 1 &= 2X \cdot \prod_{p \leqslant P} \frac{|v_1|_p^2|v_2|_p^2}{|e_3|_p} \mu'_{I,p}(e_3, v_1, v_2) \cdot \prod_{p > P} \frac{|v_1|_p^2|v_2|_p^2}{|e_3|_p} + \mathcal{O}_P(1) \\ &\quad + \mathcal{O}\left(X \cdot \frac{|e_3|}{|v_1|^2|v_2|^2} \sum_{p>P} \frac{\gcd(|v_1|^2|v_2|^2/e_3, p)}{p^2}\right) \\ &= \prod_{p \leqslant P} \mu'_{I,p}(e_3, v_1, v_2) \cdot 2 \cdot \frac{X|e_3|}{|v_1|^2|v_2|^2} + \mathcal{O}_P(1) \\ &\quad + \frac{X|e_3|}{|v_1|^2|v_2|^2} \cdot \left(\mathcal{O}(P^{-1}) + \mathcal{O}\Big(\sum_{\substack{p>P, \\ p \mid \frac{|v_1|^2|v_2|^2}{e_3}}} p^{-1}\Big)\right).\end{aligned}$$

□

Lemma 4.64. *Let $e_3 \in \mathbb{Z}$ be nonzero and let $v_1 \in \mathbb{Z}^3$ be a nonzero vector such that $e_3 \mid |v_1|^2$ and the following local conditions hold:*

- *For all $p > P$, we have $p^2 \nmid |v_1|^2$.*
- *We have $|e_3| \leqslant |v_1|$ and $\frac{|v_1|^4}{|e_3|} \leqslant X$.*

Then, the number of (v_2, d) such that $(e_3, v_1, v_2, d) \in \frac{1}{6}M'_I(X)$ is

$$\begin{aligned}\sum_{v_2,d} 1 = &\prod_{p \leqslant P} \mu'_{I,p}(e_3, v_1) \cdot 2\pi \cdot \frac{X(\log X + \log|e_3| - 4\log|v_1|)}{|v_1|^3} \\ &+ \frac{X \log X}{|v_1|^3} \cdot (o_P(1) + \mathcal{O}(P^{-1}) + \mathcal{O}(\sum_{\substack{p>P, \\ p \| |v_1|^2}} p^{-1})),\end{aligned}$$

where

$$\begin{aligned}\mu'_{I,p}(e_3, v_1) &= \int_{(v_2,d):(e_3,v_1,v_2,d) \in \mathcal{P}^{\max}_{I \otimes \mathbb{Z}_p}(\mathbb{Z}_p)} \frac{\mathrm{d}v_2}{|v_1|_p|e_3|_p} \cdot \frac{\mathrm{d}d}{|v_1|_p^2|v_2|_p^2/|e_3|_p} \\ &= \int_{\langle v_1 \rangle^\perp \subseteq \mathbb{Q}_p^3} \frac{\mathrm{d}v_2}{|v_1|_p|e_3|_p} \cdot \mu'_{I,p}(e_3, v_1, v_2).\end{aligned}$$

If one of the local conditions doesn't hold, there are no such (v_2, d).

Proof. For each $p \leqslant P$, write the set of possible $v_2 \in \langle v_1 \rangle^\perp \subsetneq \mathbb{Z}_p^3$ (such that $(e_3, v_1, v_2, d) \in \mathcal{P}^{\max}_{I \otimes \mathbb{Z}_p}(\mathbb{Z}_p)$ for some d) as the disjoint union of $\mathcal{O}_P(1)$ shifted lattices in which $\mu'_{I,p}(e_3, v_1, v_2)$ is constant.

For $p > P$, the set of possible $v_2 \in \langle v_1 \rangle^\perp \subsetneq \mathbb{Z}_p^3$ (satisfying the local conditions $e_3 \mid v_1 \times v_2$ and

$p^2 \nmid \frac{|v_1|^2|v_2|^2}{e_3}$) is (using the notation of Lemma 4.62)

$$N_p = S_p(e_3, v_1) \backslash \begin{cases} S'_p(e_3, v_1), & p \mid |v_1|^2, \\ S''_p(e_3, v_1), & p \nmid |v_1|^2. \end{cases}$$

The set of possible $v_2 \in \langle v_1 \rangle^\perp \subsetneq \mathbb{R}^3$ (satisfying the local conditions $|v_1| \leqslant |v_2|$ and $\frac{|v_1|^2|v_2|^2}{|e_3|} \leqslant X$) is

$$\{v_2 \in \langle v_1 \rangle^\perp \subsetneq \mathbb{R}^3 \mid |v_1| \leqslant |v_2| \leqslant X^{1/2}|e_3|^{1/2}|v_1|^{-1}\}.$$

You can apply Corollary 4.48 to find the sum of $\frac{1}{|v_2|^2}$ over all possible vectors v_2 outside some line $b_1\mathbb{Z}$. Lemma 4.41 tells us that there are only $\mathcal{O}(1)$ possible vectors v_2 on this line $b_1\mathbb{Z}$. □

Lemma 4.65. *Let $e_3 \in \mathbb{Z}$ be nonzero and assume that the following local conditions hold:*

- *For all $p > P$, we have $p^2 \nmid e_3$.*
- *We have $|e_3|^3 \leqslant X$.*

Then, the number of (v_1, v_2, d) such that $(e_3, v_1, v_2, d) \in \frac{1}{6}M'_I(X)$ is

$$\sum_{v_1,v_2,d} 1 = \prod_{p \leqslant P} \mu'_{I,p}(e_3) \cdot \pi^2 \cdot \frac{X(\log X - 3\log|e_3|)^2}{|e_3|} + \frac{X(\log X)^2}{|e_3|} \cdot (o_P(1) + \mathcal{O}(P^{-1}) + \mathcal{O}(\sum_{\substack{p>P,\\ p|e_3}} p^{-1})),$$

where

$$\mu'_{I,p}(e_3) = \int_{(v_1,v_2,d):(e_3,v_1,v_2,d)\in\mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)} \frac{\mathrm{d}v_1}{|e_3|_p} \cdot \frac{\mathrm{d}v_2}{|v_1|_p|e_3|_p} \cdot \frac{\mathrm{d}d}{|v_1|_p^2|v_2|_p^2/|e_3|_p} = \int_{\mathbb{Q}_p^3} \frac{\mathrm{d}v_1}{|e_3|_p} \cdot \mu'_{I,p}(e_3, v_1).$$

If one of the local conditions doesn't hold, there are no such (v_1, v_2, d).

Proof. For each $p \leqslant P$, we can write the set of possible $v_1 \in \mathbb{Z}_p^3$ (such that $(e_3, v_1, v_2, d) \in \mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)$ for some v_2, d) as the disjoint union of $\mathcal{O}_P(1)$ shifted lattices in which $\mu'_{I,p}(e_3, v_1)$ is constant.

For $p > P$, the set of possible $v_1 \in \mathbb{Z}_p^3$ (satisfying the local conditions $e_3 \mid |v_1|^2$ and $p^2 \nmid e_3$) is (using the notation of Theorem 4.50)

$$S_p(e_3) \backslash \begin{cases} S_p(e_3 p), & p \mid e_3, \\ S_p(e_3 p^2), & p \nmid e_3. \end{cases}$$

The set of possible $v_1 \in \mathbb{R}^3$ (satisfying the local conditions $|e_3| \leqslant |v_1|$ and $\frac{|v_1|^4}{|e_3|} \leqslant X$) is

$$\{v_1 \in \mathbb{R}^3 \mid |e_3| \leqslant |v_1| \leqslant X^{1/4}|e_3|^{1/4}\}.$$

Then, Theorem 4.50 and integration by parts (Lemma 4.44) show the claim. □

Lemma 4.66 (Lemma 4.43)**.** *The number of $(e_3, v_1, v_2, d) \in \frac{1}{6}M'_I(X)$ is*

$$\#\tfrac{1}{6}M'_I(X) = \prod_{p \leqslant P} \mu'_{I,p} \cdot \frac{2\pi^2}{9} \cdot X(\log X)^3 + X(\log X)^3(o_P(1) + \mathcal{O}(P^{-1})),$$

where

$$\mu'_{I,p} = \int_{\mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)} \mathrm{d}'m = \int_{\mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)} \mathrm{d}e_3 \cdot \frac{\mathrm{d}v_1}{|e_3|_p} \cdot \frac{\mathrm{d}v_2}{|v_1|_p|e_3|_p} \cdot \frac{\mathrm{d}d}{|v_1|_p^2|v_2|_p^2/|e_3|_p} = \int_{\mathbb{Q}_p} \mathrm{d}e_3 \cdot \mu'_{I,p}(e_3).$$

Proof. For each $p \leqslant P$, we can write the set of possible $e_3 \in \mathbb{Z}_p$ (such that $(e_3, v_1, v_2, d) \in \mathcal{P}^{\max}_{I\otimes\mathbb{Z}_p}(\mathbb{Z}_p)$ for some v_1, v_2, d) as the disjoint union of $\mathcal{O}_P(1)$ shifted lattices in which $\mu'_{I,p}(e_3)$ is constant.

For $p > P$, the set of possible $e_3 \in \mathbb{Z}_p$ (satisfying the local condition $p^2 \nmid e_3$) is $\mathbb{Z}_p \backslash p^2\mathbb{Z}_p$.

The set of possible $e_3 \in \mathbb{R}$ (satisfying the local condition $|e_3|^3 \leqslant X$) is $[-X^{1/3}, X^{1/3}]$.

Then, integration by parts (Lemma 4.44) shows the claim. □

This concludes the proof of Theorem 4.35 (and Theorem 1.8).

Chapter 5

Symmetric groups

5.1 Degree 3

Let $G = S_3$ by the symmetric group of degree three and let K be any field with $\mathrm{char}(K) \neq 2, 3$. We then have an isomorphism $K[G] \cong K \times K \times M_2(K)$, corresponding to the irreducible representations $\mathrm{triv}, \mathrm{sgn}, \mathrm{std}$. We define these representations as follows:

	id	(1 2)	(2 3)	(1 3)	(1 3 2)	(1 2 3)
triv	1	1	1	1	1	1
sgn	1	-1	-1	-1	1	1
std	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ -1 & -1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$

The decomposition of tensor products of irreducible representations of G is then:

$\otimes$	triv	sgn	std
triv	triv	sgn	std
sgn	sgn	triv	std
std	std	std	$\mathrm{triv} \oplus \mathrm{sgn} \oplus \mathrm{std}$

Accordingly, fix the following projection and inclusion maps $V_1 \otimes V_2 \rightleftarrows W$:

$$\begin{aligned}
\operatorname{sgn} \otimes \operatorname{sgn} &\rightleftarrows \operatorname{triv} \\
1 \otimes 1 &\mapsto 1
\end{aligned}$$

$$\begin{aligned}
\operatorname{sgn} \otimes \operatorname{std} &\rightleftarrows \operatorname{std} \\
1 \otimes \begin{pmatrix} a \\ b \end{pmatrix} &\mapsto \frac{1}{3}\begin{pmatrix} -a-2b \\ 2a+b \end{pmatrix} \\
1 \otimes \begin{pmatrix} a+2b \\ -2a-b \end{pmatrix} &\mapsfrom \begin{pmatrix} a \\ b \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
\operatorname{std} \otimes \operatorname{std} &\rightleftarrows \operatorname{triv} \\
\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} &\mapsto \frac{1}{3}(2ac + 2bd + ad + bc) \\
e_1 \otimes e_1 - \frac{1}{2}(e_1 \otimes e_2 + e_2 \otimes e_1) + e_2 \otimes e_2 &\mapsfrom 1
\end{aligned}$$

$$\begin{aligned}
\operatorname{std} \otimes \operatorname{std} &\rightleftarrows \operatorname{sgn} \\
\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} &\mapsto \frac{1}{2}(ad - bc) \\
e_1 \otimes e_2 - e_2 \otimes e_1 &\mapsfrom 1
\end{aligned}$$

$$\begin{aligned}
\operatorname{std} \otimes \operatorname{std} &\rightleftarrows \operatorname{std} \\
\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} &\mapsto \frac{1}{3}\begin{pmatrix} ac - 2bd - ad - bc \\ bd - 2ac - ad - bc \end{pmatrix} \\
ae_1 \otimes e_1 - (a+b)(e_1 \otimes e_2 + e_2 \otimes e_1) + be_2 \otimes e_2 &\mapsfrom \begin{pmatrix} a \\ b \end{pmatrix}
\end{aligned}$$

Some of the representations $\operatorname{Hom}_K(W \to V_1 \otimes V_2)$ of $K[G]_1^\times$ decompose further:

$$\begin{aligned}
\operatorname{Hom}_K(\operatorname{triv} \to \operatorname{sgn} \otimes \operatorname{sgn}) &\cong \operatorname{sgn} \otimes \operatorname{sgn} \\
\operatorname{Hom}_K(\operatorname{std} \to \operatorname{sgn} \otimes \operatorname{std}) &\cong \operatorname{sgn} \otimes M_2(\operatorname{std}) \\
&\cong (\operatorname{sgn} \otimes \mathfrak{sl}(\operatorname{std})) \oplus \operatorname{sgn} \\
\operatorname{Hom}_K(\operatorname{triv} \to \operatorname{std} \otimes \operatorname{std}) &\cong \operatorname{Sym}^2(\operatorname{std}) \oplus \operatorname{Alt}^2(\operatorname{std}) \\
&\cong \operatorname{Sym}^2(\operatorname{std}) \oplus \det(\operatorname{std}) \\
\operatorname{Hom}_K(\operatorname{sgn} \to \operatorname{std} \otimes \operatorname{std}) &\cong \frac{1}{\operatorname{sgn}}\left(\operatorname{Sym}^2(\operatorname{std}) \oplus \operatorname{Alt}^2(\operatorname{std})\right) \\
&\cong \frac{1}{\operatorname{sgn}} \operatorname{Sym}^2(\operatorname{std}) \oplus \frac{1}{\operatorname{sgn}} \det(\operatorname{std}) \\
\operatorname{Hom}_K(\operatorname{std} \to \operatorname{std} \otimes \operatorname{std}) &\cong \frac{1}{\det(\operatorname{std})} \operatorname{Sym}^3(\operatorname{std}) \oplus \operatorname{std} \oplus \operatorname{std}
\end{aligned}$$

When considering nondegenerate extensions, only the following summands remain. (The trivial

extension projects to 0 on all other summands.)

$$\begin{aligned} \text{triv} &\longrightarrow \text{sgn} \otimes \text{sgn} \\ 1 &\longmapsto 1 \otimes d \end{aligned} \qquad (d \in \text{sgn} \otimes \text{sgn})$$

$$\begin{aligned} \text{std} &\longrightarrow \text{sgn} \otimes \text{std} \\ x &\longmapsto 1 \otimes Mx \end{aligned} \qquad (M \in \text{sgn} \otimes \mathfrak{sl}(\text{std}))$$

$$\begin{aligned} \text{triv} &\longrightarrow \text{std} \otimes \text{std} \\ 1 &\longmapsto s \end{aligned} \qquad (s \in \text{Sym}^2(\text{std}))$$

$$\begin{aligned} \text{sgn} &\longrightarrow \text{std} \otimes \text{std} \\ 1 &\longmapsto e(e_1 \otimes e_2 - e_2 \otimes e_1) \end{aligned} \qquad (e \in \tfrac{\det(\text{std})}{\text{sgn}})$$

$$\begin{aligned} \text{std} &\longrightarrow \text{std} \otimes \text{std} \\ x &\longmapsto v(x) \end{aligned} \qquad (v \in \tfrac{1}{\det(\text{std})} \text{Sym}^3(\text{std}))$$

where

$$v(\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)) = (3v_1 b - v_2 a)e_1 \otimes e_1 + (v_2 b - v_3 a)(e_1 \otimes e_2 + e_2 \otimes e_1) + (v_3 b - 3v_4 a)e_2 \otimes e_2$$

for $v = v_1 e_1^3 + v_2 e_1^2 e_2 + v_3 e_1 e_2^2 + v_4 e_2^3 \in \frac{1}{\det(\text{std})} \text{Sym}^3(\text{std})$.

We can thus identify any element $m \in \mathcal{P}^{\text{nondeg}}(K)$ with a tuple

$$(d, M, s, e, v) \in K \oplus \mathfrak{sl}_2(K) \oplus \text{Sym}^2(K^2) \oplus K \oplus \text{Sym}^3(K^2).$$

The corresponding values for the trivial extension are:

$$d = 1, \qquad M = \begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix}, \qquad s = e_1^2 - e_1 e_2 + e_2^2,$$

$$e = 1, \qquad v = -e_1^2 e_2 + e_1 e_2^2.$$

For $v = v_1 e_1^3 + v_2 e_1^2 e_2 + v_3 e_1 e_2^2 + v_4 e_2^3$, define

$$\begin{aligned} \text{Hessian}(v) &= \det \begin{pmatrix} 6v_1 e_1 + 2v_2 e_2 & 2v_2 e_1 + 2v_3 e_2 \\ 2v_2 e_1 + 2v_3 e_2 & 2v_3 e_1 + 6v_4 e_2 \end{pmatrix} \\ &= 4[(3v_1 e_1 + v_2 e_2)(v_3 e_1 + 3v_4 e_2) - (v_2 e_1 + v_3 e_2)^2] \\ &= 4[(3v_1 v_3 - v_2^2)e_1^2 + (9v_1 v_4 - v_2 v_3)e_1 e_2 + (3v_2 v_4 - v_3^2)e_2^2]. \end{aligned}$$

The associativity condition is then equivalent to:

$$\begin{aligned} -4s &= \text{Hessian}(v) \\ -3dI_2 &= M^2 \\ eM &= \begin{pmatrix} -s_2 & 2s_1 \\ -2s_3 & s_2 \end{pmatrix} \end{aligned} \qquad \text{for } s = s_1 e_1^2 + s_2 e_1 e_2 + s_3 e_2^2$$

Note that M^2 is a multiple of the identity matrix I_2 for *any* trace-free 2×2-matrix M.

The discriminants are

$$\begin{aligned} \operatorname{disc}(m) &= \tfrac{1}{9} \cdot d \cdot \operatorname{disc}(s)^2 &&= \frac{\operatorname{disc}(v)^3}{e^2}, \\ \operatorname{disc}^{\langle (1\ 2) \rangle}(m) &= -\tfrac{1}{3} \cdot \operatorname{disc}(s) &&= \operatorname{disc}(v), \\ \operatorname{disc}^{\langle (1\ 2\ 3) \rangle}(m) &= d &&= \frac{\operatorname{disc}(v)}{e^2}. \end{aligned}$$

5.2 Higher degrees

Let $n \geqslant 1$ be an integer and let K be a field with $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) > n$. To an extension of K of degree n, we can then canonically associate an S_n-extension of K.

The representations that were previously used to parametrize extension of degree $n = 3, 4, 5$ are irreducible $K[G]_1^\times$-subrepresentations P of $\mathcal{H}$ (see the appendix for notation and the decomposition of $\mathcal{H}$): Levi [22] (and later Delone and Faddeev [14]) used the representation $\frac{1}{\det(\mathrm{std})} \operatorname{Sym}^3(\mathrm{std}) = X(\mathrm{std})$ for $n = 3$. Wright and Yukie [33] used the representation $\operatorname{Sym}^2(\mathrm{std}) \otimes \mathrm{2a}^* = \frac{\operatorname{Sym}^2(\mathrm{std})}{\mathrm{2a}}$ for $n = 4$ and the representation $\operatorname{Alt}^2(\mathrm{5a}') \otimes \mathrm{std}'^* = \frac{\operatorname{Alt}^2(\mathrm{5a}')}{\mathrm{std}'}$ for $n = 5$.

For any projection map $p : \mathcal{P} \to P$, denote by $\ker(P)$ the kernel of the $K[G]_1^\times$-representation P. We therefore obtain a representation P of the group $K[G]_1^\times / \ker(P)$. For this representation to parametrize S_n-extensions of K, we want the stabilizer of $p(\pi) \in P$ to be $G \hookrightarrow K[G]_1^\times / \ker(P)$. In other words, we want $G \cap \ker(P) = 1$ and the $K[G]_1^\times$-stabilizer of $p(\pi)$ should be $G \cdot \ker(P) \subseteq K[G]_1^\times$. On the other hand, to facilitate counting, we want the $K^{\mathrm{sep}}[G]_1^\times$-orbit of $p(\pi)$ to have small codimension in P. (In the above parametrizations for $n = 3, 4, 5$, the orbit was in fact dense, so we obtained a prehomogeneous vector space.)

Carefully studing the tables in the appendix, you can show that for $n = 6$, there is no such projection $p : \mathcal{P} \twoheadrightarrow P$ such that the orbit $p(\mathcal{P}^{\mathrm{nondeg}}(K^{\mathrm{sep}})) = p(K^{\mathrm{sep}}[G]_1^\times.\pi)$ has codimension less than 15.

Remark 5.1. There is no projection $p : \mathcal{P} \to P$ such that the stabilizer of $p(\pi) \in P$ in the group $K[G]_1^\times / \ker(P)$ is finite and the orbit $p(\mathcal{P}^{\mathrm{nondeg}}) \subseteq P$ has codimension less than 15.

Chapter 6

Appendix: Decompositions

Let $K = \mathbb{C}$ be the field of complex numbers. In the following tables, we analyze the space $\mathcal{H}$ for certain small groups G. First, we write down the character table of G. Then, we decompose the subspace of $\mathcal{H}$ spanned by the nondegenerate orbit $\mathcal{P}^{\mathrm{nondeg}}(K)$ into irreducible $K[G]_1^\times$-representations. We write a summand $L = \mathrm{Hom}_G(V_u \to V_i \otimes V_j)$ as $\frac{V_i \cdot V_j}{V_u}$. For each irreducible summand occuring in $\mathcal{H}$, we give its multiplicity. Furthermore, we denote by $\ker(L) \subseteq K[G]_1^\times$ the kernel of the $K[G]_1^\times$-representation L. We write $X(V_i)$ for the irreducible representation of $\mathrm{GL}(V_i)$ with highest weight $(2, 0, \ldots, 0, -1)$ and $Y(V_i)$ for the irreducible representation of $\mathrm{GL}(V_i)$ with highest weight $(1, 1, 0, \ldots, 0, -1)$. The summands of the form $\frac{\mathrm{triv} \cdot V_i}{V_i}$ (which are fixed by the unit condition (Cu)) are omitted.

Remark 6.1. Let $n \geqslant 1$ be an integer and $G = S_n$. Let K be a field of characteristic zero. To an extension of K of degree n, we can then canonically associate an S_n-extension of K.

The representations that were previously used to parametrize extension of degree $n = 3, 4, 5$ are irreducible $K[G]_1^\times$-subrepresentations P of $\mathcal{H}$: Levi [22] (and later Delone and Faddeev [14]) used the representation $\frac{1}{\det(\mathrm{std})} \mathrm{Sym}^3(\mathrm{std}) = X(\mathrm{std})$ for $n = 3$. Wright and Yukie [33] used the representation $\mathrm{Sym}^2(\mathrm{std}) \otimes 2\mathrm{a}^* = \frac{\mathrm{Sym}^2(\mathrm{std})}{2\mathrm{a}}$ for $n = 4$ and the representation $\mathrm{Alt}^2(5\mathrm{a}') \otimes \mathrm{std}'^* = \frac{\mathrm{Alt}^2(5\mathrm{a}')}{\mathrm{std}'}$ for $n = 5$.

For any projection map $p : \mathcal{H} \twoheadrightarrow P$, denote by $\ker(P)$ the kernel of the $K[G]_1^\times$-representation P. We therefore obtain a representation P of the group $K[G]_1^\times / \ker(P)$. For this representation to parametrize G-extensions of K, we need the stabilizer of $p(\pi) \in P$ to be $G \hookrightarrow K[G]_1^\times / \ker(P)$. In other words, we want $G \cap \ker(P) = 1$ and the $K[G]_1^\times$-stabilizer of $p(\pi)$ should be $G \cdot \ker(P) \subseteq K[G]_1^\times$. On the other hand, to facilitate counting, it is desirable that the $K^{\mathrm{sep}}[G]_1^\times$-orbit of $p(\pi)$ has small codimension in P.

In the above parametrizations for $n = 3, 4, 5$, the orbit was in fact dense, so we obtained a prehomogeneous vector space. Unfortunately, we are not so lucky for $n = 6$:

Remark 6.2. For $G = S_6$, there is no projection $p : \mathcal{H} \twoheadrightarrow P$ such that the stabilizer of $p(\pi) \in P$ in the group $K[G]_1^\times / \ker(P)$ is $G \hookrightarrow K[G]_1^\times / \ker(P)$ and the orbit $p(\mathcal{P}^{\mathrm{nondeg}}) \subseteq P$ has codimension less than 15.

6.1 Symmetric Group S_2

Order: 2

Conjugacy classes: $\mathbf{1} = [1,1]$, $\mathbf{2} = [2]$

Table 6.1.1: Irreducible characters for the Symmetric Group S_2

	1	**2**
Size	1	1
triv	1	1
sign	1	-1

Table 6.1.2: Nontrivial summands for the Symmetric Group S_2

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0

6.2 Symmetric Group S_3

Order: 6

Conjugacy classes: **1** = $[1,1,1]$, **2** = $[1,2]$, **3** = $[3]$

Table 6.2.1: Irreducible characters for the Symmetric Group S_3

	1	**2**	**3**
Size	1	3	2
triv	1	1	1
sign	1	-1	1
std	2	0	-1

Table 6.2.2: Nontrivial summands for the Symmetric Group S_3

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(\mathrm{std})}{\mathrm{sign}}$	1	4	-3
1	$\mathrm{Sym}^2(\mathrm{std})$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std}) \cdot \mathrm{sign}$	3	4	-1
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0
1	$\mathrm{X}(\mathrm{std})$	4	4	0

6.3 Symmetric Group S_4

Order: 24

Conjugacy classes: **1** = $[1,1,1,1]$, **2** = $[1,1,2]$, **3** = $[1,3]$, **4** = $[2,2]$, **5** = $[4]$

Table 6.3.1: Irreducible characters for the Symmetric Group S_4

	1	**2**	**3**	**4**	**5**
Size	1	6	8	3	6
triv	1	1	1	1	1
sign	1	−1	1	1	−1
2a	2	0	−1	2	0
std	3	1	0	−1	−1
std′	3	−1	0	−1	1

Table 6.3.2: Nontrivial summands for the Symmetric Group S_4

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(\mathrm{std})}{\mathrm{std}'}$	9	17	−8
1	$\frac{\mathrm{sign}\cdot\mathrm{std}}{\mathrm{std}'}$	9	17	−8
1	$\frac{\mathrm{sign}\cdot\mathrm{std}'}{\mathrm{std}}$	9	17	−8
1	$\frac{\mathrm{std}\cdot\mathrm{std}'}{\mathrm{sign}}$	9	17	−8
1	$\frac{\mathrm{Alt}^2(\mathrm{2a})}{\mathrm{sign}}$	1	4	−3
1	$\mathrm{Sym}^2(\mathrm{std}')$	6	9	−3
1	$\mathrm{Sym}^2(\mathrm{std})$	6	9	−3
1	$\mathrm{Y}(\mathrm{std}')$	6	9	−3
1	$\frac{\mathrm{2a}\cdot\mathrm{std}}{\mathrm{std}'}$	18	20	−2
1	$\frac{\mathrm{2a}\cdot\mathrm{std}'}{\mathrm{std}}$	18	20	−2
1	$\frac{\mathrm{std}\cdot\mathrm{std}'}{\mathrm{2a}}$	18	20	−2
1	$\mathrm{Sym}^2(\mathrm{2a})$	3	4	−1

Table 6.3.2: Nontrivial summands for the Symmetric Group S_4

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathfrak{sl}(2\text{a}) \cdot \text{sign}$	3	4	-1
1	$\text{Sym}^2(\text{sign})$	1	1	0
1	X(2a)	4	4	0
1	$\dfrac{\text{Sym}^2(\text{std}')}{2\text{a}}$	12	12	0
1	$\dfrac{\text{Sym}^2(\text{std})}{2\text{a}}$	12	12	0
1	$\dfrac{\text{Sym}^2(\text{std}')}{\text{std}}$	18	17	1
1	$\mathfrak{sl}(\text{std}') \cdot 2\text{a}$	16	12	4
1	$\mathfrak{sl}(\text{std}) \cdot 2\text{a}$	16	12	4
1	X(std)	15	9	6
1	$\mathfrak{sl}(\text{std}') \cdot \text{std}$	24	17	7
1	$\mathfrak{sl}(\text{std}) \cdot \text{std}'$	24	17	7

6.4 Symmetric Group S_5

Order: 120

Conjugacy classes: **1** $= [1,1,1,1,1]$, **2** $= [1,1,1,2]$, **3** $= [1,1,3]$, **4** $= [1,2,2]$, **5** $= [1,4]$, **6** $= [2,3]$, **7** $= [5]$

Table 6.4.1: Irreducible characters for the Symmetric Group S_5

	1	**2**	**3**	**4**	**5**	**6**	**7**
Size	1	10	20	15	30	20	24
triv	1	1	1	1	1	1	1
sign	1	−1	1	1	−1	−1	1
std	4	2	1	0	0	−1	−1
std′	4	−2	1	0	0	1	−1
5a	5	−1	−1	1	1	−1	0
5a′	5	1	−1	1	−1	1	0
6a	6	0	0	−2	0	0	1

Table 6.4.2: Nontrivial summands for the Symmetric Group S_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{5a \cdot 5a'}{\text{sign}}$	25	49	−24
1	$\frac{\text{sign} \cdot 5a}{5a'}$	25	49	−24
1	$\frac{\text{sign} \cdot 5a'}{5a}$	25	49	−24
1	$\frac{\text{sign} \cdot \text{std}}{\text{std}'}$	16	31	−15
1	$\frac{\text{sign} \cdot \text{std}'}{\text{std}}$	16	31	−15
1	$\frac{\text{std} \cdot \text{std}'}{\text{sign}}$	16	31	−15
1	$\text{Sym}^2(6a)$	21	36	−15
1	$\frac{\text{Sym}^2(6a)}{\text{sign}}$	21	36	−15
1	$\frac{\text{Alt}^2(\text{std}')}{6a}$	36	51	−15
1	$\frac{\text{Alt}^2(\text{std})}{6a}$	36	51	−15
1	$\text{Sym}^2(5a')$	15	25	−10

Table 6.4.2: Nontrivial summands for the Symmetric Group S_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Sym}^2(5a)$	15	25	-10
1	$\mathrm{Sym}^2(\mathrm{std}')$	10	16	-6
1	$\mathrm{Sym}^2(\mathrm{std})$	10	16	-6
1	$\mathfrak{sl}(6a)\cdot\mathrm{sign}$	35	36	-1
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0
1	$\frac{\mathrm{Alt}^2(5a')}{\mathrm{std}'}$	40	40	0
1	$\frac{\mathrm{Alt}^2(5a)}{\mathrm{std}'}$	40	40	0
1	$\frac{\mathrm{Alt}^2(5a')}{6a}$	60	60	0
1	$\frac{\mathrm{Alt}^2(5a)}{6a}$	60	60	0
1	$\frac{\mathrm{Sym}^2(\mathrm{std}')}{\mathrm{std}}$	40	31	9
1	$\frac{\mathrm{Alt}^2(6a)}{\mathrm{std}'}$	60	51	9
1	$\frac{\mathrm{Sym}^2(\mathrm{std}')}{5a'}$	50	40	10
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{5a'}$	50	40	10
1	$\frac{\mathrm{Alt}^2(6a)}{5a}$	75	60	15
1	$\mathrm{X}(\mathrm{std})$	36	16	20
1	$\frac{\mathrm{Sym}^2(5a')}{\mathrm{std}}$	60	40	20
1	$\frac{\mathrm{Sym}^2(5a)}{\mathrm{std}}$	60	40	20
1	$\frac{\mathrm{std}\cdot 5a}{\mathrm{std}'}$	80	55	25
1	$\frac{\mathrm{std}\cdot\mathrm{std}'}{5a}$	80	55	25

Table 6.4.2: Nontrivial summands for the Symmetric Group S_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}}{\mathrm{std}}$	80	55	25
1	$\frac{\mathrm{Sym}^2(5\mathrm{a}')}{5\mathrm{a}}$	75	49	26
1	$\frac{\mathrm{Sym}^2(5\mathrm{a})}{5\mathrm{a}'}$	75	49	26
1	$\mathfrak{sl}(\mathrm{std}')\cdot\mathrm{std}$	60	31	29
1	$\frac{\mathrm{std}\cdot 6\mathrm{a}}{\mathrm{std}'}$	96	66	30
1	$\frac{\mathrm{std}\cdot\mathrm{std}'}{6\mathrm{a}}$	96	66	30
1	$\frac{\mathrm{std}'\cdot 6\mathrm{a}}{\mathrm{std}}$	96	66	30
1	$\frac{\mathrm{Sym}^2(6\mathrm{a})}{\mathrm{std}}$	84	51	33
1	$\mathfrak{sl}(\mathrm{std}')\cdot 5\mathrm{a}'$	75	40	35
1	$\mathfrak{sl}(\mathrm{std})\cdot 5\mathrm{a}'$	75	40	35
1	$\frac{5\mathrm{a}\cdot 5\mathrm{a}'}{\mathrm{std}'}$	100	64	36
1	$\frac{5\mathrm{a}\cdot 5\mathrm{a}'}{\mathrm{std}}$	100	64	36
1	$\frac{\mathrm{std}\cdot 5\mathrm{a}}{5\mathrm{a}'}$	100	64	36
1	$\frac{\mathrm{std}\cdot 5\mathrm{a}'}{5\mathrm{a}}$	100	64	36
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}}{5\mathrm{a}'}$	100	64	36
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}'}{5\mathrm{a}}$	100	64	36
1	$\mathfrak{sl}(\mathrm{std}')\cdot 6\mathrm{a}$	90	51	39
1	$\mathfrak{sl}(\mathrm{std})\cdot 6\mathrm{a}$	90	51	39
1	$\mathrm{X}(5\mathrm{a}')$	70	25	45

Table 6.4.2: Nontrivial summands for the Symmetric Group S_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{X}(5\mathrm{a})$	70	25	45
2	$\frac{\mathrm{Sym}^2(6\mathrm{a})}{5\mathrm{a}'}$	105	60	45
1	$\frac{\mathrm{Sym}^2(6\mathrm{a})}{5\mathrm{a}}$	105	60	45
1	$\frac{5\mathrm{a}\cdot 6\mathrm{a}}{\mathrm{std}'}$	120	75	45
1	$\frac{5\mathrm{a}\cdot 6\mathrm{a}}{\mathrm{std}}$	120	75	45
1	$\frac{5\mathrm{a}'\cdot 6\mathrm{a}}{\mathrm{std}'}$	120	75	45
1	$\frac{5\mathrm{a}'\cdot 6\mathrm{a}}{\mathrm{std}}$	120	75	45
1	$\frac{\mathrm{std}\cdot 5\mathrm{a}}{6\mathrm{a}}$	120	75	45
1	$\frac{\mathrm{std}\cdot 5\mathrm{a}'}{6\mathrm{a}}$	120	75	45
1	$\frac{\mathrm{std}\cdot 6\mathrm{a}}{5\mathrm{a}'}$	120	75	45
1	$\frac{\mathrm{std}\cdot 6\mathrm{a}}{5\mathrm{a}}$	120	75	45
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}}{6\mathrm{a}}$	120	75	45
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}'}{6\mathrm{a}}$	120	75	45
1	$\frac{\mathrm{std}'\cdot 6\mathrm{a}}{5\mathrm{a}'}$	120	75	45
1	$\frac{\mathrm{std}'\cdot 6\mathrm{a}}{5\mathrm{a}}$	120	75	45
1	$\mathrm{Y}(6\mathrm{a})$	84	36	48
1	$\mathfrak{sl}(5\mathrm{a}')\cdot\mathrm{std}$	96	40	56
1	$\mathfrak{sl}(5\mathrm{a}')\cdot\mathrm{std}'$	96	40	56
1	$\mathfrak{sl}(5\mathrm{a})\cdot\mathrm{std}$	96	40	56

Table 6.4.2: Nontrivial summands for the Symmetric Group S_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathfrak{sl}(5\mathrm{a}) \cdot \mathrm{std}'$	96	40	56
1	$\dfrac{5\mathrm{a} \cdot 5\mathrm{a}'}{6\mathrm{a}}$	150	84	66
1	$\dfrac{5\mathrm{a} \cdot 6\mathrm{a}}{5\mathrm{a}'}$	150	84	66
1	$\dfrac{5\mathrm{a}' \cdot 6\mathrm{a}}{5\mathrm{a}}$	150	84	66
1	$\mathfrak{sl}(5\mathrm{a}') \cdot 5\mathrm{a}$	120	49	71
1	$\mathfrak{sl}(5\mathrm{a}) \cdot 5\mathrm{a}'$	120	49	71
1	$\mathfrak{sl}(5\mathrm{a}') \cdot 6\mathrm{a}$	144	60	84
1	$\mathfrak{sl}(5\mathrm{a}) \cdot 6\mathrm{a}$	144	60	84
1	$\mathfrak{sl}(6\mathrm{a}) \cdot \mathrm{std}$	140	51	89
1	$\mathfrak{sl}(6\mathrm{a}) \cdot \mathrm{std}'$	140	51	89
2	$\mathfrak{sl}(6\mathrm{a}) \cdot 5\mathrm{a}$	175	60	115
2	$\mathfrak{sl}(6\mathrm{a}) \cdot 5\mathrm{a}'$	175	60	115

6.5 Symmetric Group S_6

Order: 720

Conjugacy classes: **1** = $[1,1,1,1,1,1]$, **2** = $[1,1,1,1,2]$, **3** = $[1,1,1,3]$, **4** = $[1,1,2,2]$, **5** = $[1,1,4]$, **6** = $[1,2,3]$, **7** = $[1,5]$, **8** = $[2,2,2]$, **9** = $[2,4]$, **10** = $[3,3]$, **11** = $[6]$

Table 6.5.1: Irreducible characters for the Symmetric Group S_6

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Size	1	15	40	45	90	120	144	15	90	40	120
triv	1	1	1	1	1	1	1	1	1	1	1
sign	1	−1	1	1	−1	−1	1	−1	1	1	−1
std	5	3	2	1	1	0	0	−1	−1	−1	−1
std′	5	−3	2	1	−1	0	0	1	−1	−1	1
5a	5	−1	−1	1	1	−1	0	3	−1	2	0
5a′	5	1	−1	1	−1	1	0	−3	−1	2	0
9a	9	−3	0	1	1	0	−1	−3	1	0	0
9a′	9	3	0	1	−1	0	−1	3	1	0	0
10a	10	−2	1	−2	0	1	0	2	0	1	−1
10a′	10	2	1	−2	0	−1	0	−2	0	1	1
16a	16	0	−2	0	0	0	1	0	0	−2	0

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Sym}^2(16a)$	136	256	−120
1	$\frac{\mathrm{Sym}^2(16a)}{\mathrm{sign}}$	136	256	−120
1	$\frac{10a \cdot 10a'}{\mathrm{sign}}$	100	199	−99
1	$\frac{\mathrm{sign} \cdot 10a}{10a'}$	100	199	−99
1	$\frac{\mathrm{sign} \cdot 10a'}{10a}$	100	199	−99
1	$\frac{9a \cdot 9a'}{\mathrm{sign}}$	81	161	−80
1	$\frac{\mathrm{sign} \cdot 9a}{9a'}$	81	161	−80
1	$\frac{\mathrm{sign} \cdot 9a'}{9a}$	81	161	−80
1	$\mathrm{Sym}^2(10a')$	55	100	−45

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Sym}^2(10a)$	55	100	-45
1	$\mathrm{Sym}^2(9a')$	45	81	-36
1	$\mathrm{Sym}^2(9a)$	45	81	-36
1	$\frac{5a\cdot 5a'}{\mathrm{sign}}$	25	49	-24
1	$\frac{\mathrm{sign}\cdot 5a}{5a'}$	25	49	-24
1	$\frac{\mathrm{sign}\cdot 5a'}{5a}$	25	49	-24
1	$\frac{\mathrm{sign}\cdot \mathrm{std}}{\mathrm{std}'}$	25	49	-24
1	$\frac{\mathrm{sign}\cdot \mathrm{std}'}{\mathrm{std}}$	25	49	-24
1	$\frac{\mathrm{std}\cdot \mathrm{std}'}{\mathrm{sign}}$	25	49	-24
1	$\frac{\mathrm{Alt}^2(5a')}{10a}$	100	124	-24
1	$\frac{\mathrm{Alt}^2(5a)}{10a}$	100	124	-24
1	$\frac{\mathrm{Alt}^2(\mathrm{std}')}{10a'}$	100	124	-24
1	$\frac{\mathrm{Alt}^2(\mathrm{std})}{10a'}$	100	124	-24
1	$\mathrm{Sym}^2(5a')$	15	25	-10
1	$\mathrm{Sym}^2(5a)$	15	25	-10
1	$\mathrm{Sym}^2(\mathrm{std}')$	15	25	-10
1	$\mathrm{Sym}^2(\mathrm{std})$	15	25	-10
1	$\mathfrak{sl}(16a)\cdot \mathrm{sign}$	255	256	-1
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Sym}^2(5a')}{5a}$	75	49	26
1	$\frac{\mathrm{Sym}^2(\mathrm{std}')}{\mathrm{std}}$	75	49	26
1	$\frac{\mathrm{Sym}^2(5a')}{9a'}$	135	105	30
1	$\frac{\mathrm{Sym}^2(5a)}{9a'}$	135	105	30
1	$\frac{\mathrm{Sym}^2(\mathrm{std}')}{9a'}$	135	105	30
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{9a'}$	135	105	30
1	X(5a)	70	25	45
1	X(std)	70	25	45
1	$\mathfrak{sl}(5a') \cdot 5a$	120	49	71
1	$\mathfrak{sl}(\mathrm{std}') \cdot \mathrm{std}$	120	49	71
1	$\frac{5a \cdot 5a'}{9a}$	225	129	96
1	$\frac{5a \cdot 9a}{5a'}$	225	129	96
1	$\frac{5a \cdot 9a}{\mathrm{std}}$	225	129	96
1	$\frac{5a \cdot 9a'}{\mathrm{std}'}$	225	129	96
1	$\frac{5a' \cdot 9a}{5a}$	225	129	96
1	$\frac{5a' \cdot 9a}{\mathrm{std}'}$	225	129	96
1	$\frac{5a' \cdot 9a'}{\mathrm{std}}$	225	129	96
1	$\frac{\mathrm{std} \cdot 5a}{9a}$	225	129	96
1	$\frac{\mathrm{std} \cdot 5a'}{9a'}$	225	129	96

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{std}\cdot 9\mathrm{a}}{5\mathrm{a}}$	225	129	96
1	$\frac{\mathrm{std}\cdot 9\mathrm{a}}{\mathrm{std}'}$	225	129	96
1	$\frac{\mathrm{std}\cdot 9\mathrm{a}'}{5\mathrm{a}'}$	225	129	96
1	$\frac{\mathrm{std}\cdot \mathrm{std}'}{9\mathrm{a}}$	225	129	96
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}}{9\mathrm{a}'}$	225	129	96
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}'}{9\mathrm{a}}$	225	129	96
1	$\frac{\mathrm{std}'\cdot 9\mathrm{a}}{5\mathrm{a}'}$	225	129	96
1	$\frac{\mathrm{std}'\cdot 9\mathrm{a}}{\mathrm{std}}$	225	129	96
1	$\frac{\mathrm{std}'\cdot 9\mathrm{a}'}{5\mathrm{a}}$	225	129	96
1	$\frac{5\mathrm{a}\cdot 16\mathrm{a}}{\mathrm{std}'}$	400	304	96
1	$\frac{5\mathrm{a}\cdot 16\mathrm{a}}{\mathrm{std}}$	400	304	96
1	$\frac{5\mathrm{a}'\cdot 16\mathrm{a}}{\mathrm{std}'}$	400	304	96
1	$\frac{5\mathrm{a}'\cdot 16\mathrm{a}}{\mathrm{std}}$	400	304	96
1	$\frac{\mathrm{std}\cdot 16\mathrm{a}}{5\mathrm{a}'}$	400	304	96
1	$\frac{\mathrm{std}\cdot 16\mathrm{a}}{5\mathrm{a}}$	400	304	96
1	$\frac{\mathrm{std}\cdot 5\mathrm{a}}{16\mathrm{a}}$	400	304	96
1	$\frac{\mathrm{std}\cdot 5\mathrm{a}'}{16\mathrm{a}}$	400	304	96
1	$\frac{\mathrm{std}'\cdot 16\mathrm{a}}{5\mathrm{a}'}$	400	304	96
1	$\frac{\mathrm{std}'\cdot 16\mathrm{a}}{5\mathrm{a}}$	400	304	96

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}}{16\mathrm{a}}$	400	304	96
1	$\frac{\mathrm{std}'\cdot 5\mathrm{a}'}{16\mathrm{a}}$	400	304	96
1	$\frac{5\mathrm{a}\cdot 10\mathrm{a}'}{5\mathrm{a}'}$	250	148	102
1	$\frac{5\mathrm{a}\cdot 5\mathrm{a}'}{10\mathrm{a}'}$	250	148	102
1	$\frac{5\mathrm{a}'\cdot 10\mathrm{a}'}{5\mathrm{a}}$	250	148	102
1	$\frac{\mathrm{std}\cdot 10\mathrm{a}}{\mathrm{std}'}$	250	148	102
1	$\frac{\mathrm{std}\cdot \mathrm{std}'}{10\mathrm{a}}$	250	148	102
1	$\frac{\mathrm{std}'\cdot 10\mathrm{a}}{\mathrm{std}}$	250	148	102
1	$\mathfrak{sl}(5\mathrm{a}')\cdot 9\mathrm{a}'$	216	105	111
1	$\mathfrak{sl}(5\mathrm{a})\cdot 9\mathrm{a}'$	216	105	111
1	$\mathfrak{sl}(\mathrm{std}')\cdot 9\mathrm{a}'$	216	105	111
1	$\mathfrak{sl}(\mathrm{std})\cdot 9\mathrm{a}'$	216	105	111
1	$\mathfrak{sl}(5\mathrm{a}')\cdot 10\mathrm{a}$	240	124	116
1	$\mathfrak{sl}(5\mathrm{a})\cdot 10\mathrm{a}$	240	124	116
1	$\mathfrak{sl}(\mathrm{std}')\cdot 10\mathrm{a}'$	240	124	116
1	$\mathfrak{sl}(\mathrm{std})\cdot 10\mathrm{a}'$	240	124	116
1	$\frac{\mathrm{Sym}^2(9\mathrm{a}')}{5\mathrm{a}}$	225	105	120
1	$\frac{\mathrm{Sym}^2(9\mathrm{a}')}{\mathrm{std}}$	225	105	120
1	$\frac{\mathrm{Sym}^2(9\mathrm{a})}{5\mathrm{a}}$	225	105	120

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Sym}^2(9\mathrm{a})}{\mathrm{std}}$	225	105	120
1	$\frac{\mathrm{Sym}^2(10\mathrm{a}')}{5\mathrm{a}'}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a}')}{5\mathrm{a}}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a}')}{\mathrm{std}'}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a}')}{\mathrm{std}}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a})}{5\mathrm{a}'}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a})}{5\mathrm{a}}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a})}{\mathrm{std}'}$	275	124	151
1	$\frac{\mathrm{Sym}^2(10\mathrm{a})}{\mathrm{std}}$	275	124	151
1	$\frac{\mathrm{Alt}^2(9\mathrm{a}')}{10\mathrm{a}'}$	360	180	180
1	$\frac{\mathrm{Alt}^2(9\mathrm{a}')}{10\mathrm{a}}$	360	180	180
1	$\frac{\mathrm{Alt}^2(9\mathrm{a})}{10\mathrm{a}'}$	360	180	180
1	$\frac{\mathrm{Alt}^2(9\mathrm{a})}{10\mathrm{a}}$	360	180	180
1	$\frac{5\mathrm{a}' \cdot 9\mathrm{a}}{9\mathrm{a}'}$	405	185	220
1	$\frac{5\mathrm{a}' \cdot 9\mathrm{a}'}{9\mathrm{a}}$	405	185	220
1	$\frac{9\mathrm{a} \cdot 9\mathrm{a}'}{5\mathrm{a}'}$	405	185	220
1	$\frac{9\mathrm{a} \cdot 9\mathrm{a}'}{\mathrm{std}'}$	405	185	220
1	$\frac{\mathrm{std}' \cdot 9\mathrm{a}}{9\mathrm{a}'}$	405	185	220
1	$\frac{\mathrm{std}' \cdot 9\mathrm{a}'}{9\mathrm{a}}$	405	185	220

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(10\mathrm{a}')}{9\mathrm{a}}$	405	180	225
1	$\frac{\mathrm{Alt}^2(10\mathrm{a})}{9\mathrm{a}}$	405	180	225
1	$\frac{\mathrm{Alt}^2(9\mathrm{a}')}{16\mathrm{a}}$	576	336	240
1	$\frac{\mathrm{Alt}^2(9\mathrm{a})}{16\mathrm{a}}$	576	336	240
2	$\frac{\mathrm{Sym}^2(9\mathrm{a})}{9\mathrm{a}'}$	405	161	244
1	$\frac{5\mathrm{a}\cdot 10\mathrm{a}}{9\mathrm{a}'}$	450	204	246
1	$\frac{5\mathrm{a}\cdot 10\mathrm{a}'}{9\mathrm{a}}$	450	204	246
1	$\frac{5\mathrm{a}\cdot 9\mathrm{a}}{10\mathrm{a}'}$	450	204	246
1	$\frac{5\mathrm{a}\cdot 9\mathrm{a}'}{10\mathrm{a}}$	450	204	246
1	$\frac{5\mathrm{a}'\cdot 10\mathrm{a}}{9\mathrm{a}}$	450	204	246
1	$\frac{5\mathrm{a}'\cdot 10\mathrm{a}'}{9\mathrm{a}'}$	450	204	246
1	$\frac{5\mathrm{a}'\cdot 9\mathrm{a}}{10\mathrm{a}}$	450	204	246
1	$\frac{5\mathrm{a}'\cdot 9\mathrm{a}'}{10\mathrm{a}'}$	450	204	246
1	$\frac{9\mathrm{a}\cdot 10\mathrm{a}}{5\mathrm{a}'}$	450	204	246
1	$\frac{9\mathrm{a}\cdot 10\mathrm{a}}{\mathrm{std}}$	450	204	246
1	$\frac{9\mathrm{a}\cdot 10\mathrm{a}'}{5\mathrm{a}}$	450	204	246
1	$\frac{9\mathrm{a}\cdot 10\mathrm{a}'}{\mathrm{std}'}$	450	204	246
1	$\frac{9\mathrm{a}'\cdot 10\mathrm{a}}{5\mathrm{a}}$	450	204	246
1	$\frac{9\mathrm{a}'\cdot 10\mathrm{a}}{\mathrm{std}'}$	450	204	246

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{9a' \cdot 10a'}{5a'}$	450	204	246
1	$\frac{9a' \cdot 10a'}{std}$	450	204	246
1	$\frac{std \cdot 10a}{9a}$	450	204	246
1	$\frac{std \cdot 10a'}{9a'}$	450	204	246
1	$\frac{std \cdot 9a}{10a}$	450	204	246
1	$\frac{std \cdot 9a'}{10a'}$	450	204	246
1	$\frac{std' \cdot 10a}{9a'}$	450	204	246
1	$\frac{std' \cdot 10a'}{9a}$	450	204	246
1	$\frac{std' \cdot 9a}{10a'}$	450	204	246
1	$\frac{std' \cdot 9a'}{10a}$	450	204	246
1	$\frac{Alt^2(10a')}{10a}$	450	199	251
1	$\frac{Alt^2(10a)}{10a'}$	450	199	251
1	$\frac{10a \cdot 10a'}{5a'}$	500	223	277
1	$\frac{10a \cdot 10a'}{5a}$	500	223	277
1	$\frac{10a \cdot 10a'}{std'}$	500	223	277
1	$\frac{10a \cdot 10a'}{std}$	500	223	277
1	$\frac{5a \cdot 10a}{10a'}$	500	223	277
1	$\frac{5a \cdot 10a'}{10a}$	500	223	277
1	$\frac{5a' \cdot 10a}{10a'}$	500	223	277

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{5a' \cdot 10a'}{10a}$	500	223	277
1	$\frac{std \cdot 10a}{10a'}$	500	223	277
1	$\frac{std \cdot 10a'}{10a}$	500	223	277
1	$\frac{std' \cdot 10a}{10a'}$	500	223	277
1	$\frac{std' \cdot 10a'}{10a}$	500	223	277
1	$\mathfrak{sl}(9a') \cdot 5a$	400	105	295
1	$\mathfrak{sl}(9a') \cdot std$	400	105	295
1	$\mathfrak{sl}(9a) \cdot 5a$	400	105	295
1	$\mathfrak{sl}(9a) \cdot std$	400	105	295
2	$X(9a')$	396	81	315
2	$\frac{Sym^2(10a')}{9a'}$	495	180	315
2	$\frac{Sym^2(10a)}{9a'}$	495	180	315
1	$\frac{Alt^2(16a)}{5a'}$	600	280	320
1	$\frac{Alt^2(16a)}{std'}$	600	280	320
1	$Y(10a')$	440	100	340
1	$Y(10a)$	440	100	340
1	$\frac{5a \cdot 16a}{9a'}$	720	360	360
1	$\frac{5a \cdot 16a}{9a}$	720	360	360
1	$\frac{5a \cdot 9a}{16a}$	720	360	360

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{5a\cdot 9a'}{16a}$	720	360	360
1	$\frac{5a'\cdot 16a}{9a'}$	720	360	360
1	$\frac{5a'\cdot 16a}{9a}$	720	360	360
1	$\frac{5a'\cdot 9a}{16a}$	720	360	360
1	$\frac{5a'\cdot 9a'}{16a}$	720	360	360
1	$\frac{9a\cdot 16a}{5a'}$	720	360	360
1	$\frac{9a\cdot 16a}{5a}$	720	360	360
1	$\frac{9a\cdot 16a}{std'}$	720	360	360
1	$\frac{9a\cdot 16a}{std}$	720	360	360
1	$\frac{9a'\cdot 16a}{5a'}$	720	360	360
1	$\frac{9a'\cdot 16a}{5a}$	720	360	360
1	$\frac{9a'\cdot 16a}{std'}$	720	360	360
1	$\frac{9a'\cdot 16a}{std}$	720	360	360
1	$\frac{std\cdot 16a}{9a'}$	720	360	360
1	$\frac{std\cdot 16a}{9a}$	720	360	360
1	$\frac{std\cdot 9a}{16a}$	720	360	360
1	$\frac{std\cdot 9a'}{16a}$	720	360	360
1	$\frac{std'\cdot 16a}{9a'}$	720	360	360
1	$\frac{std'\cdot 16a}{9a}$	720	360	360

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{std}' \cdot 9\mathrm{a}}{16\mathrm{a}}$	720	360	360
1	$\frac{\mathrm{std}' \cdot 9\mathrm{a}'}{16\mathrm{a}}$	720	360	360
1	$\frac{\mathrm{Alt}^2(10\mathrm{a}')}{16\mathrm{a}}$	720	355	365
1	$\frac{\mathrm{Alt}^2(10\mathrm{a})}{16\mathrm{a}}$	720	355	365
1	$\mathfrak{sl}(10\mathrm{a}') \cdot 5\mathrm{a}$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}') \cdot 5\mathrm{a}'$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}') \cdot \mathrm{std}$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}') \cdot \mathrm{std}'$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}) \cdot 5\mathrm{a}$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}) \cdot 5\mathrm{a}'$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}) \cdot \mathrm{std}$	495	124	371
1	$\mathfrak{sl}(10\mathrm{a}) \cdot \mathrm{std}'$	495	124	371
1	$\frac{\mathrm{Sym}^2(9\mathrm{a}')}{16\mathrm{a}}$	720	336	384
1	$\frac{\mathrm{Sym}^2(9\mathrm{a})}{16\mathrm{a}}$	720	336	384
1	$\frac{\mathrm{Sym}^2(16\mathrm{a})}{5\mathrm{a}'}$	680	280	400
2	$\frac{\mathrm{Sym}^2(16\mathrm{a})}{5\mathrm{a}}$	680	280	400
1	$\frac{\mathrm{Sym}^2(16\mathrm{a})}{\mathrm{std}'}$	680	280	400
2	$\frac{\mathrm{Sym}^2(16\mathrm{a})}{\mathrm{std}}$	680	280	400
1	$\frac{10\mathrm{a} \cdot 16\mathrm{a}}{5\mathrm{a}'}$	800	379	421

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{10a \cdot 16a}{5a}$	800	379	421
1	$\frac{10a \cdot 16a}{std'}$	800	379	421
1	$\frac{10a \cdot 16a}{std}$	800	379	421
1	$\frac{10a' \cdot 16a}{5a'}$	800	379	421
1	$\frac{10a' \cdot 16a}{5a}$	800	379	421
1	$\frac{10a' \cdot 16a}{std'}$	800	379	421
1	$\frac{10a' \cdot 16a}{std}$	800	379	421
1	$\frac{5a \cdot 10a}{16a}$	800	379	421
1	$\frac{5a \cdot 10a'}{16a}$	800	379	421
1	$\frac{5a \cdot 16a}{10a'}$	800	379	421
1	$\frac{5a \cdot 16a}{10a}$	800	379	421
1	$\frac{5a' \cdot 10a}{16a}$	800	379	421
1	$\frac{5a' \cdot 10a'}{16a}$	800	379	421
1	$\frac{5a' \cdot 16a}{10a'}$	800	379	421
1	$\frac{5a' \cdot 16a}{10a}$	800	379	421
1	$\frac{std \cdot 10a}{16a}$	800	379	421
1	$\frac{std \cdot 10a'}{16a}$	800	379	421
1	$\frac{std \cdot 16a}{10a'}$	800	379	421
1	$\frac{std \cdot 16a}{10a}$	800	379	421

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{std}'\cdot 10\mathrm{a}}{16\mathrm{a}}$	800	379	421
1	$\frac{\mathrm{std}'\cdot 10\mathrm{a}'}{16\mathrm{a}}$	800	379	421
1	$\frac{\mathrm{std}'\cdot 16\mathrm{a}}{10\mathrm{a}'}$	800	379	421
1	$\frac{\mathrm{std}'\cdot 16\mathrm{a}}{10\mathrm{a}}$	800	379	421
1	$\frac{\mathrm{Sym}^2(10\mathrm{a}')}{16\mathrm{a}}$	880	355	525
1	$\frac{\mathrm{Sym}^2(10\mathrm{a})}{16\mathrm{a}}$	880	355	525
1	$\frac{9\mathrm{a}\cdot 10\mathrm{a}}{9\mathrm{a}'}$	810	260	550
1	$\frac{9\mathrm{a}\cdot 10\mathrm{a}'}{9\mathrm{a}'}$	810	260	550
1	$\frac{9\mathrm{a}\cdot 9\mathrm{a}'}{10\mathrm{a}'}$	810	260	550
1	$\frac{9\mathrm{a}\cdot 9\mathrm{a}'}{10\mathrm{a}}$	810	260	550
1	$\frac{9\mathrm{a}'\cdot 10\mathrm{a}}{9\mathrm{a}}$	810	260	550
1	$\frac{9\mathrm{a}'\cdot 10\mathrm{a}'}{9\mathrm{a}}$	810	260	550
2	$\mathfrak{sl}(9\mathrm{a})\cdot 9\mathrm{a}'$	720	161	559
1	$\mathfrak{sl}(9\mathrm{a}')\cdot 10\mathrm{a}$	800	180	620
1	$\mathfrak{sl}(9\mathrm{a}')\cdot 10\mathrm{a}'$	800	180	620
1	$\mathfrak{sl}(9\mathrm{a})\cdot 10\mathrm{a}$	800	180	620
1	$\mathfrak{sl}(9\mathrm{a})\cdot 10\mathrm{a}'$	800	180	620
1	$\frac{10\mathrm{a}\cdot 10\mathrm{a}'}{9\mathrm{a}'}$	900	279	621
2	$\frac{10\mathrm{a}\cdot 10\mathrm{a}'}{9\mathrm{a}}$	900	279	621

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
2	$\frac{9a\cdot 10a}{10a'}$	900	279	621
2	$\frac{9a\cdot 10a'}{10a}$	900	279	621
1	$\frac{9a'\cdot 10a}{10a'}$	900	279	621
1	$\frac{9a'\cdot 10a'}{10a}$	900	279	621
1	$\mathfrak{sl}(10a')\cdot 9a$	891	180	711
2	$\mathfrak{sl}(10a')\cdot 9a'$	891	180	711
1	$\mathfrak{sl}(10a)\cdot 9a$	891	180	711
2	$\mathfrak{sl}(10a)\cdot 9a'$	891	180	711
2	$\frac{\mathrm{Alt}^2(16a)}{9a}$	1080	336	744
1	$\mathfrak{sl}(10a')\cdot 10a$	990	199	791
1	$\mathfrak{sl}(10a)\cdot 10a'$	990	199	791
3	$\frac{\mathrm{Alt}^2(16a)}{10a'}$	1200	355	845
3	$\frac{\mathrm{Alt}^2(16a)}{10a}$	1200	355	845
2	$\frac{9a\cdot 16a}{9a'}$	1296	416	880
2	$\frac{9a\cdot 9a'}{16a}$	1296	416	880
2	$\frac{9a'\cdot 16a}{9a}$	1296	416	880
3	$\frac{\mathrm{Sym}^2(16a)}{9a'}$	1224	336	888
1	$\frac{\mathrm{Sym}^2(16a)}{9a}$	1224	336	888
2	$\mathfrak{sl}(9a')\cdot 16a$	1280	336	944

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
2	$\mathfrak{sl}(9\text{a})\cdot 16\text{a}$	1280	336	944
2	$\mathfrak{sl}(16\text{a})\cdot 5\text{a}$	1275	280	995
2	$\mathfrak{sl}(16\text{a})\cdot 5\text{a}'$	1275	280	995
2	$\mathfrak{sl}(16\text{a})\cdot \text{std}$	1275	280	995
2	$\mathfrak{sl}(16\text{a})\cdot \text{std}'$	1275	280	995
1	$\frac{\text{Sym}^2(16\text{a})}{10\text{a}'}$	1360	355	1005
1	$\frac{\text{Sym}^2(16\text{a})}{10\text{a}}$	1360	355	1005
2	$\frac{10\text{a}\cdot 16\text{a}}{9\text{a}'}$	1440	435	1005
2	$\frac{10\text{a}\cdot 16\text{a}}{9\text{a}}$	1440	435	1005
2	$\frac{10\text{a}'\cdot 16\text{a}}{9\text{a}'}$	1440	435	1005
2	$\frac{10\text{a}'\cdot 16\text{a}}{9\text{a}}$	1440	435	1005
2	$\frac{9\text{a}\cdot 10\text{a}}{16\text{a}}$	1440	435	1005
2	$\frac{9\text{a}\cdot 10\text{a}'}{16\text{a}}$	1440	435	1005
2	$\frac{9\text{a}\cdot 16\text{a}}{10\text{a}'}$	1440	435	1005
2	$\frac{9\text{a}\cdot 16\text{a}}{10\text{a}}$	1440	435	1005
2	$\frac{9\text{a}'\cdot 10\text{a}}{16\text{a}}$	1440	435	1005
2	$\frac{9\text{a}'\cdot 10\text{a}'}{16\text{a}}$	1440	435	1005
2	$\frac{9\text{a}'\cdot 16\text{a}}{10\text{a}'}$	1440	435	1005
2	$\frac{9\text{a}'\cdot 16\text{a}}{10\text{a}}$	1440	435	1005

Table 6.5.2: Nontrivial summands for the Symmetric Group S_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
2	$\frac{10\mathrm{a}\cdot 10\mathrm{a}'}{16\mathrm{a}}$	1600	454	1146
2	$\frac{10\mathrm{a}\cdot 16\mathrm{a}}{10\mathrm{a}'}$	1600	454	1146
2	$\frac{10\mathrm{a}'\cdot 16\mathrm{a}}{10\mathrm{a}}$	1600	454	1146
2	$\mathfrak{sl}(10\mathrm{a}')\cdot 16\mathrm{a}$	1584	355	1229
2	$\mathfrak{sl}(10\mathrm{a})\cdot 16\mathrm{a}$	1584	355	1229
2	$\mathrm{Y}(16\mathrm{a})$	1904	256	1648
3	$\mathrm{X}(16\mathrm{a})$	2160	256	1904
3	$\mathfrak{sl}(16\mathrm{a})\cdot 9\mathrm{a}$	2295	336	1959
3	$\mathfrak{sl}(16\mathrm{a})\cdot 9\mathrm{a}'$	2295	336	1959
4	$\mathfrak{sl}(16\mathrm{a})\cdot 10\mathrm{a}$	2550	355	2195
4	$\mathfrak{sl}(16\mathrm{a})\cdot 10\mathrm{a}'$	2550	355	2195

6.6 Quaternion Group Q_8

Order: 8

Conjugacy classes: $\mathbf{1} = \{1\}$, $\mathbf{2} = \{-1\}$, $\mathbf{3} = \{\pm i\}$, $\mathbf{4} = \{\pm j\}$, $\mathbf{5} = \{\pm k\}$

Table 6.6.1: Irreducible characters for the Quaternion Group Q_8

	1	**2**	**3**	**4**	**5**
Size	1	1	2	2	2
triv	1	1	1	1	1
sgni	1	1	1	−1	−1
sgnj	1	1	−1	1	−1
sgnk	1	1	−1	−1	1
std	2	−2	0	0	0

Table 6.6.2: Nontrivial summands for the Quaternion Group Q_8

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Alt}^2(\mathrm{std})$	1	4	−3
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{sgni}}$	3	4	−1
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{sgnj}}$	3	4	−1
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{sgnk}}$	3	4	−1
1	$\mathfrak{sl}(\mathrm{std}) \cdot \mathrm{sgni}$	3	4	−1
1	$\mathfrak{sl}(\mathrm{std}) \cdot \mathrm{sgnj}$	3	4	−1
1	$\mathfrak{sl}(\mathrm{std}) \cdot \mathrm{sgnk}$	3	4	−1
1	$\mathrm{Sym}^2(\mathrm{sgni})$	1	1	0
1	$\mathrm{Sym}^2(\mathrm{sgnj})$	1	1	0
1	$\mathrm{Sym}^2(\mathrm{sgnk})$	1	1	0
1	$\frac{\mathrm{sgni} \cdot \mathrm{sgnj}}{\mathrm{sgnk}}$	1	1	0
1	$\frac{\mathrm{sgni} \cdot \mathrm{sgnk}}{\mathrm{sgnj}}$	1	1	0

Table 6.6.2: Nontrivial summands for the Quaternion Group Q_8

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\dfrac{\mathrm{sgnj}\cdot\mathrm{sgnk}}{\mathrm{sgni}}$	1	1	0

6.7 Quaternion Group Q_{12}

Order: 12

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{a, a^{-1}\}$, $\mathbf{3} = \{a^2, a^4\}$, $\mathbf{4} = \{a^3\}$, $\mathbf{5} = \{x, a^2x, a^4x\}$, $\mathbf{6} = \{ax, a^3x, a^5x\}$

Table 6.7.1: Irreducible characters for the Quaternion Group Q_{12}

	1	**2**	**3**	**4**	**5**	**6**
Size	1	2	2	1	3	3
triv	1	1	1	1	1	1
sgn1	1	1	1	1	-1	-1
rho1	1	-1	1	-1	ζ_4	$-\zeta_4$
rho2	1	-1	1	-1	$-\zeta_4$	ζ_4
std1	2	1	-1	-2	0	0
std2	2	-1	-1	2	0	0

Table 6.7.2: Nontrivial summands for the Quaternion Group Q_{12}

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Alt}^2(\mathrm{std1})$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std2})}{\mathrm{sgn1}}$	1	4	-3
1	$\frac{\mathrm{rho1} \cdot \mathrm{std1}}{\mathrm{std2}}$	4	7	-3
1	$\frac{\mathrm{rho1} \cdot \mathrm{std2}}{\mathrm{std1}}$	4	7	-3
1	$\frac{\mathrm{rho2} \cdot \mathrm{std1}}{\mathrm{std2}}$	4	7	-3
1	$\frac{\mathrm{rho2} \cdot \mathrm{std2}}{\mathrm{std1}}$	4	7	-3
1	$\frac{\mathrm{std1} \cdot \mathrm{std2}}{\mathrm{rho1}}$	4	7	-3
1	$\frac{\mathrm{std1} \cdot \mathrm{std2}}{\mathrm{rho2}}$	4	7	-3
1	$\frac{\mathrm{Sym}^2(\mathrm{std1})}{\mathrm{sgn1}}$	3	4	-1
1	$\mathrm{Sym}^2(\mathrm{std2})$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std1}) \cdot \mathrm{sgn1}$	3	4	-1

Table 6.7.2: Nontrivial summands for the Quaternion Group Q_{12}

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\mathfrak{sl}(\text{std2})\cdot\text{sgn1}$	3	4	-1
1	$\dfrac{\text{Sym}^2(\text{std1})}{\text{std2}}$	6	7	-1
1	$\mathfrak{sl}(\text{std1})\cdot\text{std2}$	6	7	-1
1	$\dfrac{\text{Sym}^2(\text{rho1})}{\text{sgn1}}$	1	1	0
1	$\dfrac{\text{Sym}^2(\text{rho2})}{\text{sgn1}}$	1	1	0
1	$\text{Sym}^2(\text{sgn1})$	1	1	0
1	$\text{rho1}\cdot\text{rho2}$	1	1	0
1	$\dfrac{\text{sgn1}\cdot\text{rho1}}{\text{rho2}}$	1	1	0
1	$\dfrac{\text{sgn1}\cdot\text{rho2}}{\text{rho1}}$	1	1	0
1	X(std2)	4	4	0

6.8 Alternating Group A_4

Order: 12

Conjugacy classes: **1** $= ([1,1,1,1],0)$, **2** $= ([1,3],1)$, **3** $= ([1,3],-1)$, **4** $= ([2,2],0)$

Table 6.8.1: Irreducible characters for the Alternating Group A_4

	1	**2**	**3**	**4**
Size	1	4	4	3
triv	1	1	1	1
rho1	1	ζ_3	$-1-\zeta_3$	1
rho2	1	$-1-\zeta_3$	ζ_3	1
std	3	0	0	-1

Table 6.8.2: Nontrivial summands for the Alternating Group A_4

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Sym}^2(\mathrm{std})$	6	9	-3
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{rho1}}$	6	9	-3
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{rho2}}$	6	9	-3
1	$\mathrm{Y}(\mathrm{std})$	6	9	-3
1	$\mathfrak{sl}(\mathrm{std})\cdot\mathrm{rho1}$	8	9	-1
1	$\mathfrak{sl}(\mathrm{std})\cdot\mathrm{rho2}$	8	9	-1
1	$\frac{\mathrm{Sym}^2(\mathrm{rho1})}{\mathrm{rho2}}$	1	1	0
1	$\frac{\mathrm{Sym}^2(\mathrm{rho2})}{\mathrm{rho1}}$	1	1	0
1	$\mathrm{rho1}\cdot\mathrm{rho2}$	1	1	0
1	$\mathrm{X}(\mathrm{std})$	15	9	6

6.9 Alternating Group A_5

Order: 60

Conjugacy classes: **1** = $([1,1,1,1,1],0)$, **2** = $([1,1,3],0)$, **3** = $([1,2,2],0)$, **4** = $([5],1)$, **5** = $([5],-1)$

Table 6.9.1: Irreducible characters for the Alternating Group A_5

	1	**2**	**3**	**4**	**5**
Size	1	20	15	12	12
triv	1	1	1	1	1
e1	3	0	-1	$-\zeta_5^2-\zeta_5^3$	$1+\zeta_5^2+\zeta_5^3$
e2	3	0	-1	$1+\zeta_5^2+\zeta_5^3$	$-\zeta_5^2-\zeta_5^3$
std	4	1	0	-1	-1
f	5	-1	1	0	0

Table 6.9.2: Nontrivial summands for the Alternating Group A_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\mathrm{Sym}^2(\mathrm{f})$	15	25	-10
1	$\mathrm{Sym}^2(\mathrm{std})$	10	16	-6
1	$\frac{\mathrm{Alt}^2(\mathrm{std})}{\mathrm{e1}}$	18	24	-6
1	$\frac{\mathrm{Alt}^2(\mathrm{std})}{\mathrm{e2}}$	18	24	-6
1	$\mathrm{Sym}^2(\mathrm{e1})$	6	9	-3
1	$\mathrm{Sym}^2(\mathrm{e2})$	6	9	-3
1	$\mathrm{Y}(\mathrm{e1})$	6	9	-3
1	$\mathrm{Y}(\mathrm{e2})$	6	9	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{f})}{\mathrm{e1}}$	30	33	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{f})}{\mathrm{e2}}$	30	33	-3
1	$\frac{\mathrm{Sym}^2(\mathrm{e1})}{\mathrm{f}}$	30	33	-3
1	$\frac{\mathrm{Sym}^2(\mathrm{e2})}{\mathrm{f}}$	30	33	-3

Table 6.9.2: Nontrivial summands for the Alternating Group A_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(\mathrm{f})}{\mathrm{std}}$	40	40	0
1	$\frac{\mathrm{e1}\cdot\mathrm{e2}}{\mathrm{std}}$	36	32	4
1	$\frac{\mathrm{e1}\cdot\mathrm{std}}{\mathrm{e2}}$	36	32	4
1	$\frac{\mathrm{e2}\cdot\mathrm{std}}{\mathrm{e1}}$	36	32	4
1	$\frac{\mathrm{e1}\cdot\mathrm{e2}}{\mathrm{f}}$	45	41	4
1	$\frac{\mathrm{e1}\cdot\mathrm{f}}{\mathrm{e2}}$	45	41	4
1	$\frac{\mathrm{e2}\cdot\mathrm{f}}{\mathrm{e1}}$	45	41	4
1	$\mathfrak{sl}(\mathrm{e1})\cdot\mathrm{f}$	40	33	7
1	$\mathfrak{sl}(\mathrm{e2})\cdot\mathrm{f}$	40	33	7
1	$\frac{\mathrm{Sym}^2(\mathrm{std})}{\mathrm{f}}$	50	40	10
1	$\frac{\mathrm{e1}\cdot\mathrm{f}}{\mathrm{std}}$	60	48	12
1	$\frac{\mathrm{e1}\cdot\mathrm{std}}{\mathrm{f}}$	60	48	12
1	$\frac{\mathrm{e2}\cdot\mathrm{f}}{\mathrm{std}}$	60	48	12
1	$\frac{\mathrm{e2}\cdot\mathrm{std}}{\mathrm{f}}$	60	48	12
1	$\frac{\mathrm{std}\cdot\mathrm{f}}{\mathrm{e1}}$	60	48	12
1	$\frac{\mathrm{std}\cdot\mathrm{f}}{\mathrm{e2}}$	60	48	12
1	$\mathrm{X}(\mathrm{std})$	36	16	20
1	$\frac{\mathrm{Sym}^2(\mathrm{f})}{\mathrm{std}}$	60	40	20
1	$\mathfrak{sl}(\mathrm{std})\cdot\mathrm{e1}$	45	24	21

Table 6.9.2: Nontrivial summands for the Alternating Group A_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathfrak{sl}(\text{std}) \cdot \text{e2}$	45	24	21
1	$\mathfrak{sl}(\text{std}) \cdot \text{f}$	75	40	35
1	$\mathfrak{sl}(\text{f}) \cdot \text{e1}$	72	33	39
1	$\mathfrak{sl}(\text{f}) \cdot \text{e2}$	72	33	39
2	X(f)	70	25	45
2	$\mathfrak{sl}(\text{f}) \cdot \text{std}$	96	40	56

6.10 Dihedral Group D_4

Order: 8

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2\}$, $\mathbf{4} = \{\sigma\tau^{\text{even}}\}$, $\mathbf{5} = \{\sigma\tau^{\text{odd}}\}$

Table 6.10.1: Irreducible characters for the Dihedral Group D_4

	1	**2**	**3**	**4**	**5**
Size	1	2	1	2	2
triv	1	1	1	1	1
sign	1	1	1	−1	−1
e1	1	−1	1	1	−1
e2	1	−1	1	−1	1
std1	2	0	−2	0	0

Table 6.10.2: Nontrivial summands for the Dihedral Group D_4

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{Alt}^2(\text{std1})}{\text{sign}}$	1	4	−3
1	$\text{Sym}^2(\text{std1})$	3	4	−1
1	$\frac{\text{Sym}^2(\text{std1})}{\text{e1}}$	3	4	−1
1	$\frac{\text{Sym}^2(\text{std1})}{\text{e2}}$	3	4	−1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{e1}$	3	4	−1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{e2}$	3	4	−1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{sign}$	3	4	−1
1	$\text{Sym}^2(\text{e1})$	1	1	0
1	$\text{Sym}^2(\text{e2})$	1	1	0
1	$\text{Sym}^2(\text{sign})$	1	1	0
1	$\frac{\text{e1} \cdot \text{e2}}{\text{sign}}$	1	1	0
1	$\frac{\text{sign} \cdot \text{e1}}{\text{e2}}$	1	1	0

Table 6.10.2: Nontrivial summands for the Dihedral Group D_4

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{sign} \cdot \text{e2}}{\text{e1}}$	1	1	0

6.11 Dihedral Group D_5

Order: 10

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2, \tau^{-2}\}$, $\mathbf{4} = \{\sigma\tau^i\}$

Table 6.11.1: Irreducible characters for the Dihedral Group D_5

	1	**2**	**3**	**4**
Size	1	2	2	5
triv	1	1	1	1
sign	1	1	1	-1
std1	2	$-1-\zeta_5^2-\zeta_5^3$	$\zeta_5^2+\zeta_5^3$	0
std2	2	$\zeta_5^2+\zeta_5^3$	$-1-\zeta_5^2-\zeta_5^3$	0

Table 6.11.2: Nontrivial summands for the Dihedral Group D_5

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(\mathrm{std1})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std2})}{\mathrm{sign}}$	1	4	-3
1	$\mathrm{Sym}^2(\mathrm{std1})$	3	4	-1
1	$\mathrm{Sym}^2(\mathrm{std2})$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std1})\cdot\mathrm{sign}$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std2})\cdot\mathrm{sign}$	3	4	-1
1	$\frac{\mathrm{Sym}^2(\mathrm{std1})}{\mathrm{std2}}$	6	7	-1
1	$\frac{\mathrm{Sym}^2(\mathrm{std2})}{\mathrm{std1}}$	6	7	-1
1	$\mathfrak{sl}(\mathrm{std1})\cdot\mathrm{std2}$	6	7	-1
1	$\mathfrak{sl}(\mathrm{std2})\cdot\mathrm{std1}$	6	7	-1
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0

6.12 Dihedral Group D_6

Order: 12

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2, \tau^{-2}\}$, $\mathbf{4} = \{\tau^3\}$, $\mathbf{5} = \{\sigma\tau^{\text{even}}\}$, $\mathbf{6} = \{\sigma\tau^{\text{odd}}\}$

Table 6.12.1: Irreducible characters for the Dihedral Group D_6

	1	**2**	**3**	**4**	**5**	**6**
Size	1	2	2	1	3	3
triv	1	1	1	1	1	1
sign	1	1	1	1	−1	−1
e1	1	−1	1	−1	1	−1
e2	1	−1	1	−1	−1	1
std1	2	1	−1	−2	0	0
std2	2	−1	−1	2	0	0

Table 6.12.2: Nontrivial summands for the Dihedral Group D_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{Alt}^2(\text{std1})}{\text{sign}}$	1	4	−3
1	$\frac{\text{Alt}^2(\text{std2})}{\text{sign}}$	1	4	−3
1	$\frac{\text{e1} \cdot \text{std1}}{\text{std2}}$	4	7	−3
1	$\frac{\text{e1} \cdot \text{std2}}{\text{std1}}$	4	7	−3
1	$\frac{\text{e2} \cdot \text{std1}}{\text{std2}}$	4	7	−3
1	$\frac{\text{e2} \cdot \text{std2}}{\text{std1}}$	4	7	−3
1	$\frac{\text{std1} \cdot \text{std2}}{\text{e1}}$	4	7	−3
1	$\frac{\text{std1} \cdot \text{std2}}{\text{e2}}$	4	7	−3
1	$\text{Sym}^2(\text{std1})$	3	4	−1
1	$\text{Sym}^2(\text{std2})$	3	4	−1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{sign}$	3	4	−1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{sign}$	3	4	−1

Table 6.12.2: Nontrivial summands for the Dihedral Group D_6

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Sym}^2(\mathrm{std1})}{\mathrm{std2}}$	6	7	-1
1	$\mathfrak{sl}(\mathrm{std1}) \cdot \mathrm{std2}$	6	7	-1
1	$\mathrm{Sym}^2(\mathrm{e1})$	1	1	0
1	$\mathrm{Sym}^2(\mathrm{e2})$	1	1	0
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0
1	$\frac{\mathrm{e1} \cdot \mathrm{e2}}{\mathrm{sign}}$	1	1	0
1	$\frac{\mathrm{sign} \cdot \mathrm{e1}}{\mathrm{e2}}$	1	1	0
1	$\frac{\mathrm{sign} \cdot \mathrm{e2}}{\mathrm{e1}}$	1	1	0
1	$\mathrm{X}(\mathrm{std2})$	4	4	0

6.13 Dihedral Group D_7

Order: 14

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2, \tau^{-2}\}$, $\mathbf{4} = \{\tau^3, \tau^{-3}\}$, $\mathbf{5} = \{\sigma\tau^i\}$

Table 6.13.1: Irreducible characters for the Dihedral Group D_7

	1	**2**	**3**	**4**	**5**
Size	1	2	2	2	7
triv	1	1	1	1	1
sign	1	1	1	1	-1
std1	2	$-1-\zeta_7^2-\zeta_7^3-\zeta_7^4-\zeta_7^5$	$\zeta_7^2+\zeta_7^5$	$\zeta_7^3+\zeta_7^4$	0
std2	2	$\zeta_7^2+\zeta_7^5$	$\zeta_7^3+\zeta_7^4$	$-1-\zeta_7^2-\zeta_7^3-\zeta_7^4-\zeta_7^5$	0
std3	2	$\zeta_7^3+\zeta_7^4$	$-1-\zeta_7^2-\zeta_7^3-\zeta_7^4-\zeta_7^5$	$\zeta_7^2+\zeta_7^5$	0

Table 6.13.2: Nontrivial summands for the Dihedral Group D_7

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(\mathrm{std1})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std2})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std3})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{std1}\cdot\mathrm{std2}}{\mathrm{std3}}$	8	10	-2
1	$\frac{\mathrm{std1}\cdot\mathrm{std3}}{\mathrm{std2}}$	8	10	-2
1	$\frac{\mathrm{std2}\cdot\mathrm{std3}}{\mathrm{std1}}$	8	10	-2
1	$\mathrm{Sym}^2(\mathrm{std1})$	3	4	-1
1	$\mathrm{Sym}^2(\mathrm{std2})$	3	4	-1
1	$\mathrm{Sym}^2(\mathrm{std3})$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std1})\cdot\mathrm{sign}$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std2})\cdot\mathrm{sign}$	3	4	-1
1	$\mathfrak{sl}(\mathrm{std3})\cdot\mathrm{sign}$	3	4	-1

Table 6.13.2: Nontrivial summands for the Dihedral Group D_7

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Sym}^2(\mathrm{std1})}{\mathrm{std2}}$	6	7	-1
1	$\frac{\mathrm{Sym}^2(\mathrm{std2})}{\mathrm{std3}}$	6	7	-1
1	$\frac{\mathrm{Sym}^2(\mathrm{std3})}{\mathrm{std1}}$	6	7	-1
1	$\mathfrak{sl}(\mathrm{std1}) \cdot \mathrm{std2}$	6	7	-1
1	$\mathfrak{sl}(\mathrm{std2}) \cdot \mathrm{std3}$	6	7	-1
1	$\mathfrak{sl}(\mathrm{std3}) \cdot \mathrm{std1}$	6	7	-1
1	$\mathrm{Sym}^2(\mathrm{sign})$	1	1	0

6.14 Dihedral Group D_8

Order: 16

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2, \tau^{-2}\}$, $\mathbf{4} = \{\tau^3, \tau^{-3}\}$, $\mathbf{5} = \{\tau^4\}$, $\mathbf{6} = \{\sigma\tau^{\text{even}}\}$, $\mathbf{7} = \{\sigma\tau^{\text{odd}}\}$

Table 6.14.1: Irreducible characters for the Dihedral Group D_8

	1	**2**	**3**	**4**	**5**	**6**	**7**
Size	1	2	2	2	1	4	4
triv	1	1	1	1	1	1	1
sign	1	1	1	1	1	-1	-1
e1	1	-1	1	-1	1	1	-1
e2	1	-1	1	-1	1	-1	1
std1	2	$\zeta_8 - \zeta_8^3$	0	$-\zeta_8 + \zeta_8^3$	-2	0	0
std2	2	0	-2	0	2	0	0
std3	2	$-\zeta_8 + \zeta_8^3$	0	$\zeta_8 - \zeta_8^3$	-2	0	0

Table 6.14.2: Nontrivial summands for the Dihedral Group D_8

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{Alt}^2(\text{std1})}{\text{sign}}$	1	4	-3
1	$\frac{\text{Alt}^2(\text{std2})}{\text{sign}}$	1	4	-3
1	$\frac{\text{Alt}^2(\text{std3})}{\text{sign}}$	1	4	-3
1	$\frac{\text{e1} \cdot \text{std1}}{\text{std3}}$	4	7	-3
1	$\frac{\text{e1} \cdot \text{std3}}{\text{std1}}$	4	7	-3
1	$\frac{\text{e2} \cdot \text{std1}}{\text{std3}}$	4	7	-3
1	$\frac{\text{e2} \cdot \text{std3}}{\text{std1}}$	4	7	-3
1	$\frac{\text{std1} \cdot \text{std3}}{\text{e1}}$	4	7	-3
1	$\frac{\text{std1} \cdot \text{std3}}{\text{e2}}$	4	7	-3
1	$\frac{\text{std1} \cdot \text{std2}}{\text{std3}}$	8	10	-2
1	$\frac{\text{std1} \cdot \text{std3}}{\text{std2}}$	8	10	-2

Table 6.14.2: Nontrivial summands for the Dihedral Group D_8

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{std2} \cdot \text{std3}}{\text{std1}}$	8	10	-2
1	$\text{Sym}^2(\text{std1})$	3	4	-1
1	$\text{Sym}^2(\text{std2})$	3	4	-1
1	$\frac{\text{Sym}^2(\text{std2})}{\text{e1}}$	3	4	-1
1	$\frac{\text{Sym}^2(\text{std2})}{\text{e2}}$	3	4	-1
1	$\text{Sym}^2(\text{std3})$	3	4	-1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{e1}$	3	4	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{e2}$	3	4	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std3}) \cdot \text{sign}$	3	4	-1
1	$\frac{\text{Sym}^2(\text{std1})}{\text{std2}}$	6	7	-1
1	$\frac{\text{Sym}^2(\text{std3})}{\text{std2}}$	6	7	-1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{std2}$	6	7	-1
1	$\mathfrak{sl}(\text{std3}) \cdot \text{std2}$	6	7	-1
1	$\text{Sym}^2(\text{e1})$	1	1	0
1	$\text{Sym}^2(\text{e2})$	1	1	0
1	$\text{Sym}^2(\text{sign})$	1	1	0
1	$\frac{\text{e1} \cdot \text{e2}}{\text{sign}}$	1	1	0

Table 6.14.2: Nontrivial summands for the Dihedral Group D_8

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{sign} \cdot \text{e1}}{\text{e2}}$	1	1	0
1	$\frac{\text{sign} \cdot \text{e2}}{\text{e1}}$	1	1	0

6.15 Dihedral Group D_9

Order: 18

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2, \tau^{-2}\}$, $\mathbf{4} = \{\tau^3, \tau^{-3}\}$, $\mathbf{5} = \{\tau^4, \tau^{-4}\}$, $\mathbf{6} = \{\sigma\tau^i\}$

Table 6.15.1: Irreducible characters for the Dihedral Group D_9

	1	**2**	**3**	**4**	**5**	**6**
Size	1	2	2	2	2	9
triv	1	1	1	1	1	1
sign	1	1	1	1	1	-1
std1	2	$\zeta_9 - \zeta_9^2 - \zeta_9^5$	$-\zeta_9 + \zeta_9^2 - \zeta_9^4$	-1	$\zeta_9^4 + \zeta_9^5$	0
std2	2	$-\zeta_9 + \zeta_9^2 - \zeta_9^4$	$\zeta_9^4 + \zeta_9^5$	-1	$\zeta_9 - \zeta_9^2 - \zeta_9^5$	0
std3	2	-1	-1	2	-1	0
std4	2	$\zeta_9^4 + \zeta_9^5$	$\zeta_9 - \zeta_9^2 - \zeta_9^5$	-1	$-\zeta_9 + \zeta_9^2 - \zeta_9^4$	0

Table 6.15.2: Nontrivial summands for the Dihedral Group D_9

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\mathrm{Alt}^2(\mathrm{std1})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std2})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std3})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{Alt}^2(\mathrm{std4})}{\mathrm{sign}}$	1	4	-3
1	$\frac{\mathrm{std1} \cdot \mathrm{std2}}{\mathrm{std3}}$	8	10	-2
1	$\frac{\mathrm{std1} \cdot \mathrm{std3}}{\mathrm{std2}}$	8	10	-2
1	$\frac{\mathrm{std1} \cdot \mathrm{std3}}{\mathrm{std4}}$	8	10	-2
1	$\frac{\mathrm{std1} \cdot \mathrm{std4}}{\mathrm{std3}}$	8	10	-2
1	$\frac{\mathrm{std2} \cdot \mathrm{std3}}{\mathrm{std1}}$	8	10	-2
1	$\frac{\mathrm{std2} \cdot \mathrm{std3}}{\mathrm{std4}}$	8	10	-2
1	$\frac{\mathrm{std2} \cdot \mathrm{std4}}{\mathrm{std3}}$	8	10	-2
1	$\frac{\mathrm{std3} \cdot \mathrm{std4}}{\mathrm{std1}}$	8	10	-2

Table 6.15.2: Nontrivial summands for the Dihedral Group D_9

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{std3} \cdot \text{std4}}{\text{std2}}$	8	10	-2
1	$\text{Sym}^2(\text{std1})$	3	4	-1
1	$\text{Sym}^2(\text{std2})$	3	4	-1
1	$\text{Sym}^2(\text{std3})$	3	4	-1
1	$\text{Sym}^2(\text{std4})$	3	4	-1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std3}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std4}) \cdot \text{sign}$	3	4	-1
1	$\frac{\text{Sym}^2(\text{std1})}{\text{std2}}$	6	7	-1
1	$\frac{\text{Sym}^2(\text{std2})}{\text{std4}}$	6	7	-1
1	$\frac{\text{Sym}^2(\text{std4})}{\text{std1}}$	6	7	-1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{std2}$	6	7	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{std4}$	6	7	-1
1	$\mathfrak{sl}(\text{std4}) \cdot \text{std1}$	6	7	-1
1	$\text{Sym}^2(\text{sign})$	1	1	0
1	X(std3)	4	4	0

6.16 Dihedral Group D_{10}

Order: 20

Conjugacy classes: $\mathbf{1} = \{e\}$, $\mathbf{2} = \{\tau^1, \tau^{-1}\}$, $\mathbf{3} = \{\tau^2, \tau^{-2}\}$, $\mathbf{4} = \{\tau^3, \tau^{-3}\}$, $\mathbf{5} = \{\tau^4, \tau^{-4}\}$, $\mathbf{6} = \{\tau^5\}$, $\mathbf{7} = \{\sigma\tau^{\text{even}}\}$, $\mathbf{8} = \{\sigma\tau^{\text{odd}}\}$

Table 6.16.1: Irreducible characters for the Dihedral Group D_{10}

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Size	1	2	2	2	2	1	5	5
triv	1	1	1	1	1	1	1	1
sign	1	1	1	1	1	1	-1	-1
e1	1	-1	1	-1	1	-1	1	-1
e2	1	-1	1	-1	1	-1	-1	1
std1	2	$1+\zeta_{10}^2-\zeta_{10}^3$	$\zeta_{10}^2-\zeta_{10}^3$	$-\zeta_{10}^2+\zeta_{10}^3$	$-1-\zeta_{10}^2+\zeta_{10}^3$	-2	0	0
std2	2	$\zeta_{10}^2-\zeta_{10}^3$	$-1-\zeta_{10}^2+\zeta_{10}^3$	$-1-\zeta_{10}^2+\zeta_{10}^3$	$\zeta_{10}^2-\zeta_{10}^3$	2	0	0
std3	2	$-\zeta_{10}^2+\zeta_{10}^3$	$-1-\zeta_{10}^2+\zeta_{10}^3$	$1+\zeta_{10}^2-\zeta_{10}^3$	$\zeta_{10}^2-\zeta_{10}^3$	-2	0	0
std4	2	$-1-\zeta_{10}^2+\zeta_{10}^3$	$\zeta_{10}^2-\zeta_{10}^3$	$\zeta_{10}^2-\zeta_{10}^3$	$-1-\zeta_{10}^2+\zeta_{10}^3$	2	0	0

Table 6.16.2: Nontrivial summands for the Dihedral Group D_{10}

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L)-\dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{Alt}^2(\text{std1})}{\text{sign}}$	1	4	-3
1	$\frac{\text{Alt}^2(\text{std2})}{\text{sign}}$	1	4	-3
1	$\frac{\text{Alt}^2(\text{std3})}{\text{sign}}$	1	4	-3
1	$\frac{\text{Alt}^2(\text{std4})}{\text{sign}}$	1	4	-3
1	$\frac{\text{e1}\cdot\text{std1}}{\text{std4}}$	4	7	-3
1	$\frac{\text{e1}\cdot\text{std2}}{\text{std3}}$	4	7	-3
1	$\frac{\text{e1}\cdot\text{std3}}{\text{std2}}$	4	7	-3
1	$\frac{\text{e1}\cdot\text{std4}}{\text{std1}}$	4	7	-3
1	$\frac{\text{e2}\cdot\text{std1}}{\text{std4}}$	4	7	-3
1	$\frac{\text{e2}\cdot\text{std2}}{\text{std3}}$	4	7	-3

Table 6.16.2: Nontrivial summands for the Dihedral Group D_{10}

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\frac{\text{e2} \cdot \text{std3}}{\text{std2}}$	4	7	-3
1	$\frac{\text{e2} \cdot \text{std4}}{\text{std1}}$	4	7	-3
1	$\frac{\text{std1} \cdot \text{std4}}{\text{e1}}$	4	7	-3
1	$\frac{\text{std1} \cdot \text{std4}}{\text{e2}}$	4	7	-3
1	$\frac{\text{std2} \cdot \text{std3}}{\text{e1}}$	4	7	-3
1	$\frac{\text{std2} \cdot \text{std3}}{\text{e2}}$	4	7	-3
1	$\frac{\text{std1} \cdot \text{std2}}{\text{std3}}$	8	10	-2
1	$\frac{\text{std1} \cdot \text{std3}}{\text{std2}}$	8	10	-2
1	$\frac{\text{std1} \cdot \text{std3}}{\text{std4}}$	8	10	-2
1	$\frac{\text{std1} \cdot \text{std4}}{\text{std3}}$	8	10	-2
1	$\frac{\text{std2} \cdot \text{std3}}{\text{std1}}$	8	10	-2
1	$\frac{\text{std3} \cdot \text{std4}}{\text{std1}}$	8	10	-2
1	$\text{Sym}^2(\text{std1})$	3	4	-1
1	$\text{Sym}^2(\text{std2})$	3	4	-1
1	$\text{Sym}^2(\text{std3})$	3	4	-1
1	$\text{Sym}^2(\text{std4})$	3	4	-1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{sign}$	3	4	-1
1	$\mathfrak{sl}(\text{std3}) \cdot \text{sign}$	3	4	-1

Table 6.16.2: Nontrivial summands for the Dihedral Group D_{10}

Mult.	**Summand** L	$\dim(L)$	$\dim(K[G]_1^\times/\ker(L))$	$\dim(L) - \dim(K[G]_1^\times/\ker(L))$
1	$\mathfrak{sl}(\text{std4}) \cdot \text{sign}$	3	4	-1
1	$\dfrac{\text{Sym}^2(\text{std1})}{\text{std2}}$	6	7	-1
1	$\dfrac{\text{Sym}^2(\text{std2})}{\text{std4}}$	6	7	-1
1	$\dfrac{\text{Sym}^2(\text{std3})}{\text{std4}}$	6	7	-1
1	$\dfrac{\text{Sym}^2(\text{std4})}{\text{std2}}$	6	7	-1
1	$\mathfrak{sl}(\text{std1}) \cdot \text{std2}$	6	7	-1
1	$\mathfrak{sl}(\text{std2}) \cdot \text{std4}$	6	7	-1
1	$\mathfrak{sl}(\text{std3}) \cdot \text{std4}$	6	7	-1
1	$\mathfrak{sl}(\text{std4}) \cdot \text{std2}$	6	7	-1
1	$\text{Sym}^2(\text{e1})$	1	1	0
1	$\text{Sym}^2(\text{e2})$	1	1	0
1	$\text{Sym}^2(\text{sign})$	1	1	0
1	$\dfrac{\text{e1} \cdot \text{e2}}{\text{sign}}$	1	1	0
1	$\dfrac{\text{sign} \cdot \text{e1}}{\text{e2}}$	1	1	0
1	$\dfrac{\text{sign} \cdot \text{e2}}{\text{e1}}$	1	1	0

Bibliography

[1] S. A. Altuğ, A. Shankar, I. Varma, and K. H. Wilson. The number of quartic D_4-fields ordered by conductor. April 2017. URL: `https://arxiv.org/abs/1704.01729`.

[2] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra*. Addison–Wesley, 1994.

[3] M. Bhargava. *Higher composition laws*. PhD thesis, Princeton Univ., June 2001.

[4] M. Bhargava. Higher composition laws, III: The parametrization of quartic rings. *Ann. of Math.*, 159(3):1329–1360, 2004.

[5] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math.*, 162:1031–1063, 2005.

[6] M. Bhargava. Higher composition laws, IV: The parametrization of quintic rings. *Ann. of Math.*, 167(1):53–94, 2008.

[7] M. Bhargava and A. Shnidman. On the number of cubic orders of bounded discriminant having automorphism group c_3, and related problems. *Algebra and Number Theory*, 8(1):53–88, 2014.

[8] A. Borel. Some finitenes properties of adele groups over number fields. *Publications Mathématiques de l'I.H.É.S.*, 16:5–30, 1963.

[9] W. Bruns, B. Ichim, T. Römer, R. Sieg, and C. Söger. Normaliz. algorithms for rational cones and affine monoids. Available at `http://normaliz.uos.de`.

[10] W. Bruns, B. Ichim, and C. Söger. The power of pyramid decomposition in Normaliz. *J. Symb. Comp.*, 74:513–536, 2016.

[11] H. Cohen. Constructing and counting number fields. *Proceedings of the ICM, Beijing*, 2:129–138, 2002.

[12] H. Cohen, F. Diaz y Diaz, and M. Olivier. On the density of discriminants of cyclic extensions of prime degree. *J. reine angew. Math*, 550:169–209, 2002.

[13] J. H. Conway and D. A. Smith. *On quaternions and octonions*. AK Peters, 2003.

[14] B. N. Delone and D. K. Faddeev. The theory of irrationalities of the third degree. *Translations of Mathematical Monographs*, 10, 1964.

[15] E. Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C. R. Acad. Sci. Paris*, 254:616–618, 1962.

[16] A. Ivic, E. Krätzel, M. Kühleitner, and W. Nowak. Lattice points in large regions and related arithmetic functions: Recent developments in a very classic topic. In *Elementare und analytische Zahlentheorie*, page 89–128. Franz Steiner Verlag Stuttgart, 2006.

[17] J. W. Jones and D. P. Roberts. A database of local fields. *J. Symbolic Comput.*, 41(1):80–97, 2006.

[18] K. S. Kedlaya. Mass formulas for local Galois representations (with an appendix by Daniel Gulotta). *Int. Math. Res. Not. IMRN*, 17, 2007.

[19] I. Kiming. Explicit classifications of some 2-extensions of a field of characteristic different from 2. *Can. J. Math.*, XLII(5):825–855, 1990.

[20] J. Klüners. Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe, Habilitationsschrift, 2005.

[21] J. Klüners. Asymptotics of number fields and the Cohen–Lenstra heuristics. *Journal de théorie des nombres de Bordeaux*, 18(3):607–615, 2006.

[22] F. Levi. Kubische Zahlkörper und binäre kubische Formenklassen. *Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig, Mathematisch-Physische Klasse*, 66:26–37, 1914.

[23] G. Malle. On the distribution of Galois groups. *Journal of Number Theory*, 92:315–329, 2002.

[24] G. Malle. On the distribution of Galois groups, II. *Experimental Mathematics*, 13(2):129–135, 2004.

[25] S. Mäki. On the density of abelian number fields. *Annales Academiae Scientiarum Fennicae Series A1-Mathematica Dissertationes*, 54, 1985.

[26] M. Sato and T. Kimura. A classification of irreducible prehomogeneous vector spaces and their relative invariants. *Nagoya Math. J.*, 65:1–155, 1977.

[27] W. M. Schmidt. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Math. J.*, 35(2):327–339, 1968.

[28] J.-P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995.

[29] J.-P. Serre. *Linear representations of finite groups*, volume 42. Springer Science & Business Media, 2012.

[30] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed March 22, 2019].

[31] M. E. M. Wood. *Moduli spaces for rings and ideals*. PhD thesis, Princeton Univ., June 2009.

[32] D. J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.*, 58(3):17–50, 1989.

[33] D. J. Wright and A. Yukie. Prehomogeneous vector spaces and field extensions. *Invent. Math.*, 110(2):283–314, 1992.

[34] H. Zassenhaus. Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen. *Abh. Math. Sem. Univ. Hamburg*, 12(1):276–288, 1937.