INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

The Rigidity Method and Applications

Ian Stewart, Department of Mathematics
McGill University, Montréal

February 4, 2000

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of MSc.

Abstract

The Inverse Problem of Galois Theory is discussed. In a specific form, the problem asks whether every finite group occurs as a Galois group over $\mathbb{Q}$. An intrinsically group theoretic property called rigidity is described which confirms that many simple groups are Galois groups over $\mathbb{Q}$. Connections between rigidity and geometry are described and applications of rigidity are provided. In particular, after describing some of the theory of groups of Lie type, the rigidity criterion is applied to the exceptional Lie type groups $G_2(p)$, for primes $p > 5$. With the confirmation of a rationality condition, this establishes that $G_2(p)$ occurs as a Galois group over $\mathbb{Q}$ for all $p > 5$. Furthermore, the conjugacy classes which arise in the proof of rigidity for $G_2(p)$ are explored in detail, in the hope that a new proof might be produced which would illuminate the geometry associated to this rigid situation.

Résumé

Le problème inverse de la théorie de galois est traité. Dans une formulation particulière, le problème est de déterminer si tous les groupes finis se réalisent comme groupes de galois sur $\mathbb{Q}$. Une caractéristique intrinsèque aux groupes, appelée rigidité, est décrite, qui implique pour plusieurs groupes simples qu'ils sont des groupes de galois sur $\mathbb{Q}$. Des connections entre la rigidité et la géometrie sont décrites, et des applications de la méthode de la rigidité sont présentées. En particulier, ayant décrit la théorie des groupes de Lie sur les corps finis, le critère de rigidité est appliqué à la famille des groupes de Lie exceptionel, $G_2(p)$, pour les nombres premiers $p > 5$. Avec la confirmation d'une condition de rationalité, il est établi que $G_2(p)$ se réalise comme groupe de galois sur $\mathbb{Q}$ pour tout nombre premier $p > 5$. De plus, les classes de conjugaison qui se présentent dans la preuve de rigidité pour $G_2(p)$ sont explorés en détail, dans l'espoir qu'une preuve nouvelle puisse être produite qui illuminerait l'aspect géometrique de cette situation rigide.

Acknowledgments

I first would like to gratefully acknowledge the assistance and encouragement of my thesis supervisor, Henri Darmon, without which this work would not have been possible.

There are several people who I would like to thank for their help, mathematical or editorial: Colin Stewart, Jody Esmonde, Thomas Mattman, Kamal Khuri-Makdisi and Marc-Hubert Nicole.

This thesis is mostly expository. Below the major sources for each chapter are summarized: in the absence of a citation, it should be assumed that the source for the material is in the list below.

Chapter 1: [MM95], [Vol96], [Ser92] :

Chapter 2: [Lan93], [Hun74], [Suz82], [Suz86], [Ser77]:

Chapter 3: [MM95], [Vol96], [Ser92];

Chapter 4: [Dar98]:

Chapter 5: [Dar98], [Ser68]:

Chapter 6: [Car72], [Gor82], [War83], [Hum72]:

Chapter 7: [Cha68], [FF84]: the character table computation carried out here is not included in the original proof in [FF84]. The approach via estimates is my own.

Chapter 8: The questions raised in this chapter are based on ideas of H. Darmon.

Chapter 9: [Ebb91], [War97], [FH91]. Many of the proofs in the sections on the conjugacy classes of $G_2(p)$ are original, although the results are presumably well-known.

Contents

1 Introduction

The Galois Theory describes a natural way to associate a group to a normal field extension of $\mathbb{Q}$, specifically, the group of automorphisms of the extension field fixing $\mathbb{Q}$. It is not yet known whether this procedure may be "inverted":

Conjecture 1 (Inverse Galois Problem) *Every finite group is the Galois group of some normal extension of* $\mathbb{Q}$.

The problem is often generalized to allow base fields other than $\mathbb{Q}$. Indeed, studying the analogue of Conjecture 1 over the fields $\mathbb{C}(t)$, $\overline{\mathbb{Q}}(t)$ and $\mathbb{Q}(t)$ will be seen to be very important in studying the Inverse Galois Problem over $\mathbb{Q}$.

1.1 History

The Inverse Galois Problem was proposed by Hilbert (1892), who demonstrated that S_n and A_n are Galois groups over $\mathbb{Q}$ for all n. The first general approach to the problem was proposed by E. Noether, who established a criterion which would ensure a group G was Galois over $\mathbb{Q}$ (1918), namely if its field of invariants is rational (see [Ser92], pp xiii-xiv). The criterion is difficult to verify, and it was not until 1969 that a group was found (by Swan), the cyclic group C_{47} of order 47, which did not satisfy this rationality

condition. As C_{47} is abelian, it is easily shown to be a Galois group over $\mathbb{Q}$. Later work by Lenstra provided an explicit criterion to establish rationality for abelian groups, which is not met by many known Galois groups of small order, so another approach is probably required.

Using different techniques, by inductively solving the relevant embedding problems, Scholz and Reichart realized every finite nilpotent group as a Galois group over $\mathbb{Q}$ (1937). Their ideas were extended by Shafarevich, who established that every finite solvable group is a Galois group over $\mathbb{Q}$ (1954). This result does not guarantee that G occurs as a Galois group in a regular extension of $\mathbb{Q}(t)$, however.

1.2 Strategy

In the late 1970s, there were two important developments related to the Inverse Galois Problem. First, the classification of finite simple groups was completed, establishing that every finite simple group is an alternating group, a Lie type group, or one of 26 sporadic groups. At the same time, a new technique, the rigidity method, for realizing finite groups as Galois groups was developed (attributed variously to Fried, Belyi, Matzat and Thompson). The technique proved especially successful at realizing simple groups as Galois

groups, either over $\mathbb{Q}$ or over an abelian extension of $\mathbb{Q}$. Taken together, these developments in the theory suggest the following strategy, first made explicit by Thompson, for resolving the Inverse Galois Problem over $\mathbb{Q}$:

A) Demonstrate that every finite simple group occurs as the Galois group of some extension of $\mathbb{Q}$;

B) For an arbitrary finite group, solve the relevant "embedding problems", given that its simple composition factors occur regularly as Galois groups; that is, construct a Galois extension of $\mathbb{Q}$ with Galois group G assuming that step A has been solved (see Theorem 2.10).

Neither of the steps has been completed. Little will be said here about the embedding problems in B); for details see [MM95]. Concerning step A), the rigidity method has successfully realized all but one of the 26 sporadic simple groups as Galois groups over $\mathbb{Q}$; however, the rigidity method is only known to realize the finite simple Lie type groups defined over $\mathbb{F}_q$ when q is a small power of a prime p. Indeed, not a single Lie type group is known to be realized by the rigidity method as a Galois group over $\mathbb{Q}$ when q is a fourth power of p or higher. Thus there has been considerable research into modifying and extending the rigidity method, with some success. See

[MM95] and [Vol96] for more details.

2 Preliminaries

2.1 Galois Theory

If F is a field extension of K, $\mathrm{Aut}(F/K)$ denotes the group of field automorphisms of F which fix K.

Definition 2.1 *A field extension F/K is said to be* Galois *if $F^{\mathrm{Aut}(F/K)} = K$. Then $\mathrm{Aut}(F/K)$ is called the* Galois group *of the field extension.*

Theorem 2.2 (Galois Correspondence) *Let F/K be a Galois extension of fields with Galois group G. The assignment $H \mapsto F^H$ gives a bijective correspondence between subgroups H of G and intermediate fields $K \subset L \subset F$, where F^H is the subfield of F fixed by H. The inverse sends L to $\mathrm{Gal}(F/L)$. Under this bijection, normal subgroups $N \triangleleft G$ correspond to Galois extensions L/K, and $\mathrm{Gal}(L/K) \cong G/N$.*

For number fields F and K with rings of integers $\mathcal{O}_F$ and $\mathcal{O}_K$, the Galois group $G = \mathrm{Gal}(F/K)$ acts transitively on the set of prime ideals $\wp_i$ in $\mathcal{O}_F$ lying over a fixed prime p in $\mathcal{O}_K$. Fix a prime $\wp$ over p. The *decomposition group* $D_\wp$ at $\wp$ is the subgroup of G consisting of all $\sigma \in G$ such that $\sigma(\wp) = \wp$. Let $\bar{F} = \mathcal{O}_F/\wp$ and $\bar{K} = \mathcal{O}_K/p$. Then $\bar{F}/\bar{K}$ is a Galois extension. Let

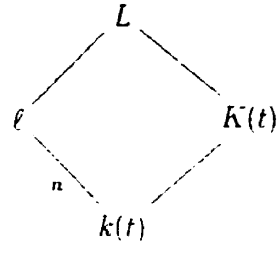
$\tilde{G} = \mathrm{Gal}(\tilde{F}/\tilde{K})$. There is a natural homomorphism $\phi_\wp : D_\wp \to \tilde{G}$, defined so that for any $f \in \mathcal{O}_F$, $\tilde{d(f)} = \phi_\wp(d)(\tilde{f})$. The kernel of $\phi_\wp$ is called the *inertia group* $I_\wp$ at $\wp$, and is trivial if and only if $\wp$ is unramified.

Let $K(t)$ denote the function field in an indeterminate t.

Definition 2.3 *A Galois extension F of $K(t)$ is said to be* regular *if $\overline{K} \cap F = K$.*

Definition 2.4 *Let K be algebraically closed, k a subfield of K, and L a finite Galois extension of $K(t)$, of degree n. The extension $L/K(t)$ is said to be* defined over k *if there is a regular Galois extension ℓ of $k(t)$ of degree n, such that $\ell \subset L$.*

This is illustrated below.



It will be of particular interest to know when a field extension $L/\overline{\mathbb{Q}}(t)$ is defined over $\mathbb{Q}$.

2.2 Representation Theory

Let V be a finite dimensional vector space over a field F. Let $\mathrm{GL}(V)$ denote the group of F-linear vector space automorphisms of V.

Definition 2.5 *A* representation ρ *of a group* G *over the field* F *is a group homomorphism from* G *to* $\mathrm{GL}(V)$.

Usually F will be taken to be $\mathbb{C}$, and in this case the representation may be called *complex*. If $F = \mathbb{F}_p$, the representation will be called *modular*. The dimension of V is called the *degree* of the representation. The representation ρ is said to be *irreducible* if the only $\rho(G)$-invariant proper subspace of V is the trivial subspace.

Definition 2.6 *The* character χ *of a complex representation* ρ *is the function from* G *to* $\mathbb{C}$ *given by* $\chi(g) = \mathrm{Tr}(\rho(g))$.

Hence $\chi(g)$ is the sum of the eigenvalues of $\rho(g)$. Since $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$, characters are class functions on G, that is, if g and h are conjugate in G, then $\chi(g) = \chi(h)$. Suppose G is a finite group. Then,

Proposition 2.7 *The number of irreducible complex representations of* G *is equal to the number of conjugacy classes in* G.

Since $\rho(g) \in \mathrm{GL}(V)$ is of finite order, its eigenvalues are roots of unity and hence

Proposition 2.8 *$\chi(g)$ belongs to $\mathbb{Z}[\mu_n]$ for all g in G, where n is the exponent of G. In particular, $\chi(g)$ is an algebraic integer.*

In particular, if $\chi(g)$ is rational, then $\chi(g)$ belongs to $\mathbb{Z}$.

2.3 Group Theory

The following definition and theorem are provided to illuminate the connection between steps A and B in Thompson's strategy, as described in the Introduction.

Definition 2.9 *A* composition series *of a group G is a series*

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{1\}$$

of subgroups of G where each G_i is a maximal normal subgroup in G_{i-1}.

From the definition, the *composition factors* G_{i-1}/G_i are simple.

Theorem 2.10 (Jordan-Hölder Decomposition Theorem) *Any two composition series of a finite group G have the same number of factors. The*

unordered sets of composition factors are identical in the two series (up to isomorphism).

Definition 2.11 *The* normalizer *in G of a subgroup H, denoted $N_G(H)$, is the subgroup of G consisting of all elements $g \in G$ for which $gHg^{-1} \subseteq H$.*

In other words, $N_G(H)$, is the largest subgroup of G in which H is normal.

Let p denote a prime number.

Definition 2.12 *A subgroup of G is called* p-local *if it is the normalizer of a subgroup of order p^r for some $r \geq 1$.*

Definition 2.13 *A subgroup of G is called* local *if it is p-local for some prime p.*

If G is a finite group and π a set of primes, then $O_\pi(G)$ denotes the largest normal subgroup of G with order divisible by a subset of the primes in π. Thus, $O_p(G)$ is the largest normal p-subgroup of G.

Definition 2.14 *An* involution *is an element $g \in G$ of order 2.*

2.4 Topology

Let C and T be topological spaces. Suppose there is a continuous surjective map $p : C \to T$, such that any $t \in T$ has a neighbourhood U such that

$p^{-1}(U)$ consists of disjoint open sets, each mapped by p homeomorphically onto U. Then C is called a *covering space* of T and p is called a *covering map*. A *universal covering space* of T is a covering space of T which is simply connected. If T is path connected, locally path connected, and locally simply connected then T has a universal covering space.

Definition 2.15 *Let C be a covering space of T with covering map p. A* deck transformation *of C is a homeomorphism $d : C \to C$ satisfying $p \circ d = p$.*

The set of deck transformations of any covering space form a group under composition. Deck transformations are important in the study of fundamental groups because of the following:

Theorem 2.16 *If T has a universal covering space U, then the fundamental group of T at any point P is isomorphic to the group of deck transformations of U.*

If $p : C \to T$ is a covering map, and $t \in T$, then the set $p^{-1}(t)$ is called the *fibre* of p at t. The isomorphism of the above theorem is proved by identifying the natural action of the group of deck transformations on $p^{-1}(t)$ with the action of $\pi(T, t)$ on $p^{-1}(t)$ which sends, for a homotopy class γ, a fixed $p^{-1}(t)$ to the endpoint of the path $p^{-1}(\gamma)$ with starting point $p^{-1}(t)$.

The covering p is called a *Galois covering* if C is connected and for every $t \in T$ the group of deck transformations of C acts transitively on the fibre of p at t. The *degree* of the covering is $n = |p^{-1}(t)|$ at any $t \in T$, and this is equal to the order of the deck transformation group. If n is finite, p is called a *finite* Galois covering.

2.5 Function Fields

Definition 2.17 *A* function field K *of dimension* n *over a field* F *is a field extension of* F *of transcendence degree* n, *where* $n \geq 1$.

A *valuation* is a function $v : K \to \mathbb{Z} \cup \infty$ satisfying $v(x) = \infty$ if and only if $x = 0$; $v(x + y) \geq \min(v(x), v(y))$; and $v(xy) = v(x) + v(y)$. The *valuation ring* R of v is the subset consisting of all $r \in K$ such that $v(r) \geq 0$. For any nonzero $x \in K$, then $x \in R$ or $x^{-1} \in R$. The ring R is a local ring; the *valuation ideal* I of R is the unique maximal ideal of R. The ideal I consists of all non-invertible elements in R, that is, all elements $r \in R$ for which $v(r) > 0$. The quotient R/I is called the *residue field* of v.

Let t be an indeterminate. Then $\mathbb{C}(t)$ is a function field of dimension 1 over $\mathbb{C}$. The valuation ideals of valuations on $\mathbb{C}(t)$ are in bijection with the elements of $\hat{\mathbb{C}}$, the Riemann sphere. For example, the points 0, 1, and ∞ in

$\hat{\mathbb{C}}$ correspond, respectively, to the valuation ideals (t), $(t-1)$, and $(1/t)$ in the valuation rings $\mathbb{C}(t)_{(t)} = \{f = \frac{p(t)}{q(t)} \mid q(0) \neq 0\}$, $\mathbb{C}(t)_{(t-1)} = \{f = \frac{p(t)}{q(t)} \mid q(1) \neq 0\}$, and $\mathbb{C}(t)_{(\frac{1}{t})} = \{f = \frac{p(t)}{q(t)} \mid \deg(p(t)) \leq \deg(q(t))\}$.

The field of rational functions on a curve with irreducible defining equation $f(x, y) = 0$ over F is a one-dimensional function field, since it is the field of fractions of $F[x, y]/f(x, y)$. Conversely, if K is a one-dimensional function field over F of characteristic zero then K is algebraic and separable over $F(x)$, where $x \in K$ is transcendental over F, and is thus generated by a single (primitive) element y over $F(x)$, which corresponds naturally to a curve over F.

2.6 Profinite Groups

Suppose given a family of groups $\{G_{n \in I}\}$, indexed by a partially ordered directed set I, and whenever $\imath \leq \jmath$ a homomorphism $f_{\jmath\imath} : G_\jmath \to G_\imath$, the $f_{\jmath\imath}$ compatible in the sense that $f_{\jmath\imath} \circ f_{k\jmath} = f_{k\imath}$, and $f_{\imath\imath}$ is the identity.

Definition 2.18 *The* inverse limit, $\varprojlim G_n$ *of the family* $\{G_n\}$ *with the homomorphisms* $f_{\jmath\imath}$ *is the subgroup of* $\prod_{n \in I} G_n$ *consisting of elements* $(g_n)_{n \in I}$, $g_n \in G_n$, *whose components satisfy* $f_{\jmath\imath}(g_\jmath) = g_\imath$ *whenever* $\imath \leq \jmath$.

A group is called *profinite* if it is isomorphic to an inverse limit of finite groups. An important example is the *p-adic integers*, denoted $\mathbb{Z}_p$, which are defined for each prime p to be $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, with the canonical system of homomorphisms. The field of p-adic numbers, $\mathbb{Q}_p$, is the quotient field of $\mathbb{Z}_p$. The *profinite completion* of a group G is the inverse limit of all finite quotients of G.

Profinite groups arise naturally in Galois theory. For example, for $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$G_{\mathbb{Q}} \cong \varprojlim G_{\mathbb{Q}}/H$$

where the inverse limit is taken over all Galois groups $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for all finite Galois extensions $K/\mathbb{Q}$ with $K \subset \overline{\mathbb{Q}}$.

More generally, fix a finite set S of points on the Riemann sphere $\hat{\mathbb{C}}$. To each point P of S there corresponds a valuation ideal in $\mathbb{C}(t)$, the ideal which is zero at P. Denote the set of these ideals by S. Denote by M_S the maximal extension of $\mathbb{C}(t)$ unramified outside S. M_S is the union of all finite extensions $N/\mathbb{C}(t)$ which are unramified outside S.

Definition 2.19 *The* algebraic fundamental group *of* $\hat{\mathbb{C}}\backslash S$ *is defined to be*

$\mathrm{Gal}(M_S/\mathbb{C}(t))$.

The algebraic fundamental group is naturally profinite: it is the inverse limit of the Galois groups of all finite Galois extensions of $\mathbb{C}(t)$ unramified outside S. The relationship between the algebraic and topological fundamental groups is discussed in section 3.1.

Let $G_{\mathbb{Q}}$ be the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$. Let $\zeta_n = e^{2\pi i/n}$ for all n. There is a natural homomorphism from $G_{\mathbb{Q}}$ onto $\hat{\mathbb{Z}}^\times$, the group of units of the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$. This is defined below by combining the homomorphisms $\phi_n : G_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^\times$, where $\phi_n(\sigma) = \ell$ if $\sigma(\zeta_n) = \zeta_n^\ell$.

Definition 2.20 *The* cyclotomic character c *is the homomorphism from* $G_{\mathbb{Q}}$ *to* $\varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$ *where* $c(\sigma) = (\phi_n(\sigma))_{1 \le n < \infty}$.

3 Inverse Galois Theory

3.1 The Inverse Galois Problem Over $\mathbb{C}(t)$

Fix a set S of r distinct valuation ideals $\wp_1, \ldots, \wp_r$ in $\mathbb{C}(t)$. Denote the corresponding subset of $\dot{\mathbb{C}}$ by S, and the corresponding points by $P_1, \ldots, P_r$ (as in section 2.6). Fix a base point P in $\dot{\mathbb{C}}$ different from every P_i. Let γ_i denote a homotopy class of loops based at P encircling the point P_i (and no other P_j). Fix a labelling of the points so that they are arranged consecutively clockwise around P. Then the relation $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r = 1$ is immediate. Hurwitz showed that this is the only essential relation in the fundamental group π of $\dot{\mathbb{C}} \backslash S$, based at P. That is.

$$\pi = \langle \gamma_1, \gamma_2, \ldots, \gamma_r \mid \gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r = 1 \rangle$$

Let G_S be the algebraic fundamental group of $\dot{\mathbb{C}} \backslash S$ (Definition 2.19). A profinite version of the Riemann Existence Theorem relates the algebraic and topological fundamental groups. Let $\hat{\pi}$ be the profinite completion of the topological fundamental group π.

Theorem 3.1 (Riemann Existence Theorem) *The algebraic fundamen-*

tal group G_S and $\hat{\pi}$ are isomorphic. Thus.

$$G_S \cong \langle \gamma_1, \gamma_2, \ldots, \gamma_r, \gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r = 1 \rangle^{\hat{}}$$

Furthermore. there is a canonical embedding of the topological fundamental group in the algebraic fundamental group under which the homotopy classes γ_i generating π are mapped respectively to generators x_i of G_S as a profinite group.

The proof relies on the identification of the topological fundamental group of $\hat{\mathbb{C}}\backslash S$ and the group of deck transformations of the universal covering space of $\hat{\mathbb{C}}\backslash S$ (Theorem 2.16). By using this identification, one can show that the finite quotients of the topological fundamental group correspond isomorphically to Galois groups of finite extensions of $\mathbb{C}(t)$ in M_S. The profinite completion of the topological fundamental group is thus isomorphic to the algebraic fundamental group, by the comments following Definition 2.19. See [MM95], pp. 4-6 for full details.

The canonical embedding introduced in Theorem 3.1 allows one to describe the inertia groups in G_S, as in the following theorem of Abhyankar.

Theorem 3.2 *The images x_i of the respective homotopy classes γ_i under the*

canonical injection from π into G_S generate procyclic inertia groups $\langle x_i \rangle^{\hat{}}$ at valuation ideals in M_S above $\wp_i$.

For a proof see [MM95], p. 6.

Theorem 3.3 *Every finite group is the Galois group of some field extension of $\mathbb{C}(t)$.*

Proof: For any finite group G which may be generated by $r-1$ elements $g_1, \ldots, g_{r-1}$, define a homomorphism ϕ from G_S onto G by

$$\phi(x_i) = \begin{cases} g_i & i \leq r-1 \\ (g_1 \cdot \ldots \cdot g_{r-1})^{-1} & i = r \end{cases} \tag{3.4}$$

Denote by F the fixed field of $\mathrm{Ker}\phi$, a normal subgroup of G_S. By Theorem 2.2, $F/\mathbb{C}(t)$ has Galois group isomorphic to

$$G_S/\mathrm{Ker}\phi \cong G$$

Hence the Inverse Galois Problem is solved over $\mathbb{C}(t)$.

□

3.2 From $\mathbb{C}(t)$ to $\overline{\mathbb{Q}}(t)$

Knowing the Inverse Galois Problem to be solved over $\mathbb{C}(t)$, one may prove that any extension $L/\mathbb{C}(t)$ is defined over a finitely generated extension of $\mathbb{Q}$ and thus over $\overline{\mathbb{Q}}$ by a specialization argument. Typically one proceeds as over $\mathbb{C}(t)$, by fixing a set S of valuation ideals in $\overline{\mathbb{Q}}(t)$, and examining the maximal extension M_S of $\overline{\mathbb{Q}}(t)$ unramified outside S. There are several ways to complete this, by using Hilbert's Irreducibility Theorem as in [Vol96] or Weil descent as in [MM95]. Indeed, the proof may be extended to solve the Inverse Galois Problem for any function field over an algebraically closed field of characteristic zero. In particular, the Inverse Galois Problem is solved over $\overline{\mathbb{Q}}(t)$. Grothendieck formulated the analogue of Theorem 3.2 in this descent, demonstrating that the generators of the algebraic fundamental group of $M_S/\overline{\mathbb{Q}}(t)$ generate procyclic inertia groups at valuation ideals above the $\wp_i \in S$. For details, see [MM95], pp. 9-12.

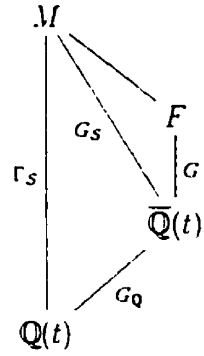
3.3 The Rigidity Method: From $\overline{\mathbb{Q}}(t)$ to $\mathbb{Q}(t)$

Before presenting the basic rigidity theorem, a series of lemmas is required. Henceforth, S will denote a set of r points in $\mathbb{P}_1(\overline{\mathbb{Q}})$ invariant as a set under $G_{\mathbb{Q}}$. Then S will denote the corresponding set of valuation ideals in $\overline{\mathbb{Q}}(t)$.

and M_S the maximal extension of $\overline{\mathbb{Q}}(t)$ unramified outside S. The group $G_S = \mathrm{Gal}(M_S/\overline{\mathbb{Q}}(t))$ is profinite, with presentation

$$\langle x_1, x_2, \ldots, x_r \mid x_1 \cdot \ldots \cdot x_r = 1 \rangle^{\widehat{}}$$

As before, one hopes to produce a homomorphism σ from $\Gamma_S = \mathrm{Gal}(M_S/\mathbb{Q}(t))$ onto G. Then $F := M_S^{\ker\sigma}$ is a Galois extension of $\mathbb{Q}(t)$ with Galois group G, and there is the following situation:



The notation of the diagram will be used throughout. Restating Grothendieck's analogue of Theorem 3.2, described at the end of Section 3.2.

Lemma 3.5 *Each generator x_i of G_S generates a procyclic inertia group $\langle x_i \rangle^{\widehat{}}$ at a valuation ideal in M_S above $\wp_i \in S$.*

Furthermore, $G_S \lhd \Gamma_S$ and $G_{\mathbb{Q}}$ is a complement of G_S, so Γ_S is a semidirect product of $G_{\mathbb{Q}}$ and G_S, and $G_{\mathbb{Q}}$ acts on G_S. This action is not fully

understood, but using Lemma 3.5, the conjugacy classes of the x_i can be described. Since $\mathcal{S}$ is invariant as a set under $G_{\mathbb{Q}}$, the $\wp_i \in \mathcal{S}$ are permuted by $\sigma \in G_{\mathbb{Q}}$, so σ may be viewed as a permutation of the indices $\{1, 2, \ldots, r\}$ (since $1 \leq i \leq r$). Let $\tilde{\sigma}$ be a lift of some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}(t)/\mathbb{Q}(t))$ to $\Gamma_{\mathcal{S}}$.

Lemma 3.6 *In $G_{\mathcal{S}}$, $(x_i)^{\tilde{\sigma}}$ is conjugate to $x_{\sigma(i)}^{c(\sigma)}$, where c is the cyclotomic character.*

See [MM95], pp. 14-15.

3.3.1 Rationality

Definition 3.7 *A conjugacy class C in a finite group G is called* rational *if for every irreducible character χ of G, $\chi(C) \in \mathbb{Q}$.*

By Proposition 2.8, C is rational if and only if $\chi(C) \in \mathbb{Z}$ for all χ. Let n be the exponent of G.

Lemma 3.8 *A class C is rational if and only if $C^a = C$ whenever $(a, n) = 1$.*

Proof: Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$, and let ρ be an irreducible representation of G, with character χ, $\rho : G \to \mathrm{GL}_r(\mathbb{C})$. There is a natural action of σ on the image of ρ by Proposition 2.8. Then $\sigma \circ \rho$ is an irreducible representation of

G, and since $\mathrm{Tr}(\sigma \circ \rho(g)) = \sigma \circ \mathrm{Tr}(\rho(g))$, the character of $\sigma \circ \rho$ is $\sigma \circ \chi$. Thus, $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ acts on the set of irreducible characters of G.

Let $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then the map $g \to g^\alpha$ defines a group-action of $(\mathbb{Z}/n\mathbb{Z})^\times$ on the set G. If $(\alpha, n) = 1$, denote by σ_α the element of $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ for which $\sigma_\alpha(\zeta_n) = \zeta_n^\alpha$ for every primitive n^{th} root of unity ζ_n. Then

$$\sigma_\alpha \circ \chi(C) = \chi(C^\alpha) \tag{3.9}$$

If for all irreducible characters χ, $\chi(C) \in \mathbb{Q}$, then $\sigma_\alpha \circ \chi(C) = \chi(C)$, so by equation (3.9), $\chi(C) = \chi(C^\alpha)$ for all χ. But then $C = C^\alpha$ by the orthogonality relations for characters. Conversely, if $C = C^\alpha$ whenever $(\alpha, n) = 1$, then by equation (3.9),

$$\begin{aligned} \sigma_\alpha \circ \chi(C) &= \chi(C^\alpha) \\ &= \chi(C) \end{aligned}$$

so $\chi(C)$ is fixed by σ_α for all α and thus $\chi(C) \in \mathbb{Q}$. □

Hence, if the class C is rational, then for any g in C, any generator of the cyclic group $\langle g \rangle$ is also in C.

By Lemma 3.8, one has the following.

Proposition 3.10 *Any conjugacy class of involutions is rational.*

3.3.2 Rigidity

For a class vector $v = (C_1, C_2, \ldots, C_r)$ of conjugacy classes of a finite group G, define Σ_v to be the set of r-tuples $(g_1, g_2, \ldots, g_r)$ such that

1. $g_i \in C_i$ for all i;

2. $\langle g_1, g_2, \ldots, g_r \rangle = G$;

3. $g_1 g_2 \ldots g_r = 1$.

Definition 3.11 *A vector v of conjugacy classes is called* rigid *if* $|\Sigma_v| = |G|$.

G acts on Σ_v by componentwise conjugation.

Lemma 3.12 *If $Z(G) = \{1\}$, then the action of G on Σ_v is free.*

Proof: Suppose for some $y \in G$ and $(g_1, \ldots, g_r) \in \Sigma_v$ that $y g_i y^{-1} = g_i$ for all i. Then y would commute with a set of generators for G and hence would be in $Z(G)$, which is assumed trivial. □

From this lemma, the following equivalent formulation of rigidity follows immediately:

Lemma 3.13 *Assume Σ_v is nonempty. If $Z(G) = \{1\}$, then v is a rigid vector of conjugacy classes if and only if the action of G on Σ_v is transitive.*

Define $H \subset \mathrm{Hom}(G_S, G)$ so that $\phi \in H$ if and only if

1. ϕ is surjective: and

2. $\phi(x_i) \in C_i$ for each i.

The following lemma is a special case of the Hurwitz classification, in [MM95], p. 25.

Lemma 3.14 *There is a bijection between the sets H and Σ_v.*

Proof: For $\phi \in H$, define an r-tuple $(g_1, \ldots, g_r)$ by $g_i = \phi(x_i)$ for each i. Then since $\phi \in H$, $g_i \in C_i$ for each i; since ϕ is surjective, $\langle g_1, \ldots, g_r \rangle = G$, and since $x_1 \cdot \ldots \cdot x_r = 1$, then $g_1 \cdot \ldots \cdot g_r = 1$, so $(g_1, \ldots, g_r) \in \Sigma_v$. Conversely, given $(g_1, \ldots, g_r) \in \Sigma_v$, define a homomorphism $\phi \in \mathrm{Hom}(G_S, G)$ by $\phi(x_i) = g_i$ for all i. Since the set of g_i generate G, ϕ is surjective, and by definition $\phi(x_i) \in C_i$ for all i. Hence ϕ is in H. □

Define a G-action on H as follows. For $g \in G$, $v \in H$, $x \in G_S$.

$$g \cdot v(x) = gv(x)g^{-1} \tag{3.15}$$

With this definition, then by the bijection between H and Σ_v above, one has

Lemma 3.16 *Σ_v and H are isomorphic as G-sets.*

The main result of this section can now be stated and proved.

Theorem 3.17 (Basic Rigidity Theorem) *Let G be a finite group, with trivial center. If there exists a class vector $(C_1, \ldots, C_r)$ of conjugacy classes of G which is rigid and rational, then G is the Galois group of a regular extension of $\mathbb{Q}(t)$.*

Remark: While the Rigidity Theorem is proved here for any r-vector of conjugacy classes, in practice the theorem is virtually always applied with $r = 3$.

The notation of this section will be used in the proof.

Proof: Choose S so that each point $P_i \in S$ is invariant under $G_{\mathbb{Q}}$. By Theorem 2.2, G_S is a normal subgroup of Γ_S, so there is the exact sequence

$$1 \to G_S \to \Gamma_S \to G_{\mathbb{Q}} \to 1$$

Let $\psi \in \mathrm{Hom}(G_S, G)$, and let $x \in G_S$. Define a Γ_S-action on $\mathrm{Hom}(G_S, G)$ as follows. For $\gamma \in \Gamma_S$,

$$(\psi \cdot \gamma)(x) = \psi(\gamma x \gamma^{-1})$$

Extend the G-action in (3.15) to $\mathrm{Hom}(G_S, G)$ so that $g \cdot \psi(x) = g\psi(x)g^{-1}$ for all $\psi \in \mathrm{Hom}(G_S, G)$. Then the G and Γ_S-actions commute: that is $(g \cdot \psi) \cdot \gamma = g \cdot (\psi \cdot \gamma)$.

By Lemma 3.16, since Σ_v is stable under the action of G, then H is stable under the action of G. By Lemmas 3.12 and 3.13, G acts freely and transitively on H.

Since the set S has been chosen so that it is fixed elementwise by $G_{\mathbb{Q}}$, then, using the notation of Lemma 3.6, $\varphi_{\sigma(i)} = \varphi_i$. Thus, by Lemma 3.6, conjugation by $\gamma \in \Gamma_S$ sends a generator x_i to a conjugate of a power of x_i. But the conjugacy classes C_i are assumed rational, so it follows from the equivalent definition of rationality in Lemma 3.8 that $\psi \cdot \gamma(x_i) \in C_i$. Thus, $\psi \cdot \gamma \in H$, and H is also stable under the action of Γ_S.

The homomorphisms $\psi \in \mathrm{Hom}(G_S, G)$ which are surjective will define Galois extensions $M_S^{\mathrm{Ker}\psi}$ of $\overline{\mathbb{Q}}(t)$ with Galois group G. Since any homo-

morphism in H defines a Galois extension of $\overline{\mathbb{Q}}(t)$ with Galois group G, to complete the proof it will suffice to show that any $\psi \in H$ may be extended to a homomorphism ϕ from Γ_S to G. Let $y \in \Gamma_S$, $\psi \in H$. As will be proved, the following defines a homomorphism ϕ from Γ_S to G which extends ψ:

$$\phi(y) \cdot \psi = \psi \cdot y$$

That is, it will be shown that there is a unique element $\phi(y)$ in G such that for all $x \in G_S$,

$$\phi(y)\psi(x)\phi(y^{-1}) = \psi(yxy^{-1})$$

and $\phi(x) = \psi(x)$ for all $x \in G_S$. H is fixed by the action of Γ_S, so $\psi \cdot y \in H$. Since G acts transitively on H, then $\phi(y)$ exists, and since G acts freely on H, $\phi(y)$ is uniquely determined. If $x \in G_S$, then for all $g \in G_S$

$$\phi(x)\psi(g)\phi(x^{-1}) = \psi(xgx^{-1}) = \psi(x)\psi(g)\psi(x^{-1})$$

so $\phi(x) \cdot \psi = \psi(x) \cdot \psi$ and $\phi(x) = \psi(x)$ for any $x \in G_S$ since G acts freely and transitively. Thus ϕ extends ψ and all of the claims have been established.

□

The theorem has many generalizations. The condition that the center be trivial, adequate for applications to simple groups, can be relaxed to allow for groups whose center has a complement. The rationality condition can also be relaxed: see [Vol96], [Ser92], [MM95]. If one is interested only in realizing G as a Galois group over the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$, then the rationality criterion can be dispensed with. That is,

Theorem 3.18 *If there is a rigid vector of conjugacy classes of G, then G is a Galois group over $\mathbb{Q}^{ab}$.*

Rigid class vectors have been found in most of the simple groups of Lie type, but in very few cases are these vectors rational; hence most simple groups of Lie type are known to occur as Galois groups over $\mathbb{Q}^{ab}$, but very few are known to occur over $\mathbb{Q}$. Twenty-four of the twenty-six sporadic simple groups are known to be realized as Galois groups over $\mathbb{Q}$ by rigidity. The two exceptions, the Mathieu groups M_{23} and M_{24} both contain rigid (but not rational) triples of conjugacy classes. Using different techniques, it was established by Matzat that M_{24} is a Galois group over $\mathbb{Q}$, leaving M_{23} as the only remaining sporadic group not known to be a Galois group over $\mathbb{Q}$. The most comprehensive account of known results may be found in [MM95].

3.4 Verifying Rigidity and Rationality

In practice one typically chooses $r = 3$, so that one is working with a triple of conjugacy classes. The following approach is often used to verify that such a triple is rigid:

1. Compute the number n of solutions (x_1, x_2, x_3) of $x_1x_2x_3 = 1$, with $x_i \in C_i$. For this there is a formula, the validity of which is proved below:

$$n = \frac{|C_1||C_2||C_3|}{|G|} \sum_{\chi} \frac{\chi(C_1)\chi(C_2)\chi(C_3)}{\chi(1)} \tag{3.19}$$

2. Determine how many of these triples (x_1, x_2, x_3) generate G. To do this, it is usually necessary to have information about maximal subgroups of G.

Proof of (3.19):

Fix an irreducible representation ρ of G. By Schur's Lemma, the centralizer of the image of ρ is the set of scalar matrices. Thus,

$$\frac{1}{|G|} \sum_{\sigma \in G} \rho(\sigma g \sigma^{-1}) = \lambda_g \mathrm{Id} \tag{3.20}$$

for each $g \in G$, as the left side commutes with $\rho(h)$ for all $h \in G$. Let χ be the character of ρ. Considering the trace of the left side, one finds that $\lambda_g = \frac{\chi(g)}{\chi(1)}$, since $\chi(1)$ is the dimension of Id.

Now, taking the product of (3.20) with the corresponding sides of equation (3.20) but with g replaced by $g_2 \in G$ allows one to inductively extend this formula to an arbitrary number r of group elements. One obtains

$$\frac{1}{|G|^r} \sum_{(\sigma_1,\ldots,\sigma_r)\in G^r} \rho(\sigma_1 g_1 \sigma_1^{-1} \ldots \sigma_r g_r \sigma_r^{-1}) = \frac{\chi(g_1)\ldots\chi(g_r)}{\chi(1)^r}\mathrm{Id}$$

By computing traces and then multiplying by $\chi(1)|G|^{r-1}$ one has

$$\frac{\chi(1)}{|G|} \sum_{(\sigma_1,\ldots,\sigma_r)\in G^r} \chi(\sigma_1 g_1 \sigma_1^{-1} \ldots \sigma_r g_r \sigma_r^{-1}) = |G|^{r-1} \frac{\chi(g_1)\ldots\chi(g_r)}{\chi(1)^{r-2}}$$

Let Φ be the characteristic function of 1 in G so that $\Phi(1) = 1$ and $\Phi(g) = 0$ for all $g \neq 1$. The orthogonality relations for characters confirm that $\Phi = \frac{1}{|G|}\sum_\chi \chi(1)\chi$ where the sum ranges over all characters χ of irreducible representations of G. Now summing the above equation over all irreducible

characters χ of G.

$$\sum_{(\sigma_1,\ldots,\sigma_r)\in G^r} \Phi(\sigma_1 g_1 \sigma_1^{-1} \ldots \sigma_r g_r \sigma_r^{-1}) = \sum_{\chi} |G|^{r-1} \frac{\chi(g_1)\ldots\chi(g_r)}{\chi(1)^{r-2}}$$

By the definition of Φ, the left side of this equation gives the number of solutions $(\sigma_1,\ldots,\sigma_r) \in G^r$ to $\sigma_1 g_1 \sigma_1^{-1} \ldots \sigma_r g_r \sigma_r^{-1} = 1$. Let C_i denote the conjugacy class of g_i. Now, the equation also counts the number of solutions n to the equation $t_1 \ldots t_r = 1$ for $t_i \in C_i$ up to centralizers of the elements g_i. That is,

$$n = \sum_{\chi} \frac{|G|^{r-1}}{|C_G(g_1)|\ldots|C_G(g_r)|} \frac{\chi(g_1)\ldots\chi(g_r)}{\chi(1)^{r-2}}$$

which may be rewritten by using $|C_G(g_i)| = \frac{|G|}{|C_i|}$ and taking $r = 3$ to give equation (3.19). □

3.5 From $\mathbb{Q}(t)$ to $\mathbb{Q}$

If rigidity criteria ensure that G is a Galois group over $\mathbb{Q}(t)$, the Hilbert Irreducibility Theorem guarantees that the extension of $\mathbb{Q}(t)$ with Galois group G can be specialized in infinitely many ways to give an extension of $\mathbb{Q}$ with Galois group G. More precisely,

Theorem 3.21 (Hilbert Irreducibility Theorem) *Let $K/\mathbb{Q}(t)$ be a regular finite Galois extension, with Galois group G, and with minimal polynomial $f(t,x) \in \mathbb{Q}[t][x]$. Then for infinitely many $t_0 \in \mathbb{Q}$, the polynomial $f(t_0,x) \in \mathbb{Q}[x]$ is the minimal polynomial of a Galois extension of $\mathbb{Q}$ with Galois group G.*

The proof is somewhat technical, and is only summarized. It is equivalent to prove that each irreducible polynomial $f(t,x)$ in $\mathbb{Q}[t][x]$ has infinitely many specializations $f(t_0,x)$ over $\mathbb{Q}$ which are irreducible in $\mathbb{Q}[x]$. Indeed, one may prove this for any finite set $\{f_i(t,x)\}$ of polynomials in $\mathbb{Q}[t][x]$, as in ([Vol96], pp. 10-18). One calls a subset S of the natural numbers *sparse* if for some r, $0 < r < 1$, and almost all natural numbers n, $|S \cap \{1,\ldots,n\}| \leq n^r$. From the definition, one sees that a finite union of sparse sets is also sparse. Now one shows that there is an integer s for which the sets $S(f_i,s) := \{n \in \mathbb{N} \mid f_i(s+\frac{1}{n},q) = 0 \text{ for some } q \in \mathbb{Q}\}$ are all sparse, using complex analytic techniques ([Vol96], pp. 16-18). Then $S := \underset{i}{\cup} S(f_i,s)$ is a finite union of sparse sets, and is therefore sparse. The complement C of S in $\mathbb{N}$ is the set of natural numbers n for which all of the $f_i(s+\frac{1}{n},x)$ are irreducible over $\mathbb{Q}$. As C is the complement of a sparse set, C is infinite, establishing the theorem.

4 Applications of Rigidity

4.1 The Symmetric Group

For those finite groups with an uncomplicated geometric interpretation, or for which generators and relations are easily manipulated, there are often elegant proofs of rigidity (not requiring the formula (3.19) or other elaborate calculations). As one example, a rigid triple is exhibited in the group S_n. Recall that elements are conjugate in S_n if and only if they have similar disjoint cycle decompositions. Let C_i denote the conjugacy class of i-cycles.

Theorem 4.1 *The triple* $v := (C_2, C_{n-1}, C_n)$ *is rigid in* S_n.

Proof: Let $(\iota, \alpha, (\iota\alpha)^{-1}) \in v$. Relabelling as necessary, let $\alpha = (1\ 2\ \ldots\ n\text{-}1)$. Then $\iota\alpha \in C_n$ if and only if $\iota = (jn)$ for some $j \neq n$. Since it is well known that S_n is generated by $(1n)$ and $(12\ldots n)$, to prove rigidity it will suffice to show that $(1n)$ and (jn) are conjugate by an element in the centralizer of α. It is easily verified that

$$\begin{pmatrix} 1 & 2 & \ldots & j & \ldots & n-1 \\ j & j+1 & \ldots & 2j-1 & \ldots & j-1 \end{pmatrix}$$

is such an element (where the bottom row is considered modulo n). □

4.2 $\mathrm{PSL}_2(\mathbb{F}_p)$

Elegant proofs of rigidity can sometimes be found for the classical finite matrix groups by interpreting them as groups of transformations of a vector space. As one example, the group $\mathrm{PSL}_2(\mathbb{F}_p)$ has many rigid triples, one of which is described in the following theorem. When $p > 2$, there are two distinct conjugacy classes of unipotents (that is, consisting of elements of order p) in $\mathrm{PSL}_2(\mathbb{F}_p)$. Let $C_p^{(1)}$ denote the conjugacy class containing the class in $\mathrm{PSL}_2(\mathbb{F}_p)$ of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (the other unipotent conjugacy class contains an identical element but with a non-square in the upper right-hand corner).

Theorem 4.2 *There is a rigid triple $v = (C_p^{(1)}, C_2, C_3)$ of unipotent classes in $G = \mathrm{PSL}_2(\mathbb{F}_p)$ for all primes $p \neq 2$.*

Proof: A triple (a_1, a_2, a_3) of unipotent elements will be produced such that $\prod a_i = 1$ and $\langle a_i \rangle = G$, unique up to conjugation. Lift (a_i) to $\mathrm{SL}_2(\mathbb{F}_p)$ and write $(\tilde{a}_i)$ for the resulting triple. Since $\mathrm{PSL}_2(\mathbb{F}_p) \cong \mathrm{SL}_2(\mathbb{F}_p)/\pm 1$, then $\prod \tilde{a}_i = \pm 1$. Now $\tilde{a}_i$ has, up to multiplication by scalars, a unique eigenvector v_i with eigenvalue 1. Since a_1 and a_2 are, by assumption, noncommuting unipotents, $\tilde{a}_1$ and $\tilde{a}_2$ cannot simultaneously stabilize the one-dimensional space spanned by v_1, so v_2 must be linearly independent from v_1. Thus,

(v_1, v_2) defines a basis for the two-dimensional space on which $\mathrm{SL}_2(\mathbb{F}_p)$ acts. Writing $\tilde{a}_1$ and $\tilde{a}_2$ with respect to this basis, using the fact that the matrices have determinant 1.

$$a_1 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \qquad a_2 = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$$

Scale v_1 by x, so that $a_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and now write $a_2 = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$ (i.e. let $y = zx$). Now, since $\tilde{a}_1\tilde{a}_2 = \pm\tilde{a}_3^{-1}$, one finds

$$\tilde{a}_3^{-1} = \pm \begin{pmatrix} 1+y & 1 \\ y & 1 \end{pmatrix}$$

As $\tilde{a}_3$ has 1 as its only eigenvalue, the trace of $\tilde{a}_3^{-1}$ is 2. The above equation thus forces $y = 0$ or $y = -4$, depending on the sign of the right-hand side. It is impossible that $y = 0$, as this would force $\tilde{a}_2$ to be the identity. Thus, $y = -4$ (here it is required that $p \neq 2$) and the triple is unique up to conjugation. It is well known that these elements generate G, and v is thus a rigid class vector for $\mathrm{PSL}_2(\mathbb{F}_p)$. □

5 Global Rigidity

5.1 The Geometry of a Rigid Class Vector

It was established in Theorem (4.2) that $v = (C_p^{(1)}, C_2, C_3)$ is a rigid class vector in $\mathrm{PSL}_2(p)$ for all primes $p > 2$. It is natural to consider the group $G = \mathrm{PSL}_2(\mathbb{Z}[\frac{1}{2}])$. There are homomorphisms $\rho_p : G \to \mathrm{PSL}_2(p)$ for all $p > 2$, given by reduction mod p. Since the class vector is rigid for all $p > 2$, one expects this information to be encoded in the structure of the "global" group G. It is first necessary to reformulate the definition of rigidity in an appropriate way, so that it applies to finite and infinite groups, as follows. Call a class vector $v = (C_1, C_2, C_3)$ in a (possibly infinite) group *rigid* if there is exactly one orbit of triples $(g_1, g_2, g_3) \in v$ under conjugation by G, where the triples satisfy the conditions $g_i \in C_i$, $g_1 g_2 g_3 = 1$, and $\langle g_i \rangle = G$.

To refine these ideas and indicate some geometrical connections, a few definitions are required. Let ℓ be a prime. An *ℓ-adic representation* of $G_{\mathbb{Q}}$ is a continuous homomorphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$, for some n. For a place ν unramified with respect to ρ, define $P_{\nu,\rho}(T) := \det(\mathrm{Id} - \mathrm{Fr}_{\nu,\rho} T)$ where T is an indeterminate and $\mathrm{Fr}_{\nu,\rho}$ is the conjugacy class of $\rho(\mathrm{Frob}_w)$ for any place w over ν.

Suppose there are ℓ-adic representations ρ_ℓ of $G_{\mathbb{Q}}$ for all but finitely many primes ℓ.

Definition 5.1 *The system of representations* $\{\rho_\ell\}$ *is a* strictly compatible system of representations *if there exists a fixed finite set* S *of primes such that*:

1. ρ_ℓ *is unramified outside* $S \cup \ell$ *for all* ℓ;

2. $P_{v,\rho_\ell}(T)$ *has rational coefficients if* $v \notin S \cup \ell$; *and*

3. $P_{v,\rho_{\ell_1}}(T) = P_{v,\rho_{\ell_2}}$ *if* $v \notin S \cup \ell_1 \cup \ell_2$.

The class vector v in $\mathrm{PSL}_2(\mathbb{F}_p)$ from Theorem 4.2 arises naturally when considering a particular family of elliptic curves over $\mathbb{Q}(t)$:

$$E(t): \quad y^2 = x(x-1)(x-t)$$

The action of $G_{\mathbb{Q}(t)}$ on the p-division points, which form a two-dimensional module, gives modular representations $\rho_p(t)$ for all $p > 2$. The $\rho_p(t)$ are so-called *Frey representations*. The image of the restriction $\rho_p(t)\,|_{G_{\bar{\mathbb{Q}}(t)}}$ is contained in $\mathrm{SL}_2(\mathbb{F}_p)$. Let $\hat{\rho}_p(t)$ be the projectivization of this restriction, so that $\hat{\rho}_p(t)$ has image in $\mathrm{PSL}_2(\mathbb{F}_p)$. Then $\hat{\rho}_p(t)$ is ramified only at 0, 1

and ∞. and generators of the corresponding three inertia groups are mapped respectively to elements in the three conjugacy classes in c. In this sense. the rigid triple c is associated to the elliptic curve $E(t)$. See [Dar98] for further details.

One might ask if this situation occurs more generally when one has a rigid triple in the rational (or S-integral) points of an algebraic group. That is. one asks whether class vectors which are rigid for almost all primes p arise from some geometric object. One would expect to be able to ask this question quite generally among the finite groups of Lie type. for two reasons. First. by definition the finite Lie type groups are equipped with a parametrization over the finite fields $\mathbb{F}_p$ for all (or almost all) primes p. Second. they are all simple or nearly simple groups. and among simple groups one finds an abundance of rigid triples of conjugacy classes. For this reason. it is worthwhile defining the Lie type groups and developing some of their structure. This is done in the next section. In particular the Lie type group $G_2(p)$ will be explored. Because of the possibility of describing $G_2(p)$ geometrically. one expects to be able to prove rigidity for this group in a way that would be convenient for addressing the questions of this section. Much of the remainder of this paper is devoted to collecting the information that would probably be necessary if

a proof of the type envisioned is indeed possible.

6 Lie Type Groups

6.1 Overview

The finite groups of Lie type are closely related to the simple Lie algebras and their associated Lie groups. First, some of the classification theory of Lie algebras is described. From the complex Lie algebra $\mathfrak{g}_2$ and its Lie group G_2 a class of finite simple groups may be produced. Indeed, for all $q = p^r$, p prime, a finite group $G_2(q)$ will be defined, simple except when $q = 2$.

6.2 Lie Theory

Definition 6.1 *A* bracket product *is a binary bilinear product on a vector space V satisfying the following for all $x, y, z \in V$:*

1. $[x, x] = 0$

2. *(Jacobi's Identity)* $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$

Definition 6.2 *A* Lie algebra *is a finite dimensional vector space over a field, endowed with a bracket product.*

For what follows, the field of scalars will be taken to be $\mathbb{C}$. In the following, let L be an arbitrary Lie algebra. L is said to be *abelian* if $[x, y] = 0$ for

all x and y in L. Let L^1 be the unique maximal ideal of L such that L/L^1 is abelian. Define L^m inductively for $m > 1$ by $L^m = [L, L^{m-1}]$. L is *nilpotent* if $L^m = 0$ for some m. The normalizer in L of a sub Lie algebra S is the set of all $x \in L$ such that $[x, S] \subset S$.

Definition 6.3 *A* Cartan subalgebra $\mathcal{H}$ *of a Lie algebra* L *is a nilpotent subalgebra of* L *satisfying* $N_L(\mathcal{H}) = \mathcal{H}$.

Associate to $x \in L$ the linear transformation $\mathrm{ad}x$ of L given by multiplication by x: that is, $\mathrm{ad}x(\ell) = [x, \ell]$ for all $\ell \in L$.

Definition 6.4 *The* adjoint representation *is the representation of* L *acting on itself where* $x \to \mathrm{ad}x$ *for all* $x \in L$.

Definition 6.5 *The* Killing Form *is the bilinear form* (x, y) *on* L *given by*

$$(x, y) = \mathrm{Tr}(\mathrm{ad}x \circ \mathrm{ad}y)$$

Definition 6.6 *A Lie algebra* L *is* semisimple *if its Killing form is nondegenerate.*

In a semisimple Lie algebra a Cartan subalgebra is a maximal abelian subalgebra $\mathcal{H}$ satisfying that $\mathrm{ad}h$ is diagonalizable for all $h \in \mathcal{H}$.

Definition 6.7 *A Lie algebra L is* simple *if* $\dim L > 1$ *and L contains no non-trivial ideals.*

Any semisimple Lie algebra is a direct sum of simple Lie algebras. As shall be described, the simple Lie algebras can be completely classified. Henceforth, L shall denote a simple Lie algebra (although most of what is described is true for semisimple Lie algebras as well). L has a Cartan subalgebra $\mathcal{H}$, and the dimension ℓ of $\mathcal{H}$ over $\mathbb{C}$ is independent of the choice of $\mathcal{H}$ and is called the *rank* of L.

6.3 Classification of Simple Lie Algebras

The *dual space* $\mathcal{H}^*$ of $\mathcal{H}$ is the set of linear functions from $\mathcal{H}$ to $\mathbb{C}$. For each $\alpha \in \mathcal{H}^*$, make the following definition.

Definition 6.8 *The* root space L_α *is the set* $\{x \in L : [h, x] = \alpha(h)x \text{ for all } h \in \mathcal{H}\}$.

L_α is nontrivial for only finitely many α, and $L_0 = \mathcal{H}$.

Definition 6.9 $\alpha \in \mathcal{H}^*$ *is a* root *of L if $\alpha \neq 0$ and L_α is nontrivial.*

Theorem 6.10 (Root Space Decomposition) *Let α be a root of L. Then*

L_α is a one-dimensional vector space over $\mathbb{C}$. Furthermore,

$$L = \mathcal{H} \oplus \bigoplus_\alpha L_\alpha$$

The Killing form is nondegenerate on $\mathcal{H}$. This allows one to construct a bijection between $\mathcal{H}$ and $\mathcal{H}^*$ as follows. Associate to any $\delta \in \mathcal{H}^*$ the unique element $t_\delta \in \mathcal{H}$ which satisfies, for all $h \in \mathcal{H}$,

$$(t_\delta, h) = \delta(h)$$

In particular, the notation t_α will be reserved for those elements in $\mathcal{H}$ which correspond to roots α. Now define a bilinear form on the dual space $\mathcal{H}^*$ by $(\delta, \gamma) = (t_\delta, t_\gamma)$, with respect to which orthogonality will be understood in $\mathcal{H}^*$. Then $(\alpha, \beta) \in \mathbb{Q}$ for any roots α, β. Furthermore, if S is any set of roots which are a basis for $\mathcal{H}^*$, any root may be written as a $\mathbb{Q}$-linear combination of roots in S. Thus, restricting scalars to $\mathbb{Q}$ makes $\mathcal{H}^*$ into an ℓ-dimensional rational Euclidean vector space E. Now one can prove

Proposition 6.11 *Suppose α is a root. If $k\alpha$ is a root, then $k = 1$ or -1. The reflection w_α of E through the plane orthogonal to α permutes the roots. Finally, $\frac{2(\alpha,\beta)}{(\beta,\beta)}$ is an integer for all roots α, β.*

The *Weyl Group* of L is the symmetry group of the root set which is generated by the reflections w_α. The last part of Proposition 6.11 motivates the definition of a new bilinear form on $\mathcal{H}^*$ by

$$\langle \delta, \gamma \rangle = \frac{2(\delta, \gamma)}{(\gamma, \gamma)}$$

Fix a basis of E consisting of roots $\{e_1, \ldots e_\ell\}$.

Definition 6.12 *A root α is* positive *with respect to the basis $\{e_1, \ldots, e_\ell\}$ if the first non-zero coefficient a_i is positive, writing $\alpha = a_1 e_1 + \ldots + a_\ell e_\ell$.*

Definition 6.13 *A root is* simple *if it is positive and cannot be expressed as the sum of two positive roots.*

Then a set of simple roots is defined once a basis $\{e_1, \ldots e_\ell\}$ is fixed.

Theorem 6.14 *The set of simple roots is a basis of E. Any positive root may be written as a $\mathbb{Z}_{\geq 0}$-linear combination of simple roots. If α and β are distinct simple roots, then $\langle \alpha, \beta \rangle \leq 0$ and $\alpha - \beta$ is not a root. Given any positive non-simple root α, a simple root β exists such that $\alpha - \beta$ is positive.*

It will be necessary in discussing Lie type groups to further refine the theory, by constructing an integral basis for the simple Lie algebras. For a root α, define $h_\alpha = \frac{2t_\alpha}{(\alpha,\alpha)}$. Previous considerations allow one to deduce

Theorem 6.15 (Chevalley Integral Basis Theorem) *Let $\alpha_1 \dots \alpha_\ell$ be a set of simple roots (with respect to some basis, as above). Then there are x_α which span the root spaces L_α satisfying the following for all roots α, β:*

1. $[h_\beta, x_\alpha] = \langle \alpha, \beta \rangle x_\alpha$;
2. $[x_\alpha, x_{-\alpha}] = h_\alpha$, *and* h_α *may be expressed as a* $\mathbb{Z}$*-linear combination of the* h_{α_i};
3. $[x_\alpha, x_\beta] = 0$ *if* $\alpha + \beta$ *is not a root; and*
4. $[x_\alpha, x_\beta] = (r+1)x_{\alpha+\beta}$ *if* $\alpha + \beta$ *is a root;* r *is the unique integer for which* $\beta - r\alpha$ *is a root and* $\beta - (r+1)\alpha$ *is not a root.*

With the notation of the above theorem, make the following definition.

Definition 6.16 *The* Chevalley Basis *of* L *consists of the* h_{α_i} *and the* x_α.

Definition 6.17 *The* structure constants $N_{\alpha,\beta}$ *of the simple Lie algebra* L *are the coefficients defined by the following:*

$$[x_\alpha, x_\beta] = N_{\alpha,\beta} x_{\alpha+\beta}$$

where $N_{\alpha,\beta} = 0$ *if* $\alpha + \beta$ *is not a root.*

The values of the structure constants may be computed by using Theorem 6.15.

A complete classification of the simple Lie algebras can be deduced from Proposition 6.11 and Theorem 6.14. The *Cartan matrix* gives one concise way to completely describe the structure of a simple Lie algebra, in the sense that all products in the Lie algbra may be determined from the matrix. A Cartan matrix is an ℓ by ℓ matrix where $a_{ij} = \langle \alpha_i, \alpha_j \rangle$. More schematically, the *Dynkin Diagram* of a semisimple Lie algebra also completely determines its structure.

Definition 6.18 *The* Dynkin Diagram *of a semisimple Lie algebra L is a graph with one vertex for each simple root α_i. Two vertices α_i and α_j are connected with $a_{ij}a_{ji}$ lines. If the* weights (α_i, α_i) *and* (α_j, α_j) *are not equal, a symbol $<$ is drawn on the lines connecting α_i and α_j, pointing to the root with smaller weight.*

The Dynkin diagram is connected if and only if the Lie algebra is simple; otherwise L is a direct sum of the simple Lie algebras corresponding to the connected components of the diagram. The theory that has been developed severely restricts the possible Dynkin diagrams of simple Lie algebras. From this, one may deduce the classification theorem of simple Lie algebras, which

is only summarized:

Theorem 6.19 *If L is a finite dimensional complex simple Lie algebra, then:*

1. *L belongs to one of the four "classical" families of Lie algebras, $\mathfrak{a}_n$, $\mathfrak{b}_n$, $\mathfrak{c}_n$ and $\mathfrak{d}_n$; or*

2. *L is one of the five exceptional Lie algebras $\mathfrak{g}_2$, $\mathfrak{f}_4$, $\mathfrak{e}_6$, $\mathfrak{e}_7$, and $\mathfrak{e}_8$.*

The subscript always denotes the number of simple roots in the Lie algebra, and hence nodes in the Dynkin diagram.

The Lie algebra of primary interest here is $\mathfrak{g}_2$, which has the Cartan matrix:

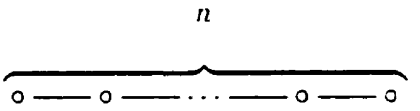
$$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

The Dynkin Diagram of $\mathfrak{g}_2$ is

$\mathfrak{g}_2$: o ≡< ≡ o

Two other simple Lie algebras will be referred to in the discussion of $\mathfrak{g}_2$. the family of *special linear* Lie algebras.

$\mathfrak{a}_n$:



and the orthogonal Lie algebra $\mathfrak{b}_3$:

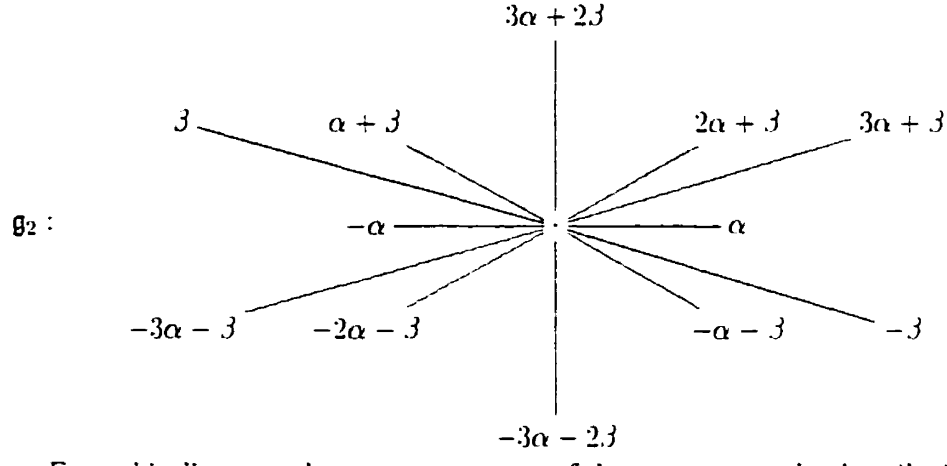
$\mathfrak{b}_3$: o —— o —>— o

Remark: The Lie group (which will be discussed in the next section) of $\mathfrak{a}_n$ is the special linear group $\mathrm{SL}_{n+1}(\mathbb{C})$. The Lie group of $\mathfrak{b}_3$ is the orthogonal group $O_7(\mathbb{C})$ consisting of orthogonal transformations.

From the Dynkin diagram. a complete diagram of the roots in $\mathfrak{g}_2$ can be constructed. The essential information for doing this is contained in Proposition 6.11. In particular. for roots α. β. then $\langle \alpha. \beta \rangle \in \mathbb{Z}$. But

$$\begin{aligned} \langle \alpha. \beta \rangle \langle \beta. \alpha \rangle &= 4 \frac{(\alpha. \beta)}{(\beta. \beta)} \frac{(\beta. \alpha)}{(\alpha. \alpha)} \\ &= 4 \frac{|\alpha|}{|\beta|} \cos\theta \frac{|\beta|}{|\alpha|} \cos\theta \\ &= 4 \cos^2 \theta \end{aligned}$$

where θ is the angle between α and β, and since this must be an integer, the possible values for θ are severely restricted. Since the values $\langle \alpha, \beta \rangle$ for simple roots α, β are evident from either a Dynkin diagram or a Cartan matrix, then the configuration of the simple roots is easily determined. Then by reflecting through planes orthogonal to the simple roots, one can generate the complete root set. In the case of $\mathfrak{g}_2$, there are two simple roots of unequal weights. The short root will be labelled α, and the long root β. From the Cartan matrix or the Dynkin diagram, it is seen that $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle = 3$, so from the above equation, $\cos\theta = \sqrt{3}/2$, and $\theta = 5\pi/6$. From this information, the entire root diagram can be constructed.



From this diagram, the symmetry group of the root set may be described.

Proposition 6.20 *The Weyl group of $\mathfrak{g}_2$ is the dihedral group $\mathcal{D}_6$ of order* 12.

To each root r, there corresponds a one-dimensional root subspace L_r of $\mathfrak{g}_2$, and by the Cartan decomposition, one thus has

$$\mathfrak{g}_2 = \mathcal{H} \oplus \sum_{i=1}^{12} L_{r_i}$$

where the sum is over the twelve roots r_i. Thus, since $\mathcal{H}$ is 2-dimensional over $\mathbb{C}$, $\mathfrak{g}_2$ is a 14-dimensional Lie algebra over $\mathbb{C}$.

6.4 Lie Groups

To each Lie algebra is naturally associated its Lie group, a family of automorphisms of the Lie algebra. Lie groups may also be characterized intrinsically: see [War83].

A linear map D from L to L is a *derivation* if it satisfies the product rule $D(fg) = fD(g) + D(f)g$. A derivation D is *nilpotent* if $D^n = 0$ for some n. For a nilpotent derivation, $\exp(D)$ is well-defined.

Definition 6.21 *For a nilpotent derivation D, its* exponential *is defined by*

$$\exp(D) = 1 + D + \frac{D^2}{2} + \frac{D^3}{3!} + \frac{D^4}{4!} \cdots$$

If $x \in L$, then $\mathrm{ad}x$ is a nilpotent derivation.

Proposition 6.22 *If D is a nilpotent derivation of L, then* $\exp(D)$ *is an automorphism of L.*

In particular, $\exp(\mathrm{ad}x_\alpha) \in \mathrm{Aut}L$, where x_α is in the Chevalley basis. For notational convenience write $X_\alpha(t)$ for $\exp(\mathrm{ad}(tx_\alpha))$ for each x_α, and any $t \in \mathbb{C}$. Fix a root α: then the group $\{X_\alpha(t) : t \in \mathbb{C}\} \cong \mathbb{C}$ since $X_\alpha(t)X_\alpha(u) = X_\alpha(t+u)$.

The Lie groups can now be defined.

Definition 6.23 *The* Lie Group *G associated to the simple Lie Algebra L is the subgroup of* $\mathrm{Aut}L$ *generated by $\{X_\alpha(t)\}$ for all roots α, all $t \in \mathbb{C}$.*

6.5 Defining Groups of Lie Type

From the Lie groups of simple Lie algebras, Chevalley was able to construct analogous families of finite groups, the *Chevalley Groups*. All have trivial center, and most are simple groups.

Theorem 6.15 establishes that the bracket product of two Chevalley basis elements can be expressed as an integral linear combination of basis elements. Write $L_{\mathbb{Z}}$ for the subset of L consisting of $\mathbb{Z}$-linear combinations of elements

in the Chevalley basis. By Theorem 6.15, $L_{\mathbb{Z}}$ is a Lie algebra over $\mathbb{Z}$. Let K be a finite field. Then $K \otimes_{\mathbb{Z}} L_{\mathbb{Z}}$ is a vector space over K. If $\{e_i\}$ is the Chevalley basis for L, then the set $\{1 \otimes e_i\}$ is a basis for $K \otimes L_{\mathbb{Z}}$. Defining a bracket product by $[1 \otimes x, 1 \otimes y] = 1 \otimes [x, y]$ makes $K \otimes L_{\mathbb{Z}}$ into a Lie algebra over K, which will be denoted L_K.

To define the associated Lie type group, one again considers families of automorphisms of the Lie algebra L_K arising from $\mathrm{ad}x_\alpha$. First, it can be shown that $(\mathrm{ad}x_\alpha)^m/m!$ stabilizes $L_{\mathbb{Z}}$. Since $\mathrm{ad}x_\alpha$ is nilpotent, $\exp(\lambda x_\alpha)$ acts on $L_{\mathbb{Z}} \otimes \mathbb{Z}[\lambda]$ where λ is an indeterminate. Thus $\exp(\lambda x_\alpha)$ acts on $L_{\mathbb{Z}} \otimes \mathbb{Z}[\lambda] \otimes K$, and by letting $\lambda \to t$, $\exp(\lambda x_\alpha)$ acts on L_K. As in the complex case, write $X_\alpha(t)$ for $\exp(\mathrm{ad}(t x_\alpha))$ for each x_α in the Chevalley basis and for $t \in K$. One may now define families of centerless finite groups for each simple Lie algebra.

Definition 6.24 *The* Chevalley Group *of the Lie algebra L over the finite field K is the group generated by all of the $X_\alpha(t)$ for nonzero simple roots α, and $t \in K$.*

Definition 6.25 *The group $G_2(q)$ is the Chevalley group of the Lie algebra $\mathfrak{g}_2$ over the field $\mathbb{F}_q$.*

6.6 Structure of Lie Type Groups

Let G be a finite group of Lie type, arising from the Lie algebra L. Let K be a finite field of characteristic p. Fix a root α. Then $X_\alpha(t+u) = X_\alpha(t)X_\alpha(u)$. Hence $\{X_\alpha(t) : t \in K\} \cong K$ as an additive group.

Definition 6.26 *The* root subgroup χ_α *of* G *attached to* α *is the subgroup* $\{X_\alpha(t) : t \in K\}$.

Root subgroups are abelian since they are isomorphic to the additive group of K. Any Chevalley group is evidently generated by its root subgroups.

For any root r, the subgroup $\langle X_r(1), X_{-r}(1)\rangle$ is closely related to $\mathrm{SL}_2(K)$ as follows.

Theorem 6.27 *There is a surjective homomorphism* ϕ *from* $\mathrm{SL}_2(K)$ *onto the subgroup* $\langle X_r(1), X_{-r}(1)\rangle$ *of* G, *under which*

$$\phi : \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \to X_r(t)$$

$$\phi : \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \to X_{-r}(t)$$

Define

$$h_\alpha(t) = X_\alpha(t)X_{-\alpha}(-t^{-1})X_\alpha(t)X_\alpha(-1)X_{-\alpha}(1)X_\alpha(-1) \tag{6.28}$$

Carrying out the relevant matrix calculation, one observes from the above theorem that the $h_\alpha(t)$ are the images of the diagonal matrices

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

Then $h_\alpha(tu) = h_\alpha(t)h_\alpha(u)$, so $H_\alpha := \{h_\alpha(t) : t \in K\}$ is a homomorphic image of K^*.

Definition 6.29 *The* Cartan subgroup H *of* G *is the subgroup of* G *generated by all of the* H_α*, for roots* α*.*

The Cartan subgroup is abelian, and normalizes each root subgroup. Define N to be the normalizer of H in G.

Theorem 6.30 $W \cong N/H$ *where* W *is the Weyl group of the Lie algebra* L*.*

Define P to be the p-Sylow subgroup of G generated by the χ_α for positive roots α. Using the product relations in, say, Theorem 6.15, one deduces that

$X_r(t) - 1$ is nilpotent on the Lie algebra, so that $X_r(t)$ is unipotent. Indeed, any element of order a p-power in G is unipotent.

Definition 6.31 *The* Borel subgroup B *of* G *is* HP, *for the Cartan subgroup* H, *and the p-Sylow subgroup* P.

The Borel subgroup B is the normalizer of P in G.

The group G can be decomposed with respect to a Borel subgroup and its Weyl group, as follows. A Weyl group W is a *Coxeter group*: that is, there is a *defining set* $\{w_1, \ldots, w_m\}$ of involutions which generate W, and the set of all relations $(w_i w_j)^{k_{ij}} = 1$ defines W, where k_{ij} is the order of $w_i w_j$. The number m is the *Lie rank* of G. Recall Theorem 6.30: for each i fix a lifting n_i to N of the defining reflections w_i of W. The Weyl group acts on the root set. Define for each $w \in W$ the subset of the positive roots by Ψ_w^- consisting of all positive roots reflected by w to negative roots. Define $P_w^- = \prod_{r \in \Psi_w^-} \chi_r$. A theorem of Bruhat describes the structure of G in terms of B and N.

Theorem 6.32 (Bruhat Decomposition) *1.* $B \cap N = H$

2. $G = BNB$

3. *For any $n \in N$ and any i,*

$$BnBn_iB \subseteq (BnB) \cup (Bnn_iB)$$

4. *For any i, $n_iBn_i \neq B$.*

5. *For every $w \in W$, fix a lift n_w of w to N. Each element $g \in G$ may be expressed in a unique way as a product bn_wp_w, where $b \in B$, $w \in W$ and $p_w \in P_w^-$.*

One can gain considerable information about maximal subgroups of G from the corresponding Dynkin diagram. First, make the following definition.

Definition 6.33 *A* parabolic subgroup *of G is a proper subgroup of G containing a Borel subgroup.*

Let Y be a parabolic subgroup of G. Let $\mathcal{O} = O_p(Y)$ be the largest normal p-subgroup of Y, where p is the characteristic of $\mathbb{F}$. Let $\overline{Y} = Y/\mathcal{O}$.

Theorem 6.34

$$\overline{Y} = \overline{H}\,\overline{Y_1}\ldots\overline{Y_r}$$

where $\overline{Y_i} \lhd \overline{Y}$ *for all* i*, and each* $\overline{Y_i}$ *is a Chevalley group over some field of characteristic* p*.*

The $\overline{Y_i}$ are called *Levi factors* of the parabolic subgroup Y. It is possible to determine all of the parabolic subgroups of G from its Dynkin diagram.

Theorem 6.35 *There is a bijection between proper subgraphs of the Dynkin diagram* D *and parabolic subgroups* Y *of* G *containing a fixed Borel subgroup* B*.*

A parabolic subgroup corresponding to a single node of the Dynkin diagram is called a *minimal parabolic subgroup*. Fix a parabolic subgroup Y and its corresponding subgraph S of D.

Theorem 6.36 *There is a bijection between the Levi factors of* Y *and the connected components of* S*. Each Levi factor is a Lie type group: its Dynkin diagram is the component of* S *determined in this bijection.*

Minimal parabolic subgroups generate G. Fix a Borel subgroup B.

Theorem 6.37 *If the Lie rank of* G *is at least 2, then* G *is generated by all of the minimal parabolic subgroups containing* B*.*

The following theorem will be referred to.

Theorem 6.38 (Borel-Tits Theorem) *If J is a maximal p-local subgroup of G, then J is a parabolic subgroup.*

There is the following useful formula, which permits calculation in a Chevalley group. Let γ and δ be linearly independent roots.

Theorem 6.39 (Chevalley Commutator Formula)

$$[X_\delta(t), X_\gamma(u)] = \prod_{i,j>0} X_{i\gamma+j\delta}(C_{ij\gamma\delta}(-t)^i u^j)$$

where the product is taken over all i, j such that $i\gamma + j\delta$ is a root, and is taken in order of increasing $i + j$. The constants $C_{ij\gamma\delta}$ are nonzero integers, $|C_{ij\gamma\delta}| \leq 3$, and are defined as follows:

$$\begin{aligned} C_{i1\gamma\delta} &= M_{\gamma,\delta,i} \\ C_{1j\gamma\delta} &= M_{\delta,\gamma,j} \\ C_{32\gamma\delta} &= \frac{1}{3} M_{\gamma+\delta,\gamma,2} \\ C_{23\gamma\delta} &= -\frac{2}{3} M_{\delta+\gamma,\delta,2} \end{aligned}$$

where $M_{r,s,n} = \frac{1}{n!} N_{r,s} N_{r,r+s} \dots N_{r,(n-1)r+s}$ where the $N_{r,s}$ are the structure constants of L. The list gives all possible values for C_{ijrs} by the classification

theory of simple Lie algebras.

As has been discussed, any Chevalley group is generated by its root elements $X_r(1)$ for roots r. A theorem of Steinberg establishes that the relations already described in this chapter are sufficient to give a definition of a Chevalley group by generators and relations.

Theorem 6.40 (Steinberg's Theorem) *Let R be the root set of a simple Lie algebra L. $L \neq \mathfrak{a}_1$. and for each $r \in R$ and each $j \in \mathbb{F}$ define a symbol $X_r(j)$. Further define $h_r(i)$ as in equation (6.28). Let $\tilde{G}$ denote the group generated by the $X_r(j)$ with the relations*

$$X_r(i)X_r(j) = X_r(i+j)$$

$$h_r(i)h_r(j) = h_r(i \cdot j)$$

and the Chevalley commutator relations with structure constants determined by L. Then $\tilde{G}/Z(\tilde{G})$ is isomorphic to the Chevalley group of L over the field $\mathbb{F}$.

6.7 Theory of Finite Simple Groups

By the classification theorem of finite simple groups, completed in 1980, it is known that virtually every finite simple group is a Lie type group.

Theorem 6.41 (Classification of Finite Simple Groups) *If G is a finite simple group, then G is one of the following:*

1. *An alternating group A_n;*
2. *A group of Lie type;*
3. *One of the 26 sporadic groups.*

From this classification, many theorems about simple groups may be proved by exhaustive verification. One example of such a theorem is the following:

Theorem 6.42 *Every finite simple group has a presentation with exactly two generators.*

No conceptual proof is known (see [Gor82]). Evidently, in order to find a rigid triple of conjugacy classes in a given finite group, it is necessary that G be generated by two elements. In this sense, Theorem 6.42 provides some justification for the Remark following Theorem 3.17.

7 Rigidity and Rationality for $G_2(p)$

7.1 The Structure of $G_2(p)$

In order to use rigidity and rationality criteria to realize $G_2(p)$ as a Galois group over $\mathbb{Q}$, it suffices to have information about

1. the conjugacy classes of $G_2(p)$;

2. the irreducible representations of $G_2(p)$ and their characters; and

3. the subgroups of $G_2(p)$.

First, the results from the preceding chapter are applied to $G_2(p)$ in order to illuminate its structure.

As the Weyl group of $G_2(p)$ is the symmetry group of the root diagram of $\mathfrak{g}_2$, one has

Proposition 7.1 *The Weyl group of $G_2(p)$ is the dihedral group $\mathcal{D}_6$ of order 12.*

With this, the Bruhat decomposition may be used to determine the order of $G_2(p)$.

Proposition 7.2

$$|G_2(p)| = p^6(p^6 - 1)(p^2 - 1)$$

Proof: By Theorem 6.32, each element of $G_2(p)$ can be expressed uniquely as the product of an element in B and an element in P_w^-, for a unique $w \in W$. Thus,

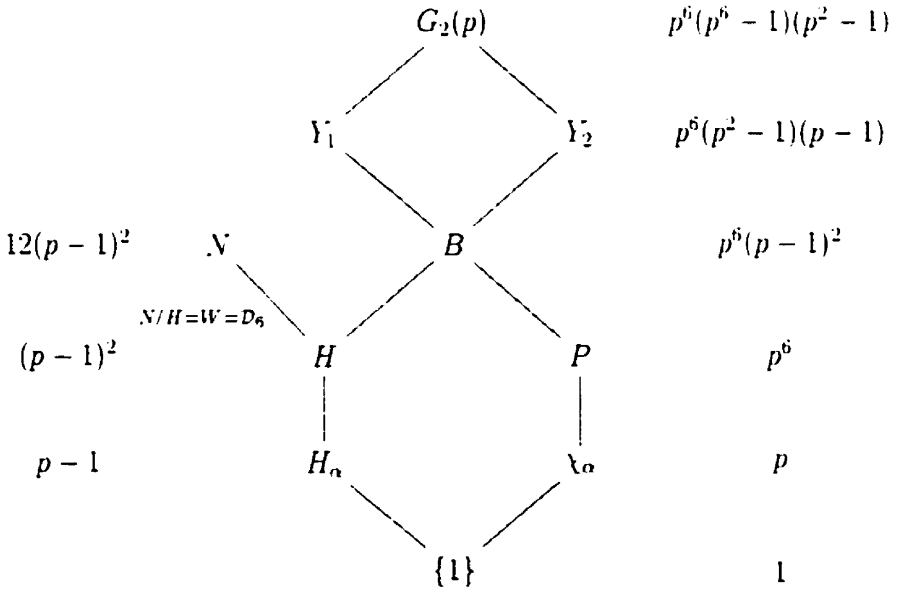
$$\begin{aligned} |G_2(p)| &= \sum_{w \in W} |B| \cdot |P_w^-| \\ &= p^6(p-1)^2 \sum_{w \in W} |P_w^-| \end{aligned}$$

The orders $|P_w^-|$ can be easily computed for each w: one has $|P_w^-| = p^{n(w)}$ where $n(w)$ is the number of positive roots which w maps to negative roots. Thus,

$$\begin{aligned} |G_2(p)| &= p^6(p-1)^2(p^6 + 2p^5 + 2p^4 + 2p^3 + 2p^2 + 2p + 1) \\ &= p^6(p^6 - 1)(p^2 - 1) \end{aligned}$$

□

Using the information from section 6.6. one may deduce the following diagram of some of the significant subgroups of $G_2(p)$. Each of the subgroups is indicated along with its order.



Many of these subgroups can be defined in terms of the generators of $G_2(p)$. Let Φ^+ denote the set of positive roots of $\mathfrak{g}_2$, with α and β the short

and long simple roots respectively. Then

$$\begin{aligned} H &\cong \langle h_\alpha, h_\beta \rangle \cong C_{p-1} \times C_{p-1} \\ P &\cong \langle X_r(1), r \in \Phi^+ \rangle \\ B &\cong \langle X_r(1), h_r, r \in \Phi^+ \rangle \\ Y_1 &\cong \langle X_{-\alpha}, X_r(1), h_r, r \in \Phi^+ \rangle \\ Y_2 &\cong \langle X_{-\beta}, X_r(1), h_r, r \in \Phi^+ \rangle \end{aligned}$$

Furthermore, the subgroups $\langle \chi_r, \chi_{-r} \rangle$ are isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$, and the group $\langle \chi_r, r \in \{\text{long roots}\} \rangle$ is isomorphic to $\mathrm{SL}_3(\mathbb{F}_p)$ as can be seen by the corresponding embedding in the Lie algebra.

This completes the investigation of the subgroups of $G_2(p)$. Here some elementary results about the conjugacy classes of $G_2(p)$ are summarized: they will be proved in section 9. First, the involutions in $G_2(p)$ form a single conjugacy class. This will be denoted by C_i. The unipotent class containing $X_\alpha(1)$ will be denoted C_α, and $C_{\alpha\beta}$ will denote the class containing $X_\alpha(1)X_\beta(1)$. The class $C_{\alpha\beta}$ is also unipotent, and consists of elements of order p when $p > 5$. The elements $X_\alpha(1)$ and $X_\alpha(1)X_\beta(1)$ are not conjugate, so these classes are distinct. Below, the characters of $G_2(p)$ which are simultaneously

nonzero on C_t. C_a and C_{aJ} are tabulated with their values. These are the only characters which make a nontrivial contribution to the sum in formula (3.19). which will be used below to establish that these conjugacy classes form a rigid triple in $G_2(p)$. Define d. e so that $e = \pm 1$. $e \equiv p \mod 3$. $d = \pm 1$. $d \equiv p \mod 4$. The following tables are taken from [FF84]: the notation for the characters has not been changed.

	1	C_t	C_α	$C_{\alpha 3}$
χ_{id}	1	1	1	1
χ_{32}	p^3+e	$p+e$	$p+e$	e
χ_{22}	$\frac{p^6-1}{p^2-1}$	$2dp+1$	p^2+1	1
$\chi_1(\pi_1)$	$\frac{(p^6-1)(p^2-1)}{(p+1)^2}$	$3(p+1)^2$	$(p+1)(2p+1)$	1
$\chi_1(\pi_1)^*$	$\frac{(p^6-1)(p^2-1)}{(p+1)^2}$	$-(p+1)^2$	$(p+1)(2p+1)$	1
$\chi_2(\pi_2)$	$\frac{(p^2-1)(p^6-1)}{(p+1)^2}$	$3(p-1)^2$	$(p-1)(2p-1)$	1
$\chi_2(\pi_2)^*$	$\frac{(p^2-1)(p^6-1)}{(p+1)^2}$	$-(p-1)^2$	$(p-1)(2p-1)$	1
$\chi_a(\pi_a)$	p^6-1	p^2-1	$-p-1$	-1
$\chi_a(\pi_a)^*$	p^6-1	$-(p^2-1)$	$-p-1$	-1
$\chi_b(\pi_b)$	p^6-1	p^2-1	$p-1$	-1
$\chi_b(\pi_b)^*$	p^6-1	$-(p^2-1)$	$p-1$	-1
$\chi'_{1a}(\pi_1,\pi_a)$	$\frac{p^6-1}{p-1}$	$(p+2)(p+1)$	$(p+1)^2$	1
$\chi'_{1a}(\pi_1,\pi_a)^*$	$\frac{p^6-1}{p-1}$	$-p(p+1)$	$(p+1)^2$	1
$\chi'_{1b}(\pi_1,\pi_b)$	$\frac{p^6-1}{p-1}$	$(p+2)(p+1)$	p^2+p+1	1
$\chi'_{1b}(\pi_1,\pi_b)^*$	$\frac{p^6-1}{p-1}$	$-p(p+1)$	p^2+p+1	1
$\chi'_{2a}(\pi_2,\pi_a)$	$\frac{p^6-1}{p+1}$	$-(p-2)(p-1)$	$-p^2+p-1$	-1
$\chi'_{2a}(\pi_2,\pi_a)^*$	$\frac{p^6-1}{p+1}$	$p(p-1)$	$-p^2+p-1$	-1
$\chi'_{2b}(\pi_2,\pi_b)$	$\frac{p^6-1}{p+1}$	$-(p-2)(p-1)$	$-(p-1)^2$	-1
$\chi'_{2b}(\pi_2,\pi_b)^*$	$\frac{p^6-1}{p+1}$	$p(p-1)$	$-(p-1)^2$	-1

Some of these characters occur more than once: their number is indicated below:

	$\#\{\chi\}$
$\chi_1(\pi_1)$	$\frac{1}{18}(p^2 - 14p + 47 + 6d + 8e)$
$\chi_1(\pi_1)^*$	$\frac{1}{18}(3p^2 - 18p + 21 - 6d)$
$\chi_2(\pi_2)$	$\frac{1}{18}(p^2 - 10p + 23 - 6d - 8e)$
$\chi_2(\pi_2)^*$	$\frac{1}{18}(3p^2 - 6p - 3 + 6d)$
$\chi_a(\pi_a)$	$\frac{1}{8}(p^2 - 4p + 3)$
$\chi_a(\pi_a)^*$	$\frac{1}{8}(p^2 - 1)$
$\chi_b(\pi_b)$	$\frac{1}{8}(p^2 - 4p + 3)$
$\chi_b(\pi_b)^*$	$\frac{1}{8}(p^2 - 1)$
$\chi'_{1a}(\pi_1, \pi_a)$	$\frac{1}{4}(p - 6 - 2e - d)$
$\chi'_{1a}(\pi_1, \pi_a)^*$	$\frac{1}{4}(p - 2 + d)$
$\chi'_{1b}(\pi_1, \pi_b)$	$\frac{1}{4}(p - 4 - d)$
$\chi'_{1b}(\pi_1, \pi_b)^*$	$\frac{1}{4}(p - 2 + d)$
$\chi'_{2a}(\pi_2, \pi_a)$	$\frac{1}{4}(p - 2 + d)$
$\chi'_{2a}(\pi_2, \pi_a)^*$	$\frac{1}{4}(p - d)$
$\chi'_{2b}(\pi_2, \pi_b)$	$\frac{1}{4}(p - 4 + 2e + d)$
$\chi'_{2b}(\pi_2, \pi_b)^*$	$\frac{1}{4}(p - d)$

The sizes of the conjugacy classes will also be required in order to use (3.19), and are summarized below; centralizers of representative elements from each class are computed in Section 9. One has

$$\begin{aligned} |C_1| &= p^1(p^2+p+1)(p^2-p+1) \\ |C_a| &= p^2(p^6-1) \\ |C_{a3}| &= p^1(p^6-1)(p^2-1) \end{aligned}$$

Remark. The class C_{a3} is called a *regular* class of unipotents; that is, it is the unique conjugacy class of unipotents of largest order in $G_2(p)$, and comes from the unique class of unipotents in the algebraic group G_2 of maximal dimension.

7.2 A Rigid Class Vector

Here a rigid and rational class vector in the finite simple group $G_2(p)$, $p > 5$, is exhibited, establishing that it occurs as a Galois group over $\mathbb{Q}$. The first published proof of this result appeared in [FF84].

Theorem 7.3 *The vector $v = (C_1, C_a, C_{a3})$ is a rational class vector for $G_2(p)$ for all primes $p > 5$.*

Proof: The class C_i is rational by Proposition 3.10. There are several ways to prove that the unipotent classes are rational. It is not difficult to explicitly calculate elements g for which $gug^{-1} = u^t$, where $u = X_\alpha(1)$ or $u = X_\alpha(1)X_\beta(1)$. Alternatively, the character table shows that $\chi(C_i) \in \mathbb{Q}$ for all irreducible characters χ. □

Theorem 7.4 *The vector $v = (C_i, C_\alpha, C_{\alpha\beta})$ is a rigid class vector for $G_2(p)$ for all primes $p > 5$.*

Let S_v denote the set of triples (g_1, g_2, g_3) with $g_i \in C_i$ satisfying that $g_1g_2g_3 = 1$. The proof will proceed in two steps. First it is established from the character table that there is one orbit of triples in S_v under conjugation by $G_2(p)$. In proving this result from the character table, one encounters difficulty presenting the explicit calculation because of its length. One may greatly condense the proof by using estimates for some of the terms that appear in the character sum. The cost of using these estimates as done below comes in a restriction of the validity of the proof to those primes $p > 19$. It should be emphasized, however, that this is only done for ease of presentation, and the result indeed holds for all $p \geq 7$: see [FF84]. The proof that the triples generate $G_2(p)$ was first given in [FF84], and requires

a detailed knowledge of simple group theory. This part of the proof is only summarized.

1. The number of triples in S_v is $|G_2(p)|$.

Proof: By the character table and formula (3.19), then

$$|S_v| = \frac{|C_t||C_\alpha||C_{\alpha\beta}|}{|G|} \sum_\chi \frac{\chi(C_t)\chi(C_\alpha)\chi(C_{\alpha\beta})}{\chi(1)}$$

It must be shown that $|S_v|/|G| = 1$. As $|S_v|/|G|$ counts the number of orbits in S_v under conjugation by G, then $|S_v|/|G|$ must be an integer. Temporarily, let $\mathcal{N}$ denote the character sum on the right hand side of the equation above. Substituting the sizes of the conjugacy classes and $|G|$,

$$\frac{|S_v|}{|G|} = \frac{p^1(p^6-1)(p^2-1)p^4(p^2-p+1)p^2(p^6-1)}{p^{12}(p^6-1)^2(p^2-1)^2} \cdot \mathcal{N} \qquad (7.5)$$

$$= \frac{(p^2+p+1)(p^2-p+1)}{p^2(p^2-1)} \cdot \mathcal{N} \qquad (7.6)$$

In order to evaluate $\mathcal{N}$, associate the following functions to the characters of $G_2(p)$. To those characters which occur in pairs χ and χ^*, associate the function

$$n_{\chi,\chi^*}(p) := \frac{\chi(C_\alpha)\chi(C_{\alpha\beta})[\chi(C_t)(\#\chi) + \chi^*(C_t)(\#\chi^*)]}{\chi(1)} \qquad (7.7)$$

One observes in the table that χ and χ^* always take on the same value on the classes C_a and C_{a3}, so n_{χ,χ^*} takes on the value

$$n_{\chi,\chi^*}(p) := \frac{\chi(C_a)\chi(C_{a3})\chi(C_t)(\#\chi) + \chi^*(C_a)\chi^*(C_{a3})\chi^*(C_t)(\#\chi^*)}{\chi(1)} \tag{7.8}$$

which appears in character sum in N. For the isolated characters χ_{22}, χ_{32} and χ_{11} for which $\#\chi = 1$, let $n_\chi(p)$ serve as an abbreviation for $\frac{\chi(C_t)\chi(C_a)\chi(C_{a3})}{\chi(1)}$. Hence

$$N = \sum_{(\chi,\chi^*)} n_{\chi,\chi^*}(p) + \sum_{\chi} n_\chi(p) \tag{7.9}$$

It will be seen that the main contribution to N comes from the trivial character in the second sum. This will be demonstrated by using estimates to bound all of the other summands. First the second sum over the isolated characters is considered. By explicit calculation, one finds

$$\begin{aligned}
\sum_{\chi} n_\chi(p) &= 1 + \frac{e(p+e)^2}{p^3+e} + \frac{(p^4-1)(2dp+1)}{p^6-1} \\
&= 1 + \frac{e(p+e)^2(p^3-e) + (p^4-1)(2dp+1)}{p^6-1} \\
&= 1 + \frac{(2d+e)p^5 + (4d+1)p^4 + p^3 + (-2d)p^2 + p - 1 - e}{p^6-1}
\end{aligned}$$

In order to bound this in absolute value, observe that it is maximized for $e = d = 1$ and that the coefficients of p are all less than or equal to five. Hence the sum of terms of fourth degree and lower can be bounded by $p^5 - 1$, since $p > 5$. Hence

$$\left| \sum_{\chi} n_{\chi}(p) \right| \leq 1 + \frac{4}{p} \tag{7.10}$$

That is, the sum over the isolated characers is $1 + O(1/p)$. Next considering the paired characters χ, χ^*, one observes immediately for $\chi_a(\pi_a)$ and $\chi_b(\pi_b)$ that the numerator in n_{χ,χ^*} is of degree at most five, while the denominator is of degree six. Closer inspection indicates that the degree five terms cancel in the numerator, and one is then able to easily estimate for these characters that $|n_{\chi,\chi^*}| < \frac{2}{p^2}$.

Now for the remaining pairs of characters, n_{χ,χ^*}, one finds summands of equally high degree in the numerator and denominator. However, in each case the highest degree terms in the numerator cancel, permitting one to deduce the existence of a constant c_χ for which $|n_{\chi,\chi^*}| < \frac{c_\chi}{p}$. This is already sufficient to deduce that $0 < N < 3/2$ if p is chosen large enough to dominate all of the c_χ, ensuring that $|S_r|/|G| = 1$, since this value must be an integer. In order to

deduce the least p for which the result applies, it is necessary to estimate each of the $n_{\chi,\chi'}$. This has been done naïvely below, proceeding with techniques analogous to those used in (7.10), computing the nonvanishing term of highest degree in the numerator and bounding the numerator's remaining terms. One arrives at the following bounds:

$$\begin{aligned}
|n_{\chi'_{1a},\chi'_{1a}}| &< \frac{3}{p} \\
|n_{\chi'_{1b},\chi'_{1b}}| &< \frac{2}{p} \\
|n_{\chi'_{2a},\chi'_{2a}}| &< \frac{2}{p} \\
|n_{\chi'_{2b},\chi'_{2b}}| &< \frac{3}{p} \\
|n_{\chi'_1,\chi'_1}| &< \frac{2}{p} \\
|n_{\chi'_2,\chi'_2}| &< \frac{3}{p}
\end{aligned}$$

where the labels for the characters have been abbreviated. Hence, substituting all of these estimates into (7.9), writing $M = N - 1$,

$$\begin{aligned}
|M| &< \frac{4}{p} + \frac{4}{p^2} + \frac{15}{p} \\
&< \frac{20}{p}
\end{aligned}$$

since by assumption $p \geq 7$. In order to use this result, a rough estimate is required for $T := \frac{(p^2+p+1)(p^2-p+1)}{p^2(p^2-1)}$ which appears in (7.5). One has $T = \frac{p^4+p^2+1}{p^4-p^2}$ so

$$\begin{aligned} 1 < T &< 1 + \frac{1}{p^2}\left(\frac{2p^2+1}{p^2-1}\right) \\ &< 1 + \frac{1}{p^2}\left(\frac{2(p+1)}{p-1}\right) \\ &< 1 + \frac{3}{p^2} \end{aligned}$$

again using that $p \geq 7$. Now, $|S_v|/|G| = \mathcal{N}T$: the above estimates can be combined as follows:

$$\begin{aligned} \mathcal{N} < \mathcal{N}T &< \mathcal{N}\left(1 + \frac{3}{p^2}\right) \\ 1 - \frac{20}{p} < \mathcal{N}T &< \left(1 + \frac{20}{p}\right)\left(1 + \frac{3}{p^2}\right) \end{aligned}$$

From this, one deduces that, for $p \geq 23$

$$0 < \mathcal{N}T < 2$$

Since $\mathcal{N}T = |S_v|/|G|$ is an integer, this forces $\mathcal{N}T = 1$. □

To prove the result for $7 \leq p \leq 19$ one can either improve the above estimates or carry out the explicit calculation of NT. One finds that $NT = 1$ (see [FF84], p. 323).

2. Each triple in S_v generates $G_2(p)$.

Summary of Proof: The complete proof appears in [FF84], but requires a detailed knowledge of finite group theory. The proof proceeds as follows: let $(g_1, g_2, g_3) \in S_v$. First, one establishes that the group $J = \langle g_1, g_2, g_3 \rangle$ is not p-local. By Theorem 6.38, J would then be contained in a parabolic Y. Indeed J is contained in the subgroup Y'' of Y generated by its p-order elements. The Levi decomposition allows one to determine the structure of $Y''/O_p(Y'')$. The image $\overline{g_1}$ of the involution g_1 in $Y''/O_p(Y'')$ is then determined to be central of order 2, which forces $\overline{g}_1\overline{g}_2\overline{g}_3 \neq 1$.

Next one shows that J is not q-local for any prime q different from p. Here information is required about q-subgroups of $G_2(p)$ and its subgroups. One uses this data and an analysis for q even and odd to show that p cannot divide the order of the normalizer of an elementary abelian q-subgroup of J.

Once it is known that J is not a local subgroup, it can be established that J is simple. First one shows that a minimal normal subgroup N of J is simple, with trivial centralizer, so that $J \subseteq \mathrm{Aut}N$. Then the classification

theory of finite simple groups is invoked in order to enumerate the possible structures of $\mathrm{Aut}N$ in order to establish that the index of N in $\mathrm{Aut}N$ is either too small to be divisible by p or is a power of q. Since p divides $|J|$ this forces $N = J$.

Finally, having demonstrated J is simple, the classification theory of finite simple groups is again used: one lists each of the finite simple groups and for each such group S, one identifies a structural feature present in J and absent in S or vice versa, forcing $S \neq J$. For only one S is it impossible to do this, namely $G_2(p)$. □

An immediate corollary of Theorems 7.3 and 7.4, by Theorem 3.17, is

Corollary 7.11 *$G_2(p)$ is a Galois group of a regular extension of $\mathbb{Q}(t)$ for all primes $p > 5$.*

And, by Theorem 3.21,

Corollary 7.12 *If $p > 5$ is a prime, then $G_2(p)$ is the Galois group of some normal field extension of $\mathbb{Q}$.*

In fact, the restriction on p may be relaxed. Thompson has shown that Σ_v is a rigid and rational triple for $G_2(5)$, although there is a slight variation required in the proof, in part because $|C_{ab}| = 25$ when $p = 5$ ([Tho84]).

$G_2(3)$ is also known to be a Galois group over $\mathbb{Q}$. Thus, $G_2(p)$ is a Galois group over $\mathbb{Q}$ for all primes $p \neq 2$.

8 Geometric Interpretations

Since it can be established that $v_p = (C_t, C_a, C_{aA})$ is a rigid class vector in $G_2(p)$ for all primes $p > 5$, one might ask whether this triple "lifts" to the group $G = G_2(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}])$. As in section 5.1, there are homomorphisms $\rho_p : G \to G_2(p)$ for all $p > 5$. Since it is possible to prove in a uniform way for $p > 5$ that the class vector is rigid, one might hope to find a "global triple" v in G which reduces mod p to give v_p for all $p > 5$. There are structural deviations in $G_2(p)$ for $p = 2, 3$ and 5 that suggest that these primes need to be inverted, as $G_2(2)$ is not simple, $G_2(3)$ has a non-trivial outer automorphism, and in $G_2(5)$ elements in the regular unipotent class C_{aA} have order $p^2 = 25$. The first question one might attempt to answer is the following.

Question 1 *For all primes $p > 5$, does the rigid vector v lifts via ρ_p to a rigid triple of conjugacy classes in G?*

That is, one asks whether the vector v in $G_2(p)$ arises from reduction mod p of a vector in G.

If the above question has an affirmative answer, then with the rigidity theorem one can prove from Theorem 7.4 that there are homomorphisms ϕ_{ℓ^n}

for each prime $\ell > 5$, and for all n

$$\rho_{\ell^n} : G_{\mathbb{Q}(t)} \to G_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

and hence an ℓ-adic representation

$$\rho_{\ell^\infty} : G_{\mathbb{Q}(t)} \to G_2(\mathbb{Z}_\ell)$$

Specializing these homomorphisms at some $t = t_0$ produces ℓ-adic representations of $G_{\mathbb{Q}}$, which shall be denoted by ψ_ℓ.

$$\psi_\ell : G_{\mathbb{Q}} \to G_2(\mathbb{Z}_\ell)$$

These representations arise from the existence of a rigid triple in $G_2(\mathbb{Z}_\ell)$, and in fact $G_2(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}])$. One is led to ask:

Question 2 *Do the homomorphisms ψ_ℓ form a strictly compatible system of ℓ-adic representations?*

If the answer to this question is affirmative, it would suggest that the system of representations arises from reduction mod ℓ on some underlying geometric object (it is conjectured that every strictly compatible system of

ℓ-adic representations has an underlying geometry in this sense). More precisely, one might ask

Question 3 *Is there a variety V over $\mathbb{Q}(t)$ and some $i \in \mathbb{N}$ such that the representations ϱ_ℓ occur as Jordan-Hölder constituents of $H^i_{\text{et}}(V_{\overline{\mathbb{Q}}(t)}, \mathbb{Q}_\ell)$ for each prime $\ell > 5$?*

9 On G_2.

In order to answer the questions of the preceding section, a new proof of rigidity for $G_2(p)$ would be required, as the character table formula does not provide the information required to lift the triple to $G_2(\mathbb{Q})$. Thompson has reportedly proved rigidity in a different way, with a lengthy calculation using generators and relations. It would be ideal to find an elegant proof of rigidity which relied on the geometric interpretation of $G_2(p)$, similar to the proof of Theorem 4.2 for $\mathrm{PSL}_2(\mathbb{F}_p)$. In the following, data about the conjugacy classes in the rigid triple from Theorem 7.4 is collected that would likely be used if such a proof were feasible for $G_2(p)$. It is assumed that the interpretation of G_2 as the automorphism group of the octonion algebra would be the key to such a proof. The goal is to identify geometric structures in $\mathbb{O}_p$ which characterize the relevant conjugacy classes.

9.1 A Representation of G_2

An irreducible seven-dimensional representation ρ of $G_2(p)$ can be described explicitly. Let e_{ij} denote the 7×7 matrix with a 1 in the $(i,j)^{\text{th}}$ position and zeros elsewhere. Assume that $w := \sqrt{2} \in \mathbb{F}_p$. Then a representation ρ

of $G_2(p)$ may be described as follows:

$$\begin{aligned}
\rho : X_\beta(1) &\mapsto \mathrm{Id} + e_{23} - e_{65} \\
\rho : X_{3\alpha+\beta}(1) &\mapsto \mathrm{Id} + e_{12} - e_{57} \\
\rho : X_{3\alpha+2\beta}(1) &\mapsto \mathrm{Id} + e_{43} - e_{67} \\
\rho : X_{-\beta}(1) &\mapsto \mathrm{Id} + e_{32} - e_{56} \\
\rho : X_{-3\alpha-\beta}(1) &\mapsto \mathrm{Id} + e_{24} - e_{75} \\
\rho : X_{-3\alpha-2\beta}(1) &\mapsto \mathrm{Id} + e_{34} - e_{76} \\
\rho : X_\alpha(1) &\mapsto \mathrm{Id} + e_{46} - e_{37} + we_{12} - we_{51} - e_{52} \\
\rho : X_{\alpha+\beta}(1) &\mapsto \mathrm{Id} + e_{27} - e_{45} + we_{13} - we_{61} - e_{63} \\
\rho : X_{2\alpha+\beta}(1) &\mapsto \mathrm{Id} - e_{53} + e_{62} - we_{41} + we_{17} - e_{47} \\
\rho : X_{-\alpha}(1) &\mapsto \mathrm{Id} - e_{64} + e_{73} - we_{21} + we_{15} - e_{25} \\
\rho : X_{-\alpha-\beta}(1) &\mapsto \mathrm{Id} - e_{72} + e_{54} - we_{31} + we_{16} - e_{36} \\
\rho : X_{-2\alpha-\beta}(1) &\mapsto \mathrm{Id} + e_{35} - e_{26} + we_{11} - we_{71} - e_{74}
\end{aligned}$$

One may verify that these satisfy the Chevalley commutator formula and the other relations in Theorem 6.40, establishing that the above matrix repre-

sentation is isomorphic to $G_2(p)$. The above representation was computed from a Lie algebra representation in [Hum72], pp. 103-104.

9.2 The Octonions

Possibly the most useful interpretation of $G_2(p)$ is as the automorphism group of the algebra of octonions $\mathbb{O}$ (often called *Cayley numbers*), defined over $\mathbb{F}_p$.

Recall that $\mathbb{C}$ may be constructed by defining a product on $\mathbb{R} \times \mathbb{R}$ as follows: $(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1 - y_2x_2, x_2y_1 + y_2x_1)$. The real quaternion algebra $\mathbb{H}$ may be constructed by defining a product on $\mathbb{C} \times \mathbb{C}$ by $(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1 - \overline{y_2}x_2, x_2\overline{y_1} + y_2x_1)$. Continuing this duplication procedure produces the octonion algebra.

Definition 9.1 *The real algebra of* octonions *is the set* $\mathbb{H} \times \mathbb{H}$ *with the product*

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1 - \overline{y_2}x_2, x_2\overline{y_1} + y_2x_1)$$

Defined in this way, $\mathbb{O}$ is a non-associative eight-dimensional division

algebra over $\mathbb{R}$. A natural basis for the octonion algebra is the set

$$\{(1,0),(i,0),(j,0),(k,0),(0,1),(0,i),(0,j),(0,k)\}$$

where $\{1,i,j,k\}$ is a basis for $\mathbb{H}$. The center $Z(\mathbb{O})$ of $\mathbb{O}$ is the one-dimensional subspace spanned by $(1,0)$.

As in $\mathbb{H}$, there is an analogue of complex conjugation. Let $(a,b) \in \mathbb{O}$. Then define conjugation in $\mathbb{O}$ as follows:

$$\overline{(a,b)} = (\bar{a},-b)$$

One defines the trace and norm on the octonions as follows:

$$\mathrm{Tr}(x) := x + \bar{x}. \quad \mathrm{N}(x) := x\bar{x}$$

The seven-dimensional space orthogonal to $Z(\mathbb{O})$ then consists of those octonions with trace 0. The trace and norm are related by the following formula, which may be proved directly from the definitions:

$$x^2 - \mathrm{Tr}(x)x + \mathrm{N}(x) = 0 \tag{9.2}$$

The bilinear form β of V is given by $\beta(x, y) = \frac{1}{2}(x\bar{y} + y\bar{x}) = \mathrm{Tr}(x\bar{y})$.

Let $\mathbb{O}_p$ denote the algebra of octonions, defined over the finite field $\mathbb{F}_p$. The theory becomes more complicated in this situation due to the presence of isotropic vectors, i.e. nonzero vectors v of norm 0. One observes from (9.2) that an isotropic v in the trace zero component of the octonions satisfies $v^2 = 0$. While $\mathbb{O}$ is a division algebra, $\mathbb{O}_p$ is not, as any isotropic is a nontrivial zero divisor. However, $\mathbb{O}_p$ is still *alternative*, that is, arbitrary elements x, y in $\mathbb{O}_p$ satisfy

$$x(xy) = x^2y \quad \text{and} \quad (xy)y = xy^2.$$

Theorem 9.3 *Let $p \geq 5$. The group of algebra automorphisms of $\mathbb{O}_p$ is isomorphic to $G_2(p)$.*

Indeed, in ([Hum72], p. 105) a correspondence is produced between the seven-dimensional representation described in section 9.1 and the action of $G_2(p)$ on the seven-dimensional complement of $Z(\mathbb{O}_p)$.

9.3 The Automorphisms of $\mathbb{O}_p$

By an automorphism of $\mathbb{O}_p$ it will be meant an algebra automorphism. First, one may observe that any automorphism of $\mathbb{O}_p$ will preserve the bilinear form on the octonions, and from this deduce that the octonion automorphisms act orthogonally and preserve length. Hence $G_2(p)$ may be embedded in $\mathrm{SO}_7(\mathbb{F}_p)$. One may give a very precise description of an octonion automorphism, but first it will be useful to record the following combinatorial result.

Proposition 9.4 *There are* $p^4(p^2+p+1)(p^2-p+1)$ *quaternion subalgebras of* $\mathbb{O}_p$.

To count the number of quaternion subalgebras of $\mathbb{O}_p$, first the number n of orthogonal unit bases for quaternion subalgebras are counted, and second, the number ℓ of orthogonal unit bases of a fixed quaternion subalgebra are counted. There are then n/ℓ quaternion subalgebras. Note first that two orthogonal unit vectors e_1 and e_2 in V_7 uniquely determine a quaternion subalgebra of $\mathbb{O}_p$, since $(1, e_1, e_2, e_1 \cdot e_2)$ is an orthogonal unit basis for a quaternion subalgebra of $\mathbb{O}_p$. Thus, e_1 may be chosen to be any unit vector in V_7, and e_2 any unit vector in $V_6 := e_1^{\perp} \subset V_7$. Hence,

$$n = \frac{1}{2}(\#\{\text{units in } V_7\}) \cdot (\#\{\text{units in } V_6\})$$

Similarly, ℓ is computed by carrying out the analogous calculation in an ambient four-dimensional space. Thus, letting V_i be an i-dimensional $\mathbb{F}_p$-vector space.

$$\ell = \frac{1}{2}(\#\{\text{units in } V_1\}) \cdot (\#\{\text{units in } V_3\})$$

These values may be computed relatively easily using Jacobi sums (an explicit formula for any dimension and any $\mathbb{F}_p$ is given in ([IR82], p. 102)); one has

$$\begin{aligned} n &= (p^6 + ep^3)(p^5 - ep^2) \\ \ell &= (p^2 + e)(p - e) \end{aligned}$$

where $e = \pm 1$, $e \equiv p \bmod 4$. Thus

$$\begin{aligned} n/\ell &= \frac{p^5(p^3 + e)(p^3 - e)}{p(p + e)(p - e)} \\ &= \frac{p^4(p^3 + 1)(p^3 - 1)}{(p + 1)(p - 1)} \\ &= p^4(p^2 - p + 1)(p^2 + p + 1) \end{aligned}$$

□

Now, one has the following description of an automorphism of the octonions.

Proposition 9.5 *Fix a quaternion subalgebra $\mathbb{H}_p$ of $\mathbb{O}_p$ and a unit vector e orthogonal to $\mathbb{H}_p$. An algebra automorphism σ of the octonions is completely described by specifying the automorphism σ induces on $\mathbb{H}_p$: the quaternion subalgebra $\sigma(\mathbb{H}_p)$; and $\sigma(e)$, which must be a unit vector orthogonal to $\sigma(\mathbb{H}_p)$. Furthermore, any σ specified in this way may be extended to an algebra automorphism of $\mathbb{O}_p$.*

First, let $\mathbb{H}_p$ have basis $(1, i, j, k)$. Then since e is orthogonal to $\mathbb{H}_p$, a basis for $\mathbb{O}_p$ is given by $(1, i, j, k, e, ei, ej, ek)$. Thus, specifying σ on $\{1, i, j, k, e\}$ determines σ completely. Conversely, one may compute the number of maps σ that one might specify in this way. One has $p^4(p^2+p+1)(p^2-p+1)$ choices for the image of $\mathbb{H}_p$ by Proposition 9.4. One has $p(p^2-1)$ automorphisms of $\mathbb{H}_p$. And a Jacobi sum calculation indicates that there are $p(p^2-1)$ possible unit images of e in the four-dimensional orthogonal complement of $\sigma(\mathbb{H}_p)$. Hence

$$p^4(p^2+p+1)(p^2-p+1)p(p^2-1)p(p^2-1) = p^6(p^6-1)(p^2-1)$$

different σ may be specified in this way. As this is precisely the order of $G_2(p) = \mathrm{Aut}\mathbb{O}_p$, every σ specified in this way must be an automorphism of $\mathbb{O}_p$. □

9.4 The Involutions

Using Proposition 9.5, it is possible to prove the following proposition.

Proposition 9.6 *All involutions are conjugate in* $G_2(p)$.

Consider the image ι of an involution in the seven-dimensional representation of $G_2(p)$. Since the representation is embedded in $\mathrm{SO}_7(\mathbb{F}_p)$, the determinant of ι must be 1. Since the determinant is the product of the eigenvalues of ι, the -1 eigenspace must have dimension 2, 4 or 6. Thus ι has at least two -1 eigenvectors i and j. Then $(1, i, j, k = ij)$ span a quaternion subalgebra of $\mathbb{O}_p$. Now $\iota(k) = \iota(i)\iota(j) = ij = k$ so k is a $+1$ eigenvector for ι. Choose an orthogonal eigenvector e so that ei, ek and ej complete a basis for $\mathbb{O}_p$. If e is assumed to be a -1 eigenvector, then ei is a $+1$ eigenvector, so the -1 eigenspace cannot be 6-dimensional. If e is assumed to be a $+1$ eigenvector, then ei and ej are both -1 eigenvectors. This forces the -1 eigenspace to have dimension 4, and the trace of ι must be -1 in the seven-dimensional representation of $G_2(p)$. In addition, doing a case analysis for the possible

eigenvalues of i and j, the $+1$ eigenspace can be seen to form a quaternion subalgebra of $\mathbb{O}_p$. The -1 eigenspace is the orthogonal complement of the $+1$ space, so ι is determined by its $+1$ eigenspace. Let $V^{\iota+}$ be the $+1$ eigenspace of ι. Then for any $g \in G_2$, the $+1$ eigenspace of $g\iota g^{-1}$ is $g(V^{\iota+})$, since

$$g\iota g^{-1}(g(V^{\iota+})) = g\iota(V^{\iota+}) = g(V^{\iota+}) \tag{9.7}$$

Hence in order to show that all involutions are conjugate in $G_2(p)$ it now suffices to show that $G_2(p)$ acts transitively on the quaternion subalgebras of $\mathbb{O}_p$. But this follows immediately from Proposition 9.5. □

As the proof above indicates, there is a one-to-one correspondence between quaternion subalgebras of $\mathbb{O}_p$ and involutions in $G_2(p)$.

Proposition 9.8 *There are $p^4(p^2+p+1)(p^2-p+1)$ involutions in $G_2(p)$.*

Proof: The number of quaternion subalgebras of $\mathbb{O}_p$ was determined in Proposition 9.4 to be $p^4(p^2+p+1)(p^2-p+1)$, and they are in bijective correspondence with the involutions in $G_2(p)$. □

Some involutions may easily be described explicitly. Consider the map ι on $\mathbb{O}_p$ which sends $(a, b) \mapsto (a, -b)$. Then ι is an involutory automorphism of $\mathbb{O}_p$, and all of the above may be easily verified for ι.

The centralizer of an involution can be described. Indeed, any $g \in C_G(t)$ must act orthogonally on the -1 eigenspace V^-. Hence $C_G(t) \hookrightarrow \mathrm{SO}_4(\mathbb{F}_p)$. As the order of $C_G(t)$ is equal to that of $\mathrm{SO}_4(\mathbb{F}_p)$, the groups are isomorphic.

9.5 The class C_α

The class C_α consists of unipotent transformations, and one is therefore able to associate a flag to an element U of C_α by considering kernels of successive powers of $N = U - 1$. Since N is nilpotent, $\ker N^i \subset \ker N^{i+1}$. One thus has a flag

$$\mathcal{F}_U : \quad 0 \longrightarrow \ker N \longrightarrow \ker N^2 \longrightarrow \cdots \longrightarrow \ker N^{r-1} \longrightarrow V = \ker N^r$$

where $N^r = 0$ and $N^{r-1} \neq 0$. If $v \in \ker N$, then $N(v) = 0$ and $(U-1)(v) = 0$, so $U(v) = v$. Conversely, if $U(v) = v$ then $v \in \ker N$. Hence $\ker N$ is the largest subspace of V which is fixed pointwise by U. Similarly, the elements of $\ker N^2$ are precisely those w for which $U(w) = n + w$ for some $n \in \ker N$: kernels of higher powers of N may be similarly reinterpreted with respect to U. The unipotent gUg^{-1}, $g \in G$, has associated flag $g(\mathcal{F}_U)$: this is verified by a calculation virtually identical to (9.7). The dimensions appearing in the flag of a unipotent are thus invariant under conjugation. For the unipotents in $G_2(p)$, these dimensions may be computed for the action of

$G_2(p)$ on the seven-dimensional subspace of $\mathbb{O}_p$ orthogonal to $Z(\mathbb{O}_p)$. From the representation in Section 9.1 the results may be readily deduced. One finds for $X_\alpha(1)$ that the nontrivial dimensions appearing in the flag are 3 and 6: that is, the flag associated to an element in C_α is

$$0 \longrightarrow V_3 \longrightarrow V_6 \longrightarrow V_7$$

using subscripts to denote the dimensions of the vector spaces in the flag.

The centralizer of $X_\alpha(1)$ may be described. By the Chevalley commutator formula, one determines that the root elements which commute with $X_\alpha(1)$ are $\{X_\alpha(t), X_{3\alpha+\beta}(t), X_{-\beta}, X_{3\alpha+2\beta}, X_{-3\alpha-2\beta}\}$. The elements $X_{3\alpha+2\beta}$ and $X_{-3\alpha-2\beta}$ generate a group of order $p(p^2-1)$ isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$, while one of these roots with the remaining three will generate the p-Sylow subgroup in the centralizer, of order p^4. The centralizer itself has order $p^4(p^2-1)$.

9.6 The regular class of unipotents

One may also compute the flag associated to elements in $C_{\alpha\beta}$: one finds the flag to be

$$1 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_3 \longrightarrow V_4 \longrightarrow V_5 \longrightarrow V_6 \longrightarrow V_7$$

again using subscripts to denote dimension.

The centralizer of a regular unipotent can be explicitly described. Fixing the element $\sigma = X_\alpha(1)X_\beta(1)$, one has that $\langle\sigma\rangle \subset C_G(\sigma)$. Further, by the Chevalley commutator formula it follows that $X_{3\alpha+2\beta}(1)$ commutes with both $X_\alpha(1)$ and $X_\beta(1)$ and hence with σ. As $\sigma^i \neq X_{3\alpha+2\beta}(1)$ for any i, one has that $C_G(\sigma) = \langle\sigma, X_{3\alpha+2\beta}(1)\rangle$ and has order p^2.

This concludes the description of the conjugacy classes in the rigid class vector v.

10 Conclusion

The group $G_2(p)$ is the Galois group of a regular extension of $\mathbb{Q}(t)$ for all odd primes $p > 5$. By the Hilbert Irreducibility Theorem, $G_2(p)$ is thus a Galois group over $\mathbb{Q}$. This was established by exhibiting a rigid and rational triple of conjugacy classes in $G_2(p)$. It is asked whether these triples arise from reduction mod p of a triple in $G_2(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}])$. Further, it is asked if the ℓ-adic representations of $G_{\mathbb{Q}}$ associated with this rigid triple form a compatible system of representations. If these questions could be answered affirmatively, one would expect there to be some geometrical object attached to these representations. For the purpose of investigating these questions, the published proof of rigidity is not satisfactory. It would thus be of interest to have a different proof of rigidity for $G_2(p)$ which incorporated geometric information about the action of $G_2(p)$ on various structures in the octonions. As a step in this direction, characterizations of the conjugacy classes in the rigid triple for $G_2(p)$ were provided in terms of the geometry of $\mathbb{O}_p$.

References

[BC70] Armand Borel and Roger Carter. *Seminar on Algebraic Groups and Related Finite Groups.* Springer-Verlag LNM 131. Berlin. 1970.

[Car72] Roger Carter. *Simple Groups of Lie Type.* John Wiley & Sons. London. 1972.

[Cha68] B. Chang. The conjugate classes of Chevalley classes of groups of type (G_2). *Journal of Algebra. 9.* pages 190–211. 1968.

[Che46] Claude Chevalley. *Theory of Lie Groups.* Princeton University Press. Princeton. 1946.

[Che51] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of one Variable.* Waverley Press. Inc.. 1951.

[Dar98] Henri Darmon. *Rigid Local Systems. Hilbert Modular Forms and Fermat's Last Theorem.* CICMA. Montréal. 1998.

[Ebb91] H-D Ebbinghaus. *Numbers.* Springer-Verlag. New York. 1991.

[FF84] W. Feit and P. Fong. Rational rigidity of $G_2(p)$ for any prime $p > 5$. In Michael Aschbacher and Daniel Gorenstein. editors. *Proceedings of the Rutgers Group Theory Year.* 1984.

[FH91] William Fulton and Joe Harris. *Representation Theory.* Springer-Verlag. New York. 1991.

[Gor82] Daniel Gorenstein. *Finite Simple Groups.* Plenum Press. New York. 1982.

[Gru67] K. Gruenberg. Profinite groups. In J.W.S. Cassels and A. Frohlich. editors. *Algebraic Number Theory.* London. 1967. Academic Press.

[Hum72] James E. Humphreys. *Theory of Lie Algebras and Representations.* Springer-Verlag. New York. 1972.

[Hun74] Thomas Hungerford. *Algebra.* Springer-Verlag. New York. 1974.

[IR82] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, New York. 1982.

[IS87] Yasutaka Ihara and Jean-Pierre Serre. *Galois Groups over* $\mathbb{Q}$*: Proceedings.* Springer Verlag. New York. 1987.

[Jac37] N. Jacobson. Cayley numbers and simple lie algebras of type g. *Duke Math Journal. 5.* pages 775–783. 1937.

[Lan93] Serge Lang. *Algebra.* Addison-Wesley. Reading. Mass.. 3rd edition. 1993.

[Mil80] J. S. Milne. *Étale Cohomology.* Princeton University Press. Princeton. 1980.

[MM95] Gunter Malle and Heinrich Matzat. *Inverse Galois Theory.* IWR preprint. Heidelberg. 1995.

[Mun75] James Munkres. *Topology: A first course.* Prentice Hall. Englewood Cliffs. NJ. 1975.

[Sam90] Hans Samelson. *Notes on Lie Algebras.* Springer-Verlag. New York. 2nd edition. 1990.

[Ser68] Jean-Pierre Serre. *Abelian ℓ-adic Representations and Elliptic Curves.* W.A. Benjamin. New York. 1968.

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups.* Springer-Verlag. New York. 1977.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory.* Jones and Bartlett. Boston. 1992.

[Sri79] Bhama Srinivasan. *Representations of Finite Chevalley Groups.* Springer-Verlag LNM 764. Berlin. 1979.

[Suz82] Michio Suzuki. *Group Theory I.* Springer-Verlag. New York. 1982.

[Suz86] Michio Suzuki. *Group Theory II.* Springer-Verlag, New York, 1986.

[Tho84] J. Thompson. Rational rigidity of $G_2(5)$. In Michael Aschbacher and Daniel Gorenstein, editors. *Proceedings of the Rutgers Group Theory Year*, 1984.

[Vol96] Helmut Volklein. *Groups as Galois Groups.* Cambridge University Press, Cambridge, 1996.

[War83] Frank W. Warner. *Differentiable Manifolds and Lie Groups.* Springer-Verlag, New York, 1983.

[War97] J.P. Ward. *Quaternions and Cayley Numbers.* Kluwer Academic Publishers, Dordrecht, 1997.