GALOIS GROUPS IN ENUMERATIVE GEOMETRY
Spring 2025

THOMAS BRAZELTON

Abstract. https://github.com/tbrazel/galois-notes

0. About

Some notes from a mini-seminar run in Spring 2025 on Galois groups of enumerative problems, following Joe Harris' 1979 paper of the same name [Har79]. These notes aren't intended to be a definitive reference, but are perhaps more narrow than the survey paper [SY21], for instance. Our goals are to fill out details and examples to better understand how to carry out computations in monodromy and enumerative geometry.

0.1. **Notation.** We modify some notation slightly (e.g. $\mathrm{Gr}(k,n)$ instead of $G(k,n)$ for the Grassmannian of affine k-planes in affine n-space), but for the most part follow closely with the notation in [Har79]. Some exceptions include using $\mathrm{Flex}_{(p_0,\ell_0)}$ and $\mathrm{HypFlex}_{(p_0,\ell_0)}$ instead of W' and W'' for the locus of degree d curves with a fixed flex or hyperflex in Section 2

0.2. **Acknowledgments.** Thank you to everyone who gave a talk in this mini-seminar: Nathan Chen, Alberto Landi, Sidhanth Raman, Michael Zeng, Zhong Zhang, and people who attended and participated, including Claudio Gómez-Gonzáles, Natalia Pacheco-Tallaj, Ben Spitz. Thank you to Joe Harris for discussions in and around this material.

Contents

1. Solvability

A foundational question in algebra is the following.

Question 1.1. Given a polynomial equation $F(u, z) = 0$, can we express u as a function in terms of z?

Locally we know the answer to be yes via the inverse function theorem, but we are interested in the shape of the equation – did we need square roots? Cube roots? Rational functions? A basic example comes in the case where $F(u, z) = z - f(u)$. Then we are asking how to go from $z = f(u)$ to an expression for u in terms of z. This is generally done via Galois theory. If K is our base field, we consider the extension

$$K(z) \hookrightarrow \frac{K(z)[u]}{(z - f(u))}.$$

We are interested in whether u can be expressed in terms of z, and via a Hilbert irreducibility argument, this is tantamount to asking whether u can be expressed in terms of elements in the base field K in the extension

$$K \hookrightarrow \frac{K[u]}{f(u) - \zeta},$$

obtained by specializing z to some value $\zeta \in K$. This question we know to be approachable from the perspective of Galois theory.

Theorem 1.2 (Galois)**.** If $L := K[u]/f(u)$ is a separable extension of K, then u is solvable in radicals if and only the Galois group $\mathrm{Gal}(L/K)$ is a solvable group.

1.1. From Galois groups of fields to enumerative problems.

In the early decades of Galois theory, mathematicians were interested in generalizing Question 1.1 away from the setting of univariate expressions $z = f(u)$, and towards more general polynomials $F(u, z) = 0$. A pillar in this direction is Hermite's work on algebraic functions [Her51], which could be considered the genesis of the alignment between Galois groups and monodromy groups. We recount his story in the notation of that paper but in contemporary language.

Consider $Y = V(F(u, z))$ as a subvariety of $\mathbb{P}^1 \times \mathbb{P}^1$, and let $\pi \colon Y \to \mathbb{P}^1$ be the projection onto the z-coordinate. Over a point $\zeta \in \mathbb{P}^1$, the fibers $\pi^{-1}(\zeta)$ are precisely the roots of the univariate polynomial $F(u, \zeta) = 0$. Assuming that F is homogeneous of degree m, we have that π is generically m-to-1.

The projection π has some ramification locus, however, and we denote this by

$$\{z_0, z_1, \ldots, z_{\mu-1}\} \subseteq \mathbb{P}^1.$$

These are precisely the values of z for which $F(u, z_i)$ has repeated roots. Pick some point $P \in \mathbb{P}^1$, not in the ramification locus, and let

$$\pi^{-1}(P) = \{u_0, u_1, \ldots, u_{m-1}\}.$$

Note that any class in $\pi_1(\mathbb{P}^1 \smallsetminus \{z_0, \ldots, z_{\mu-1}\}, P)$ induces a permutation on the roots $\{u_0, \ldots, u_{m-1}\}$. This is called the *monodromy action*. Hermite argues the following.[1]

Theorem 1.3 ([Her51])**.** A function in the roots u is a rational function in z if and only if it is invariant under the permutations obtained from lifting paths in $\pi_1(\mathbb{P}^1 \smallsetminus \{z_0, \ldots, z_{\mu-1}\}, P)$ (cf. [Har79]).

We will discuss a modern proof of this in a much more general setting following Harris (Proposition 1.8). In the years following Hermite, it became clear that these questions could be approached in the setting where we might have more variables and more equations. This leads us to the study of Galois groups of a *system* of equations. A natural source for such systems of equations came from the burgeoning field of enumerative algebraic geometry, and Jordan was the first to envision how Galois theory would be used here.

1.2. **Galois groups in enumerative geometry, a la Jordan.**

Question 1.4. Given an enumerative problem, to what field extension do we need to pass to in order to find all its solutions?

This question has its roots in 19th century algebraic geometry, and was crystallized by Jordan in Chapter III of his treatise on Galois theory:

> *Les solutions des problèmes dont il s'agit sont en général assez nombreuses, mais liées les unes aux autres par certaines relations géometriques. De ces relations on déduit immédiatement l'existence d'une fonction entière $\phi(x_0, x_1, \ldots)$ dont le group contient celui de l'équation X. Réciproquement, si l'on était certain de connaître* toutes *les relations géométriques que présente la question proposée (ou du moins celles dont les autres dérivent), le group de l'équation X contiendrait toutes les substitutions du group de $\phi(x_0, x_1, \ldots)$. Mais une semblable certitude est difficile à obtenir, malgré le soin apporté par d'habiles géomètres à l'étude de ces problèmes. Il ne serait donc pas impossible que les équations auxquelles ces problèmes donnent naissance eussent parfois une forme plus particulière encore que celle que nous allons trouver, en nous appuyant sur les résultats obtenus par nos prédécesseurs*
>
> Camille Jordan, 1870, [Jor70, pp.301-302]

Question 1.5. Are these sorts of questions *solvable*? Meaning solvable in radicals?

The six subsections of Chapter III in Jordan's book are dedicated to particular problems whose Galois group he is interested in studying. For instance:

III.I (Section 2) Given a planar cubic curve, we know by work of Hesse that it has the property that the line passing through any two of its flexes pass through the cubic at a third inflection point. As there are nine flexes, each flex lies on four of these lines, for a total of 12 lines.[2] *Can we obtain a formula for the flexes in terms of the coefficients of the cubic?*

III.II Given a quartic curve, can we find a cubic curve so that among the 12 points of intersection, they are in three sets of four colinear points? This follows work of Clebsch, who asked *contact problems* of a similar flavor (see [Jor70, (429)]).

[1] Hermite *proves* this in his paper, but it's a matter of opinion whether the two paragraphs of proof hold up to modern standards of rigor.

[2] I'd love to include a nice picture here, but unfortunately by a result of Klein, a smooth real planar cubic will have at most three of its nine flexes defined over $\mathbb{R}$ [Ron98].

III.III Again following work of Clebsch, given a quartic surface with a double conic, we can find five cones whose edges are bitangent to the surface. There are 16 lines on the quartic surface, each of which intersect the doubled conic at a single point. Can we solve for the lines given the quartic surface or the cones?

III.IV Kummer showed there exist quartic surfaces with 16 singular points, which lie in groups of six on singular tangent planes, each of which intersect other tangent planes at these six points. Can we solve for these points (or these planes) given the Kummer surface?[3]

III.V Following Steiner,[4] every smooth cubic surface has 27 lines. These lines lie on 45 tritangents, and two tritangent planes always intersect at some line, not necessarily a line on the cubic surface though. If two tritangent planes $a_1b_1c_1$ and $a_2b_2c_2$ don't meet at a line on a cubic surface, then there exists another tritangent plane $a_3b_3c_3$ for which $a_1a_2a_3$, $b_1b_2b_3$, and $c_1c_2c_3$ form tritangents. These are called *trihedral pairs*, and there are 120 of them (see e.g. [Hun96, p. 112]). Can we solve for the equations of the lines given the equation of the cubic surface? Can we incorporate the constraints imposed by the trihedral pairs?

III.VI Again following Clebsch, fix a curve C of order n and $\frac{n(n-3)}{2}$ points on it. Can we determine the curves of order $n-3$ intersecting C? For example if $n=4$, can we determine all the 28 bitangents to C?

With this in mind, let's see how to generalize Hermite's result and give a contemporary proof.

1.3. **Setup and goal.** Let X and Y be irreducible algebraic varieties of the same dimension over $\mathbb{C}$, let $\pi\colon Y \to X$ have degree $d > 0$. This induces a map on function fields $K(X) \to K(Y)$ which is a finite field extension.[5] and necessarily separable since we are in characteristic zero.

We're going to pick some nice $p \in X$ (in the region over which π is finite), and look at its fibers $\pi^{-1}(p) = \{q_1, \ldots, q_d\}$. We'll define two ways to permute the fibers – one coming from Galois theory and one coming from monodromy, and we'll demonstrate that these are equal, following [Har79, §1].

1.4. **The Galois group, formally.** By the primitive element theorem, $K(Y)$ is generated over $K(X)$ by some rational function $f \in K(Y)$ which satisfies a minimal polynomial relation:

$$P(f) = f^d + g_1 f^{d-1} + \ldots + g_{d-1} f + g_d = 0,$$

where $g_1, \ldots, g_d \in K(X)$.

Recall that $\mathcal{O}_X$ is the sheaf of holomorphic functions. We obtain the sheaf $\mathcal{K}_X$ of meromorphic functions as the quotient ring. We get an injection of sheaves $\mathcal{O}_X \to \mathcal{K}_X$. In the general scheme-theoretic setup, this need not be a field, however since our X is particularly nice (integral, Noetherian,..) it will be. So we can look at the germs of meromorphic functions around p, which forms a *field* $\mathcal{K}_{X,p}$. The covering map induces an isomorphism of fields at each q_α:

$$\pi_\alpha := \pi_*\colon K_{Y,q_\alpha} \xrightarrow{\sim} K_{X,p}.$$

Let's define ϕ to be the inclusion of fields obtained by restricting global meromorphic functions around p:

$$\phi\colon K(X) \hookrightarrow \mathcal{K}_{X,p},$$

[3]This configuration admits a really nice contemporary description in terms of θ-characteristics. We should come back and fill out the details here.

[4]The Steiner reference is his 1857 paper *Über die Flächen dritten Grades* (On cubic surfaces) [Ste57], published in Crelle's Journal, which was called Borchardt's Journal during Borchardt's tenure as editor (1856–1880). It's interesting to me that Jordan references work of Steiner, rather than work of Cayley and Salmon, from 1849 and 1847, respectively.

[5]If X and Y are affine, it's clear this function field extension is finite. In the general case, we can reduce to the affine case by looking at the generic points (since they're irreducible), see e.g. [Aut, 02NW].

and ϕ_α to be the composite

$$K(Y) \to \mathcal{K}_{Y,q_\alpha} \xrightarrow{\pi_\alpha} \mathcal{K}_{X,p}.$$

We can sit everything inside $\mathcal{K}_{X,p}$, so let's fix some notation:

(1) K is the image of $K(X)$ in $\mathcal{K}_{X,p}$ – it is the restriction of global meromorphic functions on X to a neighborhood of p
(2) L is the subfield of $\mathcal{K}_{X,p}$ generated by all the images of the ϕ_α's. — this is meromorphic functions around p, which are coming from meromorphic functions on Y that have been restricted to some neighborhood of some q_α

Finally we take our elements $f \in K(Y)$ and $g_i \in K(X)$ and sit them inside the larger field:

$$\phi\colon K(X) \to K \subseteq \mathcal{K}_{X,p}$$
$$g_i \mapsto \widetilde{g}_i.$$

and

$$\phi_\alpha\colon K(Y) \to \mathcal{K}_{X,p}$$
$$f \mapsto \widetilde{f}_\alpha.$$

Observe that all the $\widetilde{f}_\alpha$'s are distinct! This is because in order for f to generate $K(Y)$ over $K(X)$, it must take different values at each q_α.

Moreover, each of the $\widetilde{f}_\alpha$'s satisfy the image of the polynomial relation $P(f) = 0$ in L:

$$\widetilde{P}(\widetilde{f}_\alpha) = \widetilde{f}_\alpha^d + \widetilde{g}_1\widetilde{f}_\alpha^{d-1} + \ldots + \widetilde{g}_d = 0.$$

Let's think about $\widetilde{P}$ as a polynomial in $L[t]$. It is a degree d polynomial with d distinct roots, given by the $\widetilde{f}_\alpha$'s.

We claim then that L is the normalization of $K(Y)/K(X)$, (which is identically K_α/K. This is because the minimal polynomial $P(t)$ splits in L, and L is the minimal field over which this occurs. So we have argued:

Proposition 1.6. $\mathrm{Gal}(L/K)$ is Galois.

The action of the Galois group permutes all the $\widetilde{f}_\alpha$'s, which permutes the indices α, giving us an inclusion

$$\mathrm{Gal}(L/K) \hookrightarrow \Sigma_d.$$

The image of this is the *Galois group* of the enumerative problem.

1.5. **The monodromy group.** Since $\pi\colon Y \to X$ is an branched cover, it satisfies homotopy lifting away from the branched points. That is, any path in X which doesn't pass through the branch locus can be lifted to a path in Y after a starting point has been chosen.

To that end, pick some $U \subseteq X$ Zariski open containing our p and $V = \pi^{-1}(U)$ so that $\pi\colon V \to U$ is an unbranched cover. Then we obtain an inclusion

$$\pi_1(U, p) \to \Sigma_d,$$

given by the action of the deck group. The image of this is called the *monodromy group* of our enumerative problem.

1.6. **Monodromy and analytic continuation.** Let X be a Riemann surface, and consider a path $\gamma\colon [0,1] \to X$, and let's take two holomorphic germs $f \in \mathcal{O}_{X,\gamma(0)}$ and $g \in \mathcal{O}_{X,\gamma(1)}$. We say g is the *analytic continuation of f along γ* if there is a finite sequence of open sets U_i along the image of γ[6] and functions $f_i \in \mathcal{O}(U_i)$ so that $f_1 = f$ and $f_n = g$.

[6]We may assume finite since the image of γ is compact.

Theorem 1.7. If $\pi\colon Y \to X$ is an unbranched cover of a Riemann surface X, and $\gamma \in \pi_1(X, x)$ is some loop, then for any $f \in \mathcal{O}_{X,x}$, any choice of lift $\widetilde{\gamma}\colon [0,1] \to Y$, and any germ $g \in \mathcal{O}_{Y,\widetilde{\gamma}(0)}$ with $\pi_* g = f$, we have that analytic continuation of g along $\widetilde{\gamma}$ exists, and the resulting germ $\widetilde{g}$ also satisfies $\pi_* \widetilde{g} = f$.

1.7. **The main result.** We are going to prove the following:

Proposition 1.8. The Galois group G equals the monodromy group M in our setup.

The first step is to argue that $M \subseteq G$. That is, any permutation coming from monodromy can be realized by an automorphism of L over K. This follows via analytic continuation!

If we pick some $\gamma \in \pi_1(U, p)$, then any lift of γ to V will send some $\widetilde{f_\alpha}$ to some $\widetilde{f_\beta}$. In particular since $K = \mathrm{im}(K(X) \hookrightarrow \mathcal{K}_{X,p})$ is fixed under analytic continuation, and since any element in L is polynomial in germs at the q_α's, analytic continuation induces a field automorphism of L/K permuting the $\widetilde{f_\alpha}$'s. That is, this permutation lies in the Galois group.

For the other direction, we want to see that the containment $M \subseteq G$ is not strict. Indeed if it were, then the M-fixed subfield L^M would not be equal to K. So it suffices to argue that everything in L fixed by the monodromy action is actually in K. As we have seen, the monodromy action occurs via analytic continuation.

So take some $h \in L \subseteq \mathcal{K}_{X,p}$, and suppose h is fixed under analytic continuation along any lift of an element in $\pi_1(U, p)$. We want to argue that h is the restriction of a global meromorphic function on X to a neighborhood of p. We'll define a candidate one – define $\widetilde{h}$ on U by picking, for every $p' \in U$, an arc from p to p' and analytically continuing h along it. This is well-defined precisely because h is fixed under the monodromy action, so we obtain a well-defined value in a neighborhood of p', independent of the path we chose.

We now know that h extends to a meromorphic function $\widetilde{h}$ on U. We want to see that this extends to all of X. In order to do this, we exploit that $h \in L$. So h can be written as some polynomial in $\widetilde{h_\alpha}$'s, where $\widetilde{h_\alpha}$ is a meromorphic function on all of Y restricted to a neighborhood of q_α. None of these have essential singularities, and this is unchanged when taking a polynomial in them. Hence $\widetilde{h}$ has no essential singularities, and therefore extends to a meromorphic function on X whose germ at p is h. Thus $L^M = K$, and we are done.

1.8. **Galois groups over the rationals.** A priori this tells us nothing about Galois groups of enumerative problems over $\mathbb{Q}$, or field extensions of solutions, or anything like that. We can translate information happening over this complex function field to statements about rationals via *Hilbert irreducibility*. As a jumping off point, let's talk about monic univariate polynomials and their Galois groups (which is the origin of this story).

Example 1.9. Let $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ be the generic monic univariate polynomial of degree n, and let's think about it as living in $\mathbb{C}(a_1, \ldots, a_n)[x]$. Then there exist *rational numbers* $a_1, \ldots, a_n$ for which $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ is irreducible in $\mathbb{Q}[x]$. In fact the set of points $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{Q}}$ for which this property holds is Zariski dense.

Corollary 1.10. If G is the Galois group of $\mathbb{C}(a_1, \ldots, a_n)[x]/f$ then G is the Galois group of any specialization of f to $\mathbb{Q}[x]$ which is irreducible. In particular, we can compute in the generic case that $G = S_n$.

This admits a generalization to polynomials in arbitrarily many variables, so we get an application which we will refer to as Hilbert irreducibility in these notes.

Slogan 1.11 (Hilbert irreducibility)**.** Let X be a complex moduli space of geometric objects (e.g. cubic surfaces), and $\pi\colon Y \to X$ a generically finite map. Then the Galois group of π is isomorphic to the Galois group of a general object in X defined over the rationals.

As a particular case to illustrate what we mean, we will see that the Galois group of lines on complex cubic surfaces is $W(E_6)$. That implies that if X is any randomly chosen cubic surface defined over $\mathbb{Q}$, the field of definition $K/\mathbb{Q}$ of the lines on X has Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong W(E_6)$.

1.9. **An example we know and love.** Consider the incidence variety of roots of a univariate polynomial

$$Y = \{(f,t)\colon f(t) = 0\} \subseteq \mathbb{P}^d \times \mathbb{P}^1.$$

Then $Y \to \mathbb{P}^d$ is a projective bundle, whose Galois group is the full symmetric group. There are many ways to prove this, we highlight two:

(1) We can argue algebraically that the Galois group of the generic polynomial of degree d is the full symmetric group Σ_d.
(2) We can argue that the monodromy of the cover is symmetric, e.g. by showing it is 2-transitive and contains a transposition.

In either of these approaches, we obtain the Abel–Ruffini theorem as an immediate application via Hilbert irreducibility.

Theorem 1.12. If $f(x) \in \mathbb{Q}[x]$ is a polynomial of degree ≥ 5, there is no general formula in radicals for the roots of f in terms of the coefficients of f.

2. Flexes and bitangents

2.1. **Historical background.** The study of high degree plane curves (degrees three or greater) dates back to Newton, but one of the first major results in this are came from Plücker (*System der analytischen Geometrie*, page 264).

Theorem 2.1 (Plücker, 1835)**.** A general degree d planar curve has $3d(d-2)$ inflection points.

Plücker proved this by equation-bashing. We provide a slightly different proof, due to Hesse but likely predating him (see [Gra10, p. 169]).

Hesse's proof. Recall that the radius of curvature of a planar curve $F(x,y,z) = 0$ at a point (x_0, y_0, z_0) is the reciprocal of $\det(HF)_{|(x_0,y_0,z_0)}$, where HF is the Hessian matrix of F. Note that the equation $\det HF = 0$ is homogeneous of degree $3(d-2)$, and note further that a flex on a curve is precisely a point with infinite curvature radius. Hence we can count inflection points on F via the intersection with its Hessian curve, hence by Bézout's theorem we have $3d(d-2)$ flexes. □

The so-called *Plücker formulas* are highly related, and come from the same text. Plücker computed what is now called the *class* of the curve C, namely the number of tangent lines to C through another point p on the plane. Note that under pole-polar duality, this is also the degree of the *dual curve*. He observed by direct computation that the class of a general curve of degree d is $d(d-1)$.

In this direct algebraic approach, any line through p passing through two points of C (counted with multiplicity) qualifies as a tangent. Presuming that C is smooth (and if we take C to be general this is the case) then this is true on the nose, however even if C is mildly singular this fails. Plücker observed that the quantity $d(d-1)$ overcounts the honest class of the curve by two for every double point of C and by three for every cusp of C. This leads us to the formula

$$d^* = d(d-1) - 2\delta - 3\kappa$$

where δ is the number of nodes of C and κ is the number of cusps. This is the *Plücker formula*, and it resolves the so-called "duality paradox" which plagued the study of pole-polar duality since its invention. A nice exposition to these results is in Coolidge's treatise [Coo59, Chapter VI].

Terminology 2.2. A reduced irreducible planar curve C is said to be a *Plücker curve* if it falls under the scope of the Plücker formula – explicitly, if the only singularities of C and C^* are cusps and simple nodes.

Remark 2.3.

(1) More general Plücker formulae hold in which singularities are allowed to be much more badly behaved.
(2) Klein proved analogues of the Plücker formulae for real curves, treating split and non-split nodes differently. Leveraging his formula we are able to prove new results and give contemporary proofs of classical results known to Plücker, such as the fact that at most three of the nine flexes on a real cubic are real.
(3) Plücker's arguments were fairly nonrigorous, and it is ahistorical to attribute to him rigorous arguments that appear to be easy applications of his formula (for instance the computation that there are 28 bitangents to a planar quartic, attributed either to Hesse in 1848 or Jacobi in 1850).

Under duality, the Plücker formulae allow us to relate the numbers of bitangents and the numbers of flexes, since a bitangent to C is a node on C^*, and a flex on C is a cusp on C^*. If C is a Plücker curve of degree d, we then have the relationship

$$d = d^*(d^* - 1) - 2b - 2f.$$

Combining this with the number $3d(d-2)$ of flexes on C, we get

$$d = d^*(d^* - 1) - 2b - 2 \cdot 3d(d-2).$$

Let's now suppose that C is suitably general, so that it is nonsingular and hence $d^* = d(d-1)$ with no correction term. We then get

$$d = d(d-1)\,(d(d-1) - 1) - 2b - 3 \cdot 3d(d-2).$$

Solving for b we obtain

$$b = \frac{1}{2} d(d-2)(d^2 - 9). \tag{2.1}$$

This is the number of bitangents on a general smooth curve of degree d as estimated by Plücker and proven by Jacobi.

2.2. **The Plücker formulas via Riemann-Hurwitz.** TODO

2.3. **Monodromy of flexes: the setup.** Let $W_d := \mathbb{P}(H^0(\mathcal{O}_{\mathbb{P}^2}(d))) \cong \mathbb{P}^{\binom{d}{2}-1}$ be the complete linear system of degree d plane curves, and let I_0 be the locus of points on lines

$$I_0 := \{(p, \ell) \colon p \in \ell\} \subseteq \mathbb{P}^2 \times (\mathbb{P}^2)^*.$$

We let

$$I_d := \{(C, p, \ell) : m_p(C \cdot \ell) \geq 3\} \subseteq W_d \times I_0$$

be the incidence variety of curves equipped with a flex. We obtain projection maps

$$\begin{array}{ccccc} & & I_d & & \\ & \swarrow^{\pi} & & \searrow^{\eta} & \\ W_d & & & & I_0. \end{array}$$

Proposition 2.4. If $d \geq 3$, then π is generically finite of degree $3d(d-2)$.

Proof. We can argue that the general curve of degree d has only flexes and bitangents (it doesn't admit a hyperflex, a tritangent, or a flex bitangent). Hence over this open locus, π has a well-defined degree. Note we restrict to $d \geq 3$, since a conic has no flexes. Obtaining the degree is exactly the Plücker formula, which as we have seen can be derived in multiple different ways. □

We want to try to find the monodromy group of π, and the following fact will be helpful.

Proposition 2.5. The incidence variety I_d is irreducible.

Proof. We can consider the projection $\eta\colon I_d \to I_0$. Since I_0 is irreducible, we will be able to conclude (by Proposition A.3) that I_d is irreducible if η has equidimensional fibers. Indeed we can check that the fiber of η over any point $(p, \ell) \in I_0$ is exactly those degree d plane curves with a flex line ℓ at the point p. This is always a codimension three linear subspace of W_d. □

Leveraging irreducibility of I_d, we can now argue that $\mathrm{Mon}(\pi)$ acts transitively on the fibers of π.

Proposition 2.6. The monodromy group $\mathrm{Mon}(\pi)$ acts transitively on the fibers of π over any unbranched point in W_d.

Proof. Let $U \subseteq W_d$ be a Zariski open set over which π is unbranched, and hence a topological covering space. By covering space theory, the monodromy group will be transitive if and only if $\pi^{-1}(U)$ is connected. This is true because $\pi^{-1}(U) \subseteq I_d$ is a Zariski open subset of an irreducible variety (Proposition 2.5), hence topologically connected.[7] □

Proposition 2.7. The monodromy group $\mathrm{Mon}(\pi)$ is 2-transitive.

Proof. Let $(p_0, \ell_0) \in I_0$ be a fixed point and flex on some fixed curve C_0, and let $\mathrm{Stab}_{(p_0,\ell_0)} \leq \mathrm{Mon}(\pi)$ be its stabilizer in the monodromy group. We let

$$\mathrm{Flex}_{(p_0,\ell_0)} := \{C \in W_d \mid m_{p_0}(C \cdot \ell_0) \geq 3\},$$

and consider the incidence variety

$$I' := \{(C, p, \ell) \in \mathrm{Flex}_{(p_0,\ell_0)} \times I_0 \mid m_p(C \cdot \ell) \geq 3,\ p \neq p_0,\ \ell \neq \ell_0\} \subseteq \mathrm{Flex}_{(p_0,\ell_0)} \times I_0.$$

It suffices to argue that I' is irreducible, since then if U is as in the proof of Proposition 2.6, we will have that $\pi^{-1}(U) \cap I'$ is connected. Again we use η, and we get a map

$$\eta\colon I' \to I_0.$$

This surjects onto the Zariski open $\{(p, \ell) \mid p \neq p_0,\ \ell \neq \ell_0\} \subseteq \mathbb{P}^2 \times (\mathbb{P}^2)^*$, which is a Zariski open subset of the irreducible variety I_0, and hence itself irreducible. The fibers of η are linear spaces of constant codimension 3, hence again by Proposition A.3, we conclude that I' is irreducible. □

To argue that the monodromy group is full symmetric, it suffices to exhibit a transposition. Here we use this key lemma:

Lemma 2.8 ([Har79, p. 698])**.** Let $\pi\colon Y \to X$ be holomorphic of degree n, and suppose there exists some $p \in X$ so that $\pi^{-1}(p) = \{q_1, \ldots, q_{n-1}\}$ has $(n-1)$ distinct points, so that π is simple at $q_1, \ldots, q_{n-2}$, and π has a double point at q_{n-1}. Suppose further that Y is locally irreducible at q_{n-1}. Then the monodromy group of π contains a simple transposition, obtained by taking a small loop around p.

So we'd like to locate a planar curve with $3d(d-2) - 2$ simple flexes, and exactly one *hyperflex*. Note at the hyperflex the tangent line will meet to order ≥ 4, and in particular this would violate Bézout's theorem if $d \leq 3$.

[7] If not, we could write $\pi^{-1}(U)$ as the union of two disjoint Zariski open subsets, but this is a contradiction, because irreducibility of I_d means any two nonempty opens necessarily intersect.

Theorem 2.9. For $d \geq 4$, the monodromy group of $I_d \xrightarrow{\pi} W_d$ is the full symmetric group $\Sigma_{3d(d-2)}$.

Proof. We want to apply Lemma 2.8, so we need to show that a curve with exactly $3d(d-2)-1$ flexes exists, with a simple hyperflex at exactly one of these flexes, and no other interesting behaviors (no singularities or anything). We moreover need to argue that I_d is locally irreducible at this tuple.

To exhibit such a curve, we start with a fixed point $(p_0, \ell_0) \in I_0$, and consider the linear system of degree d curves with a (possibly higher order) hyperflex at (p_0, ℓ_0):

$$\mathrm{HypFlex}_{(p_0,\ell_0)} := \{C \in W_d \colon m_{p_0}(C \cdot \ell_0) \geq 4\} \subseteq W_d.$$

We claim that the generic $C \in \mathrm{HypFlex}_{(p_0,\ell_0)}$ is smooth.[8] We claim that the generic degree d curve with a hyperflex at (p_0, ℓ_0) has simple flexes at all other points. To see this, we first set up the incidence variety

$$I'' := \left\{(C, p, \ell) \in \mathrm{HypFlex}_{(p_0,\ell_0)} \times I_0 \mid m_p(C \cdot \ell) \geq 3,\ p \neq p_0,\ \ell \neq \ell_0\right\} \subseteq \mathrm{HypFlex}_{(p_0,\ell_0)} \times I_0.$$

Note that I'' is irreducible (via analogous arguments to the ones we've used to show I_d and I' are irreducible previously). The dimension of I'' is the same as the dimension of $\mathrm{HypFlex}_{(p_0,\ell_0)}$.

We claim now that the general $(C, p, \ell) \in I''$ has the property that p is a simple flex of C. Indeed the locus in I'' of curves with multiple hyperflexes is closed, hence is either equal to I'' or of strictly smaller dimension. We claim we cannot have equality – TODO how does this argument wrap? □

2.4. **Flexes on a plane cubic: geometric properties.** The following observation is classical, and its origins are hard to trace, but it was well-known at the time of Jordan (see [Jor70, p. 302]). The configuration of lines and flexes along a planar cubic is called the *Hesse arrangement* (see [Dol12, p. 118]).

Proposition 2.10. Let C be a smooth planar cubic, and consider its nine inflection points.

(1) These nine points lie on twelve lines
(2) The twelve lines meet four at a time at any given flex.

This configuration is illustrated in Figure 1.

Proof. This can be seen by endowing C with an abelian structure as an elliptic curve, after which the flexes of C can be identified with the 3-torsion points in the elliptic curve structure. □

Jordan noted (in modern language) that any monodromy of the flexes over the moduli of cubics will preserve the Hesse arrangement, in particular the resulting permutation of the nine flexes will preserve the colinearity properties they satisfy. He proved the following result.

Theorem 2.11 ([Jor70, Theorem 425])**.** Let $f(x)$ be an irreducible polynomial of degree nine, and let $\psi(x, y)$ be a rational function of two variables, which is symmetric in the variables. Suppose that f has the property that, given any two of its roots a and b, we can define a third root by the formula $c = \psi(a, b)$, which further satisfies:

$$b = \psi(a, c) \text{ and } a = \psi(b, c).$$

Then the Galois group of f is contained in the affine special linear group $\mathrm{ASL}(2, \mathbb{F}_3)$.

The immediate application of this is of course:

Corollary 2.12. The monodromy of flexes on smooth plane cubics is contained in $\mathrm{ASL}(2, \mathbb{F}_3)$.

[8] Zhang says this follows from Bertini's theorem.

Jordan didn't argue this was an equality, although Dickson and Weber did shortly thereafter (modulo a technicality about which field we are working over – a technicality which is explained by Hilbert irreducibility and the fact that nine is odd. We should explain further). We will prove this is an equality following [Har79, § II.2].

Question 2.13. Can we discuss Jordan's theorem in the language of resolvent degree?

Note 2.14. This group $\mathrm{ASL}(2,\mathbb{F}_3)$ acts on the cubic via projective transformations, and hence forms a subgroup of $\mathrm{PGL}_3(\mathbb{C})$ often called the *Hesse group* [Dol12, §3.1.4].

Note 2.15. This group $\mathrm{ASL}(2,\mathbb{F}_3)$ has GAP ID `[216,153]`.

Question 2.16. Does this group (as so many other groups in this field) admit any exceptional isomorphisms which hint at other ways to visualize the monodoromy?

2.5. **Monodromy of flexes on plane cubics.**

The Jacobian and Abel's Theorem. Let C be a smooth curve of genus g over $\mathbb{C}$. We have $H_1(C;\mathbb{Z}) \cong \mathbb{Z}^{2g}$ and by Serre duality, $H^0(C,\omega_C) \cong H^1(C,\mathcal{O}_C) \cong \mathbb{C}^g$. There is a natural inclusion $i : H_1(C;\mathbb{Z}) \to H^0(C,\omega_C)^\vee$ sending the path $(p \to q)$ to the functional $\int_p^q$. The *Jacobian* of C is

$$J(C) := \frac{H^0(C,\omega_C)^\vee}{H_1(C;\mathbb{Z})} \cong \frac{\mathbb{C}^g}{\mathbb{Z}^{2g}}.$$

If we choose a base point $p_0 \in C$, then for all $d \geq 1$, the *Abel-Jacobi map* $\mu_d : C^d \to J(C)$ sends a d-uple $(q_1,\ldots,q_d)$ to the functional $\left[\sum_{i=1}^d \int_{p_0}^{q_i}\right]$.

Theorem 2.17 (Abel's Theorem cite)**.** Two divisors D_1 and D_2 of degree d on C are linearly equivalent if and only if their images under the Abel-Jacobi map μ_d are equal. Moreover, the Abel-Jacobi map factors as

$$C^d \to \mathrm{Pic}_d(C) \xrightarrow{-d\cdot p_0} \mathrm{Pic}_0(C) \xrightarrow{\cong} J(C).$$

Corollary 2.18. The number of n-torsion points in $\mathrm{Pic}_0(C)$ is n^{2g}.

Proof. The group $\mathrm{Pic}_0(C)$ is isomorphic to the Jacobian $J(C) \cong (S^1)^{2g}$. The subgroup of n-torsion points is then $(\mathbb{Z}/n)^{2g} \subset (S^1)^{2g}$ and has order n^{2g}. □

Proposition 2.19. For an elliptic curve (E,o), the Abel-Jacobi map $\mu_1 : E \to J(E)$ is an isomorphism.

Flexes of a Plane Cubic and Monodromy. Let (E,o) be an elliptic curve. The complete linear series $|3o|$ embeds E as a smooth plane cubic curve. The divisor $3o$ is then linearly equivalent to the intersection of E with a general line ℓ.

If $p \in E$ is a flex point with tangent line ℓ, then $3p \sim 3o$, which means $[3(p-o)] = 0$ in $\mathrm{Pic}_0(C)$. By Corollary 2.18, there are $3^2 = 9$ points in $\mathrm{Pic}_0(C)$ that are 3-torsion, so E has 9 flexes.

Recall that $E \cong J(E) \cong \mathbb{C}/\Lambda$ where the lattice $\Lambda = H_1(E;\mathbb{Z})$. If $z \in \mathbb{C}$ is such that $z(\mod \Lambda)$ is a flex, then $z - o \in \frac{1}{3}\Lambda$. Therefore, the flexes of E can be obtained as the cokernel $\mathrm{coker}\left(\Lambda \xrightarrow{\cdot 3} \Lambda\right) \cong \mathbb{A}^2_{\mathbb{F}_3}$. Upon choosing an origin for $\mathbb{A}^2_{\mathbb{F}_3}$, the intersection form on $\Lambda = H_1(E;\mathbb{Z})$ descends to a bilinear form $\alpha : \mathbb{F}_3^2 \times \mathbb{F}_3^2 \to \mathbb{F}_3$.

Proposition 2.20. The monodromy group $\mathrm{Mon}(\pi)$ preserves the structure of the affine space $\mathbb{A}^2_{\mathbb{F}_3}$. Upon choosing an origin $O \in \mathbb{A}^2_{\mathbb{F}_3}$, the stabilizer subgroup Stab_O preserves the $\mathbb{F}_3$-bilinear form α.

Proof. Todo. □

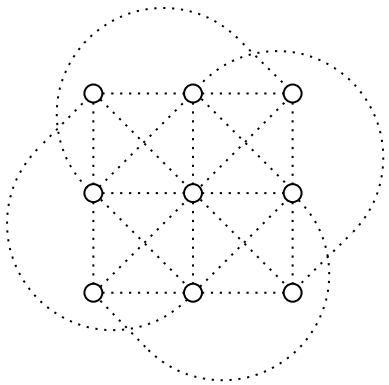


FIGURE 1. Lines on affine plane over $\mathbb{F}_3$.

2.6. **Solvability of flexes in radicals, in the style of Jordan.** Observe that $\mathrm{ASL}_2(\mathbb{F}_3)$ is a *solvable group* – this was first noticed by Jordan in [Jor70, III.III§1]. An example subnormal series exhibiting solvability is:

$$\begin{array}{ccccccc} C_4 & \hookrightarrow & Q_8 & \hookrightarrow & \mathrm{SL}_2(\mathbb{F}_3) & \hookrightarrow & \mathrm{ASL}_2(\mathbb{F}_3) \\ & & \downarrow & & \downarrow & & \downarrow \\ & & C_2 & & C_2 & & \mathbb{F}_3^2. \end{array}$$

Here for instance

$$C_4 = \left\langle \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\rangle \leq \left\langle \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \right\rangle = Q_8.$$

In particular this solvability implies that the equation for a flex point on a cubic admits a formula in radicals in terms of the coefficients for the cubic.

Question 2.21. Can we find this formula written out explicitly anywhere?

2.7. **Solving for flexes on a given cubic.** A textbook treatment is described on [MBD16, p. 333], in a section appropriately entitled *Group G of the Equation X for the Abscissas*[9] *of the Points of Inflexion.* For a general cubic $f(x, y, z) = 0$, we can restrict our attention to the affine patch $z = 1$. We then set up the equation for $f(x, y, 1) = \det Hf = 0$, and via elimination theory we can write y as a rational function in x:

$$y = \phi(x) \in \mathbb{C}(a_0, a_1, \ldots, a_9)(x),$$

where the a_i's are the coordinates of a general cubic. Finally we plug in $f(x, \phi(x), 1) = 0$ and clear denominators to obtain a degree nine polynomial in x, the roots of which are the x-coordinates of all the nine flexes on the cubic.

2.8. **Monodromy over $\mathbb{Q}$ versus over $\mathbb{C}$.** Joe remarks on [Har79, p. 696] that Jordan had initially stated the Galois group of this problem was a subgroup of $\mathrm{AGL}_2(\mathbb{F}_3)$, which is correct. Dickson and Weber stated that this containment was equality, which is not exactly incorrect.. let's consider the following computational example: we generate a random cubic over $\mathbb{Z}$, intersect it with its Hessian, eliminate a variable, and take the Galois group of the resulting degree nine polynomial. If we plug this into SageMath, we will get the following (code available on request):

```
Galois group 9T26 (E(9):2S_4) with order 432 of ...
```

[9]This is terminology in some older math books: *abscissa* means x-coordinate, and *ordinate* means y-coordinate.

This is indeed the group $\mathrm{AGL}_2(\mathbb{F}_3)$, as computed by Dickson and Weber. The reason for this is that we are computing a Galois group *over* $\mathbb{Q}$ in this example, whereas the computation of the Galois group above was taking place over $\mathbb{C}$. In many problems this isn't a difference that emerges, however this problem is special - complex conjugation is not an element of the Galois group over $\mathbb{C}$, but it *is* over $\mathbb{Q}$. This introduces an extra C_2 factor, extending the Galois group:

$$0 \to \mathrm{ASL}_2(\mathbb{F}_3) \to \mathrm{AGL}_2(\mathbb{F}_3) \to C_2 \to 0,$$

where $C_2 = \mathbb{F}_3^\times$ is the target of the determinant map.

3. Monodromy of bitangents

A classical problem is to compute the monodromy group of the 28 bitangents to a smooth planar quartic. As mentioned, this was a particular application for Galois theory envisioned by Jordan [Jor70, III.VI].

3.1. **History of bitangents to quartics.** As discussed earlier, the expression (Equation (2.1)) for the number of bitangents to a smooth curve of degree d, in terms of d, was known to Plücker in the 1830's. Despite this, Plücker's arguments are considered from a modern perspective (and likely also at the time) as sketchy at best. The so-called Plücker formulas were not rigorously proven by Plücker, and although he did sketch an accurate resolution of the pole-polar duality paradox, it did not constitute a proof.

The expression in Equation (2.1) was proven by Jacobi [Jac50], an application of which is the computation that when $d = 4$, a smooth planar quartic has 28 bitangents. This was extended shortly afterwards by Hesse, a student of Jacobi, who showed that a *general* quartic has 28 bitangents [Hes55]. Hesse's work was immensely difficult, and he likened it in a letter to Jacobi to Newton's work discovering the law of gravity [Gra10, p. 165].

For a very classical textbook treatment of the theory of bitangents to quartics, section 12 (§95-§105) of Weber's 1896 book on algebra is dedicated to this [Web96, §95-§105]. A contemporary treatment can be found in [Dol12, §6.1].

Jordan, inspired by work of Clebsch, initially asked to what extent equations for bitangents can be solved for in terms of the equations for a quartic, which is precisely the question of what the Galois group is. It's unclear to me who first solved for the Galois group of bitangents. We can write it in a number of different ways:

$$\mathrm{Sp}_6(\mathbb{F}_2) \cong W(E_7)/\{\pm 1\}.$$

It is a finite group of order $1,451,520$. The symplectic group over $\mathbb{F}_2$ is defined in Appendix B, while the connection to the Weyl group passes through the theory of Lie groups. Some references for this connection:

- ▷ See [OD88, Theorem 9] for the derivation of this group in terms of the theory of Cayley octads
- ▷ Manivel [Man06] discusses this, and mentions in the intro to the paper that the Galois groups for bitangents and lines to cubic surfaces were well-known at the beginning of the 1900's. He references a connection to Lie groups that passes through the theory of Del Pezzo surfaces of degrees 3 and 2. The point of Manivel's paper is cutting out this passage through Del Pezzos and drawing a direct connection to the Lie groups. I'd like to understand both of these stories.
- ▷ In [MBD16, p. 367], the Galois group of 28 bitangents is spelled out explicitly. The 7 in E_7 comes in here through the theory of Aronhold sets — that is, given an Aronhold set, we can solve for the remaining bitangents. What is this connection, and how does it relate to the theory of Cayley octads?

3.2. **θ-characteristics for quartics.** Recall that a *θ-characteristic* on a variety X is a square root of the canonical bundle ω_X. From this perspective it can equivalently be thought of as a divisor D for which $2D \sim K_X$.

Definition 3.1. We say a θ-characteristic, represented by a line bundle $\mathcal{L}$ on X is...

- ▷ *even* if $\dim H^0(X, \mathcal{L})$ is even
- ▷ *odd* if $\dim H^0(X, \mathcal{L})$ is odd

it's entirely possible that a θ-characteristic has no nonzero sections. So we also say a θ-characteristic represented by $\mathcal{L}$ is...

- ▷ *effective* if $\dim H^0(X, \mathcal{L}) > 0$
- ▷ *vanishing* or *non-effective* if $\dim H^0(X, \mathcal{L}) = 0$.

Remark 3.2 (reference needed)**.** If C is a complex smooth projective curve of genus g, then there is a bijection between the effective θ-characteristics on C and $\mathrm{Jac}(C)[2]$, the 2-torsion points in the Jacobian of C.

Example 3.3. An effective θ-characteristic on a smooth canonical curve of genus 3 is a bitangent.

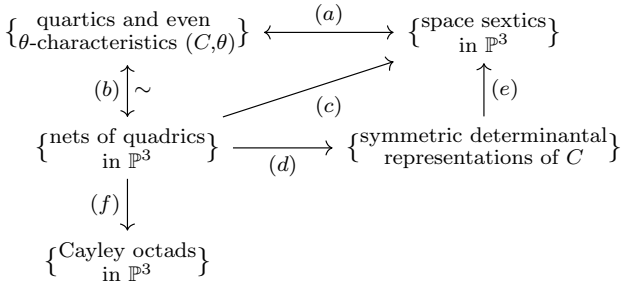
Proof. The canonical class K is the hyperplane class for the canonical embedding $C \subseteq \mathbb{P}^2$, hence as a divisor it is in general the sum of four points. If D is a θ-characteristic, it has the property that $2D \sim K$, hence if D is effective, it is a sum of two points p and q on K. We'd love to say that $2D$ is actually given by a line, since then it would be tangent to C at both p and q. This turns out to be true – it is a feature of the linear series $|K_C|$ implied by C being projectively normal.[10] □

Proposition 3.4. On a smooth canonical curve of genus $g = 3$, a θ-characteristic is odd if and only if it is effective.

Proof. How do we prove this? □

Example 3.5. If C is a smooth quartic curve, it has 28 odd (effective) θ-characteristics, corresponding to the bitangents.

What do the even θ-characteristics correspond to? It turns out they reveal quite a bit about the geometry of the quartic. We have the following maps and constructions, many of which are bijections:



(a) *Sextic space curve embeddings from even θ-characteristics*: Given a tuple (C, θ), we can consider the very ample linear series $|3\theta| = |K_C + \theta|$. This has $h^0(C, 3\theta) = 4$, hence defines an embedding $C \hookrightarrow \mathbb{P}^3$ which we can verify is of degree six.

[10] Can we explain this more? We had a discussion about definitions during Michael's talk I'd love to clarify in the notes.

To go back the other way, we consider the difference between the hyperplane class on C embedded in $\mathbb{P}^3$ and its hyperplane class under its canonical embedding in the plane. The difference between these is an even θ-characteristic.[11]

(b) *Even θ-characteristics and nets of quadrics*: This bijection is described in the proof of [GH04, 6.3].

(c) *Nets of quadrics to space sextics*: Given a net of quadrics, we can consider its subset of singular elements. Singular quadric surfaces are cones, and their vertices are points in $\mathbb{P}^3$. Varying over all singular quadrics in a net, the vertices sweep out a space curve of degree six. This process is called taking the *discriminant* of the net of sextics.

(d) *Nets of quadrics and symmetric determinantal representations*: Any quadric in $\mathbb{P}^3$ can be represented by a symmetric 4×4 matrix, so given a quadric net we can pick any three quadrics to form a basis, and consider the quartic form produced by the following determinant:

$$f = \det(xA + yB + zC).$$

This is a symmetric determinantal representation of a quartic. To go the other way, we produce the quadrics $Q_A(y) = y^T Ay$ and Q_B and Q_C arising from a symmetric determinantal representation of f and look at the net they span.

(e) *Space sextics from symmetric determinantal representations*: Given a determinantal representation (A, B, C) for the quartic C, we obtain an embedding $C \hookrightarrow \mathbb{P}^3$ via

$$\phi_\theta \colon C \to \mathbb{P}^3$$
$$[x : y : z] \mapsto \ker(xA + yB + zC).$$

(f) *Nets of quadrics to Cayley octads*: Given a net of quadric surfaces, its base locus is eight points in $\mathbb{P}^3$, which we call a *Cayley octad*.

3.3. **Cayley octads, formally.**

Definition 3.6 ([Cay69, p. 20])**.** Given eight points in $\mathbb{P}^3$ which are the base locus of a net of quadrics, we say they are a *Cayley octad*.[12]

Proposition 3.7 ([Dol12, 6.3.3])**.** Any Cayley octad arising from a quartic (C, θ) has the property that no three of its eight points are colinear, and no four are coplanar.

Suppose we are handed eight points in $\mathbb{P}^3$ satisfying Proposition 3.7. We can ask whether an associated quartic and even θ-characteristic can be uniquely recovered from this data, and the answer is yes. Moreover, we don't need all eight points to rebuild the quartic – we only need *seven of the eight points*.

3.4. **Duality via an even θ-characteristic.**

Recall we can send a curve to its *dual* by sending a point on a curve to its tangent line. With an even θ-characteristic in hand, we can reframe this in a slightly different way. Recall we have this embedding

$$\phi_\theta \colon C \to \mathbb{P}^3$$

which depended upon a choice of determinantal representation arising from θ. Similarly, we have an associated net of quadrics N_θ, and we can pick a basis for them, say

$$\operatorname{span}\{Q_1, Q_2, Q_3\} = N_\theta.$$

These give rise to a rational map

$$\psi_\theta \colon \mathbb{P}^3 \dashrightarrow \mathbb{P}^2$$
$$y \mapsto [Q_1(y) : Q_2(y) : Q_3(y)].$$

This is defined everywhere except the base locus of the net (at the Cayley octad).

[11] **Question**: Is every space sextic a genus 3 curve embedded via an even θ-characteristic?

[12] These arise in Cayley's work via the study of *octadic surfaces*, being quartic surfaces with eight nodes.

Proposition 3.8. The image $\mathrm{im}(\gamma)$ of the composite of ϕ_θ and ψ_θ is the dual curve C^*:

$$\begin{array}{ccc} C & & \\ {\scriptstyle\phi}\downarrow & \searrow^{\gamma} & \\ \mathbb{P}^3 & \overset{\psi}{\dashrightarrow} & \mathbb{P}^2. \end{array}$$

This perspective makes the connection to bitangents slightly more clear. If we look at the eight points $\{p_1, \ldots, p_8\}$ forming the indeterminacy loci of ψ, the image of $\psi(\overline{p_i p_j})$ is a single point in the dual projective plane, yielding a bitangent to the original quartic. There are $\binom{8}{2}$ such lines, yielding 28 bitangents.

See for instance [KV24, §2] for a more careful treatment of this.

3.5. **Computing the monodromy of bitangents to plane curves.** ... to show the monodromy is transitive, we have to show (by covering space theory) that the covering space is connected. To do this, we consider the projection

$$\eta\colon J_d \to J_0 \cong \mathrm{Conf}_2(\mathbb{P}^2).$$

The fiber of η over a point in J_0 is a linear subspace in J_d. So η is a fiber bundle, hence J_d is irreducible, hence connected. Then the monodromy is transitive.

Proposition 3.9. The monodromy acts 2-transitively on the fiber.

Proof. It suffices to argue that the stabilizer of a bitangent, as a subgroup of monodromy, acts on the remaining points in the fiber transitively.... TODO □

To exhibit a simple transposition, we want to find a curve with one fewer than the generic number of bitangents. It will be a curve with a simple flex bitangent. This will exist for $d \geq 5$ (because we can't have a flex bitangent for a degree four curve by Bézout).

3.6. **Monodromy of bitangents to quartics.** Given a bitangent $\overline{p_1 p_2}$ to a generic quartic C, note that $2p_1 + 2p_2 \sim K_C$ is the canonical class, i.e. a hyperplane section of the quartic. Conversely, since C is "nice" any divisor equivalent to K_C which has the form $2p_1 + 2p_2$ is cut out by a line. Here nice means projectively normal, i.e. canonically embedded by a complete linear series, and for every d, we have a surjection

$$H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d)) \twoheadrightarrow H^0(C, \mathcal{O}_C(d)).$$

Projectively normal is normal + this condition.

Hence we get a bijection between bitangents to C and divisors $p_1 + p_2$ so that $2(p_1 + p_2) \sim K_C$.

If k is any divisor with $2k \sim K_C$, then $2(p_1 + p_2 - k) = 0$. Hence $(p_1 + p_2) - k$ is a deg 0 divisor in C and $k - (p_1 + p_2)$ has order 2.

So bitangents correspond to 2-torsion points in Pic^0.

Abel-Jacobi theorem We have that

$$\mathrm{Pic}^0(C) \xrightarrow{\sim} J(C),$$

where $J(C)$ is the Jacobian

$$J(C) = H^0(C, \Omega^1_C)^* / H_1(C; \mathbb{Z}).$$

Explicitly, if we fix a basepoint $p_0 \in C$, we send $p - p_0$ to $\omega \mapsto \int_{p_0}^{p} \omega$. A priori the target depends on the path we pick between p_0 and p, however we've modded out by $H_1(C; \mathbb{Z})$ so it doesn't matter.

Bitangents correspond to some 2-torsion points in $J(C) = \mathbb{C}^3/\mathbb{Z}^6$.[13] Here we're looking at a torus, so we have a nice structure to work with to find 2-torsion stuff.

[pic – in $\mathbb{C}/\mathbb{Z}$ there are four 2-torsion points]

We know the points of order 2 in $J(C)$ form a 6D vector space $\mathbb{F}_2^6$. This has 64 elements, so not all of them are bitangents.

How does the monodromy group act on $J(C)$? We claim it preserves the affine structure (this follows from the following: if we take four bitangents, with the property that the four lines sum to zero in the jacobian, then the eight points of tangency lie on a common conic. this geometric intersection property is preserved by monodromy), so we get that

$$\mathrm{Mon}(\pi) \leq \mathrm{AGL}_6(\mathbb{F}_2).$$

It turns out there are further restrictions.

We have a skew-symmetric non-degenerate pairing

$$\widetilde{Q}\colon H_1(C;\mathbb{Z}) \times H_1(C,\mathbb{Z}) \to \mathbb{Z},$$

given by intersection with signs. This induces a form on half of the lattice

$$\begin{aligned} 4\widetilde{Q}\colon \frac{1}{2}\Lambda \times \frac{1}{2}\Lambda &\to \mathbb{Z} \\ (v,w) &\mapsto \widetilde{Q}(2v,2w). \end{aligned}$$

This is "manually imposing" the intersection form on the more dense lattice.

This in turn induces a form on the quotient (where $V = \frac{1}{2}\Lambda/\Lambda$ is our 6D vector space over $\mathbb{F}_2$ as before):

$$Q\colon V \times V \to \mathbb{Z}/2.$$

It is valued in $2\mathbb{Z}$, since if we input any two things from Λ we get something even.

This is a *strictly* skew-symmetric bilinear form.

This form is preserved by $\mathrm{Mon}(\pi)$, hence

$$\mathrm{Mon}(\pi) \leq \mathrm{AO}_6(\mathbb{F}_2).$$

Associated to any symmetric bilinear form, we will get two quadratic refinements q^+ and q_-. These are helpful in determining the *effective* semicanonical divisors. That is, we can find quadratic forms satisfying $q(v) = 0$ if and only if v represents a bitangent. The monodromy group will preserve this quadratic form, so we ultimately get the monodromy group is a subgroup of the *Steiner group* H, which is $O_6(\mathbb{Z}/2)$.

Can show that $\mathrm{Stab}_{\mathrm{Mon}(\pi)}(k_0) = O_6^-(\mathbb{Z}/2)$. Sidhanth will explain!

3.7. **Why $W(E_7)$?** Given a smooth planar quartic, we can take a cover of $\mathbb{P}^2$ branched along the quartic, and we obtain a degree two del Pezzo. This is of the form $\mathrm{Bl}_7(\mathbb{P}^2)$. A line on the del Pezzo is any curve intersecting the canonical divisor with order 1, and we have 56 such lines. The image of any of these in $\mathbb{P}^2$ is precisely one of our bitangents, and they map 2-to-1. From this perspective, $W(E_7)/\{\pm 1\}$ emerges as the Galois group analogously to how $W(E_6)$ emerges as the Galois group from $\mathrm{Bl}_6\mathbb{P}^2$.

In fact, given seven points on the plane satisfying the closed condition that no three are colinear and no six lie on a conic, we obtain a nonsingular quartic together with a choice of even θ-characteristic. In fact we have a birational isomorphism

$$\mathrm{UConf}_7(\mathbb{P}^2)/\mathrm{PGL}_3 \xrightarrow{\sim} \mathcal{M}_3^{\mathrm{ev}},$$

[13] Here $g = 3$ so $H^0(C,\Omega_C^1) \cong \mathbb{C}^3$.

where UConf is the moduli of unordered configurations, and $\mathcal{M}_3^{\text{ev}}$ is the moduli of genus three curves equipped with an even θ-characteristic [Dol12, 6.3.12]

Remark 3.10. There is a really interesting story of lattices emerging in this way (Beauville calls them *del Pezzo lattices*) [Bea22]

4. Lines on hypersurfaces

Question 4.1. How many lines lie on a general hypersurface $X_d \subseteq \mathbb{P}^n$ of degree d.

If $n = 3$, $d = 3$, then a smooth cubic surface has exactly 27 lines.

For $n = 4$, $d = 5$, it's not true that a *smooth* quintic threefold has the same number of lines, but a general quintic threefold has 2875 lines.

The *Fano variety* of lines parametrizes lines inside of a given projective variety $X \subseteq \mathbb{P}^n$.

Question 4.2. Before constructing this, for which n and d do we expect the existence of lines on a degree d hypersurface $X_d \subseteq \mathbb{P}^n$?

Consider the dimension of the space of all hypersurfaces

$$N = \dim |\mathcal{O}_{\mathbb{P}^n}(d)| = \binom{n+d}{n} - 1.$$

We get an incidence correspondence[14]

$$\Phi_{n,d} := \left\{(X, L) \in \mathbb{P}^N \times \mathbb{G}(1, n) : L \subseteq X\right\}.$$

We get two projections

$$\begin{array}{ccc} & \Phi_{n,d} & \\ {\scriptstyle \pi_1} \swarrow & & \searrow {\scriptstyle \pi_2} \\ \mathbb{P}^N & & \mathbb{G}. \end{array}$$

Proposition 4.3. The incidence variety $\Phi_{n,d}$ is smooth and irreducible of dimension $\dim(\Phi_{n,d}) = N + 2(n-1) - (d+1)$.

Proof. Observe that π_2 is a projective bundle, since over any line $[L] \in \mathbb{G}$, its fiber is all those hypersurfaces containing L. This is the same as

$$\pi_2^{-1}([L]) = \mathbb{P}H^0(\mathbb{P}^n, \mathcal{I}_L(d))^\vee.$$

This comes from the ideal sheaf sequence for a line $L \subseteq \mathbb{P}^n$, tensoring with $\mathcal{O}(d)$, then taking the LES on cohomology:

$$0 \to H^0(\mathcal{I}_L(d)) \to H^0(\mathcal{O}_{\mathbb{P}^n}(d)) \twoheadrightarrow H^0(\mathcal{O}_L(d)) \to 0$$

We can show that latter map is surjective (can extend any homogeneous polynomial in two variables to one in $n+1$ variables). Since $H^0(\mathcal{O}_L(d)) = H^0(\mathcal{O}_{\mathbb{P}^1}(d))$, we have that $H^0(\mathcal{I}_L(d))$ has constant dimension.[15] Therefore π_2 is a projective bundle. We get that

$$\begin{aligned} \dim H^0(\mathcal{I}_L(d)) &= \dim H^0(\mathcal{O}_{\mathbb{P}^n}(d)) - H^0(\mathcal{O}_L(d)) \\ &= N - (d+1). \end{aligned}$$

Then we add $2(n-1)$ back in for the dimension of the Grassmannian we are working over. □

[14] Here $\mathbb{G}(1, n)$ is the lines in $\mathbb{P}^n$, it is equivalently the affine Grassmannian $G(2, n+1)$.

[15] Jake notes: if we fix a line L, then $F_{|L} = 0$ is a linear condition on F.

The expected dimension of lines on a general $X_d \subseteq \mathbb{P}^n$ is then

$$\dim \Phi - N = 2(n-1) - (d+1).$$

We expect to have finitely many lines when this is zero, i.e. when $d = 2n-3$.

Since we computed the dimension of Φ, the equality above is an *upper bound*.

Theorem 4.4. If the expected dimension is ≥ 0 then every hypersurface contains lines (the fiber of π_1 is nonempty for every hypersurface $X \in \mathbb{P}^N$) and the dimension of the space of lines on X, denoted $F_1(X)$, is equal to the expected dimension, for a general X.

So if we're working with general hypersurfaces, then we have the expected dimension count.

Conjecture 4.5 (Debarre-de Jong)**.** If $X_d \subseteq \mathbb{P}^n$ is *any* smooth hypersurface of degree $d \leq n$, then $F_1(X)$ has dimension equal to the expected dimension $2n-3-d$.

This is false in other degree ranges.

Example 4.6. If $n = 3$ and $d = 4$, then $X_4 \subseteq \mathbb{P}^3$ is a smooth quartic K3, and a general one doesn't have any lines. By Noether–Lefschetz the very general quartic has Picard rank one. However we can write down smooth quartics which contain lines (e.g. the Fermat quartic), which would violate the conjecture above.

The main theorem we will want to prove is

Theorem 4.7. The Galois group of lines on a general hypersurface $X \subseteq \mathbb{P}^n$ of degree $2n-3$, for $n \geq 4$, is the full symmetric group.

4.1. **Construction.** Let $L \subseteq X = \{g = 0\} \subseteq \mathbb{P}^n$. Then, thinking of $g \in H^0(\mathcal{O}_{\mathbb{P}^d}(d))$, there is a restriction map to the line L:

$$\text{res}\colon H^0(\mathbb{P}^n(d)) \to H^0(\mathcal{O}_L(d)).$$

To say X contains the line is to say $g \mapsto 0$.

Key idea: If we look at the family of restrictions of sections to L, we can vary this as L ranges over points in the Grassmannian, and we can realize this as a vector bundle over $\mathbb{G}(1,n)$.

We get that the images of g under the restriction map become values of a section of this bundle.

More explicitly, let V be a vector space of dimension $n+1$, where we are thinking of $\mathbb{P}^n = \mathbb{P}(V)$. There is a bijection between lines $L \subseteq \mathbb{P}^n$ and dimension two subspaces $\Lambda \subseteq V$. Tensoring V with $\mathcal{O}_{\mathbb{G}}$, we get a trivial bundle

$$V \otimes \mathcal{O}_{\mathbb{G}} \to \mathbb{G}.$$

Inside of this we have a tautological rank two subbundle $\mathcal{S} \subseteq V \otimes \mathcal{O}_{\mathbb{G}}$, whose fiber $\mathbb{S}_{[L]}$ is Λ, where $L = \mathbb{P}(\Lambda)$ for $\Lambda \subseteq V$ a rank two subspace.

The fiber of $\mathcal{S}^\vee$ over $[L]$ is linear forms on L, which is $H^0(\mathcal{O}_L(1))$. What does it mean for a polynomial to restrict to zero? Dualizing the inclusion $\mathcal{S} \subseteq V \otimes \mathcal{O}_{\mathbb{G}}$, we get

$$V^\vee \otimes \mathcal{O}_{\mathbb{G}} \to \mathcal{S}^\vee.$$

Note that $V^\vee \otimes \mathcal{O}_{\mathbb{G}}$ is trivial, so it's recording *constant sections*. Restricting this map to some L, we get that a linear form ϕ on V is mapped to the restricted linear form $\phi_{|L}$.

We can symmetrize this to look at degree d forms, and we get

$$H^0(\mathcal{O}_{\mathbb{P}^n}(d)) = \text{Sym}^d V^\vee \to \text{Sym}^d(\mathcal{S}^\vee),$$

sending $g \mapsto g_{|L}$. The constant section g gets send to some $\sigma_g \in H^0(\text{Sym}^d V^\vee)$, and $F_1(X)$ is the zero locus of this section σ_g.

Proposition 4.8. The total Chern class of $\mathcal{S}^\vee$ is

$$c(\mathcal{S}^\vee) = 1 + \sigma_1 + \sigma_{1,1}.$$

We have $\sigma_g \in H^0(\mathrm{Sym}^d \mathcal{S}^\vee)$. Here $\mathcal{S}$ has rank two, so $\mathrm{Sym}^d(\mathcal{S}^\vee)$ has rank $d+1$. Its zero locus will then be

$$\deg c_{d+1}(\mathrm{Sym}^d \mathcal{S}^\vee) = \#\{\text{lines on a general hypersurface } X_{2n-3} \subseteq \mathbb{P}^n\}$$

We use the splitting principle and get

$$dd! \sum_k \frac{(2k)!}{k!(k+1)!} \sum_{\substack{I \subseteq \{1,\dots,n-2\} \\ \#I = n-2-k}} \prod_{i \in I} \frac{(d-2i)^2}{i(d-i)}.$$

This is https://oeis.org/A027363

Remark 4.9. There is a short discussion in the paper of when $F_1(X)$ is singular. It turns out $F_1(X)$ is singular at $u \in F_1(X) \subseteq \mathbb{G}$ if and only if the corresponding line $\lambda_u \subseteq X$ has normal bundle N with the property that $h^0(N) > 2n - 3 + d$. If we remember, this is the *expected dimension*.

By Riemann–Roch, we write

$$h^0(N) = 2n - 3 + d + h^1(N),$$

so this is the same as saying $h^1(N) > 0$.

Remark 4.10 (On the Galois group)**.**

(1) We show it's transitive (follows from Φ being irreducible)
(2) We show it's 2-transitive (fix a line L and show that Stab_L is transitive. Here is where we need $n \geq 4$)
(3) Existence of a transposition: we show that there exists an $F_1(X)$ with a point of multiplicity two (also need $n \geq 4$)

5. Lines on cubic surfaces

5.1. **The topology of cubic surfaces.** Recall that a cubic surface $S \subseteq \mathbb{P}^3$ is the blowup of $\mathbb{P}^2$ at six general points, which we will denote by $S = \mathrm{Bl}_{p_1,\dots,p_6}\mathbb{P}^2$. We denote by E_i the exceptional divisor above p_i for $i = 1, \dots, 6$. Let H be the hyperplane class on $\mathbb{P}^2$.

As smooth manifolds, S is diffeomorphic to $\mathbb{P}^2 \# 6\overline{\mathbb{P}^2}$. Hence by Mayer–Vietoris, we get that the Neron–Severi group[16] of S is

$$\mathrm{NS}(S) = H^2(S, \mathbb{Z}) = \mathbb{Z}\{H, E_1, \dots, E_6\}.$$

This is a rank 7 $\mathbb{Z}$-module, equipped with an intersection form given by the cup product. Adjunction tells us that the canonical class K_S[17] is given by

$$K_S = -3H + E_1 + \ldots + E_6.$$

Cubic surfaces are *anticanonically* embedded in $\mathbb{P}^3$, given by taking global sections of the anticanonical bundle. This tells us that the intersection of $D \subseteq S$ and $-K_S$ records how (un)twisted D is in S.

Finally, we note that we get a splitting of cohomology

$$H^2(S, \mathbb{Z}) = \mathbb{Z}\{K_S\} \oplus \mathbb{Z}\{K_S\}^\perp.$$

The orthogonal piece $\mathbb{Z}\{K_S\}^\perp$ is called the integral *primitive cohomology* of S.[18] We will denote by V or $V_\mathbb{Z}$ the primitive cohomology of S.

[16] The image of c_1.

[17] The canonical class pulls back under blowups — recall that $K_{\mathbb{P}^2} = -3H$.

[18] This borrows language from Hodge theory. Since cubic surfaces are anticanonically embedded, we have a canonical choice of Kähler class on S. The word "primitive" comes from the theory of highest weights.

5.2. **Counting lines on a cubic surface.**

Proposition 5.1. The exceptional curves $E \subseteq S$ are exactly the lines in S.

Proof. Exceptional implies that the genus of these curves are zero, and the self intersection is $E \cdot E = -1$. By the degree-genus formula (or adjunction or whatever), we have

$$g(E) = 1 + \frac{K_S \cdot E + E \cdot E}{2}.$$

Solving, we get $K_S \cdot E = -1$. This is true if and only if $(-K_S) \cdot E = 1$, thus E is linearly embedded in $\mathbb{P}^3$. □

So counting lines on S is the same as counting exceptional curves in homology. Let E be an arbitrary element of the form

$$E = \alpha H - \sum_{i=1}^{6} c_i E_i.$$

Since $c_i = E \cdot E_i$, and if we are assuming both E and E_i are lines, then either $c_i = 0$ or 1 by Bézout's theorem. Moreover, we have that

$$\begin{aligned} 1 = E \cdot (-K_S) &= \Big(\alpha H - \sum c_i E_i\Big) \cdot (3H - E_1 - \ldots - E_6) \\ &= 3\alpha - \sum c_i. \end{aligned}$$

We have two possible cases:

(1) If $\alpha = 1$ then exactly two c_i's must be equal to 1. These lines are L_{ij}, which are the strict transform of the line $\overline{p_i p_j} \subseteq \mathbb{P}^2$.
(2) If $\alpha = 2$ then *five* of the c_i's must be equal to 1. This line is denoted C_i, which is the strict transform of the conic passing through $\{p_1, \ldots, p_6\} \smallsetminus \{p_i\}$.

Altogether we have

$$\underset{\text{exceptional lines}}{6} + \underset{\text{the } L_{ij}\text{'s}}{\binom{6}{2}} + 6 = 27.$$

Theorem 5.2. There are 27 lines on S.

5.3. **The intersection form and its quadratic refinement.** Let Q be the intersection form on mod 2 cohomology, and V the mod 2 primitive cohomology – i.e. all classes which are Q-orthogonal to K_S modulo 2. The restricted form

$$Q \colon V \times V \to \mathbb{Z}/2$$

is skew-symmetric. That is, for all $D \in V_{\mathbb{Z}}$, we have that

$$1 + \frac{K_S \cdot D + D \cdot D}{2} = 1 + \frac{D \cdot D}{2} \in \mathbb{Z}.$$

Hence $D \cdot D = Q(D, D) \equiv 0 \pmod 2$.

Thus there is a *quadratic refinement* q of Q given by

$$\begin{aligned} q \colon V &\to \mathbb{Z}/2 \\ \bar{D} &\mapsto \frac{D \cdot D}{2} \pmod 2. \end{aligned}$$

We claim this *remembers* the 27 lines. Explicitly, given an exceptional curve $E \subseteq S$, we have that

$$(E + K_S)(-K_S) = 1 - 3 \equiv 0 \pmod 2.$$

This implies $E + K_S \in V$ by definition. Let's evaluate on q:

$$\begin{aligned} q(E + K_S) &= \frac{(E + K_S) \cdot (E + K_S)}{2} \\ &= \frac{1 - 3 + 2}{2} = 0. \end{aligned}$$

Thus, we get a well-defined map

$$\begin{aligned} \{\text{exceptional curve}\} &\to \{\text{roots of } q\} \\ E &\mapsto q(E + K_S). \end{aligned}$$

Moreover this is injective, because all exceptional curves are distinct, and $-K_S$ is not exceptional. Observe that

$$E = \alpha H - \sum c_i E_i \pmod 2$$

intersects to the form

$$q(E) = \alpha^2 - \sum c_i^2.$$

We can check that for $\alpha, c_i \in \{0, 1\}$, the quantity $q(E)$ is a multiple of 4 exactly 28 times. One of these is trivial (when everything is zero).

Thus q has $27 + 1$ zeros. Since q has 27 distinct roots and 27 is odd, we call q an *odd* quadratic refinement.

5.4. **Automorphisms and monodromy.**

Proposition 5.3. Let Γ be the set of lines in S. The incidence-preserving permutation group of Γ is isomorphic to $\mathrm{Aut}(V, Q, q)$. This is abstractly isomorphic to the *odd* orthogonal group $O^-(6, \mathbb{Z}/2)$. The minus sign is recording that q is an *odd* quadratic refinement of Q.

Proof. Clearly Γ spans $H^2(S, \mathbb{Z})$, so any permutation of V which preserves Q extends linearly to all of $H^2(S, \mathbb{Z})$. The anticanonical class can be written as

$$-K_S = (H - E_1 - E_2) + (H - E_3 - E_4) + (H - E_5 - E_6),$$

which is the sum of three mutually intersecting lines. Hence $-K_S$ is also fixed by the incidence-preserving permutation group of Γ. Since $-K_S$ is fixed, so is its orthogonal complement, i.e. primitive cohomology. Here σ induces an action on $V \subseteq H^2(S, \mathbb{Z}/2)$ which preserves Q and q. Moreover any induced permutation of the roots of q can be used to rebuild the permutation σ of Γ. Thus $\mathrm{Aut}(\Gamma) \cong O^-(6, \mathbb{Z}/2)$. □

Observe that six pairwise disjoint lines, together with $-K_S$, span all of $H^2(S, \mathbb{Z})$. Hence an element of $O^-(6, \mathbb{Z}/2)$ is determined by what it does to six disjoint lines. Let

$$\Omega = \{\text{sets of 6 disjoint lines} \subseteq S\}.$$

We can directly verify that this group has order 72. This implies that

$$|O^-(6, \mathbb{Z}/2)| = 6! \cdot |\Omega| = 51840.$$

Let's call $\sigma \in O^-(6, \mathbb{Z}/2)$ *elementary* if $\sigma(\gamma) = \gamma$ for *some* $\gamma \in \Omega$. That is, for some choice of six disjoint lines, γ acts by permuting them amongst themselves.

Proposition 5.4. The group $O^-(6, \mathbb{Z}/2)$ is *generated* by elementary elements.

Proof. Let $G' \leq O^-(6, \mathbb{Z}/2)$ be the subgroup generated by elementary elements, and let $\Omega' \subseteq \Omega$ be the orbit of $\{E_1, \ldots, E_6\}$ under G'. We can see that

$$|G'| = 6! |\Omega'| = 720 |\Omega'|$$

and since $|G'|$ divides 51840, we have that $|\Omega'|$ divides 72. Notice that all 72 families of disjoint 6 lines are acted upon transitively by the permutations of $\{E_1, \dots, E_6\}$. The point is that Ω' is a union of these subfamilies, and the only union having the right order is of size 72, so $\Omega' = \Omega$. □

The monodromy group of 27 lines on cubic surfaces is clearly a subgroup $M \leq O^-(6, \mathbb{Z}/2)$. This is exactly saying that monodromy proves the incidence structure of lines on a cubic surface. What turns out to be true is that this is equality.

Theorem 5.5. M contains all elementary automorphisms, hence $M = O^-(6, \mathbb{Z}/2)$.

Proof. Given some $\sigma \in O^-(6, \mathbb{Z}/2)$ we want to produce a path in the moduli space inducing that permutation. Suppose σ permutes $E_1, \dots, E_6$ on S. Blowing down to $\mathbb{P}^2$, σ defines a map permuting $p_1, \dots, p_6$. Draw some paths from p_i to $p_{\sigma(i)}$. Since being in general position is Zariski open in $(\mathbb{P}^2)^{\times 6}$, we can take the paths $p_i(t)$ connecting p_i to $p_{\sigma(i)}$ to also be in general position for all times $0 \leq t \leq 1$. We get cubic surfaces

$$S_t = \mathrm{Bl}_{p_1(t),\dots,p_6(t)},$$

still anticanonically embedded in $\mathbb{P}^3$. Moreover global sections

$$s_0(t), \dots, s_3(t) \in H^0(S_t, -K_{S_t})$$

are *also* varying continuously. Thus the monodromy action given by this path in $(\mathbb{P}^2)^{\times 6} - \Delta$ induces σ again. □

6. Galois groups to bitangents, part II (rough notes)

Goal today:

(1) recap the moduli problem
(2) prove a lemma
(3) compute the stabilizer of a bitangent
(4) show that M isn't solvable.

6.1. **What we know.** By the Plüocker formula, we have 28 bitangents, so we have an irreducible cover

$$I_4 \to W_4 = \mathbb{P}\left(H^0(\mathbb{P}^2, \mathcal{O}(4))\right).$$

Recall $J(C) \cong \mathbb{C}^3/\Lambda$, so we get a strictly skew-symmetric bilinear form

$$Q \colon V \times V \to \mathbb{F}_2$$

induced by intersection of cycles, hence preserved by M. For any $v \in V$, we have that $v + k_0$ is effective if and only if $q(v) = 0$ (here k_0 is a fixed root of K_C).

Conclusion: We have that $M \subseteq H$, where H is the Steiner subgroup of $\mathrm{AO}_6(\mathbb{Z}/2)$. This Steiner subgroup is the one preserving the zeros of q.

Fact: $H \cong O_6(\mathbb{Z}/2)$.

We want to prove

Theorem 6.1. We have $M \cong H$.

As a remark, since I_4 is irreducible, we have that M acts transitively, so it is enough to show that $\mathrm{Stab}_M(\ell_0) = O_6^-(\mathbb{Z}/2)$ for any bitangent ℓ_0. Note this was the Galois group for 27 lines!

6.2. **Relation to 27 lines.** Let $S \subseteq \mathbb{P}^3$ be an (anti-canonically embedded) smooth cubic surface, and $p \in S$ not lying on any line. Then we can project away from p, and extend this to a blowup

$$\begin{array}{ccc} \widetilde{S} & \longrightarrow & \mathbb{P}^2 \\ \downarrow & \nearrow & \\ S & & \end{array}$$

then $\widetilde{\pi}_p \colon \widetilde{S} \to \mathbb{P}^2$ is a double cover ramified over a smooth quartic C.

Lemma 6.2. ..

Proof. Let $B \subseteq \mathbb{P}^2$ be the branch locus of $\widetilde{\pi}_p$. To get its degree, we take ℓ to be a generic line on the plane, so we get $\overline{\ell_p} =: H_p \subseteq \mathbb{P}^3$ intersects S in a smooth curve C_ℓ and H is nowhere tangent to S. The strict transform of C_ℓ is

$$\widetilde{\pi}_p \colon \widetilde{C}_\ell \to \ell,$$

which is 2:1. We know that $\deg C_\ell = 3$ smooth in H, hence $g(C_\ell) = 1 = g(\widetilde{C}_\ell)$. Hence $\tilde{\pi}_p$ has 4 ramification points all with multiplicity 1. So B has degree 4.

To get smoothness of B, we take some $q \in \mathbb{P}^2$ and $\ell \subseteq H$ generic so that $q \in \ell$. Then H_ℓ meets S transversely,[19] so by the degree computation, $\ell \cap B$ is four points, so B is non-singular. □

Remark 6.3. We have also shown that if $\ell \subseteq \mathbb{P}^2$ so that $\overline{p\ell} \cap S = C_\ell$ is a smooth curve, then $\#\ell \cap B = 4$, hence ℓ is not a bitangent.

Lemma 2. Let $Q \in \widetilde{B}$, where $\widetilde{B}$ is the set-theoretic image $\widetilde{\pi}_p(B)$. Let $q \in B$ be $\widetilde{\pi}_p Q$, and let $\ell_0 = T_q B$. Then $\overline{pQ} \subseteq T_Q S$ (since $q \in B$) and $T_Q \widetilde{B} \subseteq T_Q S$ (since $\widetilde{B} \subseteq S$). And $H_{\ell_0} = T_Q S$.

Upshot: $\ell \subseteq \mathbb{P}^2$ is tangent to $q \in B$ iff H_ℓ is tangent to S at Q, iff $C_\ell = H_\ell \cap S$ is singular at Q (here $q = \widetilde{\pi}_p(Q)$).

Let $L_1, \ldots, L_{27}$ be the lines on S, and $\ell_1, \ldots, \ell_{27}$ their images in $\mathbb{P}^2$ under π_p. Since the lines L_i don't contain p, we have that ℓ_i is a line. Moreover, $\ell_i \neq \ell_j$ for $i \neq j$. This is because otherwise we would have $H_{\ell_i} = H_{\ell_j}$, so a sum of three lines contains p...

By construction for all i, we have $H_{\ell_i} = L_i + C_i$, where C_i is a smooth conic curve, and $C_i \cap L_i = \{Q_i, R_i\}$. If we let $q_i = \pi_p(Q_i)$ and $r_i = \pi_p(Q_i)$, then these are points of tangency of ℓ_i with B. It might be, however, that $q_i = r_i$.

If $q_i \neq r_i$, then ℓ_i is a *bitangent*. If $q_i = r_i$, then C_i is tangent to L_i at $Q_i = R_i$ and any line $L \neq \overline{PQ_i}$ passing through P intersects C_i and L at two distinct points, hence ℓ_i meets B only at q_i. This is a hypeflex of B.

Let $D = T_p S \cap S$, which is a cubic curve with a singularity at p, and $\ell_{28} = \pi_p(D)$ (same as taking $\widetilde{\pi}_p$ of the exceptional divisor). The intersection doesn't split, it is just a singular irreducible cubic. If we get a node, then ℓ_{28} is a bitangent. If we get a cusp, then ℓ_{28} is a hyperflex. And actually the converse holds as well. □

6.3. We identified the set of bitangents with a sub*set* $\Gamma \subseteq V \cong \mathbb{F}_2^6$. The results of this previous section yield an identification

$$V \cong P(S, \mathbb{Z}/2)$$

[19] The generic plane passing through $\overline{pq}$ is not tangent to any point of $\overline{pq} \cap S$, plus Bertini.

between V and the primitive mod two cohomology in $H^2(S, \mathbb{Z}/2)$. This isomorphism respects the quadrati forms q on V and the intersection form on $P(S, \mathbb{Z}/2)$.

Lemma 6.4. $\mathrm{Stab}_M(\ell_0) = O_6^-(\mathbb{Z}/2)$.

Proof. Take any path γ in $\mathbb{P}^{19}$ which preserves a fixed point p on every surface S_t appearing on the path, and T_pS_t so that $\ell_{28} = \ell_0$ for every t. This is a path on $\mathbb{P}^{14}$ which is the space of plane quartics. The monodromy action of γ fixes $\ell_{28} = \ell_0$ and the action on the lines $L_1, \dots, L_{27}$ corresponds to the monodromy action of γ on the remaining bitangents $\ell_1, \dots, \ell_{27}$. □

6.4. **the Galois group.** We know that the Galois group is equal to $O_6(\mathbb{Z}/2)$ with quotient $O_6^-(\mathbb{Z}/2)$.

We know it's not solvable, since $O_6^-(\mathbb{Z}/2)$ isn't (it's isomorphic to $W(E_6)$ which has an index two subgroup $U_4(2)$ which is simple).

Question 6.5. How many bitangents, in what position, do I need to solve for the other one?

Given three bitangents ℓ_0, ℓ_1, ℓ_2 whose points of intersection lie on a common conic, we can construct the cubic surface S associated to C and ℓ_0, so ℓ_1 and ℓ_2 correspond to intersecting lines. Then the corresponding group fixes the tangent plane $L_1 + L_2 + L_3$, so it sits inside a subgroup of $W(E_6)$ isomorphic to $(A_4 \times A_4) \rtimes (\mathbb{Z}/2)^3$, hence solvable.

Given four bitangents $\ell_0, \dots, \ell_3$ whose points of contact do *not* lie on a conic, construct S and then ℓ_0 becomes

7. Steiner's conics

In 1848, Jakob Steiner computed the count of smooth conics tangent to five given conics on the plane as 7776. In 1864, Chasles provided the correct answer, 3264, the namesake of the famous contemporary text on enumerative geometry [EH16]. In unpublished work, Higman proved the Galois group is 2-transitive, and Harris demonstrated it is the full symmetric group Σ_{3264} [Har79, § IV]. We'll recount this story here.

7.1. **Steiner's argument and Chasles' correction.** We let $\mathbb{P}^5 \cong \mathbb{P}\Gamma(\mathcal{O}_{\mathbb{P}^2}(2))$ the moduli space of planar conic forms. For a given smooth conic C, we let

$$\mathrm{Tan}_C \subseteq \mathbb{P}^5$$

the locus of conics which are tangent to C.

Proposition 7.1. We have that Tan_C is an irreducible hypersurface of degree six (see e.g. [EH16, p. 290])

Proof. We consider the incidence correspondence

$$\begin{array}{ccc} \{(C', p) \in \mathbb{P}^5 \times C \mid m_p(C \cdot C') \geq 2\} & \xrightarrow{\pi_2} & C \\ \downarrow{\scriptstyle \pi_1} & & \\ \mathrm{Tan}_C. & & \end{array}$$

Note that $\pi_2^{-1}(p)$ consists of all conics passing through p and having tangent line equal to T_pC at p. This is a hypersurface of degree three in $\mathbb{P}^5$.[20] Therefore we claim Tan_C is also an irreducible hypersurface. To compute the degree of Tan_C, we take a general pencil of conics and compute the

[20]Being tangent to a given line is a degree two condition, and fixing a point of tangency along the line adds an additional condition.

intersection with Tan_C. A pencil of conics is $|\mathcal{O}_{\mathbb{P}^1}(2)|$, and hence cuts out a linear series on C of degree four. This gives us a map $C \to \mathbb{P}^1$ of degree four, and Riemann–Hurwitz implies it has six branch points. □

Theorem 7.2 ([Ste48, p. 189])**.** Given five smooth conics $C_1, \ldots, C_5$, we have by Bézout's theorem that

$$\deg(\mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5}) = 6^5 = 7776.$$

What is wrong with this argument? Consider the point $[1 : 0 : \ldots : 0] \in \mathbb{P}^5$. It corresponds to the "conic" given by $x^2 = 0$. This is not a conic, but rather a doubled line. Nevertheless, it is tangent to any other conic at the two points of intersection, hence we have a continuous family of conics counted in the intersection $\cap_{i=1}^5 \mathrm{Tan}_{C_i}$. We should view this as an inevitable feature of the fact that we used a not-so-good moduli space of conics to do this problem.

Ernest de Jonquières worked on this problem in the early 1860's, but it was Luigi Cremona who is credited with observing this error that the doubled lines are counted amongst the solutions [Kle80, pp. 118-119]. A corrected computation was announced by Michel Chasles[21] in 1864 [Cha64], which was part of the work which won him the Copley medal.

Theorem 7.3 ([Cha64])**.** The number of smooth conics tangent to five is 3264.

Proof. We follow the exposition in [Kle80], with some modern terminology. Given a family of conics, we let μ denote the number of conics passing through a given point, and dually ν the number tangent to a given line. The general idea (in Chasles theory of *characteristics*) is that a condition on a family of conics, for instance being tangent to a fixed conic, can be expressed as a linear combination $\alpha\mu + \beta\nu$. We let $\mu^r\nu^s$ denote the number of conics passing through r points and tangent to s lines, and it can be easily computed that $\mu^r\nu^{5-r} = 2^{\min\{r,5-r\}}$ (cf. [Kat06, p. 42]).

Let's let $\alpha\mu + \beta\nu$ be the condition of tangency to a given conic, for some $\alpha, \beta \in \mathbb{Z}$. We want to solve for α and β, which in more contemporary language is solving for the degree of the hypersurface describing tangency (and we've seen that this is six). To do this, we note that a pencil of conics is describable as the conics passing through 4 fixed points, hence the condition μ^4. We then solve for

$$6 = \mu^4(\alpha\mu + \beta\nu) = \alpha + 2\beta.$$

Since this problem is symmetric in pole-polar duality, we get that $\alpha = \beta = 2$. Hence the condition of being tangent to a fixed conic is precisely $2\mu + 2\nu$. To solve the problem we get

$$\begin{aligned}(2\mu + 2\nu)^5 &= 2^5\left(\mu^5 + 2\binom{5}{1} + 4\binom{5}{2} + 4\binom{5}{3} + 2\binom{5}{4} + 1\right)\\ &= 32(102)\\ &= 3264.\end{aligned}$$

□

Remark 7.4. Let $X \subseteq \mathbb{P}^5 \times (\mathbb{P}^5)^*$, be the closure of the space of those (C, C^*) for which C is a smooth conic. This is called the moduli of *complete conics*. We can let μ and ν denote the pullback of the hyperplane class along the projections to $\mathbb{P}^5$ and $(\mathbb{P}^5)^*$, respectively. From this perspective, Chasles' computation can be regarded as occurring in the Chow ring $\mathrm{CH}^*(X)$ [EH16, Chapter 8].

[21] Apparently (and thankfully) Michel Chasles' infamous gullibility did not extend to his work in enumerative algebraic geometry, as he was able to correctly surmise the flaws in Jakob Steiner's work. Unfortunately, he was the victim of a prolonged scam in which he purchased forged letters written by Vrain-Denis Lucas, among them a love letter from Cleopatra to Julius Caesar written in French, and a falsified correspondence between Blaise Pascal and Isaac Newton validating Chasles' conspiracy theory that Newton had stolen his theory of gravity from Pascal [Far05, VI.4].

Remark 7.5. There is some evidence that Chasles' work indirectly (through the work of Eugène Prouhet) inspired Schubert's calculus of conditions, which later became Hilbert's 15th problem [Kle80, p. 121].

A contemporary perspective on Chasles computation is given in terms of residual intersection, following Fulton and MacPherson. We refer the reader to [EH16, 13.5.5] for this story.

7.2. **Setting up the monodromy problem.** We let $\mathbb{P}^5 \cong \mathbb{P}\Gamma(\mathcal{O}_{\mathbb{P}^2}(2))$ be the moduli space of planar conics, and $W_1 \subseteq \mathbb{P}^5$ the locus of doubled lines. We consider the incidence correspondence

$$Y := \{(C_1, \dots, C_5; C) \colon C \text{ tangent to each } C_i\} \subseteq (\mathbb{P}^5)^{\times 5} \times (\mathbb{P}^5 \smallsetminus W_1).$$

This comes with projection maps

$$\begin{array}{ccc} Y & \xrightarrow{\pi_2} & \mathbb{P}^5 \smallsetminus W_1 \\ {\scriptstyle \pi_1}\downarrow & & \\ (\mathbb{P}^5)^{\times 5} & & \end{array}$$

with fiber $\pi_1^{-1}(C_1, C_2, \dots, C_5) = \mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5} \subseteq \mathbb{P}^5 \smallsetminus W_1$. We let $X := (\mathbb{P}^5)^{\times 5}$ and we want to study the Galois group G of $\pi_1 \colon Y \to X$.

Notation 7.6. For any conic C which is not a doubled line, we let $\mathrm{Bitan}_C \subseteq \mathrm{Tan}_C \subseteq \mathbb{P}^5$ be the locus of conics bitangent to C. We let $\mathrm{Flextan}_C \subseteq \mathrm{Tan}_C$ be the locus of conics with a flextangent to C (meaning a point of intersection of order ≥ 3).

Proposition 7.7 ([Har79, p. 722])**.** Let C be a smooth conic.

(1) Tan_C, Bitan_C, and $\mathrm{Flextan}_C$ are irreducible.
(2) If D is any other conic, not tangent to C, then $\mathrm{Tan}_C \cap \mathrm{Tan}_D$ and $\mathrm{Tan}_C \cap \mathrm{Flextan}_D$ are irreducible.

Proof. todo □

Proposition 7.8. The Galois group $G = \mathrm{Gal}(\pi_1)$ is transitive.

Proof. Consider the projection

$$\pi_2 \colon Y \to \mathbb{P}^5 \smallsetminus W_1.$$

Over a smooth conic $C \in \mathbb{P}^5 \smallsetminus W_1$, the fiber is $\pi_2^{-1}(C) = \mathrm{Tan}_C^{\times 5}$. Since Tan_C is irreducible of dimension four by Proposition 7.7, we have that the fiber $\pi_2^{-1}(C)$ is irreducible of dimension 20. Suppose that C is a conic of rank two[22], then the fibers $\pi_2^{-1}(C)$ are reducible but still of rank 20.

Altogether, we claim Y can only have one irreducible component $\bar{Y}$, which is necessarily of dimension 25. All the points of Γ (where Γ is a generic fiber of π_1) necessarily lie on $\bar{Y}$. Hence G is transitive. □

Proposition 7.9. The Galois group G is 2-transitive.

Proof. Fix a conic C, we want to see that $\mathrm{Stab}_G(C)$ is transitive. To that end, we introduce the notation[23] Y_C for the incidence correspondence

$$Y_C := \left\{(C_1, \dots, C_5; C') \colon C' \in \mathrm{Tan}_{C_i} \text{ for each } i\right\} \subseteq \mathrm{Tan}_C^{\times 5} \times (\mathbb{P}^5 \smallsetminus \{W_1, C\}),$$

[22] I assume this means a line pair?
[23] The notation Y_C is overloaded in [Har79, § IV]

with projections

$$\begin{array}{ccc} Y_C & \xrightarrow{\pi_2} & \mathbb{P}^5 \smallsetminus \{W_1, C\} \\ {\scriptstyle \pi_1}\downarrow & & \\ \mathrm{Tan}_C^{\times 5} & & \end{array}$$

It is clear that $\mathrm{Stab}_G(C)$ is exactly the Galois group of this new π_1, so we want to argue that it is transitive. Again we do this by reference to π_2.

Let $U \subseteq \mathbb{P}^5 \smallsetminus (W_1 \cup \{C\})$ be the Zariski open locus of conics transverse to C. For any $D \in U$, we have that

$$\pi_2^{-1}(D) = (\mathrm{Tan}_C \cap \mathrm{Tan}_D)^{\times 5},$$

which by Proposition 7.7 is irreducible of dimension 15. Therefore Y_C has at most one irreducible component dominating $\mathrm{Tan}_C^{\times 5}$. □

Proposition 7.10. Fix five conics $C_1, \ldots, C_5$ with no two tangent, no three concurrent[24] and no three tangent to any line. Then the intersection $\mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5} \cap (\mathbb{P}^5 \smallsetminus W_1)$ consists of isolated points with

$$\sum_{C \in \mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5} \cap \mathbb{P}^5 \smallsetminus W_1} m_C(\mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5}) = 3264.$$

Moreover the local intersection multiplicity at some C is given by

$$m_C\left(\bigcap_{i=1}^{5} \mathrm{Tan}_{C_i}\right) = \prod_i \left(\sum_{p \in C \cap C_i} m_p(C \cdot C_i) - 1 \right).$$

Note that at a generic such point, C is tangent to each C_i at a single point p, with two other transverse points q_1, q_2 of intersection, so that the term in the product at C_i is exactly one, hence the conic C contributes a $+1$ to the overall count.

To exhibit a simple transposition in the Galois group, we want to find an arrangement where we have 3263 smooth conics tangent to our given C_i's. Equivalently, we can find a C whose local intersection multiplicity is two, and all the other conics have local intersection multiplicity one.

Lemma 7.11. The Galois group of the five conics problem contains a simple transposition.

Proof. Pick a conic C, and select the C_i's to be a generic point

$$(C_1, \ldots, C_5) \in \mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C,$$

so that $C_1, \ldots, C_4$ are generically tangent to C and C_5 has a flextangent with C. Since the C_i's are chosen suitably generically, they lie in the scope of the above proposition, and we have that

$$m_C(\mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5}) = 2.$$

It remains to argue that all the other $C' \in \mathrm{Tan}_{C_1} \cap \cdots \cap \mathrm{Tan}_{C_5}$ have multiplicity one. We let

$$K_C = \left\{(C_1, \ldots, C_5; C') \mid C' \in \mathrm{Tan}_{C_i} \forall i\right\} \subseteq (\mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C) \times (\mathbb{P}^5 \smallsetminus W_1 \cup \{C\})$$

We consider

$$K_C^{\geq 2} \subseteq K_C$$

[24] Concurrent here means as points in $\mathbb{P}^5$. This can be rephrased to say that no three of them lie in a pencil.

the closed subvariety of all those tuples with $m_{C'}(\mathrm{Tan}_{C_1}, \ldots, \mathrm{Tan}_{C_5})$. Now consider the diagram

$$\begin{array}{ccccc} K_C^{\geq 2} & \hookrightarrow & K_C & \xrightarrow{\pi_2} & \mathbb{P}^5 \smallsetminus W_1 \cup \{C\} \\ & \searrow & \downarrow{\scriptstyle \pi_1} & & \\ & & \mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C. & & \end{array}$$

We want to argue that $K_C^{\geq 2} \to \mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C$ is not dominant.[25] Note that

$$\pi_2^{-1}(C') = (\mathrm{Tan}_C \cap \mathrm{Tan}_{C'})^{\times 4} \times (\mathrm{Tan}_C \cap \mathrm{Flextan}_{C'}) \subseteq K_C.$$

This is irreducible of dimension 14 if C' is smooth and transverse to C, it is reducible of dimension 14 if $C' \notin \mathrm{Flextan}_C$ and dimension 15 if $C' \in \mathrm{Flextan}_C$. Hence K_C can have only one irreducible component $\overline{K_C}$ dominating $\mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C$ (since we observe that $\dim(\mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C) = 19$). We claim that $\overline{K_C} \not\subseteq K_C^{\geq 2}$, since if C' is smooth and not in Tan_C, then a generic element $(D_1, \ldots, D_5; C') \in \pi_2^{-1}(C')$ has that $D_1, \ldots, D_5$ are all tangent to C'.

Finally, we want to argue that for a generic $(C_1, \ldots, C_5) \in \mathrm{Tan}_C^{\times 4} \times \mathrm{Flextan}_C$, we have that Y is irreducible at $(C_1, \ldots, C_5; C)$. Note though that for a general $D \in \mathbb{P}^5 \smallsetminus W_1$, the fiber $\pi_2^{-1}(D)$ is irreducible at all points $(D_1, \ldots, D_5; D)$ so that $D_i \notin \mathrm{Bitan}_D$. But the condition that $D_i \in \mathrm{Bitan}_D$ isn't open – in other words no conic in a small neighborhood of C will be bitangent to a conic in a small neighborhood of C_i. □

We have therefore proven:

Theorem 7.12. The Galois group of the 3264 conics is Σ_{3264}.

7.3. **On reality for the five conics problem.** In the late 90's, Ronga, Tognoli, and Vust established the existence of five smooth real conics with the property that all 3264 solution conics are real [RTV97] (this was apparently known to Fulton but never published). A contemporary computational perspective, leveraging modern methods in numerical algebraic geometry, can be found in [TBS20]. Welshing er proved that the real count of conics is invariant of the isotopy type of the choice of five real conics – in particular if the conics are the boundaries of five disjoint disks in $\mathbb{R}\mathrm{P}^2$, then the number of conics is bounded below by 32 [Wel06, 1.7].

8. On stacks in monodromy (rough notes)

8.1. **Galois categories and fundamental groups.** If X is a space, connected and locally simply connected, and $x \in X$, there is an equivalence of categories between covers of X and left $\pi_1(X, x)$-sets. We usually restrict to finite covers and finite $\pi_1(X, x)$-sets.

Question 8.1. When does a pair $(\mathscr{C}, F)$ with $F \colon \mathscr{C} \to \mathrm{Set}$ induce an isomorphism $\mathscr{C} \sim \mathrm{Fin}_G$, where $G = \mathrm{Aut}(F)$?

Need some properties:

- ▷ $F(X)$ finite for all $X | in \mathscr{C}$
- ▷ $\mathscr{C}$ has finite limits and colimits, and F preserves them (F is *exact*)
- ▷ there is a notion of "connectedness"
- ▷ there is a notion of "Galois object" – note that $\mathrm{Aut}(x) \leq \mathrm{Aut}(F(x))$ and we'll say it's Galois if we have equality
- ▷ F reflects isomorphisms
- ▷ if X is connected, then $\mathrm{Aut}(F)$ acts on $F(X)$ transitively

[25] todo - why?

▷ $\mathrm{Aut}(F) = G$ is profinite.

Definition 8.2 ([Aut, 0BMY])**.** A pair $(\mathscr{C}, F)$ is a *Galois category* if

(1) $\mathscr{C}$ has finite limits and colimits
(2) for any $X \in \mathscr{C}$ there exist some connected X_i's so that $X \cong \amalg_i X_i$
(3) $F(X)$ is finite for all X
(4) F reflects isomorphisms and is exact

Here $X \in \mathscr{C}$ is connected if every monomorphism $Y \to X$ is an iso.

Theorem 8.3. If $(\mathscr{C}, F)$ is Galois, then

$$\mathscr{C} \xrightarrow{\sim} \mathrm{Fin}_G$$

where $G = \mathrm{Aut}(F)$.

Moreover this structure is "unique" as the groups change.

Example 8.4. If X is a scheme and $\bar{x}$ is a geometric poit in X, then we claim FEt_X is a Galois category. Here the functor is

$$\begin{aligned} \mathrm{FEt}_X &\to \mathrm{Set} \\ Y &\mapsto |Y_{\bar{x}}| \end{aligned}$$

sending Y to the underlying *set* of the space of the geometric fiber.

(1) finite limits – it has pullbacks, and a terminal object $X = X$. Finite limits – it has coproducts and coequalizers.
(2) obv
(3) obv
(4) fiber functor is exact (general fact)

Lemma 8.5. If $U, V \in \mathrm{FEt}_X$, then $\underline{\mathrm{Hom}}_X(U, V)$ is represented by some $W \to X$ finite étale.

Upshot – we have *defined* $\pi_1^{\mathrm{et}}(X, \bar{x})$.

8.2. **Stacks.** Can ask for stacks starting from categories fibered in groupoids.

Definition 8.6. A functor of stacks $\mathscr{C}_1 \to \mathscr{C}_2$ is *representable (by schemes)* if for any $T \to \mathscr{C}_2$ with $T \in \mathrm{Sch}$, we have that $\mathscr{C}_1 \times_{\mathscr{C}_2} T$ is an algebraic space (scheme).

Remark 8.7. Every property that is étale-local on the base can be extended to representable morphisms.

Definition 8.8. An algebraic (DM) stack is a stack so that there exists a scheme U and $\phi\colon U \to X$ (called the smooth presentation) which is

▷ representable
▷ smooth
▷ surjective

Given a point $x\colon \mathrm{Spec}\,(k) \to X$, with X our stack, then G_x can be defined as the pullback

$$\begin{array}{ccc} G_x & \longrightarrow & \mathrm{Spec}\,(k) \\ \downarrow & \lrcorner & \downarrow{\scriptstyle (x,x)} \\ X & \xrightarrow[\Delta]{} & X \times X. \end{array}$$

Then G_x is an algebraic space with objects automorphisms of x in X. If X is a DM stack, then G_x is discrete and has reduced stabilizers (think about them as like finite constant groups).

Example 8.9.

(1) If G is smooth and affine, acting on some U, then there exists $[U/G]$. We want it to have some universal G-principal bundle $U \to [U/G]$, so that an element (meaning a map $S \to [U/G]$ by Yoneda) has that the pullback $P \to S$ is a principal G-bundle:

$$\begin{array}{ccc} P & \longrightarrow & U \\ \downarrow & & \downarrow \\ S & \longrightarrow & [U/G]. \end{array}$$

So we *define* an object of $[U/G]$ to be a principal G-bundle over S with an equivariant map to U.

(2) If $U = *$, then we call $BG = [*/G]$, we call it a classifying stack, and an element is a G-torsor.

(3) Can present $\mathcal{M}_{g,n}$ as a stack. The coarse moduli space $M_{g,n}$ doesn't have nice properties always, so we take the smooth stack instead.

(4) Smooth cubic surfaces: let B be the base, and let $S \xrightarrow{\pi} B$ be propert and flat with $S_{\bar{b}}$ a smooth del Pezzo of degree 3 (a smooth cubic surface) for every geometric point $\bar{b} \in B$. The dualizing sheaf $\omega_{S/B}$ has the property that $\omega_{S/B}^{\vee}$ is relatively very ample, so

$$S \hookrightarrow \mathbb{P}(R^0\pi_*(\omega_{S/B}^{\vee})).$$

This is kind of similar to $\mathbb{P}^3 \times B$, but twisted. Get a map

$$\mathbb{P}^{19} - \Delta \twoheadrightarrow \mathcal{M},$$

for whatever our stack $\mathcal{M}$ is. But for any $S, S' \subseteq \mathbb{P}^3$ and iso $S \xrightarrow{\sim} S'$, this extends to all of $\mathbb{P}^3$, get an element of PGL_4. So we really write

$$\mathbb{P}^{19} \to (\mathbb{P}^{19} - \Delta)/\mathrm{PGL}_4.$$

and the map to $\mathcal{M}$ factors through this. The stacky quotient remembers more info (if we wrote two bars instead of one we get the coarse moduli space).

Theorem 8.10 (Keel-Mori, 1997)**.** Can construct coarse moduli spaces (very roughly speaking).

Theorem 8.11 (Local structure of DM stacks)**.** Let $\mathcal{X}/k$ as above, $x \in \mathcal{X}$ a closed point, and G_x, then there exists some $([\mathrm{Spec}\,(A)/G_x], \omega) \to (\mathcal{X}, x)$ étale, with $\omega \in [\mathrm{Spec}\,(A)/G_x]$ so that $G_\omega \xrightarrow{\sim} G_x$.

That is, every stack locally looks like $[\mathrm{Spec}\,(A)/G]$.

8.3. **Monodromy.** Can we use monodromy in the stacky sense to compute the one in the scheme-theoretic sense?

Let $\mathcal{X}$ be a connected algebraic stack, and $\mathrm{FEt}_{\mathcal{X}}$ the category of representable finite étale covers.

Example 8.12.

(1) X a scheme, get usual one

(2) If G is a finite group over $\mathbb{C}$ with $|G| \geq 2$, then $\mathrm{Spec}\,\mathbb{C} = * \to BG$ is a finite étale cover, with no sections. Hence $\pi_1(BG, *) \neq 0$.

Remark 8.13. The category of algebraic stacks is itself a 2-category, since we have a notion of 2-morphisms.

Definition 8.14. Let $x, x' \colon \mathrm{Spec}\,k \to \mathcal{X}$ with $k = \bar{k}$. A *hidden path* is a transformation $x \Rightarrow x'$. It is a hidden loop if $x = x'$, and we get a hidden fundamental group $\pi_1^h(X, x)$ given by the 2-automorphisms of x, which we know is G_x.

Definition 8.15. A *pointed cover* of $(\mathcal{X}, x)$ is a pair $(f, \phi) \colon (\mathcal{Y}, y) \to (\mathcal{X}, x)$ so that ϕ is a 2-morphism $x \to f(y)$, where f is representable and finite étale.

Remark 8.16.

(1) $f\colon \mathcal{Y} \to \mathcal{X}$ induces

$$\pi_1^h(\mathcal{Y}) \to \pi_1^h(\mathcal{X}).$$

Example 8.17. If G is a group scheme of finite type over $k = \bar{k}$ and G^0 is the connected component of the unity, then

$$\begin{array}{ccc} BG^0 & \longrightarrow & BG \\ \downarrow & & \downarrow \\ * & \longrightarrow & B(G/G^0). \end{array}$$

Here $\pi_1^h(BG) = G$, and BG^0 is simply connected, so we will have that

$$\pi_1(BG, *) \simeq G/G^0.$$

Remark 8.18. We have that $\pi_1^h(\mathcal{X}, x) \cong G_x$ which is an algebraic group.

Remark 8.19. If $\mathcal{X}$ is DM then $\pi_1^h(\mathcal{X}, x)$ is finite.

Definition 8.20. We can define a Galois category for $\mathcal{X}$ a connected DM stack.

This is work of Noohi, 2004

There is a map

$$\pi_1^h(\mathcal{X}, x) \xrightarrow{\omega_x} \pi_1(\mathcal{X}, x),$$

which has finite image (since they factor over G/G^0 in the previous example)

Suppose we have $\mathcal{X}$ mapping via π to its coarse moduli space X, and let $\mathcal{Y} \to \mathcal{X}$ be finite étale representable. Then $\mathcal{Y} \xrightarrow{\pi'} Y$ maps to its coarse moduli space, and this induces a map

$$\begin{array}{ccc} \mathcal{Y} & \longrightarrow & Y \\ \downarrow & & \downarrow \\ \mathcal{X} & \longrightarrow & X. \end{array}$$

The map $\bar{f}\colon Y \to X$ is *generically* étale and finite (but there are points over which it might have bigger stabilizer). Here $\bar{f}$ is étale exactly where $\pi\colon \mathcal{X} \to X$ is flat. I.e. "where G_x is constant in x."

Claim 8.21. in the above, $\mathcal{Y} \cong \mathcal{X} \times_X Y$ if and only if f induces an isomorphism between stabilizers.

Example 8.22. Let $\mathcal{M} = [\mathbb{P}^{19} - \Delta\mathrm{PGL}_4]$ and $M = (\mathbb{P}^{19} - \Delta)//\mathrm{PGL}_4$. Let $\mathcal{L} \to \mathcal{M}$ be the stack of (S, L) where $L \subseteq S$ is a line. This $\mathcal{L} \to \mathcal{M}$ is étale and finite everywhere, and degree 27. The map $L \to M$ is only generically étale and finite. The reason is that $\mathcal{M} \to M$ is generically an isomorphism (since the generic smooth cubic surface has no nontrivial automorphisms)

$$\begin{array}{ccc} \mathcal{L} & \longrightarrow & L \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \bar{f}} \\ \mathcal{M} & \longrightarrow & M. \end{array}$$

What are the monodromy groups of f and $\bar{f}$?

Fact 8.23. On a dense open $U \subseteq \mathcal{X}$, we can restrict monodromy to an open (so long as we're working with *irreducible* stuff). If $\mathcal{X}$ is not normal (e.g. when we encounter equivariant stuff), $\mathcal{Y}$ could be irreducible but not connected.

So for us, we get that $\mathrm{Mon}(f) = \mathrm{Mon}(\bar{f})$ since it was a generic isomorphism.

Fact 8.24. We have that $\mathrm{Mon}(\bar{f}) \leq W(E_6)$.

Fact 8.25. If S is a cubic surface and $G = \mathrm{Aut}(S)$, then G acts faithfully on the lines.

Hence if $x \in \mathcal{M}$ corresponds to a surface S, then we can consider

$$\omega_x \colon \pi_1^h(\mathcal{M}, x) \to \pi_1(\mathcal{M}, x)$$

which is injective and it injects in $\mathrm{Mon}(f)$.

If S_1 is the Fermat, then $\mathrm{Aut}(S)$ has order 620. If S_2 is the Clebsch, then $\mathrm{Aut}(S_2) \cong S_5$ which is 120. So jointly, they generate a subgroup of $\mathrm{Mon}(f)$ of order $\mathrm{lcm}(620, 120) = 51840/8$ of index eight.

Fact 8.26. There is only one maximal subgroup in $W(E_6)$ whose index divides eight. So our group is either everything or $U_4(2)$ which has index 2.

Fact 8.27. Does not contain order eight elements.

There do exist cubic surfaces with $\mathrm{Aut} \cong C_8$.

So these three cubic surfaces together give $W(E_6)$.

9. Resolvent degree and the Bring quintic (rough notes)

9.1. **Roots of polynomials and resolvent degree. Problem**: Find and understand formulas for roots of the polynomial

$$p(z) = z^n + a_1 z^{n-1} + \ldots + a_n.$$

Example 9.1. The quadratic polynomial $z^2 + a_1 z + a_2$ has roots

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}.$$

The operations going into this formula are addition, multiplication, and a square root.

Question 9.2. Is there a formula in radicals for a root of a generic degree n polynomial.

The Abel-Ruffini theorem says *no* for $n \geq 5$.

Proof idea: Equations are hard to solve because they have "complicated topology."

Let $\mathcal{P}_n \cong \mathbb{C}^n$ be the space of monid degree n polynomials. Let $\widetilde{\mathcal{P}}$ be the *root cover* of $\mathcal{P}_n$:

$$\widetilde{\mathcal{P}}_n = \{(p, \lambda) \mid p(\lambda) = 0\}.$$

This is a branched n-sheeted cover of $\mathcal{P}_n$ branched over the discriminant locus $V(\Delta_n(a_1, \ldots, a_n))$, consisting of polynomials with repeated roots. The monodromy of this cover is S_n.

Here $\pi_1(\mathcal{P}_n - V(\Delta_n)) = B_n$ is the braid group on n strands. This is because it can be identified with the unordered configuration space of n points in $\mathbb{C}$ (by sending a polynomial to its roots). Here the monodromy action is given by

$$B_n \twoheadrightarrow S_n.$$

Example 9.3. Given $z^d - a = 0$ for $a \in \mathbb{C}$, then as a cover

$$\pi_2 \colon \{(z, a) \mid z^d - a = 0\} \to \{a\}_{a \in \mathbb{C}},$$

we are adjoining a dth root of $a \in \mathbb{C}$. Hence π_2 is a d-sheeted branched cover, which is branched over zero. The monodromy is the cyclic group C_d.

Upshot: Building cyclic covers corresponds to adjoining dth roots.

Example 9.4. Over the base space of monic quadratic polynomials, we can take a root cover. This is degree two, branched over $V(\Delta_2) = V(a_1^2 - 4a_2)$. We have an isomorphism

$$\left\{(p,\delta) \mid \delta^2 = a_1^2 - 4a_2\right\} \xrightarrow{\sim} \{(p,\lambda) \mid p(\lambda) = 0\}$$
$$(p,\delta) \mapsto \left(p, -\frac{a_1}{2} + \frac{\delta}{2}\right).$$

We are transforming the information about roots to information about δ, which is like a square root of the discriminant. This is because having two roots allows us to reconstruct the polynomial, which is why this is an isomorphism of branched covers.

Why do we want to do this? It is because it's easier to write down topological info of this cover on the left. It is a pullback

$$\begin{array}{ccc} \{(p,\delta)\} & \dashrightarrow & \mathbb{P}^1 \\ \downarrow & \lrcorner & \downarrow{\scriptstyle z\mapsto z^2} \\ \{p(z)\} & \dashrightarrow & \mathbb{P}^1 \end{array}$$

The top horizontal map takes $(p,\delta) \mapsto \delta$, and the bottom one sends $p(z)$ to its discriminant.

So all the "topological complexity" reduces to the map $\mathbb{P}^1 \to \mathbb{P}^1$. We can write the above as

$$\begin{array}{ccc} X_1 & \longrightarrow & \widetilde{P}_2 \\ \downarrow & \lrcorner & \downarrow \\ X_0 & \dashrightarrow & P_2 \end{array}$$

Proof of Abel-Ruffini. Suppose there exist formulas in radicals for generic degree n polynomials. Then there exists the following tower:[26]

$$\begin{array}{ccc} X_r & & \\ \downarrow & \searrow & \\ \vdots & & \\ \downarrow & & \\ X_2 & \longrightarrow & \widetilde{P_n} \\ \downarrow & & \downarrow \\ X_1 & \longrightarrow & P_n = X_0, \end{array}$$

where each

$$\begin{array}{ccc} X_{i+1} & \longrightarrow & \mathbb{P}^1 \\ \downarrow & & \downarrow \\ X_i & \longrightarrow & \mathbb{P}^1 \end{array}$$

[26]The info encoded in this tower is essentially the idea of resolvent degree.

is a pullback along an endomorphism $z \mapsto z^d$ of the projective line. (**Fact**: Every cyclic cover is a pullback of a map $\mathbb{P}^1 \to \mathbb{P}^1$ along a rational map to $\mathbb{P}^1$.) This implies that we have

$$\begin{array}{ccc} X_r & \dashrightarrow & \widetilde{P}_n \\ & \searrow & \downarrow \\ & & P_n. \end{array}$$

The monodromy group of $\widetilde{P}_n \to P_n$ is S_n, and the monodromy group of $X_r \to P_n$ is some G. Then we get a surjection

$$G \twoheadrightarrow S_n.$$

Since G is given by iterated extensions of cyclic groups, we get that G is solvable, hence S_n is solvable (quotients of solvable groups are solvable), and hence $n \leq 4$. □

Note 9.5. For $n \leq 4$ such a tower exists.

Theorem 9.6 (Bring, 1786)**.** Any quintic can be reduced via radicals to a quintic of the form $P_a(z) = z^5 + az + 1$. That is, there is a formula for the general quintic in $\sqrt{-}$, $\sqrt[3]{-}$ and $\sqrt[\mathrm{Br}]{-}$ where

$$\sqrt[\mathrm{Br}]{a} = \left\{ z \mid z^5 + az + 1 = 0 \right\}.$$

The Bring family is parametrized by *one parameter* – this is an important thing to note.

Remark 9.7 (The Bring family)**.** Consider the family of polynomials $p_a(z) = z^5 + az + 1$ for $a \in \mathbb{C}$. This is a linear subspace of degree 1 in the moduli of monic quintics.

(1) The discriminant locus Δ is a set consisting of five points in $\mathbb{C}$
(2) The monodromy of the root cover restricted to the Bring family is S_5.

Around each of these five points in $\Delta \cap \{p_a\}_{a \in \mathbb{C}}$, the cover looks like a simple transposition. [Visualization available!]

Upshot: The Bring family encodes the "topological complexity" of solving quintic equations.

In tower language, we are getting a tower

$$\begin{array}{ccc} X_3 & & \\ \downarrow{\scriptstyle \sqrt[\mathrm{Br}]{-}} & \searrow & \\ X_2 & & \widetilde{P}_5 \\ \downarrow{\scriptstyle \sqrt[3]{-}} & & \downarrow \\ X_1 & & \\ \downarrow{\scriptstyle \sqrt[2]{-}} & & \\ X_0 & = & P_5 \end{array}$$

This is two pullbacks along $z \mapsto z^2$ and $z \mapsto z^3$, and adjoining the Bring radical is pulling back along the *Bring curve*

$$\mathscr{C} \to \mathbb{P}^1.$$

Here $\mathscr{C}$ is genus 4, dimension 1.

"Solving a quintic is a 1-parameter problem."

Definition 9.8. The *resolvent degree* of a branched cover $\widetilde{P}_n \to P_n$ is the least d for which there exists a formula in algebraic functions of at most d variables for the roots of a polynomial in terms of its coefficients.

Definition 9.9. The *essential dimension* $\mathrm{ed}_k(Y \dashrightarrow X)$ is the least d so that there exists a rational cover[27] $\widetilde{W} \dashrightarrow W$ with $\dim(\widetilde{W}) = \dim(W) = d$, and

$$\begin{array}{ccc} Y & \dashrightarrow & \widetilde{W} \\ \vdots & & \vdots \\ X & \dashrightarrow & W. \end{array}$$

The *resolvent degree* of $Y \dashrightarrow X$ is the minimal d for which there exists a finite *tower* of rational covers, each of essential dimension $\leq d$.

So our tower above shows

Theorem 9.10. The resolvent degree of $\widetilde{P}_5 \to P_5$ is 1.

9.2. **RD of enumerative problems.** Let $H_{3,3}(1)$ denote the moduli of (S, L) with S a smooth cubic surface and $L \subseteq S$ a line. We get a 27-sheeted cover

$$H_{3,3}(1) \to H_{3,3},$$

with monodromy $W(E_6)$.

Remark 9.11.

(1) $W(E_6)$ is not solvable, so there doesn't exist a formula for the 27 lines of a cubic surface
(2) Let $H_{3,3}(r)$ be the moduli of S and r lines on S, with superscript "skew" for r skew lines. Then
$$H_{3,3}(27) \to H^{\mathrm{skew}}_{3,3}(r)$$
is solvable for $r = 3$ but not for $r < 3$.

This means there is a formula in radicals for the 27 lines given 3 disjoint ones, but no fewer.

But formulas not in radicals do exist.

Theorem 9.12. $\mathrm{RD}(H_{3,3}(27) \to H_{3,3}(1)) \leq \mathrm{RD}(\widetilde{P}_5 \to P_5) = 1$.

Proof. Given a line on a cubic surface, we can consider the pencil of planes containing L. The residual conic degenerates at five pairs of distinct lines, giving us 11 lines in total. We can solve for the remaining 16 in radicals in terms of the 11 we have. □

Vibe: The Bring curve is highly symmetric (has automorphism group S_5), and the map to $\mathbb{P}^1$ is exactly the quotient by this automorphism group. In resolvent degree problems, highly symmetric objects like this often appear, as we leverage symmetry to drive down the resolvent degree of the problem.

Appendix A. Algebraic geometry terms and references

Here are some terms and results we might need in the notes.

Definition A.1 ([Har77, p. 91])**.** If $f\colon X \to Y$ is a morphism of varieties with Y irreducible, we say it is *generically finite* if $f^{-1}(\eta)$ is a finite set, where η is the generic point in Y.

Remark A.2. If f is locally of finite type and qcqs, being generically finite admits some equivalent conditions (see e.g. [Aut, 02NW]).

[27] Rational cover = generically finite dominant rational map

Proposition A.3. Let $f\colon X \to Y$ is a map with irreducible equidimensional fibers, with Y irreducible. Suppose that either X is equidimensional or f is proper. Then X is irreducible.

Proof. A proof can be found in https://public.websites.umich.edu/~mmustata/Note1_09.pdf □

Appendix B. On quadratic forms modulo two

By studying the integral homology of various varieties, together with their intersection forms, we obtain integral bilinear forms, and we often care about their reduction modulo two. Over $\mathbb{F}_2$ the theory of bilinear and quadratic forms gets simultaneously harder and easier.

Definition B.1. Let $V = \mathbb{Z}^n$ be a free abelian group of finite rank. Then an integral *quadratic form* is a function

$$q\colon V \to \mathbb{Z},$$

with the property that $q(rv) = r^2 q(v)$ for any $r \in \mathbb{Z}$ and $v \in V$, and so that

$$\begin{aligned} V \times V &\to \mathbb{Z} \\ (v, w) &\mapsto q(v+w) - q(v) - q(w) \end{aligned}$$

is bilinear. We denote by $\mathrm{Quad}_{\mathbb{Z}}(V)$ the set of integral quadratic forms on V.

Definition B.2. We say that a bilinear form

$$\beta\colon V \times V \to \mathbb{Z}$$

is *symmetric* if $\beta(v,w) = \beta(w,v)$ for all $v, w \in V$, and we say it is *skew-symmetric* if $\beta(v,w) = -\beta(w,v)$. We denote by $\mathrm{Sym}_{\mathbb{Z}}(V)$ the set of symmetric bilinear forms on V.

There is a map called *polarization*[28]

$$\begin{aligned} \mathrm{Quad}_{\mathbb{Z}}(V) &\to \mathrm{Sym}_{\mathbb{Z}}(V) \\ q &\mapsto [(v,w) \mapsto q(v+w) - q(v) - q(w)], \end{aligned}$$

and if we were working over a Dedekind domain in which 2 was invertible, this would be a bijection. Instead it may fail to be bijective – this is the main difficulty in studying quadratic forms over $\mathbb{Z}$ or over $\mathbb{F}_2$, say.

Terminology B.3. If $\beta \in \mathrm{Sym}_{\mathbb{Z}}(V)$, then any q which polarizes to β is called a *quadratic refinement* of β.

Definition B.4. Recall a form is said to be *symplectic* if it is skew-symmetric and non-degenerate. We denote by $\mathrm{Sp}(V)$ the group of *symplectic forms* on V.[29]

The following result is crucial.

Proposition B.5. If β is a non-degenerate alternating form on some finite-dimensional k-vector space V, then V has *even* dimension.

Proof. We can induct on $\dim(V)$, running through odd dimensions, to show that alternating implies degeneracy. Clearly if $\dim(V) = 1$, the form must be degenerate. Now suppose $\dim(V) = n$, let β be an alternating form on V, and pick some nonzero $v \in V$. If $\beta(v, -)$ is identically zero, then β is degenerate and we are done, so suppose not. Then $\beta(v,w) = a$ for some $a \neq 0$ in k. By rescaling w, we may assume $a = 1$. Since β is alternating, w cannot be a scalar multiple of v,

[28] This can be interpreted as a norm.

[29] todo – explain the group structure

hence $\text{span}\{v, w\} \subseteq V$ is a $2d$ subspace. Call it V_0. Since β is alternating, it is skew-symmetric, so β is represented by the Gram matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ for V_0 in the basis $\{v, w\}$. Then we can write $V = V_0 \oplus V^\perp$, and β is non-degenerate and alternating on $V_0^\perp$. Hence by induction, $\dim(V_0^\perp)$ is even, hence so is $\dim(V)$. □

Definition B.6. If β is a non-degenerate alternating form on V, where $\dim(V) = 2n$, then a *symplectic basis* for β is a basis

$$\{x_1, \ldots, x_n, y_1, \ldots, y_n\},$$

so that

- ▷ $\beta(x_i, y_i) = \delta_{ij}$
- ▷ $\beta(x_i, x_j) = \beta(y_i, y_j) = 0$ for all i, j.

In particular in this basis, β is represented by $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$.

Theorem B.7. Every non-degenerate alternating form on a vector space over an arbitrary field admits a symplectic basis.

Slogan B.8. There is really only *one* symplectic form on V^{2n} for any n, which is the standard one.

B.1. **In characteristic two.** A good reference for this is [Dol12, 5.1.2].

Proposition B.9. Over a field of characteristic two, alternating implies skew-symmetric, but not vice versa.

Proof. If $\beta(-,-)$ is alternating, then we can plug in $\beta(v + w, w + v)$ and see β must be skew-symmetric. The converse doesn't hold – consider for instance the identity matrix, which represents a symmetric (and hence skew-symmetric in characteristic two) form, but is clearly not alternating. □

These leaves open the question of what we should mean by a *symplectic form* over a field of characteristic two. Asking for it to be skew-symmetric is silly since this is the same as symmetry.

Definition B.10. We say a form over a field of characteristic two is *symplectic* if it is alternating, meaning $\beta(v, v) = 0$ for any $v \in V$.

Proposition B.11. In characteristic two, polarization factors through symplectic forms:

$$\begin{array}{ccc} \text{Quad}_{\mathbb{F}_2}(V) & \dashrightarrow & \text{Alt}_{\mathbb{F}_2}(V) \\ & \searrow & \downarrow \\ & & \text{Sym}_{\mathbb{F}_2}(V). \end{array}$$

Proof. Let V be an $\mathbb{F}_2$-vector space and let q be a quadratic form on V. Let $\beta(-,-)$ be the polarization. Then for any $v \in V$, we have that

$$\beta(v, v) = q(2v) - q(v) - q(v) = 4q(v) - 2q(v) = 0.$$

Hence β is symplectic. □

So how many quadratic forms polarize to the standard symplectic form on V? We study this over $\mathbb{F}_2$, specifically:

B.2. **Over a field with two elements.** Over $\mathbb{F}_2$, we always have $a^2 = a$, so some stuff simplifies.

Proposition B.12. Two forms $q, q' \in \mathrm{Quad}_{\mathbb{F}_2}(V)$ have the same polarization if and only if
$$q - q' = \ell,$$
where $\ell\colon V \to \mathbb{F}_2$ is a linear form.[30]

Proof. For the forward direction, suppose q and q' admitted the same polarization. Then for any (v, w) the output of the polarization is the same, meaning
$$q(v+w) - q(v) - q(w) = q'(v+w) - q'(v) - q'(w).$$
Rearranging, we get $(q-q')(v+w) = (q-q')(v) + (q-q')(w)$, hence their difference is linear, and letting $\ell(v) = (q-q')(v)$, we get that $\ell(av) = a^2\ell(v)$ from the definition of q and q' both being quadratic forms.

For the reverse direction, let q' be a quadratic form and $q := q' + \ell$. We want to argue that q is a quadratic form. Indeed,
$$q(av) = q'(av) + \ell(av) = a^2 q'(v) + a\ell(v) = a^2(q'(v) + \ell(v)).$$
Moreover it is clear that q and q' have the same polarization. □

Proposition B.13. Let $V \cong \mathbb{F}_2^{2n}$ have even dimension, and let $Q(V)$ be the set of quadratic forms whose polarization is the standard symplectic form. Then $Q(V)$ is an affine torsor for $\mathbb{F}_2^{2n}$.

Example B.14. Let C be any curve. Then we have an isomorphism $\mathrm{Jac}(C)[2] \cong \mathbb{F}_2^{2g}$, and this comes equipped with the *Weil pairing*, which is an alternating non-degenerate form.

We will identify $Q(V)$ with the set of θ-characteristics and this relation will be better understood.

Notation B.15. Let V be a symplectic space of dimension $2n$, with matrix $J_n = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$. With respect to this standard basis, we define
$$\mathrm{Sp}_{\mathbb{F}_2}(V) = \left\{ A \in \mathrm{GL}_{2n}(\mathbb{F}_2) \mid A^T J_n A = J_n \right\}.$$
We will also write $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ to mean the above group, indicating the rank of V but suppressing it from the notation.

By induction, we may argue that [Dol12, 5.9]:
$$\#\mathrm{Sp}_{2n}(\mathbb{F}_2) = 2^{n^2}(2^{2n}-1)(2^{2n-2}-1)\cdots(2^2-1).$$
Note that $\mathrm{Sp}(V)$ acts on $Q(V)$.

Proposition B.16. As a $\mathrm{Sp}(V)$-set, we have that $Q(V)$ is a disjoint union of two transitive $\mathrm{Sp}(V)$-sets, corresponding to the *even* and *odd* quadratic forms polarizing to the standard symplectic form on V.

Here even and odd is defined in terms of the *Arf invariant*, but is related to even and odd theta-characteristics. We denote by $O^+_{2n}(\mathbb{F}_2)$ or $O^-_{2n}(\mathbb{F}_2)$ the stabilizer in $\mathrm{Sp}(V)$ of an even (resp. odd) quadratic form. In this notation, we have an isomorphism of $\mathrm{Sp}(V)$-sets of the form:
$$Q(V) \cong \mathrm{Sp}(V)/O^+(V) \amalg \mathrm{Sp}(V)/O^-(V).$$
Here $|\mathrm{Sp}(V)/O^+(V)| = 2^{n-1}(2^n+1)$ and $|\mathrm{Sp}(V)/O^-(V)| = 2^{n-1}(2^n-1)$. We record some numbers here:

[30] Over a general field we would ask ℓ to satisfy $\ell(av) = a^2\ell(v)$ for any scalar a, but over $\mathbb{F}_2$ this condition just means $\ell(0) = 0$.

$2n$	$\#\mathrm{Sp}_{2n}(\mathbb{F}_2)$	$\#O^+_{2n}(\mathbb{F}_2)$	$\#O^-_{2n}(\mathbb{F}_2)$
2	6	2	6
4	720	72	120
6	1451520	40320	51840
8	47377612800	348364800	394813440

Appendix C. Theta-characteristics

We've discussed theta-characteristics above. Let C be a curve, and look at $\mathrm{Jac}(C)[2] \cong \mathbb{F}_2^{2g}$. This comes equipped with the Weyl pairing ω, and we can ask which quadratic forms polarize to ω. Then we have that

$$V = \mathrm{Jac}(C)[2] = \left\{v \in \mathrm{Pic}^0(C) \mid 2v = 0\right\}.$$

Theorem C.1. The θ-characteristics on a curve are in canonical bijection with $Q(V)$, that is, the set of quadratic forms on $\mathrm{Jac}(C)[2]$ polarizing to the Weil pairing.

To my knowledge this is due to Mumford. This theorem explains a few things:

- ▷ there is no canonical bijection between θ-characteristics and two-torsion points on the Jacobian, precisely due to the torsor structure above
- ▷ a choice of θ-characteristic induces a bijection, however, and all other θ-characteristics can be discussed with reference to this fixed one.

Proposition C.2. The number of theta-characteristics on a curve C of genus g over an algebraically closed field is as follows:

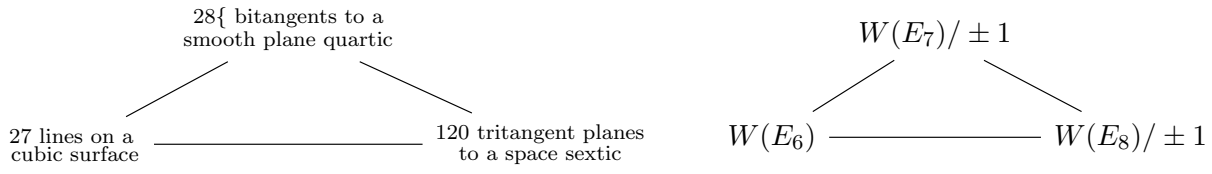
total	2^{2g}
even	$2^{g-1}(2^g+1)$
odd	$2^{g-1}(2^g-1)$

Some small-dimensional examples are as follows:

	elliptic curves	genus 2 curves (e.g. plane quartics)	genus 3 curves	genus 4 curves (e.g. some space sextics)
total	4	16	64	256
even	3	10	36	136
odd	1	6	28	120.

Appendix D. Why this ± 1 in the Weyl groups of E_7 and E_8?

In [Car96, p. 2], E. Cartan floated a *trinity*[31] of enumerative problems; we put them alongside their Galois groups as follows:



Question D.1. Why do these factors of ± 1 appear in the last two groups?

[31] See [Arn97, p. 13].

In some sense this question has no content – they appear because that *is* what the Galois group is when we compute it. Nevertheless it's the type of question someone might ask so maybe we can ask a slightly modified question – *what is different about* $W(E_6)$ *as compared to* $W(E_7)$ *and* $W(E_8)$? The answer comes from considering the reduction of the root lattice modulo two (this is a classical fact, I learned it for the first time in [Loo24]):

Proposition D.2. Let R be any ADE-type root system, and L its lattice. Then $R/\{\pm 1\} \to L/2L$ is injective, and reducing modulo two induces an injection

$$O(R)/\{\pm 1\} \to O(L/2L).$$

This is probably in Bourbaki? But for a proof see [Bea22].

Definition D.3. For $3 \leq n \leq 8$, we define the associated *del Pezzo lattice* $\mathbb{Z}\{E_0, \ldots, E_n\}$ with inner product defined by

$$E_0^2 = -1$$
$$E_i^2 = 1 \text{ for } i > 0$$
$$E_i \cdot E_j = 0 \text{ for } i \neq j.$$

That is, a signature $(1, n)$ form. The vectors of square 2 form a root system as follows:

n	type
3	$A_1 \times A_2$
4	A_4
5	D_5
6	E_6
7	E_7
8	E_8

Proposition D.4 ([Bea22])**.** Let L be a del Pezzo lattice of rank ≥ 4.

(1) Reduction modulo two induces an isomorphism $O(L)/\{\pm 1\} \xrightarrow{\sim} O(L/2L)$.
(2) Reduction modulo two induces an isomorphism from the Weyl group of the lattice or its quotient:

$$\begin{cases} W(L) \xrightarrow{\sim} O(L/2L) & n = 4, 5, 6 \\ W(L)/\{\pm 1\} \xrightarrow{\sim} O(L/2L) & n = 7, 8. \end{cases}$$

Corollary D.5. The Weyl group $W(E_6)$ is faithful on the mod two reduction of its root lattice, however $W(E_7)$ and $W(E_8)$ do not, and one needs to mod out by ± 1 to recover this property.

References

[Arn97] V. I. Arnol'd, *Symplectization, complexification and mathematical trinities*, Fields Institute Communications (1997).

[Aut] Stacks Project Authors, *Stacks Project*, https://stacks.math.columbia.edu/.

[Bea22] Arnaud Beauville, *Reduction mod. 2 of del Pezzo lattices*, September 2022.

[Car96] E. Cartan, *Sur la Reduction a sa Forme Canonique de la Structure d'un Groupe de Transformations Fini et Continu*, American Journal of Mathematics **18** (1896), no. 1, 1.

[Cay69] Prof Cayley, *A Memoir on Quartic Surfaces*, Proceedings of the London Mathematical Society **3** (1869), 19–69. MR 1577187

[Cha64] Michel Chasles, *Construction des coniques qui satisfont à cinq conditions*, Compte rendu des séances de l'académie des sciences **58** (1864), 297–315.

[Coo59] Julian Lowell Coolidge, *A treatise on algebraic plane curves*, Dover Publications, Inc., New York, 1959. MR 120551

[Dol12] Igor V Dolgachev, *Classical Algebraic Geometry: A modern view*, Cambridge University Press, 2012.

[EH16] David Eisenbud and Joe Harris, *3264 and All That*, Cambridge University Press, 2016.

[Far05] Michael Farquhar, *A Treasury of Deception_ Liars, Misleaders, Hoodwinkers, and the Extraordinary True Stories of History's Greatest Hoaxes, Fakes and Frauds*, Penguin Books, 2005.

[GH04] Benedict H. Gross and Joe Harris, *On some geometric constructions related to theta characteristics*, Contributions to Automorphic Forms, Geometry, and Number Theory, Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 279–311. MR 2058611

[Gra10] Jeremy Gray, *Worlds Out of Nothing: A Course in the History of Geometry in the 19th Century*, Springer Undergraduate Mathematics Series, Springer London, London, 2010.

[Har77] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer New York, New York, NY, 1977.

[Har79] Joe Harris, *Galois groups of enumerative problems*, Duke Mathematical Journal **46** (1979), no. 4.

[Her51] Charles Hermite, *Sur les fonctions algébriques*, Comptes Rendus de l'Académie des Sciences **XXXII** (1851).

[Hes55] Otto Hesse, *Über Determinanten und ihre Anwendung in der Geometrie, insbesondere auf Curven vierter Ordnung.*, Journal für die reine und angewandte Mathematik **49** (1855), 243–264.

[Hun96] Bruce Hunt, *The geometry of some special arithmetic quotients*, Lecture Notes in Mathematics, no. 1637, Springer, Berlin ; New York, 1996.

[Jac50] C. G. J. Jacobi, *Beweis des Satzes daß eine Curve nten Grades im Allgemeinen ... (n-2)(n2-9) Doppeltangenten hat.*, Journal für die reine und angewandte Mathematik **40** (1850), 237–260.

[Jor70] M. Camille Jordan, *Traité des substitutions*, Gauthier-Villars, Paris, 1870.

[Kat06] Sheldon Katz, *Enumerative geometry and string theory*, Student Mathematical Library IAS/Park City Mathematical Subseries, 2006.

[Kle80] Steven L. Kleiman, *Chasles's enumerative theory of conics: A historical introduction*, Studies in Algebraic Geometry, MAA Stud. Math., vol. 20, Math. Assoc. America, Washington, DC, 1980, pp. 117–138. MR 589410

[KV24] Avinash Kulkarni and Sameera Vemulapalli, *On intersections of symmetric determinantal varieties and theta characteristics of canonical curves*, Journal of Pure and Applied Algebra **228** (2024), no. 5, 107538.

[Loo24] Eduard Looijenga, *Cubic threefolds moduli and the Monster group*, November 2024.

[Man06] L. Manivel, *Configurations of lines and models of Lie algebras*, Journal of Algebra **304** (2006), no. 1, 457–486.

[MBD16] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and applications of finite groups*, Dover Publications, Inc., New York, 1916. MR 123600

[OD88] David Ortland and Igor V Dolgachev, *Point sets in projective spaces and theta functions*, Astérisque **165** (1988).

[Ron98] Felice Ronga, *Felix Klein's paper on real flexes vindicated*, Banach Center Publications **44** (1998), no. 1, 195–210.

[RTV97] Felice Ronga, Alberto Tognoli, and Thierry Vust, *The number of conics tangent to five given conics: The real case*, Revista Matemática de la Universidad Complutense de Madrid **10** (1997), no. 2, 391–421. MR 1605670

[Ste48] J. Steiner, *Elementare Lösung einer geometrischen Aufgabe, und über einige damit in Beziehung stehende Eigenschaften der Kegelschnitte*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1848** (1848), no. 37, 161–192b.

[Ste57] Jakob Steiner, *Über die Flächen dritten Grades*, Journal für die reine und angewandte Mathematik (Crelles Journal) **53** (1857), 133–141.

[SY21] Frank Sottile and Thomas Yahl, *Galois Groups in Enumerative Geometry and Applications*, August 2021.

[TBS20] Sascha Timme, Paul Breiding, and Bernd Sturmfels, *3264 Conics in a Second*, Notices of the American Mathematical Society **67** (2020), no. 01, 1.

[Web96] H Weber, *Lehrbuch der Algebra*, Braunschweig, 1896.

[Wel06] Jean-Yves Welschinger, *Towards relative invariants of real symplectic four-manifolds*, GAFA Geometric And Functional Analysis **16** (2006), no. 5, 1157–1182.