Mathematische Annalen
https://doi.org/10.1007/s00208-022-02395-8

Mathematische Annalen

Modular functions and resolvent problems

With an appendix by Nate Harman

Benson Farb[1] · Mark Kisin[2] · Jesse Wolfson[3]

Received: 8 January 2020 / Revised: 26 January 2022 / Accepted: 10 March 2022

Abstract
The link between modular functions and algebraic functions was a driving force behind the 19th century study of both. Examples include the solutions by Hermite and Klein of the quintic via elliptic modular functions and the general sextic via level 2 hyperelliptic functions. This paper aims to apply modern arithmetic techniques to the circle of "resolvent problems" formulated and pursued by Klein, Hilbert and others. As one example, we prove that the essential dimension at $p = 2$ for the symmetric groups S_n is equal to the essential dimension at 2 of certain S_n-coverings defined using moduli spaces of principally polarized abelian varieties. Our proofs use the deformation theory of abelian varieties in characteristic p, specifically Serre-Tate theory, as well as a family of remarkable mod 2 symplectic S_n-representations constructed by Jordan. As shown in an appendix by Nate Harman, the properties we need for such representations exist only in the $p = 2$ case. In the second half of this paper we introduce the notion of $\mathcal{E}$-versality as a kind of generalization of Kummer theory, and we prove that

Communicated by Vasudevan Srinivas.

The authors are partially supported by NSF grants DMS-1811772 and Jump Trading Mathlab Research Fund (BF), DMS-1601054 (MK) and DMS-1811846 (JW).
Appendix by Nate Harman Department of Mathematics, University of Michigan, Ann Arbor MI; Email nharman@umich.edu.

✉ Jesse Wolfson
wolfson@uci.edu

Benson Farb
farb@math.uchicago.edu

Mark Kisin
kisin@math.harvard.edu

[1] Department of Mathematics, University of Chicago, Chicago, IL, USA

[2] Department of Mathematics, Harvard University, Cambridge, MA, USA

[3] Department of Mathematics, University of California-Irvine, Irvine, CA, USA

Published online: 02 April 2022

many congruence covers are $\mathcal{E}$-versal. We use these $\mathcal{E}$-versality result to deduce the equivalence of Hilbert's 13th Problem (and related conjectures) with problems about congruence covers.

Contents

1 Introduction

The link between modular functions and algebraic functions was a driving force behind the 19th century development of both. Examples include the solutions by Hermite and Klein of the quintic via elliptic modular functions, degree 7 and 8 equations with Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$ via the level the level 7 modular curve, the general sextic via level 2 hyperelliptic functions, the 27 lines on smooth cubic surfaces via level 3, dimension 2 abelian functions, and the 28 bitangents on a smooth quartic via level 2, dimension 3 abelian functions.[1] With the Nazi destruction of the Göttingen research community this connection was largely abandoned, and the study of algebraic functions and resolvent problems, as pioneered by Klein, Hilbert and others, fell into relative obscurity. The purpose of this paper to reconsider the link between modular functions and classical resolvent problems. We do this from a modern viewpoint, using arithmetic techniques.

Essential dimension at p of modular functions. To fix ideas we work over $\mathbb{C}$. Recall that an *algebraic function* is a finite rational correspondence $X \xrightarrow{1:n} \mathbb{P}^1$; that is, a rational function $f : \tilde{X} \dashrightarrow \mathbb{P}^1$ on some (finite, possibly branched) cover $\tilde{X} \to X$.[2] A fundamental example is the *general degree n polynomial*, equivalently the cover

[1] See e.g. [11–13, 25, 26, 42, 43, 45, 51], as well as [48, 49].

[2] When the functions are understood, we denote an algebraic function simply by the cover $\tilde{X} \to X$.

$$\mathcal{M}_{0,n} \to \mathcal{M}_{0,n}/S_n,$$

where $\mathcal{M}_{0,n}$ denotes the moduli space of n distinct marked points in $\mathbb{P}^1$. When X is a locally symmetric variety f is called a *modular function*. A basic example is the cover $\mathcal{A}_{g,N} \to A_g$ where A_g is the (coarse) moduli space of principally polarized g-dimensional abelian varieties and $\mathcal{A}_{g,N}$ is the moduli of pairs $(A, \mathcal{B})$ with $A \in \mathcal{A}_g$ and $\mathcal{B}$ a symplectic basis for $H_1(A; \mathbb{Z}/N\mathbb{Z})$.

The relationship between modular functions and the solutions of the general degree n polynomial motivated Klein [43, 45], Kronecker [55] and others to ask about the intrinsic complexity of these algebraic functions, as measured by the number of variables to which they can be reduced after a rational change of variables. In modern terms (as defined by Buhler–Reichstein, see e.g. [62]), the *essential dimension* $ed(\tilde{X}/X) \leq \dim(X)$ of an algebraic function is the smallest $d \geq 1$ so that $\tilde{X} \to X$ is the birational pullback of a cover $\tilde{Y} \to Y$ of d-dimensional varieties.

One can also allow, in addition to rational changes of coordinates, the adjunction of radicals or other algebraic functions. This is done by specifying a class $\mathcal{E}$ of covers under which $\tilde{X} \to X$ can be pulled back before taking ed of the resulting cover. This gives the essential dimension $\mathrm{ed}(\tilde{X}/X; \mathcal{E})$ relative to the class $\mathcal{E}$ of "accesory irrationalities". For example, if one fixes a prime p and pulls back by covers of degree prime to p, one obtains the notion of *essential dimension at* p, denoted $\mathrm{ed}(\tilde{X}/X; p)$ (see e.g. [64]). The idea of accessory irrationality was central to the approaches of Klein and Hilbert to solving equations. We axiomatize this notion in Definition 4.1 below and explore its consequences in Sect. 4.

The general degree n polynomial is universal for covers with Galois group S_n, even allowing prime-to-p accessory irrationalities; that is, for all $p \geq 2$ and for $\mathrm{ed}(S_n; p)$ defined as the maximum of $\mathrm{ed}(\tilde{X}/X; p)$ for all S_n-covers $\tilde{X} \to X$, we have:

$$\mathrm{ed}(\mathcal{M}_{0,n}/\mathcal{M}_{0,n}; p) = \mathrm{ed}(S_n; p).$$

With the many examples relating the general degree n polynomial to modular functions, it is natural to ask if the same "maximal complexity property" holds for modular functions. Our first result states that for $p = 2$ this is indeed the case. To explain this, for a subgroup $G \subset \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ set $\mathcal{A}_{g,G} := \mathcal{A}_{g,N}/G$.

Theorem 1 *Let $n \geq 2$, $g = \lceil \frac{n}{2} \rceil - 1$, and let $N \geq 3$ be odd. There exists an embedding $S_n \subset Sp_{2g}(\mathbb{F}_2) \subset Sp_{2g}(\mathbb{Z}/2N\mathbb{Z})$ such that*

$$ed(\mathcal{A}_{g,2N}/\mathcal{A}_{g,S_n}; 2) = \lfloor n/2 \rfloor = ed(S_n; 2).$$

We remark that what we actually prove is the first equality. The second equality then follows from a result of Meyer–Reichstein [59,Corollary 4.2]. In particular, one sees from their result that $\mathrm{ed}(S_n; p)$ takes its maximal value for $p = 2$, so this case is, in some sense, the most interesting.

One ingredient in the proof of Theorem 1 comes from the link between binary forms and hyperelliptic functions; specifically, Jordan proved that the monodromy of the 2-torsion points on the universal hyperelliptic Jacobian gives a mod 2 symplectic

S_n-representation. These remarkable representations were rediscovered and studied by Dickson [18] in 1908. We deduce Theorem 1 by applying the following general result to these representations.

Theorem 2 *Let G be a finite group, and $G \to Sp_{2g}(\mathbb{F}_p)$ a representation. If $U \subset Sp_{2g}$ is the unipotent of a Siegel parabolic then*

$$ed(\mathcal{A}_{g,pN}/\mathcal{A}_{g,G};\, p) \geq \dim_{\mathbb{F}_p} G \cap U(\mathbb{F}_p)$$

Theorem 2 is of most interest for those G which admit a symplectic representation with $\dim_{\mathbb{F}_p} G \cap U(\mathbb{F}_p) = \mathrm{ed}(G;\, p)$, where $\mathrm{ed}(G;\, p)$ is the essential dimension at p of a *versal* branched cover with group G (see Definition 4.4 below). For $G = S_n$, a result of Harman (Theorems A.1 and A.2) says that this is possible only for $p = 2$, and only using the particular mod 2 symplectic representation of Jordan/Dickson! We also show that for G the $\mathbb{F}_q$-points of a split semisimple group of classical type, there is a symplectic representation of G for which the lower bound in Theorem 2 is either equal or nearly equal to the maximal rank of an elementary abelian p-group in G. The only near-misses occur for odd orthogonal groups. Note however, that this rank is in general less than $\mathrm{ed}(G;\, p)$.

***$\mathcal{E}$*-versal modular functions.** Kummer theory gives that for each $d \geq 2$ the cover $\mathbb{P}^1 \to \mathbb{P}^1/(\mathbb{Z}/d\mathbb{Z})$ has the following universal property: any $\mathbb{Z}/d\mathbb{Z}$ cover $\tilde{X} \to X$ is rationally pulled back from it. It follows that $\mathrm{ed}(\tilde{X}/X;\, p) = 1$ for any such $\tilde{X} \to X$. Klein's *Normalformsatz* states that, while the icosahedral cover $\mathbb{P}^1 \to \mathbb{P}^1/A_5$ is not universal in the above sense (indeed $\mathrm{ed}(\mathcal{M}_{0,5} \to \mathcal{M}_{0,5}/A_5) = 2$), there exists a $\mathbb{Z}/2\mathbb{Z}$ accessory irrationality

$$\begin{array}{ccc} \tilde{Y} & \to & \tilde{X} \\ \downarrow & & \downarrow \\ Y & \to & X \end{array}$$

such that $\tilde{Y} \to Y$ is birational to a pullback of $\mathbb{P}^1 \to \mathbb{P}^1/A_5$. This nonabelian version of Kummer's theorem is a kind of classification of actions of A_5 on all varieties. We say in this case that $\mathbb{P}^1 \to \mathbb{P}^1/A_5$ is *$\mathcal{E}$-versal* with respect to any collection $\mathcal{E}$ of covers containing $\mathbb{Z}/2\mathbb{Z}$ covers. Note that this cover is modular; indeed it is equivariantly birational to the cover $\mathbb{H}^2/\Gamma_2(5) \to \mathbb{H}^2/\mathrm{SL}_2(\mathbb{Z})$, where $\mathbb{H}^2$ is the hyperbolic plane and $\Gamma_2(5)$ is the level 5 congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$; here we are using the natural isomorphism $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

In Sect. 4 we axiomatize the idea of $\mathcal{E}$-versality and we give a number of examples (most classically known) of congruence covers that are $\mathcal{E}$-versal for various groups G. The connection between these $\mathcal{E}$-versality results with the first part of this paper is that $\mathcal{E}$-versal G-covers always maximize $\mathrm{ed}(\tilde{X}/X;\, \mathcal{E})$ over all G-covers $\tilde{X} \to X$. In Sect. 4 we apply such $\mathcal{E}$-versality results to exhibit further the close relationship between modular functions and roots of polynomials. Specifically, Hilbert's 13th Problem, and his Sextic and Octic Conjectures (see Sect. 4 for their exact statements) are phrased in terms of the resolvent degree of the degree 6, 7 and 8 polynomials. The *resolvent*

degree $\mathrm{RD}(\tilde{X}/X)$ is the smallest d such that $\tilde{X} \to X$ is covered by a composite of covers, each of essential dimension $\leq d$ (see e.g. [3, 7, 23]). Applying various $\mathcal{E}$-versality results, we deduce in Sect. 4 the equivalence of each of Hilbert's conjectures with a conjecture about the resolvent degree of a specific modular cover. For example, we show the following(see Sect. 4.2 for terminology). For $\Gamma < \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ a lattice, let $M_\Gamma : (\mathbb{H}^2 \times \mathbb{H}^2)/\Gamma$; these are complex-algebraic varieties called *Hilbert modular surfaces*.

Proposition 3 *For $\mathcal{E}$ any class of accessory irrationalities containing all quadratic and cubic covers and composites thereof, the Hilbert modular surface*

$$M_{\widetilde{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}],3)}} \to M_{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])}$$

is $\mathcal{E}$-versal for A_6, where $\widetilde{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}], 3)}$ denotes the kernel of the map

$$SL_2\left(\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]\right) \to PGL_2(\mathbb{F}_9) \cong A_6.$$

In particular, Hilbert's Sextic Conjecture is equivalent to the statement that the resolvent degree of this cover equals 2.

Similarly, we show that such a modular reformulation is possible not only for general polynomials of low degree, but also for each of the algebraic functions considered by Klein and his school [25, 41, 45, 50].

Methods. The proof of Theorem 2 uses a refinement of the results of [24], which is explained in Sect. 1. In *loc. cit*, we used Serre-Tate theory to give lower bounds on the essential at p for the coverings $\mathcal{A}_{g,pN} \to \mathcal{A}_{g,N}$, when restricted to (some) subvarieties $\mathcal{Z} \subset \mathcal{A}_{g,N}$. Here we drop the assumption that $\mathcal{Z}$ is a subvariety and allow certain maps $\mathcal{Z} \to \mathcal{A}_{g,N}$ (cf. Proposition 2.6). In particular, we can apply the resulting estimate to $\mathcal{Z} = \mathcal{A}_{g,G}$ for G a subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_p)$, which yields the lower bound for $\mathrm{ed}(\mathcal{A}_{g,pN}/\mathcal{A}_{g,G}; p)$ in Theorem 2.

One may compare the bounds given by Theorem 2 to those obtained in [24,Sect. 4] for certain finite simple groups of Lie type. The bound in the case of odd orthogonal groups in *loc. cit* is weaker than the one given here because of the restriction on the signature of Hermitian symmetric domains associated to odd orthogonal groups. On the other hand the coverings we consider here correspond to rather more exotic congruence subgroups than those of *loc. cit*.

2 Moduli of Abelian varieties

2.1 Extension classes

2.1.1. Fix a prime p, and let V be a complete discrete valuation ring of characteristic 0, with perfect residue field k of characteristic p, and a uniformizer $\pi \in V$. Let

$A = V[\![x_1, \ldots, x_n]\!]$ be a power series ring over V. We denote by $\mathfrak{m}_A \subset A$ the maximal ideal, and $\bar{\mathfrak{m}}_A = \mathfrak{m}_A/\pi A$. and set $\tilde{X} = \operatorname{Spec} A$, and $X = \operatorname{Spec} A[1/p]$. We will denote by $k[\epsilon] = k[X]/X^2$ the dual numbers over k.

Recall [24,3.1.2] that there is a commutative diagram

$$\begin{array}{ccc} A^\times/(A^\times)^p & \xrightarrow{\sim} & \operatorname{Ext}^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \\ \downarrow & & \downarrow \\ A[1/p]^\times/(A[1/p]^\times)^p & \xrightarrow{\sim} & \operatorname{Ext}^1_{X}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \end{array}$$

where the terms on the right are extensions as $\mathbb{Z}/p\mathbb{Z}$-sheaves. The vertical maps are injective, and the extensions in the image of the map on the right are called *syntomic*. There is also a map [24,3.1.5]

$$\theta_A : \operatorname{Ext}^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \xrightarrow{\sim} A^\times/(A^\times)^p \to \bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2.$$

which sends a class represented by a function $f \in 1 + \mathfrak{m}_A$ to $f - 1$.

Lemma 2.1 *Let $\mathscr{U} \subset Ext^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ be an $\mathbb{F}_p$-subspace of dimension $\leq n$. Suppose that for every map $h : A \to k[\epsilon]$ the image of $\mathscr{U}$ under the induced map*

$$Ext^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \to Ext^1_{Spec\, k[\epsilon]}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \tag{2.1}$$

is nontrivial. Then the map

$$\theta_A : \mathscr{U} \otimes_{\mathbb{F}_p} k \to \bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2 \tag{2.2}$$

is an isomorphism; in particular $\dim_{\mathbb{F}_p} \mathscr{U} = n$.

Proof Since the image of $\mathscr{U}$ under 2.1 is nontrivial, the composite

$$\theta_A : \mathscr{U} \otimes_{\mathbb{F}_p} k \to \bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2 \to \epsilon \cdot k$$

is nontrivial for every h. This implies that 2.2 is surjective, and since $\dim_{\mathbb{F}_p} \mathscr{U} \leq n$ it is injective, and $\dim_{\mathbb{F}_p} \mathscr{U} = n$. □

2.1.2. We call a subspace $\mathscr{U} \subset \operatorname{Ext}^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ satisfying the conditions of Lemma 2.1 *nondegenerate*, and we fix such a subspace. Now assume that V contains a primitive p^{th} root of unity, and fix a geometric point $\bar{x}$ of X. Then

$$\operatorname{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p) \xrightarrow{\sim} H^1(X, \mu_p) = H^1_{\text{ét}}(X, \mu_p) = \operatorname{Hom}(\pi_1(X, \bar{x}), \mu_p).$$

If $\mathscr{U}' \subset \mathscr{U}$ is a subspace, denote by $X(\mathscr{U}') \to X$ the finite étale cover corresponding to $\mathscr{U}'$. That is, $X(\mathscr{U}')$ is the cover corresponding to the intersection of all the elements of $\operatorname{Hom}(\pi_1(X, \bar{x}), \mu_p)$ that are images of elements of $\mathscr{U}'$. We let $\tilde{X}' = \operatorname{Spec} A(\mathscr{U}')$ denote the normalization of $\tilde{X}$ in $X(\mathscr{U}')$.

Lemma 2.2 *For any $\mathscr{U}' \subset \mathscr{U}$ the ring $A(\mathscr{U}')$ is a power series ring over V. Further,*

$$\dim_k \mathfrak{T}(\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2 \to \bar{\mathfrak{m}}_{A(\mathscr{U}')}/\mathfrak{m}^2_{A(\mathscr{U}')}) = \dim_{\mathbb{F}_p}(\mathscr{U}/\mathscr{U}'). \tag{2.3}$$

Proof Let $f_1, \ldots, f_r \in A^\times$ be elements with $1 - f_i \in \mathfrak{m}_A$, and such that the images of $f_1, \ldots, f_r$ in $\mathrm{Ext}^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ form an $\mathbb{F}_p$-basis for $\mathscr{U}'$. By definition, $X(\mathscr{U}') = \mathrm{Spec}\, A[1/p](\sqrt[p]{f_1}, \ldots, \sqrt[p]{f_r})$. To prove the first claim, it suffices to show that

$$A(\sqrt[p]{f_1}, \ldots, \sqrt[p]{f_r}) = A[z_1, \ldots, z_r]/(z_i^p - f_i)$$

is a power series ring over V. Since $\mathscr{U}$ is nondegenerate, the images of $f_1, \ldots, f_r$ are k-linearly independent in $\mathfrak{m}_A/\mathfrak{m}_A^2$. Hence, after a change of coordinates, we can assume that $A \xrightarrow{\sim} V[\![x_1, \ldots, x_n]\!]$ with $x_i = f_i - 1$ for $i = 1, \ldots r$. Then we have

$$A[z_1, \ldots, z_r]/(z_i^p - f_i) \xrightarrow{\sim} V[\![z_1 - 1, \ldots, z_r - 1, x_{r+1}, \ldots, x_n]\!].$$

This also shows 2.3, as both sides are equal to $n - r$. □

2.2 Monodromy on the ordinary locus

2.2.1. Fix an integer $g \geq 1$, a prime $p \geq 2$, and a positive integer $N \geq 2$ coprime to p. Consider the ring $\mathbb{Z}[\zeta_N][1/N]$, where ζ_N is a primitive Nth root of 1. Denote by $\mathcal{A}_{g,N}$ the $\mathbb{Z}[\zeta_N][1/N]$-scheme which is the coarse moduli space of principally polarized abelian schemes A of dimension g equipped with a basis of $A[N]$ that is symplectic with respect to the Weil pairing defined by ζ_N. When $N \geq 3$, this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_N][1/N]$. For a $\mathbb{Z}[\zeta_N][1/N]$-algebra B, denote by $\mathcal{A}_{g,N/B}$ the base change of $\mathcal{A}_{g,N}$ to B. If no confusion is likely to result, we sometimes denote this base change simply by $\mathcal{A}_{g,N}$.

From now on, unless stated otherwise, we assume that $N \geq 3$ and we let $\mathcal{A} \to \mathcal{A}_{g,N}$ be the universal abelian scheme. The p-torsion subgroup $\mathcal{A}[p] \subset \mathcal{A}$ is a finite flat group scheme over $\mathcal{A}_{g,N}$ which is étale over $\mathbb{Z}[\zeta_N][1/Np]$. Let $x \in \mathcal{A}_{g,N}$ be a point with residue field $\kappa(x)$ of characteristic p, and $\mathcal{A}_x$ the corresponding abelian variety over $\kappa(x)$.

The set of points x such that $\mathcal{A}_x$ is ordinary is an open subscheme $\mathcal{A}^{\mathrm{ord}}_{g,N} \subset \mathcal{A}_{g,N} \otimes \mathbb{F}_p$. We denote by $\widehat{\mathcal{A}}^{\mathrm{ord}}_{g,N}$ the formal completion of $\mathcal{A}_{g,N}$ along $\mathcal{A}^{\mathrm{ord}}_{g,N}$. We denote by $\mathcal{A}^{\mathrm{ord,an}}_{g,N}$ the "generic fibre" of $\widehat{\mathcal{A}}^{\mathrm{ord}}_{g,N}$ as a p-adic analytic space.[3]

Denote by k an algebraically closed perfect field of characteristic p, and let $K/W[1/p]$ be a finite extension with ring of integers $\mathcal{O}_K$ and uniformizer π. Assume that K is equipped with a choice of primitive N^{th} root of 1, $\zeta_N \in K$, so that we may consider all the objects introduced above over $\mathcal{O}_K$. Let $\bar{K}/K$ be an algebraic closure.

[3] The reader may think of any version of the theory of p-adic analytic spaces they prefer (Tate, Raynaud, Berkovich, or Hüber's adic spaces), as this will have no bearing on our arguments.

Proposition 2.3 *Fix a geometric point $x \in \widehat{\mathcal{A}}_{g,N}^{ord,an}(\bar{K})$ and denote by $\bar{x} \in \mathcal{A}_{g,N}^{ord}$ its reduction.The covering $\mathcal{A}_{g,pN} \to \mathcal{A}_{g,N}$ corresponds to a surjective representation*

$$\pi_1(\mathcal{A}_{g,N}, x) \to Sp_{2g}(\mathbb{F}_p). \tag{2.4}$$

1. *There exists a Siegel parabolic $P \subset Sp_{2g/\mathbb{F}_p}$ with unipotent radical U, such that 2.4 induces a surjective representation*

$$\pi_1(\widehat{\mathcal{A}}_{g,N}^{ord,an}, x) \to P(\mathbb{F}_p). \tag{2.5}$$

2. *Let $A = \widehat{\mathcal{O}}_{\mathcal{A}_{g,N},\bar{x}}$ be the completion of the local ring at $\bar{x}$. Then (2.4) induces a surjective representation*

$$\pi_1(Spec\, A[1/p], x) \to U(\mathbb{F}_p). \tag{2.6}$$

Proof The first claim is well known. Indeed, the existence of the Weil pairing on $\mathcal{A}[p]$ implies that $\mathcal{A}_{g,pN}$ corresponds to a symplectic representation. A comparison with the topological fundamental group shows that the image of the *geometric* fundamental group $\pi_1(\mathcal{A}_{g,N} \otimes_K \bar{K}, x)$ is $\mathrm{Sp}_{2g}(\mathbb{F}_p)$, so the representation is surjective.

Now recall, that a *Siegel parabolic* is the stabilizer of a maximal isotropic subspace in the underlying vector space of a symplectic representation. Equivalently it is a parabolic with abelian unipotent radical. All such parabolics are conjugate. Over $\widehat{\mathcal{A}}_{g,N}^{\mathrm{ord}}$ the finite flat group scheme $\mathcal{A}[p]$ is an extension

$$0 \to \mathcal{A}[p]^m \to \mathcal{A}[p] \to \mathcal{A}[p]^{\text{ét}} \to 0 \tag{2.7}$$

of an étale by a multiplicative group scheme, where étale locally $\mathcal{A}[p]^{\text{ét}} \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^g$ and $\mathcal{A}[p]^m \xrightarrow{\sim} \mu_p^g$. The Weil pairing induces a map of group schemes

$$\mathcal{A}[p] \times \mathcal{A}[p] \to \mu_p.$$

which identifies $\mathcal{A}[p]$ with its Cartier dual, and induces an isomorphism $\mathcal{A}[p]^m$ with the Cartier dual of $\mathcal{A}[p]^{\text{ét}}$. In particular, this shows that $\mathcal{A}[p]_x^m \subset \mathcal{A}[p]_x$ corresponds to a maximal isotropic subspace under the Weil pairing. This defines a Siegel parabolic such that (2.4) maps $\pi_1(\widehat{\mathcal{A}}_{g,N}^{\mathrm{ord,an}}, x)$ into $P(\mathbb{F}_p)$. By [22,V, Prop. 7.2] the image of the composite

$$\pi_1(\widehat{\mathcal{A}}_{g,N}^{\mathrm{ord,an}}, x) \to P(\mathbb{F}_p) \to (P/U)(\mathbb{F}_p)$$

is surjective. Hence it suffices to prove (2).

For this, we adopt the notation of 2.1 applied with A as in (2). Since we are assuming k is algebraically closed, over A, the group schemes $\mathcal{A}[p]^{\text{ét}}$ and $\mathcal{A}[p]^m$ are isomorphic to $(\mathbb{Z}/p\mathbb{Z})^g$ and μ_p^g respectively. In particular, the map (2.6) factors through $U(\mathbb{F}_p)$. Let $\mathscr{U} \subset \mathrm{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ be the span of the g^2 syntomic extension classes defining the extension (2.7). Note that $U(\mathbb{F}_p)$ is an elementary abelian p-group of rank $n =$

$\dim_{\mathbb{F}_p} U = \dim \mathcal{A}_g = \binom{g+1}{2}$. Any $\mathbb{F}_p$-linear map $s : U(\mathbb{F}_p) \to \mathbb{F}_p$ induces a representation

$$\pi_1(\operatorname{Spec} A[1/p], x) \to \mu_p(\bar{K}) \xrightarrow{\sim} \mathbb{F}_p$$

(choosing pth root of unity), and hence a class in

$$c(s) \in \operatorname{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p) \xrightarrow{\sim} H^1(X, \mathbb{F}_p).$$

The subspace $\mathscr{U}$ is the span of all the classes $c(s)$. This shows $\dim \mathscr{U} \leq n$, with equality only if (2.6) is surjective. However, by [24,3.2.2], one sees that $\mathscr{U}$ satisfies the conditions of Lemma 2.1, so that $\dim \mathscr{U} = n$, which completes the proof of the lemma. □

Corollary 2.4 *With the notation above, $Hom_{\mathbb{F}_p}(U(\mathbb{F}_p), \mathbb{F}_p)$ is naturally identified with a nondegenerate subspace $\mathscr{U} \subset Ext^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.*

Proof The proof of the Proposition 2.3 shows that there is a natural map

$$\operatorname{Hom}_{\mathbb{F}_p}(U(\mathbb{F}_p), \mathbb{F}_p) \to \operatorname{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$$

whose image $\mathscr{U}$ is a nondegenerate subspace of dimension $n = \dim_{\mathbb{F}_p} U$. □

2.3 Essential dimension

2.3.1. We refer the reader to [24,Sect. 2] for the definitions and facts we will need about essential dimension and essential dimension at p. We remind the reader that for K a field and $Y \to X$ a finite étale map of finite type K-schemes, $\operatorname{ed}(Y/X; p)$ denotes the essential dimension at p of $Y_{\bar{K}} \to X_{\bar{K}}$, where $\bar{K}$ is an algebraic closure of K.

2.3.2. We continue to use the notation introduced above. In particular $A = \widehat{\mathcal{O}}_{\mathcal{A}_{g,N},\bar{x}}$ denotes the complete local ring which is a power series ring over $\mathcal{O}_K$ in $n = \binom{g+1}{2}$ variables.

Lemma 2.5 *Let $g : A \to B$ and $f : C \to B$ be maps of power series rings over $\mathcal{O}_K$, with f a flat map. Suppose there exists a finite étale covering $Y' \to Spec\, C[1/p]$ and an isomorphism of étale coverings $\varepsilon : f^*Y' \xrightarrow{\sim} g^*\mathcal{A}[p]$ over Spec $B[1/p]$. Then*

$$\dim(\mathfrak{m}_A/\mathfrak{m}_A^2 \to \mathfrak{m}_B/\mathfrak{m}_B^2) \subset \dim(\mathfrak{m}_C/\mathfrak{m}_C^2 \to \mathfrak{m}_B/\mathfrak{m}_B^2).$$

In particular,

$$\dim_k \mathfrak{m}_C/\mathfrak{m}_C^2 \geq \dim_k \mathfrak{m}_A/\mathfrak{m}_A^2 \to \mathfrak{m}_B/\mathfrak{m}_B^2).$$

Proof By [24,2.1.8], we may assume that Y' is an extension of a constant étale group scheme by a constant multiplicative group scheme, and that ε is an isomorphism of

extensions. By [24,3.1.4, 3.1.5], the extension Y' is syntomic, and we may assume that the isomorphism $f^*Y' \xrightarrow{\sim} g^*\mathcal{A}[p]$ extends to an isomorphism of finite flat group schemes (which automatically respects the extension structure) over Spec B.

Now let $h : B \to k[\epsilon]$ be any map which vanishes on the image of $\bar{\mathfrak{m}}_C/\bar{\mathfrak{m}}_C^2$, so that h induces the constant map $C \to k$. Then $h^*f^*Y' \xrightarrow{\sim} h^*g^*\mathcal{A}[p]$ is a split extension over Spec $k[\epsilon]$. It follows from [24,3.2.2] that $h \circ g(\mathfrak{m}_A) = 0$, which proves the inclusion in the lemma. □

2.3.3. We introduce the following notation. For a map $f : X \to Y$ of smooth k-schemes, we let

$$r(f) = \max_{x \in X(k)} \dim_k \Im(\bar{\mathfrak{m}}_{f(x)}/\bar{\mathfrak{m}}_{f(x)}^2 \to \bar{\mathfrak{m}}_x/\bar{\mathfrak{m}}_x^2)$$

For f a map of smooth $\mathcal{O}_K$-schemes, set $r(f) = r(f \otimes k)$. Note that $r(f)$ does not change if we restrict f to a dense open subset in X.

Proposition 2.6 *Let $\mathcal{Z}$ be a smooth, connected $\mathcal{O}_K$-scheme, and let $\mathcal{Z} \to A_{g,N/\mathcal{O}_K}$ be a map of $\mathcal{O}_K$-schemes such that the image of the special fiber, $\mathcal{Z}_k$, meets the ordinary locus $\mathcal{A}_{g,N}^{ord} \subset \mathcal{A}_{g,N/k}$. Then*

$$ed(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K; p) \geq r(f)$$

Proof The proof of this is almost the same as that of Theorem [24,3.2.6]. The only difference is that we use Lemma 2.5 instead of Lemma 3.2.4 of *loc. cit* at the end of the proof. □

Example 2.7 Let $\mathcal{H}_g$ denote the moduli of hyperelliptic curves of genus g. Let $\mathcal{H}_g[n]$ be the moduli of pairs $(C, \mathcal{B})$ where C is a hyperelliptic genus g curve and $\mathcal{B}$ is a symplectic basis for $H_1(C; \mathbb{Z}/n\mathbb{Z})$. Let $\tau : \mathcal{H}_{g/\mathcal{O}_K} \to \mathcal{A}_{g/\mathcal{O}_K}$ denote the Torelli map. By [56,Theorem 1.2], τ is an embedding only when the characteristic of k is prime to 2; when k is of characteristic 2, $r(\tau) = g+1$. Because of this, [24,Theorem 3.2.6] does not give a lower bound on $\mathrm{ed}(\mathcal{H}_g[2]/\mathcal{H}_g; 2)$. Using Proposition 2.6 above instead, as well as the argument of [24,Corollary 3.2.7], we obtain

$$\mathrm{ed}(\mathcal{H}_g[2]/\mathcal{H}_g; 2) \geq g + 1.$$

Remark 2.8 More generally, Proposition 2.6 gives an arithmetic tool for obtaining lower bounds on the essential dimension at p, analogous to the "fixed point method" (cf. [62]). As forthcoming work of Brosnan–Fakhrudin [8] demonstrates, the fixed point method applied to the toroidal boundary recovers the bounds of Theorem 1 and similar bounds for non-compact locally symmetric varieties (including those not of Hodge type); it also allows one to use toroidal boundary components other than those corresponding to Siegel parabolics. However, as remarked in [24], we are not aware of methods besides Proposition 2.6 that apply to unramified nonabelian covers of compact varieties.

2.3.4. Proposition 2.3 implies that the monodromy group of $\mathcal{A}_{g,pN} \to \mathcal{A}_{g,N}$ can be identified with $\mathrm{Sp}_{2g}(\mathbb{F}_p)$. Fix such an identification. Let G be a subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_p) \subset \mathrm{Sp}_{2g}(\mathbb{Z}/pN\mathbb{Z})$. Denote by $\mathcal{A}_{g,G} \to \mathcal{A}_{g,N}$ the finite, normal, covering corresponding to G.

Theorem 2.9 *Let p be a prime, and let $N \geq 3$ be prime to p. $G \subset Sp_{2g}(\mathbb{F}_p) \subset Sp_{2g}(\mathbb{Z}/pN\mathbb{Z})$. Then*

$$ed(\mathcal{A}[p]|_{\mathcal{A}_{g,G}}/\mathcal{A}_{g,G};\, p) \geq \max_U \dim_{\mathbb{F}_p} U \cap G,$$

where the maximum on the right hand side is over all unipotent radicals of Siegel parabolics in $Sp_{2g}(\mathbb{F}_p)$.

Proof Let $U_0 \subset \mathrm{Sp}_{2g}(\mathbb{F}_p)$ be an abelian unipotent subgroup such that $\dim_{\mathbb{F}_p} U_0 \cap G$ achieves the maximum. Let $U \subset \mathrm{Sp}_{2g}/_{\mathbb{F}_p}$ be the abelian unipotent subgroup defined in Proposition 2.3. Because all Siegel parabolics are conjugate in $\mathrm{Sp}_{2g}(\mathbb{F}_p)$, there exists a conjugate of G, denoted $G' \subset \mathrm{Sp}_{2g}(\mathbb{F}_p)$, such that

$$\dim_{\mathbb{F}_p} U(\mathbb{F}_p) \cap G' = \dim_{\mathbb{F}_p} U_0 \cap G.$$

Because conjugate subgroups give isomorphic covers, and because $\mathrm{ed}(-;\, p)$ is a birational invariant,

$$\mathrm{ed}(\mathcal{A}[p]|_{\mathcal{A}_{g,N,G}}/\mathcal{A}_{g,N,G};\, p) = \mathrm{ed}(\mathcal{A}[p]|_{\mathcal{A}_{g,N,G'}}/\mathcal{A}_{g,N,G'};\, p).$$

It therefore suffices to prove the theorem under the assumption that $U_0 = U(\mathbb{F}_p)$. For this, it suffices to consider the case $G = U(\mathbb{F}_p) \cap G$. In the following we slightly abuse notation and write U for $U(\mathbb{F}_p)$.

Let $x \in \mathcal{A}_{g,N}(k)$ be a point in the ordinary locus. By (2) of Proposition 2.3, there exists $y \in \mathcal{A}_{g,pN}(k)$ and $x' \in A_{g,N,U}(k)$ with y mapping to x' and x, such that the natural map

$$A := \widehat{\mathcal{O}}_{\mathcal{A}_{g,N},x} \to \widehat{\mathcal{O}}_{\mathcal{A}_{g,N,U},x'}$$

is an isomorphism, and such that, if $B = \widehat{\mathcal{O}}_{\mathcal{A}_{g,pN},y}$, then

$$\mathrm{Spec}\, B[1/p] \to \mathrm{Spec}\, A[1/p]$$

is a U-covering.

Let $\mathscr{U} = \mathrm{Hom}_{\mathbb{F}_p}(U, \mathbb{F}_p)$, and $\mathscr{U}'_G = \mathrm{Hom}_{\mathbb{F}_p}(U/(U \cap G), \mathbb{F}_p)$. By Corollary 2.4, $\mathscr{U}$ is identified with a nondegenerate subspace of $\mathrm{Ext}^1_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ where $X = \mathrm{Spec}\, A[1/p]$. Now let $A' = \widehat{\mathcal{O}}_{\mathcal{A}_{g,N,U\cap G},\bar{x}''}$, where x'' denotes the image of y in $\mathcal{A}_{g,N,U\cap G}$. Since $\mathcal{A}_{g,N,U\cap G}$ is normal, using the notation of 2.1.2., we have $A' = A(\mathscr{U}'_G)$. Hence, by Lemma 2.2, we have

$$\dim_k \Im(\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2 \to \bar{\mathfrak{m}}_{A'}/\mathfrak{m}_{A'}^2) = \dim_{\mathbb{F}_p} U \cap G,$$

and A' is a power series ring over $\mathcal{O}_K$.

Since x was any point in the ordinary locus, this shows that $r(f) \geq \dim_{\mathbb{F}_p} U \cap G$, where $f : \mathcal{A}_{g,N,U\cap G} \to \mathcal{A}_{g,N}$, and that $\mathcal{A}_{g,N,U\cap G}$ is smooth over $\mathcal{O}_K$, over the ordinary locus of $\mathcal{A}_{g,N}$. Combining this with Proposition 2.6 proves the theorem. □

3 Modular symplectic representations of finite groups

3.1 General finite groups

Let p be prime, G a finite group and V a faithful, finite-dimensional G-representation over $\mathbb{F}_p$. The pairing

$$ev\colon V \otimes V^\vee \to \mathbb{F}_p$$

extends to a G-invariant symplectic form on $V \oplus V^\vee$. We refer to the associated representation

$$G \to \mathrm{Sp}(V \oplus V^\vee)$$

as the *diagonal (symplectic) representation* associated to V.

Lemma 3.1 *Let $H \subset G$ be an elementary abelian p-subgroup, such that H maps to the unipotent radical of a maximal parabolic in $GL(V)$. Then there exists a Siegel parabolic of $P \subset Sp(V \oplus V^\vee)$ with unipotent radical U such that, under the diagonal representation associated to V,*

$$H \subset U \cap G.$$

Proof Any maximal parabolic in $\mathrm{GL}(V)$ is the stabilizer $P(W)$ of a subspace $W \subset V$. Let $U(W)$ denote the unipotent radical of $P(W)$. Let $W^\perp \subset V^\vee$ denote the dual subspace. Then $W \oplus W^\perp$ is a Lagrangian subspace of $V \oplus V^\vee$, and

$$\mathrm{GL}(V) \cap \mathrm{Stab}_{\mathrm{Sp}(V\oplus V^\vee)}(W \oplus W^\perp) = \mathrm{Stab}_{\mathrm{GL}(V)}(W) = P(W).$$

Hence

$$\mathrm{GL}(V) \cap U(W \oplus W^\perp) = U(W),$$

where $U(W \oplus W^\perp)$ is the unipotent radical of $\mathrm{Stab}_{\mathrm{Sp}(V\oplus V^\vee)}(W \oplus W^\perp)$, the Siegel parabolic corresponding to $W \oplus W^\perp$. In particular $H \subset U(W) \subset U(W \oplus W^\perp)$, the Siegel parabolic corresponding to $W \oplus W^\perp$. □

3.1.1. Let

$$s_p(G) := \max_{U\subset \mathrm{GL}(V)} \dim_{\mathbb{F}_p} U \cap G$$

where the maximum is taken over all faithful representations G of V, and unipotents U of maximal parabolics in $\mathrm{GL}(V)$. Proposition 3.1 and Theorem 2.9 immediately imply the following.

Corollary 3.2 *For some g, there exists a congruence cover $\mathcal{A}_{g,p} \to \mathcal{A}_{g,G}$ with*

$$ed(\mathcal{A}_{g,p}/\mathcal{A}_{g,G};\, p) \geq s_p(G).$$

Remark 3.3 While Corollary 3.2 implies that $\mathrm{ed}(G;\, p) \geq s_p(G)$, this is not hard to show directly, e.g. by [9,Lemma 4.1]. In fact, let

$$r_p(G) := \max_{H \subset G} \dim_{\mathbb{F}_p} H$$

where the maximum is taken over all elementary abelian p-groups $H \subset G$. Then $\mathrm{ed}(G;\, p) \geq r_p(G) \geq s_p(G)$. The novelty of Corollary 3.2 is that (a) this lower bound can be realized by an explicit congruence cover; and (b) the congruence cover, and thus the lower bound, comes from modular representation theory at the relevant prime, rather than from ordinary representation theory in characteristic 0 (as in e.g. [9] or the theorem of Karpenko–Merkurjev [40]).

The corollary is most interesting in those cases where $s_p(G)$ is large. In the remainder of this section we give examples where $s_p(G)$ is equal to, or at least very close to $r_p(G)$. These consist of the case of alternating groups when $p = 2$, and the case where G is the $\mathbb{F}_q$-points of a split semisimple group of classical type.

3.2 The groups S_n and A_n

We now specialize to the symmetric groups S_n and the alternating groups A_n.

3.2.1. We would like to apply Corollary 3.2 to the case of symmetric and alternating groups. Meyer–Reichstein [59,Corollary 4.2] proved that $\mathrm{ed}(S_n;\, p) = r_p(S_n)$ and similarly for A_n for all n and p. However, in Appendix A, Harman shows that for $p > 2$, $s_p(S_n) < r_p(S_n)$ and similarly for A_n. The purpose of this section is to show—see Proposition 3.4 below—that one has $s_2(S_n) = r_2(S_n)$ for all n, and $s_2(A_n) = r_2(A_n)$ (resp. $s_2(A_n) = r_2(A_n) - 1$) for $n = 2, 3$ (resp. 0, 1) modulo 4. This uses a remarkable mod 2 symplectic representation of S_n, discovered by Dickson. Harmon's results imply that for $n \geq 5$, this is the only mod 2 representations for which the unipotent of a maximal parabolic meets S_n in a maximal elementary abelian 2-group.

Recall the "permutation irrep" V of S_n over $\mathbb{F}_p$.[4] For $p \nmid n$ this is the analogue over $\mathbb{F}_p$ of the standard permutation irrep in characteristic 0, i.e. the invariant hyperplane

$$V = \{(a_1, \ldots, a_n) \in \mathbb{F}_p^n \mid \sum a_i = 0\}$$

For $p \mid n$ the diagonal line $\Delta := \{(a, \ldots, a)\} \subset \mathbb{F}_p^n$ is an invariant subspace of the invariant hyperplane, and

$$V = \{(a_1, \ldots, a_n) \in \mathbb{F}_p^n \mid \sum a_i = 0\}/\Delta.$$

[4] The results of Dickson [18] and Wagner [71, 72] show that the permutation irrep is a minimal-dimensional faithful irrep for $n > 8$ and $p = 2$, or for $n > 6$ and p odd.

Dickson [18] showed that over $\mathbb{F}_2$, the permutation irrep of S_n is a symplectic representation. Let

$$d_n := \left\lceil \frac{n}{2} \right\rceil - 1,$$

so that Dickson's representation gives a "Dickson embedding" $S_n \subset \mathrm{Sp}_{2d_n}(\mathbb{F}_2)$.

Proposition 3.4 *Let $N \geq 3$ be odd. For all $n \geq 2$, consider the Dickson embedding $S_n \subset Sp_{2d_n}(\mathbb{F}_2) \subset Sp_{2d_n}(\mathbb{Z}/2N\mathbb{Z})$. There exists a Siegel parabolic with unipotent radical U such that*

$$\dim_{\mathbb{F}_2} U \cap S_n = \left\lfloor \frac{n}{2} \right\rfloor,$$
$$\dim_{\mathbb{F}_2} U \cap A_n = \left\lfloor \frac{n}{2} \right\rfloor - 1.$$

By Theorem 2.9, for all $n \geq 1$:

$$ed(\mathcal{A}_{d_n,2N}/\mathcal{A}_{d_n,S_n}; 2) = \left\lfloor \frac{n}{2} \right\rfloor = ed(S_n; 2),$$
$$ed(\mathcal{A}_{d_n,2N}/\mathcal{A}_{d_n,A_n}; 2) = \left\lfloor \frac{n}{2} \right\rfloor - 1,$$

i.e.

$$ed(\mathcal{A}_{d_n,2N}/\mathcal{A}_{d_n,A_n}; 2) = \begin{cases} ed(A_n; 2) - 1 & n = 0, 1 \ mod\ 4 \\ ed(A_n; 2) & n = 2, 3 \ mod\ 4 \end{cases}$$

Proof Let V denote the permutation irrep of $_n$ over $\mathbb{F}_2$, as in [18], i.e.

$$V = H/\Delta = \left\{ (x_1, \ldots, x_{2\lceil \frac{n}{2} \rceil}) \in \mathbb{F}_2^{2\lceil \frac{n}{2} \rceil} \;\middle|\; \sum_i x_i = 0 \right\} / \{(x, \ldots, x) \in \mathbb{F}_2\}$$

A convenient basis for V is given by the cosets in H of

$$e_i := [(\underbrace{0, \ldots, 1, \ldots, 0}_{1 \text{ in the } ith \text{ place}}, 0, 1)]$$

for $i = 1, \ldots, 2d_n$. With respect to this basis the action of $S_{2d_n} \subset S_n$ is the standard permutation action of S_{2d_n} on $\mathbb{F}_2^{2d_n}$. Dickson [18,p. 124] proved that the S_n action on $\mathbb{F}_2^{2d_n}$ preserves the symplectic form $\sum_{1 \leq i \neq j \leq d_n} x_i y_j$. We now change basis for ease of studying a Lagrangian. Let

$$\omega_i := e_{2i-1} + e_{2i}$$

$$\omega_i^\vee = \textstyle\sum_{j=0}^{2i-1} e_j.$$

A straightforward computation shows that the planes $W = \langle \{\omega_i\}_{i=1}^n \rangle$ and $W^\perp = \langle \{\omega_i^\vee\}_{i=1}^n \rangle$ are dual Lagrangians written with dual Lagrangian bases.

Now fix W and let $P := \mathrm{Stab}(W)$ be the corresponding Siegel parabolic with unipotent U. From the Lagrangian basis for W, we see that

$$\mathbb{F}_2^{\lfloor \frac{n}{2} \rfloor} = \left\langle (12), (34), \ldots, \left(2 \left\lfloor \frac{n}{2} \right\rfloor - 1\ 2 \left\lfloor \frac{n}{2} \right\rfloor\right) \right\rangle \subset U \cap S_n \tag{3.1}$$

But this is a maximal elementary abelian 2-group in S_n, so (3.1) is an equality. Thus

$$U \cap A_n = \left\langle (12)(34), \ldots, (12)\left(2 \left\lfloor \frac{n}{2} \right\rfloor - 1\ 2 \left\lfloor \frac{n}{2} \right\rfloor\right) \right\rangle = \mathbb{F}_2^{\lfloor \frac{n}{2} \rfloor - 1}$$

as claimed. □

3.3 Finite groups of Lie type

Proposition 3.5 *Let $q = p^r$, and $G = H(\mathbb{F}_q)$, where H is one of the semisimple Lie groups SL_m, SO_{2m+1}, Sp_{2m} with $m \geq 2$ or SO_{2m}, with $m \geq 4$. Let $\rho : H \to GL(V)$ be the standard representation of H over $\mathbb{F}_q$. Then there exists a parabolic $P(W) \subset GL(V)$ with unipotent radical U, such that $\dim_{\mathbb{F}_q} W = \lfloor \frac{\dim V}{2} \rfloor$, and $r'_p(G) := \dim_{\mathbb{F}_q} G \cap U$ satisfies:*

- *If $G = SL_m(\mathbb{F}_q)$, then $r'_p(G) = \lfloor \frac{m^2}{4} \rfloor$.*
- *If $G = Sp_{2m}(\mathbb{F}_q)$ then $r'_p(G) = \frac{m(m+1)}{2}$.*
- *If $G = SO_{2m}(\mathbb{F}_q)$ then $r'_p(G) = \frac{m(m-1)}{2}$.*
- *If $G = SO_{2m+1}(\mathbb{F}_q)$ then $r'_p(G) = \frac{m(m-1)}{2}$.*

We have $r \cdot r'_p(G) = r_p(G)$ in all cases except if $G = SO_{2m+1}$, in which case $r_p(G)/r = \frac{m(m+1)}{2}$ if q is even and $r_p(G)/r = \frac{m(m-1)}{2} + 1$ (resp. 5, resp. 3) if q is odd and $m \geq 4$, (resp. $m = 3$, resp. $m = 2$).

Proof We use the standard representations of the root systems of each of the groups H. In each case, we will recall the weights appearing in V, specify the subspace $W \subset V$, and describe a subgroup $U_G \subset H$ as a sum of root spaces. In each case if r is a root appearing in U_G and w, w' are weights appearing in W and V/W respectively, then $r + w$ does not appear in V, and $r + w'$ does not appear in V/W. This implies that $U_G \subset H \cap U$.

If $G = \mathrm{SL}_m(\mathbb{F}_q)$, then the weights of V are $e_1, \ldots, e_m$, and $W = \langle e_1, \ldots, e_{\lfloor \frac{m}{2} \rfloor} \rangle$. The roots appearing in U_G are $e_i - e_j$ with $i \leq \lfloor \frac{m}{2} \rfloor < j$.

If $G = \mathrm{Sp}_{2m}(\mathbb{F}_q)$, then the weights of V are $\pm e_1, \ldots, \pm e_m$, and $W = \langle e_1, \ldots, e_m \rangle$. The roots appearing in U_G are $e_i + e_j$ and $2e_i$ for $1 \leq i < j \leq m$.

If $G = \mathrm{SO}_{2m}(\mathbb{F}_q)$, then the weights of V are $\pm e_1, \ldots, \pm e_m$, and $W = \langle e_1, \ldots, e_m \rangle$. The roots appearing in U_G are $e_i + e_j$ for $1 \leq i < j \leq m$.

If $G = \mathrm{SO}_{2m+1}(\mathbb{F}_q)$, then the weights of V are $\pm e_1, \ldots, \pm e_m, 0$ and $W = \langle e_1, \ldots, e_m \rangle$. The roots appearing in U_G are $e_i + e_j$ for $1 \leq i < j \leq m$.

The maximal elementary abelian p-subgroups of $H(\mathbb{F}_q)$ for each group H appearing above are computed in [4]. In particular, for G equal to one of $\mathrm{SL}_m(F_q)$, $\mathrm{Sp}_{2m}(\mathbb{F}_q)$, $\mathrm{SO}_{2m}(\mathbb{F}_q)$, one sees that U_G is already a maximal elementary abelian p-subgroup, so that $U_G = H \cap U$ and $r \cdot r'_p(G) = r_p(G)$. For $G = \mathrm{SO}_{2m+1}(\mathbb{F}_q)$ the claims about $r_p(G)$ also follows from *loc. cit*, and it remains only to prove that $U_G = H \cap U$ in this case.

To see this, consider $v = \sum_r a_r r \in \mathrm{Lie}\,(H \cap U)$ where r is a positive root of H and a_r is a scalar. Now V is a cyclic highest weight module for Lie H. Using this and that v annihilates $e_j \in W$, one gets $a_r = 0$ if $r = e_i - e_j$. Similarly, since v annihilates $-e_j \in V/W$, $a_r = 0$ for $r = e_j$. Thus $v \in U_G$. □

Remark 3.6 Note that when q is even, one has $\mathrm{SO}_{2m+1}(\mathbb{F}_q) \simeq \mathrm{Sp}_{2m}(\mathbb{F}_q)$, so that $s_p(G) = r_p(G)$ in this case.

4 Classical problems and congruence covers

Beginning with the work of Hermite on the quintic [31], the use of modular functions to solve algebraic equations is a major theme of 19th century work, including Klein's icosahedral solution of the quintic [43], the Klein–Burkhardt formula for the 27 lines on a cubic surface [11–13, 45], the Klein–Gordan solution of equations with Galois group the simple group PSL(2, 7) [28, 42], and the Klein–Fricke solution of the sextic [25, 47]. Underlying this work is the fact that problems of algebraic functions are often *equivalent* to problems of modular functions and congruence covers.

Our goal in this section is to record the classical equivalences, and add to them using recent advances in uniformization. We begin by axiomatizing the notion of accessory irrationality, and recalling the general context in which to take up Klein's call to "fathom the nature and significance of the necessary accessory irrationalities" [43,p. 174]. We then recall the general setup of congruence covers of locally symmetric varieties in order to state the precise equivalences.

While many of the results of this section are implicit in the classical literature, as far as we can tell, with the exception of Klein's *Normalformsatz* [43], that various classical problems are in fact *equivalent* has gone unremarked in the literature until quite recently [23].

4.1 Accessory irrationalities and $\mathcal{E}$-versality

For the rest of the paper we fix an algebraically closed field K of characteristic 0.

4.1.1. By a *branched cover* $Y \to X$, we mean a dominant, finite map of normal K-schemes of finite type. Branched covers form a category: a map $(Y' \to X') \to (Y \to X)$ is a commutative diagram

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

If $f : X' \to X$ is a map of normal K-schemes of finite type, denote by f^*Y the normalization of $Y \times_X X'$. If X is irreducible with geometric generic point $\Omega \to X$ (i.e. an algebaic closure of $K(X)$), then $Y \to X$ corresponds to a finite set S_Y with an action of $\pi_1(U, \Omega)$ for some dense open $U \subset X$, where $\pi_1(U, \Omega)$ denotes the étale fundamental group of U at Ω. We denote by $\mathrm{Mon}(Y/X)$ the image of $\pi_1(U, \Omega)$ in $\mathrm{Aut}(S_Y)$.

4.1.2. We now introduce the notion of a class of *accessory irrationalities* (cf. Klein [43, 46], see also Chebotarev [14]). These are branched covers introduced to manipulate some fixed branch cover of interest $Y \to X$ (hence the term "accessory"). To indicate this visually, we will use the notation $Y \to X$ to denote a general branched cover of interest, and we will use the notation $E \to X$ to denote an accessory irrationality.

Definition 4.1 (*Accessory irrationalities*). A *class of accessory irrationalities* is a full subcategory $\mathcal{E}$ of the category of branched covers. If $\mathcal{E}(X) \subset \mathcal{E}$ denotes the subcategory consisting of branched covers $\tilde{X} \to X$, then we require that $\mathcal{E}(X)$ is stable under isomorphisms, and satisfies the following conditions.

(1) For any X, the identity $X \to X$ is in $\mathcal{E}(X)$.
(2) For any map $f : X' \to X$ of normal K-schemes of finite type, f^* induces a functor $f^* : \mathcal{E}(X) \to \mathcal{E}(X')$.
(3) $\mathcal{E}(X \coprod X') = \mathcal{E}(X) \times \mathcal{E}(X')$.
(4) $\mathcal{E}(X)$ is closed under products: If $E, E' \in \mathcal{E}(X)$, then $E \times_X E' \in \mathcal{E}(X)$.
(5) If $U \subset X$ is dense open, then the map $\mathcal{E}(X) \to \mathcal{E}(U)$ induced by restriction is an equivalence of categories.
(6) If $E \to X' \to X$ are branched covers and if $E \to X$ is in $\mathcal{E}(X)$ then $E \to X'$ is in $\mathcal{E}(X')$.

Axiom (2) implies that $\mathcal{E}$ is a category fibered over the category of normal K-schemes. Note that Axiom (3) implies that it is enough to specify $\mathcal{E}(X)$ for X connected.

Definition 4.2 Fix a class $\mathcal{E}$ of accessory irrationalities. The *essential dimension* of a cover $\tilde{X} \to X$, with respect to $\mathcal{E}$ is:

$$\mathrm{ed}(\tilde{X}/X; \mathcal{E}) := \min_{(E \to X) \in \mathcal{E}} \mathrm{ed}(E \times_X \tilde{X}/E).$$

Example 4.3 Some of the core classical examples of $\mathcal{E}$ are as follows (for simplicity we specify $\mathcal{E}(X)$ only for X connected):

(1) For $\mathcal{E}(X) = \{\mathrm{id} : X \to X\}$, the quantity $\mathrm{ed}(\tilde{X}/X; \mathcal{E})$ is just the essential dimension $\mathrm{ed}(\tilde{X}/X)$.
(2) Let p be a prime and let $\mathcal{E}(X)$ be the subcategory of branched covers of X whose degree is coprime to p. Then $\mathrm{ed}(\tilde{X}/X; \mathcal{E})$ is the *essential dimension at* p. We emphasize that, although it leads to the same notion of essential dimension at p, we do not insist that E is connected, as this version of the definition does not satisfy Axiom (3) of Definition 4.1.
(3) Let $\mathcal{E}(X)$ be the set of covers $E \to X$ with $\mathrm{Mon}(E/X)$ abelian. Then $\mathrm{ed}(\tilde{X}/X; \mathcal{E})$ is the *abelian resolvent degree*. Likewise, we can consider the class of accessory

irrationalities with nilpotent (resp. solvable) monodromy, to obtain the *nilpotent* (resp. *solvable*) resolvent degree (see [14, 15, 46]).

(4) Let G be a finite simple group, and let $\mathcal{E}(X)$ consist of all $E \to X$ such that for each connected component E' of E, the branched cover $E' \to X$ is Galois and a composition series for $\mathrm{Aut}(E'/X)$ has no factor isomorphic to G. We write $\mathrm{ed}(\tilde{X}/X; G)$ for $\mathrm{ed}(\tilde{X}/X; \mathcal{E})$.

Definition 4.4 ($\mathcal{E}$-*versality*). Let $\mathcal{E}$ be a class of accessory irrationalities. A Galois branched cover $\tilde{X} \to X$ with group G is $\mathcal{E}$-*versal* if for any other Galois G-cover $\tilde{Y} \to Y$, and any Zariski open $U \subset X$, there exists

(1) an accessory irrationality $E \to Y$ in $\mathcal{E}(Y)$,
(2) a nontrivial rational map $f\colon E \to U$, and
(3) an isomorphism $f^*\tilde{X}|_U \cong \tilde{Y}|_E$.

Remark 4.5 If $\mathcal{E}$ is the trivial class of accessory irrationalities, i.e. $\mathcal{E}(X)$ only contains the identity, then $\mathcal{E}$-versal is just "versal" in the usual sense of the term (see e.g. [27,Sect. 1.5]).

If $\mathcal{E}' \subset \mathcal{E}$ are classes of accessory irrationalities, then $\mathcal{E}'$-versality for a G-cover implies $\mathcal{E}$-versality. In particular a cover which is versal is $\mathcal{E}$-versal for any class $\mathcal{E}$.

Example 4.6 (1) Hilbert's Theorem 90 implies that for a finite group G, and a faithful linear action $G \circlearrowleft \mathbb{A}^n$, the map $\mathbb{A}^n \to \mathbb{A}^n/G$ is versal (see [21]).

(2) The Merkujev–Suslin Theorem [58,Theorem 16.1] implies that for every faithful, projective-linear action $G \circlearrowleft \mathbb{P}^n$, the map $\mathbb{P}^n \to \mathbb{P}^n/G$ is solvably versal, i.e. $\mathcal{E}$-versal for the class $\mathcal{E}$ of solvable branched covers.[5]

Lemma 4.7 *Let G be a finite group, let $\mathcal{E}$ be a class of accessory irrationalities, and let $\tilde{X} \to X$ be an $\mathcal{E}$-versal G-cover.*

(1) Let $\tilde{X} \to \tilde{Z}$ be a G-equivariant dominant rational map. Then $\tilde{Z} \to \tilde{Z}/G$ is an $\mathcal{E}$-versal G-cover.
(2) Let $H \subset G$ be any subgroup. Then $\tilde{X} \to \tilde{X}/H$ is an $\mathcal{E}$-versal H-cover.

Proof The first statement follows immediately from the definition. For the second, let $\tilde{Y} \to Y$ be a Galois H-cover. Then

$$\tilde{Y} \times_H G \to Y$$

is a Galois G-cover which is H-equivariantly isomorphic to $\tilde{Y} \times G/H \to Y$. By $\mathcal{E}$-versality, for any Zariski open $U \subset X$, there exists an accessory irrationality

$$E \to Y$$

in $\mathcal{E}$, and a rational map

$$f\colon E \to U$$

[5] *Mutatis mutandis*, this follows by the same reasoning as in [21].

with an isomorphism of G-covers

$$f^*\tilde{X} \cong (\tilde{Y} \times_H G)|_E.$$

By the Galois correspondence for covers, the H-equviariant isomorphism above implies that $E \to U$ factors through a map

$$\tilde{f}\colon E \to (\tilde{X}/H)|_U$$

We conclude that $\tilde{f}^*\tilde{X} \cong \tilde{Y}|_E$ and that $\tilde{X} \to \tilde{X}/H$ is $\mathcal{E}$-versal for H as claimed. □

Remark 4.8 Example 4.6(1) and Lemma 4.7(1) immediately imply that for each $n \geq 5$, the cover $\mathcal{M}_{0,n} \to \mathcal{M}_{0,n}/S_n$ is versal for the group S_n.

4.1.3. We can also consider the *resolvent degree* of a cover $\tilde{X} \to X$, which is somewhat different from, but related to the idea of the general notion of essential dimension defined above. To explain this, write $E_\bullet \to X$ for a tower of branched covers $E = E_r \to \cdots \to E_0 = X$. The *resolvent degree* of $\tilde{X} \to X$ is defined as

$$\mathrm{RD}(\tilde{X}/X) = \min_{E_\bullet \to X} \max \left\{ \mathrm{ed}(E \times_X \tilde{X}/E), \{\mathrm{ed}(E_i/E_{i-1})\}_{i=1}^r \right\}$$

where $E_\bullet \to X$ runs over all sequences of covers.

When $\mathrm{Mon}(\tilde{X}/X)$ is simple, it follows from [23,Cor. 2.18] that the definition of $\mathrm{RD}(\tilde{X}/X)$ does not change if we consider only $E_\bullet \to X$ such that the composition $\pi_1(E, \Omega) \to \pi_1(X, \Omega) \to \mathrm{Mon}(\tilde{X}/X)$ is surjective and $\mathrm{ed}(E_i/E_{i-1}) < \dim(X)$ (n.b. here as above, $\Omega \to X$ denotes a geometric generic point). In particular

$$\min_{E_\bullet \to X} \mathrm{ed}(E \times_X \tilde{X}/E) \leq \mathrm{RD}(\tilde{X}/X) \tag{4.1}$$

where $E_\bullet \to X$ runs over sequences of covers satisfying these conditions. On the other hand, in every known example, the current best upper bound for $\mathrm{RD}(-)$ can be exhibited using such a sequence $E_\bullet \to X$ which in addition satisfies $\mathrm{ed}(E \times_X \tilde{X}/E) \geq \mathrm{ed}(E_{i+1}/E_i)$, for $i = 1, \ldots, r$.

Hilbert [33, 34] made three conjectures on the resolvent degree of the general degree n polynomial; equivalently on

$$\mathrm{RD}(n) := \mathrm{RD}(\mathcal{M}_{0,n}/(\mathcal{M}_{0,n}/S_n)) = \mathrm{RD}(\mathcal{M}_{0,n}/(\mathcal{M}_{0,n}/A_n)).$$

Conjecture 1 (**Hilbert**) The following equalities hold:

$$\begin{aligned} \textit{SexticConjecture} &: \mathrm{RD}(6) = 2. \\ \textit{13thProblem} &: \mathrm{RD}(7) = 3. \\ \textit{OcticConjecture} &: \mathrm{RD}(8) = \mathrm{RD}(9) = 4. \end{aligned}$$

The upper bounds in Conjecture 1 are known; the first two are due to Hamilton, the last to Hilbert.

Our interest in $\mathcal{E}$-versality comes from the following lemma, which is proven *mutatis mutandis* by the same argument as in the proof of [23,Proposition 3.7].

Lemma 4.9 *Let $\mathcal{E}$ be a class of accessory irrationalities and let $\tilde{X} \to X$ be an $\mathcal{E}$-versal G-cover. For any Galois branched cover $\tilde{Y} \to Y$ with monodromy G,*

$$ed(\tilde{Y}/Y; \mathcal{E}) \leq ed(\tilde{X}/X; \mathcal{E}).$$

In particular, for any other $\mathcal{E}$-versal G-cover $\tilde{X}' \to X'$,

$$ed(\tilde{X}'/X'; \mathcal{E}) = ed(\tilde{X}/X; \mathcal{E}).$$

Further, if $\mathcal{E}$ is any of the classes of Example 4.3 and if G is simple, then

$$RD(\tilde{Y}/Y) \leq RD(\tilde{X}/X) \text{ and } RD(\tilde{X}'/X') = RD(\tilde{X}/X).$$

Lemma 4.9 makes precise the classical discovery that $\mathcal{E}$-versal G-covers provide "normal forms" to which every other G-cover or can be reduced. Notably, for many groups G of classical interest, congruence covers are $\mathcal{E}$-versal for a natural choice of $\mathcal{E}$.

Remark 4.10 While the notion of versality has been studied intensively for several decades, many of the most interesting normal forms, beginning with Klein's *Normalformsatz*, rely on the notion of *solvable versality*, which is substantially more flexible. For example, a versal G-variety of minimal dimension must be unirational. On the other hand, there are no rational A_6 curves (by Klein's classification of finite Möbius groups), and the level 3 Hilbert modular surface of discriminant 5, which is solvably versal for A_6 and conjectured by Hilbert to be of minimal dimension among such varieties, has arithmetic genus equal to 5 (see the discussion in the proof of Proposition 4.14 below). A better understanding of the geometric implications of solvable versality (and related notions) could shed significant light on the underpinnings of Hilbert's conjectures.

4.2 $\mathcal{E}$-versal congruence covers

We can now record the $\mathcal{E}$-versal congruence covers that we know. Klein's *Normalformsatz* provides the paradigmatic example for what follows.

4.2.1. Write $\mathbb{A}_f$ for the group of finite adeles over $\mathbb{Q}$. Let G be a group-scheme of finite type over $\mathbb{Z}$ whose generic fiber, which we also denote by G, is a connected semisimple group. Since G is of finite type, $G(\widehat{\mathbb{Z}}) = \varprojlim_n G(\mathbb{Z}/n\mathbb{Z})$ is profinite. Recall that $G(\mathbb{A}_f)$ is naturally a locally compact topological group which depends only on the generic fiber of G, and for which the subgroup $G(\widehat{\mathbb{Z}}) \subset G(\mathbb{A}_f)$, with its natural profinite topology, is open; this construction goes back to Weil [73].

A subgroup $\Gamma \subset G(\mathbb{Q})$ is called a *congruence subgroup* if it contains $G(\mathbb{Q}) \cap K$ for some compact open $K \subset G(\mathbb{A}_f)$. This is equivalent to requiring that for some positive integer n, Γ contains

$$G(\mathbb{Z}, n) := \ker(G(\mathbb{Z}) \to G(\mathbb{Z}/n)) = \ker(G(\widehat{\mathbb{Z}}) \to G(\mathbb{Z}/n)) \cap G(\mathbb{Q}).$$

We assume that the quotient X of $G(\mathbb{R})$ by a maximal compact subgroup is a Hermitian symmetric domain. Then for any congruence subgroup Γ, a theorem of Baily–Borel asserts that $M_\Gamma := X/\Gamma$ is a complex, quasiprojective variety, cf. [17,2.1.2]. For $\Gamma' \subset \Gamma$ congruence subgroups, there is a natural covering map $M_{\Gamma'} \to M_\Gamma$.

For L a totally real number field, and G a group scheme of finite type over $\mathcal{O}_L$ whose generic fiber is a connected semisimple group, one can apply the above to $\mathrm{Res}_{L/\mathbb{Q}}G$ instead of G. More precisely, we write simply $\mathrm{Res}_{L/\mathbb{Q}}G$ for the $\mathbb{Z}$-group scheme $\mathrm{Res}_{\mathcal{O}_L/\mathbb{Z}}G$. Then we have $G(\mathcal{O}_L) \xrightarrow{\sim} \mathrm{Res}_{L/\mathbb{Q}}G(\mathbb{Z})$ and when we write $G(\mathcal{O}_L)$ we mean that we are working the Hermitian symmetric domain and congruence subgroups associated with the group $\mathrm{Res}_{L/\mathbb{Q}}G$. Similarly, we write $G(\mathcal{O}_L, n)$ for $(\mathrm{Res}_{L/\mathbb{Q}}G)(\mathbb{Z}, n)$. If $L = \mathbb{Q}(\sqrt{d})$ is real quadratic, denote by $G(\mathcal{O}_L, \sqrt{d})$ the kernel of

$$\mathrm{Res}_{L/\mathbb{Q}}G(\mathbb{Z}) = G(\mathcal{O}_L) \to G(\mathcal{O}_L/\sqrt{d}).$$

If L is quadratic imaginary and a, b are non-negative integers, one can consider the unitary group $\mathrm{U}(a, b)$ of signature a, b defined by L. This is the subgroup scheme of $\mathrm{Res}_{\mathcal{O}_L/\mathbb{Z}}\mathrm{GL}_n$, where $n = a + b$, which fixes the standard Hermitian (with respect to conjugation on K) form of signature (a, b). One also has the corresponding projective unitary group $\mathrm{PU}(a, b)$.

In fact for the rest of this section we take $L = \mathbb{Q}(\omega)$, where ω is a primitive cube root of 1, and we will only need groups of signature $n - 1, 1$. We denote by $\mathrm{PU}(n-1,1)(\mathbb{Z}, \sqrt{-3})$ the kernel of the composite

$$\mathrm{PU}(n-1,1)(\mathbb{Z}) \to \mathrm{Res}_{\mathcal{O}_L/\mathbb{Z}}\,\mathrm{PGL}_n(\mathbb{Z}) = \mathrm{PGL}_n(\mathcal{O}_L) \to \mathrm{PGL}_n(\mathbb{F}_3).$$

Theorem 4.11 *(*Klein's Normalformsatz*,* [43]*). Let $\mathcal{E}$ be any class of accessory irrationalities containing all quadratic branched covers. Let $\widetilde{SL_2(\mathbb{Z}, 5)} := \ker(SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}/5\mathbb{Z}))$. Then the level 5 cover of the modular curve*

$$M_{\widetilde{SL_2(\mathbb{Z},5)}} \to M_{SL_2(\mathbb{Z})}.$$

is an $\mathcal{E}$-versal $PSL_2(\mathbb{F}_5) = A_5$-cover. In particular, for any branched cover $\tilde{X} \to X$ with monodromy A_5,

$$ed(\tilde{X}/X; \mathcal{E}) = RD(\tilde{X}/X) = 1.$$

This is in contrast to Klein's theorem that $\mathrm{ed}(A_5) = 2$. We can add another example for A_5, which was studied in detail by Hirzebruch [35], and was likely known to Kronecker, Klein and Hilbert.

Proposition 4.12 *The level 2 cover of the Hilbert modular surface*

$$M_{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}],2)} \to M_{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])}$$

is versal for A_5.

Proof Let $C \subset \mathbb{P}^4$ be Clebsch's diagonal cubic surface, i.e. C is the vanishing of the first and third elementary symmetric polynomials in $x_0, \ldots, x_4$. By [35,Theorem 1], there is a birational equivalence

$$C \simeq M_{\mathrm{SL}_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}],2)}.$$

By the proof of [35,Theorem 2], this birational equivalence is in fact $\mathrm{SL}_2(\mathbb{F}_4) = A_5$-equivariant. Next, an 1861 theorem of Hermite [32] shows that there is a dominant A_5-equivariant dominant rational map

$$\mathbb{A}^5 \to C,$$

where the source is the permutation representation of A_5 (see [54] for a modern treatment of this map, see [6, 16, 63] for other treatments of Hermite's theorem). By Hilbert's Theorem 90, $\mathbb{A}^5$ is versal. The proposition now follows from Lemma 4.7. □

Similar to, but less well-known than, Klein's normalformsatz is the following (see [28, 42], [36,pp. 318–319] and [25,Vol. II, Part 2, Chaps. 1–2]). Denote by $\mathrm{PSL}(2, 7)$ the image of $\mathrm{SL}_2(\mathbb{F}_7) \to \mathrm{PGL}_2(\mathbb{F}_7)$; this is a simple group.

Proposition 4.13 (Normal forms for $PSL(2, 7)$).

(1) *Let* $PGL_2^+(\mathbb{Z}[\sqrt{7}]) \subset PGL_2(\mathbb{Z}[\sqrt{7}])$ *denote the subgroup of elements which lift to an element of* $GL_2(\mathbb{Z}[\sqrt{7}])$ *with totally positive determinant. The cover*

$$M_{PGL_2(\mathbb{Z}[\sqrt{7}],\sqrt{7})} \to M_{PGL_2^+(\mathbb{Z}[\sqrt{7}])}$$

of Hilbert modular surfaces is versal for the simple group $PSL(2, 7)$.

(2) *Let* $\mathcal{E}$ *be any class of accessory irrationalities containing all* S_4*-covers. Let* $\widetilde{SL_2(\mathbb{Z}, 7)}$ *denote the kernel of the surjection* $SL_2(\mathbb{Z}) \to PSL(2, 7)$. *Then the level 7 modular curve*

$$M_{\widetilde{SL_2(\mathbb{Z},7)}} \to M_{SL_2(\mathbb{Z})}$$

is an $\mathcal{E}$*-versal* $PSL(2, 7)$*-cover. In particular, for any branched cover* $\tilde{X} \to X$ *with monodromy* $PSL(2, 7)$,

$$ed(\tilde{X}/X; \mathcal{E}) = RD(\tilde{X}/X) = 1.$$

Proof We remark that $\mathbb{Z}[\sqrt{7}]^\times = \{\pm\epsilon^n\}$ where $\epsilon = 8 + 3\sqrt{7}$ is the fundamental unit. Hence $\mathrm{PGL}_2(\mathbb{Z}[\sqrt{7}], \sqrt{7}) \subset \mathrm{PGL}_2^+(\mathbb{Z}[\sqrt{7}])$, and in particular, the latter group is a congruence subgroup.

Consider the modular curve $M_{\widetilde{\mathrm{SL}_2(\mathbb{Z},7)}}$. This has genus 3, and so the action of $\mathrm{PSL}(2,7)$ on 1-forms gives a linear action of $\mathrm{PSL}(2,7)$ on $\mathbb{A}^3$, and an equivariant dominant rational map $\mathbb{A}^3 \to \mathbb{P}^2$. Lemma 4.7 then implies that $\mathbb{P}^2$ is versal for $\mathrm{PSL}(2,7)$. As noted on [36,pp. 318–319], there is a $\mathrm{PSL}(2,7)$-equivariant birational isomorphism

$$\mathbb{P}^2 \cong M_{\mathrm{PGL}_2(\mathbb{Z}[\sqrt{7}],\sqrt{7})}.$$

This proves the first statement of the proposition.

The second statement follows from [28, 42]. In modern language, it suffices to construct an accessory irrationality $E \to \mathbb{P}^2/\mathrm{PSL}(2,7)$ and a $\mathrm{PSL}(2,7)$-equivariant dominant rational map

$$\mathbb{P}^2|_E \to M_{\widetilde{\mathrm{SL}_2(\mathbb{Z},7)}}.$$

For this, the canonical embedding of the modular curve $M_{\widetilde{\mathrm{SL}_2(\mathbb{Z},7)}}$ gives a $\mathrm{PSL}(2,7)$-equivariant map

$$M_{\widetilde{\mathrm{SL}_2(\mathbb{Z},7)}} \to \mathbb{P}^2.$$

As Klein discovered, the image of this map is a quartic curve, the so-called "Klein quartic". Fixing any $\mathrm{PSL}(2,7)$-invariant pairing on $\mathbb{P}^2$, there is a rational map

$$\mathbb{P}^2 \to \mathcal{M}_{0,4}/S_4.$$

which sends a point $x \in \mathbb{P}^2$ to the intersection of the dual line L_x with the Klein quartic. Let

$$E = \mathcal{M}_{0,4}|_{\mathbb{P}^2}.$$

Then there is a $\mathrm{PSL}(2,7)$-equivariant dominant map

$$\mathbb{P}^2|_E \to M_{\widetilde{\mathrm{SL}_2(\mathbb{Z},7)}}$$

as claimed. □

We can add the following result to the above.

Proposition 4.14 (Normal forms for the sextic).

(1) The congruence cover

$$\mathcal{A}_{2,2} \to \mathcal{A}_2$$

and the Picard modular 3-fold

$$\mathcal{M}_{PU(3,1)(\mathbb{Z},\sqrt{-3})} \to M_{PU(3,1)(\mathbb{Z})}$$

are versal for A_6.[6]

(2) *For* $\mathcal{E}$ *any class of accessory irrationalities containing all quadratic covers and composites thereof, the congruence cover*

$$\mathcal{A}_{2,3}/\mathbb{F}_3^\times \to \mathcal{A}_{2,A_6}$$

and the Picard modular 3-fold

$$M_{PU(3,1)(\mathbb{Z},2)} \to M_{PU(3,1)(\mathbb{Z},A_6)}$$

are $\mathcal{E}$*-versal for* A_6.

(3) *For* $\mathcal{E}$ *any class of accessory irrationalities containing all quadratic and cubic covers and composites thereof, the Hilbert modular surface*

$$M_{\widetilde{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}],3)}} \to M_{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])}$$

is $\mathcal{E}$*-versal for* A_6*, where* $\widetilde{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}],3)}$ *denotes the kernel of the map* $SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}]) \to PGL_2(\mathbb{F}_9) = A_6$.

In particular (cf. Remark 4.8 and Lemma 4.9) Hilbert's Sextic Conjecture is equivalent to the statement that the resolvent degree of any (and thus each) of the above covers is $\dim(M_{SL_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])}) = 2$.

Let $\mathrm{PSp}(4,3)$ denote the image of $\mathrm{Sp}_4(\mathbb{F}_3) \to \mathrm{PSp}_4(\mathbb{F}_3)$; this is a simple group. To prove the proposition, we make use of the following lemma.

Lemma 4.15 *Let* $PSp(4,3)$ *act linearly on* $\mathbb{P}^3$ *and let* $G \subset PSp(4,3)$ *be any subgroup. Let* $\mathcal{E}$ *be any class of accessory irrationalities containing all composites of quadratic covers. Then* $\mathbb{P}^3$ *is an* $\mathcal{E}$*-versal* G*-variety.*

Proof There is (see e.g. [1]) an $\mathrm{Sp}_4(\mathbb{F}_3)$-equivariant dominant rational map

$$\mathbb{A}^4 \to \mathbb{P}^3.$$

Lemma 4.7 then implies that $\mathbb{P}^3$ is versal for $\mathrm{Sp}_4(\mathbb{F}_3)$ As observed in the proof of [23,Theorem 4.3], this implies that $\mathbb{P}^3$ is $\mathcal{E}$-versal for $\mathrm{PSp}(4,3)$ and thus, by Lemma 4.7 for any $G \subset \mathrm{PSp}(4,3)$ as well. □

[6] Recall that there are exceptional isomorphisms $\mathrm{Sp}_4(\mathbb{F}_2) \cong O_4^+(\mathbb{F}_3) \cong S_6$.

Proof of Proposition 4.14 For versality, as in the proof of Proposition 4.12, it suffices to prove that there are A_6-equivariant birational isomorphisms

$$\mathcal{M}_{0,6} \cong \mathcal{A}_{2,2} \cong M_{\mathrm{PU}(3,1)(\mathbb{Z},\sqrt{-3})} \tag{4.2}$$

where $\mathcal{M}_{0,6}$ is the moduli of 6 distinct points in $\mathbb{P}^1$. The first isomorphism of (4.2) is the classical period map which sends 6 points in $\mathbb{P}^1$ to the Jacobian of the hyperelliptic curve branched at those points. For the second, consider the *Segre cubic threefold* X_3 in $\mathbb{P}^5$ given by

$$X_3 := \left\{ [x_0 : \cdots : x_5] \in \mathbb{P}^5 : \sum_{i=0}^{5} x_i = 0 = \sum_{i=0}^{5} x_i^3 \right\}.$$

The permutation action of S_6 on $\mathbb{P}^5$ leaves invariant X_3, permuting its 10 nodes. Kondo [53] proved that X_3 is isomorphic to the Satake–Bailey–Borel compactification of the Picard modular 3-fold $M_{\mathrm{PU}(3,1)(\mathbb{Z},\sqrt{-3})}$. One can check that the birational map $M_{\mathrm{PU}(3,1)(\mathbb{Z},\sqrt{-3})} \to X_3$ is S_6-equivariant (cf. e.g. [65,p. 6, Lemma 2.1]).

Hunt proves in [37,Theorem 3.3.11] that the dual variety to X_3 is the so-called *Igusa quartic* $\mathcal{I}_4$, which is the moduli space of 6 points on a conic in $\mathbb{P}^2$. The two varieties X_3 and $\mathcal{I}_4$ are S_6-equivariantly birational. The Igusa quartic $\mathcal{I}_4$ is the Satake compactification of $\mathcal{A}_{2,2}$. The second birational isomorphism in (4.2) is the composition of these.

Now let $\mathcal{E}$ be any class of accessory irrationalities containing all quadratic covers and composites thereof. As explained in Hunt [37,Chap. 5.3], there is a 6 : 1 (in particular, dominant) PSp(4, 3)-equivariant rational map

$$\mathbb{P}^3 \to \mathcal{B}$$

where the action of PSp(4, 3) on $\mathbb{P}^3$ is linear and where $\mathcal{B}$ denotes the "Burkhardt quartic". There is also a PSp(4, 3)-equivariant birational isomorphism

$$\mathcal{B} \cong \mathcal{A}_{2,3}/\mathbb{F}_3^{\times}.$$

Lemma 4.15 implies that $\mathcal{A}_{2,3}/\mathbb{F}_3^{\times}$ is $\mathcal{E}$-versal for $G = A_6 \subset \mathrm{PSp}(4, 3)$.

Thus $\mathcal{A}_{2,3}/\mathbb{F}_3^{\times}$ is $\mathcal{E}$-versal for any subgroup of PSp(4, 3), in particular A_6. Finally, Hunt [37,Theorem 5.6.1] proved that $\mathcal{B}$ is PSp(4, 3)-equivariantly biregularly isomorphic to the Baily–Borel compactification of $M_{\mathrm{PU}(3,1)(\mathbb{Z},2)}$.

For the last statement, let $\mathcal{E}$ be any class of accessory irrationalities containing all composites of quadratic and cubic covers. By [70,Chap. VIII, Theorem 2.6], there exists a $\mathrm{PSL}_2(\mathbb{F}_9) = A_6$-equivariant birational isomorphism

$$M_{\widetilde{\mathrm{SL}_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}],3)}} \cong V_{1,2,4} \subset \mathbb{P}^5$$

where $V_{1,2,4}$ is the common vanishing locus of the 1st, 2nd and 4th elementary symmetric polynomials and A_6 acts on $\mathbb{P}^5$ via the permutation representation. As above,

it suffices to construct an accessory irrationality $E \to \mathbb{A}^6/A_6$ in $\mathcal{E}$ and an equivariant dominant rational map

$$\mathbb{A}^6|_E \to V_{1,2,4}.$$

This follows from the classical theory of Tschirnhaus transformations (see e.g. [74] for a contemporary treatment). Recall that a *Tschirnhaus transformation* $T_{\mathbf{b}}$, for some $\mathbf{b} := (b_0, \ldots, b_5) \in \mathbb{A}^6$, is the assignment which sends a root z of the generic sextic to

$$\sum_{i=0}^{5} b_i z^i.$$

This defines an S_6-equivariant rational map

$$T_{\mathbf{b}} \colon \mathbb{A}^6 \to \mathbb{A}^6$$

Letting $\mathbf{b}$ vary, we have an $\mathbb{A}^6_{\mathbf{b}}$ parameter space of Tschirnhaus tranformations for each sextic, which we view as a trivial bundle

$$\pi_1 \colon \mathbb{A}^6 \times \mathbb{A}^6_{\mathbf{b}} \to \mathbb{A}^6.$$

We also have an evaluation map

$$ev \colon \mathbb{A}^6 \times \mathbb{A}^6_{\mathbf{b}} \to \mathbb{A}^6$$

By direct computation (see e.g. [74,Definition 3.5 and Lemma 3.6]), $ev^{-1}(\widetilde{V_{1,2,4}})$, i.e. the preimage under the map ev of the affine cone over $V_{1,2,4}$, is the intersection of a (trivial) family of hyperplanes $\widetilde{T}_1$, a cone over a generically smooth quadric $\widetilde{T}_2$ (for smoothness, see e.g. [74,Lemma 2.6]), and a quartic cone $\widetilde{T}_4$. By the classical theory of quadrics (e.g. [74,Lemma 5.10]), there exists a finite, generically étale map

$$E_0 \to \mathbb{A}^6/A_6$$

with monodromy a 2-group such that the quadric cone $\widetilde{T}_2|_{E_0}$ contains a (trivial) family $\mathcal{L} \to E_0$ of 2-planes over E_0. The intersection

$$\mathcal{L} \times_{E_0} \widetilde{T}_4$$

is thus the affine cone over a family of 4 distinct points in $\mathbb{P}^1$. There thus exists an S_4-cover

$$E \to E_0$$

and a section $\sigma : E \to ev^{-1}(\widetilde{V_{1,2,4}})|_E$. The map

$$ev \circ \sigma : \mathbb{A}^6|_E \to V_{1,2,4}$$

gives the dominant map we seek. By construction $E \to \mathbb{A}^6/A_6$ is in the class $\mathcal{E}$, and thus $V_{1,2,4}$ is indeed $\mathcal{E}$-versal. □

Proposition 4.16 (Normal forms for the 27 lines).

(1) The congruence cover

$$\mathcal{M}_{PU(4,1)(\mathbb{Z},\sqrt{-3})} \to M_{PU(4,1)(\mathbb{Z})}$$

is versal for $O_5^+(\mathbb{F}_3) \cong W(E_6)$. [7]

(2) For $\mathcal{E}$ any class of accessory irrationalities containing all quadratic covers and composites thereof, the congruence cover

$$\mathcal{A}_{2,3}/\mathbb{F}_3^\times \to \mathcal{A}_2$$

and the Picard modular 3-fold

$$M_{PU(3,1)(\mathbb{Z},2)} \to M_{PU(3,1)(\mathbb{Z})}$$

are $\mathcal{E}$-versal for the simple group $PSp(4,3) \cong W(E_6)^+$ (the normal index 2-subgroup of $W(E_6)$).

In particular, [23,Conjecture 1.8] implies and is implied by the resolvent degree of any (and thus each) of the above covers equaling $\dim(\mathcal{A}_2) = 3$.

Proof By Allcock–Carlson–Toledo [2], there exists an $O_5^+(\mathbb{F}_3) \cong W(E_6)$-equivariant birational isomorphism

$$\mathcal{H}_{3,3}(27) \simeq M_{\mathrm{PU}(4,1)(\mathbb{Z},\sqrt{-3})}$$

from the moduli $\mathcal{H}_{3,3}(27)$ of smooth cubic surfaces with a full marking of the intersection of their 27 lines to the Picard modular 4-fold.

By [20,Lemma 6.1] $\mathcal{H}_{3,3}(27)$ is versal for $W(E_6)$. By Lemma 4.7, both varieties are therefore versal for any subgroup of $W(E_6)$.

The remaining statements follow from the proof of Proposition 4.14 above. Concretely, there we showed that $\mathcal{A}_{2,3}/\mathbb{F}_3^\times$ was $\mathcal{E}$-versal for any subgroup of PSp(4, 3), in particular for PSp(4, 3) itself. Together with the PSp(4, 3)-equivariant birational isomorphism

$$\mathcal{A}_{2,3}/\mathbb{F}_3^\times \simeq M_{\mathrm{PU}(3,1)(\mathbb{Z},2)}$$

recalled in the proof of Proposition 4.14, this implies the result. □

[7] Recall that there is an exceptional isomorphism of $O_5^+(\mathbb{F}_3)$ with the Weyl group of E_6.

Proposition 4.17 (Normal forms for the septic, the octic, and 28 bitangents). *Let $G \subset Sp_6(\mathbb{F}_2)$ be any subgroup. Then the cover*

$$\mathcal{A}_{3,2} \to \mathcal{A}_{3,G}$$

is versal for G. In particular (cf. Remark 4.8 and Lemma 4.9) :

(1) Hilbert's 13th Problem is equivalent to

$$RD(\mathcal{A}_{3,2}/\mathcal{A}_{3,A_7}) = 3.$$

(2) Hilbert's Octic Conjecture [33,p. 248] is equivalent to

$$RD(\mathcal{A}_{3,2}/\mathcal{A}_{3,A_8}) = 4.$$

(3) [23,Problem 5.5(2)], which asks for the resolvent degree of finding a bitangent on a planar quartic, is equivalent to asking for $RD(\mathcal{A}_{3,2} \to \mathcal{A}_3)$.

Proof This follows as in the proof of [23,Proposition 5.7], which in turn draws on [19] and ideas of Coble. As explained there, there exists an $\mathrm{Sp}_6(\mathbb{F}_2)$-equivariant dominant rational map

$$\mathbb{A}^7 \to \mathcal{H}_{4,2}(28) \simeq \mathcal{M}_3[2]$$

where $\mathcal{H}_{4,2}(28)$ denotes the moduli of smooth planar quartics with a marking of their 28 bitangents, and $\mathcal{M}_3[2]$ denotes the moduli of genus 3 curves with full level 2 structure. The period mapping gives an $Sp_6(\mathbb{F}_2)$-equivariantly birational isomorphism

$$\mathcal{M}_3[2] \simeq \mathcal{A}_{3,2},$$

and thus $\mathcal{A}_{3,2}$ is a versal G-variety for any $G \subset \mathrm{Sp}_6(\mathbb{F}_2)$ as claimed. □

4.2.2. By Klein [44], the action $A_7 \circlearrowleft \mathbb{P}^3$ is solvably versal. As a result, Hilbert's 13th problem is equivalent to the assertion that the cover $\mathbb{P}^3 \to \mathbb{P}^3/A_7$ is a normal form of minimal dimension.

Question 4.18 Is there a congruence cover $X_{\Gamma'} \to X_\Gamma$ with Galois group A_7 and $\dim X_\Gamma = 3$ which is also $\mathcal{E}$-versal for one of the classes of accessory irrationalities considered in Example 4.3?

Finding such a congruence cover would give the transcendental part of Klein's 3-variable solution of the degree 7, as in [43,Chap. 5.9]. Note that Prokhorov's classification [61,Theorem 1.5] of finite simple groups acting birationally on rationally connected 3-folds gives strong constraints on any possible congruence cover.

Question 4.19 Is there a congruence cover $X_{\Gamma'} \to X_\Gamma$ with Galois group A_8 and $\dim X_\Gamma = 4$ which is also $\mathcal{E}$-versal for one of the classes of accessory irrationalities considered in Example 4.3?

4.2.2.1. As Propositions 4.14 and 4.17 show, for $g = 2, 3$ the $\mathrm{Sp}_{2g}(\mathbb{F}_2)$-variety $\mathcal{A}_{g,2}$ is G-versal for any subgroup $G \subset \mathrm{Sp}_{2g}(\mathbb{F}_2)$. Hence for $n = 6, 7, 8$ the resolvent degree of the cover $\mathcal{A}_{d_n,2} \to \mathcal{A}_{d_n,A_n}$ is equal to $\mathrm{RD}(n)$, as defined in the introduction. Interestingly, Hilbert's conjectured value for resolvent degree, and the value of the essential dimension at 2 for these covers, almost agree :

n	6	7	8	9
Hilbert: $\mathrm{RD}(n)$	2	3	4	4
$\mathrm{ed}(A_n; 2)$	2	2	4	4

Note that in these cases the value of $\mathrm{ed}(\mathcal{A}_{d_n,2} \to \mathcal{A}_{d_n,A_n}; 2) = \mathrm{ed}(A_n; 2)$ is already given by Proposition 3.4, except when $n = 8$ and $g = 3$, in which case Proposition 3.4 gives the lower bound 3. The actual value $\mathrm{ed}(\mathcal{A}_{3,2} \to \mathcal{A}_{3,A_8}; 2) = 4$ follows from versality (e.g. from Lemma 4.9 applied to the modular cover $\mathcal{A}_{4,2} \to \mathcal{A}_{4,A_8}$ arising from the diagonal representation of $A_8 = \mathrm{SL}_4(\mathbb{F}_2)$; the ed at 2 of this cover follows from Corollary 3.2).

Acknowledgements The authors would like to thank Robert Guralnick for pointing out a mistake in an earlier version of this paper. We also thank Igor Dolgachev, Bert van Geemen, Bruce Hunt, Aaron Landesman, Curt McMullen, Zinovy Reichstein and Ron Solomon for helpful correspondence. We thank the anonymous referee for helpful comments and suggestions.

Appendix by Nate Harman

A On quadratic representations of S_n

A.1 Statement of results

Recall that any linear representation of a p-group G over a field k of characteristic p contains a non-zero invariant vector, in particular this implies that the only irreducible representation of G over k is the trivial representation. This does not mean that all representations are trivial though, there are non-split extensions of trivial representations and understanding their structure is a central part of modular representation theory.

In a non-semisimple setting, one basic invariant of a representation is its *Lowey length*. For representations of p-groups in characteristic p it can be defined as follows: Start with a representation V and then quotient it by its space of invariants to obtain a new representation $V' = V/V^G$, then repeat this process until the quotient is zero. The Lowey length is the number of steps this takes.

In the above work Farb, Kisin, and Wolfson analyze certain special representations of symmetric groups in characteristic 2, the so-called Dickson embeddings. Typically denoted $D^{(n-1,1)}$ in the representation theory literature, these representations have the following key property: Let $n = 2m$ or $2m + 1$, these representations have Lowey length 2 when restricted to the rank m (which is the maximum possible) elementary abelian 2-subgroup H_n generated by $(1, 2), (3, 4), \ldots,$ and $(2m - 1, 2m)$.

This motivates the following definition: We say that an irreducible representation of a S_n in characteristic p is *quadratic* with respect to a maximal rank elementary

abelian p-subgroup H if it has Lowey length 2 upon restriction to H. The purpose of this note is to prove first that this is only a characteristic 2 phenomenon, and second that these representations $D^{(n-1,1)}$ are the only representations which are quadratic with respect to some maximal rank elementary abelian p-subgroup for n sufficiently large ($n \geq 9$).

In characteristic $p > 2$, the maximal rank elementary abelian p-subgroups in S_n are just those generated by a maximal collection of disjoint p-cycles. Our first main theorem tells us that there are no quadratic representations in characteristic $p > 2$, and in fact we can detect the failure to be quadratic here by restricting to a single p-cycle.

Theorem A.1 *Any irreducible representation of S_n with $n \geq p$ in characteristic $p > 2$ which is not a character has Lowey length at least 3 upon restriction to the copy of C_p generated by $(1, 2, \ldots, p)$, and therefore is not quadratic with respect to any maximal rank elementary abelian p-subgroup.*

Note that in any characteristic $p > 2$ the characters of S_n are just the trivial and sign representations.

In characteristic 2 things are a bit more complicated. While the subgroup H_n of S_n is a maximal rank elementary 2-subgroup, it is no longer the unique such subgroup up to conjugation. Recall that in S_4 there is the Klein four subgroup $K = \{e, (12)(34), (13)(24), (14)(23)\}$, which is a copy of C_2^2 not conjugate to H_4.

We can construct other maximal rank elementary 2-subgroups of S_n by taking products

$$\underbrace{K \times K \times \cdots \times K}_{m \text{ times}} \times H_{n-4m} \subset \underbrace{S_4 \times S_4 \times \cdots \times S_4}_{m \text{ times}} \times S_{n-4m} \subset S_n$$

and up to conjugacy though these are all the maximal rank elementary abelian 2-subgroups inside S_n.

S_8 has a special irreducible representation $D^{(5,3)}$ of dimension 8 which upon restriction A_8 decomposes as a direct sum $D^{(5,3)+} \oplus D^{(5,3)-}$ of two representations of dimension 4. These representations realize the "exceptional" isomorphism $A_8 \cong GL_4(\mathbb{F}_2)$, or rather they realize two different isomorphisms differing by either by conjugating A_8 by a transposition in S_8 or by the inverse-transpose automorphism of $GL_4(\mathbb{F}_2)$. Under this isomorphism the subgroup $K \times K \subset A_8$ gets identified with the subgroup of matrices of the form

$$\begin{bmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

which is manifestly quadratic. Our second main theorem will be to show that there are no other quadratic representations other than the Dickson embedding once n is at least 9.

Theorem A.2 *Suppose V is a non-trivial irreducible representation of S_n with $n \geq 9$ over a field of characteristic 2 which is quadratic with respect to a maximal rank elementary abelian 2-subgroup H. Then $V \cong D^{(n-1,1)}$, and H is conjugate to H_n.*

A.2 Proofs of main theorems

We will be assuming a familiarity with the modular representation theory of symmetric groups. A standard reference for this material the book [38] of James, which we will be adopting the notation from and referring to for all the basic results we need. The irreducible representations of S_n in characteristic p are denoted by D^{λ}, for p-regular partitions λ of n. These arise as quotients of the corresponding Specht modules S^{λ}, which are well behaved reductions of the ordinary irreducible representations in characteristic zero.

A.2.1 Proof of Theorem A.1

First we will reduce the problem to just looking at representations of S_p. For that we have the following lemma:

Lemma A.1 (1) *Every irreducible representation V of S_n with $n \geq p$ in characteristic $p > 3$ which is not a character has a composition factor when restricted to S_p which is not a character.*

(2) *Every irreducible representation V of S_n with $n \geq 4$ in characteristic 3 which is not a character has a composition factor when restricted to S_4 which is not a character.*

Proof For part (a) suppose V only has composition factors which are characters when restricted to S_p. If we restrict this to the alternating group A_p all the composition factors must be trivial, as A_p only has the trivial character. If we further restrict to A_{p-1} the whole action must be trivial because representations of A_{p-1} are semisimple in characteristic p. However if the action of A_{p-1} is trivial on V then so is the action of the entire normal subgroup generated by A_{p-1} inside S_n, which we know is all of A_n if $n > 3$. So V must be the trivial as a representation of A_n, and is therefore a character of S_n.

For part (b), let's again suppose V only has composition factors that are characters when restricted to S_4, which implies it only has trivial composition factors when restricted to A_4. If we further restrict to the Klein four subgroup K the whole action must be trivial because representations of K are semisimple in characteristic $p \neq 2$. As before we see V must be trivial for the normal subgroup of S_n generated by K, which we know is all of A_n for $n > 4$. Therefore V is a character. □

Remark: The modification for characteristic 3 is necessary because in characteristic 3 the only irreducible representations of S_3 are the trivial and sign representations. Theorem A.1 holds vacuously in this case.

It is now enough to prove Theorem A.1 for S_p in characteristic $p > 3$, and for S_4 in characteristic 3. Let's first focus on the case where $p > 3$. If λ is a p-core, then

Nakayama's conjecture (which is actually a theorem, see [38] Theorem 21.11) tells us $D^\lambda = S^\lambda$ is projective, and hence remains projective when restricted to C_p and therefore has Lowey length p. This leaves those irreducible representations corresponding to hook partitions $\lambda = (p-k, 1^k)$.

In the simplest case where $\lambda = (p-1, 1)$ then D^λ is the $(p-2)$-dimensional quotient of the standard $(p-1)$-dimensional representation $S^{(p-1,1)}$ by its one dimensional space of invariants, and one can easily verify this forms a single $(p-2)$-dimensional indecomposable representation of C_p. Peel explicitly computed the decomposition matrices for S_p in characteristic p (see [38] Theorem 24.1), and it follows from his calculation that the remaining irreducible representations D^λ with $\lambda = (p-k, 1^k)$ for $1 < k \leq p-2$ are just exterior powers $\Lambda^k D^{(p-1,1)}$ of this $(p-2)$-dimensional representation.

Since $k < p$ we know that $\Lambda^k D^{(p-1,1)}$ is a direct summand of $(D^{(p-1,1)})^{\otimes k}$, which as a representation of C_p is just the unique $(p-2)$-dimensional indecomposable representation tensored with itself k times. Tensor product decompositions for representations of cyclic groups are known explicitly ([29] Theorem 3), and in particular it is known that a tensor product of two odd dimensional indecomposable representations of C_p always decomposes as a direct sum of odd dimensional indecomposable representations. So we see $(D^{(p-1,1)})^{\otimes k}$ and $\Lambda^k D^{(p-1,1)} = D^{(p-k,1^k)}$ only have odd length indecomposable factors when restricted to C_p. If it had Lowey length 1 when restricted to C_p that means the action is trivial, which implies the action of A_p must also be trivial as A_p is simple, but that would imply the original representation of S_n was a character.

In the characteristic 3 case there are only two irreducible representations of S_4, they are the standard 3-dimensional representation $S^{(3,1)} = D^{(3,1)}$ and its sign twisted version $S^{(2,1,1)} = D^{(2,1,1)}$. These are 3-core partitions so again by Nakayama's conjecture they are both projective and therefore remain projective when restricted to C_3 and have Lowey length 3. □

A.2.2 Proof of Theorem A.2

The overall structure of the proof will be to successively rule different classes of representations and maximal rank elementary abelian 2-subgroups through a sequence of lemmas. The first such lemma will let us rule out those irreducible representations D^λ where λ is a 2-regular partition with at least 3 parts.

Lemma A.2 *If λ is a 2-regular partition with at least 3 parts, then the irreducible representation D^λ of S_n contains a projective summand when restricted to S_6.*

Proof: Note that any 2-regular partition λ with at least 3 parts can be written as $(3,2,1) + \mu = (\mu_1 + 3, \mu_2 + 2, \mu_3 + 1, \mu_4, \ldots, \mu_\ell)$ for some partition $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell)$. James and Peel [39] constructed explicit Specht filtrations for $Ind_{S_6 \times S_{n-6}}^{S_n}(S^{(3,2,1)} \otimes S^\mu)$, which have S^λ as the top filtered quotient. In particular this implies $Ind_{S_6 \times S_{n-6}}^{S_n}(S^{(3,2,1)} \otimes S^\mu)$ has D^λ as a quotient. However by Frobenius reciprocity we know that

$$\mathrm{Hom}_{S_n}(Ind_{S_6\times S_{n-6}}^{S_n}(S^{(3,2,1)}\otimes S^{\mu}), D^{\lambda}) \cong \mathrm{Hom}_{S_6\times S_{n-6}}(S^{(3,2,1)}\otimes S^{\mu}, Res_{S_6\times S_{n-6}}^{S_n}(D^{\lambda})).$$

So since the left hand side is nonzero, the right hand side is as well.

Now if we look at $S^{(3,2,1)}\otimes S^{\mu}$ as a representation of S_6 it is just a direct sum of $\dim(S^{\mu})$ copies of $S^{(3,2,1)}$, which we know is irreducible and projective by Nakayama's conjecture. In particular the image under any nonzero homomorphism is also just a direct sum of copies of $S^{(3,2,1)}$, so D^{λ} must contain at least one copy of $S^{(3,2,1)}$ as a direct summand. □

Corollary A.1 *If λ is a 2-regular partition with at least 3 parts, then D^{λ} is not quadratic with respect to any maximal rank elementary abelian 2-subgroup of S_n.*

Proof. After conjugating we may assume that our maximal rank elementary abelian subgroup intersects S_6 in an elementary abelian 2-group of rank at least 2. The previous lemma says any such irreducible representation must contain projective summand when restricted to S_6, and then this summand remains projective upon restriction to the intersection of S_6 with our maximal rank elementary 2-subgroup. Projective representations of C_2^2 have Lowey length 3, so the Lowey length for the entire maximal rank elementary abelian 2-subgroup of S_n must be at least that big. □

This reduces the problem to understanding what happens for two-part partitions $\lambda = (a, b)$. These representations are much better understood then the general case. For one thing, the branching rules for restriction are completely known in this case, although we'll just need the following simplified version:

Lemma A.3 (See [52] Theorem 3.6, following [66]). *If (a, b) is a two-part partition of n with $a - b > 1$ then $D^{(a-1,b)}$ appears as a subquotient with multiplicity one inside the restriction of $D^{(a,b)}$ to S_{n-1}, and the other composition factors are all of the form $D^{(a-1+r,b-r)}$ with $r > 0$.*

Recall that we defined $H_{2k} \subset S_{2k}$ to be the elementary abelian 2-subgroup of S_{2k} generated by the odd position adjacent transpositions $(2i - 1, 2i)$ for $1 \leq i \leq k$, we will also consider H_{2k} as a subgroup of S_n for $n > 2k$ via the standard inclusions of S_{2k} into S_n. The next lemma will be to settle for us exactly which representations are have Lowey length 2 when restricted to the standard maximal rank elementary abelian subgroup H_n.

Lemma A.4 *$D^{(n-k,k)}$ contains a projective summand when restricted to H_{2k}.*

Proof: We know from the branching rules (Lemma A.3) that $D^{(n-k,k)}$ contains a copy of $D^{(k+1,k)}$ as a subquotient when restricted to S_{2k+1}, so it is enough to verify it for $D^{(k+1,k)}$. Moreover $H_{2k} \subset S_{2k}$ so really this calculation is taking place inside $M(2k) := \mathrm{Res}_{S_{2k}}^{S_{2k+1}} D^{(k+1,k)}$.

These representations $D^{(k+1,k)}$ and $M(2k)$ are well studied. Benson proved $D^{(k+1,k)}$ is a reduction modulo 2 of the so-called basic spin representation of S_{2k+1} in characteristic zero ([5] Theorem 5.1). Nagai and Uno ([69] Theorem 2, or see [60] Proposition 3.1 for an account in English), gave explicit matrix presentations for $M(2k)$ and showed that they have the following recursive structure:

$$\mathrm{Res}_{S_{2i}\times S_{2m-2i}}^{S_{2m}} M(2m) \cong M(2i)\otimes M(2m-2i)$$

In particular since $M(2)$ can easily be seen to be the regular representation of $S_2 = H_2$, it follows by induction that $M(2k)$ is projective (and just a single copy of the regular representation) for H_{2k}. □

Corollary A.2 *The only nontrivial irreducible representation of S_n which is quadratic with respect to H_n is $D^{(n-1,1)}$.*

Proof: Corollary A.1 tells us that if λ has at least 3 parts, D^λ has Lowey length at least 3 when restricted to H_n. Then Lemma A.4 tells us that $D^{(n-k,k)}$ has Lowey length at least $k+1$ as a H_n representation and is therefore not quadratic for $k > 1$. □

To finish the proof of Theorem A.2 we need to show that for n at least 9 that there are no representations which are quadratic with respect to to any of these other maximal rank elementary abelian 2-subgroups $K^m \times H_{n-4k}$ with $m \geq 1$. Lemma A.1 rules out D^λ for λ of length at least 3, so again we will just need to address the case when λ is a length 2 partition.

We do this through a series of lemmas ruling out different cases, but first will state the following well-known fact from the modular representation theory of symmetric groups:

Lemma A.5 ([38] Theorem 9.3). *If λ is a partition of n, then S^λ restricted to S_{n-1} admits a filtration*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_N \cong S^\lambda$$

such that the successive quotients M_i/M_{i-1} are isomorphic to Specht modules S_μ, and S^μ appears if and only if μ is obtained from λ by removing a single box, in which case it appears with multiplicity one.

Lemma A.6 *$D^{(n-1,1)}$, for $n \geq 5$, contains a projective summand when restricted to K, and is therefore not quadratic with respect to any group containing K.*

Proof: It suffices to prove it for $D^{(4,1)}$ as every $D^{(n-1,1)}$ for $n > 5$ contains it as a composition factor upon restriction to S_5 by Lemma A.3. This representation $D^{(4,1)}$ is just the 4 dimensional subspace of $\mathbb{F}_2^5$ where the sum of the coordinates is zero. If we restrict this representation to S_4 this can be identified with the standard 4-dimensional permutation representation via the map $(a, b, c, d) \to (a, b, c, d, -a-b-c-d)$. The restriction of the standard action of S_4 on a 4-element set to K is simply transitive, so this representation is just a copy of the regular representation. □

Lemma A.7 *$D^{(n-2,2)}$ for $n \geq 7$ and $D^{(n-3,3)}$ for $n \geq 9$ each contain a projective summand when restricted to K, and are therefore not quadratic with respect to any group containing K.*

Proof: It suffices to prove it for $D^{(5,2)}$ and $D^{(6,3)}$ as every $D^{(n-2,2)}$ for $n > 7$ contains $D^{(5,2)}$ as a composition factor upon restriction to S_7, and similarly every $D^{(n-2,2)}$ for $n > 7$ contains $D^{(6,3)}$ as a composition factor upon restriction to S_9 by Lemma A.3.

For S_7 and S_9 the decomposition matrices are known explicitly and we have that $D^{(5,2)} = S^{(5,2)}$ and $D^{(6,3)} = S^{(6,3)}$ (see the appendix of [38]). For Specht modules the

branching rules are given by Lemma A.5 and $S^{(5,2)}$ and $S^{(6,3)}$ both contain $S^{(4,1)}$ as a subquotient upon restriction to S_5. The result then follows from the previous lemma. □

Lemma A.8 *$D^{(n-k,k)}$ for $k \geq 4$ and $n \geq 2k+1$ is not quadratic when restricted to $K^m \times H_{n-4m}$ for any $m \geq 1$.*

Proof: We know by Lemma A.4 these are projective upon restriction to H_{2k}, and are therefore projective when restricted to the intersection of H_{2k} with $K^m \times H_{n-4m}$. This intersection has rank at least 2 since $k \geq 4$, and therefore projective objects have Lowey length at least 3. This completes the proof of Theorem A.2. □

A.3 Modifications for A_n

We will now briefly describe what changes if we work with alternating groups instead of symmetric groups, but we will omit some of the details of the calculations. First a quick summary of the modular representation theory of alternating groups in terms of the theory for symmetric groups:

Upon restriction from S_n to A_n, the irreducible representations D^λ either remain irreducible, or split as a direct sums $D^\lambda \cong D^{\lambda+} \oplus D^{\lambda-}$ of two irreducible non-isomorphic representations of the same dimension; all irreducible representations of A_n are uniquely obtained this way. We'll note that in characteristic $p > 2$ this is a standard application of Clifford theory, but in characteristic 2 it is a difficult theorem of Benson ([5] Theorem 1.1). Moreover it is known exactly which D^λ split this way, but we won't go into the combinatorics here.

When $p > 2$ the maximum rank abelian p-groups in S_n all lie in A_n, and the proof of Theorem A.1 goes through without modification to give the following theorem.

Theorem A.1'. *Any non-trivial irreducible representation of A_n with $n \geq p$ in characteristic $p > 2$ has Lowey length at least 3 upon restriction to the copy of C_p generated by $(1, 2, \ldots, p)$, and is therefore not quadratic with respect to any maximal rank elementary abelian p-subgroup.*

When $p = 2$, the difference is more dramatic. It is no longer true that every maximum rank abelian 2-subgroup of S_n lies in A_n, in particular H_n is not a subgroup of A_n. Let $\tilde{H}_n$ denote the intersection of H_n and A_n, this has rank one less than H_n. The maximal rank elementary abelian 2-subgroups of A_n are as follows:

If $n = 4b$ or $4b+1$ then up to conjugacy the only maximal rank elementary abelian 2-subgroup inside A_n is K^b, and it is of rank $2b$. If $n = 4b+2$ or $4b+3$ then all maximal rank elementary abelian 2-subgroups in S_n still have maximal rank when intersected with A_n, and up to conjugacy the maximal rank elementary abelian 2-subgroups inside A_n are of the form:

$$\underbrace{K \times K \times \cdots \times K}_{m \text{ times}} \times \tilde{H}_{n-4m} \subset \underbrace{A_4 \times A_4 \times \cdots \times A_4}_{m \text{ times}} \times A_{n-4m} \subset A_n$$

and these have rank $2b-1$.

The appropriate modification to Theorem A.2 for alternating groups is the follow-ing:

Theorem A.2'. *Suppose V is a non-trivial irreducible representation of A_n with $n \geq 9$ over a field of characteristic 2 which is quadratic with respect to a maximal rank elementary abelian 2-subgroup H. Then $n \equiv 2$ or 3 modulo 4, $V \cong D^{(n-1,1)}$, and H is conjugate to $\tilde{H}_n$.*

The proof of Theorem A.2 mostly goes through in this case. Some additional care is needed to handle the representations $D^{\lambda+}$ and $D^{\lambda-}$ which are not restrictions of irreducible representations of S_n, however one simplifying observation is that since $D^{\lambda+}$ and $D^{\lambda-}$ just differ by conjugation by a transposition, they are actually isomorphic to one another upon restriction to a maximal rank elementary abelian 2-subgroup. We will omit the remaining details though.

References

1. Abbot, R., Bray, J., Linton, S., Nickerson, S., Norton, S., Parker, R., Suleiman, I., Tripp, J., Walsh, P., Wilson, R.: Atlas of finite group representations, v.3, http://brauer.maths.qmul.ac.uk/Atlas/v3/ (2019)
2. Allcock, D., Carlson, J.A., Toledo, D.: The complex hyperbolic geometry of the moduli space of cubic surfaces. J. Alg. Geom. **11**, 659–754 (2002)
3. Arnold, Vladimir: Shimura, Goro: Superpositions of algebraic functions. Proc. Sym- posia in Pure Math. **28**, 45–46 (1976)
4. Michael, J.J.: Barry, Large abelian subgroups of Chevalley groups. J. Austral. Math. Soc. Ser. A **27**(1), 59–87 (1979)
5. Benson, Dave: Spin modules for symmetric groups. J. Lond. Math. Soc. **38**(2), 250–262 (1988)
6. Brassil, Matthew: Reichstein, Zinovy: Hermite's theorem via Galois cohomology. Arch. Math. **112**, 467–473 (2019)
7. Brauer, Richard: On the resolvent problem. Ann. Mat. Pura Appl. **102**, 45–55 (1975)
8. Brosnan, P., Fakrhuddin, N.: Fixed points in toroidal compact- ifications of Shimura varieties and essential dimension of congruence covers. arXiv:2007.01752 (2020)
9. Buhler, J., Reichstein, Z.: On the essential dimension of a finite group. Compos. Math., 106 (2), 159–179, 1997
10. Buhler, J., Reichstein, Z.: On Tschirnhaus transformations. In: Topics in Number Theory (University Park, PA, 1997) 467(2) (1999), pp. 127–142
11. Burkhardt, H.: Grundzüge einer allgemeinen Systematik der hyperelliptischen Functionen I Ordnung. Math. Ann. 35 (1890) 198-296
12. H. Burkhardt, Untersuchungen aus dem Gebiete der hyperelliptischen Modulfunctionen. Zweiter Teil. Math. Ann. 38 (1891), 161-224
13. H. Burkhardt, Untersuchungen aus dem Gebiete der hyperelliptischen Modulfunctionen.III. Math. Ann. 41 (1893), 313-343
14. Chebotarev, N.G.: Die Probleme der modernen Galoisschen Theorie. In: Proceedings of the ICM (1932)
15. Chebotarev, N.G., Nikolai Grigorievich Chebotarev: The problem of resolvents and critical manifolds. Izvestia Akad. Nauk SSSR **7**, 123–146 (1943)
16. Coray, Daniel: Cubic hypersurfaces and a result of hermite. Duke Math. J. **54**, 657–670 (1987)
17. Deligne, P.: Variétés de Shimura: interprétation modulaire, et techniques de con- struction de modèles canoniques. In: Automorphic Forms, Representations and L-Functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, OR, 1977), Part 2 (1979), pp. 247–289
18. Dickson, L.E., Leonard Eugene Dickson: Representations of the general symmetric group as linear groups in finite and infinite fields. Trans. AMS **9**(2), 121–148 (1908)
19. Dolgachev, I., Ortland, D.: Point Sets in Projective Spaces and Theta Functions (1988)
20. Duncan, A.., Reichstein, Z.: Pseudo-reflection groups and essential dimension. J. Lond. Math. Soc. **90**(3), 879–902 (2014)
21. Duncan, A.: Versality of algebraic group actions and rational points on twisted varieties. J. Alg. Geom. **24**, 499–530 (2015)

22. Faltings, G., Chai, C.-L.: Degeneration of abelian varieties, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22 (Springer-Verlag, Berlin, 1990). With an appendix by David Mumford
23. Farb, Benson, Wolfson, J.: Resolvent degree, Hilbert's 13th problem and geometry. L'Enseignement Math. **65**(3), 303–376 (2019)
24. Farb, B., Kisin, M., Wolfson, J.: Essential dimension of congruence covers. Compositio Math. **157**(11), 2407–2432 (2021)
25. Fricke, Robert: Lehrbuch der Algebra, vol. 2. Viewig und Sohn, Braunschweig (1926)
26. R. Fricke and F. Klein, Vorlesungen über die Theorie der automorphen Functionen. Teubner, Berlin, 1912
27. Garibaldi, S., Merkurjev, A., Serre, J.-P.: Cohomological invariants in Galois cohomology. University Lecture Series, vol. 28 (American Mathematical Society, Providence, RI, 2003)
28. Gordan, Paul: Ueber Gleichungen siebenten Grades mit einer Gruppe von 168 Substi- tutionen. Math. Ann. **20**, 515–530 (1882)
29. Green, J.A.: The modular representation algebra of a finite group. Illinois Journal of Mathematics **6**(4), 607–619 (1962)
30. Grove, L.C.: Classical groups and geometric algebra. In: Graduate Studies in Math., vol. 39, AMS (2000)
31. Hermite, Charles: Sur la résolution de l'equation du cinquième degré. Comptes rendus de l'Académie des Sciences **46**, 508–515 (1858)
32. Hermite, C.: Sur l'invariant du 18e ordre des formes du cinquième degré et sur le rôle qu'il joue dans la résolution de l'équation du cinquième degré, extrait de deux lettres de M Hermite à l'éditeur. J. Reine Angew. Math. 59 (1861), 304–305
33. Hilbert, David: Uber die Gleichung neunten Grades. Math. Ann. **97**(1), 243–250 (1927)
34. Hilbert, D.: Problems, Mathematical: Proceedings of the 1900 ICM, English translation reprinted in Bull. AMS **37**(4), 407–436 (2000)
35. Hirzebruch, Friedrich: Hilbert's Modular Group of the Field Q(v 5) and the Cubic Di- agonal Surface of Clebsch and Klein. Russ. Math. Surv. **31**(5), 153–166 (1976)
36. Hirzebruch, F.: The Ring of Hilbert Modular Forms for Real Quadratic Fields of Small Discriminant, Modular Functions of One Variable, VI (Proc. Second Int. Conf., Univ. Bonn, Bonn, 1976) Lecture Notes in Math., vol. 627, pp. 287-323 (1977)
37. Hunt, B.: The Geometry of Some Special Arithmetic Quotients. Springer Lect. Notes in Math., vol. 1637 (1996)
38. G.D. James, The Representation Theory of Symmetric Groups, Lecture Notes in Mathematics, vol. 682. Springer, Berlin 1978
39. James, G.D., Peel, M.H.: Specht series for skew representations of symmetric groups. Journal of Algebra **56**(2), 343–364 (1979)
40. Karpenko, Nikita A., Merkurjev, Alexander S.: Essential dimension of finite p- groups. Invent. Math. **172**(3), 491–508 (2008)
41. Klein, Felix: Ueber eine geometrische Repräsentation der Resolventen algebraischer Gleichungen. Math. Ann. **4**, 346–358 (1871)
42. Klein, Felix: Ueber die Auflösung gewisser Gleichungen vom siebenten und achten Grade. Math. Ann. **15**, 252–282 (1879)
43. Klein, Felix: Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade (Lectures on the Icosahedron and the Solution of the Equation of the Fifth Degree). Tübner, Leipzig (1884)
44. Klein, F.: Zur Theorie der allgemeinen Gleichungen sechsten und siebenten Grades. Math. Ann. **28**, 499–532 (1887)
45. Klein, Felix: Sur la resolution, par les fonctions hyperelliptiques de l'equation du vingt-septieme degre, de laquelle depend la determination des vingt-sept droites d'une surface cubique. J. Math. Pure. Appl. **4**, 169–176 (1888)
46. F. Klein, Lectures on Mathematics, MacMillan and Co., New York, 1894
47. Klein, Felix: Uber die Auflösung der allgemeinen Gleichungen fünften und sechsten Grades. Journal für die reine und angewandte Mathematik **129**, 150–174 (1905)
48. Klein, F.: Gesammelte Mathematische Abhandlungen, Vol. 2, Springer, Berlin, 1922
49. Klein, F., Gesammelte Mathematische Abhandlungen, Vol. 3, Springer, Berlin, 1922

50. Klein, F.: Vorlesungen uber die Entwicklung der Mathematik im 19. Jahrhundert, Springer, Berlin (1926)
51. Klein, F., Fricke, R.: Vorlesungen über die Theorie der elliptischen Modul- funktionen, vol. 1, 2. Teubner, Leipzig (1892)
52. A.S. Kleshchev, Branching rules for symmetric groups and applications. In: R.W. Carter and J. Saxl (eds.), Algebraic Groups and their Representations. Springer, Dordrecht, 1998, pp. 103-130
53. Kondo, S.: The Segre Cubic and Borcherds Products. Arithmetic and Geometry of K3 Surfaces and Calabi-Yau Threefolds, vol. 67, pp. 549–565 (2013)
54. Kraft, Hanspeter: A result of Hermite and equations of degree 5 and 6. J. Algebra **297**, 234–253 (2006)
55. Kronecker, Leopold: Ueber die Gleichungen fünften Grades. Journal für die reine und angewandte Mathematik **59**, 306–310 (1861)
56. Landesman, A.: The Torelli map restricted to the hyperelliptic locus. arXiv:1911.02084 (2019)
57. Merkurjev, Alexander: Essential dimension. Bull. AMS **54**(4), 635–661 (2017)
58. Merkurjev, Alexander: Suslin, Andrei: K-Cohomology of Severi-Brauer Varieties and the Norm Residue Homomorphism. Math. USSR Izv. **21**(2), 307–340 (1983)
59. Meyer, Aurel: Reichstein, Zinovy: The essential dimension of the normalizer of a maximal torus in the projective linear group. Algebra & Number Theory **3**(4), 467–487 (2009)
60. T. Okuyama, On a certain simple module and cohomology of the symmetric group over GF(2). Kyoto Univ. Dep. Bull. 1581 (2008), 58-63
61. Prokhorov, Y.: Simple finite subgroups of the Cremona group of rank 3. J. Algebraic Geom. **21**(3), 563–600 (2012)
62. Reichstein, Z.: Essential Dimension, Proceedings of the International Congress of Mathematicians (2010)
63. Reichstein, Zinovy: On a Theorem of Hermite and Joubert. Canad. J. Math. **51**(1), 69–95 (1999)
64. Reichstein, Z., Youssin, B.: Essential dimensions of algebraic groups and a resolution theorem for G-varieties. Can. J. Math. **52**(5), 1018–1056 (2000). With an appendix by J. Kollár and E. Szabò
65. Shepherd-Barron, Nick: Taylor, Richard: Mod 2 and Mod 5 Icosahedral Representa- tions. J. Amer. Math. Soc. **10**(2), 283–298 (1997)
66. Sheth, Jagat: Branching rules for two row partitions and applications to the inductive systems for symmetric groups. Communications in Algebra **27**(9), 3303–3316 (1999)
67. Shimura, Goro: On purely transcendental fields of automorphic functions of several variables. Osaka Jour. Math. **1**, 1–14 (1964)
68. D.E. Taylor, Geometry of the Classical Groups Sigma Series in Pure Math. Helderberg Verlag, Berlin, 1992
69. Uno, K.: The rank variety of a simple module of a symmetric group. RIMS Kokyuroku **1251**, 8–15 (2002)
70. G. van der Geer, Hilbert modular surfaces, Springer-Verlag, Berlin 1988
71. Wagner, A.: The Faithful Linear Representation of Least Degree of S n and A n over a Field of Characteristic 2. Math. Z. 151, 127–137 (1976)
72. Wagner, A.: The Faithful Linear Representation of Least Degree of S n and A n over a Field of Odd Characteristic. Math. Z. **154**, 103–114 (1977)
73. Weil, A.: Adeles and algebraic groups. In: Progress in Mathematics, vol. 23. Birkhäuser, Boston, MA (1982). With appendices by M. Demazure and T. Ono
74. Wolfson, Jesse: Tschirnhaus transformations after Hilbert. L'Enseignement Math. **66**(3), 489–540 (2020)