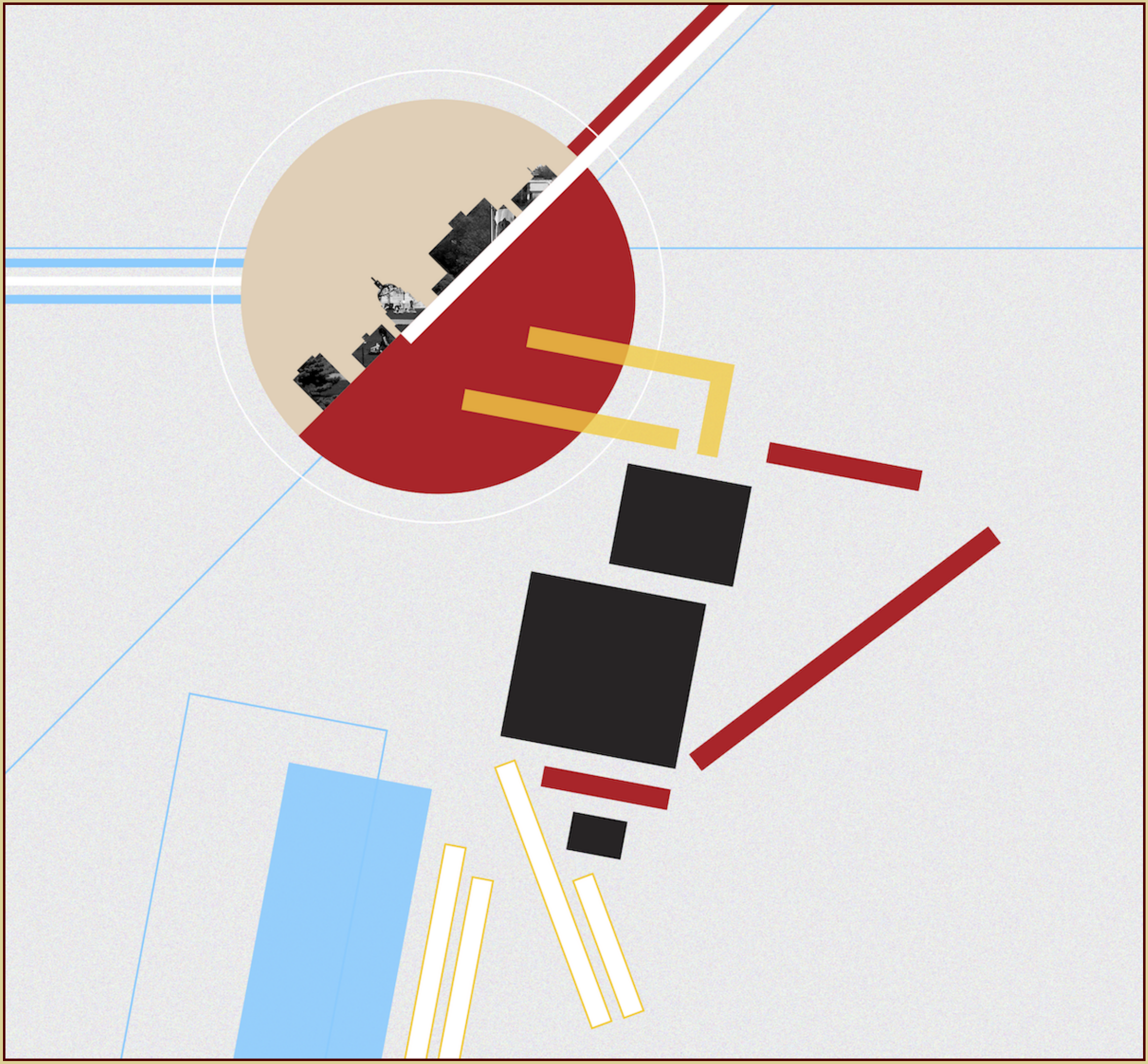
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth
Algorithmic Number Theory Symposium

Arithmetic statistics of Galois groups

David Kohel



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.353

Arithmetic statistics of Galois groups

David Kohel

We develop a computational framework for the statistical characterization of Galois characters with finite image, with application to characterizing Galois groups and establishing equivalence of characters of finite images of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1. Introduction

The absolute Galois group $\mathcal{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a fundamental object of study in number theory. The objective of this work is to develop an explicit computational framework for the study of its finite quotients. We may replace $\mathcal{G}$ with the absolute Galois group of any global field, but restrict to that of $\mathbb{Q}$ for simplicity of exposition.

As point of departure, we consider an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n as input. We set $K = \mathbb{Q}[x]/(f(x))$, denote by L its normal closure and write $\mathcal{G}(K)$ for the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ equipped with a permutation representation in $\mathcal{S}_n$ determined by the action on the roots of $f(x)$. Let $\mathcal{P}_S(\mathbb{Z})$ be the set of primes coprime to the finite set S of primes ramified in $\mathbb{Z}[x]/(f(x))$.

The statistical perspective we develop expresses the map from $\mathcal{P}_S(\mathbb{Z})$ to factorization data as an equidistributed map to a finite set $\mathcal{X}(K)$ equipped with a probability function induced from the Haar measure on $\mathcal{G}(K)$. A Frobenius lift at p, defined up to conjugacy, acts on the roots of $f(x)$. The permutation action on the roots of $f(x)$ induces a representation in $\mathrm{O}(n)$, fixing the formal sum of the roots. The orthogonal complement gives the standard representation in $\mathrm{O}(n-1)$, spanned by differences of basis elements. Let $P(x)$ be the characteristic polynomial of Frobenius in the permutation representation and

$$S(x) = P(x)/(x-1) = x^{n-1} - s_1 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1}$$

be the characteristic polynomial in the standard representation. This polynomial is independent of choices of lift of Frobenius and choice of basis. As such, the coordinates $(s_1, \ldots, s_{n-1}) \in \mathbb{Z}^{n-1}$ are invariants of the Frobenius conjugacy class Frob_p in the set $\mathcal{C}\ell(\mathcal{G}(K))$ of conjugacy classes of $\mathcal{G}(K)$. Denote the finite set of such class points by $\mathcal{X}(K)$. We note that the class points are entirely determined by the

MSC2010: 11R21, 11R32, 11R44.
Keywords: arithmetic statistics, Galois groups.

factorization data of $f(x)$ mod p, and $\mathcal{X}(K) \subset \mathbb{Z}^{n-1}$ is equipped with the structure of a finite probability space, induced from the cover $\mathcal{C}\ell(\mathcal{G}(K)) \to \mathcal{X}(K)$. The irreducible characters are known to form an orthogonal basis for the class functions on $\mathcal{C}\ell(\mathcal{G}(K))$, and the rational characters are integer-valued class functions on the class space $\mathcal{X}(K)$.

In what follows we develop this approach by describing systems of rational characters on $\mathcal{G}(K)$ algebraically as a basis of polynomials in $\mathbb{Z}[s_1, \dots, s_{n-1}]$ modulo the defining ideal for $\mathcal{X}(K)$, together with their associated inner product. As a consequence we develop algorithms for the characterization of Galois groups, and more generally, tools for determining equivalence of finite Galois representations.

2. Representations of orthogonal groups

Let G be a compact Lie group. In practice, G will be an orthogonal group

$$G = \mathrm{O}(n-1) \subset \mathrm{O}(n) \quad \text{or} \quad G = \mathrm{SO}(n-1) \subset \mathrm{O}(n-1),$$

or a finite permutation group, equipped with the standard representation in $\mathrm{O}(n-1)$,

$$G \subseteq \mathcal{S}_n \subset \mathrm{O}(n-1) \quad \text{or} \quad G \subseteq \mathcal{A}_n \subset \mathrm{SO}(n-1).$$

The standard representation of $\mathcal{S}_n$ provides the motivation for an algebraic presentation of the character ring of a permutation group. For the character theory of permutation groups, we appeal to known algorithms for its computation.

The symmetric group $\mathcal{S}_n$ acts on a set of n elements, and the linear extension to a basis of $\mathbb{Z}^n \subset \mathbb{R}^n$ gives the *permutation representation* of $\mathcal{S}_n$, extending its action on the basis $\{e_1, \dots, e_n\}$. Since $\boldsymbol{e}_1 + \cdots + \boldsymbol{e}_n$ is fixed by $\mathcal{S}_n$, a line is fixed, and we consider the action on the hyperplane spanned by the orthogonal complement. In the basis $\{\boldsymbol{e}_1 - \boldsymbol{e}_2, \dots, \boldsymbol{e}_{n-1} - \boldsymbol{e}_n\}$, we obtain the *standard representation* of $\mathcal{S}_n$ in $\mathrm{O}(n-1)$. The choice of basis is noncanonical, but the character theory is independent of any such choice. The orthogonal group $\mathrm{O}(n)$ and its subgroup $\mathrm{O}(n-1)$ have two connected components, with principal component $\mathrm{SO}(n-1) \subset \mathrm{SO}(n)$, such that $\mathcal{A}_n = \mathcal{S}_n \cap \mathrm{SO}(n-1)$.

Representation ring. For a compact Lie group G, we denote the set of conjugacy classes of G by $\mathcal{C}\ell(G)$. We define the representation ring of G,

$$\mathfrak{R}(G) = \bigoplus_{\chi} \mathbb{Z}\chi,$$

as the free abelian group on irreducible characters $\chi : G \to \mathbb{C}$ of finite degree. We identify addition with direct sum, and thereby the abelian submonoid $\bigoplus \mathbb{N}\chi \subseteq \mathfrak{R}(G)$ with characters, and define multiplication on $\mathfrak{R}(G)$ by the linear extension of tensor product on $\bigoplus \mathbb{N}\chi$. We refer to elements of $\mathfrak{R}(G)$ as virtual characters.

As class functions, $\mathfrak{R}(G)$ can be identified with a subring of complex-valued functions on $\mathcal{C}\ell(G)$. Indeed, when G is finite, the number h of conjugacy classes (and of irreducible characters) is finite, and the character table is defined as the evaluation vectors

$$(\chi_i(\mathcal{C}_1), \dots, \chi_i(\mathcal{C}_h))$$

in the ring $\mathbb{C}^h = \mathbb{C} \times \cdots \times \mathbb{C}$, for χ_i running over the irreducible characters, forming a generator set for the representation ring. For a subfield $F \subset \mathbb{C}$, we denote by $\mathfrak{R}_F(G)$ the subring of F-valued virtual characters. While $\mathfrak{R}(G) = \mathfrak{R}_{\mathbb{Q}}(G)$ for $G = \mathcal{S}_n$ or $G = \mathrm{O}(n-1)$, for a general finite group that we may consider, the field of definition of an irreducible character may be a proper extension of $\mathbb{Q}$.

Considering the group $\mathrm{O}(n)$ in $\mathrm{GL}_n(\mathbb{R})$, an element g satisfies a characteristic polynomial of the form

$$x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n.$$

The coefficient s_1 is the trace in its representation on $\mathbb{R}^n$, and s_n is its determinant character. We note that s_k is an invariant of the class of g, and we can identify $g \mapsto s_k$ as characters. Specifically, s_k is the character on the k-th exterior power $\bigwedge^k \mathbb{R}^n$. We recall the structure of the character ring for $\mathrm{O}(n)$ (see [19]).

Lemma 1. *The virtual character ring $\mathfrak{R}(O(n))$ is generated by s_k, $1 \le k \le n$, and*

$$\mathfrak{R}(\mathrm{O}(n)) \cong \frac{\mathbb{Z}[s_1, \dots, s_n]}{(s_k s_n - s_{n-k}, s_n^2 - 1)}.$$

The restriction $\mathrm{Res} : \mathfrak{R}(\mathrm{O}(n)) \to \mathfrak{R}(\mathrm{SO}(n))$ *surjects on*

$$\mathfrak{R}(\mathrm{SO}(n)) \cong \frac{\mathbb{Z}[s_1, \dots, s_n]}{(s_k - s_{n-k}, s_n - 1)},$$

with kernel ideal $(s_n - 1)$.

Remark. If $n = 2m$ or $n = 2m+1$, then $\mathfrak{R}(\mathrm{SO}(n)) = \mathbb{Z}[s_1, \dots, s_m]$, and $\mathfrak{R}(\mathrm{O}(n))$ is an extension by the quadratic character $\xi = s_n$ such that $\xi|_{\mathrm{SO}(n)} = 1$.

Algebraic parametrization. If H is a subgroup of G, there is an induced map $\mathcal{C}\ell(H) \to \mathcal{C}\ell(G)$ on conjugacy classes and concomitant restriction homomorphism $\mathrm{Res} : \mathfrak{R}(G) \to \mathfrak{R}(H)$ on representation rings. Applied to the standard representation of $\mathcal{S}_n$ in $\mathrm{O}(n-1)$, the restriction homomorphism equips the representation ring of $\mathfrak{R}(\mathcal{S}_n)$ with a surjective restriction map from $\mathfrak{R}(\mathrm{O}(n-1))$, giving an algebraic presentation of $\mathfrak{R}(\mathcal{S}_n)$ by polynomials in $\mathbb{Z}[s_1, \dots, s_{n-1}]$ modulo the defining ideal $(s_k s_{n-1} - s_{n-k-1}$, $s_{n-1}^2 - 1)$. Given a permutation group $G \subset \mathcal{S}_n$, the subsequent restriction captures a significant subring of $\mathfrak{R}_{\mathbb{Q}}(G) \subset \mathfrak{R}(G)$.

As a tool to characterize permutation groups in $\mathcal{S}_n$, for subgroups G and H, with $H \subseteq G \subseteq \mathcal{S}_n$, we develop the *branching rules* — explicit forms for the decomposition

$$\mathrm{Res}(\chi_i) = \sum_{j=1}^{n_i} a_{ij} \psi_j$$

of irreducible characters $\{\chi_1, \dots, \chi_r\}$ on G in terms of the irreducible characters $\{\psi_1, \dots, \psi_s\}$ on H. In light of the algebraic parametrization by $\mathbb{Z}[s_1, \dots, s_{n-1}]$, we deduce the kernel ideals $I_G \subseteq I_H$ for each permutation group in the lattice (poset) of subgroups. A basis of generators provides test functions for membership in a given subgroup. We develop the algorithmic details later.

Using the Brauer–Klimyk formula (see [3, Proposition 22.9]), it is possible to develop recursive formulas for the character theory of orthogonal groups, as done in [17; 18] for $\mathrm{USp}(2m)$, and using the algebraic presentation, to deduce recursive branching rules for $\mathrm{Res} : \mathfrak{R}(\mathrm{O}(n-1)) \to \mathfrak{R}(G)$. Instead, we content ourselves with the algebraic parametrization from $\mathfrak{R}(\mathrm{O}(n-1))$ and exploit the well-established computational character theory of permutation groups to develop branching rules in the lattice of permutation subgroups of $\mathcal{S}_n$.

3. Representations of permutation groups

Let G be a *permutation group* — a finite group equipped with an embedding in $\mathcal{S}_n$. The *cycle type* of $g \in G$ is the multiset of cardinalities of its orbits under the action of $\mathcal{S}_n$ on $\{1, \ldots, n\}$. A multiset can be denoted by a tuple $(d_1, \ldots, d_t)$ or a formal product $m_1^{e_1} \cdots m_s^{e_s}$, where

$$d_1 \le d_2 \le \cdots \le d_t \quad \text{or} \quad m_1 < \cdots < m_s \quad \text{such that } \sum_{i=1}^{t} d_i = \sum_{i=1}^{s} e_i m_i = n.$$

The cycle type is invariant under conjugation in $\mathcal{S}_n$; thus the cycle type is well-defined for the conjugacy class $\mathcal{C} = \mathcal{C}(g) \in \mathcal{C}\ell(G)$, where $\mathcal{C}(g) = \{xgx^{-1} : x \in G\}$.

Lemma 2. *The map $\mathcal{C}\ell(\mathcal{S}_n) \to \bigl\{(d_1, \ldots, d_t) : \sum_{i=1}^{t} d_i = n\bigr\}$ from conjugacy classes of $\mathcal{S}_n$ to cycle types is a bijection.*

Proof. Clearly, giving a cyclic ordering to any partition of $\{1, \ldots, n\}$ into orbits determines an element of $\mathcal{S}_n$; hence the map is surjective. Moreover, by definition the symmetric group is n-transitive, conjugating any cyclically ordered orbit partition to any other of the same cycle type. Consequently the map is injective. □

Remark. For a permutation group $G \subset \mathcal{S}_n$ the induced map $\mathcal{C}\ell(G) \to \mathcal{C}\ell(\mathcal{S}_n)$ in general is neither injective nor surjective. The failure of injectivity means that the cycle type fails to distinguish the conjugacy classes. We will later see this in the failure of $\mathfrak{R}(\mathcal{S}_n)$ to surject on $\mathfrak{R}(G)$. In fact, the irreducible characters are known to form a basis of the class functions on G (see [16, Theorem 6]); hence the failure to separate conjugacy classes means that the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_n)$ does not surject on $\mathfrak{R}(G)$.

On the one hand, the cycle type of a conjugacy class characterizes the class. On the other hand, the characteristic polynomial (hence its coefficients) is a class invariant of an orthogonal group element, and the permutation and standard representations thus provide other class invariants. We make this association explicit. Let $(d_1, \ldots, d_t)$ be the cycle type of an element $g \in \mathcal{S}_n$. It is easy to see that the characteristic polynomial of the permutation representation of g is

$$P(x) = (x^{d_1} - 1) \cdots (x^{d_t} - 1) = (x^{m_1} - 1)^{e_1} \cdots (x^{m_s} - 1)^{e_s}.$$

The eigenvalue on the trivial space is 1, so the characteristic polynomial in the standard representation is

$$S(x) = \frac{P(x)}{(x-1)} = x^{n-1} - s_1 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1},$$

and $(s_1, \dots, s_{n-1})$ is the tuple of class invariants associated to the conjugacy class $\mathcal{C}(g)$ under the standard representation in $\mathrm{O}(n-1)$. This gives the following lemma.

Lemma 3. *The map $\mathcal{C}\ell(\mathcal{S}_n) \to \mathbb{Z}^{n-1}$ from conjugacy classes to the $(n-1)$-tuples $(s_1, \dots, s_{n-1})$ of coefficients of the characteristic polynomial under the standard embedding is injective.*

Proof. By Lemma 2 the map from conjugacy classes to cycle types is a bijection. However, by unique factorization in $\mathbb{Q}[x]$, a polynomial of the form $(x^{d_1} - 1) \cdots (x^{d_t} - 1)$ is uniquely determined by the cycle type $(d_1, \dots, d_t)$; hence the map to its coefficients $(s_1, \dots, s_{n-1})$ is injective. □

Representation rings and character tables. Let G be a permutation group and let $\mathcal{C}\ell(G) = \{\mathcal{C}_1, \dots, \mathcal{C}_h\}$ and $\{\chi_1, \dots, \chi_h\}$ be its irreducible characters. For a conjugacy class $\mathcal{C}$, define the ideal

$$\mathfrak{m}_{\mathcal{C}} = \{f \in \mathfrak{R}(G) : f(\mathcal{C}) = 0\}$$

such that the value $f(\mathcal{C})$ of a virtual character f at $\mathcal{C}$ is a well-defined class in the residue class ring $\mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}}$. The character table of G is typically represented as a matrix whose i-th row is the evaluation vector $(\chi_i(\mathcal{C}_1), \dots, \chi_i(\mathcal{C}_h))$. With this notation, we interpret as the embedding of the character χ_i in the product ring, under the injection

$$\mathfrak{R}(G) \to \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_1} \times \cdots \times \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_h}.$$

Lemma 4. *The image of the homomorphism $\mathfrak{R}(G) \to \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_1} \times \cdots \times \mathfrak{R}(G)/\mathfrak{m}_{\mathcal{C}_h}$ has finite index in its codomain.*

Proof. Clearly $\mathfrak{R}(G)$ is torsion-free, since the image of a virtual character is a subring of $\mathbb{C}$. Thus $\mathfrak{R}(G)$ embeds in $\mathfrak{R}(G) \otimes \mathbb{Q}$, which is an étale algebra, isomorphic to the product of its quotients X_i (see [2] for details). It follows that the index is finite. □

More generally in the direction of the lemma, [2] finds that the center of the group ring $\mathbb{Q}[G]$ over $\mathbb{Q}$ and the tensor product of the representation ring $\mathfrak{R}(G) \otimes \mathbb{Q}$ are related by Brauer equivalence. We give two examples below. In view of the restriction map from $\mathfrak{R}(\mathcal{S}_n)$ to $\mathfrak{R}(G)$, and since all characters on $\mathcal{S}_n$ are rational, the image of $\mathfrak{R}(\mathcal{S}_n) = \mathfrak{R}_{\mathbb{Q}}(\mathcal{S}_n)$ lies in the subring $\mathfrak{R}_{\mathbb{Q}}(G) \subset \mathfrak{R}(G)$. In the examples below, we illustrate the role of nontrivial Galois action and of quadratic characters in the failure of surjectivity of $\mathfrak{R}(\mathcal{S}_n)$ on $\mathfrak{R}(G)$ and on $\mathfrak{R}_{\mathbb{Q}}(G)$. In the next section we exploit the embedding by interpolating the character table values by the polynomial presentation $\mathbb{Z}[s_1, \dots, s_{n-1}] \to \mathfrak{R}_{\mathbb{Q}}(G)$.

Orthogonality relations. The role of arithmetic statistics of G comes from the orthogonality relations for the irreducible characters. Let $\{\chi_1, \dots, \chi_h\}$ be the irreducible characters for G, and $A(G)$ be the character matrix

$$A(G) = \begin{bmatrix} \chi_1(\mathcal{C}_1) & \cdots & \chi_1(\mathcal{C}_h) \\ \vdots & & \vdots \\ \chi_h(\mathcal{C}_1) & \cdots & \chi_h(\mathcal{C}_h) \end{bmatrix}.$$

The orthogonality relations for characters (see [16, Section 2.3]), expressed in terms of group elements, reformulated in terms of conjugacy classes, takes the form

$$\delta_{ij} = \langle \chi_i, \chi_j \rangle_G := \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \sum_{k=1}^{h} \frac{|\mathcal{C}_k|}{|G|} \chi_i(\mathcal{C}_k)\overline{\chi_j(\mathcal{C}_k)}.$$

Set $D(G)$ to be the diagonal matrix with diagonal entries $(p_1, \dots, p_h)$, where $p_k = |\mathcal{C}_k|/|G|$ is the weight of the conjugacy class $\mathcal{C}_k$. The orthogonality relations are then expressed by the equality

$$I_h = A(G)D(G)A(G)^\dagger,$$

where † denotes the conjugate transpose. The matrix $D(G)$ can be viewed as the inner product matrix of the Haar measure induced by G on $\mathcal{C}\ell(G)$.

Rational character table. Let χ be a character on G, let m be the exponent of G, and let $\mathcal{C} = \mathcal{C}(g)$ be a conjugacy class. As the trace of a representation of g, the value $\chi(\mathcal{C})$ lies in $\mathbb{Z}[\zeta_m]$, since each of its eigenvalues are in $\boldsymbol{\mu}_m = \langle \zeta_m \rangle$. We thus obtain two actions of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$. Denote by $\sigma : (\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ the isomorphism such that $\zeta_m^{\sigma(k)} = \zeta_m^k$. The first of the actions is on conjugacy classes, by $\mathcal{C}(g) \mapsto \mathcal{C}(g^k)$, and the second on characters by $\chi^{\sigma(k)}(\mathcal{C}(g)) = \chi(\mathcal{C}(g))^{\sigma(k)}$. Considering the action on eigenvalues we see immediately that

$$\chi^{\sigma(k)}(\mathcal{C}(g)) = \chi(\mathcal{C}(g^k)).$$

Restriction from $\mathfrak{R}(\mathcal{S}_n)$. Only characters in the image of $\mathfrak{R}(\mathcal{S}_n)$ can be parametrized by polynomials in $\mathbb{Z}[s_1, \dots, s_{n-1}]$ from the standard representation. We note by example, that the preimage of $\mathcal{C}$ in $\mathcal{C}\ell(\mathcal{S}_n)$ under the induced map $\mathcal{C}\ell(G) \to \mathcal{C}\ell(\mathcal{S}_n)$ can split into an even number of conjugacy class separated by a quadratic character not coming from $\mathcal{S}_n$. We observe this phenomenon for $G = D_4$ and $G = Q_8$ in the examples section below.

4. Algorithms for Galois representations

In what follows we describe algorithms for testing equivalence of finite Galois characters. As the principal application, we consider input $f(x)$ of degree n, determining a number field $K = \mathbb{Q}[x]/(f(x))$, and describe how to evaluate a sample set of primes S at characters on the permutation group $\mathcal{G}(K)$. The approach is completely general, allowing one to compare the set of characters on the absolute group $\mathcal{G}$ mapping through permutation groups $\mathcal{G}(K_1)$ and $\mathcal{G}(K_2)$ determined by number fields K_1 and K_2.

Factorization types of irreducible polynomials. Consider an irreducible polynomial $f(x)$ in $\mathbb{Z}[x]$ of degree n, set $K = \mathbb{Q}[x]/(f(x))$ and let L be its normal closure with maximal order $\mathcal{O}_L$. For a rational prime p and prime $\mathfrak{P}$ over p in $\mathcal{O}_L$, the Frobenius lift $\mathrm{Frob}_{\mathfrak{P}}$ is the unique element of the decomposition subgroup $D_{\mathfrak{P}} \subset G = \mathcal{G}(K)$ such that

$$\mathrm{Frob}_{\mathfrak{P}}(a) \equiv a^p \bmod \mathfrak{P}$$

for all a in $\mathcal{O}_L$. Denote by Frob_p the conjugacy class of $\mathrm{Frob}_{\mathfrak{P}}$ in $\mathcal{C}\ell(G)$.

For p not dividing $\mathrm{disc}(f(x))$ we define the *factorization type* of $f(x)$ mod p to be the multiset of degrees of the factorization of $f(x)$ in $\mathbb{F}_p[x]$, which we may denote by $(d_1, \dots, d_t)$, where $d_1 \le \cdots \le d_t$ and $d_1 + \cdots + d_t = n$. We can now identify the data of the factorization type with the cycle type of the Galois group $G = \mathcal{G}(K)$ equipped with its embedding in $\mathcal{S}_n$.

Lemma 5. *The factorization type of* $f(x)$ mod p *is the cycle type of* $\mathrm{Frob}_p \subset \mathcal{G}(K)$.

Proof. The factorization $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ is determined from $f(x) \equiv f_1(x) \cdots f_t(x) \bmod p$, with $\mathfrak{p}_k = (p, f_k(x))$ a prime of degree $d_k = \deg(f_k)$. The Galois group acts transitively on primes of $\mathcal{O}_L$ over p, and there exist conjugates $\mathfrak{P}_1, \dots, \mathfrak{P}_t$ over $\mathfrak{p}_1, \dots, \mathfrak{p}_t$, from which we see that d_k divides $\deg(\mathfrak{P})$, and each d_k is the cardinality of an orbit of roots modulo p under the action of $\mathrm{Frob}_{\mathfrak{P}}$. □

Character inner products as expectation. The factorization type of a polynomial gives a means of taking random samples of character values $(s_1, \dots, s_{n-1})$ at a set S of primes mapping to the group G. Other data, for particular characters, may come from weight-1 modular eigenforms, character sums, or Kronecker symbols. Let S be such a sample set of primes, and ψ, χ two characters which can be evaluated on S. We write $\psi(p)$ and $\chi(p)$ for the values of the characters at a sample point. We obtain an approximation for the orthogonal product $\langle \psi, \chi \rangle$ as the expectation of $\psi\overline{\chi}$:

$$\langle \psi, \chi \rangle = \mathrm{E}(\psi\overline{\chi}) \sim \mathrm{E}_S(\psi\overline{\chi}) = \frac{1}{|S|} \sum_{p \in S} \psi(p)\overline{\chi}(p).$$

If the multiplicity of each irreducible character in the support of ψ and χ is 1, then $m = \langle \psi, \chi \rangle$ is an integer counting the number of irreducible characters in the support of both ψ and χ. When ψ and χ are irreducible, to determine equality $\psi = \chi$, one needs only sufficient precision to distinguish the one bit $\langle \psi, \chi \rangle = 0$ or $\langle \psi, \chi \rangle = 1$.

The interest in working with irreducible characters, or nearly irreducible characters as captured by the image of restriction from $\mathfrak{R}(\mathcal{S}_n)$, is that the variance of the character products $\psi\overline{\chi}$ is minimized, and the number of primes needed to recognize is convergence small, as observed by Shieh [17; 18] in the case of symplectic groups $\mathrm{USp}(2m)$ (see also [9]).

One should note that in view of classifying the Galois group, nonvanishing of an element of the kernel ideal of the restriction $\mathfrak{R}(\mathcal{S}_n) \to \mathfrak{R}(G)$ can be used to provably exclude G as a Galois group. This was already observed by Pohst [14], who proposed the use of factorization types as a lower bound for the Galois group, and that for $n \ge 8$ the factorization types, and their probabilities, fail to separate groups.

This statement, however, concerns the data of the induced Haar measure on $\mathcal{C}\ell(G)$, and not that of the character table of G. Precisely we have two data structures on $\mathcal{C}\ell(G)$ at our disposal, that of a probability space and of class functions (given by a character table)

- $\mathcal{C}\ell(G)$ with Haar measure $p : \mathcal{C}\ell(G) \to \mathbb{R}$, and
- $\mathbb{C}^h = \mathrm{Hom}(\mathcal{C}\ell(G), \mathbb{C})$ with orthonormal basis $\{\chi_1, \dots, \chi_h\}$.

Due to the failure of surjectivity of the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_n)$, the subset of characters determined from the cycle types are unlikely to separate groups for sufficiently large n. Nevertheless, the joint data of Haar measure and character table, plus the system of restriction maps coming from common embeddings in $\mathcal{S}_n$ gives more information than either the Haar measure or character table alone.

Restriction kernel ideal. To a conjugacy class $\mathcal{C}$ for $\mathcal{S}_n$ we associate an ideal $\mathfrak{m}_{\mathcal{C}}$ in $\mathbb{Z}[s_1, \dots, s_{n-1}]$ of the form

$$\mathfrak{m}_{\mathcal{C}} = (s_1 - s_1(\mathcal{C}), \dots, s_{n-1} - s_{n-1}(\mathcal{C})),$$

where $(s_1(\mathcal{C}), \dots, s_{n-1}(\mathcal{C}))$ are the values of s_i at $\mathcal{C}$. Then the kernel ideal for the restriction of $\mathfrak{R}(\mathcal{S}_n)$ to $\mathfrak{R}(G)$ is the intersection ideal

$$I(G) = \bigcap_{\mathcal{C} \in \pi(\mathcal{C}\ell(G))} \mathfrak{m}_{\mathcal{C}},$$

where $\pi : \mathcal{C}\ell(G) \to \mathcal{C}\ell(\mathcal{S}_n)$.

Example. Consider the restriction from $\mathfrak{R}(O(3))$ to $\mathfrak{R}(\mathcal{S}_4)$. Since

$$\mathfrak{R}(O(3)) = \frac{\mathbb{Z}[s_1, s_2, s_3]}{(s_1 s_3 - s_2, s_3^2 - 1)}$$

and the values of (s_1, s_2, s_3) are in

$$\{(3, 3, 1),\ (-1, -1, 1),\ (0, 0, 1),\ (-1, 1, -1),\ (1, -1, -1)\},$$

we obtain a defining ideal of $\mathcal{S}_4$ given by the additional generators

$$s_1(s_1+1)(s_1 - s_3 - 2), \quad s_1(s_1+1)(s_1-1)(s_1-3), \quad (s_1+1)(s_1-1)(s_3-1).$$

The map $\mathcal{C}\ell(D_4) \to \mathcal{C}\ell(\mathcal{S}_4)$ fails to surject on $(0, 0, 1)$; hence there are only four maximal ideals in the intersection and the kernel ideal for $\mathfrak{R}(\mathcal{S}_4) \to \mathfrak{R}(D_4)$ is generated by

$$s_1^2 - s_1 - s_2 - s_3 - 2, \quad s_2 - s_1 s_3,\ s_3^2 - 1.$$

The first polynomial is not in the kernel ideal for $\mathfrak{R}(\mathcal{S}_4)$ and its vanishing provides a test for D_4. Geometrically, it means that the tensor square of the representation with trace s_1 decomposes into a direct sum of representations with trace $s_1 + s_2 + s_3 + 2$.

Restriction homomorphism. Let $H \subset G$ be permutation groups, and set $\ell = |\mathcal{C}\ell(H)|$ and $h = |\mathcal{C}\ell(G)|$ equal to the cardinalities of their conjugacy class sets. Suppose that $\{\psi_1, \dots, \psi_\ell\}$ and $\{\chi_1, \dots, \chi_h\}$ are the irreducible characters, which are given by embeddings in $\mathbb{C}^\ell$ and $\mathbb{C}^h$, respectively. We thus have isomorphisms

$$\mathfrak{R}(H) = \bigoplus_{i=1}^{\ell} \mathbb{Z}\psi_i \to \Lambda(H) \subset \mathbb{C}^\ell \quad \text{and} \quad \mathfrak{R}(G) = \bigoplus_{j=1}^{h} \mathbb{Z}\chi_j \to \Lambda(G) \subset \mathbb{C}^h,$$

where $\Lambda(H)$ and $\Lambda(G)$ are the lattices in $\mathbb{C}^\ell$ and $\mathbb{C}^h$ spanned by the rows of the character table. The restriction homomorphism $\mathfrak{R}(G) \mapsto \mathfrak{R}(H)$ is induced by the map $\pi : \mathcal{C}\ell(H) \to \mathcal{C}\ell(G)$, by

$$\chi \mapsto (\chi(\pi(\mathcal{C}_1)), \dots, \chi(\pi(\mathcal{C}_\ell))) \in \Lambda(H) \subset \mathbb{C}^\ell.$$

The linear transformation $\Lambda(G) \to \Lambda(H)$ gives the restriction homomorphism as an integral $(h \times \ell)$-matrix with respect to the respective bases of irreducible characters. The rows of this matrix can be interpreted as *branching rules*, giving the decomposition of an irreducible character on G as a sum of irreducible characters on H.

Inside each $\Lambda(G)$ we have a sublattice (generally of lower rank) $\Lambda_{\mathbb{Q}}(G) = \Lambda(G) \cap \mathbb{Q}^h$ of rational-valued characters. We recall that for a conjugacy class $\mathcal{C}$ of group elements of order m, the value of $\chi(\mathcal{C})$ is a sum of eigenvalues in $\mathbb{Q}(\zeta_m)$. We thus obtain an action by the Galois group of a cyclotomic field on the irreducible characters. As a consequence, the lattice $\Lambda_{\mathbb{Q}}(G)$ is generated by the sums over Galois orbits of irreducible characters. Since these orbits are disjoint, this basis of rational characters remains orthogonal, but not orthonormal, since $\langle \chi, \chi \rangle$ measures the cardinality of the orbit (assuming χ is a sum of irreducible characters of multiplicity 1). On the other hand, the restriction images $\mathrm{Res}^G_H(\Lambda(G)) \subset \Lambda(H)$ and $\mathrm{Res}^G_H(\Lambda_{\mathbb{Q}}(G)) \subset \Lambda_{\mathbb{Q}}(H)$ do not possess natural reduced orthogonal bases. In order to determine a generating set which is small with respect to the orthogonality relations on characters, we need to apply a constrained lattice reduction inside the submonoid of characters:

$$\bigoplus_{j=1}^{\ell} \mathbb{N}\psi_j \subset \bigoplus_{j=1}^{\ell} \mathbb{Z}\psi_j = \mathfrak{R}(H).$$

Rather than a generic LLL algorithm, we need to carry out a structured lattice reduction in the character monoid order to be able to invoke the heuristic arguments for convergence of small characters.

Algebraic parametrization. In order to interpret factorization types of polynomials (or splitting types of primes) as conjugacy classes on which we can apply the class functions $s_1, \dots, s_{n-1}$, we need to find an explicit algebraic parametrization

$$\frac{\mathbb{Z}[s_1, \dots, s_{n-1}]}{I(\mathcal{S}_n)} \to \mathfrak{R}(\mathcal{S}_n) \to \mathrm{Res}^{\mathcal{S}_n}_G(\Lambda(\mathcal{S}_n)) \subseteq \Lambda(G).$$

The presentation $\mathbb{Z}[s_1, \dots, s_{n-1}]/I(\mathcal{S}_n) \to \mathfrak{R}(\mathcal{S}_n)$ comes from the standard representation of $\mathcal{S}_n$, and its composition into $\Lambda(\mathcal{S}_n)$ can be effectively computed. In order to lift characters in $\Lambda(\mathcal{S}_n)$ back to representative polynomials in $(s_1, \dots, s_{n-1})$, we must invert

$$\frac{\mathbb{Z}[s_1, \dots, s_{n-1}]}{I(\mathcal{S}_n)} \to \Lambda(\mathcal{S}_n).$$

As noted above, the isomorphism $\mathfrak{R}(\mathcal{S}_n) \to \Lambda(\mathcal{S}_n)$ is obtained by the Chinese remainder theorem. More precisely, over $\mathbb{Q}$, we obtain a product decomposition of the étale algebra $\mathfrak{R}(\mathcal{S}_n) \otimes \mathbb{Q}$,

$$\mathfrak{R}(\mathcal{S}_n) \otimes \mathbb{Q} \to \frac{\mathfrak{R}(\mathcal{S}_n)}{\mathfrak{m}_{C_1}} \otimes \mathbb{Q} \times \cdots \times \frac{\mathfrak{R}(\mathcal{S}_n)}{\mathfrak{m}_{C_h}} \otimes \mathbb{Q} \cong \mathbb{Q}^h,$$

under which $\mathfrak{R}(\mathcal{S}_n) \cong \Lambda(\mathcal{S}_n) \subseteq \mathbb{Z}^h$. Since the generators $s_1, \dots, s_{n-1}$ can be evaluated at conjugacy classes, we can evaluate a basis of monomials modulo $I(\mathcal{S}_n)$ and invert a matrix to determine the preimage of a basis of irreducible characters. The same applies to a basis of characters in $\operatorname{Res}^{\mathcal{S}_n}_G(\Lambda(\mathcal{S}_n))$ modulo the restriction kernel $I(G)$.

Database of restriction-induction. Databases of transitive permutation groups of degree up to 30 are available in GAP [10] and Magma [1; 7], computed by Greg Butler, John McKay, Gordon Royle and Alexander Hulpke (see [5; 4; 15; 8; 12]). The above is intended to motivate an interest in a metastructure of the restriction relations (and adjoint induction relations) between character rings $\mathfrak{R}(G)$, and for the algebraic parametrizations arising from the restriction homomorphism from orthogonal groups.

5. Explicit computations

We illustrate the approach through arithmetic statistics of character theory by applying the methods to groups of low degree. First we analyze the dihedral and quaternionic groups D_4 and Q_8 of order 8, the smallest groups sharing the same character table. Then we consider an example of a pair of permutation groups of degree 8 and order 16 whose cycle types and induced Haar measure on $\mathcal{S}_8$-conjugacy classes are equal. We show how an auxiliary (sub)field suffices to distinguish the characters using joint Frobenius cycle data. In a final example, we treat different permutation representations of $\mathcal{A}_5$ to show how this approach can be used to establish the equivalence of the absolute Galois representations determined by different fields.

***Dihedral and quaternionic groups of order* 8.** The groups D_4 and Q_8, known to share the same character table, can nevertheless be separated by the restriction data coming from a permutation representation. We first recall that the common character table takes the form

$$A(G) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 2 & -2 & 0 & 0 & 0 \end{bmatrix},$$

with weights $\left(\frac{1}{8}, \frac{1}{8}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)$ on the conjugacy classes. The semisimple group algebras $\mathbb{Q}[D_4]$ and $\mathbb{Q}[Q_8]$ have Wedderburn decompositions

$$\mathbb{Q}[D_4] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q}) \quad \text{and} \quad \mathbb{Q}[Q_8] \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H},$$

where $\mathbb{H}$ is the quaternion algebra over $\mathbb{Q}$ ramified at 2 and ∞. These decompositions correspond to the four linear characters and sole degree-2 irreducible representation.

Only the former group, D_4, embeds in $\mathcal{S}_4$, which shows that the permutation embedding contains distinguishing information not in the character table. We make explicit the above approach through character theory for the degree-4 permutation representation. Let $\{1, \chi_1, \chi_2, \chi_3, \chi_4\}$ be a basis of characters, with χ_1, χ_2, and $\chi_3 = \chi_1\chi_2$ quadratic linear characters, and χ_4 of degree 2. The standard representation of $\mathcal{S}_4$ in O(3) provides irreducible characters

$$\{1, s_1, s_2, s_3, s_1^2 - s_1 - s_2 - 1\},$$

where s_3 is the quadratic determinant character, s_1 and $s_2 = s_1 s_3$ are degree-3 representations, and the last one is of degree 2. Computing the inner product matrices for these characters on $\mathcal{S}_4$ and D_4, we obtain

$$\begin{bmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1&0&0&0&1\\ 0&2&1&0&0\\ 0&1&2&0&0\\ 0&0&0&1&1\\ 1&0&0&1&2 \end{bmatrix}.$$

For example, this was the output to the nearest integer for the expectation method on a sample size of 16 unramified primes, for the polynomials $x^4 + x + 1$ and $x^4 - 2x^2 + 2$ with respective Galois groups $\mathcal{S}_4$ and D_4.

One identifies the polynomial expression $\chi = s_1^2 - s_1 - s_2 - 1$ for the irreducible degree-2 character χ on $\mathcal{S}_4$, which decomposes into a direct sum $1 + s_3$ on D_4, from which we deduce that $s_1^2 - s_1 - s_2 - s_3 - 2$ is in the kernel ideal $I(D_4)$. Similarly, we read from the inner products $\langle s_1, s_1\rangle = \langle s_2, s_2\rangle = 2$ and $\langle s_1, s_2\rangle = 1$ on D_4 that each of s_1 and s_2 decompose into two irreducible characters, which share a common irreducible summand. The restriction homomorphism from $\mathfrak{R}(\mathcal{S}_4)$ thus captures

$$1, \quad s_1 = \chi_1 + \chi_4, \quad s_2 = \chi_2 + \chi_4, \quad s_3 = \chi_3.$$

The restriction fails to span all characters, because the conjugacy classes are not separated by characters on $\mathcal{S}_4$. Indeed the cycle types of the five conjugacy classes in $\mathcal{C}\ell(D_4)$ are 1^4, $1^2 2^1$, 2^2, 2^2, and 4^1, and hence the two classes of cycle type 2^2 map to the same class in $\mathcal{C}\ell(\mathcal{S}_4)$.

The missing character χ_1 is easily recovered. It arises from the quadratic subfield (here with defining polynomial $x^2 - 2x + 2$), which can be expressed as a Legendre symbol. In terms of the basis of characters $\{1, s_1, s_2, s_3, \chi_1\}$, we now obtain an inner product matrix,

$$\left[\begin{array}{cccc|c} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&2&1&1\\ 0&0&1&2&0\\ \hline 0&0&1&0&1 \end{array}\right],$$

which can be reduced to an orthonormal basis for $\mathfrak{R}(D_4)$.

Since both D_4 and Q_8 admit permutation representations of degree 8, we carry out a similar analysis of the permutation representations of degree 8 for D_4 and Q_8, given by

$$D_4 \cong \left\langle \begin{matrix} (1,8)(2,7)(3,4)(5,6), \\ (1,2)(3,5)(4,6)(7,8), \\ (1,6)(2,4)(3,8)(5,7) \end{matrix} \right\rangle \quad \text{and} \quad Q_8 \cong \left\langle \begin{matrix} (1,2,4,7)(3,6,8,5), \\ (1,3,4,8)(2,5,7,6) \end{matrix} \right\rangle .$$

The cycle types 1^8, 2^4, 4^2 arise with probabilities $\left(\frac{1}{8}, \frac{5}{8}, \frac{1}{4}\right)$ in D_4, whereas in Q_8, these same types have probabilities $\left(\frac{1}{8}, \frac{1}{8}, \frac{3}{4}\right)$. Both groups embed in $\mathcal{A}_8 \subset \mathrm{SO}(7)$; hence the character rings are parametrized by $\mathfrak{R}(\mathrm{SO}(7)) \cong \mathbb{Z}[s_1, s_2, s_3]$ ($s_7 = 1$ and $s_4 = s_3,\ s_5 = s_2,\ s_6 = s_1$). Since the cycle types are the same, the kernel ideals agree, but the Haar measures differentiate the groups. However, a naive tabulation of the probabilities gives a poor empirical invariant. In fact, computing these probabilities is tantamount to evaluating the expectations of the idempotents e_1, e_2, e_3 under the isomorphism

$$\mathfrak{R}(G) \otimes \mathbb{Q} = \frac{\mathbb{Q}[s_1, s_2, s_3]}{I(G) \otimes \mathbb{Q}} \to \frac{\mathfrak{R}(G) \otimes \mathbb{Q}}{\mathfrak{m}_{\mathcal{C}_1} \otimes \mathbb{Q}} \times \frac{\mathfrak{R}(G) \otimes \mathbb{Q}}{\mathfrak{m}_{\mathcal{C}_2} \otimes \mathbb{Q}} \times \frac{\mathfrak{R}(G) \otimes \mathbb{Q}}{\mathfrak{m}_{\mathcal{C}_3} \otimes \mathbb{Q}} \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}.$$

To express this computation in the character ring framework, we scale by the group order to have integer values. As a general strategy for a group $G \subset \mathcal{S}_n$ this amounts to asking whether the scaled idempotents converge to

$$(\langle |G| e_1, 1\rangle, \ldots, \langle |G| e_s, 1\rangle) = (|\mathcal{C}_1|, \ldots, |\mathcal{C}_s|),$$

where $\mathcal{C}_i$ are the $\mathcal{S}_n$-conjugacy classes for G.

Let $\{1, \chi_1, \chi_2, \chi_3, \psi\}$ be a basis of irreducible characters for D_4, and $\{1, \chi_1', \chi_2', \chi_3', \psi'\}$ be a basis of irreducible characters for Q_8. The parametrization gives a $\mathbb{Q}$-basis $\{1, s_1, s_2\}$ and an idempotent basis $\{e_1, e_2, e_3\}$ which are characteristic functions for the evaluations on conjugacy classes. A reduced basis for the image of $\mathfrak{R}(\mathcal{S}_8)$ in $\mathfrak{R}(D_4)$ is $\{1, \sigma_1, \sigma_2\}$, described as follows in these respective bases:

D_4	$\{1, s_1, s_2\}$	$\{e_1, e_2, e_3\}$	$\{1, \chi_1, \chi_2, \chi_3, \psi\}$
1	1	$e_1+e_2+e_3$	1
σ_1	$-s_1+\frac{1}{2}s_2-\frac{1}{2}$	$2e_1-e_2+e_3$	$\chi_1+\psi$
σ_2	$2s_1-\frac{1}{2}s_2+\frac{1}{2}$	$4e_1-2e_3$	$\chi_1+\chi_2+\chi_3$

Similarly, a reduced basis for the image of $\mathfrak{R}(\mathcal{S}_8)$ in $\mathfrak{R}(Q_8)$ is $\{1, \tau_1, \tau_2\}$, expressed in the respective bases as follows:

Q_8	$\{1, s_1, s_2\}$	$\{e_1, e_2, e_3\}$	$\{1, \chi_1', \chi_2', \chi_3', \psi'\}$
1	1	$e_1+e_2+e_3$	1
τ_1	$-s_1+\frac{1}{2}s_2-\frac{3}{2}$	$2e_1-2e_2$	ψ'
τ_2	$3s_1-s_2+3$	$3e_1+3e_2-e_3$	$\chi_1'+\chi_2'+\chi_3'$

Relative to the parametrizations from $\mathfrak{R}(\mathrm{SO}(7))$, the bases (σ_1, σ_2) and (τ_1, τ_2) are related by $(\sigma_1, \sigma_2) = (\tau_1 + 1, \tau_1 + \tau_2 - 1)$, and inversely $(\tau_1, \tau_2) = (\sigma_1 - 1, \sigma_1 + \sigma_2 + 2)$. We thus express $(8e_1, 8e_2, 8e_3)$ in the respective bases

	$\{1, s_1, s_2\}$	$\{1, \sigma_1, \sigma_2\}$	$\{1, \tau_1, \tau_2\}$
$8e_1$	s_1+1	$1+\sigma_1+\sigma_2$	$1+2\tau_1+\tau_2$
$8e_2$	$5s_1-2s_2+7$	$5-3\sigma_1+\sigma_2$	$1-2\tau_1+\tau_2$
$8e_3$	$-6s_1+2s_2$	$2+2\sigma_1-2\sigma_2$	$6-2\tau_2$

giving inclusions of submodules $\langle 8e_1, 8e_2, 8e_3\rangle \subset \langle 1, \sigma_2, \sigma_3\rangle = \langle 1, \tau_2, \tau_3\rangle \subset \langle e_1, e_2, e_3\rangle$.

Computing the expectations of the test functions $\{1, \sigma_1, \sigma_2\}$ for D_4 on polynomials with Galois groups $G = D_4$ or Q_8, the Gram matrix $M(G) = (\mathrm{E}(\sigma_i\sigma_j))$ $(\sigma_0 = 1)$ takes the form

$$M(G) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 3 \end{bmatrix}, \quad \text{where } G = D_4 \text{ and otherwise } \begin{bmatrix} 1 & 1 & -1 \\ 1 & 2 & 0 \\ -1 & 0 & 5 \end{bmatrix}.$$

With respect to test functions $\{1, \tau_1, \tau_2\}$ for Q_8, the Gram matrices are

$$M(G) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}, \quad \text{where } G = Q_8 \text{ and otherwise } \begin{bmatrix} 1 & -1 & 2 \\ -1 & 3 & -3 \\ 2 & -3 & 7 \end{bmatrix}.$$

It should be clear that the full Gram matrix gives a more complete picture of the orthogonality relations of characters than the triple of inner products $(\langle 8e_1, 1\rangle)$, $(\langle 8e_2, 1\rangle)$, $(\langle 8e_3, 1\rangle)$, which is just one linear combination of the rows in the above Gram matrices.

In the next section, we show that the choice of reduced basis for the target group gives a better set of test functions, converging more rapidly to the asymptotic Gram matrix. With respect to the polynomials $x^8 + 6x^4 + 1$ of Galois group D_4 and $x^8 - 12x^6 + 36x^4 - 36x^2 + 9$ of Galois group Q_8, we obtain reasonably good convergence (to within a half integer) with the first 80 primes.

***Nondistinguished representations of degree* 8.** The first example of nonisomorphic permutation representations not distinguished by their cycle types and Haar measure are the degree-8 groups of order 16 denoted by 8T10 and 8T11 (see the LMFDB [6] Galois groups database). Specifically we define the representative groups

$$G_0 = \langle (1,2,3,8)(4,5,6,7), (1,5)(3,7)\rangle, \quad G_1 = \langle (1,3,5,7)(2,4,6,8), (1,4,5,8)(2,3,6,7), (1,5)(3,7)\rangle$$

whose character tables are given by

$$A(G_0) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & i & -i & -i & i \\ 1 & -1 & -1 & 1 & -1 & 1 & -i & i & -i & i \\ 1 & -1 & -1 & 1 & -1 & 1 & i & -i & i & -i \\ 1 & -1 & -1 & 1 & 1 & -1 & -i & i & i & -i \\ 2 & -2 & 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad A(G_1) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 2 & -2 & -2i & 2i & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -2 & 2i & -2i & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

with respective probabilities $\left(\frac{1}{16}, \frac{1}{16}, \frac{1}{16}, \frac{1}{16}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}\right)$. We note that the first eight characters are linear, and the latter two are of degree 2. The linear characters admit a group structure, isomorphic to $C_2 \times C_4$ and C_2^3, respectively. We denote the characters by $\{1, \chi_1, \chi_2, \chi_3, \rho_1, \overline{\rho}_1, \rho_2, \overline{\rho}_2, \psi_1, \psi_2\}$ and $\{1, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6, \xi_7, \psi, \overline{\psi}\}$. In the groups G_0 and G_1 the character of the standard representation (of degree 7) decomposes as

$$s_1 = \chi_1 + \rho_1 + \overline{\rho}_1 + \psi_1 + \psi_2 \quad \text{and} \quad s_1 = \xi_1 + \xi_2 + \xi_2 + \psi + \overline{\psi},$$

respectively, but the individual characters in s_1 are not separated.

Given the obvious Galois action (on the codomain field $\mathbb{Q}(i)$), we see that the subrings $\mathfrak{R}_{\mathbb{Q}}(G_0)$ and $\mathfrak{R}_{\mathbb{Q}}(G_1)$ have different ranks, 8 and 9. On the other hand, the images of the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_8)$ have rank 4 in each of $\mathfrak{R}(G_0)$ and $\mathfrak{R}(G_1)$, generated for instance by $\{1, s_1, s_2, s_3\}$. Moreover, since exactly the same four cycle types occur, with the same probabilities $\left(\frac{1}{16}, \frac{5}{16}, \frac{1}{8}, \frac{1}{2}\right)$, the characters in the image of restriction from $\mathfrak{R}(\mathcal{S}_8)$ to $\mathfrak{R}(G_0)$ and $\mathfrak{R}(G_1)$ cannot be differentiated.

Let K_0 and K_1 be number fields whose normal closures have respective Galois groups G_0 and G_1. In order to distinguish these fields, it suffices to construct missing characters from the linear character groups. In fact these number fields have nontrivial automorphism groups, isomorphic to V_4 and C_4, respectively. This induces respective subfield lattices of the forms

$$\begin{tikzcd}
 & K_0 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F_0' \arrow[dr, dash] & F_0 \arrow[d, dash] & F_0'' \arrow[dl, dash] \\
 & G_0 \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & K_1 \arrow[d, dash] & \\
 & F_1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
G_1' \arrow[dr, dash] & G_1 \arrow[d, dash] & G_1'' \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

For each field we recover a significant subgroup of the linear character groups from the quartic and quadratic characters. In fact there is a unique cyclic subfield $F_0/\mathbb{Q}$ in K_0 which recovers the characters ρ_1, $\overline{\rho}_2$, and $\chi_1 = \rho_1^2$. (The other fields F_0' and F_0'' are nonnormal.) And there exists a unique biquadratic field $F_1/\mathbb{Q}$ in K_1 which yields the quadratic characters ξ_1, ξ_2, ξ_3. The pairs (K_0, F_0) and (K_1, F_1) give characters on the pairs of permutation groups of degree 8 and 4, $(G_0, G_0/H_0 \cong C_4)$ and $(G_1, G_1/H_1 \cong V_4)$, such that the joint factorization types of Frobenius characters separate the Galois structures.

Representations of $\mathcal{A}_5$. We denote the irreducible characters of the alternating groups $\mathcal{A}_5$ by $\{1, \chi_1, \chi_2, \chi_3, \chi_4\}$, where χ_1 is the character of the degree-4 standard representation, χ_2 is the character of a degree-5 representation, and χ_3 and χ_4 are the conjugate characters of degree-3 icosahedral representations over $\mathbb{Q}(\sqrt{5})$. The rational representations are thus spanned by the orthogonal characters $\{1, \chi_1, \chi_2, \chi_3 + \chi_4\}$ of degrees 1, 4, 5, and 6.

On the other hand, the permutation representation of $\mathcal{A}_5$ in $\mathcal{S}_5$ gives a parametrization by

$$\mathfrak{R}(\mathrm{SO}(4)) = \frac{\mathbb{Z}[s_1, s_2, s_3, s_4]}{(s_1 - s_3, s_4 - 1)} \cong \mathbb{Z}[s_1, s_2],$$

and while $|\mathcal{C}\ell(\mathcal{A}_5)| = 5$, there are two conjugacy classes which map to the same cycle type 5^1 in $\mathcal{C}\ell(\mathcal{S}_5)$. Thus the restriction from $\mathfrak{R}(\mathcal{S}_5)$ gives a basis of four independent characters, and we identify

$$(1, s_1, s_1^2 - s_2 - s_1 - 1, s_2) = (1, \chi_1, \chi_2, \chi_3 + \chi_4).$$

In addition to its degree-5 permutation representation, $\mathcal{A}_5$ admits a faithful permutation representation in $\mathcal{S}_6$. In the restriction of $\mathbb{Z}[s_1, s_2] \cong \mathfrak{R}(\mathrm{SO}(5))$ we recognize the same characters equipped with a different parametrization

$$(1, s_1^2 - 2s_1 - s_2 - 1, s_1, s_2 - \chi_1) = (1, \chi_1, \chi_2, \chi_3 + \chi_4).$$

Consider the number fields, each with Galois group $\mathcal{A}_5$, defined by polynomials

$$f = x^5 - 5x^4 + 48x^3 + 28x^2 + 5x - 1,$$
$$g = x^6 + 4x^5 + 10x^4 - 10x^3 + 17x^2 + 10x + 1,$$

constructed as subfields of the same normal closure. Although not isomorphic, we can construct the inner product matrix of the same characters set $\{1, \chi_1, \chi_2, \chi_3 + \chi_4\}$ on $\mathcal{A}_5$ with respect to its different embeddings in $\mathcal{S}_5$ and $\mathcal{S}_6$. Jointly evaluating the characters on factorization types of f or g with those of either f or g, yields the same diagonal inner product matrix ($= \mathrm{diag}(1, 1, 1, 2)$ to nearest integer). This gives a means of recognizing the same character of the absolute Galois group via different presentations. The arithmetic statistic approach through character theory gives a powerful tool to not only characterize Galois groups, but to recognize equivalence of finite representations of the absolute Galois group $\mathcal{G}$ which may arise in different contexts.

6. Variance, covariance and convergence

The focus on irreducible characters provides, on the one hand, a theoretic framework for understanding the arithmetic statistics of Frobenius distributions. On the computational side, irreducible characters provide test functions with optimal convergence properties. Naively, in view of the orthogonality relations for a system $\{\chi_1, \dots, \chi_r\}$ of irreducible characters as test functions, it suffices to recognize the integer $\langle \chi_i, \chi_j \rangle = \delta_{ij}$ to one bit of precision. Furthermore, for $\chi_i \neq 1$ and $\chi_j \neq 1$ the inner products $\langle \chi_i, 1 \rangle = \langle \chi_j, 1 \rangle = 0$ imply that χ_i and χ_j have mean 0; hence we can interpret

$$\mathrm{E}_S(\chi_i \overline{\chi}_j) = \frac{1}{|S|} \sum_{p \in S} \chi_i(p) \overline{\chi}_j(p)$$

as a (sample) variance ($i = j$) or covariance ($i \neq j$) of the sample S, we see that the use of irreducible characters (or of reduced characters in $\mathfrak{R}(G)$ as the next best approximation when irreducible characters are not in the restriction image from $\mathfrak{R}(\mathcal{S}_n)$) minimizes the variance of the test functions, and orthogonality minimizes the covariance.

We can illustrate the convergence properties with the lattice of subgroups between the representation of $\mathrm{PSL}_2(\mathbb{F}_7)$ on $\mathbb{P}^1(\mathbb{F}_7)$ and $\mathcal{S}_8$

$$\begin{tikzcd}
\mathrm{PGL}_2(\mathbb{F}_7) \cong G_1 \arrow[rr, hook] & & \mathcal{S}_8 \\
\mathrm{PSL}_2(\mathbb{F}_7) \cong H_1 \arrow[u, hook] \arrow[r, hook] & H_2 \arrow[r, hook] & \mathcal{A}_8 \arrow[u, hook]
\end{tikzcd}$$

with respective orders $|H_1| = 168$, $|G_1| = 336$, and $|H_2| = 1344$.

Let $h(G)$ be the number of conjugacy classes of G, equal to the number of irreducible characters and to the rank of $\mathfrak{R}(G)$; let $r(G)$ be the number of characters irreducible over $\mathbb{Q}$, equal to the rank of $\mathfrak{R}_{\mathbb{Q}}(G)$; and let $s(G)$ the rank of the image of the restriction of $\mathfrak{R}(\mathcal{S}_n)$ to $\mathfrak{R}(G)$. For each of the groups we give the respective numbers $h(G)$, $r(G)$ and $s(G)$, as well as a representative polynomial (from the LMFDB [6]) with Galois group G:

G	$h(G)$	$r(G)$	$s(G)$	$f_G(x)$
$\mathcal{S}_8$	22	22	22	x^8-x-1
$\mathcal{A}_8$	14	12	12	$x^8-2x^7+3x^5-5x^4+2x^3+2x^2-x+1$
G_1	9	8	8	$x^8-x^7+x^6+4x^5-x^4-3x^3+5x^2-2x+1$
H_2	11	10	8	$x^8-4x^7+8x^6-9x^5+7x^4-4x^3+2x^2+1$
H_1	6	5	5	$x^8-4x^7+7x^6-7x^5+7x^4-7x^3+7x^2+5x+1$

For the generic group $\mathcal{S}_n$ the characters $(1, s_1, \dots, s_{n-1})$ are irreducible on $\mathcal{S}_n$ and form a system of test functions for $\mathcal{S}_n$. On $\mathcal{A}_n$ and its subgroups the relations $s_{n-1-i} = s_i$ hold, and so the characters $(1, s_1, \dots, s_m)$, where $n = 2m+1$ or $2m+2$, form a system of test functions for $\mathcal{A}_n$.

The Gram matrices $M(G)$ with respect to the test characters $(1, s_1, \dots, s_7)$ for $G = \mathcal{S}_8$, $\mathcal{A}_8$, and G_1, respectively are

$$M(\mathcal{S}_8) = \begin{bmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{bmatrix}, \quad M(\mathcal{A}_8) = \begin{bmatrix} 1&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&1&0 \\ 0&0&1&0&0&1&0&0 \\ 0&0&0&1&1&0&0&0 \\ 0&0&0&1&1&0&0&0 \\ 0&0&1&0&0&1&0&0 \\ 0&1&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&1 \end{bmatrix}, \quad M(G_1) = \begin{bmatrix} 1&0&0&0&1&0&0&0 \\ 0&1&0&1&1&1&0&0 \\ 0&0&3&2&1&1&1&0 \\ 0&1&2&6&4&1&1&1 \\ 1&1&1&4&6&2&1&0 \\ 0&1&1&1&2&3&0&0 \\ 0&0&1&1&1&0&1&0 \\ 0&0&0&1&0&0&0&1 \end{bmatrix}.$$

For the indicated representative polynomials, characters $(\chi_1, \dots, \chi_r)$ and set of nonramified primes S, we define the error matrix $Z_S(G) = \mathrm{E}_S(\chi_i \overline{\chi}_j) - M(G)$ and for an $(r \times r)$-matrix $Z = (z_{ij})$ we define the

	$\mathcal{S}_8$			$\mathcal{A}_8$		
k	$\|Z_S(G)\|_2$	$\|Z_S(G)\|_8$	$\|Z_S(G)\|_\infty$	$\|Z_S(G)\|_2$	$\|Z_S(G)\|_8$	$\|Z_S(G)\|_\infty$
1	0.104870 $<$	0.184799 $<$	0.257812	0.080624 $<$	0.112569 $<$	0.140625
2	0.104915 $<$	0.197659 $<$	0.269531	0.099134 $<$	0.174740 $<$	0.226562
3	0.093747 $<$	0.189553 $<$	0.255208	0.074997 $<$	0.128586 $<$	0.166666
4	0.072267 $<$	0.138632 $<$	0.191406	0.057739 $<$	0.092246 $<$	0.119140
5	0.063890 $<$	0.112834 $<$	0.151562	0.058826 $<$	0.128167 $<$	0.181250
6	0.063620 $<$	0.115167 $<$	0.171875	0.053728 $<$	0.112338 $<$	0.158854
7	0.052897 $<$	0.083975 $<$	0.116071	0.049278 $<$	0.098191 $<$	0.138392
8	0.045921 $<$	0.070367 $<$	0.097656	0.036335 $<$	0.065900 $<$	0.092773

Table 1. Approximation for $G = \mathcal{S}_8$ and $G = \mathcal{A}_8$ on sample sets of first $128k$ nonramified primes.

normalized ℓ_p-norms

$$\|Z\|_p = \left(\frac{1}{r^2}\sum_{i,j} |z_{ij}|^p\right)^{1/p} \quad \text{and} \quad \|Z\|_\infty = \max_{i,j}\{|z_{ij}|\}.$$

In particular we need $\|Z_S(G)\|_\infty < 0.50$ in order for the approximation to round to $M(G)$. We say that a sequence stably converges to $M(G)$ after m terms if $\|Z_S(G)\|_\infty < 0.50$ for all initial segments S of the sequence with $|S| > m$.

Setting S equal to the first $128k$ nonramified primes, in the case of $\mathcal{S}_8$ and $\mathcal{A}_8$ the symmetric functions give good convergence in the ℓ_2, ℓ_8 and ℓ_∞-norms to $M(G)$ on small sample sets consisting of the first $128k$ nonramified primes; see Table 1.

Even with sample size 128, we obtain a close approximation to the correct Gram matrix, and the convergence remains stable. In contrast, for the group G_1 (of index 120 in $\mathcal{S}_8$) taking increments of size 1024 we find that $2^{14} = 1024 \cdot 16$ primes gives an exact approximation of $M(G_1)$ (in the ℓ_∞-norm) but that at least $1024 \cdot 22$ primes are needed for stable convergence; see Table 2.

k	$\|Z_S(G)\|_2$	$\|Z_S(G)\|_8$	$\|Z_S(G)\|_\infty$	k	$\|Z_S(G)\|_2$	$\|Z_S(G)\|_8$	$\|Z_S(G)\|_\infty$
1	0.876885 $<$	1.841975 $<$	2.686523	10	0.187304 $<$	0.375945 $<$	0.533105
2	0.229706 $<$	0.475835 $<$	0.701171	11	0.211544 $<$	0.429012 $<$	0.613725
3	0.437539 $<$	0.862551 $<$	1.233723	12	0.231261 $<$	0.465137 $<$	0.665364
4	0.542897 $<$	1.080542 $<$	1.525878	13	0.279154 $<$	0.560439 $<$	0.800030
5	0.267850 $<$	0.528893 $<$	0.756054	14	0.201504 $<$	0.399819 $<$	0.572195
6	0.365931 $<$	0.733534 $<$	1.035156	15	0.189139 $<$	0.375454 $<$	0.534960
7	0.199105 $<$	0.407255 $<$	0.580217	16	0.178182 $<$	0.348732 $<$	0.493652
8	0.229675 $<$	0.471416 $<$	0.672363	17	0.143345 $<$	0.282338 $<$	0.397633
9	0.111158 $<$	0.231270 $<$	0.333224	18	0.136637 $<$	0.266879 $<$	0.378417

Table 2. Approximation for $G = G_1$ on sample sets of $1024k$ primes.

k	$\|Z_S(G)\|_2$		$\|Z_S(G)\|_8$		$\|Z_S(G)\|_\infty$	k	$\|Z_S(G)\|_2$		$\|Z_S(G)\|_8$		$\|Z_S(G)\|_\infty$
1	0.191903	$<$	0.557482	$<$	0.937500	9	0.114006	$<$	0.234514	$<$	0.392361
2	0.107457	$<$	0.204107	$<$	0.312500	10	0.116967	$<$	0.233938	$<$	0.390625
3	0.111166	$<$	0.316320	$<$	0.531250	11	0.120169	$<$	0.241507	$<$	0.403409
4	0.085609	$<$	0.199992	$<$	0.335937	12	0.090920	$<$	0.197313	$<$	0.330729
5	0.087717	$<$	0.208395	$<$	0.350000	13	0.093108	$<$	0.180276	$<$	0.300480
6	0.094278	$<$	0.217121	$<$	0.364583	14	0.070129	$<$	0.145311	$<$	0.243303
7	0.103194	$<$	0.236602	$<$	0.397321	15	0.074861	$<$	0.160193	$<$	0.268750
8	0.110885	$<$	0.249000	$<$	0.417968	16	0.030534	$<$	0.066387	$<$	0.111328

Table 3. Approximation for $G = G_1$ on sample sets of $128k$ primes, using a basis of irreducible characters.

Extending the computation further, we find that the apparent stable convergence fails when $\|Z_S(G_1)\|_\infty > 0.50$ for $|S| = 1024 \cdot k$ for $19 \le k \le 21$ and again in the range $45 \le k \le 48$.

Passing to a basis of rational irreducible characters ($r(G_1) = s(G_1)$), the rational character table $A(G_1)$ and the inner product matrix $D(G_1)$ of the Haar measure on conjugacy classes are respectively

$$A(G_1) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 6 & -2 & 0 & 0 & 2 & 0 & -1 & 0 \\ 12 & 4 & 0 & 0 & 0 & 0 & -2 & 0 \\ 7 & -1 & 1 & 1 & -1 & 1 & 0 & -1 \\ 7 & -1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 8 & 0 & -2 & -1 & 0 & 1 & 1 & 0 \\ 8 & 0 & 2 & -1 & 0 & -1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad D(G_1) = \frac{1}{336} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 21 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 28 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 56 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 42 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 56 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 48 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 84 \end{bmatrix},$$

which determine the diagonalized matrix $M(G_1) = A(G_1)D(G_1)A(G_1)^t = \operatorname{diag}(1, 1, 1, 2, 1, 1, 1, 1)$ with respect to the rational irreducible characters. With respect to this basis, in increments of $128k$ primes, we find stable convergence after just $512 = 128 \cdot 4$ primes; see Table 3.

For the subgroup chain $H_1 \subset H_2 \subset \mathcal{A}_8$, starting with the characters $(1, s_1, s_2, s_3)$, irreducible on $\mathcal{A}_8$, we find a similar analysis. In particular, the Gram matrices with respect to this basis are

$$M(\mathcal{A}_8) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad M(H_2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}, \quad M(H_1) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 4 & 3 \\ 1 & 2 & 3 & 10 \end{bmatrix}.$$

In the former two cases, the characters are orthogonal and irreducible or nearly so (s_3 decomposes as a sum of three distinct irreducibles on H_2), and convergence is relatively good. In contrast, the Gram matrix $M(H_1)$ has determinant 14, and is far from being orthogonal or irreducible (except for 1 and s_1) on H_1. In increments of 1024, we find stable convergence only after $2^{15} = 1024 \cdot 32$ primes; see Table 4.

k	$\|Z_S(G)\|_2$		$\|Z_S(G)\|_8$		$\|Z_S(G)\|_\infty$	k	$\|Z_S(G)\|_2$		$\|Z_S(G)\|_8$		$\|Z_S(G)\|_\infty$
1	1.300776	$<$	2.685076	$<$	3.787109	17	0.162082	$<$	0.331846	$<$	0.467773
2	0.457035	$<$	0.943691	$<$	1.331054	18	0.249476	$<$	0.507743	$<$	0.715332
3	0.316304	$<$	0.671333	$<$	0.948242	19	0.260497	$<$	0.533048	$<$	0.751336
4	0.149549	$<$	0.327977	$<$	0.463623	20	0.250136	$<$	0.514311	$<$	0.725195
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
13	0.201940	$<$	0.417409	$<$	0.588792	29	0.183952	$<$	0.364100	$<$	0.511112
14	0.219831	$<$	0.449876	$<$	0.634137	30	0.193960	$<$	0.384122	$<$	0.539257
15	0.207462	$<$	0.427431	$<$	0.602799	31	0.148770	$<$	0.290129	$<$	0.406060
16	0.170705	$<$	0.352046	$<$	0.496520	32	0.132390	$<$	0.258615	$<$	0.362091

Table 4. Approximation for $G = H_1$ on sample sets of $1024k$ primes.

k	$\|Z_S(G)\|_2$		$\|Z_S(G)\|_8$		$\|Z_S(G)\|_\infty$	k	$\|Z_S(G)\|_2$		$\|Z_S(G)\|_8$		$\|Z_S(G)\|_\infty$
1	0.227868	$<$	0.301886	$<$	0.406250	9	0.064413	$<$	0.088651	$<$	0.114583
2	0.225747	$<$	0.296604	$<$	0.398437	10	0.079219	$<$	0.104501	$<$	0.132812
3	0.127307	$<$	0.165588	$<$	0.216145	11	0.091419	$<$	0.119029	$<$	0.154829
4	0.149822	$<$	0.191605	$<$	0.250000	12	0.056475	$<$	0.076844	$<$	0.097656
5	0.166819	$<$	0.214155	$<$	0.271875	13	0.047871	$<$	0.066901	$<$	0.086538
6	0.085019	$<$	0.114926	$<$	0.148437	14	0.041653	$<$	0.062817	$<$	0.083705
7	0.101179	$<$	0.132950	$<$	0.166294	15	0.029993	$<$	0.041051	$<$	0.053125
8	0.114860	$<$	0.148922	$<$	0.193359	16	0.041465	$<$	0.054989	$<$	0.069335

Table 5. Approximation for $G = H_1$ on sample sets of $128k$ primes, using a basis of irreducible characters.

Going further one finds that the ℓ_∞-norm gradually decreases and does indeed stay below 0.50 after this point. In contrast, in terms of the basis $(1, \chi_1 = \varphi + \overline{\varphi}, \chi_2, \chi_3, \chi_4)$ of irreducible characters over $\mathbb{Q}$, of degrees $(1, 6, 6, 7, 8)$ given by

$$\chi_1 = \tfrac{1}{2}(4s_2 + 3s_3 - s_1s_2 - 4s_1 - 2), \quad \chi_3 = s_1,$$
$$\chi_2 = \tfrac{1}{4}(2s_2 + 5s_3 - s_1s_2 - 6s_1 - 4), \quad \chi_4 = \tfrac{1}{2}(s_1s_2 + 2s_1 + 2 - 2s_2 - 3s_3),$$

the test characters stable converge to $M(H_1)$ after only 128 primes, with results here in increments of 128 primes; see Table 5.

These convergence results give empirical support to the principle of using irreducible characters as test functions, based on the theoretical interpretation of inner product relations on characters as variance and covariance. Moreover, when using irreducible characters, the number of primes necessary to recognize the Gram matrix associated to a Galois group is strikingly small.

7. Asymptotics in the degree

In analyzing the character theory of a permutation group of large degree, one must avoid certain bottlenecks in the complexity. First the number of transitive permutation groups is too large to enumerate,

k	$\lVert Z_S(G)\rVert_2$	$\lVert Z_S(G)\rVert_8$	$\lVert Z_S(G)\rVert_\infty$	k	$\lVert Z_S(G)\rVert_2$	$\lVert Z_S(G)\rVert_8$	$\lVert Z_S(G)\rVert_\infty$
1	0.512041 <	1.947691 <	3.843750	17	0.122505 <	0.279019 <	0.473345
2	0.256200 <	0.868283 <	1.609375	18	0.118703 <	0.265146 <	0.452473
3	0.180087 <	0.525172 <	0.929687	19	0.114018 <	0.254474 <	0.432360
4	0.251753 <	0.848164 <	1.571289	20	0.110361 <	0.248728 <	0.442968
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
13	0.161766 <	0.376064 <	0.648137	29	0.110513 <	0.283699 <	0.530980
14	0.151537 <	0.350967 <	0.611049	30	0.108019 <	0.275711 <	0.514713
15	0.139688 <	0.325884 <	0.550000	31	0.105191 <	0.262830 <	0.491053
16	0.128557 <	0.298173 <	0.504638	32	0.102228 <	0.251891 <	0.468505

Table 6. Approximation for $G = W(E_8)/Z(W(E_8))$ on sample sets of $256k$ primes, using a basis of irreducible characters.

and so clearly the poset must be navigated in a lazy fashion. Second, the number of conjugacy classes (hence of irreducible characters) for $\mathcal{S}_n$ is too large to enumerate. For the generic groups $\mathcal{S}_n$ and $\mathcal{A}_n$, the characters $(1, s_1, \dots, s_{n-1})$ and $(1, s_1, \dots, s_m)$, where $n = 2m+1$ or $2m+2$, give a subset of rational irreducible test functions (when $n = 2m+2$, the character s_m is the sum of two characters on $\mathcal{A}_n$, conjugate over a quadratic field). In general the number of conjugacy classes is the partition number $p(n)$, whose asymptotic growth is known by [11] to be

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

In particular, we will treat a nontrivial example of degree 120 (and 240) despite the large size $p(120) = 1844349560$ (and $p(240) = 105882246722733$) of the corresponding partition numbers. Finally, computation of the kernel ideal of the restriction $\mathfrak{R}(O(n-1)) \to \mathfrak{R}(G)$ by Groebner basis algorithms is prohibitively expensive, even if the $s(G)$ points in the kernel can be computed.

Polynomials with interesting Galois groups of large degree, outside the generic groups $\mathcal{S}_n$ and $\mathcal{A}_n$ and cyclic and dihedral groups C_n and D_n rely on specific constructions. We consider such an example of Jouve, Kowalski and Zywina [13], a polynomial $f(x)$ of degree 240 with Galois group the Weyl group $W(E_8)$ of the lattice E_8, of order 696729600. In contrast to the large number of conjugacy classes of $\mathcal{S}_{240}$, the number of conjugacy classes of $W(E_8)$ is 112, and the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_{240})$ has full rank. We take the quotient of order 348364800 by its center, which is the Galois group of the degree-120 polynomial $g(x)$ such that $f(x) = g(x^2)$. The quotient group $G = W(E_8)/Z(W(E_8))$ has 67 conjugacy classes, all characters are rational, and the restriction homomorphism from $\mathfrak{R}(\mathcal{S}_{120})$ is a subring of rank 65. We consider the 18 absolutely irreducible rational characters in the image. In increments of 256 primes, we compute the convergence to the Gram matrix $A(G)$ for these 18 characters to $2^{13} = 256 \cdot 32$ primes; see Table 6.

Extending the computation further suggests that the convergence to $M(G)$ is stable for $m > 2^{13}$.

8. Conclusion

A standard tool in Galois group computation is to recognize the probable group from an analysis of Frobenius cycle types. We use an explicit polynomial parametrization of the character ring to identify the irreducible characters in the restriction from orthogonal groups and subsequently from the symmetric group. As in the thesis work of Shieh [17; 18], with the view to classifying Sato–Tate groups, it is recognized that the irreducible characters on the target group provide optimal test functions for recognizing (or rejecting) a given group coming from a Galois representation. We develop this perspective in the application to the parametrized representation rings of finite groups, with associated lattice structure. Although we focus on Galois groups arising from splitting fields of polynomials over $\mathbb{Q}$, the same methods apply to Galois representations coming from L-series and modular forms, families of exponential sums, and global fields of any characteristic.

At a higher level, the approach through character theory and arithmetic statistics lets us identify when Frobenius distributions of different degrees admit a common Galois subrepresentation. Examples arise in the form of fields with isomorphic normal closures, as described in the above examples of $\mathcal{A}_5$ representations, but more generally one can recognize whether two normal fields admit a common subfield. In this framework, orthogonality relations of characters are measured by correlations of Frobenius distributions associated to different representations of the absolute Galois group. This perspective has promising potential for the computational investigation of Galois representations.

Acknowledgements

The author thanks Fernando Rodriguez-Villegas for suggesting the specialization to finite groups of the author's work with Yih-Dar Shieh and Gilles Lachaud, on explicit character theory of orthogonal groups, and for providing notes of his talk in Leiden on the analysis of Galois groups by explicit character theory (see also the 2012 bachelor's thesis of van Bommel [20]). Thanks go also to Claus Fieker for discussions of his algorithm and code in Magma for constructing subfields of the normal closure of a given number field, used in building test examples of number fields with common Galois closure. Finally, the author thanks an anonymous referee for suggesting the permutation groups 8T10 and 8T11 as the first example (of lowest degree) for which the cycle distributions fail to distinguish the groups. This work is dedicated to the memory of Gilles Lachaud and our conversations on explicit character theory of compact Lie groups.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[2] Jos Brakenhoff, *The representation ring and the center of the group ring*, master's thesis, Universiteit Leiden, 2005.

[3] Daniel Bump, *Lie groups*, 2nd ed., Graduate Texts in Mathematics, no. 225, Springer, 2013. MR 3136522

[4] Greg Butler, *The transitive groups of degree fourteen and fifteen*, J. Symbolic Comput. **16** (1993), no. 5, 413–422. MR 1271082

[5] Gregory Butler and John McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911. MR 695893

[6] The LMFDB collaboration, *The L-functions and modular forms database*, 2018, http://www.lmfdb.org/.

[7] Magma computational algebra group, *The Magma handbook*, 2018, https://magma.maths.usyd.edu.au/magma/handbook/.

[8] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8. MR 1635715

[9] Francesc Fité and Xavier Guitart, *On the rank and the convergence rate towards the Sato–Tate measure*, Int. Math. Res. Not. (2017).

[10] The GAP group, *GAP – Groups, Algorithms, and Programming*, 2018, version 4.8.10, https://www.gap-system.org.

[11] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115. MR 1575586

[12] Alexander Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), no. 1, 1–30. MR 2168238

[13] Florent Jouve, Emmanuel Kowalski, and David Zywina, *An explicit integral polynomial whose splitting field has Galois group $W(E_8)$*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 761–782. MR 2523316

[14] Michael E. Pohst, *Computing invariants of algebraic number fields*, Group theory, algebra, and number theory, de Gruyter, Berlin, 1996, pp. 53–73. MR 1440204

[15] Gordon F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987), no. 2, 255–268. MR 922391

[16] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, no. 42, Springer, 1977. MR 0450380

[17] Yih-Dar Shieh, *Arithmetic aspects of points counting and Frobenius distributions*, Ph.D. thesis, Aix-Marseille Université, 2015.

[18] Yih-Dar Shieh, *Character theory approach to Sato–Tate groups*, LMS J. Comput. Math. **19** (2016), suppl. A, pp. 301–314. MR 3540962

[19] Masaru Takeuchi, *A remark on the character ring of a compact Lie group*, J. Math. Soc. Japan **23** (1971), 662–675. MR 0293010

[20] Raymond van Bommel, *Using the Chebatorev density theorem to compute the size of Galois groups*, bachelor's thesis, Universiteit Leiden, 2012.

Received 2 Mar 2018. Revised 9 Sep 2018.

DAVID KOHEL: david.kohel@univ-amu.fr
Aix-Marseille Université, CNRS, Centrale Marseille, I2M, Marseille, France

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

The cover image is based on a design by Linh Chi Bui.

Electronic copies can be obtained free of charge from http://msp.org/obs/2 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine