ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 34, Number 4, Winter 2004

# FROBENIUS CLASSES IN ALTERNATING GROUPS

DAVID P. ROBERTS

ABSTRACT. We present a method, based on an old idea of Serre, for completely computing Frobenius classes in alternating groups. We contrast this method with other approaches in examples involving the alternating groups $A_3$ and $A_9$. The method can be useful for proper subgroups of alternating groups as well, and we present examples involving the 168-element group $PSL_2(7) = GL_3(2)$ and the Mathieu group $M_{24}$.

**1. Introduction.** Let $f \in \mathbf{Z}[x]$ be a monic degree $n$ irreducible polynomial. Let $X$ be its set of complex roots. Let $G$ be the Galois group of $f$. By definition, $G$ is a subgroup of the symmetric group $S_X$. A standard fact is that $G$ is contained in the alternating group $A_X$ if and only if the field discriminant $d$ of $\mathbf{Q}[x]/f(x)$ is a square. Equivalently, $G \subseteq A_X$ if and only if the polynomial discriminant $D = dc^2$ of $f$ is a square.

In general, for $G$ a finite group we denote by $G^\natural$ its set of conjugacy classes. For example, the class-set $S_n^\natural$ is naturally identified, via lengths of disjoint cycles, with the set $P_n$ of partitions of $n$. In this paper, we are concerned with the class-set $A_n^\natural$. For $n \geq 3$, the natural map $A_n^\natural \to S_n^\natural$ is never quite injective, as two classes can be sent to one.

In the situation of the first paragraph, for each prime $p$ not dividing $d$ there is a Frobenius class $\mathrm{Fr}_p \in G^\natural$. Let $\mathrm{Fr}_p^S$ be the image of $\mathrm{Fr}_p$ under the natural map $G^\natural \to S_n^\natural$. Then, as is very well known, $\mathrm{Fr}_p^S$ is just the partition giving the degrees of the irreducible factors of $f$ in the ring $\mathbf{Z}_p[x]$, where $\mathbf{Z}_p$ is the ring of $p$-adic integers. The computation is easier for $p$ not dividing $D$, as then it suffices to factor over the finite field $\mathbf{F}_p$, rather than over $\mathbf{Z}_p$.

Now, assuming $d$ is a square, and imposing our conventions in Sections 2 and 3 to remove a single global sign ambiguity, one has a natural map from $G^\natural$ to $A_n^\natural$. Let $\mathrm{Fr}_p^A$ be the image of $\mathrm{Fr}_p$ in $A_n^\natural$.

Received by the editors on September 21, 2001, and in revised form on May 28, 2002.

Then to compute Frobenius elements $\mathrm{Fr}_p^A$, not just $\mathrm{Fr}_p^S$, one has to resolve the ambiguities associated with the failure of $A_n^\natural \to S_n^\natural$ to be injective.

In the case $n = 5$, the class-set in question is $A_5^\natural = \{11111, 221, 311, 5+, 5-\}$. In [**3**, p. 53] Buhler presents a method which he attributes to Serre for resolving the unique ambiguity of $5+$ versus $5-$. In this paper we describe the natural extension of this method to arbitrary $n$, which we still call the Serre method. The method does not require that one actually know $G$, just that $d$ is a square.

To compute Frobenius elements $\mathrm{Fr}_p$ fully in $G^\natural$ for general $G$, one often works with numerical approximations of the complex roots. Section 7.2 of [**1**] provides a sample such computation with $G = GL_3(2) \subset A_7$. In contrast, the Serre method for computing $\mathrm{Fr}_p^A$ does not require any computations with complex roots. In this respect, it is like the simple computation of the partitions $\mathrm{Fr}_p^S$. The map $GL_3(2)^\natural \to A_7^\natural$ is injective, and so the computations in [**1**, Section 7.2] could have been done by a mechanical application of Serre's method. This connection with [**1**] was one of our motivations for writing the present paper.

In Section 2, we review what we need from alternating groups. In Section 3, we present the method in conceptual terms. In Section 4, we explain how one carries out the method in practice, under the simplifying assumption that $p$ does not divide $2D$, so that one can do all computations modulo $p$. A short *Mathematica* implementation in this context is available at `http://cda.mrs.umn.edu/∼roberts/`.

The remaining sections concern examples. In Sections 5 and 6, we work out examples with $G = A_3$ and $G = A_9$, comparing the Serre method with other methods available in these cases. In Section 7, we apply Serre's method to the Trinks polynomial $x^7 - 7x + 3$ with Galois group $PSL_2(7) = GL_3(2)$ and discuss connections with classical and nonclassical modular forms. The Serre method works with minimal modification over finitely generated domains, not just over $\mathbf{Z}$. In Section 8, we work out an example with ground ring $R = \mathbf{F}_{47}[t]$ and $G$ the Mathieu group $M_{24}$.

**2. Alternating groups and ambiguous classes.** The material in this section is well known, the book [**7**] being a general reference. Our presentation is organized to facilitate the application to Serre's method.

Let $S_n$ be the group of permutations of the set $\{1, 2, \ldots, n\}$. A partition $\lambda$ of $n$ is a finite sequence of positive integers $\lambda_1, \lambda_2, \ldots$ satisfying $\lambda_i \geq \lambda_{i+1}$ and summing to $n$. For $\lambda$ a partition of $n$, we let $g_\lambda$ be the permutation obtained by inserting parentheses and removing commas in $1, 2, \ldots, n$, so that one has a $\lambda_1$-cycle followed by a $\lambda_2$-cycle, and so on. As examples, with $n = 8$,

$$\begin{aligned} g_{5,1,1,1} &= (1,2,3,4,5)(6)(7)(8), \\ g_{5,3} &= (1,2,3,4,5)(6,7,8). \end{aligned}$$

In $S_n$, if an element has cycle structure $\lambda$ then it is conjugate to $g_\lambda$. This fact yields the bijection $S_n^\natural \to P_n$ mentioned in the introduction.

Let $A_n$ be the subgroup of even permutations in $S_n$. Its conjugacy class-set $A_n^\natural$ maps surjectively to the set $P_n^{\text{even}}$ consisting of partitions $\lambda$ with an even number of even parts $\lambda_i$. However this map is not injective for $n \geq 3$, as we will explain in this paragraph. Define a partition $\lambda$ of $n$ to be ambiguous if its parts $\lambda_i$ are distinct and odd. So the ambiguous partitions for $3 \leq n \leq 15$ are as follows.

| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 3,1 | 5 | 5,1 | 7 | 7,1 | 9 | 9,1 | 11 | 11,1 | 13 | 13,1 | 15 |
| | | | | | 5,3 | 5,3,1 | 7,3 | 7,3,1 | 9,3 | 9,3,1 | 11,3 | 11,3,1 |
| | | | | | | | | | 7,5 | 7,5,1 | 9,5 | 9,5,1 |
| | | | | | | | | | | | | 7,5,3 |

Let $Z_\lambda$ be the centralizer of $g_\lambda$ in $S_n$. For $k \geq 1$, let $m_k$ be the number of times $k$ is a part of $\lambda$. Then $|Z_\lambda| = \prod m_k! k^{m_k}$. For $\lambda$ ambiguous, $|Z_\lambda|$ is odd and so $Z_\lambda \subseteq A_n$. For $\lambda$ nonambiguous, $|Z_\lambda|$ is even and in fact $Z_\lambda \not\subseteq A_n$. Because of this distinction, $A_n^\natural$ has two classes which map to a given ambiguous partition and one class which maps to a given non-ambiguous partition in $P_n^{\text{even}}$. For $\lambda$ an ambiguous partition, we let $\lambda+$ be the class of $g_\lambda$ and $\lambda-$ be the other class. Thus, for example, $A_5^\natural = \{11111, 221, 311, 5+, 5-\}$, as stated in the Introduction. We will continue the practice of sometimes dropping commas when the meaning is clear, writing e.g. 311 for $3, 1, 1$.

Let $X$ be an $n$-element set. There are $n!$ total orderings of $X$, i.e., $n!$ bijections from $X$ to the standard $n$-element set $\{1, 2, \ldots, n\}$.

These total orderings are permuted simply transitively by $S_n$ by post-composition. If $n \geq 2$, they fall into two orbits under $A_n$. An orientation on $X$ is by definition the datum of one of these two orbits.

We now come to the key group-theoretic construction underlying the Serre method. Let $X$ be an $n$-element set with a permutation $F : X \to X$. A total ordering on $X$ will be called $F$-respectful if it is obtained in the following way: choose an ordering of the $F$-orbits of $X$ so that the orbits $X_1$, $X_2, \ldots$ weakly decrease in size; from each orbit $X_i$, choose an element $x_{i,1}$ and for $j = 2, \ldots, |X_i|$, define $x_{i,j} = Fx_{i,j-1}$; give $X$ the resulting lexicographic ordering. Suppose there are $m_k$ orbits of size $k$. Then there are $\prod_k m_k!$ ways to choose a weakly size-decreasing order of the orbits. There are $\prod_k k^{m_k}$ ways to choose the initial elements $x_{i,1}$. So the set $O_F$ of $F$-respectful orderings has $\prod_k m_k! k^{m_k}$ elements, this number being exactly $|Z_\lambda|$. In fact, $Z_\lambda$ acts freely and transitively on $O_F$. Each ordering in $O_F$ determines an orientation of $X$ and all these orientations are the same if and only if $\lambda$ is ambiguous. In summary, if the orbit partition of the permutation $F$ is ambiguous, then $F$ determines an orientation on $X$, which we will call the $F$-orientation.

Our final topic in this section will play a role only in Sections 6–8. Let $\lambda$ be an ambiguous partition and let $m$ be the least common multiple of its parts. The issue is to determine for what $i \in (\mathbf{Z}/m)^\times$ the power $g_\lambda^i$ is still in the class $\lambda+$, rather than $\lambda-$. To resolve this issue, for $p$ an odd prime number let $\omega_p : (\mathbf{Z}/p)^\times \to \{+,-\}$ be the unique surjective character, i.e. the one sending squares to the identity element $+$ and nonsquares to $-$. More generally, for $l$ an odd positive integer with prime factorization $\prod p^{e_p}$, let $\omega_l = \prod \omega_p^{e_p}$. Here we view each $\omega_p$ as a character on $(\mathbf{Z}/l)^\times$ via the ring-surjection $\mathbf{Z}/l \to \mathbf{Z}/p$. Finally, define $\omega_\lambda : (\mathbf{Z}/m)^\times \to \{+,-\}$ to be the product of the $\omega_{\lambda_i}$, again suppressing the ring surjections $\mathbf{Z}/m \to \mathbf{Z}/\lambda_i$ from the notation. The basic fact is that

$$g_\lambda^i \in \lambda\omega_\lambda(i).$$

In particular, no power of $g_\lambda$ is in $\lambda-$ if and only if $P = \prod \lambda_i$ is a perfect square. In this case, all irreducible characters of $A_n$ take rational values on the classes $\lambda+$ and $\lambda-$. Otherwise, there are characters taking a non-rational value in $\mathbf{Q}(\sqrt{\omega_4(P)P})$ on $\lambda+$ and the conjugate value on $\lambda-$; here $\omega_4(P) = +$ if $P \equiv 1$ (4) and $\omega_4(P) = -$ if $P \equiv 3$ (4). This rationality structure on $A_n^\natural$ is visible for $5 \leq n \leq 12$ in the Atlas [**4**].

## 3. The method.

For each prime $p$, fix $\overline{\mathbf{F}}_p$, an algebraic closure of $\mathbf{F}_p$. Let $\mathbf{Z}_p^{\mathrm{un}}$ be the corresponding maximal unramified extension of the $p$-adic integers $\mathbf{Z}_p$, so that the residue field of $\mathbf{Z}_p^{\mathrm{un}}$ is $\overline{\mathbf{F}}_p$. The Frobenius operator $\mathrm{Frob}_p : \overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$ is the automorphism $x \mapsto x^p$. It lifts to a unique automorphism in characteristic zero, which we denote by the same symbol, $\mathrm{Frob}_p : \mathbf{Z}_p^{\mathrm{un}} \to \mathbf{Z}_p^{\mathrm{un}}$.

We continue with the notation of the introduction: $f \in \mathbf{Z}[x]$ is a monic irreducible degree $n$ polynomial, $X$ its set of complex roots, $G \subseteq S_X$ its Galois group and $d \in \mathbf{Z}$ its field discriminant. Frobenius elements can be defined in this context as follows. Let $X_p$ be the set of roots of $f$ in $\mathbf{Z}_p^{\mathrm{un}}$. One has $|X_p| = n$ if and only if $p$ does not divide $d$. Let $L$ be the subring of $\mathbf{C}$ generated by $X$. One has embeddings $L \to \mathbf{Z}_p^{\mathrm{un}}$ if and only if $p$ does not divide $d$. In this case, there are $|G|$ embeddings $L \to \mathbf{Z}_p^{\mathrm{un}}$ giving $|G|$ different bijections $X \to X_p$. These embeddings and bijections are permuted simply transitively by $G = \mathrm{Aut}\,(L) \subseteq S_X$. Frobenius classes are defined by transport of structure from $X_p$ to $X$.

**Definition 3.1.** Let $f \in \mathbf{Z}[x]$ and its associated objects be as above. Let $p$ be a prime not dividing $d$ and let $e : L \to \mathbf{Z}_p^{\mathrm{un}}$ be an embedding. Then $\mathrm{Fr}_{p,e} \in G$ is defined by $\mathrm{Fr}_{p,e}x = (e^{-1} \circ \mathrm{Frob}_p \circ e)x$. The conjugacy class of $\mathrm{Fr}_{p,e}$ is independent of $e$ and denoted $\mathrm{Fr}_p \in G^\natural$

Recall that that the polynomial discriminant $D$ of $f$ is given by

$$\prod_{i<j} (\alpha_i - \alpha_j)^2 = D, \tag{3.1}$$

where we have arbitrarily ordered the complex roots,

$$X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}. \tag{3.2}$$

Now assume that the discriminant $D$ is a square, hence positive. Then

$$\prod_{i<j} (\alpha_i - \alpha_j) = \pm\sqrt{D}. \tag{3.3}$$

We say that the ordering (3.2) is positive or negative, according to the sign of (3.3). For $p$ not dividing $d$, we have the direct analogs of

(3.1)–(3.3) with $X$ replaced by $X_p$. We give $X$ its positive orientation and all the $X_p$ their positive orientation too. The bijections $e : X \to X_p$ coming from embeddings $L \to \mathbf{Z}_p^{\mathrm{un}}$ then preserve orientation. The sets $A_X^\natural$, $A_{X_p}^\natural$, and $A_n^\natural$ are thereby canonically identified. Our main theorem is now clear from the definition of Frobenius elements, and the fact that we are using a $\mathrm{Frob}_p$-respectful ordering on $X_p$.

**Theorem 3.1.** *Let $f \in \mathbf{Z}[x]$ be a monic degree $n$ irreducible polynomial with a square discriminant $D$. Let $p$ be a prime number not dividing the field discriminant $d$. Factor $f$ over $\mathbf{Z}_p$, writing*

$$f = \prod_{i=1}^{k} f_i \tag{3.4}$$

*with $f_i$ irreducible in $\mathbf{Z}_p[x]$ of degree $\lambda_i$ with $\lambda_i \geq \lambda_{i+1}$. Suppose the $\lambda_i$ are odd and distinct so that there is a sign $\varepsilon_p$ to be determined to identify $Fr_p^A \in A_n^\natural$.*

*For $i = 1, \ldots, k$, let $\beta_{i,1} \in \mathbf{Z}_p^{\mathrm{un}}$ be a root of $f_i$. For $j = 2, \ldots, \lambda_i$ define $\beta_{i,j} = Frob_p \beta_{i,j-1}$. Order the set of indices $(i, j)$ lexicographically. Define the semi-discriminant of $f$ at $p$ to be the integer*

$$\Delta_p = \prod_{(i,j)<(i',j')} (\beta_{i,j} - \beta_{i',j'}). \tag{3.5}$$

*Then*

$$\varepsilon_p = \Delta_p/\sqrt{D}. \tag{3.6}$$

**4. Implementation.** A computational problem with the method as just described is that one needs to actually construct a large enough subring of $\mathbf{Z}_p^{\mathrm{un}}$ and then find roots within it. Here is a computational improvement, which for simplicity we present assuming the additional hypothesis that $p$ does not divide $2D$. This extra hypothesis allows us to work at the level of $\overline{\mathbf{F}}_p$ rather than $\mathbf{Z}_p^{\mathrm{un}}$.

Continuing with the notation of Theorem 3.1, define for each index $i$ a finite field

$$F_{p^{\lambda_i}} = \mathbf{F}_p[\gamma_i]/f_i(\gamma_i).$$

For $j = 1, \ldots, \lambda_i$, define $\gamma_{i,j} = \gamma_i^{p^{j-1}}$. Then one has the formula

$$\Delta_p = \left(\prod_{i=1}^{k} \prod_{j<j'} (\gamma_{i,j} - \gamma_{i,j'})\right)\left(\prod_{i<i'} \mathrm{Res}_x(f_i, f_{i'})\right) \in \mathbf{F}_p, \tag{4.1}$$

with $\mathrm{Res}_x$ indicating the resultant with respect to $x$. Formula (4.1) agrees with formula (3.5) for the following reason. Embed each $F_{p^{\lambda_i}}$ into $\overline{\mathbf{F}}_p$ by sending $\gamma_i$ to $\beta_i$, so that $\gamma_{i,j}$ is sent to $\beta_{i,j}$. Then for $i < i'$,

$$\mathrm{Res}_x(f_i, f_{i'}) = \prod_{j,j'} (\beta_{i,j} - \beta_{i',j'}),$$

so all the factors of (3.5) are accounted for.

The URL mentioned in the introduction contains an implementation of Theorem 3.1 via (4.1) in *Mathematica*, under the command `FrobA`. Allowing $p$ to be one of the divisors of $2D$ not dividing $d$ would require substantially more complicated code. Section 7 contains a computation with $p = 2$ which illustrates the sort of thing one would have to add to `FrobA` to treat the general case.

## 5. Cyclotomic reciprocity: An $A_3$ example.

In this section and the next, we compare the Serre method for getting information on Frobenius elements with two well-known methods. The three methods let one go beyond simply computing factor partitions $\mathrm{Fr}_p^S$ in three mostly different directions. However we have chosen our examples so that the Serre method and one of the other methods each work.

Let $f \in \mathbf{Z}[x]$ and its associated objects be as in Sections 1–3. Let $G^{\mathrm{ab}} = G/[G,G]$ be the abelianization of the Galois group $G$. Then one has a natural surjection $G^\natural \to G^{\mathrm{ab}}$. For $p$ a prime not dividing $d$, let $\mathrm{Fr}_p^{\mathrm{ab}}$ be the image of the Frobenius element $\mathrm{Fr}_p$. Then cyclotomic reciprocity says that $\mathrm{Fr}_p^{\mathrm{ab}}$ depends only on the class of $p$ modulo $C$, with $C$ being some divisor of $d$.

As the example for this section, we take $f(x) = x^3 - 3x + 1$. Its discriminants are $d = D = 81$. Applying the `FrobA` program for the primes $5 \le p \le 47$ yields the information on the second line.

| Class $\mu$ in $A_3^\natural$ | 111 | 3+ | 3− |
|---|---|---|---|
| Primes with $\mathrm{Fr}_p \in \mu$ | 17,19, 37 | 7,11,29,43,47 | 5,13,23,31,41 |
| Same primes, modulo 9 | 8, 1, 1 | 7, 2, 2, 7, 2 | 5, 4, 5, 4, 5 |

The third line illustrates cyclotomic reciprocity, which applies here with $C = 9$.

For $n = 4$, the unique ambiguity is 31+ versus 31−. This ambiguity can be resolved by cyclotomic reciprocity because $A_4^{\mathrm{ab}}$ is cyclic of order 3. For $n \geq 5$, the ambiguities resolved by the Serre method are not resolvable by cyclotomic reciprocity, since $A_n^{\mathrm{ab}}$ is the trivial group.

**6. Rational classes and resolvents: An $A_9$ example.** Let $G$ be a finite group with exponent $e$ and let $G^\natural$ be its class-set. The group $(\mathbf{Z}/e)^\times$ acts on $G$ by exponentiating elements. This action passes to an action on conjugacy classes: $[g]^i = [g^i]$. Let $G^{\mathrm{rat}}$ be the quotient set $G^\natural/(\mathbf{Z}/e)^\times$.

Let $f \in \mathbf{Z}[x]$ and associated objects be as in Sections 1–3. Once one has identified the Galois group $G$ of $f \in \mathbf{Z}[x]$, one can compute Frobenius elements $\mathrm{Fr}_p^{\mathrm{rat}} \in G^{\mathrm{rat}}$ by means of looking at factorization partitions over $\mathbf{Z}_p$ of suitable resolvents.

As our example for this section, take $f(x) = x^9 + 27x - 24 \in \mathbf{Z}[x]$. Its discriminants are the squares $d = 2^{18}3^{26}$ and $D = 2^{26}3^{26}$. Its Frobenius partitions $\mathrm{Fr}_p^S$ include the two ambiguous partitions 9 and 531, so the only possibility for the Galois group $G$ is the entire alternating group, as $A_9$ does not have a proper transitive subgroup with order divisible by 5. The primes $p < 100$ giving rise to these two partitions and the associated signs computed by `FrobA` are

| | + | − |
|---|---|---|
| 531 | 19,29 | 7,41 |
| 9 | 79 | 11,23. |

Now $531+^{-1} = 531-$ from the end of Section 2, the associated quadratic field being $\mathbf{Q}(\sqrt{-15})$. However no power of 9+ is 9−. The classes 9+ and 9− being each rational, it is possible to distinguish these two classes by means of resolvents.

Our point is that the resolvent method is both conceptually and computationally more difficult than the Serre method of distinguishing $9+$ from $9-$. The resolvent method works as follows. In the Atlas, note that the characters $\chi_{35a}$ and $\chi_{35b}$ are the only ones which do not satisfy $\chi(9A) = \chi(9B)$. Note also that $A_9$ has two permutation representations of degree 120. One has character $\chi_1 + \chi_{35a} + \chi_{84a}$ and the other has character $\chi_1 + \chi_{35b} + \chi_{84a}$. So we can use these representations to distinguish $9A$ from $9B$. Again from the Atlas, we see that the stabilizer of either of these permutation representations is a group of the form $\Sigma L_2(8) = SL_2(8).3$. Following [**2**], we work with

$$\Sigma L_2(8) = \langle (12)(35)(46)(79),\ (234)(678) \rangle.$$

The two resolvents we will use are $r_+$ and $r_-$, defined in several steps as follows.

First, there are $9!/3!^3 = 1680$ functions $e : \{1, 2, \ldots, 9\} \to \{0, 1, 2\}$ having three elements in each fiber. The group $\Sigma L_2(8)$ acts on this set. There are two orbits, one $E$ of order 168 and the other one of order $1680 - 168 = 1512 = |\Sigma L_2(8)|$. A function belonging to $E$ is

$$1, 2, 3 \longmapsto 0, \qquad 4, 5, 8 \longmapsto 1, \qquad 6, 7, 9 \longmapsto 2.$$

Second, let $\Sigma$ be the subgroup of $S_9$ consisting of elements $\sigma$ which fix 1, fix 2, and stabilize the set $\{3, 4\}$. So $\Sigma$ has $2! \cdot 5! = 240$ elements; it is a set of representatives for the left cosets of $\Sigma L_2(8)$. Let $\Sigma_+ = \Sigma \cap A_9$ and write $\Sigma = \Sigma_+ \coprod \Sigma_-$, so that $\Sigma_+$ and $\Sigma_-$ each have 120 elements. Finally, put

$$r_\varepsilon(x) = \prod_{\sigma \in \Sigma_\varepsilon} \left( x - \sum_{e \in E} \prod_{j=1}^{9} \alpha_{\sigma j}^{e(j)} \right),$$

with $\alpha_1, \ldots, \alpha_9$ the roots of $f$, ordered so that (3.3) holds with a positive sign. The $r_\varepsilon$ are both in $\mathbf{Z}[x]$. Explicitly, both have the form

$$x^{120} + 8{,}640\, x^{119} + 32{,}814{,}720\, x^{118} + 69{,}208{,}390{,}656\, x^{117} + \cdots$$

The next term of $r_+$ is $79{,}456{,}787{,}896{,}320\, x^{116}$ while the next term of $r_-$ is $79{,}574{,}334{,}142{,}464\, x^{116}$. The coefficients of both $r_+$ and $r_-$ grow monotonically in absolute value, with constant term having 288 digits in each case. The entire polynomials are available at `http://cda.mrs.umn.edu/~roberts/`.

For $p \neq 2, 3$, one has the corresponding factor partitions $\lambda_{+,p}$ and $\lambda_{-,p}$. One has equality $\lambda_{+,p} = \lambda_{-,p}$ unless $\mathrm{Fr}_p^S$ is the partition 9. In this case they differ:

$$\begin{aligned} \mathrm{Fr}_p \in 9+ &\iff \lambda_{+,p} = 9^{13}1^3 &&\iff \lambda_{-,p} = 9^{13}3 \\ \mathrm{Fr}_p \in 9- &\iff \lambda_{+,p} = 9^{13}3 &&\iff \lambda_{-,p} = 9^{13}1^3. \end{aligned}$$

One can confirm these relations computationally at the primes $p = 11$, 23, and 79.

## 7. Connections with two types of automorphic forms: A $PSL_2(7) = GL_3(2)$ example.

The examples of the last two sections involved polynomials with Galois group all of $A_n$. However, as we mentioned in the introduction, the Serre method can be useful even when $G$ is a proper subgroup of $A_n$.

One sequence of examples consists of the simple groups $PSL_2(p)$, with $p \geq 5$ a prime. The group $G = PSL_2(p)$ is embedded in a degree $p+1$ alternating group via its natural action on the projective line over $\mathbf{F}_p$. Here the map $G^\natural \to G^{\mathrm{rat}}$ has large fibers, but a very simple description, as follows. First, an element of $G^{\mathrm{rat}}$ is determined by the order of a representing element $g$. The possible orders are 1, 2, the other divisors of $(p-1)/2$, the other divisors of $(p+1)/2$, and finally $p$. Thus, for example, we would write $PSL_2(11)^{\mathrm{rat}} = \{1; 2; 5; 3, 6; 11\}$. The elements 1 and 2 each have one preimage in $G^\natural$. An element $d$ of the third or fourth type has $\phi(d)/2$ preimages, $\phi$ being the Euler phi function. Finally, the element $p$ has 2 preimages. So $PSL_2(11)^\natural$ would have the form $\{1; 2; 5A, 5B; 3, 6; 11A, 11B\}$. The structure just described is visible for $p \leq 31$ in the Atlas.

The groups $PSL_2(p)$ arise as Galois groups in the classical theory of modular forms on the complex upper half plane. There, by looking at Hecke eigenvalues, or equivalently Fourier coefficients, one can distinguish all elements in $G^\natural$ except that the two preimages of $p \in G^{\mathrm{rat}}$ are not distinguished. Complementing this perfectly, the only ambiguity resolved by the Serre method is to distinguish the two preimages of $p$, the corresponding partition being the ambiguous partition $p1$.

A second sequence of examples consists of the simple groups $GL_n(2)$, with $n$ varying over integers $\geq 3$. This group acts on the projective space $\mathbf{P}^{n-1}(2) = \mathbf{F}_2^n - \{(0, \ldots, 0)\}$ in two distinct ways, by the standard action $A \cdot v = Av$ and by the dual action $A \cdot v = A^{-T}v$, where the superscript indicates inverse-transpose. The group $GL_n(2)$ has elements of order $2^n - 1$. These elements are called Coxeter elements and one of their nice properties is that they act with one orbit in both actions. Since $2^n - 1$ is congruent to 3 modulo 4, if a Coxeter element $g \in GL_n(2) \subset A_{2^n-1}$ has sign $+$ then $g^{-1}$ has sign $-$. Thus, for this second sequence too, the Serre method resolves some ambiguities.

Fields having Galois groups of the form $GL_n(p)$ have been computationally connected to nonclassical automorphic forms on symmetric spaces associated with $GL_n(\mathbf{R})$ by Ash and others, [**1**] being one of several such papers. This theory allows one to separate out the Coxeter classes by automorphic computations.

The two sequences of groups just described overlap in one group via an exceptional isomorphism $PSL_2(7) = GL_3(2)$. For the example in this section, we let $G$ be this group. So $G$ comes with transitive permutations $\rho_8$, $\rho_{7a}$, and $\rho_{7b}$, as discussed above. The set of conjugacy classes of $G$ is $\{1, 2, 3, 4, 7A, 7B\}$, with $7A$ and $7B$ the unipotent classes in the $PSL_2(7)$ realization and the Coxeter classes in the $GL_3(2)$ realization.

In [**10**], Trinks found a trinomial with Galois group $G$, namely $f_{7a}$ below. If we write its roots as $\alpha_i$ and form the monic degree 35 polynomial with roots $\alpha_i + \alpha_j + \alpha_k$ indexed by $i < j < k$, this resolvent polynomial factors into a degree 28 polynomial and $f_{7b}$ below. By a more complicated resolvent construction, one gets $f_8$:

$$\begin{aligned}
f_{7a}(x) &= x^7 - 7x + 3,\\
f_{7b}(x) &= x^7 + 14x^4 - 42x^2 - 21x + 9,\\
f_8(x) &= x^8 - 4x^7 + 7x^6 - 7x^5 + 7x^4 - 7x^3 + 7x^2 + 5x + 1.
\end{aligned}$$

The corresponding discriminants are the squares $d_{7a} = d_{7b} = 3^6 7^8$, $D_{7a} = D_{7b} = 3^8 7^8$, $d_8 = 3^8 7^8$, and $D_8 = 3^{12} 7^8$. The fields $\mathbf{Q}[x]/f_{7a}(x)$ and $\mathbf{Q}[x]/f_{7b}(x)$ are nonisomorphic. However, by construction, the three polynomials have the same splitting field $K$ in $\mathbf{C}$.

Applying `FrobA` gives the following data for the odd primes different from 3 and 7.

| | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_{7a}$ | 7+ | | 7+ | | 7+ | 421 | 331 | 331 | 331 | 7− | 7+ |
| $f_{7b}$ | 7− | | 7− | | 7− | 421 | 331 | 331 | 331 | 7+ | 7− |
| $f_8$ | 71− | | 71− | | 71− | 44 | 3311 | 3311 | 3311 | 71+ | 71− |

We computed the signs at the prime 2 by working modulo 4. The Frobenius automorphism of $\mathbf{Z}/4[x]/f_{7a}(x)$ sends $x$ to $x^2 + g(x)$ where $g(x)$ is a multiple of 2. Requiring that $x^2 + g(x)$ also be a root of $f_{7a}(x)$ modulo 4 forces the Frobenius automorphism to be $x \mapsto x^2+2x^3+2x^4$. Similarly, the Frobenius automorphism of $\mathbf{Z}/4[x]/f_{7b}(x)$ is $x \mapsto 3x^2 + 2x^4 + 2x^6$. In the remaining case, one has

$$f_8(x) = (x^7 + 3x^6 + x^4 + 2x^3 - x^2 + 1)(x + 1) \in \mathbf{Z}/4[x].$$

The Frobenius automorphism corresponding to the first factor is $x \mapsto 2 + x^2 + 2x^3 + 2x^5$. The signs can then be calculated using (4.1) with both sides viewed in $\mathbf{Z}/4$.

This example illustrates the presence of our global sign convention. For $G_{7a}$ and $G_{7b}$ can be regarded as the same group, namely $\mathrm{Gal}\,(K/\mathbf{Q})$. However our conventional injections $G^\natural_{7a} \to A^\natural_7$ and $G^\natural_{7b} \to A^\natural_7$ do not agree.

For both the classical case and the higher rank case, only a small number of examples have been explicitly worked out in the literature, but these small collections of examples include the Trinks field in both cases. For connections with classical modular forms, see [**9**]. For connections with higher rank forms, see [**1**, Table 5].

**8. Another ground ring: An $M_{24}$ example.** The Serre method extends to ground domains $R$ which are finitely generated over $\mathbf{Z}$, so that all maximal ideals $P$ have $R/P$ finite and Frobenius elements $\mathrm{Fr}_P$ are defined. If $R$ has characteristic two, one can work with a lift to $\mathbf{Z}/4$, so as to distinguish $\Delta$ from $-\Delta$. Alternatively, one can work with Jacobson's two quantities [**6**, Exercise 4.8.3] as substitutes for $\Delta$ and $-\Delta$. We have restricted our presentation so far to $R = \mathbf{Z}$ in order to make the main ideas clear without an excess of notation.

We close with an example with $R \neq \mathbf{Z}$ to illustrate in an informal way the extension to general $R$. Our ground ring is $\mathbf{F}_{47}[t]$ and our polynomial is

$$f(x) = (x^2{+}1)^{12}{+}t27(x^3{+}37x^2{+}30x{+}31)^5(x^4{+}16x^3{+}43x^2{+}36x{+}25).$$

The discriminant of $f$ is $D = t^{22}(t-1)^8$; we take $\sqrt{D} = t^{11}(t-1)^4$ to be the positive square root.

We obtained $f$ by starting with the main polynomial $g(u)$ in [**5**] and first reducing its coefficients from $\mathbf{Z}[t]$ to $\mathbf{F}_{47}[t]$. We chose to work modulo a prime because the coefficients of the original polynomial are too large to print. We chose to work modulo 47 because here two of the four singular $t$-values come together so that one has only three singular $t$-values, namely 0, 1, and $\infty$. We then made a complicated change of coordinates from $u$ to $x$ to put the polynomial in the standard form $a(x) + tc(x)$. The associated ramification partitions as in, say [**8**], are

$$\lambda_0 = 12^2, \quad \lambda_1 = 2^8 1^8, \quad \lambda_\infty = 5^4 1^4.$$

Here $\lambda_0$ and $\lambda_\infty$ are visible from (8.1), as encoding the multiplicities of the roots in $\overline{\mathbf{F}}_{47}$ of $a(x)$ and $c(x)$ respectively, with $x = \infty$ to be regarded as a root of $c(x)$ with multiplicity 5. The partition $\lambda_1$ is not directly visible from (8.1), but likewise encodes the multiplicities of the roots of $f(x)$ in $\overline{\mathbf{F}}_{47}$ after specialization to $t = 1$. The field of Puiseux series $\overline{\mathbf{F}}_{47}((t^{1/12}))$ is an adequate substitute for $\mathbf{C}$, as $f(x)$ has 24 roots here, say $\alpha_1, \ldots, \alpha_{24}$. The virtue of starting with the polynomial in [**5**] is that we know that $G$ is contained in a Mathieu group $M_{24} \subset A_{24}$; this fact would be difficult to prove given merely $f(x)$ itself.

Specializing $t = 2, \ldots, 46$ gives homomorphisms $\mathbf{F}_{47}[t] \to \mathbf{F}_{47}$ and hence Frobenius elements which we will denote $\mathrm{Fr}_2, \ldots, \mathrm{Fr}_{46}$. Our program `FrobA` works with minor modifications: it doesn't matter that $\mathbf{F}_{47}$ is arising as a residue field of $\mathbf{F}_{47}[t]$ rather than as a residue field of $\mathbf{Z}$. The $t \in \{2, \ldots, 46\}$ which give rise to ambiguous partitions are given on the following table under the sign calculated by `FrobA`.

| | $+$ | $-$ |
|---|---|---|
| (23,1) | 22 | 23, 42 |
| (21,3) | 7, 10, 21, 35 | 9, 14, 34 |
| (15,5,3,1) | | 2, 31, 33, 37 |

The fact that the three printed partitions arose suffices to prove that $G$ is all of $M_{24}$, as one can deduce from the maximal subgroup list given in the Atlas [**4**]. Information about $M_{24}$ used in the next paragraph is also from the Atlas.

The conjugacy classes $23A$ and $23B$ in $M_{24}^\natural$ are conjugate over $\mathbf{Q}(\sqrt{-23})$ and map bijectively to $(23,1)+$ and $(23,1)-$ in $A_{24}^\natural$, which are also conjugate over $\mathbf{Q}(\sqrt{-23})$. Very similarly, the conjugacy classes $21A$ and $21B$ in $M_{24}^\natural$ are conjugate over $\mathbf{Q}(\sqrt{-7})$ and map bijectively to $(21,3)+$ and $(21,3)-$ in $A_{24}^\natural$, which are also conjugate over $\mathbf{Q}(\sqrt{-7})$. In contrast, classes $15A$ and $15B$ are conjugate over $\mathbf{Q}(\sqrt{-15})$ in $M_{24}$. They both map to the ambiguous partition $(15,5,3,1)$. However $(15,5,3,1)+$ and $(15,5,3,1)-$ are both rational classes, by the end of Section 2, as $15\cdot 5\cdot 3\cdot 1$ is a perfect square. So $15A$ and $15B$ are sent to the same class in $A_{24}^\natural$. Readers who doubt the convenience of the Serre method are invited to try to properly place the Frobenius elements $\mathrm{Fr}_2$, $\mathrm{Fr}_{31}$, $\mathrm{Fr}_{33}$, and $\mathrm{Fr}_{37}$ into the two conjugacy classes $15A$ and $15B$.

## REFERENCES

**1.** A. Ash, D. Doud and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), 521–579.

**2.** J. Bray, S. Linton, S.P. Norton, R.A. Parker, S. Rogers, I. Suleiman, J. Tripp, P. Walsh and R.A. Wilson, *Atlas of finite group representations*, v. 1 (2000), available at `http://www.mat. bham.ac.uk/atlas/`

**3.** J.P. Buhler, *Icosahedral Galois representations*, Lecture Notes in Math., vol. 654, Springer-Verlag, New York, 1978.

**4.** J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *Atlas of finite groups*, Oxford Univ. Press, Oxford, 1985.

**5.** L. Granboulan, *Construction d'une extension régulière de* $\mathbf{Q}(t)$ *de groupe de Galois* $M_{24}$, Experiment. Math. **5** (1996), 3–14.

**6.** N. Jacobson, *Basic algebra* I, W.H. Freeman and Co., New York, 1974.

**7.** G. James and A. Kerber, *The representation theory of the symmetric group*, Encyclopedia Math. Appl. **16**, Addison-Wesley, New York, 1981.

**8.** G. Malle, *Fields of definition of some three point ramified field extensions*, *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994.

**9.** J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ Duke Math. J. **54** (1987), 179–230.

**10.** W. Trinks, *Ein Beispiel eines Zahlkörpers mit der Galoisgruppe* $PSL(3,2)$ *über* $\mathbf{Q}$, manuscript, Univ. Karlsruhe, 1968.

Division of Science and Mathematics, University of Minnesota-Morris,
MN 56267
*E-mail address:* `roberts@mrs.umn.edu`