IDENTIFYING FROBENIUS ELEMENTS IN GALOIS GROUPS

TIM AND VLADIMIR DOKCHITSER

Abstract. We present a method to determine Frobenius elements in arbitrary Galois extensions of global fields, which may be seen as a generalisation of Euler's criterion. It is a part of the general question how to compare splitting fields and identify conjugacy classes in Galois groups, that we will discuss as well.

Contents

1. Introduction

A classical study in number theory concerns Frobenius elements in Galois groups of global fields. One aspect is how to determine Frobenius at a given prime using only the arithmetic of the ground field, answered by class field theory when the extension is abelian. This paper studies the questions how to compare splitting fields and identify conjugacy classes in Galois groups in general (see §2-4). The application to Frobenius elements is the following

Theorem 1.1. *Let K be a global field and $f(x) \in K[x]$ a separable polynomial with Galois group G. There is a polynomial $h(x) \in K[x]$ and polynomials $\Gamma_C \in K[x]$ indexed by the conjugacy classes C of G such that*

$$\mathrm{Frob}_{\mathfrak{p}} \in C \quad \Leftrightarrow \quad \Gamma_C\Big(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q)\Big) = 0 \mod \mathfrak{p}$$

for almost all primes $\mathfrak{p}$ of K; here $\mathbb{F}_q$ is the residue field at $\mathfrak{p}$.

This is proved in §5. We note directly that one can usually take $h(x) = x^2$ (see below), in particular $\mathrm{Tr}(x^{q+2})$ then determines the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$. We will explain how it can be seen as a generalisation of Euler's criterion $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \mod p$ for general polynomials, and how it recovers classical formulae for Frobenius elements in cyclotomic and Kummer extensions (§5-6). In §7 we give explicit examples for non-abelian Galois groups, including formulae that determine the splitting behaviour of general cubics and quartics.

The theorem is explicit for practical purposes. Indeed, our motivation was computing L-series of Artin representations for arbitrary Galois groups, which require the knowledge of Frobenius elements at all primes (see Remark 5.8). The polynomials Γ_C have degree $|C|$ and can be explictly given by

$$\Gamma_C(X) \;=\; \prod_{\sigma\in C}\bigl(X-\sum_{j=1}^{n} h(a_j)\sigma(a_j)\bigr),$$

where $a_1,...,a_n$ are the roots of f in some splitting field. The 'almost all primes' in the theorem are those not dividing the denominators of the coefficients of f, its leading coefficient and the resultants $\mathrm{Res}(\Gamma_C,\Gamma_{C'})$ for $C\neq C'$; the latter simply says that the Γ_C mod $\mathfrak{p}$ are pairwise coprime. (This condition always fails for ramified primes, see Remark 5.6.) Finally, the only constraint on h is that the resulting Γ_C are coprime over K. This holds for almost all h, in the sense that the admissible ones of degree at most $n-1$ form a Zariski dense open subset of K^n. Also, a fixed h with $1<\deg h<n$ (e.g. $h(x)=x^2$) will work for almost all f that define the same field (see §8).

To illustrate our approach to Frobenius elements, let us do a simple case by hand:

Example 1.2. The polynomial $f(x)=x^5+2x^4-3x^3+1$ has Galois group $G=\mathrm{D}_{10}$ over $K=\mathbb{Q}$. If we number its complex roots by

$$a_1\approx -3.01,\quad a_2\approx -0.35-0.53i,\quad a_3\approx 0.85-0.31i,\quad a_4=\overline{a_3},\quad a_5=\overline{a_2},$$

then G is generated by the 5-cycle (12345) and complex conjugation (25)(34). It is easy to see that $f(x)$ is irreducible over $\mathbb{F}_2$, so $\mathrm{Frob}_2\in G$ is in one of the two conjugacy classes of 5-cycles, either $[(12345)]$ or $[(12345)^2]$. How can we check which one it is?

Consider the expressions,

$$\begin{aligned} n_1 &= a_1a_2+a_2a_3+a_3a_4+a_4a_5+a_5a_1,\\ n_2 &= a_1a_3+a_2a_4+a_3a_5+a_4a_1+a_5a_2. \end{aligned}$$

If we think of G as the group of symmetries of a pentagon, the sums are taken over all edges and over all diagonals respectively. Therefore they are clearly G-invariant, i.e. rational numbers. Moreover, as a_i are algebraic integers, n_1 and n_2 are in fact integers, readily recognised from their complex approximations as being 2 and -5.

Now suppose b_1 is a root of $f(x)$ in $\mathbb{F}_{2^5}$, and $b_i=b_{i-1}^2$ for $i=2,3,4,5$ are its other roots ordered by the action of the Frobenius automorphism. Then

$$N=b_1b_2+b_2b_3+b_3b_4+b_4b_5+b_5b_1$$

is in $\mathbb{F}_2$. By considering the reduction modulo a prime $\mathfrak{q}$ above 2 in the splitting field, we see that if $\mathrm{Frob}_{\mathfrak{q}}$ is (12345) or $(12345)^{-1}$, then $n_1\equiv N$ mod 2. Similarly, if $\mathrm{Frob}_{\mathfrak{q}}$ is $(12345)^2$ or $(12345)^3$, then $n_2\equiv N \mod 2$.

Computing in $\mathbb{F}_2^5$ (or noting that $N = \mathrm{Tr}_{\mathbb{F}_2[x]/f(x)}(x^3)$) we find that $N = 0$, so Frob_2 must be in $[(12345)]$.

In the language of Theorem 1.1, we took $h(x) = x$ and proved that

$$\Gamma_{[(12345)]} = (x-2)^2 \qquad \text{and} \qquad \Gamma_{[(12345)^2]} = (x+5)^2$$

distinguish between the two conjugacy classes of 5-cycles: if $f(x)$ is irreducible mod p (and $p \neq 7$, so that $2 \not\equiv -5$), then

$$\mathrm{Frob}_p \in C \quad \Leftrightarrow \quad \Gamma_C(\mathrm{Tr}_{\mathbb{F}_p[x]/f(x)}(x^{p+1})) = 0 \mod p.$$

This choice of $h(x)$ was in some sense deceptively simple, because the roots n_i of the Γ_C's were integers. (We used that the conjugacy classes of 5-cycles are self-inverse in D_{10}.) Generally, these roots would be algebraic integers of degree $|C|$. For example, $h(x) = x^2$ leads to

$$\Gamma_{[(12345)]} = x^2 + 5x + 18 \qquad \text{and} \qquad \Gamma_{[(12345)^2]} = x^2 - 11x + 42,$$

and $\mathrm{Tr}(x^{p+2})$ is a root of one of them whenever $f(x) \mod p$ is irreducible.

We end with a few words about the history of the problem of computing Frobenius elements. It is a classical theorem that their cycle types can be read off from the degrees of the factors of $f(x)$ mod p. Thus the problem has an elementary solution if the Galois group is the full symmetric group S_n or, generally, a permutation group whose conjugacy classes are determined by cycle type. Another classical example is the alternating group A_5, which has two conjugacy classes of 5-cycles. A solution in this case was pointed out by Serre (see Buhler [3] p. 53), and generalised by Roberts [5] to all alternating groups. (This goes under the name 'Serre's trick' and was used for instance by Booker [1] in his work on L-series for icosahedral representations.)

Notation. Throughout the paper we use the following notation:

K	ground field
$f(x)$	separable polynomial in $K[x]$ of degree n
L	some extension of K where f splits completely
$\boldsymbol{a} = [a_1, ..., a_n]$	ordered roots of f in L
$K(\boldsymbol{a})$	field generated by the a_i over K (a splitting field of f)
$G_{\boldsymbol{a}}$	Galois group of f, considered as a subgroup of S_n via its permutation action on $[a_1, ..., a_n]$.
$\mathfrak{p}$	prime of K, when K is a global field
$\mathbb{F}_q$	residue field at $\mathfrak{p}$
$\mathrm{Frob}_{\mathfrak{p}}$	any (arithmetic) Frobenius element at $\mathfrak{p}$ in $G_{\boldsymbol{a}}$
$e^F_{\boldsymbol{a}}, \Gamma, M^F_{\boldsymbol{a},\Psi}$	see Definitions 2.2, 2.7, 3.4 and 4.3.

Recall that a global field is a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_p(T)$. The Frobenius element in $\mathrm{Gal}(L/K)$ at $\mathfrak{p}$ is characterised by $\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^q \mod \mathfrak{q}$ for all $x \in L$ that are integral at some fixed prime $\mathfrak{q}$ of L above $\mathfrak{p}$. The element $\mathrm{Frob}_{\mathfrak{p}}$ is well-defined modulo inertia and up to conjugation. In particular, its conjugacy class is well-defined if $\mathfrak{p}$ is unramified in L/K.

The symmetric group S_n acts on n-tuples by

$$[c_1,...,c_n]^\sigma = [c_{\sigma^{-1}(1)},...,c_{\sigma^{-1}(n)}].$$

It acts on the ring of polynomials in n variables $K[x_1,...,x_n]$ by $\sigma(x_i)=x_{\sigma(i)}$; thus, for a polynomial $F\in K[x_1,...,x_n]$,

$$F^\sigma([c_1,...,c_n]) = F([c_1,...,c_n]^{\sigma^{-1}}),$$

where $F([...])$ is the evaluation of F on the n-tuple.

Acknowledgements. The first author is supported by a Royal Society University Research Fellowship. The second author would like to thank Gonville & Caius College, Cambridge, where part of this research was carried out.

2. Isomorphisms of splitting fields

In this section we introduce our main tools. The reader who is only interested in applications to Frobenius elements may skip to §5 and prove Theorem 5.3 directly (at the expense of not seeing the origins of Γ_C).

As a motivation, consider the following general question:

Problem 2.1. *Suppose we are given a separable polynomial $f(x)\in K[x]$ of degree n which splits completely in $L\supset K$ and $L'\supset K$. Given the roots $a_1,...,a_n$ and $b_1,...,b_n$ of f in L and L', find a bijection between them that comes from an isomorphism of splitting fields of f inside L and L'.*

We assume that we know the Galois group of f over K as a permutation group on the roots in L, but we do not want to construct the splitting fields explicitly. Instead, we will evaluate polynomials in $K[x_1,...,x_n]$ on the roots in L and L' taken in various orders and try to extract information out of the values (as in Example 1.2).

Definition 2.2. For $F\in K[x_1,...,x_n]$ define the *evaluation map* $\mathrm{S}_n\to K(\boldsymbol{a})$ by

$$e^F_{\boldsymbol{a}}(\sigma) = F([a_1,...,a_n]^\sigma).$$

Definition 2.3. For a subgroup T of S_n a *T-invariant F* is an element of $K[x_1,...,x_n]$ whose stabiliser is precisely T.

Remark 2.4. Any $F\in K[x_1,...,x_n]$ is evidently T-invariant if we take for T its stabiliser in S_n. Also, any subgroup $T<\mathrm{S}_n$ has a T-invariant, e.g.

$$F=\sum_{t\in T} m^t, \qquad m = x_1^{n-1}x_2^{n-2}\cdots x_{n-1},$$

since clearly the stabiliser of m in S_n is $\{1\}$.

Lemma 2.5. *Let F be a T-invariant and $\sigma,\tau\in\mathrm{S}_n$.*

1. $e^F_{\boldsymbol{a}^\tau}(\sigma) = e^F_{\boldsymbol{a}}(\sigma\tau)$.
2. $g(e^F_{\boldsymbol{a}}(\sigma)) = e^F_{\boldsymbol{a}}(\sigma g^{-1})$ *for* $g\in G_{\boldsymbol{a}}$.
3. *The map* $e^F_{\boldsymbol{a}}:\mathrm{S}_n\to K(\boldsymbol{a})$ *is constant on the right cosets* $T\sigma$.

Proof. (1) $e^F_{\boldsymbol{a}^\tau}(\sigma) = F((\boldsymbol{a}^\tau)^\sigma) = F(\boldsymbol{a}^{\sigma\tau}) = e^F_{\boldsymbol{a}}(\sigma\tau)$.
(2) For $g \in G_{\boldsymbol{a}}$,

$$\begin{aligned} g(e^F_{\boldsymbol{a}}(\sigma)) &= g(F([a_1,...,a_n]^\sigma)) &&= F([g(a_1),...,g(a_n)]^\sigma) \\ &= F(([a_1,...,a_n]^{g^{-1}})^\sigma) &&= F([a_1,...,a_n]^{\sigma g^{-1}}) \quad = \quad e^F_{\boldsymbol{a}}(\sigma g^{-1}). \end{aligned}$$

(3) For $\tau \in T$,

$$\begin{aligned} e^F_{\boldsymbol{a}}(\tau\sigma) &= F([a_1,...,a_n]^{\tau\sigma}) &&= F(([a_1,...,a_n]^\sigma)^\tau) \\ &= F^{\tau^{-1}}([a_1,...,a_n]^\sigma) &&= F([a_1,...,a_n]^\sigma) \quad = \quad e^F_{\boldsymbol{a}}(\sigma). \end{aligned}$$

□

Remark 2.6. Part (3) of the lemma says that the values of F on the various permutations $\boldsymbol{a}^\sigma$ of the roots are essentially the right cosets of T in S_n. It may accidentally happen that the same value occurs on two right cosets, but it is always possible to adjust the original polynomial f to prevent this (see Lemma 8.1c). Part (2) of Lemma 2.5 says that the action of the Galois group $\mathrm{Gal}(K(\boldsymbol{a})/K)$ on these values translates into right multiplication by $G_{\boldsymbol{a}}$. This motivates the following

Definition 2.7. For a double coset $D = T\sigma_0 G_{\boldsymbol{a}}$ in S_n, define the corresponding 'minimal polynomial'

$$\Gamma^F_{\boldsymbol{a},\sigma_0} = \Gamma^F_{\boldsymbol{a},D}(X) = \prod_{\sigma \in T\backslash D} (X - e^F_{\boldsymbol{a}}(\sigma)) \in K[X].$$

By Lemma 2.5 (3), this is well-defined.

Remark 2.8. Note that by Lemma 2.5 (2), $G_{\boldsymbol{a}}$ permutes the linear factors of $\Gamma^F_{\boldsymbol{a},D}$ transitively, so it is a power of an irreducible polynomial in $K[X]$. If $e^F_{\boldsymbol{a}} : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective, then $\Gamma^F_{\boldsymbol{a},D}(X)$ is irreducible, and hence the minimal polynomial of $e^F_{\boldsymbol{a}}(\sigma_0)$.

Remark 2.9. The point is that the $\Gamma^F_{\boldsymbol{a},D}(X)$ are K-rational objects, and they can be used to compare different splitting fields:

Proposition 2.10. *Let $\boldsymbol{a}, \boldsymbol{b}$ be orderings of roots of f in two splitting fields of f, and let $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$ be an isomorphism. If $e^F_{\boldsymbol{a}} : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective, then for every double coset $D \in T\backslash \mathrm{S}_n / G_{\boldsymbol{a}}$,*

$$\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0 \quad \Leftrightarrow \quad \boldsymbol{b} = [\phi(a_1),...,\phi(a_n)]^\sigma \textit{ for some } \sigma \in D.$$

Proof. We have that $\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0$ if and only if $F(\boldsymbol{b}) = \phi(x)$ for some root x of $\Gamma^F_{\boldsymbol{a},D}$ in $K(\boldsymbol{a})$. Such roots are $e^F_{\boldsymbol{a}}(\sigma)$ for some $\sigma \in D$, so

$$\begin{aligned} \Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0 \quad &\Leftrightarrow \quad F(\boldsymbol{b}) = \phi(e^F_{\boldsymbol{a}}(\sigma)) && \text{for some } \sigma \in D \\ &\Leftrightarrow \quad F(\phi^{-1}(\boldsymbol{b})) = e^F_{\boldsymbol{a}}(\sigma) = F(\boldsymbol{a}^\sigma) && \\ &\Leftrightarrow \quad \phi^{-1}(\boldsymbol{b}) = (\boldsymbol{a}^\sigma)^\tau = \boldsymbol{a}^{\tau\sigma} && \text{for some } \tau \in T \\ &\Leftrightarrow \quad \boldsymbol{b} = \phi(\boldsymbol{a}^{\sigma'}) = \phi(\boldsymbol{a})^{\sigma'} && \text{for some } \sigma' \in D. \end{aligned}$$

□

Theorem 2.11. *Let F be a $G_{\boldsymbol{a}}$-invariant with $e^F_{\boldsymbol{a}}$: $G_{\boldsymbol{a}} \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ injective. If $F(\boldsymbol{b}) = F(\boldsymbol{a}) \in K$, then $a_i \mapsto b_i$ defines an isomorphism $K(\boldsymbol{a}) \to K(\boldsymbol{b})$.*

Proof. Take $T = G_{\boldsymbol{a}}$ and D the principal double coset $G_{\boldsymbol{a}} 1 G_{\boldsymbol{a}}$, and apply the proposition. Since $\Gamma^F_{\boldsymbol{a},D}(X) = X - F(\boldsymbol{a})$, we have $\Gamma^F_{\boldsymbol{a},D}(F(\boldsymbol{b})) = 0$, so $\boldsymbol{b} = \phi(\boldsymbol{a})^\sigma$ for some $\sigma \in G_{\boldsymbol{a}}$ and some isomorphism $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$. Then $\phi \circ \sigma$ is the required isomorphism. □

Remark 2.12. This gives a solution to Problem 2.1:

Pick a $G_{\boldsymbol{a}}$-invariant F, e.g. using Remark 2.4. Adjusting f if necessary, we may assume that $e^F_{\boldsymbol{a}} : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective (Lemma 8.1c). In L', keep permuting the roots of f until $F(\boldsymbol{b})$ becomes $F(\boldsymbol{a}) \in K$. When this happens, $a_i \mapsto b_i$ defines an isomorphism of the two splitting fields.

Note however, that in the worst case we are evaluating a polynomial with $|G|$ terms on $|G \backslash \mathrm{S}_n / G|$ permutations. So the complexity is about $n!$ operations, which is impractical for large n.

Example 2.13 (D_{10}-extensions)**.** Suppose $f(x) \in K[x]$ has degree 5, and $G_{\boldsymbol{a}} = \mathrm{Gal}(f/K)$ is the dihedral group D_{10}, generated by (12345) and (25)(34). Take

$$F(x_1, ..., x_5) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1.$$

This is a T-invariant with $T = G_{\boldsymbol{a}}$: it is clearly invariant under D_{10}, and on the other hand a permutation preserving F is determined by $x_1 \mapsto x_i$, $x_2 \mapsto x_{i\pm 1}$, so there are at most 10 choices. In particular, $F(a_1, ..., a_5)$ is invariant under the Galois group, and so lies in K. Substituting the a_i into F in all possible orders gives the values

$$e^F_{\boldsymbol{a}}(\sigma^{-1}) = a_{\sigma(1)}a_{\sigma(2)} + a_{\sigma(2)}a_{\sigma(3)} + a_{\sigma(3)}a_{\sigma(4)} + a_{\sigma(4)}a_{\sigma(5)} + a_{\sigma(5)}a_{\sigma(1)}.$$

Clearly each one occurs at least 10 times for varying $\sigma \in \mathrm{S}_5$, corresponding to the fact that $e^F_{\boldsymbol{a}}$ factors through $\mathrm{D}_{10} \backslash \mathrm{S}_5$. The assumption that the map $e^F_{\boldsymbol{a}} : T \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective simply says that there are no more repetitions, and there are $120/10 = 12$ distinct values.

Suppose that this is indeed the case, and let $b_1, ..., b_5$ be the roots of f in some other splitting field. If we substitute the b_i in F in all possible orders $\boldsymbol{b}^\sigma$, we get again 12 values, one of which is $F(a_1, ..., a_5) \in K$. There are 10 isomorphisms $K(\boldsymbol{a}) \to K(\boldsymbol{b})$ obtained from one another by composing with Galois. They are determined by $\boldsymbol{a} \mapsto \boldsymbol{b}^\sigma$ for 10 permutations $\sigma \in \mathrm{S}_n$. Clearly, for each of these σ, we have $F(\boldsymbol{b}^\sigma) = F(\boldsymbol{a})$. But, since every value is taken exactly 10 times, we have the converse as well: if $F(\boldsymbol{b}^\sigma) = F(\boldsymbol{a})$ for some $\sigma \in \mathrm{S}_n$, then $\boldsymbol{a} \mapsto \boldsymbol{b}^\sigma$ must define an isomorphism of the splitting fields. So to find an isomorphism, we only need to locate $F(\boldsymbol{a})$ among the 12 values $F(\boldsymbol{b}^\sigma)$.

Note that the other values $F(\boldsymbol{b}^\sigma)$ are not in general K-rational, so we cannot compare them with the values on $\boldsymbol{a}$. Their minimal polynomials are the $\Gamma^F_{\boldsymbol{a},D}(X)$ for the 4 double cosets $\mathrm{D}_{10} \backslash \mathrm{S}_5 / \mathrm{D}_{10}$.

3. Recognising conjugacy in Galois groups

In questions such as computing Frobenius elements in Galois groups it is not necessary to compare the roots in two splitting fields. It suffices to identify the conjugacy class of a specific Galois automorphism:

Problem 3.1. *Let $f(x) \in K[x]$ be a separable polynomial which splits completely in $L \supset K$, and suppose we know $G = \mathrm{Gal}(f/K)$ as a permutation group on the roots in L. If L' is another field where f splits completely and we are given a permutation of the roots of f in L' which comes from some Galois automorphism, find the conjugacy class of this automorphism in G.*

Remark 3.2. An isomorphism ϕ of the two splitting fields of f induces an isomorphism of Galois groups G and G'. We would like to identify an element $\mathcal{B} \in G'$ as an element $\mathcal{A} \in G$. Note that $\mathcal{A}$ depends on the choice of ϕ. As any two isomorphisms differ by a Galois automorphism, the conjugacy class $[\mathcal{A}]$ is well-defined and this is what we are after.

It is easy to see that a solution to Problem 2.1 answers Problem 3.1 as well, so this is a weaker question. However, we aim for a more practical solution (see Remark 2.12). We may clearly restrict our attention to one cycle type in S_n. For convenience, throughout the section we we also fix a representative:

Notation 3.3. Fix an element $\xi \in \mathrm{S}_n$ and write $Z_\xi < \mathrm{S}_n$ for its centraliser.

Definition 3.4. Suppose $\Psi \in \mathrm{S}_n$ is conjugate to ξ, in other words they have the same cycle type, say $\xi = \sigma_0 \Psi \sigma_0^{-1}$. For a T-invariant F and an ordering $\boldsymbol{a}$ of the roots of f, define the polynomial

$$M^F_{\boldsymbol{a},\Psi}(X) = \prod_{\sigma \in (Z_\xi \cap T)\backslash Z_\xi \sigma_0} \Gamma^F_{\boldsymbol{a},\sigma}(X).$$

It is well-defined by Lemma 2.5(3). Note that $Z_\xi \sigma_0$ is the set of all permutations that conjugate Ψ to ξ, in particular it is independent of the choice of σ_0.

Remark 3.5. The situation we have in mind is that we have two sets of roots $\boldsymbol{a}$ and $\boldsymbol{b}$ of f in different splitting fields. So there is an isomorphism $\phi\colon K(\boldsymbol{a}) \to K(\boldsymbol{b})$, but we do not have it explicitly. However, suppose we know that an automorphism $\mathcal{A} \in \mathrm{Gal}(K(\boldsymbol{a})/K)$ corresponds to $\mathcal{B} \in \mathrm{Gal}(K(\boldsymbol{b})/K)$ under ϕ, and that they permute the roots by

$$\mathcal{A}(\boldsymbol{a}) = \boldsymbol{a}^\Psi, \quad \mathcal{B}(\boldsymbol{b}) = \boldsymbol{b}^\xi, \qquad \Psi, \xi \in \mathrm{S}_n.$$

Then $\{\boldsymbol{a}^\sigma\}_{\sigma \in Z_\xi \sigma_0}$ is the set of all reorderings of $\boldsymbol{a}$ on which $\mathcal{A}$ acts as ξ, and $M^F_{\boldsymbol{a},\Psi}(X)$ is the smallest K-rational polynomial that has $F(\boldsymbol{a}^\sigma)$ as roots for all such σ. But $\phi^{-1}(\boldsymbol{b})$ must be one of these reorderings because $\mathcal{B}$ acts on $\boldsymbol{b}$ as ξ. The upshot is that $M^F_{\boldsymbol{a},\Psi}(X)$ has $F(\boldsymbol{b})$ as a root, and its construction does not require the knowledge of ϕ. In other words, if $M^F_{\boldsymbol{a},\Psi}(F(\boldsymbol{b})) \neq 0$, then we know that $\mathcal{A}$ does not correspond to $\mathcal{B}$ under any isomorphism. (In §4 we will take $T = Z_\xi$ and turn this into an if and only if statement.)

Lemma 3.6. *Let $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$ be an isomorphism of two splitting fields of f, and define $\rho \in \mathrm{S}_n$ by $\boldsymbol{b} = \phi(\boldsymbol{a}^\rho)$. Then*

$$M^F_{\boldsymbol{a},\rho^{-1}\Phi\rho} = M^F_{\boldsymbol{b},\Phi}.$$

Proof. Write $\Psi = \rho^{-1}\Phi\rho$. Pick σ_Φ with $\xi = \sigma_\Phi\Phi\sigma_\Phi^{-1}$, and let $\sigma_\Psi = \sigma_\Phi\rho$, so that

$$\sigma_\Psi\Psi\sigma_\Psi^{-1} = \sigma_\Phi\rho\Psi\rho^{-1}\sigma_\Phi^{-1} = \sigma_\Phi\Phi\sigma_\Phi^{-1} = \xi.$$

By definition,

$$M^F_{\boldsymbol{b},\Phi} = \prod_{\sigma\in(Z_\xi\cap T)\backslash Z_\xi\sigma_\Phi} \Gamma^F_{\boldsymbol{b},\sigma}, \qquad M^F_{\boldsymbol{a},\Psi} = \prod_{\sigma\in(Z_\xi\cap T)\backslash Z_\xi\sigma_\Psi} \Gamma^F_{\boldsymbol{a},\sigma}.$$

We claim that

$$\Gamma^F_{\boldsymbol{a},s\sigma_\Psi} = \Gamma^F_{\boldsymbol{b},s\sigma_\Phi} \qquad \text{for } s \in Z_\xi.$$

First we show that they have the same degree. Because $G_{\boldsymbol{b}} = \rho G_{\boldsymbol{a}}\rho^{-1}$ by the definition of ρ,

$$\begin{aligned}\deg \Gamma^F_{\boldsymbol{a},s\sigma_\Psi} &= |T\backslash Ts\sigma_\Psi G_{\boldsymbol{a}}| = |T\backslash Ts\sigma_\Psi G_{\boldsymbol{a}}\rho^{-1}| \\ &= |T\backslash Ts\sigma_\Phi\rho G_{\boldsymbol{a}}\rho^{-1}| = |T\backslash Ts\sigma_\Phi G_{\boldsymbol{b}}| = \deg \Gamma^F_{\boldsymbol{b},s\sigma_\Phi}.\end{aligned}$$

Since both polynomials are powers of irreducible ones, it now suffices to identify one of the roots:

$$\begin{aligned}e^F_{\boldsymbol{a}}(s\sigma_\Psi) &= e^F_{\boldsymbol{a}}(s\sigma_\Phi\rho) = F(\boldsymbol{a}^{s\sigma_\Phi\rho})) = F(\phi^{-1}(\boldsymbol{b})^{s\sigma_\Phi})) \\ &= F(\phi^{-1}(\boldsymbol{b}^{s\sigma_\Phi})) = \phi^{-1}(F(\boldsymbol{b}^{s\sigma_\Phi})) = \phi^{-1}(e^F_{\boldsymbol{b}}(s\sigma_\Phi)).\end{aligned}$$

□

Corollary 3.7. *The map $\Psi \mapsto M^F_{\boldsymbol{a},\Psi}$ is constant on every conjugacy class of $G_{\boldsymbol{a}}$ with cycle type ξ.*

Proof. By the lemma above, $M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},g\Psi g^{-1}}$ for $g \in G_{\boldsymbol{a}}$. □

We now have an approach to Problem 3.1:

Proposition 3.8. *Let $\boldsymbol{a}, \boldsymbol{b}$ be orderings of the roots of f in two different splitting fields, and suppose $\Psi \in G_{\boldsymbol{a}}$ and $\Phi \in G_{\boldsymbol{b}}$ have cycle type ξ. If the polynomials $M^F_{\boldsymbol{a},\psi}$ are distinct for ψ in different conjugacy classes of $G_{\boldsymbol{a}}$ of cycle type ξ, then*

$$\begin{array}{c}\textit{there is an isomorphism } K(\boldsymbol{a}) \to K(\boldsymbol{b}) \\ \textit{under which } \Psi \textit{ corresponds to } \Phi\end{array} \iff M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{b},\Phi}.$$

If, moreover, the $M^F_{\boldsymbol{a},\psi}$ are pairwise coprime, then this occurs precisely when $M^F_{\boldsymbol{a},\Psi}(F(\boldsymbol{b}^\sigma)) = 0$ for some (any) $\sigma \in \mathrm{S}_n$ with $\xi = \sigma\Phi\sigma^{-1}$.

Proof. '$\Rightarrow$' is Lemma 3.6. For '$\Leftarrow$', pick any isomorphism $\phi : K(\boldsymbol{a}) \to K(\boldsymbol{b})$. The polynomial $M^F_{\boldsymbol{b},\Phi}$ agrees with some $M^F_{\boldsymbol{a},\psi}$ by the lemma, and Ψ lies in the conjugacy class of ψ by assumption. Composing ϕ with an automorphism of $K(\boldsymbol{a})/K$ (which corresponds to conjugating ψ) we obtain the required isomorphism. □

Example 3.9 (Serre's trick [3, 5])**.** Suppose $\operatorname{char} K \neq 2$, $f \in K[x]$ has degree n, and $G_{\boldsymbol{a}} = \operatorname{Gal}(f/K)$ is the alternating group A_n. There is a particularly nice T-invariant with $T = \mathrm{A}_n$, a 'square root of the discriminant'

$$F(x_1, ..., x_n) = \prod_{i<j} (x_i - x_j).$$

The only double cosets $TxG_{\boldsymbol{a}}$ in S_n are $D = \mathrm{A}_n$ and its complement D' in S_n. Clearly $\Gamma^F_{\boldsymbol{a},D}(X) = X - F(\boldsymbol{a})$ and $\Gamma^F_{\boldsymbol{a},D'}(X) = X + F(\boldsymbol{a})$, and $F(\boldsymbol{a})^2 = \operatorname{Disc} f$ is the discriminant of f. So if $\boldsymbol{b}$ is the list of roots of f in some other splitting field, we find that

$$\begin{array}{c} a_i \mapsto b_i \text{ defines an} \\ \text{isomorphism } K(\boldsymbol{a}) \to K(\boldsymbol{b}) \end{array} \quad \Leftrightarrow \quad \prod_{i<j}(a_i - a_j) = \prod_{i<j}(b_i - b_j).$$

This illustrates Theorem 2.11 in the case of A_n. To explain Proposition 3.8 in this setting, suppose $\xi \in \mathrm{S}_n$ is a product of cycles of distinct odd degrees, so that there are two conjugacy classes $[\Psi_1], [\Psi_2]$ in $G_{\boldsymbol{a}} = \mathrm{A}_n$ of cycle type ξ (e.g. 5-cycles in A_5). Say $\sigma_1\Psi_1\sigma_1^{-1} = \xi = \sigma_2\Psi_2\sigma_2^{-1}$ with $\sigma_1 \in \mathrm{A}_n$ and $\sigma_2 \notin \mathrm{A}_n$. In this case $Z_\xi \subset \mathrm{A}_n = T$, so

$$\begin{aligned} M^F_{\boldsymbol{a},\Psi_1}(X) &= \Gamma^F_{\boldsymbol{a},\sigma_1}(X) = \Gamma^F_{\boldsymbol{a},D}\,(X) = X - F(\boldsymbol{a}), \\ M^F_{\boldsymbol{a},\Psi_2}(X) &= \Gamma^F_{\boldsymbol{a},\sigma_2}(X) = \Gamma^F_{\boldsymbol{a},D'}(X) = X + F(\boldsymbol{a}). \end{aligned}$$

Suppose again that $\boldsymbol{b}$ is the list of roots of f in some other splitting field, and $\mathcal{B} \in \operatorname{Gal}(K(\boldsymbol{b})/K)$ is an automorphism of cycle type ξ. Rearranging the b_i if necessary, assume that $\mathcal{B}$ acts on the b_i as ξ, i.e. $\mathcal{B}(\boldsymbol{b}) = \boldsymbol{b}^\xi$. The statement of the proposition is that

$$\begin{array}{c} \mathcal{B} \text{ comes from } [\Psi_1] \text{ under an} \\ \text{isomorphism } K(\boldsymbol{a}) \to K(\boldsymbol{b}) \end{array} \quad \Leftrightarrow \quad \prod_{i<j}(a_i - a_j) = \prod_{i<j}(b_i - b_j),$$

which is precisely Serre's trick. The same invariant F may sometimes be used in other subgroups of S_n to distinguish between the conjugacy classes of such cycle types. (It determines whether the two classes are conjugate in A_n or not.)

4. The directed edges invariant

As before, suppose $f(x) \in K[x]$ is separable and $\boldsymbol{a} = [a_1, ..., a_n]$ are its (ordered) roots in a splitting field. We apply the results of §3 when $T = Z_\xi$, the centraliser of ξ. This is particularly nice for two reasons: first, the polynomials $M^F_{\boldsymbol{a},\psi}$ of Proposition 3.8 are irreducible and distinct, and second, it is easy to write down a T-invariant with just n terms and of degree 3 (compare the polynomials in Remark 2.4 and Example 4.2).

Proposition 4.1. *Let $\xi \in \mathrm{S}_n$ with centraliser Z_ξ. Suppose that F is a Z_ξ-invariant such that $e^F_{\boldsymbol{a}} : Z_\xi \setminus \mathrm{S}_n \to K(\boldsymbol{a})$ is injective. Let $\Psi, \Psi' \in G_{\boldsymbol{a}}$ be two elements of cycle type ξ. Then*

1. *$M^F_{\boldsymbol{a},\Psi}$ is irreducible, and equals $\Gamma^F_{\boldsymbol{a},\sigma}$ for any $\sigma \in \mathrm{S}_n$ with $\xi = \sigma\Psi\sigma^{-1}$.*
2. *$M^F_{\boldsymbol{a},\Psi}$ has degree $|[\Psi]|$.*
3. *$M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},\Psi'}$ if and only if Ψ and Ψ' are conjugate in $G_{\boldsymbol{a}}$.*

Proof. For brevity, write $Z = Z_\xi$. Pick $\sigma, \sigma' \in \mathrm{S}_n$ with $\sigma\Psi\sigma^{-1} = \xi = \sigma'\Psi(\sigma')^{-1}$.
(1) By definition,

$$M^F_{\boldsymbol{a},\Psi} \;=\; \prod_{\tau \in (Z\cap Z)\backslash Z\sigma} \Gamma^F_{\boldsymbol{a},\tau} \;=\; \Gamma^F_{\boldsymbol{a},\sigma}.$$

It is irreducible by the assumed injectivity of $e^F_{\boldsymbol{a}}$ (see Remark 2.8).
(2) By definition,

$$\begin{aligned} \deg \Gamma^F_{\boldsymbol{a},\sigma} &= |Z\backslash Z\sigma G_{\boldsymbol{a}}| = \frac{|Z\sigma G_{\boldsymbol{a}}|}{|Z|} = \frac{|\sigma^{-1} Z\sigma G_{\boldsymbol{a}}|}{|Z|} \\ &= \frac{|G_{\boldsymbol{a}}|}{|G_{\boldsymbol{a}} \cap \sigma^{-1} Z\sigma|} = \frac{|G_{\boldsymbol{a}}|}{|\operatorname{Cent}_{G_{\boldsymbol{a}}}(\Psi)|} = |[\Psi]|. \end{aligned}$$

(3) If Ψ and Ψ' are conjugate, then $M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},\Psi'}$ by Corollary 3.7. Conversely, suppose that $M^F_{\boldsymbol{a},\Psi} = M^F_{\boldsymbol{a},\Psi'}$. Since $e^F_{\boldsymbol{a}}$ is injective, $Z\sigma G_{\boldsymbol{a}} = Z\sigma' G_{\boldsymbol{a}}$, so $\sigma' = s\sigma g$ for some $s \in Z$ and $g \in G_{\boldsymbol{a}}$. Then

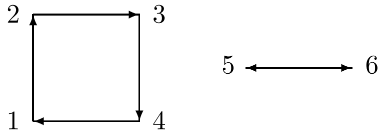
$$\Psi' = (\sigma')^{-1}\xi\sigma' = g^{-1}\sigma^{-1}s^{-1}\xi s\sigma g = g^{-1}\sigma^{-1}\xi\sigma g = g^{-1}\Psi g,$$

so $[\Psi'] = [\Psi]$. □

Example 4.2 (The directed edges invariant)**.** Let $\xi \in \mathrm{S}_n$ and fix a polynomial $h \in K[x]$ of degree at least 2. Define

$$F(x_1, ..., x_n) = \sum_{j=1}^{n} h(x_j)\, x_{\xi(j)}.$$

It can be visualised as the directed edges in a graph that define the action by ξ. For instance, for $\xi = (1234)(56) \in \mathrm{S}_6$ and $h(x) = x^2$,



$$F \;=\; x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_1 \;+\; x_5^2x_6 + x_6^2x_5$$

It is clearly a Z_ξ-invariant.

Definition 4.3. Fix $h(x) \in K[x]$. For each conjugacy class C in $G_{\boldsymbol{a}}$ define

$$\Gamma_C(X) = \prod_{\sigma \in C} (X - \sum_{j=1}^{n} h(a_j)\sigma(a_j)).$$

Lemma 4.4. *Let F be as in Example 4.2. Then for every $\Psi \in G_{\boldsymbol{a}}$,*

$$M^F_{\boldsymbol{a},\Psi}(X) = \Gamma_{[\Psi]}(X).$$

Proof. Pick $\sigma \in \mathrm{S}_n$ with $\sigma\Psi\sigma^{-1} = \xi$. First, suppose $\tau \in [\Psi]$ and $u_\tau \in \mathrm{S}_n$ satisfies $u_\tau^{-1}\xi u_\tau = \tau$. Then

$$\begin{aligned} e^F_{\boldsymbol{a}}(u_\tau) &= F(\boldsymbol{a}^{u_\tau}) = \sum_i h(a_{u_\tau^{-1}(i)})a_{u_\tau^{-1}(\xi(i))} \\ &= \sum_j h(a_j)a_{u_\tau^{-1}\xi u_\tau(j)} = \sum_j h(a_j)\tau(a_j). \end{aligned}$$

On the other hand, note that for $t \in Z_\xi$ and $g \in G_{\boldsymbol{a}}$,

$$(t\sigma g)^{-1}\xi(t\sigma g) = g^{-1}\sigma^{-1}t^{-1}\xi t\sigma g = g^{-1}\sigma^{-1}\xi\sigma g = g^{-1}\Psi g.$$

So for $\tau = g^{-1}\Psi g \in [\Psi]$,

$$\{u_\tau \in S_n \mid u_\tau^{-1}\xi u_\tau = \tau\} = Z_\xi\sigma g,$$

because the left-hand side is clearly some right coset of Z_ξ. This equality gives a correspondence between $[\Psi]$ and $Z_\xi\backslash Z_\xi\sigma G_{\boldsymbol{a}}$. So

$$\begin{aligned} M^F_{\boldsymbol{a},\Psi}(X) &= \Gamma^F_{\boldsymbol{a},\sigma}(X) = \prod_{u \in (Z_\xi\backslash Z_\xi\sigma G_{\boldsymbol{a}})} (X - e^F_{\boldsymbol{a}}(u)) \\ &= \prod_{\tau \in [\Psi]} (X - \sum_{j=1}^{n} h(a)\tau(a_j)) = \Gamma_{[\Psi]}(X), \end{aligned}$$

as claimed. □

Corollary 4.5. *Let $\boldsymbol{a}, \boldsymbol{b}$ be orderings of the roots of f in two different splitting fields, and let $\Psi \in G_{\boldsymbol{a}}$ and $\Phi \in G_{\boldsymbol{b}}$. If the $\Gamma_C(X)$ are pairwise coprime for different conjugacy classes of $G_{\boldsymbol{a}}$, then*

$$\begin{array}{c}\textit{there is an isomorphism } K(\boldsymbol{a}) \to K(\boldsymbol{b}) \\ \textit{under which } \Psi \textit{ corresponds to } \Phi,\end{array} \iff \Gamma_{[\Psi]}\Big(\textstyle\sum_j h(b_j)\Phi(b_j)\Big) = 0.$$

The condition that the Γ_C are coprime is satisfied for $h(x)$ in a Zariski dense open set in the space of all polynomials of degree at most $n-1$.

Proof. The equivalence follows from Proposition 3.8 and the lemma above. For the last assertion apply Lemma 8.2. □

5. Frobenius elements

Now suppose K is a global field. We turn to our initial problem of computing Frobenius elements in Galois groups. We use the following remarkable property of the directed edges invariant:

Proposition 5.1. *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial with roots $a_1, ..., a_n \in \bar{\mathbb{F}}_q$ counted with multiplicity, and let $\phi = \mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. For every polynomial $h(x) \in \mathbb{F}_q[x]$,*

$$\sum_{j=1}^{n} h(a_j)\phi(a_j) = \mathrm{Tr}_{A/\mathbb{F}_q}(h(X)X^q),$$

where X is the class of x in the algebra $A = \mathbb{F}_q[x]/f$.

This is an immediate consequence of the lemma below (with $H(x) = h(x)x^q$).

Lemma 5.2. *Let k be a field and $f(x) \in k[x]$ a polynomial with roots $a_1, ..., a_n \in \bar{k}$ counted with multiplicity. Then for every $H(x) \in k[x]$,*

$$\sum_{j=1}^{n} H(a_j) = \mathrm{Tr}_{A/k}(H(X)),$$

where X is the class of x in $A = k[x]/f$.

Proof. Consider X as a linear map $A \to A$, $Y \mapsto XY$. Its minimal polynomial is f, since $f(X) = 0$ but no linear combination of $1, X, ..., X^{n-1}$ is zero. So the generalised eigenvalues of X are exactly the a_i, and those of $H(X)$ are therefore $H(a_i)$ (look at the Jordan normal form of X over $\bar{k}$). The result follows. □

Theorem 5.3 (Generalised Euler's criterion)**.** *Let K be a global field and $f(x) \in K[x]$ a separable polynomial with roots $a_1, ..., a_n$ in $\bar{K}$ and Galois group G. Fix $h(x) \in K[x]$ and for each conjugacy class C of G set*

$$\Gamma_C(X) = \prod_{\sigma \in C} (X - \sum_{j=1}^{n} h(a_j)\sigma(a_j)).$$

(a) *The polynomials $\Gamma_C(X)$ have coefficients in K.*

(b) *Let $\mathfrak{p}$ be a prime of K with residue field $\mathbb{F}_q$, and C a conjugacy class of G. If $\mathfrak{p}$ does not divide the denominators of the coefficients of f and h, the leading coefficient of f and the resultants $\mathrm{Res}(\Gamma_C, \Gamma_{C'})$ for $C' \neq C$, then the coefficients of $\Gamma_C(X)$ are integral at $\mathfrak{p}$ and*

$$\mathrm{Frob}_{\mathfrak{p}} \in C \quad \Leftrightarrow \quad \Gamma_C\Big(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q)\Big) = 0 \mod \mathfrak{p}.$$

(c) *For all $h(x)$ in some Zariski dense open set in the space of polynomials of degree at most $n-1$, we have $\mathrm{Res}(\Gamma_C, \Gamma_{C'}) \neq 0$ for every pair of conjugacy classes $C \neq C'$.*

Proof. (a) This follows from Lemma 4.4, Definition 3.4 and Remark 2.8.

(b) $\Gamma_C(X)$ is clearly integral at the required primes.

'$\Rightarrow$': if $\mathrm{Frob}_{\mathfrak{p}} \in C$ then $\sum_{j=1}^{n} h(a_j)\,\mathrm{Frob}_{\mathfrak{p}}(a_j)$ is a root of $\Gamma_C(X)$ by the definition of Γ_C, and it reduces mod $\mathfrak{p}$ to $\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q)$ by Proposition 5.1.

'$\Leftarrow$': the polynomial $\Gamma_C(X)$ is distinguished from the others by any one of its root mod $\mathfrak{p}$ by the assumption that $\mathfrak{p} \nmid \mathrm{Res}(\Gamma_C, \Gamma_{C'})$ for $C \neq C'$.

(c) Apply Lemma 8.2. □

Remark 5.4 (Choice of h)**.** If the resultants $\mathrm{Res}(\Gamma_C, \Gamma_{C'})$ are non-zero, Theorem 5.3b describes the Frobenius element for all but finitely many primes $\mathfrak{p}$. If one of the resultants vanishes, equivalently Γ_C has a common factor with some $\Gamma_{C'}$, the statement does not apply to C for any $\mathfrak{p}$. However, this is rare and easily avoided by choosing a different h; most choices will work by Theorem 5.3c.

Alternatively, for any fixed h with $1 < \deg h < n$ it is possible to replace f by another polynomial $\tilde{f}$ of degree n with the same splitting field so that the resulting Γ_C are coprime. To see this, consider

$$\gamma_C(X) = \prod_{\sigma \in C} (X - \sum_{j=1}^{n} h(x_j) x_{\sigma(j)}),$$

and note that they are coprime as polynomials in X over $K(x_1, ..., x_n)$. Now apply Lemma 8.1b to $F_1 = \prod_{C \neq C'} \mathrm{Res}(\gamma_C, \gamma_{C'})$ and $F_2 = 0$. We obtain a Zariski dense open set of polynomials $B(t)$ of degree at most $n-1$ for which $\tilde{f} = \prod_j (x - B(a_j))$ works.

Remark 5.5 (Euler's criterion)**.** The classical criterion $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \mod p$ says that $a^{\frac{p-1}{2}} = \pm 1$ determines whether $x^2 - a$ has a root modulo p. Similarly, to see whether $x^3 - a$ has a root modulo $p \equiv 1 \mod 3$ one checks whether $a^{\frac{p-1}{3}}$ is 1 or another third root of unity in $\mathbb{F}_p^\times$, etc.

One can reformulate this as a matrix statement: take a 2×2 matrix M with minimal polynomial $x^2 - a$ (respectively 3×3 and $x^3 - a$). Then M^{p-1} is the scalar matrix with $a^{\frac{p-1}{2}}$ (respectively $a^{\frac{p-1}{3}}$) on the diagonal, so its trace determines whether the polynomial has a root in $\mathbb{F}_p$; e.g. for $x^3 - a$ the distinction is whether $\frac{1}{3}\,\mathrm{Tr}\, M^{p-1}$ is 1 or a root of $x^2 + x + 1$.

Theorem 5.3 generalises this to arbitrary polynomials over global fields. Observe that for a polynomial

$$f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0$$

the trace in the theorem can be interpreted as a trace of a matrix, e.g.

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^d) = \mathrm{Tr} \begin{pmatrix} & & & -c_0 \\ 1 & & & -c_1 \\ & \ddots & & \vdots \\ & & 1 & -c_{n-1} \end{pmatrix}^d \mod q.$$

Therefore (a minor modification of) the trace $\mathrm{Tr}\, M^{q-1}$ for a matrix M with minimal polynomial f determines the splitting behaviour of f mod $\mathfrak{p}$ and the conjugacy class of Frobenius, in the same way as above. See also examples in §7.

Remark 5.6 (Ramified primes)**.** The condition that $\mathfrak{p}$ does not divide any resultant $\mathrm{Res}(\Gamma_C, \Gamma_{C'})$ excludes all primes that ramify in the splitting field of f over K. Indeed, if $\sigma \neq 1$ is an element of inertia at $\mathfrak{q}$ for some $\mathfrak{q}|\mathfrak{p}$, it is easy to see that $\Gamma_{[1]}$ and $\Gamma_{[\sigma]}$ have a common root mod $\mathfrak{p}$.

Remark 5.7 (Extending to all $\mathfrak{p}$)**.** In order to deal with the primes dividing the resultants, we may work over the completion $K_\mathfrak{p}$ instead of the residue field $\mathbb{F}_q$. Compute the splitting field $L/K_\mathfrak{p}$ of f and the roots $b_1, .., b_n$. Choose a lift Ψ of the Frobenius element in $\mathrm{Gal}(L/K_\mathfrak{p})$ and evaluate

$$\sum_{j=1}^{n} h(b_j)\Psi(b_j).$$

This number is now a root of precisely one of the Γ_C, and this C is the conjugacy class of the chosen Frobenius lift Ψ. (See Corollary 4.5.)

Remark 5.8 (Artin L-functions)**.** Suppose L/K is a Galois extension of number fields with Galois group G, represented as a splitting field of some polynomial $f(x) \in K[x]$. Recall that a complex representation ρ of G is called an *Artin representation*. It has an L-series defined by the Euler product over all primes of K,

$$L(\rho, s) = \prod_{\mathfrak{p}} \frac{1}{P_\mathfrak{p}(q^{-s})}.$$

Here q is the size of the residue field at $\mathfrak{p}$ and

$$P_\mathfrak{p}(T) = \det(1 - \mathrm{Frob}_\mathfrak{p} T \mid \rho^{I_\mathfrak{p}})$$

is the inverse characteristic polynomial of Frobenius on the subspace of ρ fixed by the inertia group $I_\mathfrak{p}$ at $\mathfrak{p}$.

Theorem 5.3 and Remark 5.7 allow us to explicitly compute the coefficients of such L-series. For the unramified primes, they recover the conjugacy class of $\mathrm{Frob}_\mathfrak{p}$ in G, which determines the local polynomial $P_\mathfrak{p}(T)$. For the ramified primes, it suffices to find the restriction of ρ to the local Galois group $G_\mathfrak{p}$ at $\mathfrak{p}$ with respect to an embedding $G_\mathfrak{p} \hookrightarrow G$ as a decomposition group. Assuming we can find $G_\mathfrak{p}$, Remark 5.7 enables us to identify the conjugacy class in G of any element of $G_\mathfrak{p}$, under this embedding. This is sufficient to compute the character of ρ on $G_\mathfrak{p}$, and thus also $\rho^{I_\mathfrak{p}}$ and $P_\mathfrak{p}(T)$. Note that we have *not* actually found the decomposition group at $\mathfrak{p}$ as a subgroup of G, which appears to be a harder problem.

This algorithm to compute Frobenius elements and L-series of Artin representations has now been implemented in Magma [2].

Remark 5.9 (Complexity)**.** From the complexity point of view, the computation of Frobenius elements for ‘good’ primes has two steps:

One is the initial precomputation of the polynomials Γ_C, each of which takes $O(n|C|)$ operations in some field containing the a_j (e.g. $\mathbb{C}$ or $\bar{\mathbb{Q}}_p$). This needs to be done for all conjugacy classes that are not determined by their cycle type.

The second step deals with a specific prime $\mathfrak{p}$ of K with residue field $\mathbb{F}_q$. We determine the cycle type of $\mathrm{Frob}_{\mathfrak{p}}$ by computing $\gcd(f, x^{q^j} - x)$ for $j \le n/2$, which takes $O(n \log q)$ multiplications of $n \times n$ matrices over $\mathbb{F}_q$. Then we evaluate the trace $\mathrm{Tr}(h(x)x^q)$ with another $O(n+\log q)$ matrix multiplications. Finally, we substitute the trace into all Γ_C corresponding to the cycle type of $\mathrm{Frob}_{\mathfrak{p}}$, which is $O(d)$ coefficient reductions and multiplications in $\mathbb{F}_q$, where d is the number of elements in G of this cycle type.

Here is as an illustration for polynomials of degree at most 11. There are 474 transitive groups G on at most 11 points, for each of which we took a polynomial $f \in \mathbb{Q}[x]$ with $\mathrm{Gal}\, f = G$ as a permutation group on the roots. (We used the database in Magma [2] V2.16.) For each G we computed Frob_p for all $p < 100000$ with $p \nmid \mathrm{Disc}(f)$, using Serre's trick (Example 3.9) and the above algorithm. Together with the Galois group computation and the precomputation of the Γ_C this took under 15 seconds on a 2GHz Pentium notebook for each G, with only four exceptions that took longer: $G = \mathrm{A}_5^2 \rtimes \mathrm{C}_2$, $\mathrm{A}_5^2 \rtimes \mathrm{C}_2^2$, $\mathrm{A}_5^2 \rtimes \mathrm{C}_4$ and M_{11}.

Remark 5.10 (Additional symmetries)**.** Suppose all conjugacy classes of elements of some order o and a fixed cycle type are closed under the power maps $g \mapsto g^k$ for k in some non-trivial subgroup $H \subset (\mathbb{Z}/o\mathbb{Z})^\times$ (for instance they are self-inverse, like in dihedral groups). Then one may replace $\Gamma_C(X)$ in Theorem 5.3 by

$$\prod_\sigma \Bigl(X - \sum_{j=1}^n h(a_j) \bigl(\textstyle\sum_{k\in H} \sigma^k(a_j) \bigr) \Bigr),$$

taking the product over some representatives for C modulo the action of H, and modifying the trace accordingly. In practice, this speeds up the computation of the Γ_C, as their degree drops by a factor of $|H|$.

6. Examples: abelian groups

If the Galois group is abelian, its conjugacy classes are of size 1, and all the Γ_C of Theorem 5.3 are linear, $\Gamma_C(X) = X - r_C$ with $r_C \in K$. For a good choice of $h(x)$ and all but finitely many primes $\mathfrak{p}$, the trace $\mathrm{Tr}(h(x)x^q)$ agrees with exactly one of the r_C modulo $\mathfrak{p}$, which then determines the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$.

In the examples below, ζ_n denotes a primitive nth root of unity.

Example 6.1. Let $K = \mathbb{Q}(i)$ and

$$f(x) = x^4 + 2x^3 + (3+3i)x^2 + 4ix - 1 + i.$$

Its complex roots are $a_1 = -0.31795 - 0.57510i$, $a_2 = 0.50870 - 1.1289i$, $a_3 = -1.4682 + 1.8471i$ and $a_4 = -0.72255 - 0.14308i$ to 5 decimal places. The splitting field L is a C_4-extension of $\mathbb{Q}(i)$, non-Galois over $\mathbb{Q}$, and the Galois group of L/K is $\langle(1234)\rangle < \mathrm{S}_4$. Take $h(x) = x^2$. An elementary computation gives

$$\begin{array}{lcllcl} \Gamma_{[\mathrm{id}]} & = & X - (10 + 6i), & \Gamma_{[(1234)]} & = & X - (4 + 4i), \\ \Gamma_{[(13)(24)]} & = & X - (-2 + 2i), & \Gamma_{[(1432)]} & = & X + 8. \end{array}$$

For a prime $\mathfrak{p} \neq (1+i), (2-i), (3)$ (the primes dividing $r_C - r_{C'}$ for $C \neq C'$) with residue field $\mathbb{F}_q$, we deduce that the Frobenius at $\mathfrak{p}$ is determined by

$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+2}) \equiv$	$10+6i$	$4+4i$	$-2+2i$	-8
$\mathrm{Frob}_{\mathfrak{p}} \quad =$	id	(1234)	(13)(24)	(1432)

Example 6.2 (Kummer extensions)**.** Suppose $\zeta = \zeta_n \in K$ and $L = K(\sqrt[n]{s})$ is a Kummer extension of degree n. It is abelian with Galois group C_n whose elements are determined by

$$\sigma_i : \sqrt[n]{s} \quad \longmapsto \quad \zeta^i \sqrt[n]{s}, \qquad i = 1, \ldots, n.$$

Take $f(x) = x^n - s$ and $h(x) = x^{n-1}$. Then

$$\Gamma_{[\sigma_i]}(X) = X - \sum_{j=1}^{n} h(\zeta^j \sqrt[n]{s})\sigma_i(\zeta^j \sqrt[n]{s}) = X - ns \cdot \zeta^i.$$

For a prime $\mathfrak{p}$ of K with residue field $\mathbb{F}_q$, because $n \mid q-1$, we have

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{x^n - s}/\mathbb{F}_q}(x^{q+n-1}) = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{x^n - s}/\mathbb{F}_q}(s^{\frac{q-1}{n}+1}) = ns \cdot s^{\frac{q-1}{n}}.$$

So Theorem 5.3 says that for $\mathfrak{p} \nmid ns$,

$$\mathrm{Frob}_{\mathfrak{p}} = \sigma_i \quad \Leftrightarrow \quad s^{\frac{q-1}{n}} \equiv \zeta^i \mod \mathfrak{p},$$

which is the classical criterion for Kummer extensions.

Example 6.3 ($\mathbb{Q}(\zeta_p)/\mathbb{Q}$)**.** Let $\zeta = \zeta_p$ for some prime $p > 2$, and take

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(\zeta), \quad f(x) = x^{p-1} + \ldots + x + 1.$$

Thus $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, with elements $\sigma_i : \zeta \mapsto \zeta^i$ for $i = 1, \ldots, p-1$. For $h(x) = x^2$ we have $\Gamma_{[\sigma_i]}(X) = X - r_i$ with $r_i \in \mathbb{Q}$ given by

$$r_i = \sum_{j=1}^{p-1} (\zeta^j)^2 \sigma_i(\zeta^j) = \sum_{j=1}^{p-1} \zeta^{j(2+i)} = \begin{cases} -1, & i \neq p-2, \\ p-1, & i = p-2. \end{cases}$$

For a prime q of $\mathbb{Q}$,

$$\begin{array}{rcl} \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q) & = & \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+2}) \quad \equiv \quad \mathrm{Tr}_{\frac{\mathbb{Z}[x]}{f(x)}/\mathbb{Z}}(x^{q+2}) \mod q \\ & \equiv & \mathrm{Tr}_{F/\mathbb{Q}}(\zeta^{q+2}) \qquad \equiv \quad \begin{cases} -1, & p \nmid q+2 \\ p-1, & p \mid q+2 \end{cases} \mod q. \end{array}$$

Hence Theorem 5.3b shows that for all $q \neq p$,

$$\mathrm{Frob}_q = \sigma_{p-2} \iff q \equiv -2 \mod p.$$

The same computation with $h(x) = x^{p-k}$ for varying k yields the classical criterion

$$\mathrm{Frob}_q = \sigma_k \iff q \equiv k \mod p.$$

Note that none of these $h(x)$ work for all conjugacy classes simultaneously, because the $\Gamma_{[\sigma_j]}$ are not coprime. This tends to happen when the roots of f are 'too nice' and $h(x)$ is 'too simple'. By Lemma 8.2, most h do work. In our example, a general polynomial

$$h(x) = \lambda_1 x^{p-1} + \ldots + \lambda_{p-1}x + \lambda_p$$

has

$$\Gamma_{[\sigma_i]}(X) = X + h(1) - p\lambda_i,$$

and these are distinct if and only if $\lambda_1, \ldots, \lambda_{p-1}$ are. The primes to which the theorem then applies are those not dividing $p\prod(\lambda_i - \lambda_j)$ in this case.

Example 6.4 (Cyclotomic extensions)**.** In general, suppose $L = K(\zeta_n)$ is some cyclotomic extension, and $f(x)$ is the minimal polynomial of ζ_n over K. As in the previous example, $G = \mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, and we write σ_i for the automorphism with $\sigma_i(\zeta_n) = \zeta_n^i$. We do the same computation as above: for $h(x) = x^k$ and $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$,

$$\Gamma_{[\sigma_i]}(X) = X - \sum_{g\in G} g(\zeta_n)^k \sigma_i(g(\zeta_n)) = X - \sum_{g\in G} g(\zeta_n)^{k+i} = X - \mathrm{Tr}_{L/K}(\zeta_n^{k+i})$$

and

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{k+q}) \equiv \mathrm{Tr}_{L/K}(\zeta_n^{k+q}) \mod \mathfrak{p}.$$

Because $\mathrm{Tr}_{L/K}(\zeta_n^j)$ is $|G|$ precisely when $n|j$, the polynomial $\Gamma_{[\sigma_{n-k}]}$ differs from all the other $\Gamma_{[\sigma_j]}$'s, and we find that

$$\mathrm{Frob}_{\mathfrak{p}} = \sigma_{n-k} \iff q \equiv n - k \mod n$$

for almost all $\mathfrak{p}$. (One may improve 'almost all' to 'all $\mathfrak{p} \nmid n$' by taking several h.)

Remark 6.5. The fact that we obtained a simple formula for Frobenius elements for cyclotomic and Kummer extensions relied on the existence of a universal expression for the trace $\mathrm{Tr}(h(x)x^q) \mod \mathfrak{p}$. It follows from class field theory that there are such formulae in all abelian extensions.

For instance, consider Example 6.1 of a C_4-extension of $K = \mathbb{Q}(i)$ from the point of view of class field theory. There the conductor of L/K is $N = (1+i)^4(2-i) = 8-4i$, and the group $(\mathcal{O}_K/N)^\times$ is $\mathrm{C}_4 \times \mathrm{C}_4 \times \mathrm{C}_2$, with generators i, 7 and $3-2i$ respectively. For a prime $\mathfrak{p} = (\alpha) \subset \mathbb{Z}[i]$ not dividing N, if $\alpha \equiv i^a 7^b (3-2i)^c \mod N$, then $\mathrm{Frob}_{\mathfrak{p}} = (1234)^b$.

Now compare this with the description of Frobenius in Example 6.1. Writing $\mathbb{F}_q = \mathbb{Z}[i]/\mathfrak{p}$ and Tr for $\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}$, we get 4 congruences for the traces,

$$\begin{array}{llll}
\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^0(3-2i)^c \mod N & \Leftrightarrow & \mathrm{Tr}(x^{q+2})\equiv 10+6i \mod \mathfrak{p}\\
\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^1(3-2i)^c \mod N & \Leftrightarrow & \mathrm{Tr}(x^{q+2})\equiv 4+4i \mod \mathfrak{p}\\
\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^2(3-2i)^c \mod N & \Leftrightarrow & \mathrm{Tr}(x^{q+2})\equiv -2+2i \mod \mathfrak{p}\\
\mathfrak{p}=(\alpha),\ \alpha\equiv i^a 7^3(3-2i)^c \mod N & \Leftrightarrow & \mathrm{Tr}(x^{q+2})\equiv -8 \mod \mathfrak{p}
\end{array}$$

for $\mathfrak{p} \neq (1+i), (2-i), (3)$.

Note that if one had a way to prove these congruences directly, one would have a proof of Artin reciprocity in the extension L/K.

7. Examples: non-abelian groups

We continue with examples to Theorem 5.3. When G is non-abelian, the only difference is that the Γ_C are no longer linear.

Example 7.1. Let $K = \mathbb{Q}$ and $f(x) = x^3 - 2$. It has Galois group S_3 and roots $a_1 = \sqrt[3]{2}, a_2 = \zeta\sqrt[3]{2}$ and $a_3 = \zeta^2\sqrt[3]{2}$, where ζ is a primitive cube root of unity. Take $h(x) = x^2/6$ (the factor 1/6 is only chosen for convenience) and compute the polynomials Γ_C for the three conjugacy classes:

$$\begin{aligned}
\Gamma_{[\mathrm{id}]} &= X - \tfrac{1}{6}(a_1^2a_1 + a_2^2a_2 + a_3^2a_3)\\
&= X - 1\\
\Gamma_{[(12)]} &= (X - \tfrac{1}{6}(a_1^2a_2 + a_2^2a_1 + a_3^3))(X - \tfrac{1}{6}(a_1^2a_3 + a_2^3 + a_3^2a_1))(X - \tfrac{1}{6}(a_1^3 + a_2^2a_3 + a_3^2a_2))\\
&= (X - \tfrac{1}{3}(\zeta + \zeta^2 + 1))(X - \tfrac{1}{3}(\zeta^2 + 1 + \zeta))(X - \tfrac{1}{3}(1 + \zeta + \zeta^2))\\
&= X^3\\
\Gamma_{[(123)]} &= (X - \tfrac{1}{6}(a_1^2a_2 + a_2^2a_3 + a_3^2a_1))(X - \tfrac{1}{6}(a_1^2a_3 + a_2^2a_1 + a_3^2a_2))\\
&= (X - \tfrac{1}{3}(\zeta + \zeta + \zeta))(X - \tfrac{1}{3}(\zeta^2 + \zeta^2 + \zeta^2)) = (X - \zeta)(X - \zeta^2)\\
&= X^2 + X + 1.
\end{aligned}$$

On the other hand, for a rational prime $q = 3m + k$ with $k = 1$ or 2,

$$\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{x^3-2}/\mathbb{F}_q}(\tfrac{1}{6}x^{q+2}) = \mathrm{Tr}(\tfrac{1}{6}2^{m+1}x^{k-1}) = \begin{cases} 2^m, & k{=}1 \\ 0, & k{=}2 \end{cases} = \begin{cases} 2^{\frac{q-1}{3}}, & q{\equiv}1 \mod 3 \\ 0, & q{\equiv}2 \mod 3 \end{cases}.$$

The conclusion of Theorem 5.3 is that, as expected, for $q \neq 2, 3$,

$$\begin{array}{lll}
q \equiv 1 \mod 3,\ 2 \in (\mathbb{F}_q)^{\times 3} & \Longrightarrow & \mathrm{Frob}_q = \mathrm{id},\\
q \equiv 1 \mod 3,\ 2 \notin (\mathbb{F}_q)^{\times 3} & \Longrightarrow & \mathrm{Frob}_q \in [(123)],\\
q \equiv 2 \mod 3 & \Longrightarrow & \mathrm{Frob}_q \in [(12)].
\end{array}$$

Clearly, an identical computation goes through for $f(x) = x^3 - c$ (with $h(x) = x^2/3c$) over any global field K with $\zeta \notin K$.

We can also take a general cubic polynomial and obtain an analogue of Euler's criterion for its factorisation modulo primes:

Theorem 7.2. *Let $f(x) = x^3 + bx + c$ be a separable cubic polynomial over a global field K, and $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$. Write*

$$T = \mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1}) = \mathrm{Tr}\begin{pmatrix}0 & 0 & -c\\ 1 & 0 & -b\\ 0 & 1 & 0\end{pmatrix}^{q+1} \qquad \bmod \mathfrak{p}.$$

If $\mathfrak{p}$ does not divide $3b(4b^2 + 27b^2)$ and the denominators of b and c, then

$$\begin{array}{llll} T \equiv -2b & \bmod \mathfrak{p} & \Leftrightarrow & f(x) \text{ has 3 roots mod } \mathfrak{p},\\ T \equiv b & \bmod \mathfrak{p} & \Leftrightarrow & f(x) \text{ is irreducible mod } \mathfrak{p},\\ T \text{ is a root of } x^3-3b^2x-2b^3-27c^2 & & \Leftrightarrow & f(x) \text{ has 1 root mod } \mathfrak{p}. \end{array}$$

Proof. We compute the polynomials Γ_C for $G = \mathrm{S}_3$, $h(x) = x$ by expressing their coefficients in terms the elementary symmetric functions $a_1+a_2+a_3=0$, $a_1a_2+a_2a_3+a_3a_1 = b$ and $a_1a_2a_3 = -c$:

$$\begin{array}{lcl} \Gamma_{[\mathrm{id}]} &=& X - (a_1^2+a_2^2+a_3^2) = X - (a_1+a_2+a_3)^2+2(a_1a_2+a_1a_3+a_2a_3)\\ &=& X + 2b\\ \Gamma_{[(12)]} &=& (X-(a_1a_2+a_2a_1+a_3^2))(X-(a_1a_2+a_2a_1+a_3^2))(X-(a_1a_2+a_2a_1+a_3^2))\\ &=& X^3 - 3b^2X - 2b^3-27c^2\\ \Gamma_{[(123)]} &=& (X - (a_1a_2+a_2a_3+a_3a_1))(X - (a_1a_3+a_2a_1+a_3a_2))\\ &=& (X - b)^2. \end{array}$$

The least common multiple of their pairwise resultants is $3b(4b^3 + 27c^2)$, which completes the proof by Theorem 5.3. □

An identical computation can be done for polynomials of higher degree, as long as one has the patience to work out the coefficients of the Γ_C's. Here is the corresponding result for quartics:

Theorem 7.3. *Let $f(x) = x^4 + bx^2 + cx + d$ be a separable quartic polynomial over K, and $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$. Then the value $\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1})$ is a root of one of the polynomials*

$$\begin{array}{lcl} \Gamma_{[\mathrm{id}]} &=& X + 2b\\ \Gamma_{[(12)(34)]} &=& X^3 - 2bX^2 - 16dX + 32bd - 8c^2\\ \Gamma_{[(12)]} &=& X^6 + 4bX^5 + (2b^2 + 8d)X^4 + (-12b^3 + 48bd - 26c^2)X^3\\ && -(23b^4 - 120b^2d + 108bc^2 + 112d^2)X^2\\ && -(16b^5 - 128b^3d + 138b^2c^2 + 256bd^2 + 216c^2d)X\\ && -4b^6 + 48b^4d - 56b^3c^2 - 192b^2d^2 - 288bc^2d - 27c^4 + 256d^3\\ \Gamma_{[(123)]} &=& X^4 + (-2b^2 + 8d)X^2 - 8c^2X + b^4 - 8b^2d + 8bc^2 + 16d^2\\ \Gamma_{[(1234)]} &=& X^3 - 2bX^2 + (b^2 - 4d)X + c^2. \end{array}$$

If $\mathfrak{p}$ does not divide the denominators of b, c and d and the pairwise resultants of the Γ_c, then this determines the degrees in the factorisation of f mod $\mathfrak{p}$: they are the cycle lengths of the permutation in the index of Γ.

A theorem of Brumer (see [4] Thm. 2.3.5) states that any Galois extension L/K with Galois group $G = \mathrm{D}_{10}$ is a splitting field of

$$f_{a,b}(x) = x^5 + (a-3)x^4 + (b-a+3)x^3 + (a^2-a-1-2b)x^2 + bx + a$$

for some $a, b \in K$. Using a similar argument to $G = \mathrm{S}_3$ and S_4, we find

Theorem 7.4. *Suppose L/K is the splitting field of $f_{a,b}(x)$ as above, with $G = \mathrm{Gal}(L/K) \cong \mathrm{D}_{10}$. If $\mathfrak{p}$ a prime of K with residue field $\mathbb{F}_q$, not dividing $3a-b+1$ and the denominators of a and b and such that $f \mod \mathfrak{p}$ is irreducible, then $\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1})$ is either $-2a+b+1$ or $a+2$ modulo $\mathfrak{p}$. This determines which of the two conjugacy classes of 5-cycles contains $\mathrm{Frob}_\mathfrak{p}$.*

Remark 7.5. In this setting, if $\mathrm{Frob}_\mathfrak{p}$ is not a 5-cycle, it is either the identity or an element of order 2. In the former case, $\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(x^{q+1})$ is $a^2-4a-2b+3 \mod \mathfrak{p}$; in the latter it is a root of

$$\begin{aligned}\Gamma_{[(23)(45)]} = {} & x^5-(a-3)^2x^4+(31-2a^3+4b-3b^2+a^2(11+2b)-2a(21+2b))x^3\\ & +(12a^3(3+2b)-a^2(137+44b)+a(114+6b-28b^2)-51+7a^4-4a^5-20b+14b^2-2b^3)x^2\\ & +(40+16a^5-8a^6+32b-17b^2-4b^3+a^4(58+42b)+a^2(182+18b-52b^2)\\ & +4a^3(-49-21b+b^2)-2a(65+13b-17b^2+6b^3))x\\ & +8a^6-4a^7+4a^5(7+5b)-4a^4(32+17b)+2a^3(123+85b+4b^2)\\ & -a^2(245+218b+24b^2)-2a(-30-6b+51b^2+22b^3)+2(-6-8b+3b^2+b^3-4b^4).\end{aligned}$$

Example 7.6. Here is another example, to illustrate what the Γ_C look like in general. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(E[3])$, the 3-torsion field of the elliptic curve $E : y^2 + y = x^3 - x^2$. Then $\mathrm{Gal}(L/K) \cong \mathrm{GL}_2(\mathbb{F}_3)$, and L is the splitting field of

$$f(x) = x^8 - 9x^7 + 18x^6 + 33x^5 - 93x^4 - 15x^3 - 23x^2 - 36x - 27.$$

The Γ_C for $h(x) = x^2$ are

$$\begin{aligned}
\Gamma_{[\mathrm{id}]} &= x-144\\
\Gamma_{[(13)(24)(56)(78)]} &= x-3\\
\Gamma_{[(24)(57)(68)]} &= x^{12}-699x^{11}+204666x^{10}-32922129x^9+3212225793x^8-196600821903x^7+\\
&= 7340079612456x^6-145234777501584x^5+566948224573848x^4+\\
&= 267477005624480823x^3-187604198442957555x^2-2946247136394353892x-\\
&= 24290099658154516203\\
\Gamma_{[(148)(273)]} &= x^8-546x^7+120102x^6-14088342x^5+989228043x^4-43566817716x^3+\\
&= 1248800990265x^2-21583664066961x+167939769912993\\
\Gamma_{[(1432)(5768)]} &= x^6-258x^5+26448x^4-1344378x^3+34859664x^2-445164021x+2926293624\\
\Gamma_{[(174382)(56)]} &= x^8-264x^7+29292x^6-1698042x^5+51288993x^4-654852960x^3+\\
&= 3360584547x^2-277935306777x+7299371089503\\
\Gamma_{[(15473628)]} &= x^6-258x^5+26250x^4-1336755x^3+35700471x^2-477465444x+2707751520\\
\Gamma_{[(16483527)]} &= x^6-258x^5+28230x^4-1674048x^3+57362760x^2-1097286921x+9616023198
\end{aligned}$$

Example 7.7. As an indication to the kind of Artin L-series that may be numerically computed, we give an example with a big Galois group over $\mathbb{Q}$. We take $G = \mathrm{PGSp}(4, \mathbb{F}_3)$ of order 51840, realised through the Galois action on the 3-torsion of the Jacobian of a genus 2 curve, and evaluate the Artin L-series of an irreducible 6-dimensional representation of G.

Specifically, G is the unique double cover of the simple group $\mathrm{Sp}(4, \mathbb{F}_3)/\mathbb{F}_3^\times$ in $\mathrm{PGL}(4, \mathbb{F}_3) = \mathrm{GL}(4, \mathbb{F}_3)/\mathbb{F}_3^\times$. To obtain it as a Galois group, take the hyperelliptic curve

$$\mathcal{C}/\mathbb{Q}: \;\; y^2 - (x^2 + 1)y = x^5 - x^4 + x^3 - x^2.$$

Consider the field $\mathbb{Q}(J[3])$ obtained by adjoining to $\mathbb{Q}$ the coordinates of the 3-torsion points of its Jacobian $J/\mathbb{Q}$. Then $\mathrm{Gal}(\mathbb{Q}(J[3])/\mathbb{Q})$ is $\mathrm{GSp}(4, \mathbb{F}_3)$. The group we want is $G = \mathrm{GSp}(4, \mathbb{F}_3)/\{\pm 1\}$, and it can be obtained from the Galois action on the 40 lines through the origin in $J[3]$. Specifically, if $(P)+(Q)-2(O) \in J[3]$ is a non-zero point with $P=(x_P,y_P), Q=(x_Q,y_Q)$, the minimal polynomial f of x_Px_Q over $\mathbb{Q}$ has Galois group G;

$$f = x^{40}+27x^{39}+39x^{38}-61x^{37}+\ldots+2259x^3+3471x^2+1057x+69.$$

In its action on the roots of f, the group has several conjugacy classes of the same cycle type, and the largest Γ_C that we need has degree 2160 (using Remark 5.10).

The group has two irreducible 6-dimensional representations, ρ and ρ' (whose trace on elements of order 10 in G is $+1$ and -1 respectively). The curve $\mathcal{C}$ has good reduction outside 2 and 3, so $L/\mathbb{Q}$ is unramified at all primes $p \neq 2,3$. The conductor of ρ is $2^{10}3^{17}$ and we used our machinery to compute the local polynomials for the Artin L-series $L(\rho,s)$ for primes up to 410203. Using Magma [2], we then evaluate

$$L(\rho,1) \approx 1.852529796, \qquad L(\rho,2) \approx 1.119877506$$

to 10 digits precision; this computation relies implicitly on the validity of Artin's conjecture for ρ. The total time to compute f, $\mathrm{Gal}(f/\mathbb{Q})$, the Γ_C, the L-series and the L-values was 7 hours on a Sun Ultra 24 workstation.

8. Appendix: Two lemmas on Zariski density

Lemma 8.1. *Suppose K is an infinite field, $f \in K[t]$ is a separable polynomial of degree n and $a_1,...,a_n$ are its roots in some splitting field L.*

(a) *If $F,G \in K[x_1,...,x_n]$ take the same values on*

$$\begin{aligned} x_1 &= \beta_0+\beta_1 a_1+\ldots+\beta_{n-1}a_1^{n-1} \\ &\cdots \\ x_n &= \beta_0+\beta_1 a_n+\ldots+\beta_{n-1}a_n^{n-1} \end{aligned}$$

for all $[\beta_1,...,\beta_n] \in K^n$, then $F=G$.

(b) *Suppose $F_1,...,F_d \in K[x_1,...,x_n]$ are distinct. There exists a polynomial $B(t)=\beta_0+\ldots+\beta_{n-1}t^{n-1} \in K[t]$ such that $B(a_1),...,B(a_n)$ generate L and the F_i take distinct values on $[B(a_1),...,B(a_n)]$. The set of such B is Zariski dense in $K \oplus Kt \oplus \cdots \oplus Kt^{n-1}$.*

(c) *Let F be a T-invariant for some $T < \mathrm{S}_n$. There is a Zariski dense open set of polynomials $B(t) \in K \oplus Kt \oplus \cdots \oplus Kt^{n-1}$ for which $\boldsymbol{a}'=[B(a_1),...,B(a_n)]$ generate L and $e^F_{\boldsymbol{a}'}: T\setminus \mathrm{S}_n \to L$ is injective.*

Proof. (a) Let $U=K(t_1,...,t_n)$. As a first step, we observe that K^n is Zariski dense in $\mathbb{A}^n_U=U^n$: this is clear for $n=1$ as K is infinite; generally, if K^n were not Zariski dense, it would be contained in a (not necessarily irreducible) hypersurface of some degree d, so it would contain at most d hyperplanes. But, by induction, it contains all $\{r\}\times U^{n-1}$ for all $r \in K$, which gives a contradiction.

Therefore, as F and G are continuous in the Zariski topology, they agree on all of U^n, i.e. on all the above combinations with $[\beta_1,...,\beta_n] \in U^n$.

Now solve the system of equation $\sum_{j=0}^{n-1} a_i^j \beta_j = t_j$ for $\beta_1, ..., \beta_n$. (This is possible because $a_i \neq a_k$ for $i \neq k$, so the Vandermonde matrix is invertible.) Using this solution we find that $F(t_1, ..., t_n) = G(t_1, ..., t_n)$, so $F = G$ as polynomials.

(b) Put $F(x_1, ..., x_n) = \prod_{i<j}(x_i - x_j)(F_i - F_j)$ and $G = 0$ and apply (a). This gives a polynomial $B(t) = \beta_0 + \ldots + \beta_{n-1}t^{n-1} \in K[t]$ which clearly satisfies the 'distinct values' condition. Furthermore, $B(a_i) \neq B(a_j)$ guarantees the 'generate L' condition as well: the Galois action permutes the $B(a_i)$ in the same way as the a_i, so the Galois group has the same order. Finally, consider $F(B(a_1), ..., B(a_n))$ as a polynomial in $\beta_0, ..., \beta_{n-1}$. Its zero set is Zariski closed in $\mathbb{A}^n$ and we proved that its complement is non-empty. This proves the last claim.

(c) Apply (b) to the set of polynomials $\{F^\sigma\}_{\sigma \in T\backslash \mathsf{S}_n}$, using that, by definition, $e^F_{\boldsymbol{a}'}(\sigma^{-1}) = F((\boldsymbol{a}')^{\sigma^{-1}}) = F^\sigma(\boldsymbol{a}')$. □

Lemma 8.2. *Suppose K is an infinite field, $f \in K[t]$ is a separable polynomial of degree n and $a_1, ..., a_n$ are its roots in some splitting field L. Then on a Zariski dense open set of polynomials $h(x)$ in $K \oplus Kx \oplus \ldots \oplus Kx^{n-1} \cong \mathbb{A}^n_K$, the values*

$$v_h(\sigma) = \sum_{j=1}^{n} h(a_j)\sigma(a_j), \qquad \sigma \in G = \mathrm{Gal}(L/K)$$

are distinct.

Proof. For any $\sigma \in G$, the map $E_\sigma : h \mapsto v_h(\sigma)$ is K-linear $K^n \to L$. So E_σ agrees with E_τ on a K-linear subspace for every $\sigma, \tau \in G$. If none of these subspaces is all of K^n, then the complement of their union is the desired set (non-empty since K is infinite). It remains to prove that $E_\sigma \neq E_\tau$ for $\sigma \neq \tau$.

Suppose $E_\sigma = E_\tau : K^n \to L$. Then their extensions by linearity to maps $L^n \to L$ agree as well. In other words, $v_h(\sigma) = v_h(\tau)$ for all h in $L \oplus Lx \oplus \ldots \oplus Lx^{n-1}$. In particular, taking

$$h(x) = \prod_{j \neq i}(x - a_j)$$

we get that $\sigma(a_i) = \tau(a_i)$. As this holds for all i, it follows that $\sigma = \tau$. □

References

[1] A. R. Booker, Numerical tests of modularity, J. Ramanujan Math. Soc. 20. (2005), no. 4, 283-339.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I: The user language, J. Symb. Comput. 24, No. 3–4 (1997), 235–265.

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

[4] C. U. Jensen, A. Ledet and N. Yui, Generic Polynomials, Constructive Aspects of the Inverse Galois Problem, Mathematical Sciences Research Institute Publications, Cambridge University Press, 2002.

[5] D. P. Roberts, Frobenius classes in alternating groups, Rocky Mountain J. Math. 34 no. 4 (2004), 1483–1496.

Robinson College, Cambridge CB3 9AN, United Kingdom
E-mail address: `t.dokchitser@dpmms.cam.ac.uk`

Emmanuel College, Cambridge CB2 3AP, United Kingdom
E-mail address: `v.dokchitser@dpmms.cam.ac.uk`