14.8 COMPUTATION OF GALOIS GROUPS OVER $\mathbb{Q}$

In the determination of the Galois groups of polynomials of degrees ≤ 4 in Section 6 and in the determination of the Galois group of the polynomial $x^5 - 6x + 3$ in the previous section we observed that it was possible to obtain useful information regarding the Galois group from the *cycle types* of the automorphisms as elements in S_n. This is very useful in computing Galois groups of polynomials over $\mathbb{Q}$ and we now briefly describe the theoretical justification.

Let $f(x)$ be a polynomial with rational coefficients. In determining the Galois group of $f(x)$ we may assume that $f(x)$ is separable and has integer coefficients. Then the discriminant D of $f(x)$ is an integer and is nonzero.

For any prime p, consider the reduction $\overline{f}(x) \in \mathbb{F}_p[x]$ of $f(x)$ modulo p. If p divides D then the reduced polynomial $\overline{f}(x)$ has discriminant $\overline{D} = 0$ in $\mathbb{F}_p$, so is not separable.

If p does not divide D, then $\overline{f}(x)$ is a separable polynomial over $\mathbb{F}_p$ and we can factor $\overline{f}(x)$ into distinct irreducibles

$$\overline{f}(x) = \overline{f}_1(x)\overline{f}_2(x) \cdots \overline{f}_k(x) \qquad \text{in } \mathbb{F}_p[x].$$

Let n_i be the degree of $\overline{f}_i(x)$, $i = 1, 2, \ldots, k$.

The importance of this reduction is provided by the following theorem from algebraic number theory which is an elementary consequence of the study of the arithmetic in finite extensions of $\mathbb{Q}$ (and which we take for granted).

Theorem. For any prime p not dividing the discriminant D of $f(x) \in \mathbb{Z}[x]$, the Galois group over $\mathbb{F}_p$ of the reduction $\overline{f}(x) = f(x) \pmod{p}$ is permutation group isomorphic to a subgroup of the Galois group over $\mathbb{Q}$ of $f(x)$.

The meaning of the statement "permutation group isomorphic" in the theorem is that not only is the Galois group of the reduction $\overline{f}(x)$ mod p of $f(x)$ isomorphic to a subgroup of the Galois group of $f(x)$ but that there is an ordering of the roots of $\overline{f}(x)$ and of $f(x)$ (depending on p) so that under this isomorphism the action of the corresponding automorphisms as permutations of these roots is the same. In particular there are automorphisms in the Galois group of $f(x)$ with the same cycle types as the automorphisms of $\overline{f}(x)$.

The Galois group of $\overline{f}(x)$ is a *cyclic* group since every finite extension of $\mathbb{F}_p$ is a cyclic extension. Let σ be a generator for this Galois group over $\mathbb{F}_p$ (for example, the Frobenius automorphism). The roots of $\overline{f}_1(x)$ are permuted amongst themselves by the Galois group, and given any two of these roots there is a Galois automorphism taking the first root to the second (recall that the group is said to be *transitive* on the roots when this is the case). Similarly, the Galois group permutes the roots of each of the factors $\overline{f}_i(x)$, $i = 1, 2, \ldots, k$ transitively. Since these factors are relatively prime we also see that no root of one factor is mapped to a root of any other factor by any element of the Galois group.

View σ as an element in S_n by labelling the n roots of $\overline{f}(x)$ and consider the cycle decomposition of σ, which is a product of k distinct permutations since σ permutes

the roots of each of the factors $\overline{f}_i(x)$ amongst themselves. By the observations we just made, the action of σ on the roots of $\overline{f}_1(x)$ must be a cycle of length n_i since otherwise the powers of σ could not be transitive on the roots of $\overline{f}_1(x)$. Similarly the action of σ on the roots of $\overline{f}_i(x)$ gives a cycle of length n_i, $i = 1, 2, \ldots, k$.

We see that the automorphism σ generating the Galois group of $\overline{f}(x)$ has cycle decomposition $(n_1, n_2, \ldots, n_k)$ where $n_1, n_2, \ldots, n_k$ are the degrees of the irreducible factors of $f(x)$ reduced modulo p, which gives us the following result.

Corollary 41. For any prime p not dividing the discriminant of $f(x) \in \mathbb{Z}[x]$, the Galois group of $f(x)$ over $\mathbb{Q}$ contains an element with cycle decomposition $(n_1, n_2, \ldots, n_k)$ where $n_1, n_2, \ldots, n_k$ are the degrees of the irreducible factors of $f(x)$ reduced modulo p.

Example

Consider the polynomial $x^5 - x - 1$. The discriminant of this polynomial is $2869 = 19 \cdot 151$ so we reduce at primes $\neq 19, 151$. Reducing mod 2 the polynomial $x^5 - x - 1$ factors as $(x^2 + x + 1)(x^3 + x^2 + 1)$ (mod 2) so the Galois group has a (2,3)-cycle. Cubing this element we see the Galois group contains a transposition.

Reducing mod 3 the polynomial is irreducible, as follows: $x^5 - x - 1$ has no roots mod 3 so if it were reducible mod 3 then it would have an irreducible quadratic factor, hence would have a factor in common with $x^9 - x$ (which is the product of all irreducible polynomials of degrees 1 and 2 over $\mathbb{F}_3$), hence a factor in common with either $x^4 - 1$ or $x^4 + 1$, hence a factor in common with either $x^5 - x$ or $x^5 + x$, hence a factor in common with either -1 or $2x + 1$ which it obviously does not. This shows both that $x^5 - x - 1$ is irreducible in $\mathbb{Z}[x]$ and that there is a 5-cycle in its Galois group.

Since S_5 is generated by any 5-cycle and any transposition, it follows that the Galois group of $x^5 - x - 1$ is S_5 (so in particular this polynomial cannot be solved by radicals, (cf. Exercise 21 of Section 7).

The arguments in the example above indicate how to construct polynomials with S_n as Galois group. We use the fact that a transitive subgroup of S_n containing a transposition and an $n - 1$-cycle is S_n. Let f_1 be an irreducible polynomial of degree n over $\mathbb{F}_2$. Let $f_2 \in \mathbb{F}_3[x]$ be the product of an irreducible polynomial of degree 2 with irreducible polynomials of odd degree (for example, an irreducible polynomial of degree $n - 3$ and x if n is even and an irreducible polynomial of degree $n - 2$ if n is odd). Let $f_3 \in \mathbb{F}_5[x]$ be the product of x with an irreducible polynomial of degree $n - 1$. Finally, let $f(x) \in \mathbb{Z}[x]$ be any polynomial with

$$\begin{aligned} f(x) &\equiv f_1(x) \pmod 2 \\ &\equiv f_2(x) \pmod 3 \\ &\equiv f_3(x) \pmod 5. \end{aligned}$$

The reduction of $f(x)$ mod 2 shows that $f(x)$ is irreducible in $\mathbb{Z}[x]$, hence the Galois group is transitive on the n roots of $f(x)$. Raising the element given by the factorization of $f(x)$ mod 3 to a suitable odd power shows the Galois group contains a transposition. The factorization mod 5 shows the Galois group contains an $n - 1$-cycle, hence the Galois group is S_n.

Proposition 42. For each $n \in \mathbb{Z}^+$ there exist infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ with S_n as Galois group over $\mathbb{Q}$.

There are extremely efficient algorithms for factoring polynomials $f(x) \in \mathbb{Z}[x]$ modulo p (cf. Exercises 12 to 17 of Section 3), so the corollary above is an effective procedure for determining some of the cycle types of the elements of the Galois group. In using Corollary 41 some care should be taken not to assume that a *particular* cycle is an element of the Galois group. For example, one factorization might imply the existence of a (2,2) cycle, say (12)(34) and another factorization imply the existence of a transposition. One cannot conclude that the transposition is necessarily (12), however (nor (34), nor (13), etc.). The choice of (12)(34) to represent the first cycle fixes a particular ordering on the roots and this may not be the ordering with respect to which the transposition appears as (12).

Corollary 41 is particularly efficient in determining when the Galois group is large (e.g., S_n), since a transitive group containing sufficiently many cycle types must be S_n (for example, a transitive subgroup of S_n containing a transposition and an $n-1$-cycle is S_n, as used above). The most difficult Galois groups to determine in this way are the *small* Galois groups (e.g., a cyclic group of order n), since factorization after factorization will produce only elements of orders dividing n and one is not sure whether there will be some p yet to come producing a cycle type inconsistent with the assumption of a cyclic Galois group. If one could "compute forever" one could at least be sure of the precise distribution of cycle types among the elements of the Galois group in the following sense: suppose the Galois group $G \subseteq S_n$ has order N and that there are n_T elements of G with cycle type T (e.g., (2,2)-cycles, transpositions, etc.) so that the "density" of cycle type T in G is $d_T = n_T/N$. Then it is possible to define a density on the set of prime numbers (so that it makes sense to speak of "1/2" the primes, etc.) and we have the following result (which relies on the Tchebotarov Density Theorem in algebraic number theory).

Theorem. The density of primes p for which $f(x)$ splits into type T modulo p is precisely d_T.

This says that if we knew the factorization of $f(x)$ modulo every prime we could at least determine the number of elements of G with a given cycle type. Unfortunately, even this would not be sufficient to determine G (up to isomorphism): it is known that there are nonisomorphic groups containing the same number of elements of all cycle types (there are two nonisomorphic groups of order 96 in S_8 both having cycle type distributions: 1 1-cycle, 6 (2,2)-cycles, 13 (2,2,2,2)-cycles, 32 (3,3)-cycles, 12 (4,4)-cycles, 32 (2,6)-cycles). There are infinitely many such examples (the regular representation of the elementary abelian group of order p^3 and for the nonabelian group of order p^3 of exponent p give two nonisomorphic groups in S_{p^3} whose nonidentity elements are all the product of p^2 p-cycles for any prime p).

In practice one uses the factorizations of $f(x)$ modulo small primes to get an idea of the probable Galois group (based on the previous result). One then tries to prove this is indeed the Galois group — often a difficult problem. For polynomials of small degree, definitive algorithms exist, based in part on the computation of *resolvent* polynomials.