

# GALOIS GROUPS AS PERMUTATION GROUPS

KEITH CONRAD

## 1. INTRODUCTION

A Galois group is a group of field automorphisms under composition. By looking at the effect of a Galois group on field generators we can interpret the Galois group as permutations, which makes it a subgroup of a symmetric group. This makes Galois groups into relatively concrete objects and is particularly effective when the Galois group turns out to be a symmetric or alternating group.

## 2. AUTOMORPHISMS OF FIELDS AS PERMUTATIONS OF ROOTS

The *Galois group of a polynomial*  $f(T) \in K[T]$  over  $K$  is defined to be the Galois group of a splitting field for  $f(T)$  over  $K$ . We do not require  $f(T)$  to be irreducible in  $K[T]$ .

**Example 2.1.** The polynomial  $T^4 - 2$  has splitting field  $\mathbf{Q}(\sqrt[4]{2}, i)$  over  $\mathbf{Q}$ , so the Galois of  $T^4 - 2$  over  $\mathbf{Q}$  is isomorphic to  $D_4$ . The splitting field of  $T^4 - 2$  over  $\mathbf{R}$  is  $\mathbf{C}$ , so the Galois group of  $T^4 - 2$  over  $\mathbf{R}$  is  $\text{Gal}(\mathbf{C}/\mathbf{R}) = \{z \mapsto z, z \mapsto \bar{z}\}$ , which is cyclic of order 2.

**Example 2.2.** The Galois group of  $(T^2 - 2)(T^2 - 3)$  over  $\mathbf{Q}$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . Its Galois group over  $\mathbf{R}$  is trivial since the polynomial splits completely over  $\mathbf{R}$ .

Writing  $f(T) = (T - r_1) \cdots (T - r_n)$ , the splitting field of  $f(T)$  over  $K$  is  $K(r_1, \dots, r_n)$ . Each  $\sigma$  in the Galois group of  $f(T)$  over  $K$  permutes the  $r_i$ 's since  $\sigma$  fixes  $K$  and therefore  $f(r) = 0 \Rightarrow f(\sigma(r)) = 0$ . The automorphism  $\sigma$  is completely determined by its permutation of the  $r_i$ 's since the  $r_i$ 's generate the splitting field over  $K$ . A permutation of the  $r_i$ 's can be viewed as a permutation of the subscripts  $1, 2, \dots, n$ .

**Example 2.3.** Consider the Galois group of  $T^4 - 2$  over  $\mathbf{Q}$ . The polynomial has 4 roots:  $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$ . Two generators of  $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$  are the automorphisms  $r$  and  $s$  where  $r(\sqrt[4]{2}) = i\sqrt[4]{2}$  and  $r(i) = i$ , and  $s(\sqrt[4]{2}) = \sqrt[4]{2}$  and  $s(i) = -i$ . The effect of the Galois group on  $\sqrt[4]{2}$  and  $i$  is in Table 1.

Automorphism	1	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
Value on $\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
Value on $i$	$i$	$i$	$i$	$i$	$-i$	$-i$	$-i$	$-i$

TABLE 1.

The effect of  $r$  on the roots of  $T^4 - 2$  is

$$r(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad r(i\sqrt[4]{2}) = -\sqrt[4]{2}, \quad r(-\sqrt[4]{2}) = -i\sqrt[4]{2}, \quad r(-i\sqrt[4]{2}) = \sqrt[4]{2},$$

which is a 4-cycle, while the effect of  $s$  on the roots of  $T^4 - 2$  is

$$s(\sqrt[4]{2}) = \sqrt[4]{2}, \quad s(i\sqrt[4]{2}) = -i\sqrt[4]{2}, \quad s(-i\sqrt[4]{2}) = i\sqrt[4]{2}, \quad s(-\sqrt[4]{2}) = -\sqrt[4]{2},$$

which swaps  $i\sqrt[4]{2}$  and  $-i\sqrt[4]{2}$  while fixing  $\sqrt[4]{2}$  and  $-\sqrt[4]{2}$ . So  $s$  is a 2-cycle on the roots.

Indexing the roots of  $T^4 - 2$  as

$$(2.1) \quad r_1 = \sqrt[4]{2}, \quad r_2 = i\sqrt[4]{2}, \quad r_3 = -\sqrt[4]{2}, \quad r_4 = -i\sqrt[4]{2},$$

the automorphism  $r$  acts on the roots like (1234) and the automorphism  $s$  acts on the roots like (24). With this indexing of the roots, the Galois group of  $T^4 - 2$  over  $\mathbf{Q}$  becomes the group of permutations in  $S_4$  in Table 2.

Automorphism	1	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
Permutation	(1)	(1234)	(13)(24)	(1432)	(24)	(12)(34)	(13)	(14)(23)

TABLE 2.

**Example 2.4.** If we label the roots of  $(T^2 - 2)(T^2 - 3)$  as

$$r_1 = \sqrt{2}, \quad r_2 = -\sqrt{2}, \quad r_3 = \sqrt{3}, \quad r_4 = -\sqrt{3},$$

then the Galois group of  $(T^2 - 2)(T^2 - 3)$  over  $\mathbf{Q}$  becomes the following subgroup of  $S_4$ :

$$(2.2) \quad (1), \quad (12), \quad (34), \quad (12)(34).$$

Numbering the roots of  $f(T)$  in different ways can identify the Galois group with different subgroups of  $S_n$ .

**Example 2.5.** Renaming  $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$  in this order as  $r_2, r_4, r_3, r_1$  identifies the Galois group of  $T^4 - 2$  over  $\mathbf{Q}$  with the subgroup of  $S_4$  in Table 3, which is not the same subgroup of  $S_4$  in Table 2.

Automorphism	1	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
Permutation	(1)	(1243)	(14)(23)	(1342)	(14)	(13)(24)	(23)	(12)(34)

TABLE 3.

**Example 2.6.** If we label  $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$  in this order as  $r_2, r_4, r_1, r_3$  then the Galois group of  $(T^2 - 2)(T^2 - 3)$  over  $\mathbf{Q}$  turns into the following subgroup of  $S_4$ :

$$(2.3) \quad (1), \quad (13), \quad (24), \quad (13)(24).$$

This is not the same subgroup as (2.2).

In general, associating to each  $\sigma$  in the Galois group of  $f(T)$  over  $K$  its permutation on the roots of  $f(T)$ , viewed as a permutation of the subscripts of the roots when we list them as  $r_1, \dots, r_n$ , is a homomorphism from the Galois group to  $S_n$ . This homomorphism is injective since its kernel is trivial: an element of the Galois group that fixes each  $r_i$  is the identity on the splitting field. Thinking about the Galois group of a polynomial with degree  $n$  as a subgroup of  $S_n$  is the original viewpoint of Galois. (The description of Galois theory in terms of field automorphisms is due to Dedekind and, with more abstraction, Artin.)

Two different choices for indexing the roots of  $f(T)$  can lead to different subgroups of  $S_n$ , but they will be conjugate subgroups. For instance, the subgroups in Tables 2 and 3 are conjugate by the permutation  $\begin{pmatrix} 1234 \\ 2431 \end{pmatrix} = (124)$ , which is the permutation turning one indexing of the roots into the other, and the subgroups (2.2) and (2.3) are conjugate by

$\begin{pmatrix} 1234 \\ 2413 \end{pmatrix} = (1243)$ . Although the Galois group of  $f(T)$  over  $K$  does not have a canonical embedding into  $S_n$  in general, its image in  $S_n$  is well-defined *up to an overall conjugation*. For example, without fixing an indexing of the roots, it doesn't make sense to ask if a particular permutation like  $(132)$  is in the Galois group as a subgroup of  $S_n$ , but it does make sense to ask if the Galois group contains a permutation with a particular cycle type (like a 3-cycle).

We can speak about Galois groups of irreducible or reducible polynomials, like  $T^4 - 2$  or  $(T^2 - 2)(T^2 - 3)$  over  $\mathbf{Q}$ . Only for an irreducible polynomial does the Galois group have a special property, called transitivity, when we turn the Galois group into a subgroup of  $S_n$ . A subgroup  $G \subset S_n$  is called *transitive* when, for all  $i \neq j$  in  $\{1, 2, \dots, n\}$ , there is a permutation in  $G$  sending  $i$  to  $j$ .

**Example 2.7.** The subgroups of  $S_4$  in Tables 2 and 3 are transitive. This corresponds to the fact that for each pair of roots of  $T^4 - 2$  there is an element of its Galois group over  $\mathbf{Q}$  taking the first root to the second.

**Example 2.8.** The subgroup of  $S_4$  in (2.2) is not transitive since no element of the subgroup takes 1 to 3. This corresponds to the fact that an element of  $\text{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q})$  can't send  $\sqrt{2}$  to  $\sqrt{3}$ .

Being transitive is not a property of an abstract group. It is a property of subgroups of  $S_n$ .<sup>1</sup> A conjugate subgroup of a transitive subgroup of  $S_n$  is also transitive since conjugation on  $S_n$  amounts to listing the numbers from 1 to  $n$  in a different order.

**Theorem 2.9.** *Let  $f(T) \in K[T]$  be separable of degree  $n$  with Galois group  $G_f$  over  $K$ .*

- (a) *If  $f(T)$  is irreducible over  $K$  then  $|G_f|$  is divisible by  $n$ .*
- (b) *The polynomial  $f(T)$  is irreducible in  $K[T]$  if and only if  $G_f$  is a transitive subgroup of  $S_n$ .*

*Proof.* (a) For a root  $r$  of  $f(T)$  in  $K$ ,  $[K(r) : K] = n$  is a factor of the degree of the splitting field over  $K$ , which is the size of the Galois group over  $K$ .

(b) First suppose  $f(T)$  is irreducible. For two roots  $r_i$  and  $r_j$  of  $f(T)$ , we can write  $r_j = \sigma(r_i)$  for some  $\sigma$  in the Galois group of  $f(T)$  over  $K$ . Therefore the Galois group, as a subgroup of  $S_n$ , sends  $i$  to  $j$ , so it is a transitive subgroup. Now suppose  $f(T)$  is reducible (so  $n \geq 2$ ). It is a product of distinct irreducibles since it is separable. Let  $r_i$  and  $r_j$  be roots of different irreducible factors of  $f(T)$ . These irreducible factors are the minimal polynomials of  $r_i$  and  $r_j$  over  $K$ . For each  $\sigma$  in the Galois group of  $f(T)$  over  $K$ ,  $\sigma(r_i)$  has the same minimal polynomial over  $K$  as  $r_i$ , so we can't have  $\sigma(r_i) = r_j$ . Therefore, as a subgroup of  $S_n$ , the Galois group of  $f(T)$  does not send  $i$  to  $j$ , so it is not a transitive subgroup of  $S_n$ .  $\square$

### 3. THE GROUP $S_p$ AS A GALOIS GROUP

We will give a criterion that implies a Galois group of prime degree  $p$  is as large as possible, namely  $S_p$ .

**Lemma 3.1.** *In  $S_p$ , a permutation of order  $p$  is a  $p$ -cycle.*

<sup>1</sup>More generally, it is a property of groups equipped with a specific action on a set. Subgroups of  $S_n$  have a natural action on the set  $\{1, 2, \dots, n\}$ .

*Proof.* Let  $\pi \in S_p$  have order  $p$  and decompose into disjoint nontrivial cycles as  $\pi = \pi_1\pi_2 \cdots \pi_r$ , with  $n_i$  being the order of  $\pi_i$ .

Method 1: Suppose  $\pi$  is not a  $p$ -cycle. Since we're in  $S_p$ , each  $\pi_i$  is therefore a cycle of length less than  $p$ , so each  $n_i$  is less than  $p$  (in fact the length of the cycle  $\pi_i$  is  $n_i$ ). Since the order of a product of disjoint cycles is the least common multiple of the orders of the cycles,  $p = \text{lcm}(n_1, \dots, n_r)$ . However, each  $n_i$  is less than  $p$ , so not divisible by  $p$ , and therefore  $\text{lcm}(n_1, \dots, n_r)$  is not divisible by  $p$ . This is a contradiction.

Method 2: the order of  $\pi_1\pi_2 \cdots \pi_r$  is  $\text{lcm}(n_1, \dots, n_r)$ . Therefore  $p = \text{lcm}(n_1, \dots, n_r)$ . Since  $p$  is a prime number and  $n_i > 1$ , we have  $n_i = p$  for all  $i$ . Thus  $\pi$  is a product of disjoint  $p$ -cycles. Since  $\pi$  is in  $S_p$ , there can't be even two disjoint  $p$ -cycles, so  $\pi$  is a single  $p$ -cycle.  $\square$

**Theorem 3.2.** *Let  $f(T) \in \mathbf{Q}[T]$  be an irreducible polynomial of prime degree  $p$  with all but two roots in  $\mathbf{R}$ . The Galois group of  $f(T)$  over  $\mathbf{Q}$  is isomorphic to  $S_p$ .*

*Proof.* Let  $L = \mathbf{Q}(r_1, \dots, r_p)$  be the splitting field of  $f(T)$  over  $\mathbf{Q}$ . The permutations of the  $r_i$ 's by  $\text{Gal}(L/\mathbf{Q})$  provide an embedding  $\text{Gal}(L/\mathbf{Q}) \hookrightarrow S_p$  and  $|\text{Gal}(L/\mathbf{Q})|$  is divisible by  $p$  by Theorem 2.9, so  $\text{Gal}(L/\mathbf{Q})$  contains an element of order  $p$  by Cauchy's theorem. In  $S_p$ , the only permutations of order  $p$  are  $p$ -cycles (Lemma 3.1). So the image of  $\text{Gal}(L/\mathbf{Q})$  in  $S_p$  contains a  $p$ -cycle.

We may take  $L$  to be a subfield of  $\mathbf{C}$ , since  $\mathbf{C}$  is algebraically closed. Complex conjugation restricted to  $L$  is a member of  $\text{Gal}(L/\mathbf{Q})$ . Since  $f(T)$  has only two non-real roots by hypothesis, complex conjugation transposes two of the roots of  $f(T)$  and fixes the others. Therefore  $\text{Gal}(L/\mathbf{Q})$  contains a transposition of the roots of  $f(T)$ . (This is the reason for the hypothesis about all but two roots being real.)

We now show the only subgroup of  $S_p$  containing a  $p$ -cycle and a transposition is  $S_p$ , so  $\text{Gal}(L/\mathbf{Q}) \cong S_p$ . By suitable labeling of the numbers from 1 to  $p$ , we may let 1 be a number moved by the transposition, so our subgroup contains a transposition  $\tau = (1a)$ . Let  $\sigma$  be a  $p$ -cycle in the subgroup. As a  $p$ -cycle,  $\sigma$  acts on  $\{1, 2, \dots, p\}$  by a single orbit, so some  $\sigma^i$  with  $1 \leq i \leq p-1$  sends 1 to  $a$ :  $\sigma^i = (1a \dots)$ . This is also a  $p$ -cycle, because  $\sigma^i$  has order  $p$  in  $S_p$  and all elements of order  $p$  in  $S_p$  are  $p$ -cycles, so writing  $\sigma^i$  as  $\sigma$  and suitably reordering the numbers  $2, \dots, p$  (which replaces our subgroup by a conjugate subgroup), we may suppose our subgroup of  $S_p$  contains the particular transposition  $(12)$  and the particular  $p$ -cycle  $(12 \dots p)$ . For  $n \geq 2$ , it is a theorem in group theory that the particular transposition  $(12)$  and  $n$ -cycle  $(12 \dots n)$  generate  $S_n$ , so our subgroup is  $S_p$ .  $\square$

**Remark 3.3.** While  $S_p$  is generated by each transposition and  $p$ -cycle for  $p$  prime, it is not true that  $S_n$  is generated by each transposition and  $n$ -cycle for general  $n$ . For example,  $(13)$  and  $(1234)$  generate a proper subgroup of  $S_4$  (one of the subgroups of order 8).

**Example 3.4.** The polynomial  $T^3 - T - 1$  is irreducible in  $\mathbf{Q}[T]$  since it is irreducible mod 2 or since it is a cubic without a rational root. It has one real root (approximately 1.3247), and one root of a cubic is all but two roots, so its Galois group over  $\mathbf{Q}$  is isomorphic to  $S_3$ .

**Example 3.5.** The polynomials  $T^3 - 3T - 1$  and  $T^3 - 4T - 1$  are both irreducible in  $\mathbf{Q}[T]$  since they are cubics without a rational root. Each polynomial has three real roots (check!), so we can't use Theorem 3.2 to determine their Galois groups over  $\mathbf{Q}$ .

**Example 3.6.** The quintic polynomial  $T^5 - T - 1$  is irreducible in  $\mathbf{Q}[T]$  since it is irreducible mod 3. It has one root in  $\mathbf{R}$ , not all but two roots in  $\mathbf{R}$ , so Theorem 3.2 does not tell us the Galois group.

**Example 3.7.** The quintic polynomial  $T^5 - 4T - 1$  is irreducible in  $\mathbf{Q}[T]$  since it is irreducible mod 3. It has three real roots, which is all but two roots, so its Galois group over  $\mathbf{Q}$  is isomorphic to  $S_5$ .

#### 4. ALTERNATING GROUPS AND THE DISCRIMINANT

The next thing we will do with Galois groups as subgroups of  $S_n$  is determine when they lie in  $A_n$ . Without fixing a labeling of the roots of  $f(T)$ , its Galois group is determined as a subgroup of  $S_n$  only up to conjugation, but it is still meaningful to ask if the Galois group is a subgroup of  $A_n$  since  $A_n \triangleleft S_n$ . We will introduce a numerical invariant of polynomials, called the discriminant, to determine when the Galois group is in  $A_n$ .

**Definition 4.1.** For a nonconstant  $f(T) \in K[T]$  of degree  $n$  that factors over a splitting field as

$$f(T) = c(T - r_1) \cdots (T - r_n),$$

the *discriminant* of  $f(T)$  is defined to be

$$\text{disc } f = \prod_{i < j} (r_j - r_i)^2.$$

**Example 4.2.** The polynomial  $(T - 1)(T - 3)(T - 7)$  has discriminant  $2^2 \cdot 6^2 \cdot 4^2 = 2304$ .

**Example 4.3.** The discriminant of  $T^2 + aT + b = (T - r)(T - r')$  is

$$(r - r')^2 = r^2 - 2rr' + r'^2 = (r + r')^2 - 4rr' = a^2 - 4b,$$

which is the usual discriminant of a monic quadratic polynomial.<sup>2</sup>

The number  $\text{disc } f$  is nonzero if  $f(T)$  is separable and is 0 if  $f(T)$  is not separable. When  $f(T)$  is separable,  $\text{disc } f$  is a symmetric polynomial in the  $r_i$ 's, so it is fixed by  $\text{Gal}(K(r_1, \dots, r_n)/K)$  and therefore  $\text{disc } f \in K$  by Galois theory. We have  $\text{disc } f \in K$  if  $f(T)$  is not separable too, since in that case  $\text{disc } f$  is 0.

Because  $\text{disc } f$  is a symmetric polynomial in the roots of  $f(T)$ , when  $f(T)$  is monic its discriminant is a polynomial in the coefficients of  $f(T)$  (which are, up to sign, the elementary symmetric functions of the roots). In low-degree cases, explicit formulas for discriminants of some trinomials are

$$\begin{aligned} \text{disc}(T^2 + aT + b) &= a^2 - 4b, \\ \text{disc}(T^3 + aT + b) &= -4a^3 - 27b^2, \\ \text{disc}(T^4 + aT + b) &= -27a^4 + 256b^3, \\ \text{disc}(T^5 + aT + b) &= 256a^5 + 3125b^4. \end{aligned}$$

**Example 4.4.** The discriminant of  $T^3 - T - 1$  is  $-23$ , the discriminant of  $T^3 - 3T - 1$  is  $81$ , and the discriminant of  $T^3 - 4T - 1$  is  $229$ .

More generally [3, p. 41],

$$\text{disc}(T^n + aT + b) = (-1)^{n(n-1)/2} ((-1)^{n-1} (n-1)^{n-1} a^n + n^n b^{n-1}),$$

and even more generally, for  $0 < m < n$  and  $(m, n) = 1$ ,

$$\text{disc}(T^n + aT^m + b) = (-1)^{n(n-1)/2} b^{m-1} ((-1)^{n-1} m^m (n-m)^{n-m} a^n + n^n b^{n-m}).$$

<sup>2</sup>The term ‘‘discriminant’’ was introduced by J. J. Sylvester in 1851 [5, p. 406] as a type of determinant for cubic polynomials. Previously, for quadratic polynomials, it was called the polynomial’s determinant.

If  $(m, n)$  is not necessarily 1 then [4, Theorem 2]

$\text{disc}(T^n + aT^m + b) = (-1)^{n(n-1)/2} b^{m-1} ((-1)^{n/d-1} m^{m/d} (n-m)^{(n-m)/d} a^{n/d} + n^{n/d} b^{(n-m)/d})^d$ ,  
where  $d = (m, n)$ . We will not derive these formulas here.

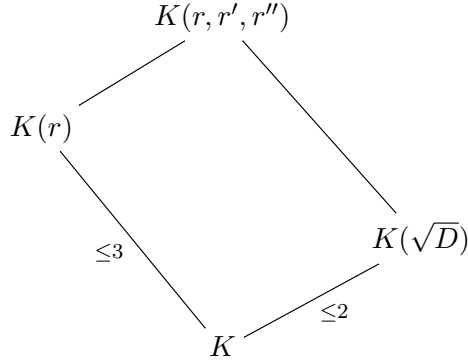
**Example 4.5.** Taking  $m = 2$  and  $n = 4$ ,

$$\text{disc}(T^4 + aT^2 + b) = 16b(a^2 - 4b)^2.$$

**Theorem 4.6.** *Let  $K$  not have characteristic 2 and let  $f(T)$  be a separable cubic in  $K[T]$  with a root  $r$  and discriminant  $D$ . The splitting field of  $f(T)$  over  $K$  is  $K(r, \sqrt{D})$ .*

Note we are *not* assuming  $f(T)$  is irreducible here.

*Proof.* The roots and the discriminant of  $f$  don't change if we multiply  $f$  by a nonzero constant, so we may assume  $f(T)$  is monic. Let  $f(T)$  have roots  $r, r',$  and  $r''$ , so the splitting field of  $f(T)$  over  $K$  is  $K(r, r', r'')$ .



Over  $K(r)$ , we can remove a linear factor and write  $f(T) = (T - r)g(T)$ , where  $g(r) \neq 0$ . Explicitly,  $g(T) = (T - r')(T - r'')$ . (Since  $f$  is monic, so is  $g$ .) By the quadratic formula on  $g(T)$ ,  $K(r, r', r'') = K(r, \sqrt{\text{disc } g})$ . It is simple to check, since  $f$  is monic, that  $\text{disc } f = g(r)^2 \text{disc } g$ . Since  $g(r) \in K^\times$ ,  $K(r, \sqrt{\text{disc } g}) = K(r, \sqrt{\text{disc } f}) = K(r, \sqrt{D})$ .  $\square$

**Theorem 4.7.** *Let  $f(T) \in K[T]$  be separable of degree  $n$ . If  $K$  does not have characteristic 2, then the embedding of the Galois group of  $f(T)$  over  $K$  into  $S_n$  as permutations of the roots of  $f(T)$  has image in  $A_n$  if and only if  $\text{disc } f$  is a square in  $K$ .*

*Proof.* Set  $\delta = \prod_{i < j} (r_j - r_i) \neq 0$ , so  $\delta \in K(r_1, \dots, r_n)$  and  $\delta^2 = \text{disc } f \in K$ . Therefore  $\text{disc } f$  is a square in  $K$  if and only if  $\delta \in K$ .

For  $\sigma \in \text{Gal}(K(r_1, \dots, r_n)/K)$ , let  $\varepsilon_\sigma = \pm 1$  be its sign as a permutation of the  $r_i$ 's. By one of the definitions of the sign of a permutation,

$$\sigma(\delta) = \prod_{i < j} (\sigma(r_j) - \sigma(r_i)) = \varepsilon_\sigma \prod_{i < j} (r_j - r_i) = \varepsilon_\sigma \delta,$$

so  $\sigma(\delta) = \pm\delta$ . Since  $\delta \neq 0$  and  $K$  doesn't have characteristic 2,  $\delta \neq -\delta$ . We have  $\sigma \in A_n$  if and only if  $\varepsilon_\sigma = 1$ , so  $\sigma \in A_n$  if and only if  $\sigma(\delta) = \delta$ . Therefore the Galois group of  $f(T)$  over  $K$  is in  $A_n$  if and only if  $\delta$  is fixed by the Galois group, which is the same as  $\delta \in K$ .  $\square$

**Remark 4.8.** Theorem 4.7 is completely false in characteristic 2: discriminants of polynomials are always squares in characteristic 2 but  $S_n$  can occur as a Galois group. For example, if  $F$  is a field of characteristic 2, then over  $F(u)$  the polynomial  $T^3 + uT + u$  is separable and irreducible with discriminant  $u^2$  (a square) and Galois group  $S_3$ .

Theorem 4.7 lets us determine the Galois groups of irreducible cubic polynomials outside of characteristic 2.

**Theorem 4.9.** *Let  $K$  not have characteristic 2 and let  $f(T)$  be a separable irreducible cubic in  $K[T]$  with Galois group  $G_f$  over  $K$ .*

- (a) *If  $\text{disc } f$  is a square in  $K$  then  $G_f \cong A_3$ .*
- (b) *If  $\text{disc } f$  is not a square in  $K$  then  $G_f \cong S_3$ .*

*Proof.* Since  $K(r)$  is inside the splitting field,  $|G_f|$  divisible by  $[K(r) : K] = 3$ . The permutations of the roots of  $f(T)$  by  $G_f$  gives an embedding of  $G_f$  into  $S_3$ , so the image is either  $A_3$  or  $S_3$  since these are the only subgroups of  $S_3$  with order divisible by 3. Theorem 4.7 says the image is in  $A_3$  (and thus equal to  $A_3$ ) if and only if  $\text{disc } f$  is a square in  $K$ .

This can also be proved by the formula for the splitting field of a cubic in Theorem 4.6. □

**Example 4.10.** In Example 3.4 we saw  $T^3 - T - 1$  has Galois group  $S_3$  over  $\mathbf{Q}$ . We can see again that  $T^3 - T - 1$  has Galois group  $S_3$  over  $\mathbf{Q}$  since its discriminant is  $-23$  (Example 4.4) and this is not a rational square.

**Example 4.11.** The Galois groups of  $T^3 - 3T - 1$  and  $T^3 - 4T - 1$  over  $\mathbf{Q}$  were left undetermined in Example 3.5 since all of their roots are real. Now we can compute the Galois groups. From Example 4.4,  $T^3 - 3T - 1$  has discriminant 81 (a square) and  $T^3 - 4T - 1$  has discriminant 229 (a prime). Therefore  $T^3 - 3T - 1$  has Galois group  $A_3$  over  $\mathbf{Q}$  and  $T^3 - 4T - 1$  has Galois group  $S_3$  over  $\mathbf{Q}$ . So although  $T^3 - 3T - 1$  and  $T^3 - 4T - 1$  both have all real roots, their Galois groups are not isomorphic. Each root of  $T^3 - 3T - 1$  generates the splitting field over  $\mathbf{Q}$ , but this is not true for a root of  $T^3 - 4T - 1$ .

**Remark 4.12.** The cubics  $T^3 - 2T + 1$  and  $T^3 - 7T - 6$  have respective discriminants 5 and  $400 = 20^2$ , but this does *not* mean their Galois groups over  $\mathbf{Q}$  are  $S_3$  and  $A_3$ . Both polynomials are reducible (factoring as  $(T - 1)(T^2 + T - 1)$  and  $(T + 1)(T + 2)(T - 3)$ ). Do not forget to check that a cubic is irreducible before you use Theorem 4.9!

The following fantastic theorem of Dedekind uses factorization of a polynomial mod  $p$  to tell us when a Galois group over  $\mathbf{Q}$  contains permutations with particular cycle structure.

**Theorem 4.13 (Dedekind).** *Let  $f(T) \in \mathbf{Z}[T]$  be monic irreducible over  $\mathbf{Q}$  of degree  $n$ . For a prime  $p$  not dividing  $\text{disc } f$ , let the monic irreducible factorization of  $f(T) \pmod p$  be*

$$f(T) \equiv \pi_1(T) \cdots \pi_k(T) \pmod p$$

*and set  $d_i = \deg \pi_i(T)$ , so  $d_1 + \cdots + d_k = n$ . The Galois group of  $f(T)$  over  $\mathbf{Q}$ , viewed as a subgroup of  $S_n$ , contains a permutation of type  $(d_1, \dots, d_k)$ .*

The best proof of Theorem 4.13 uses algebraic number theory.<sup>3</sup> More elementary proofs are in [1, pp. 398–400] and [2, pp. 302–304].

**Example 4.14.** We compute the Galois group of  $T^4 - T - 1$  over  $\mathbf{Q}$  using Theorem 4.13.

This polynomial is irreducible mod 2, so it is irreducible over  $\mathbf{Q}$ . Let its roots be  $r_1, r_2, r_3, r_4$ . The extension  $\mathbf{Q}(r_1)/\mathbf{Q}$  has degree 4, so the Galois group of  $T^4 - T - 1$  over  $\mathbf{Q}$  has order divisible by 4. Since the Galois group embeds into  $S_4$ , its size is either 4, 8, 12, or 24. The discriminant of  $T^4 - T - 1$  is  $-283$ , which is not a rational square, so the Galois group is not a subgroup of  $A_4$ . This eliminates the possibility of the Galois group

<sup>3</sup>See <https://kconrad.math.uconn.edu/blurbs/gradnumthy/galois-Q-factor-mod-p.pdf>.

having order 12, because the only subgroup of  $S_4$  with order 12 is  $A_4$ . (Quite generally, the only subgroup of index 2 in  $S_n$  is  $A_n$  for  $n \geq 2$ .) There are subgroups of  $S_4$  with orders 4, 8, and (of course) 24 outside of  $A_4$ , so no other size but 12 is eliminated yet.

Using Theorem 4.13 with  $p = 7$ , the irreducible factorization of  $T^4 - T - 1 \pmod{7}$  is

$$T^4 - T - 1 \equiv (T + 4)(T^3 + 3T^2 + 2T + 5) \pmod{7}.$$

Theorem 4.13 says the Galois group of  $T^4 - T - 1$  over  $\mathbf{Q}$  contains a permutation of the roots with cycle type  $(1, 3)$ , so the group has order divisible by 3. This proves it is  $S_4$ .

**Example 4.15.** Let  $f(T) = T^4 + 8T + 12$ . We will find its Galois group  $G_f$  over  $\mathbf{Q}$ . It can be shown that  $f(T)$  is reducible mod  $p$  for all primes  $p$ , so the reduction mod  $p$  test doesn't imply that  $f(T)$  is irreducible over  $\mathbf{Q}$ . Let's look at *how*  $f(T)$  factors into irreducibles modulo two primes:

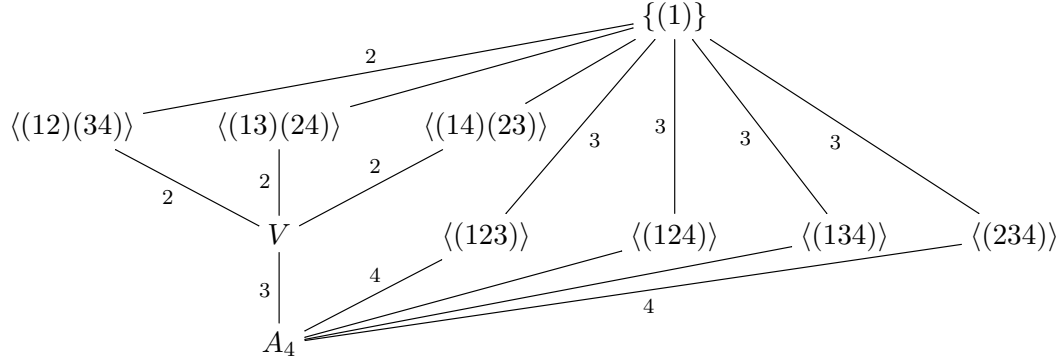
$$T^4 + 8T + 12 \equiv (T + 1)(T^3 + 4T^2 + T + 2) \pmod{5},$$

$$T^4 + 8T + 12 \equiv (T^2 + 4T + 7)(T^2 + 13T + 9) \pmod{17}.$$

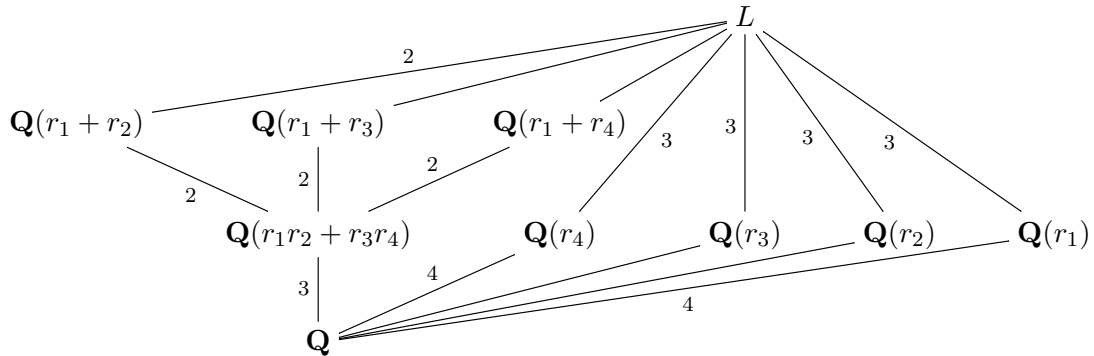
These are only consistent with  $f(T)$  being irreducible over  $\mathbf{Q}$  (why?). Thus  $4 \mid |G_f|$ .

Since  $\text{disc } f = 331776 = 576^2$  is a rational square,  $G_f \subset A_4$ . Thus  $|G_f|$  is 4 or 12. By the factorization of  $f(T)$  mod 5 above,  $G_f$  contains a permutation of the roots of  $f$  with cycle type  $(1, 3)$ , which is a 3-cycle, so  $|G_f|$  is divisible by 3, and thus  $12 \mid |G_f|$ , so  $G_f \cong A_4$ : the even permutations of the roots of  $f$  extend to automorphisms of the splitting field of  $f$  over  $\mathbf{Q}$ , while the odd permutations do not.

Let's list all the subfields of the splitting field of  $T^4 + 8T + 12$  over  $\mathbf{Q}$ . Here is the lattice (upside down) of subgroups of  $A_4$ .



The corresponding subfield lattice of  $L = \mathbf{Q}(r_1, r_2, r_3, r_4)$  is as follows.



The normal subgroups of  $A_4$  are  $\{1\}$ ,  $V$ , and  $A_4$ , so the only subfield of  $L$  that is Galois over  $\mathbf{Q}$  other than  $L$  and  $\mathbf{Q}$  is  $\mathbf{Q}(r_1r_2+r_3r_4)$ . Since  $[L : \mathbf{Q}(r_1)] = 3$  is prime and  $r_2 \notin \mathbf{Q}(r_1)$ , we have  $L = \mathbf{Q}(r_1, r_2)$ , so  $[\mathbf{Q}(r_1, r_2) : \mathbf{Q}] = 12$ .

The sums  $r_1+r_2$ ,  $r_1+r_3$ , and  $r_1+r_4$  are roots of  $T^6 - 48T^2 - 64$  (check!) and  $r_1r_2+r_3r_4$  is a root of  $T^3 - 48T - 64$ . Roots of  $T^3 - 48T - 64$  are squares of roots of  $T^6 - 48T^2 - 64$ . It is left to the reader to check that  $r_1r_2+r_3r_4 = (r_1+r_2)^2 = (r_3+r_4)^2$ .

**Remark 4.16.** Our Galois group computations have an application to “nonexistent fields.” If  $r$  is a root of  $T^4 + 8T + 12$  then  $[\mathbf{Q}(r) : \mathbf{Q}] = 4$  and there is *no* quadratic field in  $\mathbf{Q}(r)$ : such a field would, by the Galois correspondence, lead to a subgroup of index 2 in  $A_4$  and there is no such subgroup. More generally, for  $k \geq 2$  there are complex numbers that have degree  $2^k$  over  $\mathbf{Q}$  and the field they generate over  $\mathbf{Q}$  contains no quadratic extension of  $\mathbf{Q}$ .

**Example 4.17.** Let’s determine the Galois group of  $T^5 - T - 1$  over  $\mathbf{Q}$ , which was left unresolved in Example 3.6. Its irreducible factorization mod 2 is

$$T^5 - T - 1 = (T^2 + T + 1)(T^3 + T^2 + 1) \pmod{2}.$$

Because the polynomial is irreducible over  $\mathbf{Q}$ , 5 divides the size of the Galois group. From the mod 2 factorization, the Galois group contains a permutation of the roots with cycle type  $(2, 3)$ , which has order 6, so the Galois group has size divisible by  $5 \cdot 6 = 30$ . Since the Galois group is a subgroup of  $S_5$ , its size is either 30, 60, or 120.

It turns out that there is no subgroup of  $S_5$  with order 30 and the only subgroup of order 60 is  $A_5$ . The discriminant of  $T^5 - T - 1$  is  $2869 = 19 \cdot 151$ , which is not a rational square, so the Galois group is not in  $A_5$  by Theorem 4.7. Therefore the Galois group is  $S_5$ .

Theorem 3.2 gave us a sufficient condition for an irreducible in  $\mathbf{Q}[T]$  of prime degree  $p$  to have Galois group  $S_p$ : all but 2 roots are real. This condition does not apply to  $T^3 - 4T - 1$  or  $T^5 - T - 1$ , although by Examples 4.11 and 4.17 their Galois groups over  $\mathbf{Q}$  are  $S_3$  and  $S_5$ . Using Theorem 4.13, there is a different “all but 2 roots” hypothesis that implies a Galois group is  $S_p$ .

**Corollary 4.18.** *Let  $f(T) \in \mathbf{Z}[T]$  be monic irreducible over  $\mathbf{Q}$  of prime degree  $p$ . If there is a prime number  $\ell$  not dividing  $\text{disc } f$  such that  $f(T) \pmod{\ell}$  has all but two roots in  $\mathbf{F}_\ell$ , then the Galois group of  $f(T)$  over  $\mathbf{Q}$  is isomorphic to  $S_p$ .*

*Proof.* The proof of Theorem 3.2 can be used again except for the step explaining why the Galois group of  $f(T)$  over  $\mathbf{Q}$  contains a transposition. In Theorem 3.2 this came from the use of complex conjugation to transpose two non-real roots, assuming there are only two non-real roots. We aren’t assuming that now. By hypothesis the factorization of  $f(T) \pmod{\ell}$  has all linear factors except for one quadratic irreducible factor. Therefore Theorem 4.13 says the Galois group contains a permutation of the roots with cycle type  $(1, 1, \dots, 1, 2)$ , which is a transposition in  $S_p$ .  $\square$

**Example 4.19.** From Examples 3.4 and 4.11, the polynomials  $T^3 - T - 1$  with discriminant  $-23$  and  $T^3 - 4T - 1$  with discriminant  $229$  each have Galois group  $S_3$  over  $\mathbf{Q}$ . We can check this again with Corollary 4.18:  $T^3 - T - 1 \pmod{5}$  has one root in  $\mathbf{F}_5$  and  $T^3 - 4T - 1 \pmod{2}$  has one root in  $\mathbf{F}_2$ .

**Example 4.20.** In Example 3.7 we saw  $T^5 - 4T - 1$  has Galois group  $S_5$  over  $\mathbf{Q}$  because it has all but two real roots. We can also compute the Galois group with Corollary 4.18: the discriminant is  $-259019$  (a negative prime number) and  $T^5 - 4T - 1 \pmod{19}$  has all but two roots in  $\mathbf{F}_{19}$ .

**Example 4.21.** Returning to Example 4.17, we can show the Galois group over  $\mathbf{Q}$  of  $T^5 - T - 1$  is  $S_5$  in another way:  $T^5 - T - 1$  has discriminant  $2869 = 19 \cdot 151$  and by a computer search  $T^5 - T - 1 \pmod{163}$  has all but two roots in  $\mathbf{F}_{163}$ .

**Remark 4.22.** We can't use Corollary 4.18 to show  $T^4 - T - 1$  has Galois group  $S_4$  over  $\mathbf{Q}$  (Example 4.14) since 4 is not prime.

**Example 4.23.** For a prime  $p$ , the polynomial  $T^p - T - 1$  is irreducible mod  $p$ , so it is irreducible over  $\mathbf{Q}$  and its Galois group over  $\mathbf{Q}$  is a subgroup of  $S_p$  that contains a  $p$ -cycle by the first paragraph of the proof of Theorem 3.2. Using algebraic number theory,<sup>4</sup> it can be shown that this Galois group is generated by transpositions, so the Galois group is  $S_p$ .

If we seek an analogue of Theorem 3.2 for a Galois group to be isomorphic to  $A_p$ , using 3-cycles in place of transpositions, there is no analogue since an irreducible polynomial over  $\mathbf{Q}$  can't have all but three roots in  $\mathbf{R}$  (the number of non-real roots is always even). But  $f(T) \pmod{\ell}$  could have all but three roots in  $\mathbf{F}_\ell$  for some  $\ell$ ! This suggests the next result.

**Corollary 4.24.** *Let  $f(T) \in \mathbf{Z}[T]$  be monic irreducible over  $\mathbf{Q}$  of prime degree  $p \geq 3$  with disc  $f$  a perfect square. If there is a prime number  $\ell$  not dividing disc  $f$  such that  $f(T) \pmod{\ell}$  has all but three roots in  $\mathbf{F}_\ell$ , then the Galois group of  $f(T)$  over  $\mathbf{Q}$  is isomorphic to  $A_p$ .*

*Proof.* Let  $G$  be the Galois group, so  $G$  is a subgroup of  $A_p$  since disc  $f$  is a square. The Galois group has order divisible by  $p$ , so it contains a  $p$ -cycle. From the factorization of  $f(T) \pmod{\ell}$  and Theorem 4.13,  $G$  contains a 3-cycle. It is a theorem of C. Jordan that for every prime  $p \geq 3$ , each  $p$ -cycle and 3-cycle in  $S_p$  generate  $A_p$ , so  $G \cong A_p$ .  $\square$

**Example 4.25.** The polynomial  $T^5 + 20T + 16$  has discriminant  $2^{16}5^6$ . It is irreducible mod 3, so it's irreducible over  $\mathbf{Q}$ . Modulo 7, its irreducible factorization is

$$T^5 + 20T + 16 \equiv (T - 4)(T - 5)(T^3 + 2T^2 + 5T + 5) \pmod{7}.$$

All but three roots are in  $\mathbf{F}_7$ , so  $T^5 + 20T + 16$  has Galois group over  $\mathbf{Q}$  isomorphic to  $A_5$ .

In Table 4 are the trinomial polynomials whose Galois group over  $\mathbf{Q}$  has been computed by the methods of this section.

$f(T)$	Galois group over $\mathbf{Q}$
$T^3 - T - 1$	$S_3$
$T^3 - 3T - 1$	$A_3$
$T^3 - 4T - 1$	$S_3$
$T^4 - T - 1$	$S_4$
$T^4 + 8T + 12$	$A_4$
$T^5 - T - 1$	$S_5$
$T^5 - 4T - 1$	$S_5$
$T^5 + 20T + 16$	$A_5$

TABLE 4.

The sufficient conditions for  $f(T)$  to have Galois group  $S_p$  in Corollary 4.18 and  $A_p$  in Corollary 4.24 are also necessary, by the following hard theorem of Chebotarev that serves as a converse to Dedekind's Theorem 4.13.

<sup>4</sup>See Step 2 of the proof of the theorem in [https://kconrad.math.uconn.edu/blurbs/gradnumthy/galois\\_selmerpoly.pdf](https://kconrad.math.uconn.edu/blurbs/gradnumthy/galois_selmerpoly.pdf).

**Theorem 4.26** (Chebotarev). *Let  $f(T) \in \mathbf{Z}[T]$  be monic irreducible over  $\mathbf{Q}$  of degree  $n$ . If an automorphism in the Galois group of  $f(T)$  over  $\mathbf{Q}$  permutes the roots of  $f(T)$  with cycle type  $(d_1, \dots, d_k)$ , then there are infinitely many primes  $\ell$  not dividing disc  $f$  such that the monic irreducible factorization of  $f(T) \bmod \ell$  is*

$$f(T) \equiv \pi_1(T) \cdots \pi_k(T) \bmod \ell,$$

where the  $\pi_i(T)$ 's are distinct and  $d_i = \deg \pi_i(T)$ .

Chebotarev's theorem actually says more (the set of such  $\ell$  has a positive density related to conjugacy classes in the Galois group), but the version above is enough for us here.

**Corollary 4.27.** *If  $f(T) \in \mathbf{Z}[T]$  is monic irreducible of prime degree  $p$  with Galois group over  $\mathbf{Q}$  isomorphic to  $S_p$  (resp.,  $A_p$ ) then there are infinitely many primes  $\ell$  not dividing disc  $f$  such that  $f(T) \bmod \ell$  has all but two roots (resp., all but three roots) in  $\mathbf{F}_\ell$ .*

*Proof.* The group  $S_p$  has a 2-cycle and the group  $A_p$  for  $p > 2$  has a 3-cycle. Therefore Theorem 4.26 implies there are infinitely many primes  $\ell$  not dividing disc  $f$  such that  $f(T) \bmod \ell$  is an irreducible quadratic times linear polynomials in the first case and is an irreducible cubic times linear polynomials in the second case.  $\square$

For example,  $T^5 - T - 1 \bmod \ell$  has all but two roots in  $\mathbf{F}_\ell$  when  $\ell = 163, 193, 227, 307, \dots$  (there is no simple pattern to this list, but it continues indefinitely),  $T^5 - 4T - 1 \bmod \ell$  has all but two roots in  $\mathbf{F}_\ell$  when  $\ell = 19, 23, 83, 97, \dots$ , and  $T^5 + 20T + 16$  has all but three roots in  $\mathbf{F}_\ell$  when  $\ell = 7, 11, 17, 23, \dots$ . In practice, it is easy to prove when a monic irreducible in  $\mathbf{Z}[T]$  with prime degree  $p$  has Galois group  $A_p$  or  $S_p$  over  $\mathbf{Q}$  by searching for a prime  $\ell$  such that Corollary 4.18 or 4.24 applies. There are extensions of these ideas to polynomials of nonprime degree, so verifying an irreducible polynomial of degree  $n$  has Galois group over  $\mathbf{Q}$  that is isomorphic to  $S_n$  or  $A_n$  in practice is easy.

Proving a Galois group is small (not  $S_n$  or  $A_n$ ) is a completely separate matter, which we will not discuss here.

**Corollary 4.28.** *Let  $f(T) \in \mathbf{Z}[T]$  be monic irreducible over  $\mathbf{Q}$ . The Galois group of  $f(T)$  over  $\mathbf{Q}$  has an element of prime order  $p$  if and only if there is a prime  $\ell$  not dividing disc  $f$  such that the irreducible factors of  $f(T) \bmod \ell$  have degree 1 and  $p$ . If there is one such  $\ell$  then there are infinitely many such  $\ell$ .*

*Proof.* A permutation has prime order  $p$  if and only if its cycle type is  $(1, \dots, 1, p, \dots, p)$ . Theorem 4.13 says that if there is a prime  $\ell$  not dividing disc  $f$  such that all irreducible factors of  $f(T) \bmod \ell$  have degree 1 or  $p$  then there is a permutation in the Galois group of  $f(T)$  over  $\mathbf{Q}$  whose cycles have length 1 and  $p$ , so it has order  $p$ . Conversely, if a permutation of order  $p$  occurs in the Galois group of  $f(T)$  over  $\mathbf{Q}$  then Theorem 4.26 says that there are infinitely many primes  $\ell$  not dividing disc  $f$  such that all the irreducible factors of  $f(T) \bmod \ell$  have degree 1 or  $p$ .  $\square$

Corollary 4.28 suggests a way to find prime factors of the order of the Galois group  $G$  of  $f(T)$  over  $\mathbf{Q}$ : factor  $f(T) \bmod \ell$  for many primes  $\ell$  and see which factorizations have degrees  $1, \dots, 1, p, \dots, p$  for a prime  $p$ . Such  $p$  divide  $|G|$ , and all prime factors of  $|G|$  arise in this way. To find all prime factors of  $|G|$  in this way, we want an effective Chebotarev theorem: a bound  $B$  such that all degree-types occur modulo the primes  $\ell \leq B$ . You can find such results by googling "effective chebotarev," but the versions I have seen describe  $B$  in terms of the splitting field, e.g., using  $|G|$ , and this isn't good if we don't yet know  $|G|$ .

## REFERENCES

- [1] D. Cox, “Galois Theory,” Wiley, Hoboken, NJ, 2004.
- [2] N. Jacobson, “Basic Algebra I,” 2nd ed., Freeman, 1985.
- [3] P. Samuel, “Algebraic Theory of Numbers,” Dover, 2008.
- [4] R. Swan, *Factorization of Polynomials over Finite Fields*, Pacific J. Math. **12** (1962), 1099–1106.
- [5] J. J. Sylvester, *On a remarkable discovery in the theory of canonical forms and of hyperdeterminants*, Philosophical Magazine **2** (1851), 391–410. URL <https://babel.hathitrust.org/cgi/pt?id=mdp.39015024087580&view=1up&seq=1039>.