

# RECOGNIZING GALOIS GROUPS $S_n$ AND $A_n$

KEITH CONRAD

## 1. INTRODUCTION

If  $f(X) \in K[X]$  is a separable irreducible polynomial of degree  $n$  and  $G_f$  is its Galois group over  $K$  (the Galois group of the splitting field of  $f(X)$  over  $K$ ), then the group  $G_f$  can be embedded into  $S_n$  by writing the roots of  $f(X)$  as  $r_1, \dots, r_n$  and identifying each automorphism in the Galois group with the permutation it makes on the  $r_i$ 's.

Whether thinking about  $G_f$  as a subgroup of  $S_n$  in this way really helps us compute  $G_f$  depends on how well we can conjure up elements of  $G_f$  as permutations of the roots.

For instance, when  $K = \mathbf{Q}$  there is a fantastic theorem of Dedekind that tells us about the Galois group as a permutation group if we factor  $f(X) \bmod p$  for different prime numbers  $p$ . If

$$f(X) \equiv \pi_1(X) \cdots \pi_m(X) \bmod p$$

where the  $\pi_i(X)$ 's are distinct monic irreducibles mod  $p$ , with  $d_i = \deg \pi_i$ , then Dedekind's theorem says there is an element in the Galois group of  $f(X)$  over  $\mathbf{Q}$  that permutes the roots with cycle type  $(d_1, \dots, d_m)$ .

**Example 1.1.** Let  $f(X) = X^6 + X^4 + X + 3$ . Here are the factorizations of  $f(X)$  modulo the first few primes:

$$\begin{aligned} f(X) &\equiv (X+1)(X^2+X+1)(X^3+X+1) \bmod 2, \\ f(X) &\equiv X(X+2)(X^4+X^3+2X^2+2X+2) \bmod 3, \\ f(X) &\equiv (X+3)^2(X^4+4X^3+3X^2+X+2) \bmod 5, \\ f(X) &\equiv (X^2+5X+2)(X^4+2X^3+3X^2+2X+5) \bmod 7, \\ f(X) &\equiv (X+6)(X^5+5X^4+4X^3+9X^2+X+6) \bmod 11, \\ f(X) &\equiv (X^2+8X+1)(X^2+9X+10)(X^2+9X+12) \bmod 13. \end{aligned}$$

From the factorizations modulo 2 and 3, Dedekind's theorem says  $G_f$ , as a subgroup of  $S_6$ , contains permutations of cycle type  $(1, 2, 3)$  and  $(1, 1, 4)$  (namely a 4-cycle). The factorization mod 5 does not tell us anything by Dedekind's theorem, because there is a multiple factor. From the later primes, we see  $G_f$  contains permutations of the roots with cycle types  $(2, 4)$ ,  $(1, 5)$  (a 5-cycle), and  $(2, 2, 2)$ .

Actually, we need to know first that  $f(X)$  is irreducible over  $\mathbf{Q}$  before any of that is justified. Irreducibility can be read off from the factorizations above, since a factorization over  $\mathbf{Q}$  can be scaled to a (monic) factorization over  $\mathbf{Z}$ . If  $f(X)$  were reducible over  $\mathbf{Q}$  it would have a factor in  $\mathbf{Z}[X]$  of degree 1, 2, or 3. From  $p = 7$  (or 13) we see there is no linear factor. From  $p = 11$  there is no quadratic factor. From  $p = 3$  (or 5 or 7 or 11 or 13) there is no cubic factor.

It is important to remember that Dedekind's theorem does not correlate any information about the permutations coming from different primes. For instance, permutations in  $G_f$

associated to the factorizations mod 2 and 11 each fix a root, but we can't be sure if these are the same root.

**Example 1.2.** Let  $f(X) = X^6 + 15X^2 + 18X - 20$ . Here are its irreducible factorizations modulo small primes:

$$\begin{aligned} f(X) &\equiv X^2(X+1)^4 \pmod{2}, \\ f(X) &\equiv (X^2+1)^3 \pmod{3}, \\ f(X) &\equiv X(X+3)^5 \pmod{5}, \\ f(X) &\equiv (X+5)(X+6)(X^2+5X+5)^2 \pmod{7}, \\ f(X) &\equiv (X+1)(X^5+10X^4+X^3+10X^2+5X+2) \pmod{11}, \\ f(X) &\equiv (X^3+2X^2+4X+10)(X^3+11X^2+11) \pmod{13}. \end{aligned}$$

It is left to the reader to explain from these why  $f(X)$  is irreducible over  $\mathbf{Q}$ . We can't determine anything about  $G_f$  from the factorizations at any  $p \leq 7$  since they all have multiple factors. From  $p = 11$  and  $p = 13$ , we see  $G_f$  contains permutations of the roots of  $f(X)$  with cycle types  $(1, 5)$  (a 5-cycle) and  $(3, 3)$ .

Once we know some cycle types of permutations in  $G_f$ , as a subgroup of  $S_n$ , we can often prove the Galois group has to be  $S_n$  or  $A_n$  because  $G_f$  is a transitive subgroup of  $S_n$  (any root of  $f(X)$  can be carried to any other root by the Galois group, which is what being transitive means) and there are several theorems in group theory saying a transitive subgroup of  $S_n$  containing certain cycle types has to be  $A_n$  or  $S_n$ .

## 2. STATEMENT OF THEOREMS AND SOME APPLICATIONS

Here are theorems giving conditions under which a transitive subgroup of  $S_n$  is  $A_n$  or  $S_n$ .

**Theorem 2.1.** *For  $n \geq 2$ , a transitive subgroup of  $S_n$  that contains a transposition and a  $p$ -cycle for some prime  $p > n/2$  is  $S_n$ .*

**Theorem 2.2.** *For  $n \geq 3$ , a transitive subgroup of  $S_n$  that contains a 3-cycle and a  $p$ -cycle for some prime  $p > n/2$  is  $A_n$  or  $S_n$ .*

By Bertrand's postulate (proved by Chebyshev), for  $n \geq 2$  there is a prime  $p$  such that  $n/2 < p \leq n$ , so every  $S_n$  for  $n \geq 2$  contain a  $p$ -cycle for some prime  $p > n/2$ . Since a cycle of odd length is even, every  $A_n$  for  $n \geq 3$  contains a  $p$ -cycle prime for some prime  $p > n/2$ . Therefore the hypotheses of Theorem 2.1 and 2.2 are not restrictive.

We will illustrate these theorems with examples in  $\mathbf{Q}[X]$ . Whether or not the discriminant of an irreducible polynomial in  $\mathbf{Q}[X]$  is a square tells us when its Galois group is in  $A_n$  or not. So if we want to check whether the Galois group is big ( $A_n$  or  $S_n$ ), first determine if the discriminant is a square, which tells us which group ( $A_n$  or  $S_n$ ) to aim for. Theorems 2.1 and 2.2 are directly applicable to Galois groups over  $\mathbf{Q}$  using Dedekind's theorem.

**Example 2.3.** Let  $f(X) = X^6 + X^4 + X + 3$ , as in Example 1.1. Its discriminant is  $-13353595 < 0$ , which is not a square and we'll show the Galois group over  $\mathbf{Q}$  is  $S_6$ . We saw in Example 1.1 that the Galois group contains permutations of the roots with cycle types  $(1,2,3)$ ,  $(1,1,4)$ ,  $(2,4)$ ,  $(1,5)$ , and  $(2,2,2)$ . In particular, there is a 5-cycle in the Galois group. By Theorem 2.1 (with  $n = 6$  and  $p = 5$ ),  $G_f = S_6$  provided we show  $G_f$  contains a transposition. None of the cycle types we found is a transposition, but the third power of

a permutation with cycle type  $(1, 2, 3)$  is a transposition (why?). Therefore  $G_f$  contains a transposition.

The cycle types we used,  $(1, 2, 3)$  and  $(1, 5)$ , came from the factorizations of  $f(X) \bmod 2$  and  $f(X) \bmod 11$ . In principle the “right” way to show  $G_f$  contains a transposition is not by the trick of cubing a permutation of type  $(1, 2, 3)$ , but by finding a prime  $p$  at which  $f(X) \bmod p$  has distinct irreducible factors of degree 2, 1, 1, 1, and 1. You’ll have to wait a while for that. Such a factorization occurs for the first time when  $p = 311$ :

$$f(X) \equiv (X^2 + 50X + 142)(X + 7)(X + 118)(X + 203)(X + 244) \pmod{311}.$$

**Example 2.4.** Let  $f(X) = X^7 - X - 1$ . The first few factorizations of  $f(X) \bmod p$  are as follows:

$$\begin{aligned} f(X) &\equiv X^7 + X + 1 \pmod{2}, \\ f(X) &\equiv (X^2 + X + 2)(X^5 + 2X^4 + 2X^3 + 2X + 1) \pmod{3}, \\ f(X) &\equiv (X + 3)(X^6 + 2X^5 + 4X^4 + 3X^3 + X^2 + 2) \pmod{5}. \end{aligned}$$

Since  $f(X) \bmod 2$  is irreducible,  $f(X)$  is irreducible over  $\mathbf{Q}$ . Its discriminant is  $-776887 < 0$ , so we’ll try to show the Galois group over  $\mathbf{Q}$  is  $S_7$ . The mod 2 factorization says the Galois group contains a 7-cycle on the roots. The factorization mod 3 gives us a permutation in the Galois group of cycle type  $(2, 5)$ , whose 5th power is a transposition, so  $G_f = S_7$  by Theorem 2.1. (The first prime  $p$  such that  $f(X) \bmod p$  has a factorization of “transposition type”  $(2, 1, 1, 1, 1, 1)$  is 191, so it’s faster to use the power method on the  $(2, 5)$ -permutation to find a transposition in the Galois group.)

**Example 2.5.** Let  $f(X) = X^7 - 7X + 10$ . Here are factorizations mod 2 and 3:

$$\begin{aligned} f(X) &\equiv X(X + 1)^2(X^2 + X + 1)^2 \pmod{2}, \\ f(X) &\equiv (X^2 + 2X + 2)(X^5 + X^4 + 2X^3 + 2X + 2) \pmod{3}. \end{aligned}$$

We can’t say anything from the mod 2 factorization since there’s a multiple factor. The mod 3 factorization gives us a permutation in the Galois group over  $\mathbf{Q}$  of cycle type  $(2, 5)$ , whose square is a 5-cycle and whose fifth power is a transposition. Since  $5 > 7/2$ , this means  $G_f = S_7$  by Theorem 2.1.

But wait: we forgot to check  $f(X)$  is irreducible in  $\mathbf{Q}[X]$ . In fact it isn’t. One factor is  $X^2 - X + 2$  and it’s left to the reader to find the second factor by division. So our Galois group arguments were bogus. You must always check first that your polynomial is irreducible.

**Example 2.6.** Let  $f(X) = X^6 + 15X^2 + 18X - 20$ . From Example 1.2, we know  $f(X)$  is irreducible over  $\mathbf{Q}$  and its factorization mod 11 gives us a 5-cycle in the Galois group over  $\mathbf{Q}$ . Since  $\text{disc } f = 2893401000000 = 1701000^2$ ,  $G_f \subset A_6$ . To prove  $G_f = A_6$  using Theorem 2.2, we just need to find a 3-cycle. The factorization mod 13 in Example 1.2 gives us an element of order 3, but not a 3-cycle. We get a 3-cycle in  $G_f$  from the factorization mod 17:

$$f(X) \equiv (X + 2)(X + 9)(X + 10)(X^3 + 13X^2 + 7X + 15) \pmod{17}.$$

**Example 2.7.** Let  $f(X) = X^7 - 56X + 48$ . It’s irreducible mod 5, so  $f(X)$  is irreducible over  $\mathbf{Q}$  and  $G_f$  contains a 7-cycle on the roots. The discriminant is  $265531392^2$ , so  $G_f \subset A_7$ . Theorem 2.2 tells us  $G_f = A_7$  once we know there is a 3-cycle in  $G_f$ . The factorization

$$f(X) \equiv (X^2 + 9X + 5)(X^2 + 17X + 17)(X^3 + 20X^2 + 18X + 3) \pmod{23}$$

gives us a permutation in the Galois group of cycle type  $(2, 2, 3)$ , whose square is a 3-cycle.

### 3. PROOFS OF THEOREMS

*Proof.* (of Theorem 2.1) This argument is adapted from [1]. Let  $G$  be a transitive subgroup of  $S_n$  containing a transposition and a  $p$ -cycle for some prime  $p > n/2$ . For  $a$  and  $b$  in  $\{1, 2, \dots, n\}$ , write  $a \sim b$  if  $(ab) \in G$  (that is, either  $a = b$  so  $(ab)$  is the identity permutation, or  $a \neq b$  and there is a 2-cycle in  $G$  exchanging  $a$  and  $b$ ). Let's check  $\sim$  is an equivalence relation on  $\{1, 2, \dots, n\}$ .

Reflexive: Clearly  $a \sim a$  for any  $a$ .

Symmetric: This is clear.

Transitive: Suppose  $a \sim b$  and  $b \sim c$ . We want to show  $a \sim c$ . We may assume  $a, b$ , and  $c$  are distinct (otherwise the task is trivial). Then  $(ab)$  and  $(bc)$  are transpositions in  $G$ , so  $(ab)(bc)(ab) = (ac)$  is in  $G$ .

Our goal is to show there is only one equivalence class: if all elements of  $\{1, 2, \dots, n\}$  are equivalent to each other than any transposition  $(ab)$  lies in  $G$ , so  $G = S_n$ .

The group  $G$  preserves the equivalence relation: if  $a \sim b$  then  $ga \sim gb$  for any  $g$  in  $G$ . (For  $g \in G$  and  $1 \leq i \leq n$ , we write  $gi$  for  $g(i)$ .) This is clear if  $a = b$ . If  $a \neq b$  then  $(ab)$  is a transposition in  $G$  and its conjugate  $g(ab)g^{-1}$  is also in  $G$ . It's a general fact that the conjugate of any cyclic permutation is a cycle of the same length. More precisely, for any cyclic permutation  $(a_1 a_2 \dots a_k)$  in  $S_n$  and any  $\pi$  in  $S_n$ ,

$$\pi(a_1 a_2 \dots a_k)\pi^{-1} = (\pi a_1 \pi a_2 \dots \pi a_k).$$

Therefore  $g(ab)g^{-1} = (ga gb)$ , so the transposition  $(ga gb)$  is also in  $G$ .

Break up  $G$  into equivalence relations for  $\sim$ . Let  $[a]$  be the equivalence class of  $a$ . The group  $G$  acts on equivalence classes by  $g[a] = [ga]$ ; we already showed this is well-defined. Since  $G$  acts transitively on  $\{1, 2, \dots, n\}$ , it acts transitively on the equivalence classes: for any  $a$  and  $b$ , there is some  $g \in G$  such that  $ga = b$ , so  $g[a] = [b]$ . Moreover, the action of  $g$  provides a function  $[a] \rightarrow [b]$  given by  $x \mapsto gx$  (if  $x \sim a$  then  $gx \sim ga = b$ ) and the action of  $g^{-1}$  provides a function  $[b] \rightarrow [a]$  given by  $x \mapsto g^{-1}x$  that is inverse to the action of  $g$  sending  $[a]$  to  $[b]$ . Therefore all equivalence classes have the same size.

Let  $M$  be the common size of the equivalence classes and let  $N$  be the number of equivalence classes, so  $n = MN$ . Since  $G$  contains a transposition and the two numbers in a transposition in  $G$  are equivalent,  $M \geq 2$ . We want to show  $N = 1$ . By hypothesis there is a  $p$ -cycle in  $G$ . Call it  $g$ . The group  $\langle g \rangle$  has order  $p$ , so the orbits of  $\langle g \rangle$  on the equivalence classes each have size 1 or  $p$ . (When a finite group acts on a set, all orbits have order dividing the order of the group, by the orbit-stabilizer formula.) If some orbit has size  $p$ , say  $[a], [ga], \dots, [g^{p-1}a]$ , then  $N \geq p$  so

$$n = MN \geq Mp \geq 2p > 2\frac{n}{2} = n,$$

a contradiction. Therefore all  $\langle g \rangle$ -orbits have size 1, so for every  $a \in \{1, 2, \dots, n\}$  we have  $[ga] = [a]$ , which means  $a \sim ga$  for all  $a$ . Since  $g$  is a  $p$ -cycle, by relabeling (which amounts to replacing  $G$  with a conjugate subgroup in  $S_n$ ) we can assume  $g = (12 \dots p)$ . That means  $2 = g(1), 3 = g(2), \dots, p = g(p-1)$ , so because  $a \sim ga$  for all  $a$  we have

$$1 \sim 2 \sim 3 \sim \dots \sim p,$$

so the equivalence class [1] has size at least  $p$ . Therefore  $M \geq p$  so

$$n = MN \geq pN > \frac{n}{2}N,$$

hence  $N < 2$ , so  $N = 1$ . ■

*Proof.* (of Theorem 2.2) Let  $G$  be a transitive subgroup of  $S_n$  containing a 3-cycle and a  $p$ -cycle for some prime  $p > n/2$ . Since any transitive subgroup of  $S_3$  is  $A_3$  or  $S_3$ , we can assume  $n \geq 4$ . Then  $p > n/2 \geq 2$ , so  $p$  is odd. A cycle with an odd number of terms has even sign (think about 3-cycles, or even more simple 1-cycles!), so any  $p$ -cycle is even. We will show  $G$  contains a set of 3-cycles that generates  $A_n$ , so  $G$  is  $A_n$  or  $S_n$ .

For  $a$  and  $b$  in  $\{1, 2, \dots, n\}$ , set  $a \sim b$  if  $a = b$  or there is a 3-cycle  $(abc)$  in  $G$ . We will check this is an equivalence relation on  $\{1, 2, \dots, n\}$

Reflexive: Clear.

Symmetric: If  $a \neq b$  and  $a \sim b$  then some 3-cycle  $(abc)$  is in  $G$ , so its inverse  $(abc)^{-1} = (bac)$  is in  $G$ , so  $b \sim a$ .

Transitive: This will be trickier than the transitivity proof in Theorem 2.1 because we will have 5 parameters to keep track of and need to worry about the possibility that some of them may be equal.

Suppose  $a \sim b$  and  $b \sim c$ . We want to show  $a \sim c$ . It is easy if any of these three numbers are equal, so we may assume  $a, b$ , and  $c$  are all distinct. Then  $(abd)$  and  $(bce)$  are in  $G$  for some  $d$  and  $e$  with  $d \neq a$  or  $b$  and  $e \neq b$  or  $c$ . It might happen that  $d = e$  or  $d = c$  or  $e = a$ . To show  $G$  contains a 3-cycle  $(ac*)$ , we need to take separate cases to deal with these possible equalities.

Case 1:  $a, b, c, d, e$  are distinct. The conjugate

$$(bce)(abd)(bce)^{-1} = (bce)(abd)(bec) = (acd)$$

is in  $G$ , so  $a \sim c$ .

Case 2:  $d = e$ , so  $a, b, c, d$  are distinct. Here  $(abd)$  and  $(bcd)$  are in  $G$ , so  $G$  contains

$$(bcd)(abd)(bcd)^{-1} = (bcd)(abd)(bdc) = (acb).$$

Case 3:  $d = c$  and  $e \neq a$ , so  $a, b, c, e$  are distinct. Here  $(abc)$  and  $(bce)$  are in  $G$ , so  $G$  contains

$$(bce)(abc)(bce)^{-1} = (bce)(abc)(bec) = (ace).$$

Case 4:  $d \neq c$  and  $e = a$ , so  $a, b, c, d$  are distinct. Here  $(abd)$  and  $(bca)$  are in  $G$ , so  $G$  contains

$$(abd)(bca)^{-1} = (abd)(bac) = (acd).$$

Case 5:  $d = c$  and  $e = a$ , so we only have three numbers  $a, b$ , and  $c$  with  $(abc)$  and  $(bca)$  in  $G$ . Of course  $(bca) = (abc)$ , so all we have to work with here is  $(abc)$ . Invert it:  $G$  contains

$$(abc)^{-1} = (acb).$$

Thus  $a \sim c$ , so  $\sim$  is transitive.

This equivalence relation is preserved by  $G$ : if  $g \in G$  and  $a \sim b$  then  $ga \sim gb$ . This is obvious if  $a = b$ . If  $a \neq b$  then some 3-cycle  $(abc)$  is in  $G$ , so the conjugate

$$g(abc)g^{-1} = (ga \ gb \ gc)$$

is in  $G$ . Therefore  $ga \sim gb$ .

For  $a \in \{1, 2, \dots, n\}$ , write  $[a]$  for the equivalence class of  $a$ . The group  $G$  acts on equivalence classes by  $g[a] = [ga]$  and all equivalence classes have the same size. Let  $M$  be

the common size of the equivalence classes and  $N$  be the number of equivalence classes, so  $n = MN$ . Since  $G$  contains a 3-cycle and the numbers in a 3-cycle in  $G$  are equivalent,  $M \geq 3$ .

Let  $g \in G$  be a  $p$ -cycle, so the orbits of  $\langle g \rangle$  on the equivalence classes have size 1 or  $p$ . We will show all the sizes are 1. If there is an orbit of size  $p$  then  $N \geq p$ , so

$$n = MN \geq Mp \geq 3p > 3\frac{n}{2} > n,$$

a contradiction. Thus  $\langle g \rangle$  fixes all the equivalence classes, so  $a \sim ga$  for all  $a \in \{1, 2, \dots, n\}$ . Therefore, as in the proof of Theorem 2.1,  $M \geq p$  so

$$n = MN \geq pN > \frac{n}{2}N,$$

so  $N < 2$ , which means  $N = 1$ . Thus any  $a \neq b$  belongs to a 3-cycle  $(abc)$  in  $G$ . This is *not* saying all 3-cycles are in  $G$ : it says for any two distinct numbers  $a$  and  $b$  in  $\{1, 2, \dots, n\}$  there is some 3-cycle  $(abc) \in G$ . We will show the 3-cycles

$$(123), (124), \dots, (12n)$$

are all in  $G$ , and this set of 3-cycles is known to generate  $A_n$ .

If  $n = 3$  then the hypothesis that  $G$  contains a 3-cycle means  $G$  contains  $A_3$ , so we may assume  $n \geq 4$ .

Since  $1 \sim 2$  there is some  $(12c)$  in  $G$  where  $c$  is not 1 or 2. For every  $d \neq c, 1$ , or  $2$ , we want to show  $(12d) \in G$ . Since  $c \sim d$ , some 3-cycle  $(cde)$  is in  $G$ , where  $e$  is not  $c$  or  $d$ . The numbers 1, 2,  $c$ , and  $d$  are distinct by hypothesis, as are  $c, d$ , and  $e$ , but  $e$  might equal 1 or 2. To show  $(12d)$  is in  $G$  we take cases.

Case 1:  $e \neq 1$  or  $2$ , so 1, 2,  $c, d, e$  are distinct. The conjugate

$$(cde)(12c)(cde)^{-1} = (cde)(12c)(ced) = (12d)$$

is in  $G$ .

Case 2:  $e = 1$ . Here  $(12c)$  and  $(cd1)$  are in  $G$ , so  $G$  contains

$$(cd1)(12c) = (12d).$$

Case 3:  $e = 2$ . Here  $(12c)$  and  $(cd2)$  are in  $G$ , so  $G$  contains

$$(12c)(cd2)^{-1} = (12c)(c2d) = (12d).$$

■

Here are some other theorems in group theory in the spirit of Theorem 2.1.

**Theorem 3.1.** *For  $n \geq 2$ , a transitive subgroup of  $S_n$  that contains a transposition and an  $(n-1)$ -cycle is  $S_n$ .*

*Proof.* Let  $G$  be a transitive subgroup of  $S_n$  containing an  $(n-1)$ -cycle. By suitable labeling,  $G$  contains the particular  $(n-1)$ -cycle  $\sigma = (12 \dots n-1)$ . This cycle fixes  $n$  and moves all the other numbers around. We can't say for sure which transpositions are in  $G$ , only that some transposition is in it. Say  $(ab)$  is a transposition in  $G$ . For any  $g \in G$ ,  $G$  contains the conjugate transposition  $g(ab)g^{-1} = (ga gb)$ . Since  $G$  is a transitive subgroup, there is a  $g \in G$  such that  $gb = n$ . Necessarily  $ga \neq gb$ , so  $G$  contains a transposition  $\tau = (in)$  where  $i = ga \in \{1, 2, \dots, n-1\}$ .

For  $j = 1, 2, \dots, n$ ,  $G$  contains the transposition

$$\sigma^j \tau \sigma^{-j} = (\sigma^j(i) \sigma^j(n)) = (i+j n).$$

Therefore  $G$  contains  $(1n), (2n), \dots, (n-1n)$ . For any  $i \neq j$  that also don't equal  $n$ ,  $G$  contains

$$(in)(jn)(in) = (ij).$$

Therefore  $G$  contains all transpositions, so  $G = S_n$ . ■

It's left to the reader to return to Examples 2.3 and 2.4 and solve them using Theorem 3.1 in place of Theorem 2.1. For large  $n$ , Theorem 2.1 is more flexible than Theorem 3.1 since it only requires you find a  $p$ -cycle with some prime  $p > n/2$  rather than specifically an  $(n-1)$ -cycle.

**Theorem 3.2.** *For  $n \geq 2$ , a transitive subgroup of  $S_n$  that contains a transposition and has a generating set of cycles of prime order is  $S_n$ .*

*Proof.* See [3, pp. 139–140]. ■

Theorem 3.2 appears to be less simple to apply to specific examples than the other theorems, because it requires knowing a generating set of cycles of prime order in the Galois group. It's one thing to know a few cycle types in  $G_f$ , by Dedekind's theorem, but how could we know generating cycle types in  $G_f$  before we know  $G_f$ ? Using a lot more mathematics, there really are situations where Theorem 3.2 can be applied to compute Galois groups over  $\mathbf{Q}$ . For instance, Osada [2] showed the Galois group of  $X^n - X - 1$  over  $\mathbf{Q}$  is  $S_n$  using the special case of Theorem 3.2 for cycles of prime order 2: a transitive subgroup of  $S_n$  generated by transpositions must be  $S_n$ .

#### REFERENCES

- [1] P. X. Gallagher, The large sieve and probabilistic Galois theory, in "Analytic Number Theory," Proc. Symp. Pure Math. **24**, Amer. Math. Soc., Providence, 1973, 91–101.
- [2] H. Osada, *The Galois groups of the polynomials  $X^n + aX^l + b$* , J. Number Theory **25** (1987), 230–238.
- [3] J-P. Serre, "Lectures on the Mordell–Weil Theorem," F. Vieweg & Sohn, Braunschweig, 1989.