THE GALOIS GROUP OF $x^n - x - 1$ OVER $\mathbf{Q}$

KEITH CONRAD

1. Introduction

In 1956, Selmer [4] proved $x^n - x - 1$ is irreducible for all $n \geq 2$. Its splitting field over $\mathbf{Q}$ turns out to have Galois group S_n. This provides an example that's easy to remember of a family of irreducible polynomials over $\mathbf{Q}$ of each degree with a full symmetric group as Galois group. We will use algebraic number theory (inertia groups) to compute the Galois group of the splitting field of $x^n - x - 1$ over $\mathbf{Q}$ and look briefly at the ring of integers generated by a root of $x^n - x - 1$.

2. Galois group of $x^n - x - 1$ over $\mathbf{Q}$

The Galois group of the splitting field of $x^n - x - 1$ over $\mathbf{Q}$ was first determined for *all* $n \geq 2$ by Nart and Vila [2].

Theorem 2.1 (Nart, Vila)**.** *The splitting field of $x^n - x - 1$ over $\mathbf{Q}$ has Galois group S_n.*

This was later proved independently by Osada [3]. While we focus on $x^n - x - 1$ for concreteness, both [2] and [3] were concerned with Galois groups of more general irreducible trinomials.

Proof. Our proof will be given in two steps. The first step is group theory, and the second step is the algebraic number theory that justifies the application of the first step to $x^n - x - 1$.

Step 1: The Galois group of the splitting field of $x^n - x - 1$ over $\mathbf{Q}$ embeds into S_n by acting on the roots of $x^n - x - 1$ and fixing a labeling of the roots. This action makes the Galois group a transitive subgroup of S_n since $x^n - x - 1$ is irreducible over $\mathbf{Q}$. We will prove a sufficient condition for a *transitive* subgroup G of S_n to be S_n for each $n \geq 2$: G is generated by transpositions. We will show this in two ways.

Our first proof is taken from [3, Lemma 5]. Relabeling the roots if necessary, we can assume that G contains the transposition (12). The transpositions $(12), (13), \ldots, (1n)$ are known to be a generating set for S_n. We will show they are all in G. The result is obvious if $n = 2$, so take $n \geq 3$. Pick k from 3 to n. We want to show $(1k) \in G$. Since G acts transitively on $\{1, 2, \ldots, n\}$ and is assumed to be generated by transpositions, there are transpositions $\tau_1, \tau_2, \ldots, \tau_r$ in G such that

$$(\tau_r \cdots \tau_2 \tau_1)(2) = k,$$

and we can assume each τ_i moves the number $(\tau_{i-1} \cdots \tau_1)(2)$ since otherwise τ_i could be removed from the equation without affecting its validity. Set $j_1 = \tau_1(2)$ and $j_i = (\tau_i \tau_{i-1} \cdots \tau_1)(2)$ for $i = 2, \ldots, r-1$, so $\tau_1 = (2, j_1)$, $\tau_2 = (j_1, j_2), \ldots, \tau_{r-1} = (j_{r-2}, j_{r-1})$, and $\tau_r = (j_{r-1}, k)$. with each τ_i being an actual transposition (not the identity). The path we get from 2 to k by applying these transpositions is

$$2 \to j_1 \to j_2 \to \cdots \to j_{r-2} \to k.$$

We can assume no j_i is 2, since otherwise $(\tau_r \cdots \tau_{i+1})(2) = k$ and we could drop the transpositions $\tau_1, \ldots, \tau_i$ from consideration.

Set $g := \tau_r \cdots \tau_2 \tau_1 \in G$. If none of $j_1, \ldots, j_{r-1}$ are 1, then $g(1) = 1$ so G contains $g(12)g^{-1} = (g(1), g(2)) = (1k)$. If some j_i is 1 then $\tau_{i+1}(1) = \tau_{i+1}(j_i) = j_{i+1}$. Set $h = \tau_r \tau_{r-1} \cdots \tau_{i+1} \in G$, so $h(1) = k$. Also $h(2) = 2$ since none of $j_i, j_{i+1}, \ldots, j_{r-1}, k$ equal 2. Then G contains $h(12)h^{-1} = (h(1), h(2)) = (k, 2) = (2k)$ so G also contains $(12)(2k)(12) = (1k)$.

Our second proof that $G = S_n$ is taken from [5, Lemma 1, §10.2], where it is shown more generally that a transitive subgroup of S_n that contains a transposition and is generated by cycles of prime order must be all of S_n. We specialize to the case that the generating cycles are 2-cycles.

We will prove by induction that for all $m \leq n$ there is a subset $M \subset \{1, 2, \ldots, n\}$ of size m such that $\mathrm{Sym}(M) \subset G$, where $\mathrm{Sym}(M)$ is the subgroup of S_n consisting of the permutations that fix the elements in the complement of M, so $\mathrm{Sym}(M) \cong S_m$. The case $m = 1$ is obvious since the identity of S_n belongs to G. Suppose now that $1 \leq m < n$ and we have such a subset M of size m. We will show by contradiction that there is a transposition $\tau = (ij)$ in G such that $i \in M$ and $j \notin M$. If there were no such transposition in G, then every transposition (ij) in G has i and j both in M or both not in M. Thus all transpositions in G preserve M and its complement, so G preserves M and its complement (the group G is generated by transpositions), but that contradicts the transitivity of G on $\{1, 2, \ldots, n\}$. Therefore some $(ij) \in G$ has $i \in M$ and $j \notin M$. Let $M' = M \cup \{j\}$, so $|M'| = m + 1 \leq n$. Let $H = \langle \mathrm{Sym}(M), (ij) \rangle$, so $H \subset G$ and $\mathrm{Sym}(M) \subset H \subset \mathrm{Sym}(M')$. Since $\mathrm{Sym}(M)$ links every element of M to i, and (ij) links i to j, H links every element of M' to j. Therefore H acts transitively on M', so $[H : \mathrm{Stab}_H(j)] = |M'| = m + 1$. What is $\mathrm{Stab}_H(j)$? Each element of this stabilizer group fixes the complement of M' as well as j, so $\mathrm{Stab}_H(j) \subset \mathrm{Sym}(M)$. The reverse containment is obvious, so $\mathrm{Stab}_H(j) = \mathrm{Sym}(M)$. Thus $|H| = |\mathrm{Sym}(M)|(m + 1) = (m + 1)!$, so $H = \mathrm{Sym}(M')$. That proves $\mathrm{Sym}(M') \subset G$.

Step 2: We will now show that the Galois group of the splitting field of $x^n - x - 1$ over $\mathbf{Q}$ is generated by transpositions. Then Step 1 implies the group is S_n.

Let K be the splitting field of $x^n - x - 1$ over $\mathbf{Q}$ and $G = \mathrm{Gal}(K/\mathbf{Q})$. By algebraic number theory, G is generated by its nontrivial inertia subgroups $I(\mathfrak{p}|p)$, where $\mathfrak{p}$ runs over the nonzero prime ideals of $\mathcal{O}_K$ that ramify over $\mathbf{Q}$. We will show each nontrivial $I(\mathfrak{p}|p)$ is generated by a transposition of the roots of $x^n - x - 1$. Suppose $\sigma \in I(\mathfrak{p}|p)$ and σ is nontrivial. There is some root α of $x^n - x - 1$ such that $\sigma(\alpha) \neq \alpha$. But also $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{p}$ because $\sigma \in I(\mathfrak{p}|p)$, so $x^n - x - 1$ has $\alpha \bmod \mathfrak{p}$ as a multiple root in characteristic p. We will show $x^n - x - 1 \bmod p$ has at most one multiple root, and its multiplicity as a root is 2. Then for each root β of $x^n - x - 1$ *other* than α or $\sigma(\alpha)$, the reduction $\beta \bmod \mathfrak{p}$ is a simple root of $x^n - x - 1 \bmod p$, so the necessary congruence $\sigma(\beta) \equiv \beta \bmod \mathfrak{p}$ implies $\sigma(\beta) = \beta$. Thus, as a permutation of the roots of $x^n - x - 1$, σ is the transposition $(\alpha\ \sigma(\alpha))$.

Suppose r is a multiple root of $x^n - x - 1$ in characteristic p. Then r is a root of $x^n - x - 1$ and its derivative: $r^n - r - 1 = 0$ and $nr^{n-1} - 1 = 0$ in characteristic p. The second equation implies $n \neq 0$ and $r^n = r/n$ in characteristic p, so $r/n = r + 1$. Thus $(1/n - 1)r = 1$, so $(1 - n)r = n$. Thus $n - 1 \neq 0$ and $r = n/(1 - n) \in \mathbf{F}_p$. Therefore the only possible multiple root of $x^n - x - 1$ in characteristic p is $n/(1 - n) \bmod p$. To see that it is a root with multiplicity two, if it is a multiple root at all, consider the second derivative $n(n - 1)x^{n-2}$, whose value at r is $n(n - 1)r^{n-2}$, which is nonzero in characteristic p. Thus r is a root of $x^n - x - 1 \bmod p$ with multiplicity two. □

3. The ring of integers associated to $x^n - x - 1$

It is a basic result in algebraic number theory that if $f(x) \in \mathbf{Z}[x]$ is monic irreducible with squarefree discriminant and root α then $\mathbf{Z}[\alpha]$ is the ring of integers of $\mathbf{Q}(\alpha)$. If $2 \leq n \leq 100$ then the discriminant of $x^n - x - 1$ is squarefree, and based on a probabilistic heuristic, Boyd, Martin, and Thom [1] conjecture that the density of n such that $\mathrm{disc}(x^n - x - 1)$ is squarefree is around 99.34%.

The first n for which the discriminant of $x^n - x - 1$ is not squarefree is $n = 130$, when the discriminant is divisible by 83^2 (and not by the square of other primes).

Theorem 3.1. *If $\alpha^{130} - \alpha - 1 = 0$ then $\mathbf{Z}[\alpha]$ is not the ring of integers of $\mathbf{Q}(\alpha)$.*

Proof. We modify an argument by David Speyer [6] in reply to a math.stackexchange question for the case $n = 257$.

Let $K = \mathbf{Q}(\alpha)$. If its ring of integers $\mathcal{O}_K$ is $\mathbf{Z}[\alpha] \cong \mathbf{Z}[x]/(x^{130} - x - 1)$, then for each prime p the decomposition of (p) in $\mathcal{O}_K$ matches how $x^{130} - x - 1 \bmod p$ factors. For the prime 83, PARI gives an irreducible factorization

$$x^{130} - x - 1 \equiv (x - 8)^2(x - 20)f_{22}(x)f_{42}(x)f_{63}(x) \bmod 83,$$

so the ideal (83) in $\mathcal{O}_K$ would be ramified: divisible in $\mathcal{O}_K$ by the square of a prime ideal with residue field degree 1.

However, the ideal (83) in $\mathcal{O}_K$ turns out to be unramified. We will prove this by p-adic methods. The polynomial $x^{130} - x - 1$ has 3 roots in $\mathbf{Q}_{83}$: approximately $8 + 12 \cdot 83 + \ldots$, $8 + 74 \cdot 83 + \ldots$, and $20 + 30 \cdot 83 + \ldots$ with PARI. Therefore the ideal (83) in $\mathcal{O}_K$ has three prime ideal factors of residue field degree 1 and three others with residue field degree 22, 42, and 63, so (83) in $\mathcal{O}_K$ is unramified. Due to this mismatch, $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$. □

References

[1] D. W. Boyd, G. Martin, M. Thom, Squarefree Values of Trinomial Discriminants, *LMS J. Comput. Math.* **18** (2015), 148–169, http://arxiv.org/pdf/1402.5148v1.pdf.

[2] E. Nart and N. Vila, Equations of the type $X^n + aX + b$ with absolute Galois group S_n, *Rev. Univ. Santander* **2** (1979), 821–825.

[3] H. Osada, The Galois groups of the polynomials $x^n + ax^l + b$, *J. Number Theory* **25** (1987), 230–238.

[4] E. Selmer, On the Irreducibility of Certain Trinomials, *Math. Scand.* **4** (1956), 287–302.

[5] J-P. Serre, "Lectures on the Mordell–Weil Theorem," 2nd ed., Vieweg, Braunschweig, 1990.

[6] D. Speyer, answer to https://math.stackexchange.com/questions/82258.