Inverse Galois Problems for S_p and Abelian Groups

LU Junyu

February 18, 2021

In this short article, we construct a field extension E over the rationals $\mathbb{Q}$ with Galois group $\mathrm{Gal}(E/\mathbb{Q}) \cong S_p$, p prime, or $\mathrm{Gal}(E/\mathbb{Q})$ any finite abelian group. If it is the latter case, the extension E is so constructed that it is a subfield of some cyclotomic extension.

Lemma 0.1. *Let p be a prime. If a subgroup G of the symmetric group S_p contains a transposition and a p-cycle, then G is the whole group S_p.*

Proof. After renaming elements, we can assume the transposition $\sigma = (1\ 2)$. We can write a p-cycle τ as $\tau = (1\ i_2\ \cdots\ i_p)$ after rotations on τ, if necessary. Now $i_j = 2$ for some $2 \leq j \leq p$, and then $\tau^{j-1} = (1\ 2\ \cdots)$ is also a p-cycle. After renaming elements, we get $\sigma = (1\ 2), \tau = (1\ 2 \cdots\ p)$ and then σ, τ generate S_p. $\square$

Theorem 0.2. *Let $f \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree p, p prime. If f has precisely two complex roots and $p-2$ real roots, then the Galois group of f is isomorphic to the symmetric group S_p.*

Proof. Fix an algebraic closure $\overline{\mathbb{Q}} \subset \mathbb{C}$. Let E be the splitting field of f over $\mathbb{Q}$ and α one of the roots. Note that $E/\mathbb{Q}$ is a Galois extension and $\mathrm{Gal}(E/\mathbb{Q})$ is (isomorphic to) a subgroup of S_p. Since f is irreducible, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ and so $p \mid [E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})|$. By Cauchy's theorem (or Sylow's theorem), $\mathrm{Gal}(E/\mathbb{Q})$ contains an element of order p. But the only elements in S_p of order p are p-cycles. Hence $\mathrm{Gal}(E/\mathbb{Q})$ contains a p-cycle. Note the complex conjugation exchanges the two complex roots of f and fixes reals, so it is also an element in $\mathrm{Gal}(E/\mathbb{Q})$ and is a transposition indeed. Since $\mathrm{Gal}(E/\mathbb{Q})$ contains a transposition and a p-cycle, $\mathrm{Gal}(E/qq)$ is the whole group S_p by the lemma above. $\square$

Example 0.3. Probably the simplest example of a polynomial over $\mathbb{Q}$ with Galois group S_n $(n > 1)$ is $x^n - x - 1$. This is proved in a paper by H. Osada in J. Number Theory, 25(1987), 230–238.

Example 0.4. Let $p \geq 5$ be a prime. Define $f(x), g(x) \in \mathbb{Q}[x]$ as

$$g(x) = (x^4+4)(x-2)(x-4)\cdots(x-2(p-2)),\ f(x) = g(x) - 2.$$

If we draw f, g on the plane, we see that $g(x)$ interests x-axis at $2, 4, \ldots, 2(p-2)$ and that $g(x) > 2$ for $x = 3, 5, 7, \ldots, 2p-1$. The graph of f is obatined by shifting down 2 units of that of g. Therefore, f has precisely $p-2$ real roots. Write $f(x)$ as

$$f(x) = x^p + d_{p-1}x^{p-1} + \cdots + d_0.$$

Then $d_0 = 4k - 2$ for some nonzero integer k and hence $2^2 \nmid d_0$ while it is easily seen that $2 \mid d_j$ for $j = 0, \ldots, d-1$. By Eisenstein's criterion, f is irreducible. And Theorem 0.2 says the Galois group of f over $\mathbb{Q}$ is S_p.

Now we move the the case where we want the Galois group be finite abelian. Recall from the classification on finite abelian groups, we can write a finite abelian group G as

$$G \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r},$$

where p_i are primes not necessarily distinct and e_r are positive integers. And for two rings R_1, R_2, we have

$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

The following theorem is a special case of Dirichlet's theorem about primes in arithmetic progression. To be self-contained, we prove it using cyclotomic polynomials

Theorem 0.5. *Let $n > 1$ be a positive integer. Then there are infinitely many primes p such that $p \equiv 1 \pmod{n}$.*

Proof. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. We first note that $\Phi_1(0) = -1$ and $\Phi_n(0) = 1$ for $n \geq 2$. This can be easily done by induction on $n \geq 2$. Hence the constant term for $\Phi_n(x)$ is 1 when $n > 1$.

Claim: Let p be a prime. If $p \mid \Phi_n(x_0)$ for some integer x_0, then $p \mid n$ or $p \equiv 1 \pmod{n}$.

Proof of Claim: Note that $p \mid \Phi_n(x_0) \mid x_0^n - 1$. We must have $p \nmid x_0$. Let k be the order of x_0 in $(\mathbb{Z}/p)^*$. Since $|(\mathbb{Z}/p)^*| = p-1$, we have $k \mid (p-1)$ and so $p \equiv 1 \pmod{k}$. Since $x_0^n \equiv 1 \pmod{p}$, we have $k \mid n$. If $k = n$, then $p \equiv 1 \pmod{n}$ and we are done. If $k < n$, then $p \mid x_0^k - 1$ implies $p \mid \Phi_d(x_0)$ for some $d \leq k < n$. Since p also divides $\Phi_n(x_0)$, x_0 is a double root of $x^n - 1$ when we regard it as a polynomial in $\mathbb{F}_p[x]$. This can only happen if p divides n.

Assume that there are only finitely many primes $p \equiv 1 \pmod{n}$. We define

$$N = n \prod_{p \text{ prime}, \, p \equiv 1 \pmod{n}} p.$$

Then $N > n > 1$ is well-defined. Consider the monic polynomial $\Phi_n(x)$. We have $\Phi_n(N^k) > 1$ for some large enough integer k. Let p be a prime divisor of $\Phi_n(N^k)$. Note the constant term of $\Phi_n(x)$ is 1 and then $\Phi_n(N^k) - 1$ is a multiply of N. But $p \mid \Phi_n(N^k)$ implies $p \nmid \Phi_n(N^k) - 1$ and $p \nmid N$ and $p \nmid n$. It follows from the claim that $p \equiv 1 \pmod{n}$. On the other hand $p \nmid N$ means p is not any of the primes in the definition of N. Contradiction. $\square$

We need one lemma more before going to construct abelian extensions.

Lemma 0.6. *Let G be a finite abelian group. Then there is a surjective homomorphism*

$$\phi : (\mathbb{Z}/n)^* \to G$$

for some positive integer n.

Proof. By the classification of finite abelian groups, we can write

$$G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r,$$

where $\mathbb{Z}/n_i$ is a cyclic group of order n_i.

Since there are infinitely many primes $p \equiv 1 \pmod{n_i}$, we can choose distinct primes p_i such that $p_i = n_i m_i + 1$ for some positive integer m_i for $i = 1, \ldots, r$. Now $(\mathbb{Z}/p_i)^*$ is a cyclic group of order $n_i m_i$ and hence there is a surjection $\phi_i : (\mathbb{Z}/p_i)^* \to \mathbb{Z}/n_i$. Collecting all the surjections, we can define a surjective homomorphism

$$\phi : (\mathbb{Z}/p_1)^* \times \cdots \times (\mathbb{Z}/p_r)^* \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r,\ (a_1, \ldots, a_r) \mapsto (\phi_1(a_1), \ldots, \phi_r(a_r)).$$

Note that $(\mathbb{Z}/p_1)^* \times \cdots \times (\mathbb{Z}/p_r)^* = (\mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_r)^*$ and that by Chinese Remainder Theorem $\mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_r \cong \mathbb{Z}/(p_1 \ldots p_r)$. We get a surjection $\phi' : (\mathbb{Z}/(p_1 \ldots p_r))^* \to G$. $\square$

Theorem 0.7. *Let G be a finite abelian group. Then there is a subfield E of $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root for some positive integer n, such that E is Galois over $\mathbb{Q}$ and Gal$(E/\mathbb{Q}) \cong G$.*

Proof. By the lemma above, we can find a positive integer n such that there is a surjection

$$\phi : (\mathbb{Z}/n)^* \to G.$$

Then the kernel $H = \ker(\phi)$ is a normal subgroup.

Now let $E = \mathbb{Q}(\zeta_n)^H$ be the fixed subfield of H. Since H is normal, by the fundamental theorem about Galois theory, $E/\mathbb{Q}$ is Galois and

$$\text{Gal}(E/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\text{Gal}(\mathbb{Q}(\zeta_n)/E) \cong (\mathbb{Z}/n)^*/H \cong G.$$

$\square$

Note the difference between this theorem and Kronecker-Weber theorem. Kronecker-Weber theorem says *every* abelian extension over the rationals can be embedded into a cyclotomic extension, while we we constructed *some* extension with Galois group a finite abelian group G that happens to embed into a cyclotomic extension.

Theorem 0.8 (Kronecker-Weber)**.** *Let $E/\mathbb{Q}$ be a finite Galois extension such that Gal$(E/\mathbb{Q})$ is abelian. Then there is a root of unity ζ such that $E \subset \mathbb{Q}(\zeta)$.*

Now we prove a special case of Kronecker-Weber theorem.