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.

Through all this article, ζ_n is a primitive n-th root and $\Phi_n(x)$ is the n-th cyclotomic polynomial, where n is a positive integer.

Lemma 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. □

Theorem 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. □

Example 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 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 obtained 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 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 and 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 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 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 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 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 $E \subset \mathbb{Q}(\zeta)$.*

And we will prove a special case of Kronecker-Weber theorem.

Theorem 9. *Let $p > 2$ be a prime. Then the only quadratic subfield over $\mathbb{Q}$ of $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root, is $M = \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$ and $M = \mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$.*

Note this theorem leads immediately a corollary about quadratic extensions.

Corollary 10. *Let E be a quadratic Galois extension over $\mathbb{Q}$. Then E embeds to some cyclotomic extension.*

Proof. Note that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ and $i \in \mathbb{Q}(\zeta_4)$. We fix an algebraic closure $\mathbb{Q} \subset E \subset \overline{\mathbb{Q}} \subset \mathbb{C}$. A quadratic extension E over $\mathbb{Q}$ looks like $E = \mathbb{Q}(\sqrt{d})$ from some square-free integer d. We can do inductions on the prime factors of

$$d = \pm \prod_{p_i | n} p_i,$$

with the observation that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ if $m \mid n$. $\square$

We need a technical lemma before proving Theorem 9.

Lemma 11. *Let $p > 2$ be a prime and g a generator of $\mathbb{F}_p^*$. Then the number of solutions of the equation $x^2 + gy^2 = r$ over $\mathbb{F}_p$ for some $r \in \mathbb{F}_p$ is given as*

$$|\{(x,y) \in \mathbb{F}_p^2 | x^2 + gy^2 = r\}| = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 4 \textit{ and } r = 0, \\ p+1 & \textit{if } p \equiv 1 \pmod 4 \textit{ and } r \neq 0, \\ 2p-1 & \textit{if } p \equiv 3 \pmod 4 \textit{ and } r = 0, \\ p-1 & \textit{if } p \equiv 3 \pmod 4 \textit{ and } r \neq 0. \end{cases}$$

Proof. Consider the case $p \equiv 1 \pmod 4$. The equation $x^2 + gy^2 = 0$ has the trivial solutions only. If not, say $y \neq 0$, then $g = -(x^2/y^2) = -(x/y)^2$ but this says $g^{(p-1)/2} = (x/y)^{p-1} = 1$ contradicting to the assumption that g is a generator of $\mathbb{F}_p^*$. Therefore, the quadratic polynomial $T^2 + g \in \mathbb{F}_p[T]$ has no solution in $\mathbb{F}_p$. Let $\alpha = \sqrt{-g}$ be one of its roots. Then $\mathbb{F}_p[\alpha]/\mathbb{F}_p$ is a Galois extension of degree 2. The norm of an element $a + b\alpha \in \mathbb{F}_p[\alpha]$ is given as $\mathrm{N}(a + b\alpha) = a^2 + b^2 g$. The norm mapping $\mathrm{N} : \mathbb{F}_p[\alpha]^\times \to \mathbb{F}_p \times$ is a group homomorphism. The map is surjective since $\mathrm{N}(\alpha) = g$ and the kernel is of size $|\mathbb{F}_p[\alpha]^\times|/|\mathbb{F}_p^\times| = (p^2-1)/(p-1) = p+1$. Namely, for each $r \in \mathbb{F}_p^*$ we will get $p+1$ solutions $x + y\alpha$ with $\mathrm{N}(x + y\alpha) = x^2 + y^2\alpha = r$.

Now consider the case $p \equiv 3 \pmod 4$. In this case, -1 is not a quadratic residue and so $-g$ is, say $-g = \beta^2$ for some $\beta \in \mathbb{F}_p^*$. We have $x^2 + gy^2 = (x - \beta y)(x + \beta y) = 0$ if and only if $x = \pm\beta y$ and so we get $2p-1$ solutions. Now consider the polynomial $T^2 - g \in \mathbb{F}_p[x]$ and let $\alpha = \sqrt{g}$ be one of its roots and $\gamma \in \mathbb{F}_p$ with $\gamma^2 = -1$. Then the norm map

$$\mathrm{N} : \mathbb{F}_p[\alpha] \to \mathbb{F}_p, x + y\gamma\alpha \mapsto x^2 - y^2\gamma^2 g = x^2 + y^2 g$$

is surjective since $\mathrm{N}(\gamma\alpha) = g$. The restriction of N on the non-zero-norm element is again a group homomorphism. The size of kernel is then $(p^2 - (2p-1))/(p-1) = p-1$. Namely, there are precisely $p-1$ solutions for $\mathrm{N}(x + y\gamma\alpha) = x^2 + gy^2 = r$ for each $r \neq 0$. $\square$

Proof of Theorem 9. Note that $(\mathbb{Z}/q)^* = \mathbb{F}_p^*$ is of order $p - 1 = 2m$ for some positive integer m. Let g be a generator of $\mathbb{F}_p^*$ and ζ a primitive p-th root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/q)^*$ and is generated by σ who is defined by $\sigma(\zeta) = \zeta^g$. Hence $\langle\sigma^2\rangle$ is a subgroup of index 2 in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

The fixed subfield $E = \mathbb{Q}(\zeta)^{\langle\sigma^2\rangle}$ is then a quadratic extension over $\mathbb{Q}$. Note that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian and every subgroup is normal. Therefore, $E/\mathbb{Q}$ is Galois.

Note that elements

$$\alpha = \sigma^2(\zeta) + \cdots + \sigma^{p-1}(\zeta) = \zeta^{g^2} + \zeta^{g^4} + \cdots + \zeta^{g^{p-1}} = \sum_{i=1}^{\frac{p-1}{2}} \zeta^{g^{2i}} = \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}}$$

$$\beta = \sigma(\alpha) = \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i+1}}$$

are invariant under σ^2. Because the terms ζ^j in α, β run out all possibilities of the form ζ^j for some $0 < j < p$ as g is a generator, we see either $\alpha \notin \mathbb{Q}$ or $\beta \notin \mathbb{Q}$, otherwise, ζ would satisfy a polynomial of degree $< p-1$ in $\mathbb{Q}[x]$. Without loss of generality, we assume $E = \mathbb{Q}(\alpha)$.

We want to construct a quadratic with α, β its roots:

$$x^2 - (\alpha+\beta)x + \alpha\beta.$$

Note that

$$\alpha + \beta = \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}} + \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i+1}} = \sum_{i=1}^{p-1} \zeta^i = (\sum_{i=0}^{p-1} \zeta^i) - 1 = \Phi_p(\zeta) - 1 = -1.$$

Hence indeed $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. And then

$$\alpha\beta = (\sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}})(\sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2j+1}}) = \sum_{i=0}^{\frac{p-3}{2}} \sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2i}+g^{2j+1}} = \sum \zeta^{x^2+gy^2},$$

where $x = g^i$ and $y = g^j$ for $i, j = 0, \ldots, (p-3)/2$ and the number of such term $\zeta^{x^2+gy^2}$ is $(p-1)^2/4$. Note that

$$(g^i)^2 = g^{2i} = g^{2i+(p-1)} = (g^{i+\frac{p-1}{2}})^2.$$

Extending the range of $x = g^i$ and $y = g^j$ to $i, j = 0, \ldots, p-2$, we get

$$4\alpha\beta = \sum_{x,y \in \mathbb{F}_p^*} \zeta^{x^2+gy^2}.$$

First consider the case $p \equiv 1 \pmod 4$. By the lemma above, we can count the number of solutions of $x^2 + gy^2 = r$. But we need to exclude the case where x or y is zero. If $r = 0$, then the quadratic form $x^2 + gy^2$ is non-isotopic, which means the only solution is $x = y = 0$.Thus if $x, y \in \mathbb{F}_p^*$, then $x^2 + gy^2$ is never 0. Then in how many ways we can get $r \neq 0$, the lemma above says there are $p+1$. But we have to exclude the case $x = 0$ or $y = 0$. If r is a quadratic residue, then we get two solution for x if $y = 0$ and no solution for y if $x = 0$. If r is not a quadratic residue, then we get no solution for x if $y = 0$ and two solution for y if $x = 0$. Either case, we get $p - 1$ solutions for $x, y \in \mathbb{F}_p^*$. And hence

$$4\alpha\beta = (p-1)\sum_{i=1}^{p-1} \zeta^i = -(p-1).$$

And the minimal polynomial of α, β is $x^2 + x - (p-1)/4$ and then

$$\pm(\alpha - \beta) = \sqrt{\Delta} = \sqrt{1^2 - 4 \cdot (-\frac{p-1}{4})} = \sqrt{p} \in E = \mathbb{Q}(\alpha).$$

Therefore, $E = \mathbb{Q}(\sqrt{p})$.

Now consider the case $p \equiv 3 \pmod 4$. In this case, the quadratic residue is isotopic, which means we get nontrivial solution for $x^2 + gy^2 = 0$. The number of solutions is then $2p - 1$ by the lemma above. But we have to exclude the trivial solution $x = y = 0$. So indeed, there are $2p - 2$ solution when $x, y \in \mathbb{F}_p^*$. Exactly the same argument as last case, we get $p - 3$ solutions for $x^2 + gy^2 = r$ for each $r \neq 0$ when $x, y \in \mathbb{F}_p^*$. Therefore, we have

$$4\alpha\beta = 2p - 2 + (p-3)\sum_{i=1}^{p-1} \zeta^i = 2p - 2 - (p-3) = p + 1.$$

And the minimal polynomial of α, β is $x^2 + x + (p+1)/4$ and then

$$\pm(\alpha - \beta) = \sqrt{\Delta} = \sqrt{1^2 - 4 \cdot (\frac{p+1}{4})} = \sqrt{-p} \in E = \mathbb{Q}(\alpha).$$

Therefore, $E = \mathbb{Q}(\sqrt{-p})$. $\square$