9.3 Galois' Theorem

What is one of the most important applications of Galois theory?

9.3.0 Theorem. *Let $K \subseteq L$ be a Galois field extension. The Galois group* $\mathrm{Gal}(L/K)$ *is solvable if and only if the field extension $K \subseteq L$ is solvable.*

Proof. We prove the forward implication in three steps.

Reduction to the radical case: Since $K \subseteq L$ is solvable, it lies in a radical extension $K \subseteq L'$. The theorem from last Tuesday shows that the Galois closure $K \subseteq M$ of $K \subseteq L'$ is radical over K. Thus, we have $K \subseteq L \subseteq M$ where M is radical and Galois over K.

Suppose that $\mathrm{Gal}(M/K)$ is solvable. As $K \subseteq L$ is Galois, we have an isomorphism $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K) \,/\, \mathrm{Gal}(M/L)$. The quotient of a solvable group is also solvable, so $\mathrm{Gal}(L/K)$ is solvable. Hence, it suffices to prove that $\mathrm{Gal}(M/K)$ is solvable. In other words, we can assume that $K \subseteq L$ is radical and Galois.

Adjunction of roots of unity: Suppose that $K \subseteq L$ is radical and Galois. If we adjoin a primitive mth root of unity ζ to both K and L, the resulting field extension $K(\zeta) \subseteq L(\zeta)$ is radical because $L(\zeta)$ is the compositum of $K(\zeta)$ and L. This field extension is also Galois. If we can show that $\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)$ is solvable, then it will imply that $\mathrm{Gal}(L/K)$ is solvable. Thus, we may assume without loss of generality that K contains any mth root of unity we want.

Proof of solvability: Since $K \subseteq L$ is radical, there are intermediate fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L$ such that, for all $1 \leqslant j \leqslant n$, we have $K_j = K_{j-1}(\gamma_j)$ where ${\gamma_j}^{m_j} \in K_{j-1}$ for some positive $m_j \in \mathbb{Z}$. By the previous step, we may assume that K contains a primitive m_jth root of unity ζ_j for all $1 \leqslant j \leqslant n$. We claim that $K_{j-1} \subseteq K_j$ is Galois with a cyclic Galois group.

To prove this, observe that $1, \zeta_j, \zeta_j^2, \ldots, \zeta_j^{m_j-1}$ are the distinct m_jth roots of unity, which means that $\gamma_j, \zeta_j\gamma_j, \zeta_j^2\gamma_j, \ldots, \zeta_j^{m_j-1}\gamma_j$ are the distinct roots of $x^{m_j} - {\gamma_j}^{m_j} \in K_{j-1}[x]$. Since $\zeta_j \in K \subseteq K_{j-1}$, we have $K_{j-1}(\gamma_j, \zeta_j\gamma_j, {\zeta_j}^2\gamma_j, \ldots, {\zeta_j}^{m_j-1}\gamma_j) = K_{j-1}(\gamma_j)$. This shows that $K_{j-1} \subseteq K_j = K_{j-1}(\gamma_j)$ is Galois. Let $\sigma \in \mathrm{Gal}(K_j/K_{j-1})$. There is a unique integer $0 \leqslant \ell \leqslant m_j - 1$ such that $\sigma(\gamma_j) = \zeta_j^\ell \gamma_j$. One verifies that $\sigma \mapsto [\ell]$ defines an injective group homomorphism from $\mathrm{Gal}(K_j/K_{j-1}) \to \mathbb{Z} \,/\, \langle m_j \rangle$. It follows that $\mathrm{Gal}(K_j/K_{j-1})$ is cyclic.

We now prove solvability. For all $0 \leqslant j \leqslant n$, consider the subgroups $G_j := \mathrm{Gal}(L/K_j) \subseteq \mathrm{Gal}(L/K)$. Because the Galois correspondence is inclusion-reversing, we obtain

$$\{\mathrm{id}_L\} = \mathrm{Gal}(L/L) = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 = \mathrm{Gal}(L/K)\,.$$

Focus on the field extensions $K_{j-1} \subseteq K_j \subseteq L$. The field extension $K_{j-1} \subseteq L$ is Galois because K_{j-1} is an intermediate field in the Galois extension $K \subseteq L$. Moreover, the field extension $K_{j-1} \subseteq K_j$ is also Galois as established above. The Galois correspondence implies that G_j is normal in G_{j-1} with

$$G_{j-1} \,/\, G_j = \mathrm{Gal}(L/K_{j-1}) \,/\, \mathrm{Gal}(L/K_j) \cong \mathrm{Gal}(K_j/K_{j-1})\,.$$

This Galois group is cycle, so G_{j-1}/G_j is abelian. Since this is true for all $1 \leqslant j \leqslant n$, we deduce that $\mathrm{Gal}(L/K)$ is solvable.

We prove the backward implication in two steps.

A special case: Let $K \subseteq L$ be a Galois field extension whose Galois group is solvable. In addition, assume that K has the following property: K has a primitive pth root of unity for every prime p that divides $|\mathrm{Gal}(L/K)|$. We claim that $K \subseteq L$ is radical. Since $\mathrm{Gal}(L/K)$ is solvable, we have subgroups

$$\{\mathrm{id}_L\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = \mathrm{Gal}(L/K)\,.$$

Consider the fixed fields $K_j := L^{G_j} \subseteq L$ for all $1 \leqslant j \leqslant n$. Since the Galois correspondence is inclusion-reversing, we obtain

$$K = L^{G_0} \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L^{G_n} = L\,.$$

Because G_j is normal in G_{j-1}, the Galois correspondence implies that $G_{j-1}/G_j \cong \mathrm{Gal}(K_j/K_{j-1})$. Since the index $[G_{j-1} : G_j]$ is prime, we have $\mathrm{Gal}(K_j/K_{j-1}) \cong \mathbb{Z}/\langle p\rangle$ for some prime $p \in \mathbb{Z}$.

It follows that $K_{j-1} \subseteq K_j$ satisfies the conditions of the Lemma from last Thursday's class, so the field K_j is obtained from K_{j-1} by adjunction of a pth root of an element in K_{j-1}. This establishes that the field extension $K \subseteq L$ is radical.

The general case: Assume only that the field extension $K \subseteq L$ is Galois with a solvable Galois group. Let ζ be a primitive mth root of unity where $m := |\mathrm{Gal}(L/K)|$. The Galois group $\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)$ is solvable because $\mathrm{Gal}(L/K)$ is.

The group isomorphism $\mathrm{Gal}(L/K) \cong \mathrm{Gal}\big(L(\zeta)/K\big)/\mathrm{Gal}\big(L(\zeta)/L\big)$ is induced by the group homomorphism $\mathrm{Gal}\big(L(\zeta)/K\big) \to \mathrm{Gal}(L/K)$ defined by restricting an automorphism of $L(\zeta)$ to L. Similarly, $\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)$ being a subgroup of $\mathrm{Gal}\big(L(\zeta)/K\big)$ gives another group homomorphism $\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big) \to \mathrm{Gal}(L/K)$ defined by restriction to L. However, the kernel of this second map is the identity, because elements of the kernel are the identity on both L and $K(\zeta)$. Hence, the second group homomorphism is injective, and Lagrange's Theorem implies that $m = |\mathrm{Gal}(L/K)|$ is a multiple of $|\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)|$.

Now, let p be a prime dividing $|\mathrm{Gal}\big(L(\zeta)/K(\zeta)\big)|$. It follows that p divides m. Since ζ is a primitive mth root of unity, $\zeta^{m/p}$ is a primitive pth root of unity. Since $\zeta^{m/p} \in K(\zeta)$, we conclude that $K(\zeta) \subseteq L(\zeta)$ satisfies the hypothesis in the special case. Thus, $K(\zeta) \subseteq L(\zeta)$ is radical by the special case. However, $K \subseteq K(\zeta)$ is radical, so $K \subseteq L(\zeta)$ is radical by the basic properties of radical extensions. Since $K \subseteq L(\zeta)$ is radical, the inclusion $L \subseteq L(\zeta)$ implies that L lies in a radical extension of K. Therefore, $K \subseteq L$ is solvable. □

9.4 Solving Polynomials by Radicals

How does group theory lead to new insights into the roots?

9.4.0 Definition. Let $f \in K[x]$ be nonconstant with splitting field $K \subseteq L$. A root $\alpha \in L$ of f is *expressible by radicals over* K if α lies is some radical field extension of K. The polynomial f is *solvable by radicals over* K if the field extension $K \subseteq L$ is solvable.

9.4.1 Proposition. *Let K be a field of characteristic 0, and let $f \in K[x]$ be irreducible. The polynomial f is solvable by radicals over K if and only if f has a root expressible by radicals over K.*

Proof. One implication is trivial. Suppose that f has a root α is some radical extension of K. Thus, the field extension $K \subseteq K(\alpha)$ is solvable, and its Galois closure $K \subseteq K(\alpha) \subseteq M$ is also solvable.

Since a Galois extension is normal and f is irreducible over K with a root in M, the polynomial f splits completely over M. Thus, M contains the splitting field of f over K. The claim follows because $K \subseteq M$ is solvable. □

9.4.2 Theorem. *Assume that the field K has characteristic 0. A polynomial $f \in K[x]$ is solvable by radicals over K if and only if the Galois group of f over K is solvable.* ■

The Galois group of $f \in K[x]$ is $\mathrm{Gal}(L/K)$ where L is the splitting field of f over K.

9.4.3 Proposition. *Let K be a field of characteristic 0. Every polynomial in $K[x]$ of degree at most 4 is solvable by radicals.*

Proof. If f is separable, then the Galois group of f is isomorphic to a subgroup of $\mathfrak{S}_n$. Since $\mathfrak{S}_n$ is solvable for all $n \leqslant 4$, the previous theorem establishes the claim.

When f is not separable, let $g := f/\gcd(f, f')$ be its squarefree part. By construction, g is separable and $\deg(g) \leqslant 3$. The splitting field for f over K is also the splitting field for g. Applying the first paragraph to g, we deduce that f is solvable by radicals. □

9.4.4 Theorem. *For all $n \geqslant 4$, the alternating group A_n is simple.* ■

A group G is *simple* if its only normal subgroups are $\{e\}$ and G; see MATH310?

9.4.5 Corollary. *The groups A_n and $\mathfrak{S}_n$ are solvable if and only if $n \leqslant 4$.*

Proof. When $n \leqslant 4$, one demonstrates that A_n and $\mathfrak{S}_n$ are solvable by explicitly constructing appropriate chains of normal subgroups.

Suppose that $n \geqslant 5$. The group A_n is not abelian and simple. The only normal subgroups of A_n have index $|A_n| \neq p$ and 1, so A_n is not solvable. Having A_n as a subgroup, $\mathfrak{S}_n$ cannot be solvable. □

The 3-cycles (3 1 2) and (4 1 2) in A_n do not commute.

9.4.6 Theorem. *Let K be a field of characteristic 0, and let $e_1, e_2, \ldots, e_n$ be the elementary symmetric polynomials in $K[x_1, x_2, \ldots, x_n]$. For all $n \geqslant 5$, the universal polynomial $\widetilde{f} \in K(e_1, e_2, \ldots, e_n)[x]$ of degree n is not solvable by radicals over $K(e_1, e_2, \ldots, e_n)$, and no root of the polynomial $\widetilde{f}$ is expressible by radicals over $K(e_1, e_2, \ldots, e_n)$.*

Galois theory lead to a better understanding of the Abel–Ruffini theorem, which states that there is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

Proof. The first part follows from the previous theorem because $\mathfrak{S}_n$ is not solvable when $n \geqslant 5$. The second part follows from the first proposition because $\widetilde{f}$ irreducible over K. □

9.4.7 Lemma. *For each prime $p \in \mathbb{Z}$, every group of order p^m where $m \in \mathbb{N}$ is solvable.*

To prove that the center is nontrivial, one considers the class equation of the p-group modulo p.

Sketch of proof. Let G be a group of order p^m. Every finite p-group has a nontrivial center, so $Z(G)$ contains a subgroup of order p.

We construct the relevant subgroups by induction on m. When $m = 1$, $G \cong \mathbb{Z}/\langle p \rangle$ is abelian and solvable. Suppose that $m > 1$. Since $Z(G)$ is nontrivial, choose a subgroup H of $Z(G)$ of order p. It follows that H is a normal subgroup of the ambient group G, H is abelian, and $|G/H| = p^{m-1}$. The induction hypothesis implies that the quotient G/H is solvable. The chain $\{e\} \subset H \subset G$ of normal subgroups has abelian quotients, so G is solvable. □

9.4.8 Fundamental Theorem of Algebra (Girard 1649, Argand 1813)**.** *Every nonconstant polynomial in $\mathbb{C}[x]$ splits completely over $\mathbb{C}$.*

When $|G|$ is odd, $H = \{e\}$. In other words, H is a subgroup of G such that $|H|$ is the highest power of 2 dividing $|G|$.

This argument relies on exactly the same lemmas as the earlier proof.

Artin's proof. It suffices to prove that every nonconstant polynomial in $\mathbb{R}[x]$ splits completely over $\mathbb{C}$. Given such a polynomial f, let L be its splitting field. As $\mathbb{R}$ has characteristic 0, $\mathbb{R} \subseteq L$ is Galois. Let $G := \operatorname{Gal}(L/\mathbb{R})$ and let H be a 2-Sylow subgroup of G.

By the Galois correspondence, the fixed field $\mathbb{R} \subseteq L^H$ has degree $[L^H : \mathbb{R}] = [G : H] = |G| / |H|$. The definition of H ensures that $\mathbb{R} \subseteq L^H$ has odd degree. When $\alpha \in L^H$ is a primitive element over $\mathbb{R}$, the minimal polynomial $p \in \mathbb{R}[x]$ of α has odd degree. Every polynomial of odd degree in $\mathbb{R}[x]$ has a root in $\mathbb{R}$, so p has a root in $\mathbb{R}$. Since minimal polynomials are irreducible, this means that g must have degree 1, which means $L^H = \mathbb{R}$.

Now, the Galois correspondence implies that $H = G$, so $|G| = 2^m$ for some $m \in \mathbb{N}$. If $m = 0$, then G is trivial and $L = \mathbb{R}$. Hence, f splits completely over $\mathbb{R}$ in this case. Suppose that $m \geqslant 1$. Because every group of order 2^m is solvable, there exists subgroups

$$\{\mathrm{id}_L\} = G_m \subseteq G_{m-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 = G$$

such that G_j is normal in G_{j-1} of index 2 for all $1 \leqslant j \leqslant m$. Since the Galois correspondence is inclusion-reversing, we obtain

$$\mathbb{R} = L^{G_0} \subseteq L^{G_1} \subseteq L^{G_2} \subseteq \cdots$$

such that $L^{G_{j-1}} \subseteq L^{G_j}$ has degree 2 for all j. Since $m \geqslant 1$, we have the degree 2 extension $\mathbb{R} \subseteq L^{G_1}$. The minimal polynomial of a primitive element of this field extension is a quadratic polynomial with no real roots. It follows that $L^{G_1} \cong \mathbb{C}$.

Now suppose that $n \geqslant 2$. Since $L^{G_1} \subseteq L^{G_2}$, we have a degree 2 extension of $\mathbb{C}$. Since every quadratic polynomial in $\mathbb{C}[x]$ splits completely over $\mathbb{C}$, this is impossible. Thus, we must have $m = 1$, which implies that $|G| = 2$ and $L = L^{G_1} \cong \mathbb{C}$. □

10.0 Cyclotomic Extensions

What is the Galois group of a cyclotomic field extension?

10.0.0 Definition. For any positive $n \in \mathbb{Z}$, set $\zeta_n := \exp(2\pi i/n) \in \mathbb{C}$. The *nth cyclotomic polynomial* $\Phi_n \in \mathbb{Z}[x]$ is

$$\Phi_n := \prod_{\gcd(j,n)=1} (x - \zeta_n^j) .$$

By construction, the degree of Φ_n is the number of integers j satisfying $0 \leqslant j \leqslant n$ and $\gcd(j,n) = 1$, so $\deg(\Phi_n) = \left|(\mathbb{Z}/\langle n\rangle)^\times\right| = \phi(n)$, where ϕ denotes the Euler's totient function.

10.0.1 Remark. We have $\Phi_2 = x + 1$, $\Phi_4 = x^2 + 1$, and $\Phi_p = x^{p-1} + x^{p-2} + \cdots + 1$ for all prime $p \in \mathbb{Z}$.

10.0.2 Lemma. *The cyclotomic polynomials satisfy*

$$x^n - 1 = \prod_{d|n} \Phi_d .$$

Proof. Organize the factorization according to d:

$$x^n - 1 = \prod_{|n} \prod_{\gcd(j,n)=d} (x - \zeta_n^j) .$$

The equation $\gcd(j,n) = d$ implies that $j = dk$ and $n = d\frac{n}{d}$, where $\gcd(k, \frac{n}{d})$. Hence, $0 \leqslant j < n$ becomes $0 \leqslant dk < d\frac{n}{d}$ or $0 \leqslant k < \frac{n}{d}$, and $\zeta_n^d = \zeta_{n/d}$, so $x - \zeta_n^j = x - \zeta_n^{dk} = x - \zeta_{n/d}^k$. It follows that

$$\prod_{\gcd(j,n)=d} (x - \zeta_n^j) = \prod_{\gcd(k,n/d)=1} (x - \zeta_{n/d}^k) = \Phi_{n/d} .$$

It remains to show that Φ_n has integer coefficients. We proceed by induction on n. The base case $n = 1$ is trivial because $\Phi_1 = x - 1$. When $n > 1$, the induction hypothesis implies that

$$x^{n-1} - 1 = \Phi_n \prod_{d|n, d<n} \Phi_d .$$

Since the product is a monic polynomial with integer coefficients, it follows that Φ_n also is. □

10.0.3 Remark. For any prime $p \in \mathbb{Z}$, we have $x^{p^2} - 1 = \Phi_1 \Phi_p \Phi_{p^2}$, so

$$\Phi_{p^2} = \frac{x^{p^2} - 1}{x^p - 1} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^{2p} + x^p + 1 .$$

10.0.4 Lemma. *Assume that $f \in \mathbb{Z}[x]$ is monic of positive degree, and let $p \in \mathbb{Z}$ be prime. When f_p denotes the monic polynomial whose roots are the pth powers of the roots of f, we have $f_p \in \mathbb{Z}[x]$ and the coefficients of f and f_p are congruent modulo p.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ denote the roots of f. It follows that

$$\begin{aligned} f_p &= \prod_{j=1}^{r} (x - \alpha_j^p) \\ &= x^r - e_1(\alpha_1^p, \alpha_2^p, \ldots, \alpha_r^p) x^{r-1} + \ldots + (-1)^r e_n(\alpha_1^p, \alpha_2^p, \ldots, \alpha_r^p) . \end{aligned}$$

For all $1 \leqslant j \leqslant n$, observe that $e_j(x_1^p, x_2^p, \ldots, x_r^p)$ is a symmetric polynomial and $e_j(x_1^p, x_2^p, \ldots, x_r^p) - e_j(x_1, x_2, \ldots, x_r)^p \in \mathbb{Z}[e_1, e_2, \ldots, e_r]$.

In the ring $\mathbb{Z}/\langle p\rangle\,[x_1, x_2, \dots, x_n]$, the Frobenius homomorphism and Fermat's Litte theorem give

$$e_j(\alpha_1^p, \alpha_2^p, \dots, \alpha_r^p) \equiv e_j(\alpha_1, \alpha_2, \dots, \alpha_r)^p \equiv e_j(\alpha_1, \alpha_2, \dots, \alpha_r) \mod p\,.$$

Thus, the coefficients of f and f_p are congruent modulo p. Since $e_j(\alpha_1, \alpha_2, \dots, \alpha_r) \in \mathbb{Z}$ for all j, and the difference has integer coefficients, we conclude that $e_j(\alpha_1^p, \alpha_2^p, \dots, \alpha_r^p) \in \mathbb{Z}$. □

10.0.5 Proposition. *The cyclotomic Φ_n is irreducible over $\mathbb{Q}$.*

Proof. Let $f \in \mathbb{Q}[x]$ be an irreducible factor of Φ_n. By the Gauss Lemma for polynomials, we may assume that $f \in \mathbb{Z}[x]$ and $\Phi_n = fg$ for some $g \in \mathbb{Z}[x]$. We may also assume that f and g are monice because Φ_n is.

Let p be a prime not dividing n. We first claim that ζ_n^p is a root of f whenever ζ_n is a root of f. Suppose otherwise: $f(\zeta_n) = 0$ and $f(\zeta_n^p) \neq 0$. Let $f_p \in \mathbb{Z}[x]$ be the monic polynomial whose roots are the pth powers of the roots of f. The roots of f_p are distinct primitive nth roots of unity, which implies that f_p divides Φ_n. If f and f_p has a common root, then f would divide f_p because f is irreducible. This would force $f = f_p$ because they are monic of the same degree. However, $f = f_p$ is impossible because $f(\zeta_n) = 0$ and $f(\zeta_n^p) \neq 0$. Thus, these polynomials have no common roots, so $\Phi_n = ff_ph$ for some monic $h \in \mathbb{Z}[x]$. Since the images of f and f_p coincide in $\mathbb{F}_p[x]$, this factorization would imply that the images of Φ_n and $x^n - 1$ are not separable in $\mathbb{F}_p[x]$. However $x^n - 1$ is separable because p does not divide n.

The claim implies that every primitive nth root of unity is a root of f. As f divides Φ_n, we see that $f = \Phi_n$ and Φ_n is irreducible. □

10.0.6 Corollary. *For all positive $n \in \mathbb{Z}$, the degree of the cyclotomic extension is $\big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] = |(\mathbb{Z}\,/\langle n\rangle)^\times| = \phi(n)$.* ■

10.0.7 Theorem. *There exists a group isomorphism*

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big) \cong (\mathbb{Z}/\langle n\rangle)^\times$$

such that the automorphism $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big)$ maps to congruence class $[\ell]_n \in \big(\mathbb{Z}/\langle n\rangle\big)^\times$ if and only if $\sigma(\zeta_n) = \zeta_n^\ell$.

Proof. As the splitting field for cyclotomic polynomial Φ_n over $\mathbb{Q}$, the field extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ is Galois. Moreover, an automorphism $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big)$ is uniquely determined by $\sigma(\zeta_n)$, which is a root of Φ_n because ζ_n is. Hence, there exists $\ell \in \mathbb{Z}$ that is relatively prime to n such that $\sigma(\zeta_n) = \zeta_n^\ell$. The map from $\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big)$ to $(\mathbb{Z}\,/\langle n\rangle)^\times$ defined by $\sigma \mapsto [\ell]_n$ is well-defined because $\zeta_n^k = \zeta_n^\ell$ if and only if $k \equiv \ell \mod n$. If $\sigma(\zeta_n) = \zeta_n^\ell$ and $\tau(\zeta_n) = \zeta_n^k$, then we see that $(\sigma \circ \tau)(\zeta_n) = \sigma(\zeta_n^k) = (\zeta_n^\ell)^k = \zeta_n^{\ell k}$, so this map $\sigma \mapsto [\ell]_n$ is a group homomorphism. Since $\sigma \mapsto [1]$ if and only if $\sigma(\zeta_n) = \zeta_n$ or equivalently $\sigma = \mathrm{id}_{\mathbb{Q}(\zeta_n)}$, this group homomorphism is injective. Since $|\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big)| = \big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] = |(\mathbb{Z}\,/\langle n\rangle)^\times|$, we conclude that $\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big) \to (\mathbb{Z}/\langle n\rangle)^\times$ is an isomorphism. □