Lecture 16 : Applications and Illustrations of the FTGT

Objectives

(1) Fundamental theorem of algebra via FTGT.
(2) Gauss' criterion for constructible regular polygons.
(3) Symmetric rational functions.
(4) Galois group of some binomials.

Keywords and phrases: Fundamental theorem of algebra, constructible regular polygons, symmetric rational functions.

The Galois correspondence between the set of subfields of a finite Galois extension E/F and the set of subgroups of the Galois group $G(E/F)$ converts problems about roots of a separable polynomial to problems about the Galois group of its splitting field. We shall see that difficult problems about polynomials are converted into much simpler problems about finite groups.

The Galois correspondence is perhaps the first example of a well-established technique in mathematics: find a suitable formulation for a problem in one branch of mathematics in another branch where the problem becomes much easier to solve.

We will see that the Galois correspondence is powerful enough to provide new ways to prove old results and solve new problems as well. This will be demonstrated here by giving a new proof of the fundamental theorem of algebra. We will also finish the proof of Gauss' criterion for constructibility of regular polygons. We shall derive an expression for $\cos 2\pi/17$ in terms of square roots which proves that a seventeen sided regular polygon is constructible by ruler and compass.

We will provide concrete examples of Galois correspondence for some polynomials. In later sections we will derive formulas for the roots of cubic and quartic polynomials as a consequence of the Galois correspondence. Let us begin by proving:

The Fundamental Theorem of Algebra

Theorem 16.1. *The field of complex numbers is algebraically closed.*

Proof. Let $f(x) = \sum a_i x^i \in \mathbb{C}[x]$. Write $\bar{f}(x) = \sum \bar{a}_i x^i$ where $-$ denotes the complex conjugation. Then $g(x) = f(x)\bar{f}(x) \in \mathbb{R}[x]$. Hence it is enough to prove $g(x)$ has a complex root.

The splitting field E of $g(x)$ over $\mathbb{C}$ is a splitting field of $(x^2+1)g(x)$ over $\mathbb{R}$. Hence $E/\mathbb{R}$ is a Galois extension. Since $2 \mid [E : \mathbb{R}]$, the Galois group $G = G(E/\mathbb{R})$ has a 2- Sylow subgroup say S. If $S < G$ then $E \supset E^S \supset \mathbb{R}$. We know $[E : E^S] = |S|$. Thus $[E^S : \mathbb{R}]$ is odd. But $\mathbb{R}$ admits no proper odd degree algebraic extensions. Hence $S = G$. Thus G is a 2-group. If $|G| = 2$, then $E = \mathbb{C}$ and we are done. If $|G| = 4$, then $[E : \mathbb{C}] = 2$. But $\mathbb{C}$ admits no quadratic extension. Thus $|G| \geq 8$. Let $H < G(E/\mathbb{C})$ of index 2. Then $[E^H : \mathbb{C}] = 2$, which is a contradiction. Hence $E = \mathbb{C}$. □

Gauss' Criterion for Constructible Regular Polygons

Lemma 16.2. *Let m, n be coprime natural numbers. If regular polygons of m sides and n sides are constructible then so is a regular mn-gon.*

Proof. There exist integers x, y so that $xm + yn = 1$. Hence

$$\frac{2\pi}{mn} = \frac{2\pi x}{n} + \frac{2\pi y}{m}.$$

Since $2\pi x/n$ and $2\pi y/m$ are constructible, so is $2\pi/mn$. □

Proposition 16.3. *Let ζ be a complex primitive p^{th} root of unity where p is a prime number. Then $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a cyclic group of order $p-1$.*

Proof. If $\sigma \in G$, then σ restricted to the cyclic group $U = (\zeta)$ is an automorphism. Hence $\sigma(\zeta) = \zeta^{i_\sigma}$ for some $i = 1, 2, \ldots, p-1$. Define a group homomorphism $\psi : G \to U(\mathbb{Z}/p\mathbb{Z}) = \{1, 2, \ldots, p-1\}$ by $\psi(\sigma) = i_\sigma$. It is easy to see that ψ is an isomorphism. □

Theorem 16.4 (Gauss). *A regular polygon of n sides is constructible if and only if $n = 2^r p_1 p_2 \ldots p_s$ where $r \in \mathbb{N}$ and $p_1, p_2, \ldots, p_s$ are distinct Fermat primes.*

Proof. We have already proved the necessity. For sufficiency, note that by the above lemma and the fact that angles can be bisected by ruler and compass, it is enough to prove that if p is a Fermat prime then $\cos(2\pi/p)$

is a constructible real number. Let ζ be a primitive p^{th} root of unity. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1 = 2^t$ for some t, the Galois group $G = G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic of order 2^t. Hence every intermediate subfield of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$. In particular $K = \mathbb{Q}(\cos 2\pi/p)$ is a Galois extension of $\mathbb{Q}$ of degree 2^{t-1}. Since $G(K/\mathbb{Q})$ is a 2-group of order 2^{t-1}, there a chain of subgroups G_i having order 2^i for $i = 0, 1, \ldots, t-1$. Hence

$$\mathbb{Q} \subset K^{G_{t-2}} \subset K^{G_{t-3}} \subset \cdots \subset K^{G_0} = K$$

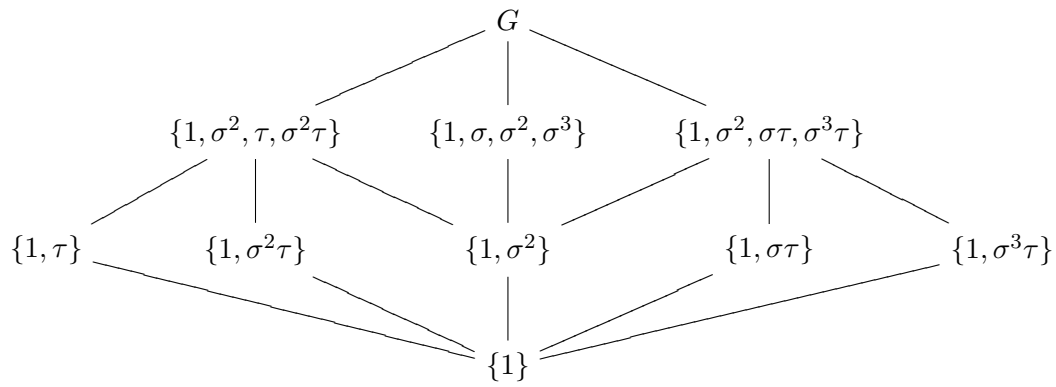
is a tower of real quadratic extensions terminating with K. Hence $\cos 2\pi/p$ is a constructible real number. □

Example 16.5. Let K be a splitting field of $x^4 - 2$ over $\mathbb{Q}$. We find the Galois group $G = G(K/\mathbb{Q})$ and show how to find subfields of $K/\mathbb{Q}$.

The polynomial $f(x) = x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Let $a = \sqrt[4]{2}$ be the real 4th root of 2. Then the roots of $f(x)$ in $\mathbb{C}$ are $a, -a, ia, -ia$. The splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(a, i)$ and $[K : \mathbb{Q}] = 8$. Hence $G = G(K/\mathbb{Q})$ is a group of order 8. An automorphism in G maps a to one of the four roots of $f(x)$ and it maps i to either i or $-i$. Let τ be the conjugation map and σ be defined by $\sigma(a) = ia$. Check that

$$o(\sigma) = 4,\ o(\tau) = 2 \quad \text{and } \sigma\tau\sigma\tau = id.$$

The lattice of the subgroups of G is:



By Galois correspondence, there are 10 intermediate subfields of $K/\mathbb{Q}$. These are all fixed fields of the subgroups displayed above. Set $H = \{1, \sigma, \sigma^2, \sigma^3\}$.

Since $[K : K^H] = o(H) = 4$ we see that $[K^H : \mathbb{Q}] = 2$. Since i is fixed by each element of H, we conclude that $K^H = \mathbb{Q}(i)$. Set $L = \{1, \tau\}$. Since $[K : K^L] = o(L) = 2$, we see that $[K^L : \mathbb{Q}] = 4$. Since $\tau(a) = a$, $K^L = \mathbb{Q}(a)$.

Set $M = \{1, \sigma\tau\}$. Since $[K : K^M] = o(M) = 2$, $[K^M : \mathbb{Q}] = 4$. The orbit of a under the action of M is $\{a, ia\}$. Adding the elements of this orbit we get $b = a + ia$. Hence $a + ia \in K^M$. To find $g(x) = \text{ irr } (b, \mathbb{Q})$, we find all the conjugates of b by applying the automorphisms in G. This way we see that the orbit of b under the action of G is $\{b, -b, a - ia, -a + ia\}$. Hence $\deg_{\mathbb{Q}}(b) = 4$. Hence $K^M = \mathbb{Q}(b)$. The other fixed fields can be found similarly.

Example 16.6. We discuss the Galois group of $x^p - 2$, where p is an odd prime, We will show that it is isomorphic to the group

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{F}_p \text{ and } a \neq 0 \right\}.$$

Put $\omega = e^{2\pi i/p}$ and $\alpha = \sqrt[p]{2}$. The roots of $x^p - 2$ are $\alpha, \alpha\omega, \alpha\omega^2, \ldots, \alpha\omega^{p-1}$. Thus $K = \text{Spl}(x^p - 2, \mathbb{Q}) = \mathbb{Q}(\alpha, \omega)$ and $[K : \mathbb{Q}] = p(p-1)$. If $\sigma \in G(K/\mathbb{Q})$, then $\sigma(\alpha) = \alpha\omega^{i(\sigma)}$ and $\sigma(\omega) = \omega^{j(\sigma)}$, where $1 \leq j(\sigma) \leq (p-1)$ and $i(\sigma) = 0, 1, \ldots, (p-1)$. Define

$$\psi : G(K/\mathbb{Q}) \to G \text{ by } \psi(\sigma) = \begin{bmatrix} j(\sigma) & i(\sigma) \\ 0 & 1 \end{bmatrix}.$$

Define $\sigma, \tau \in G(K/\mathbb{Q})$ by

$$\tau(\alpha) = \alpha\omega^a,\ \tau(\omega) = \omega^b,\ \sigma(\alpha) = \alpha\omega^c, \text{ and } \sigma(\omega) = \omega^d.$$

Therefore

$$\psi(\sigma) = \begin{bmatrix} d & c \\ 0 & 1 \end{bmatrix},\ \psi(\tau) = \begin{bmatrix} b & a \\ 0 & 1 \end{bmatrix},\ \psi(\sigma)\psi(\tau) = \begin{bmatrix} bd & c + ad \\ 0 & 1 \end{bmatrix}.$$

Since

$$\begin{aligned} \tau\sigma(\alpha) &= \tau(\alpha\omega^a) = \alpha\omega^{c+ad} \\ \tau\sigma(\omega) &= \tau(\omega^d) = \omega^{bd} \end{aligned}$$

we have

$$\psi(\tau\sigma) = \begin{bmatrix} bd & c+ad \\ 0 & 1 \end{bmatrix} = \psi(\tau)\psi(\sigma).$$

Therefore ψ is a group homomorphism. As

$$\text{Ker } \psi = \{\sigma : d = 1 \text{ and } c = 0\} = \{id\},$$

we conclude that ψ is an isomorphism.

Example 16.7. Let $x_1, x_2, \ldots, x_n$ be indeterminates over a field F. The symmetric group S_n acts on $E = F(x_1, x_2, \ldots, x_n)$, the fraction field of the ring of polynomials $F[x_1, \ldots, x_n]$. If $\sigma \in S_n$ then $\phi_\sigma : E \to E$ defined by $\phi_\sigma(x_i) = x_{\sigma(i)}$ is an automorphism of E. If $\sigma_1, \sigma_2 \in S_n$ then $\phi_{\sigma_1\sigma_2} = \phi_{\sigma_1}\phi_{\sigma_2}$. Thus $G = \{\phi_\sigma : \sigma \in S_n\}$ is a group of automorphism of E and it is isomorphic to S_n. Let x be a variable over E and consider the polynomial ring $E[x]$. Then

$$\begin{aligned} g(x) &= (x - x_1)(x - x_2)\cdots(x - x_n) \in E[x] \\ &= x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n \end{aligned}$$

Where σ_i's are the elementary symmetric functions of $x_1 \ldots, x_n$. The automorphism $\phi_\sigma : E \to E$ can be extended to $E[x]$ by fixing x which we again denote by ϕ_σ. Therefore

$$\phi_\sigma(g(x)) = (x - x_{\sigma(1)})(x - x_{\sigma(2)})\cdots(x - x_{\sigma(n)}) = g(x)$$

Thus $\phi_\sigma(\sigma_i) = \sigma_i$ for all $i = 1, 2, \ldots, n$. Hence $F(\sigma_1, \sigma_2, \cdots, \sigma_n) \subset E^G$. Notice that $E = F(\sigma_1, \ldots, \sigma_n, x_1, \ldots x_n)$. So E is a splitting field of $g(x)$ over $F(\sigma_1, \ldots, \sigma_n)$ and $g(x)$ is separable. If $\pi \in G(E/F(\sigma_1, \ldots, \sigma_n))$ then π permutes the roots of $g(x)$, hence $\pi = \phi_\sigma$ for some σ. Thus $G = G(E/F(\sigma_1 \ldots, \sigma_n))$. Therefore symmetric rational functions are rational functions of symmetric functions.