NAProject 2018 Module IV: Computing Galois Groups Lectures 1 and 2: June 25-26, 2018

Let K be a field and $f \in K[X]$ a separable monic polynomial of degree n. Galois gave answer to the question of how to know whether the equation $f(X) = 0$ is solvable by radicals. In the previous three modules the strategy developed by Galois was introduced. We recall it.

Step 1: (Module II, Lectures 1, 2). We construct the splitting field K_f of f over K, the unique (up to isomorphism) extension K_f such that:

(a) $f(X) = (X - \alpha_1) \cdots (X - \alpha_n) \in K_f[X]$;
(b) $[K_f : K] \leq (\deg f)|$.

Step 2: (Module II, Lectures 3, 6, Milne 3.2). We construct the Galois Group G of the polynomial f over K, namely, $G = \mathrm{Gal}(K_f/K) = \{\phi : K_f \to K_f | \phi$ is an isomorphism and $\phi|_K =$ identity$\}$, with $|G_f| = [K_f : K]$.

Step 3: (Module III, Lecture 3). We stablish a one-to-one correspondende between the subfields of K_f containing K and the subgroups of $G = \mathrm{Gal}(K_f/K)$, known as *the fundamental theorem of Galois theory* (Milne, 3.16), $\{$ subgroups of $G\} \leftrightarrow \{$ intermediate fields $K \subset M \subset K_f\}$ given by $H \mapsto K_f^H$; $M \mapsto \mathrm{Gal}(K_f/M)$ which satisfies, among others, the following properties

(a) the correspondence is order reversing: $H_1 \supset H_2 \Leftrightarrow K_f^{H_1} \subset K_f^{H_2}$;

(b) indexes equal degrees: $(H_1 : H_2) = [K_f^{H_2} : K_f^{H_1}]$;

(c) H is normal in $G \Leftrightarrow K_f^H$ is normal (and, hence, Galois) over K, in which case, $\mathrm{Gal}(K_f^H/K) \simeq G/H$.

Step 4: Galois, 1832): *The equation $f = 0$ is solvable by radicals if and only if the Galois group G_f of f is solvable.* (Module III, Lecture 6, Milne 3.27.) This theorem reduces de question to computing G_f studying whether of not G_f is solvable.

The Galois Group of a polynomial

Proposition 1. Let K be a field, and let $f(X) \in K[X]$ be a separable polynomial with splitting field $K_f = K[\alpha_1, \ldots, \alpha_n]$, with $\mathrm{Zeros}(f) = \{\alpha_1, \ldots, \alpha_n\}$ and Galois group $G_f = \mathrm{Gal}(K_f/K)$.

(i) G_f permutes the roots of f: If $\sigma \in G_f$ and $\alpha_i \in \mathrm{Zeros}(f)$, then $\sigma(\alpha_i) = \alpha_j \in \mathrm{Zeros}(f)$

(ii) There exists an injective homomorphism $\theta : G_f \to S_{\mathrm{Zeros}(f)} \simeq S_n$, which allows us to identify G_f with its image in S_n (which we will do from now on). It also implies that $|G_f|$ divides $n!$.

Examples: $f(X) = X^4 - 4 \in \mathbb{Q}[X]$, $f(X) = X^3 - 1$, $f(X) = X^6 - 1$ and $f(X) = X^3 - 2$

Example 1: We consider the polynomial $f(X) = X^4 - 4 \in \mathbb{Q}[X]$. Then, since the polynomial factorizes in $\mathbb{C}[X]$ as $f(X) = (X^2 - 2)(X^2 + 2) = (X - \sqrt{2})(X + \sqrt{2})(X_i\sqrt{2})(X + i\sqrt{2}) \in \mathbb{C}[X]$, its splitting field is $\mathbb{Q}[\sqrt{2}, i]$, with $[\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}[\sqrt{2}] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4$. Thus, we can view $\mathbb{Q}[\sqrt{2}, i]$ as a vector-space of dimension 4 over $\mathbb{Q}$, with base, for example, $B = \{1, \sqrt{2}, i, i\sqrt{2}\}$.

Let us compute $G = \mathrm{Gal}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q})$. Every $\phi \in G$ is an isomorphism $\phi : \mathbb{Q}[\sqrt{2}, i] \to \mathbb{Q}[\sqrt{2}, i]$ with $\phi|_{\mathbb{Q}} = \text{Id.}$, so it is a $\mathbb{Q}$-isomorphism of $\mathbb{Q}[\sqrt{2}, i]$ seen as vector-space over $\mathbb{Q}$, and it will be determined by the images of the elements of any base, for example B. Notice that it suffices to find the images under ϕ of $\sqrt{2}$ and i. Since ϕ is a homomorphism, we know that $\phi(1) = 1$ and $\phi(i\sqrt{2}) = \phi(1)\phi(\sqrt{2})$. Thus, we need only to determine the image under ϕ of $\sqrt{2}$ and i.

$$(\sqrt{2})^2 = 2 \Rightarrow \phi((\sqrt{2})^2) = \phi(2) = \phi(1{+}1) = \phi(1){+}\phi(1) = 2 \Rightarrow \phi(\sqrt{2})^2 = 2 \to \phi(\sqrt{2}) = \Big\{\sqrt{2} - \sqrt{2}$$

$$(\sqrt{i})^2 = -1 \Rightarrow \phi((\sqrt{i})^2) = \phi(-1) = -1 \Rightarrow \phi(\sqrt{i})^2 = -1 \Rightarrow \phi(\sqrt{i}) = \{i - i$$

Consequently, $G = \{\phi_1 = \text{Id.}, \phi_2, \phi_3, \phi_4\}$, with

$$\phi_1(\sqrt{2}) = \sqrt{2},\ \phi_1(i) = i,\ \phi_1(i\sqrt{2}) = i\sqrt{2};$$
$$\phi_2(\sqrt{2}) = -\sqrt{2},\ \phi_2(i) = i,\ \phi_2(i\sqrt{2}) = -i\sqrt{2};$$
$$\phi_3(\sqrt{2}) = \sqrt{2},\ \phi_3(i) = -i,\ \phi_3(i\sqrt{2}) = -i\sqrt{2};$$
$$\phi_4(\sqrt{2}) = -\sqrt{2},\ \phi_4(i) = -i,\ \phi_4(i\sqrt{2}) = i\sqrt{2}$$

The zeros of f are $\mathrm{Zeros}(f) = \{\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = i, \alpha_4 = i\sqrt{2}\}$. Thus, the inyective homomorphism $\theta : G \hookrightarrow S_{\mathrm{Zeros}(f)} \simeq S_4$, allows us to identify G with $H = \{\text{Id.}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} < S_4$, via

$$\phi_1 \leftrightarrow \text{Id.},\ \phi_2 \leftrightarrow (1\ 2)(3\ 4),\ \phi_3 \leftrightarrow (3\ 4),\ \phi_4 \leftrightarrow (12).$$

There are five subgroups in G: G, which fixes the field $\mathbb{Q}[\sqrt{2}, i]^G = \mathbb{Q}$; $\langle(1\ 2)\rangle$, which fixes the field $\mathbb{Q}[\sqrt{2}, i]^{\langle(1\ 2)\rangle} = \mathbb{Q}[i\sqrt{2}]$; $\langle(3\ 4)\rangle$, which fixes the field $\mathbb{Q}[\sqrt{2}, i]^{\langle(3\ 4)\rangle} = \mathbb{Q}[\sqrt{2}]$; $\langle(1\ 2)(3\ 4)\rangle$, which fixes the field $\mathbb{Q}[\sqrt{2}, i]^{\langle(1\ 2)(3\ 4)\rangle} = \mathbb{Q}[i]$; and $\{\text{Id.}\}$ which fixes $\mathbb{Q}[\sqrt{2}, i]$. Thus, the Galois correspondence is

$$\mathbb{Q}[\sqrt{2}, i] \leftrightarrow \{\text{Id.}\}\mathbb{Q}[i\sqrt{2}] \leftrightarrow \langle(1\ 2)\rangle\mathbb{Q}[\sqrt{2}] \leftrightarrow \langle(3\ 4)\rangle\mathbb{Q}[i] \leftrightarrow \langle(1\ 2)(3\ 4)\rangle\mathbb{Q} \leftrightarrow G$$

Example 2: We consider the polynomial $f(X) = X^3 - 1 \in \mathbb{Q}[X]$. Then, since the polynomial factorizes in $\mathbb{C}[X]$ as $f(X) = (X - 1)(X^2 + X + 1) = (X - 1)(X - \omega)(X - \omega^2) \in \mathbb{C}[X]$, with $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$, root of the equation $\omega^2 + \omega + 100$, its splitting field is $\mathbb{Q}[\omega]$, with $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$. Thus, we can view $\mathbb{Q}[\sqrt{-3}$ as a vector-space of dimension 2 over $\mathbb{Q}$, with base, for example, $B = \{1, \omega\}$. Let us compute $G = \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$. This time, every $\phi \in G$ will be determined by the image of ω.

$$(\omega)^2 + \omega + 1 = 0 \Rightarrow \phi(\omega)^2 + \phi(\omega) + 1 = 0 \Rightarrow \phi(\omega) = \{\omega - \omega$$

Consequenly, $G = \{\phi_1 = \text{Id.}, \phi_2\}$, with $\phi_2(\omega) = \omega^2$. The zeros of f are $\mathrm{Zeros}(f) = \{\alpha_1 = 1, \alpha_2 = \omega, \alpha_3 = \omega^2\}$. Thus, the inyective homomorphism $\theta : G \hookrightarrow S_{\mathrm{Zeros}(f)} \simeq S_3$, allows us to identify G with $\langle(2\ 3)\rangle < S_3$, via

$$\phi_1 \leftrightarrow \text{Id.},\ \phi_2 \leftrightarrow (2\ 3).$$

Being of order 2, G has no proper subgroups, just as the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-3})$ has no proper sub-extensions, since it is of degree 2 and 2 is prime.

Example 3: We consider the polynomial $f(X) = X^6 - 1 \in \mathbb{Q}[X]$. Then, since the polynomial factorizes in $\mathbb{C}[X]$ as $f(X) = (X^3 - 1)(X^3 + 1) = (X - 1)(X^2 + X + 1)(X+1)(X^2 - X + 1)) = (X-1)(X-\omega)(X-\omega^2)(X+1)(X+\omega)(X+\omega^2) \in \mathbb{C}[X]$, its splitting field is $\mathbb{Q}[\omega]$, and we are in the same situation as in the previous example. Thus $X^3 - 1$ and $X^6 - 1$ share the same splitting field, namelly $\mathbb{Q}(\omega) = \mathbb{Q}(i\sqrt{3})$.

Example 4: We consider the polynomial $f(X) = X^3 - 2 = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2}) \in \mathbb{C}[X]$. Its splitting field is $\mathbb{Q}[\sqrt[3]{2}, \omega]$, with $[\mathbb{Q}[\sqrt[3]{2}, \omega] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[3]{2}, \omega] : \mathbb{Q}[\sqrt[3]{2}] \cdot [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 2 \cdot 3 = 6$. Thus, we can view $\mathbb{Q}[\sqrt[3]{2}, \omega]$ as a vector-space of dimension 6 over $\mathbb{Q}$, with base, for example, $B = \{1, \sqrt[3]{2}, \sqrt[3]{2^2}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{2^2}\}$.

Every $\phi \in G = \mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}, \omega]/\mathbb{Q})$ will be determined by the images of $\sqrt[3]{2}$ and ω.

$$(\sqrt[3]{2})^3 = 2 \Rightarrow \phi(\sqrt[3]{2})^3 = 2 \Rightarrow \to \phi(\sqrt[3]{2}) = \Big\{ \sqrt[3]{2}\omega\sqrt[3]{2}\omega^2\sqrt[3]{2}$$

$$(\omega)^2 + \omega + 1 = 0 \Rightarrow \phi(\omega)^2 + \phi(\omega) + 1 = 0 \Rightarrow \phi(\omega) = \{\omega - \omega$$

Consequenly, $G = \{\mathrm{Id.}, \rho, \rho^2, \tau\}$, with

$$\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \rho(\omega) = \omega,$$

$$\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2,$$

with $\rho^3 = \tau^2 = \mathrm{Id.}$, and $\tau\rho = \rho^2\tau$. The zeros of f are $\mathrm{Zeros}(f) = \{\alpha_1 = \sqrt[3]{2}, \alpha_2 = \omega\sqrt[3]{2}, \alpha_3 = \omega^2\sqrt[3]{2}\}$. Thus, the inyective homomorphism $\theta : G \hookrightarrow S_{\mathrm{Zeros}(f)} \simeq S_3$, allows us to identify G with the subgroup $H = \langle (1\ 2\ 3), (2\ 3) \rangle < S_3$, via

$$\phi_1 \leftrightarrow \mathrm{Id.},\ \rho \leftrightarrow (1\ 2\ 3),\ \rho = 2 \leftrightarrow (1\ 3\ 2),\ \tau \leftrightarrow (2\ 3).$$

But then, $\langle (1\ 2\ 3), (2\ 3) \rangle = S_3$, so $G \simeq S_3$. There are six subgroups in G: G, which fixes the field $\mathbb{Q}[\sqrt[3]{2}, \omega]^G = \mathbb{Q}$; $\langle (1\ 2\ 3) \rangle$, which fixes the only quadratic sub-field, $\mathbb{Q}[\sqrt[3]{2}, \omega]^{\langle (1\ 2\ 3) \rangle} = \mathbb{Q}[\omega]$; $\langle (12) \rangle$, which fixes the field $\mathbb{Q}[\sqrt[3]{2}]^{\langle (1\ 2) \rangle} = \mathbb{Q}[\omega^2\sqrt[3]{2}]$; $\langle (1\ 3) \rangle$, which fixes the field $\mathbb{Q}[\sqrt[3]{2}]^{\langle (1\ 3) \rangle} = \mathbb{Q}[\omega\sqrt[3]{2}]$; $\langle (2\ 3) \rangle$ which fixes $\mathbb{Q}[\sqrt[3]{2}]^{\langle (2\ 3) \rangle} = [\sqrt[3]{2}]$; and $\{\mathrm{Id.}\}$ which fixes $\mathbb{Q}[\sqrt{2}, i]$. Thus, the Galois correspondence is

$$\mathbb{Q}[\sqrt[3]{2}, \omega] \leftrightarrow \{\mathrm{Id.}\}\mathbb{Q}[\omega[\sqrt[3]{2}] \leftrightarrow \langle (1\ 3) \rangle\mathbb{Q}[\omega^2[\sqrt[3]{2}] \leftrightarrow \langle (1\ 2) \rangle\mathbb{Q}[\sqrt[3]{2}] \leftrightarrow \langle (2\ 3) \rangle\mathbb{Q}[\omega] \leftrightarrow (1\ 2\ 3)\mathbb{Q} \leftrightarrow G = S_3$$