Lecture 21 : Galois Theory Begins

Évariste Galois (1811– 1832) pioneered this theory which examines how the solution of $f(x) = 0$ for $f(x) \in F[x]$ is attained in some extension field K/F ... in short, the secret is locked away in the algebraic structure of the splitting field. It will take a few lectures to unpack the details.

Def^{n} ① An isomorphism σ of K is called an <u>automorphism</u> of K and we write $\sigma \in \text{Aut}(K)$. If $\alpha \in K$ we write $\sigma\alpha$ for $\sigma(\alpha)$.

② An automorphism $\sigma \in \text{Aut}(K)$ is said to <u>fix</u> an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If F is subset of K, then an automorphism σ is said to <u>fix</u> F if it fixes <u>all</u> the elements of F; $\sigma a = a \quad \forall a \in F$.

Notice any automorphism fixes 1; $\sigma(1) = 1$ then since 1 generates the prime subfield of a given field we find $\sigma a = a \quad \forall a \in$ prime subfield. It follows $\text{Aut}(\mathbb{Q}) = \{1\}$ and $\text{Aut}(\mathbb{F}_p) = \{1\}$ where we use 1 to denote identity mapping.

Def^{n}/ Let K/F be an extension of fields. Let $\mathrm{Aut}(K/F)$ be the collection of automorphisms which fix F.

Proposition (1)

$\mathrm{Aut}(K)$ is a group under composition and $\mathrm{Aut}(K/F)$ is a subgroup.

Proof: If $\sigma_1, \sigma_2 \in \mathrm{Aut}(K)$ then $\sigma_1\sigma_2, \sigma_1^{-1} \in \mathrm{Aut}(K)$ since composition and inverse of an isomorphism is once again an isomorphism. Also, $1 \in \mathrm{Aut}(K) \neq \emptyset$ hence $\mathrm{Aut}(K)$ is subgroup of all bijections of K under composition. If $\sigma, \tau \in \mathrm{Aut}(K/F)$ then

$$\sigma\tau x = \sigma x = x \quad \forall x \in F \Rightarrow \sigma\tau \in \mathrm{Aut}(K/F)$$

$$x = \sigma\sigma^{-1}x = \sigma^{-1}\sigma x \Rightarrow \sigma^{-1}x = x \Rightarrow \sigma^{-1} \in \mathrm{Aut}(K/F)$$

thus $\mathrm{Aut}(K/F)$, which contains 1, is subgroup of $\mathrm{Aut}(K)$. //

Proposition 2:

Let K/F be a field extension and $\alpha \in K$ algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$ $\sigma\alpha$ is a root of the minimal poly. for α over F. That is, Aut (K/F) permutes the roots of irreducible polys. Equivalently, any polynomial in F having α as root also has $\sigma\alpha$ as a root.

Proof: Suppose that $a_0, a_1, \ldots, a_{n-1} \in F$ and α satisfies the equation $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 = 0$. Suppose $\sigma \in \mathrm{Aut}(K/F)$ then

$$\sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = \sigma(0)$$

$$\Rightarrow (\sigma(\alpha))^n + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} + \cdots + \sigma(a_2)(\sigma(\alpha))^2 + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) = 0$$

However, $\sigma(a_{n-1}) = a_{n-1}, \ldots, \sigma(a_2) = a_2, \sigma(a_1) = a_1, \sigma(a_0) = a_0$ thus,

$$(\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \cdots + a_2(\sigma(\alpha))^2 + a_1\sigma(\alpha) + a_0 = 0$$

Therefore, if $f(x) \in F[x]$ and $f(\alpha) = 0$ then we have shown $f(\sigma(\alpha)) = 0$ for any $\sigma \in \mathrm{Aut}(K/F)$, the proposition follows. //

Remark: when K extends F by the adjoinment of one or several generators as in $K = F(\alpha)$ or $K = F(\alpha, \beta)$ etc. Then to understand the structure of $\mathrm{Aut}(K/F)$ is essentially governed by how generators of K over F can map to other generators, these will be roots to some common polynomial. Anyway, since every $\sigma \in \mathrm{Aut}(K/F)$ fixes F, the part which makes σ special falls on elements of K outside F.

$\boxed{E1}$ $K = \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ has generators $\pm\sqrt{2}$ (roots of x^2-2). Then $\tau \in Aut(K/\mathbb{Q})$ a.k.a. $\tau \in Aut(\mathbb{Q}(\sqrt{2}))$ since $\mathbb{Q}$ is prime subfield any automorphism fixes rational #'s within K.

$$\tau(a+b\sqrt{2}) = a \pm b\sqrt{2}$$

We either have $\sqrt{2} \underbrace{\longmapsto}_{1} \sqrt{2}$ or $\sqrt{2} \underbrace{\longmapsto}_{\sigma} -\sqrt{2}$

$$\underbrace{\boxed{Aut(\mathbb{Q}(\sqrt{2})) = \{1, \sigma\}}}_{\text{cyclic group of order 2.}} \qquad \sigma\sigma = 1$$

$\boxed{E2}$ $K = \mathbb{Q}(\sqrt[3]{2})$, $\tau \in Aut(K/\mathbb{Q})$ is determined by its action on $\sqrt[3]{2}$,

$$\tau\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right) = a + b\,\tau\sqrt[3]{2} + c(\tau\sqrt[3]{2})^2$$

Now, τ being a field $\mathbb{Q}$-fixing automorphism we know τ must map to solutions of x^3-2 (since $\sqrt[3]{2}$ is root of x^3-2). But, $\sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2 \notin \mathbb{Q}(\sqrt[3]{2})$ thus we <u>must</u> map $\sqrt[3]{2} \longmapsto \sqrt[3]{2}$ under τ

$\therefore$ $\underline{\tau = 1}$ and $\boxed{Aut(\mathbb{Q}(\sqrt[3]{2})) = \{1\}}$

If K/F is a finite extension of F then $\mathrm{Aut}(K/F)$ is a finite group. Generally, to each extension K/F we can associate the group $\mathrm{Aut}(K/F)$. This also goes the other way and associate an extension to a particular subgroup of automorphisms.

Proposition (3)

Let $H \leq \mathrm{Aut}(K)$ be a subgroup of Automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.

Proof: Def^n/ $F = K^H = \{x \in K \mid \sigma(x) = x \quad \forall \sigma \in H\}$

Let $h \in H$ and $a, b \in F = K^H$ then $h(a) = a$, $h(b) = b$ thus $h(a \pm b) = h(a) \pm h(b) = a \pm b$ $\therefore$ $a \pm b \in F$. Also, $h(ab) = h(a)h(b) = ab$ and $h(a^{-1}) = h(a)^{-1} = a^{-1}$ thus $ab, a^{-1} \in F$. Thus F is closed under addition and multiplication, we've shown F is a subfield of K.//

Def^n/ If $H \leq \mathrm{Aut}(K)$ then K^H is the fixed field of H

Remark: the proof of Prop. 3 did not use the subgroup property of H. We could just as well take $S \subseteq \mathrm{Aut}(K)$ where S is any old subset of automorphisms of K and form $K^S = \{x \in K \mid \sigma(x) = x \quad \forall \sigma \in S\}$ this is still a subfield of K by proof of Prop 3.

PROPOSITION (4)

The association of groups to fields and fields to groups defined in Propositions 2 & 3 is an inclusion reversing association,

(1.) if $F_1 \subseteq F_2 \subseteq K$ for subfields F_1 & F_2 then $Aut(K/F_2) \leq Aut(K/F_1)$.

(2.) if $H_1 \leq H_2 \leq Aut(K)$ are subgroups of $Aut(K)$ with associated fixed fields F_1 and F_2 then $F_2 \subseteq F_1$. $(K^{H_2} \subseteq K^{H_1})$

$\boxed{\text{Remark:}}$ $F_1 \subseteq F_2 \implies Aut(K/F_2) \leq Aut(K/F_1)$

$H_1 \leq H_2 \implies K^{H_2} \subseteq K^{H_1}$

Proof: we just need to show the inclusions since Prop 1 & 2 already give $Aut(K/F)$ a subgroup and K^H a subfield. Suppose $F_1 \subseteq F_2 \subseteq K$ and $\sigma \in Aut(K/F_2)$ then suppose $x \in F_1$ then $x \in F_2$ since $F_1 \subseteq F_2$ and so $\sigma(x) = x$ since σ fixes F_2. Hence $\sigma \in Aut(K/F_1)$ since it fixed an arbitrary F_1 element $\therefore Aut(K/F_2) \subseteq Aut(K/F_1)$. Likewise, if $H_1 \leq H_2 \leq Aut(K)$ and $a \in K^{H_2}$ then for any $\tau \in H_1$ we have $\tau \in H_2$ thus $\tau(a) = a$ and so $a \in K^{H_1}$ $\therefore$ $K^{H_2} \subseteq K^{H_1}$ //

Proposition (5)

Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then

$$|\mathrm{Aut}(E/F)| \leq [E:F]$$

with equality if $f(x)$ is separable over F

Proof: maybe next time, see p. 561–562 of §14.1 of D&F. //

In fact, it can be shown that $|\mathrm{Aut}(K/F)| \leq [K:F]$ for <u>any</u> finite extension K/F.

Def^n/ Let K/F be a finite extension. Then K is said to be GALOIS over F and K/F is a <u>GALOIS EXTENSION</u> if $|\mathrm{Aut}(K/F)| = [K:F]$.
If K/F is Galois, the group automorphisms $\mathrm{Aut}(K/F)$ is called the <u>GALOIS GROUP</u> of K/F and we denote $\mathrm{Aut}(K/F) = \mathrm{Gal}(K/F)$.

Corollary (6)

If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

Def^n/ If $f(x)$ is a separable polynomial over F, then the Galois group of $f(x)$ over F is the Galois group of the splitting field of $f(x)$ over F