Galois Theory

Math 31 – Summer 2013

Dartmouth College

August 21, 2013

Galois and Abel

Évariste Galois

Niels Henrik Abel

The Idea of Galois

Permute the roots of $f(x) = (x^2 - 2)(x^2 - 3)$:

$$\iota = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ -\sqrt{3} \mapsto -\sqrt{3} \end{cases} \qquad \sigma_1 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ -\sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

$$\sigma_2 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ -\sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ -\sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \sigma_3 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ -\sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ -\sqrt{3} \mapsto \sqrt{3} \end{cases}$$

Permutation of roots = "change of basis" for splitting field K

$$\begin{array}{c}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \\ \Big\downarrow \sigma_3 \\ \{1, -\sqrt{2}, -\sqrt{3}, \sqrt{6}\}\end{array}$$

This map is a ring homomorphism from K to K, and it's actually an automorphism of K that fixes $\mathbb{Q}$.

Modern Galois Theory

These automorphisms are denoted by:

$$\text{Gal}(K/\mathbb{Q}) = \{\sigma \in \text{Aut}(K) : \sigma(a) = a \text{ for all } a \in \mathbb{Q}\}.$$

Galois group of K over $\mathbb{Q}$. Also,

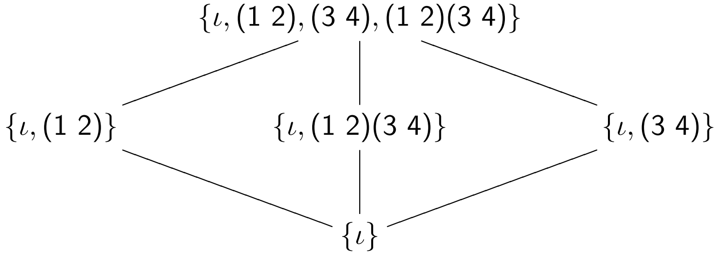
$$\text{Gal}(K/\mathbb{Q}) \cong \text{Gal}(f).$$

Note:

$$|\text{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}].$$

Subgroup Lattice

Ex: $f(x) = (x^2 - 2)(x^2 - 3)$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

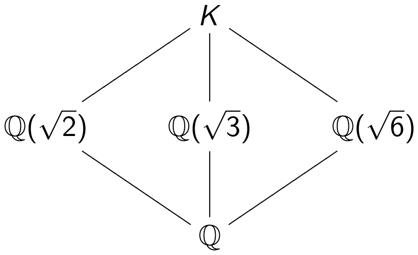


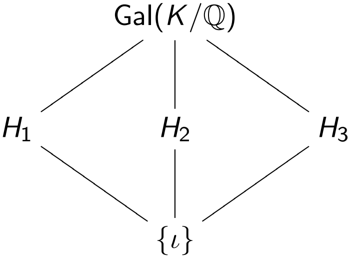
Subgroups and Fields

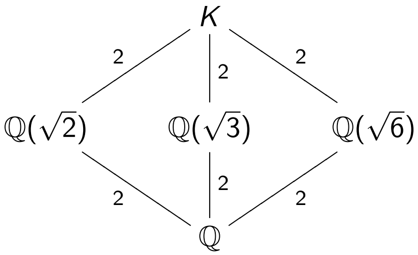
$H_1 = \{\iota, (3\ 4)\}$ fixes the field $\mathbb{Q}(\sqrt{2})$.

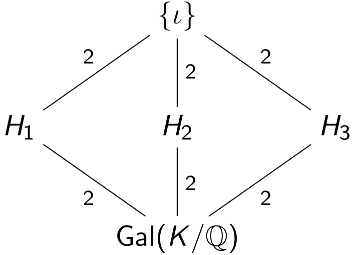
$H_2 = \{\iota, (1\ 2)\}$ fixes the field $\mathbb{Q}(\sqrt{3})$.

$H_3 = \{\iota, (1\ 2)(3\ 4)\}$ fixes the field $\mathbb{Q}(\sqrt{6})$.









In general: if F is a subfield of K, then

$$[F : \mathbb{Q}] = [\mathrm{Gal}(K/\mathbb{Q}) : \mathrm{Gal}(K/F)].$$

Galois Theory in a Nutshell

The main things to take away:

1. $|\text{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$
2. There is a one-to-one correspondence between subgroups of G and subfields of K.
3. If F is a subfield of K, then

$$[F : \mathbb{Q}] = [\text{Gal}(K/\mathbb{Q}) : \text{Gal}(K/F)].$$