II. Galois group of an extension.

First properties and examples.

Let E be a field; recall that an automorphism of E is a field isomorphism $\sigma : E \to E$. The set $\mathrm{Aut}(E)$ of all automorphisms of E is a group for the composition of maps. Let $k \subset E$ be a subfield, that is E/k is a field extension. Then:

$$\mathrm{Gal}(E/k) := \{ \sigma \in \mathrm{Aut}(E) : \sigma(x) = x \quad \forall x \in k \}$$

is a subgroup of $\mathrm{Aut}\, E$.

Definition II. 1 $\mathrm{Gal}(E/k)$ is called the Galois group of the extension E/k.

Recall that E is a k-vector space i

Exercise I.2. Every $\sigma \in Gal(E/k)$ is an invertible k-linear map of E.

Example II.3 : Let $k = \mathbb{R}$, $E = \mathbb{C}$. Show that $Gal(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, \sigma\}$ where σ is the complex conjugation.

Let now $f \in k[X]$ be a polynomial and $E \supset k$ a field extension in which f is a product of linear factors (f splits in $E[X]$, and let $R(f) \subset E$ be the set of roots.

Lemma II.4 (Prop. A-5.1) The group $Gal(E/k)$ permutes the set $R(f)$ of roots of f.

Proof: ~~Let $\sigma \in Gal(E|k)$ and $\alpha \in R(f)$~~

Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in k[X]$

$\alpha \in R(f)$ and $\sigma \in Gal(E|k)$.

We have:

$$0 = \sigma(f(\alpha)) = \sigma(a_n \alpha^n + \cdots + a_0)$$

$$= \sigma(a_n)\sigma(\alpha)^n + \cdots + \sigma(a_0)$$

$$= a_n \sigma(\alpha)^n + \cdots + a_0$$

$$= f(\sigma(\alpha))$$

Which implies $\sigma(\alpha) \in R(f)$. Thus $\sigma(R(f)) \subset R(f)$ and since σ is injective and $R(f)$ is finite we have $\sigma(R(f)) = R(f)$. ∎

Let $f \in k[X]$.

Def. II.5 The Galois group of f "is" the Galois group $Gal(E|k)$ where E is a splitting field of f.

Exercise II.6. Show that if E and E' are splitting fields of f the groups $Gal(E/k)$ and $Gal(E'/k)$ are isomorphic.

Recall that if X is a set we denote by $S_X = Aut_{Sets}(X)$ the group of all bijections of X and if $n \in \mathbb{N}$, by $S_n = Aut_{Sets}(\{1, 2, \dots, n\})$ the group of permutations of n elements.

(Lemma A.5.2 / Thm. A.5.3)

Lemma II.7 If $E \supset k$ is the splitting field of a polynomial $f \in k[x]$, then the restriction map

$$Gal(E/k) \longrightarrow S_{R(f)}$$

$$\sigma \longmapsto \sigma|_{R(f)}$$

is an injective group homomorphism.

In particular $Gal(E/k)$ is isomorphic to a subgroup of $S_{R(f)}$.

Proof: That it is a homomorphism follows from $(\sigma\tau)|_{R(f)} = \sigma|_{R(f)} \circ \tau|_{R(f)}$.

Now let $R(f) = \{\beta_1, \ldots, \beta_n\} \subset E$.

Since $E = k(\beta_1, \ldots, \beta_n)$

$$= \left\{ \frac{f(\beta_1, \ldots, \beta_n)}{g(\beta_1, \ldots, \beta_n)} : f, g \in k[X_1, \ldots, X_n],\ g(\beta_1, \ldots, \beta_n) \neq 0 \right\}$$

We have:

$$\sigma\left(\frac{f(\beta_1, \ldots, \beta_n)}{g(\beta_1, \ldots, \beta_n)}\right) = \frac{f(\sigma(\beta_1), \ldots, \sigma(\beta_n))}{g(\sigma(\beta_1), \ldots, \sigma(\beta_n))}$$

Thus if $\sigma(\beta_i) = \beta_i$, $1 \leq i \leq n$ we get that $\sigma = id_E$ which proves injectivity.

□

Observe that we did not put the cardinality of $R(f)$ in relation with the degree of f.

In fact:

Example II.8: $k = \mathbb{F}_p(t)$, $f(X) = X^p - t$

Then (1) $f \in \mathbb{F}_p(t)[X]$ is irreducible.

(2) If E is a splitting field of f,

$|R(f)| = 1$.

We leave (1) as an exercise and show (2): let $\alpha \in E$ be a root of f, that is $\alpha^p = t$. Then we have using that E has characteristic p:

$$(X-\alpha)^p = X^p - \alpha^p = X^p - t.$$

Thus by uniqueness of factorization we conclude $R(f) = \{\alpha\}$.

22.2.18.