Def IV.12 : A finite extension E/k is a Galois extension if it satisfies any of the equivalent properties in Thm IV-11.

Let $k \subseteq B \subseteq E$ with E/k Galois; it is not necessarily true that B/k is, since it doesn't need to be normal.

However

Corollary IV.13 If E/k is Galois, so is E/B.

Proof: Indeed if $f \in k[x]$ is a separable polynomial with $SF\ E$, then $f \in B[x]$ is separable as well and its splitting field is E. ∎

We now give a criterion in the above situation for B/k to be Galois:

Proposition IV.14 Let $k \subset B \subset E$ with E/k Galois. Then:

B/k is Galois $\iff \sigma(B) = B \quad \forall \sigma \in Gal(E/k)$

Proof. ($\Rightarrow$) If B/k is Galois, there is $g \in k[X]$ (separable) whose splitting field is B. But for every $\sigma \in Gal(E/k)$, $\sigma(R(g)) = R(g)$ which with $B = k(R(g))$ implies $\sigma(B) = B$.

($\Leftarrow$): We can define the restriction homomorphism:

$$Gal(E/k) \longrightarrow Gal(B/k)$$
$$\sigma \longmapsto \sigma|_B$$

and let H be its image. We have

$$k \subset B^{Gal(B/k)} \subset B^{H} \subset E^{Gal(E/k)} = k$$

which implies $k = B^{Gal(B|k)}$. ∎

Application to fields of rational functions.

Let k be a field; recall that the field of rational functions on n indeterminates

$$k(T_1, \dots, T_n)$$

is the fraction field of the polynomial ring $k[T_1, \dots, T_n]$.

Recall that the latter is an integral domain.

Consider now the polynomial

$$f \in k(T_1, \dots, T_n)[X]$$

defined by $f(X) = (X - T_1) \cdots (X - T_n)$.

$$= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

then $a_n = 1$,

$$a_{n-1} = -\sum_{i=1}^{n} r_i \quad \ldots, \quad a_0 = (-1)^n r_1 \cdots r_n$$

and in general:

$$a_{n-d} = (-1)^d \underbrace{\sum_{i_1 < \cdots < i_d} r_{i_1} \cdots r_{i_d}}_{e_d(r_1, \ldots, r_n)}$$

where $e_d \in k[T_1, \ldots, T_n]$ is the d'th elementary symmetric polynomial.

Now given $\rho \in S_n$, define $\forall\ r = \frac{p}{q} \in k(T_1, \ldots, T_n)$:

$$A_\rho r(T_1, \ldots, T_n) = \frac{p(T_{\rho(1)}, \ldots, T_{\rho(n)})}{q(T_{\rho(1)}, \ldots, T_{\rho(n)})}.$$

Observe

(1) $r \longmapsto \rho_\sigma r$ is $\forall \sigma \in S_n$ a field automorphism of $k(Y_1, \dots, Y_n)$.

(2) $\rho_\sigma e_d = e_d \qquad 0 \leq d \leq n.$

The first observation is an exercise, while for the second: observe that $\rho_\sigma e_d$ is $(-1)^d$ times the coefficient of

$$(X - Y_{\sigma(1)}) \cdots (X - Y_{\sigma(n)})$$

of degree X^{n-d}. But this polynomial equals: $(X - Y_1) \cdots (X - Y_n)$.

Thus, putting $K = k(e_0, \dots, e_n)$

$$E = k(Y_1, \dots, Y_n)$$

the above hom. gives a hom.

$$S_n \longrightarrow \mathrm{Gal}(E/K). \quad (*)$$

Observe: $f \in k(e_0, .., e_n)[X]$ has splitting field E and in particular is separable. Hence E/K is a Galois extension. In addition $(*)$ must be an isomorphism since $\mathrm{Gal}(E/K)$ injects into $\mathrm{Sym}\{Y_1, \dots, Y_n\}$.

Thus:

Theorem IV.15 Every symmetric rational function over k is a rational function in the elementary symmetric polynomials.

Proof: By Galois theory:

$$k(Y_1, \dots, Y_n)^{S_n} = k(e_1, \dots, e_n).$$

∎

Now we are going to treat the fundamental theorem(s) of Galois theory, also called Galois correspondence.

Given a group G call $Sub(G) = \{H \subset G : H \text{ is a subgroup of } G\}$ and given a field extension E/k,

$Int(E/k) = \{B \subset E : B \text{ is a subfield of } E \text{ containing } k\}$,

the set of all intermediary subfields of E/k. Both sets $Sub(G)$ and $Int(E/k)$ are ordered by inclusion.

Theorem IV.16 Let E/k be a (finite) Galois extension.

(1) The map $\gamma : Sub(Gal(E/k)) \longrightarrow Int(E/k)$

$$H \longmapsto E^H$$

which to every subgroup of $Gal(E/k)$ associates its fixed field is an inclusion reversing bijection whose inverse is given by

$$\delta : Int(E/k) \longrightarrow Gal(E/k)$$
$$B \longmapsto Gal(E/B),$$

which is order reversing as well.

(2) $B \in Int(E/k)$ is a Galois extension of k iff $Gal(E/B)$ is a normal subgroup of $Gal(E/k)$, in which case

$$Gal(E/k)/Gal(E/B) \cong Gal(B/k).$$

Proof (1) Since $Gal(E/k)$ is finite, Corollary IV-10 implies that if $E^{H_1} = E^{H_2}$ then $H_1 = H_2$, that is, δ is injective.

Next we show that $\gamma\delta = Id_{Int(E/k)}$.

We have $\gamma\delta(B) = \gamma(\mathrm{Gal}(E|B)) = E^{\mathrm{Gal}(E|B)}$

and the latter equals B by Thm IV-11 (2) since (see Cor. IV.13) E/B is a Galois extension. ~~Thus δ is injective and $\gamma\delta = \mathrm{id}_{\mathrm{Int}(E|k)}$ which implies that~~

Thus δ is surjective and hence bijective. But then $\gamma\delta = \mathrm{Id}_{\mathrm{Int}(E|k)}$ implies that γ is bijective as well.

(2) Assume B/k is a Galois extension, then it is in particular a normal extension and hence by Thm II.26, $\sigma(B) = B$ $\forall \sigma \in \mathrm{Gal}(E/k)$ and $\mathrm{Gal}(E/B)$ is the kernel of the homomorphism

$$\mathrm{Gal}(E/k) \longrightarrow \mathrm{Gal}(B/k)$$
$$\sigma \longmapsto \sigma(B)$$

that induces an isomorphism

$$Gal(E/k)/Gal(E/\Omega) \cong Gal(\Omega/k).$$

In particular $Gal(E/B)$ is a normal subgroup of $Gal(E/k)$.

Conversely: assume $Gal(E/B)$ is a normal subgroup of $Gal(E/k)$; we are going to show that $\sigma(B) = B$ $\forall \sigma \in Gal(E/k)$. By Prop IV.14 this will imply that B/k is Galois. Now since E/B is Galois, we have

$$B = E^{Gal(E/B)}.$$

Thus let $\sigma \in Gal(E/k)$ and $\xi \in B = E^{Gal(E/B)}$.

Then, $\forall\, h \in Gal(E/B)$:

$$h(\sigma(\xi)) = \sigma(\sigma^{-1}h\sigma)(\xi), \text{ but}$$

$\sigma^{-1}h\sigma \in Gal(E/B)$, hence $\sigma^{-1}h\sigma(\xi) = \xi$

which implies $h(\sigma(\beta)) = \sigma(\beta)$ and

thus $\sigma(\beta) \in E^{Gal(E/B)} = B$. ∎

Example IV.17.

Let $f(X) = X^3 - 2 \in \mathbb{Q}(X)$ and

E its splitting field.

First we observe that f is irreducible:

[indeed otherwise it would have a

root $\frac{p}{q} \in \mathbb{Q}$; say p, q coprime. But

then $p^3 = 2q^3 \Rightarrow 2 | p \Rightarrow 8 | 2q^3 \Rightarrow$

$4 | q^3 \Rightarrow 2 | q$ contr.]

Let $\beta = \sqrt[3]{2} \in \mathbb{R}$, $\omega = e^{\frac{2\pi i}{3}}$.

Then the roots of f are

$$\alpha_1 = \beta, \quad \alpha_2 = \beta\omega, \quad \alpha_3 = \beta\omega^2.$$