Take account that $\sigma_i(c_j) = c_j \quad \forall i,j$:

$$\sum_{i=1}^{n} c_i \, \sigma_i(y_i) = 0.$$

Which can be restated as:

$$\begin{pmatrix} \sigma_1(y_1) & \cdots & \sigma_1(y_n) \\ \vdots & & \\ \sigma_n(y_1) & \cdots & \sigma_n(y_n) \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

But, by our choice of $y_1, \ldots, y_n$, the rank (over E) of this matrix is n.

Hence $c_1 = \cdots = c_n = 0$. ∎

Now we can conclude:

Prop. IV-9: Let $G \subset \mathrm{Aut}\, E$ be a finite subgroup. Then $[E : E^G] = |G|$.

Proof: By contradiction: let $|G| = n$, $G = \{\sigma_1, \dots, \sigma_n\}$ and $b_1, \dots, b_m$ a set of E that is linearly independent over E^G with $m > n$.

Consider the linear map

$$T: E^m \longrightarrow E^n$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \mapsto \begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_m) \\ \vdots & & \\ \sigma_n(b_1) & \cdots & \sigma_n(b_m) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Then $\operatorname{Ker} T \neq (0)$.

Main observation: if $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \operatorname{Ker} T$, then $\begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_m) \end{pmatrix} \in \operatorname{Ker} T \quad \forall \sigma \in G$.

Indeed: if $\sum_{j=1}^{m} \sigma_i(b_j) x_j = 0 \quad \forall i$, $1 \leq i \leq n$.

then $\sum_{j=1}^{m} \sigma \sigma_i(b_j) \sigma(x_j) = 0$.

Now since G is a group,

$$\sigma \sigma_i = \sigma_{s(i)}$$

where $s \in S_n$ is a permutation.

Therefore $$\sum_{j=1}^{m} \sigma_{s(i)}(b_j) \sigma(x_j) = 0 \quad \forall i$$

which proves the observation.

Let now r = minimal number of non-zero coordinates for a nonzero vector $v \in \ker T$.

Claim: $r \geq 2$. Otherwise there is say $\begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \ker T$, $x_1 \neq 0$

that is, $x_1 \begin{pmatrix} \sigma_1(b_1) \\ \vdots \\ \sigma_n(b_1) \end{pmatrix} = 0$ which together with $b_1 \neq 0$ leads to a contradiction.

19.4.88

Thus $r \geq 2$: pick now such a vector

$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in \ker T$ with r non-zero coordinates; ~~aa~~.

observe that $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \notin (E^G)^m$

since otherwise we would have with $\sigma_1 = id$,

$$\sum_{i=1}^{m} b_i x_i = 0$$

contradicting the assumption that $b_1, \ldots, b_m$ is linearly independent over E^G.

Thus there is $\sigma \in G$ with

$$\begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_m) \end{pmatrix} \neq \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Say $\sigma(x_1) \neq x_1$, in particular $x_1 \neq 0$.

Then: $\frac{1}{\sigma(x_1)}\begin{pmatrix}\sigma(x_1)\\ \vdots \\ \sigma(x_m)\end{pmatrix} - \frac{1}{x_1}\begin{pmatrix}x_1\\ \vdots \\ x_m\end{pmatrix} \in \ker T$

is a ~~non-zero~~ vector in $\ker T$ with at least one more vanishing coordinate.

Hence it vanishes, that is:

$$0 \neq \begin{pmatrix}1\\ x_2/x_1\\ \vdots \\ x_m/x_1\end{pmatrix} \in \ker T \cap (E^G)^m$$

a contradiction. ∎

We can draw the following remarquable conclusion:

Corollary IV-10. Let G and H be finite subgroups of $\mathrm{Aut}\, E$. Then

$$E^G \subset E^H \iff H < G.$$

Proof: ($\Leftarrow$) is clear.

($\Longrightarrow$) Assume $H \not\subseteq G$. Then there is $\sigma \in H$ with $\sigma \notin G$. But σ fixes every element of E^H, hence of E^G. This implies $E^G = E^{G \cup \{\sigma\}}$ and using prop. IV.9 and lemma IV.7:

$$|G| = [E : E^G] = [E : E^{G \cup \{\sigma\}}]$$

$$\geq |G \cup \{\sigma\}| = |G| + 1$$

a contradiction. ∎

Separability really comes to the forefront in the next result that lays the basis for the Galois correspondence and leads to the notion of Galois extension.

Recall that

— an irreducible polynomial is separable if it has no repeated roots.

— an arbitrary polynomial is separable if its irreducible factors are.

Theorem IV-11 :

Let E/k be a finite extension with Galois group $G := Gal(E/k)$.

The following are equivalent:

(1) E is the splitting field of a separable polynomial in $k[x]$.

(2) $k = E^G$

(3) Any irreducible polynomial in $k[x]$ that has a root in E splits in E.

(1) is separable and

Proof (1) $\Rightarrow$ (2) By Thm. IV.17 (2)

$[E:k] = |G|$; by Prop. IV-9, $[E:E^G] = |G|$

which together with $E^G \supset k$ implies $E^G = k$.

(2) $\Rightarrow$ (3)

Let $p \in k[x]$ be irreducible and $\alpha \in E$

$p(\alpha) = 0$. Let $St(\alpha) = \{\sigma \in G : \sigma(\alpha) = \alpha\}$

and define

$$q(x) := \prod_{\sigma \in G/St(\alpha)} (x - \sigma(\alpha)) .$$

Then: (1) q is a monic polynomial

(2) q has no repeated roots.

(3) $R(q) \subset R(p)$

(4) $q \in E^G[x] = k[x]$.

As a result, q divides p hence $q = p$

Which shows (3).

(3) $\Rightarrow$ (1)

Let $k \subset E' \subset E$ with $[E' : k]$ maximal such that E' is the splitting field of a separable polynomial $f' \in k[x]$. If $E' \neq E$, there is $\alpha \in E \setminus E'$. Then $p := \operatorname{irr}(\alpha, k) \in k[x]$ is an irreducible polynomial with a root in E; hence p is separable and splits in E. Now $f = p \cdot f'$ is separable, splits in E; let E'' be the splitting field of f. Then $E' \subsetneq E''$ which contradicts max. of $[E' : k]$. Hence $E' = E$.

□

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

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 $a_n = 1$,

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

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 $e_d \in k[r_1, \ldots, r_n]$ is the d'th elementary symmetric polynomial.

Now given $\rho \in S_n$, define $\forall\ r = \frac{p}{q} \in k(r_1, \ldots, r_n)$:

$$\rho_* r(r_1, \ldots, r_n) = \frac{p(r_{\rho(1)}, \ldots, r_{\rho(n)})}{q(r_{\rho(1)}, \ldots, r_{\rho(n)})}.$$

Observe

(1) $r \mapsto \rho_\sigma r$ 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: $f \in k(e_0, \dots, e_n)[X]$ 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:

$$k(Y_1, \dots, Y_n)^{S_n} = k(e_0, \dots, e_n).$$

∎