IV The Galois correspondence.

One way to motivate the Galois correspondence is via the question whether the converse of Thm III.18 holds, that is:

Assume $Gal(E/k)$ is solvable, does it imply that f is solvable by radicals?

More generally, is there a correspondence between subgroups of $Gal(E/k)$ and intermediary fields, that is extensions

$$k \subset \square \subset E.$$

The answer is yes under an additional hypothesis on E/k, namely separability. This is the main topic of this chapter.

Given a subset $H \subset \mathrm{Aut}\, E$, define

$$E^H = \{ a \in E : \sigma(a) = a \ \ \forall \sigma \in H \}.$$

This is clearly a subfield of E.

Def IV.1 E^H is the fixed field of H.

Remark IV.2: The correspondence

$$H \longmapsto E^H$$

is order reversing, that is: $H_1 \subset H_2$

$$\Rightarrow E^{H_2} \subset E^{H_1}.$$

Example IV.3: If E/k is an extension, then $k \subset E^{\mathrm{Gal}(E/k)}$.

As we know from Example II.8 with $k = \mathbb{F}_p(t)$ and $f(X) = X^p - t$,

E = Splitting field of f : $\mathrm{Gal}(E/k) = (e)$

so that $k \subsetneq E^{\mathrm{Gal}(E/k)} = E$.

This is one reason why separability will now play a major role.

Our first goal for now will be to determine the degree $[E : E^H]$ where $H < \mathrm{Aut}\, E$ is a finite subgroup of $\mathrm{Aut}\, E$. This will be done in the following sequence of lemmas.

Let now G be any group and E a field.

Def. IV.4 A character of G in E is an element of $\mathrm{Hom}(G, E^\times)$, that is a homomorphism from G into the multiplicative group $E^\times$.

Let E^G be the E-vector space of all E-valued functions on G.

Then

Prop. IV-5 (Dedekind) $\mathrm{Hom}(G, E^\times)$ is a linearly independent subset of E^G.

Proof. (By contradiction). Let $n \geq 1$ be minimal such that there are n distinct characters $\sigma_1, \ldots, \sigma_n$ that are linearly dependent. That is, there exist $c_1, \ldots, c_n$ in E not all zero such that

$(*)$ $c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0 \quad \forall x \in G.$

Observe — $n \geq 2$, indeed a character never vanishes.

— by minimality, $c_1 \neq 0, \ldots, c_n \neq 0$.

Since $\sigma_1 \neq \sigma_n$ there is $y \in G$ with $\sigma_1(y) \neq \sigma_n(y)$.

Evaluating at xy we get:

$$c_1 \sigma_1(x)\sigma_1(y) + \cdots + c_n \sigma_n(x)\sigma_n(y) = 0 \quad \forall x$$

Thus

$$c_1 \sigma_1(x)\frac{\sigma_1(y)}{\sigma_n(y)} + \cdots + c_{n-1}\sigma_{n-1}(x)\frac{\sigma_{n-1}(y)}{\sigma_n(y)} + c_n\sigma_n(x) = 0$$

which by subtracting from (x) gives:

$$(xx) \quad c_1\left(1 - \frac{\sigma_1(y)}{\sigma_n(y)}\right)\sigma_1(x) + \cdots + c_{n-1}\left(1 - \frac{\sigma_{n-1}(y)}{\sigma_n(y)}\right)\sigma_{n-1}(x) = 0$$

$\forall x$

Since $c_1\left(1 - \frac{\sigma_1(y)}{\sigma_n(y)}\right) \neq 0$, (xx) is a non-trivial linear dependence between $\sigma_1, \ldots, \sigma_{n-1}$ and hence contradicts the minimality of n. ∎

We will apply this to a finite subset $G \subset \mathrm{Aut}\, E$ in order to get a lower bound on $[E : E^G]$. But first we

We recall

Sublemma IV-6 : Let E be a field and S a set. Let $\{\sigma_1, \dots, \sigma_n\} \subset E^S$ be a linearly independent ~~set~~ n-tuple. Then there are elements $s_1, \dots, s_n$ in S such that:

$$\begin{pmatrix} \sigma_1(s_1) \\ \vdots \\ \sigma_n(s_1) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_1(s_n) \\ \vdots \\ \sigma_n(s_n) \end{pmatrix}$$

are linearly independent vectors in E^n.

Proof: Consider the subset of E^n

$$\overline{\sigma} := \left\{ \begin{pmatrix} \sigma_1(s) \\ \vdots \\ \sigma_n(s) \end{pmatrix} : s \in S \right\}$$

and let V be the vector subspace generated by it. If $V \neq E^n$ then there is a nonzero linear form $\lambda : E^n \to E$ with $V \subset \ker \lambda$.

Let $c_1, \dots, c_n$ not all zero with

$$\chi \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = c_1 y_1 + \dots + c_n y_n .$$

Then $\sum_{i=1}^{n} c_i \sigma_i(s) = 0 \quad \forall s \in S$,

contradiction. But then we can find in σ a basis of E^n, which proves the lemma. ∎

Lemma IV -7. Let $H = \{\sigma_1, \dots, \sigma_n\} \subset \mathrm{Aut}\, E$ be a subset consisting of n elements. Then $[E : E^H] \geq n$.

Remark IV -8 : In this situation we should not expect a more precise result since $E^H = E^{\langle H \rangle}$ where $\langle H \rangle$ is the subgroup of $\mathrm{Aut}\, E$ generated by H.

Proof: $\sigma_1|_{E^\times}, \dots, \sigma_n|_{E^\times}$ are n distinct characters of $E^\times$ in $E^\times$, hence by Prop. IV.5 linearly independent in $E^{E^\times}$.

Thus there are $y_1, \dots, y_n$ in $E^\times$ such that

$$\begin{pmatrix} \sigma_1(y_1) \\ \vdots \\ \sigma_n(y_1) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_1(y_n) \\ \vdots \\ \sigma_n(y_n) \end{pmatrix}$$

are lin. independent in E^n.

Claim: $\{y_1, \dots, y_n\} \subset E$ is linearly independent when we consider E as E^H-vector space.

Indeed: Let $c_1, \dots, c_n$ in E^H with

$$\sum_{i=1}^{n} c_i y_i = 0.$$

Applying $\sigma_1, \dots, \sigma_n$ we get, taking

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

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

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

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

which proves the observation.

Let now r = minimal number of non-zero coordinates for a non-zero 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.