§10.2

Recall that, if E is a splitting field of a separable polynomial in $F[x]$, then $|\mathrm{Gal}(E/F)| = [E:F]$.

(†) [More generally, we always have the fllg:
If E is a finite extension of F, then

$$|\mathrm{Gal}(E/F)| \leq [E:F].$$
]

To prove this, we will use a lemma about characters of a group in a field. [This is a big topic in math (harmonic analysis and representation theory), but ~~here~~ it's just used in passing in our context.]

Defn A character of a group G in a field F is a homomorphism from G to F^*.

Defn A finite n-tuple $\{\sigma_1, \ldots, \sigma_n\}$ of functions from a set X to a field F is linearly dependent if there exist elements $a_1, \ldots, a_n \in F$, not all zero, such that $\sum_{i=1}^{n} a_i \sigma_i = 0$.

Lemma Any finite nonempty set of characters of a group G in a field F is linearly independent (i.e, not linearly dependent).

[It is redundant to say "finite set of distinct characters" since we are referring to a set. The ~~set of elements~~ elements in the set can be arranged into an n-tuple of distinct elements.]

So — I'm abusing ~~not~~ defn. a little bit, ~~but~~ and so is our author

7

<u>Proof</u> is by <u>induction</u> on the number of characters.
The base case is $n=1$ and this is easy — <u>DO IT</u>!
Assume the induction hypothesis that any ~~of~~ $n-1$ distinct characters $\varphi_1, \dots, \varphi_{n-1}$ of G in F are independent.
Let $\varphi_1, \dots, \varphi_n$ be distinct homomorphisms from G into F^*, and let $a_1, \dots, a_n$ be elements of F such that

$$\sum_{i=1}^{n} a_i \varphi_i = 0 .$$

This means that (*) $\displaystyle\sum_{i=1}^{n} a_i \varphi_i(g) = 0 \quad \forall\, g \in G$

Fix $h \in G$ and
Replace g with hg: $\displaystyle\sum_{i=1}^{n} a_i \overbrace{\varphi_i(h)\varphi_i(g)}^{\varphi_i(hg)} = 0 \quad \forall\, g \in G$

Now multiply (*) by $\varphi_1(h)$: $\displaystyle\sum_{i=1}^{n} a_i \varphi_1(h)\varphi_i(g) = 0 \quad \forall\, g \in G$

Subtract to get $\displaystyle\sum_{i=2}^{n} a_i(\varphi_i(h) - \varphi_1(h))\varphi_i(g) = 0 \quad \forall\, g \in G$

The induction hypothesis implies that

$$a_i(\varphi_i(h) - \varphi_1(h)) = 0 \quad \text{for } i = 2, 3, \dots, n.$$

For each $i = 2 \dots n$, since $\varphi_i \neq \varphi_1$, $\exists\, h \in G$ s.th. $\varphi_i(h) - \varphi_1(h) \neq 0$, and so $a_i = 0$.

Thus (*) reduces to $a_1 \varphi_1 = 0$, and thus $a_1 = 0$, as in the base case you proved.

<u>Proof of (†)</u> Instead of doing a "formal" proof, let's talk thru this one.

Suppose that $[E:F]=n$

Take elements $\sigma_0 \ldots \sigma_n \in Gal(E/F)$.

We <u>want to show</u> that they can't be distinct.

To do so, <u>we will find</u> $a_0, \ldots, a_n \in E$ such that (not all zero)

(*) $$\sum_{j=0}^{n} a_j \sigma_j = 0 \quad \text{as a map from } E \text{ to } E.$$

Since $\sigma_j \in Aut(E)$, they are characters of E^* in E, so the $\{\sigma_j\}$ being dependent implies they are <u>not</u> distinct.

Now lets find such $a_j \in E$. (*) means

$$\sum_{j=0}^{n} a_j \sigma_j(u) = 0 \quad \forall\, u \in E$$

Lets first try to find $\{a_j\}$ that work for u in a basis $\{v_1, \ldots, v_n\}$ for ${}_FE$ (E as a vec. sp. over F).

That means we need $\{a_j\}$ such that

$$\sum_{j=0}^{n} a_j \sigma_j(v_i) = 0 \quad \text{for } i=1,\ldots,n$$

This is a homogeneous system of n equations for $n+1$ "unknowns" $\{a_j\}_{j=0}^{n}$, so there is always a nonzero solution $\{a_j\}_{j=0}^{n}$, meaning not all a_j are zero (one is nonzero).

Now, to go back to all $u \in E$; let $u \in E$ be given, and since $\{v_1, \ldots v_n\}$ is a basis for E over F, $\exists\, r_i \in F$ $(i=1,\ldots,n)$ s.th. $u = \sum_{i=1}^{n} r_i v_i$.

So $$\sum_{j=0}^{n} a_j \sigma_j(u) = \sum_{j=0}^{n} a_j \sigma_j\Big(\sum_{i=1}^{n} r_i v_i\Big) = \sum_{j=0}^{n} a_j \sum_{i=1}^{n} \sigma_j(r_i)\sigma_j(v_i)$$

$$= \sum_{j=0}^{n} a_j \sum_{i=1}^{n} r_i \sigma_j(v_i) = \sum_{i=1}^{n} r_i \sum_{j=0}^{n} a_j \sigma_j(v_i) = \sum_{i=1}^{n} r_i \cdot 0 = 0 \quad \checkmark$$

<u>Defn</u> Let E be a field, and let G be a finite subgroup of $\mathrm{Aut}(E)$. Define
$$E_G = \{a \in E : \sigma(a) = a \ \forall \sigma \in G\},$$
the <u>fixed field</u> of G.

Fact: E_G is a field.

<u>Theorem</u> (Dedekind–Artin) $[E : E_G] = |G|$

<u>Proof</u> Since $G \subset \mathrm{Gal}(E/E_G)$, $[E:E_G] \geq |G|$ by a previous theorem. Set $|G| = n < \infty$. It suffices to <u>prove that each subset of E containing $n+1$ elements is linearly dependent over E_G.</u>
Let Y be a subset of E with $|Y| = n+1$. The equations

$$(*) \qquad \sum_{u \in Y} x_u \sigma u = 0, \quad \sigma \in G$$

form an $n \times (n+1)$ homogeneous linear system for $\{x_u\}_{u \in Y}$, and thus there is a nonzero solution $x : Y \to E$ (i.e., $\exists\, u \in Y : x_u \neq 0$). Let this solution be minimal in the sense that the set $Y' = \{u \in Y : x_u \neq 0\}$ has minimal order over all nonzero solutions; and assume that, for some $v \in Y'$, $u_v = 1$ (show this is possible)

For each $\tau \in G$, $(*)$ yields

$$0 = \tau \sum_{u \in Y'} x_u \sigma u = \sum_{u \in Y'} \tau x_u \tau\sigma u \quad \forall \sigma \in G,$$

and since $\tau : G \to G :: \sigma \mapsto \tau\sigma$ is a bijection, we obtain

$$(\dagger) \qquad \sum_{u \in Y'} \tau x_u \sigma u = 0 \quad \forall \sigma \in G \ \forall \tau \in G.$$

(10)

By subtracting from (*) the same equation with $\tau = \varepsilon$, we obtain (remember $u_v = 1$ so $\tau(x_v) = 1$)

$$\sum_{u \in Y' \setminus \{v\}} (\tau x_u - x_u)\, \sigma u = 0 \quad \forall \sigma \in G \quad \forall \tau \in G$$

Since $\{\tau x_u - x_u\}_{u \in Y' \setminus \{v\}}$ is a solution to (*)

~~with fewer~~ and $|Y' \setminus \{v\}| < |Y'|$, the minimality of the solution $\{x_u\}$ implies that

$$\tau x_u - x_u = 0 \quad \forall \tau \in G \quad \forall u \in Y' \setminus \{v\}.$$

Thus $x_u \in E_G \quad \forall u \in Y' - \{v\}$ and therefore

$$\sum_{u \in Y} x_u u = 0$$

is a nonzero linear combination of the elements of Y with coefficients in E_G. This implies that the $n+1$ elements of Y are linearly dependent.

Correspondence between intermediate fields and subgroups

Let E/F be a field extension and $G = \mathrm{Gal}(E/F)$.

Given an intermediate field $K : F \subset K \subset E$ and a subgroup $H < G$, define

$$G > K' = \mathrm{Gal}(E/K) = \{\sigma \in G : \sigma(u) = u \ \forall\ u \in K\}$$

$$E > H^\circ = E_H = \{u \in E : \sigma(u) = u \ \forall\ \sigma \in H\}$$

H° is the fixed field of H, and K' is the galois group of E/K.

Lemma 2 of the textbook is straightforward to prove directly from the definitions of K' and H°.

(1-2) $K \subseteq K_1 \Rightarrow K' \supseteq K_1'$ and $H \subseteq H_1 \Rightarrow H^\circ \supseteq H_1^\circ$

(3-4) $K \subseteq K'^\circ$ and $H \subseteq H^{\circ\prime}$

(5-6) $K'^{\circ\prime} = K'$ and $H^{\circ\prime\circ} = H^\circ$

Defn For $F \subset K \subset E$ and $H < G$,

K'° is the Galois closure of K, and K is galois-closed if $K'^\circ = K$.
$H^{\circ\prime}$ is the Galois closure of H, and H is galois-closed if $H^{\circ\prime} = H$.

Thus the maps $K \mapsto K'$ and $H \mapsto H^\circ$ are inverse bijections between Galois-closed intermediate fields and Galois-closed subgroups.

(12)

Def. A field extension E/F is called a *Galois* extension if F is Galois-closed.

Thus, the Galois extensions are exactly those of the form

$$E/E_G,$$

where G is a subgroup of $\mathrm{Aut}(E)$.

Theorem 3 Let E/F be a finite field extension. The fllg are equivalent:

1. E/F is a Galois extension
2. $\forall\, u \in E$, the minimal polynomial of u over F is separable and splits in $E[x]$
3. E is the splitting field of a separable polynomial in $F[x]$.

$G = \mathrm{Gal}(E/F)$ **Sketch of Proof**

$(1)\Rightarrow(2)$ Suppose E/F is Galois. Let p be the min polyn of $u \in E$, over F.

Set $X = \{\sigma(u) : \sigma \in G\}$

Set $f(x) = \prod_{v \in X}(x - v)$. For each $\sigma \in G$, we have

$$\sigma f(x) = \prod_{v \in V}(x - \sigma(v)) = \prod_{v \in V}(x - v),$$

so the coefficients of f are fixed by G. Since E/F is Galois, the coeff. of f are in F, so $f(x) \in F[x]$. All the roots of f (the elements of X) are also roots of p, so in fact $p = f$. So p is sep & splits in $E[x]$.

$(2) \Rightarrow (3)$ This one is quite straightforward sort of by induction.

$(3) \Rightarrow (1)$ This uses the Dedekind–Artin theorem

$[E:F] = |G|$

by Theorem 5. on p. 4 of these notes.

$$\begin{array}{c} E \\ | \\ E_G \\ | \\ F \end{array}$$

$[E:E_G] = |G|$

by Dedekind-Artin

Since $[E:F] = [E:E_G][E_G:F]$

we obtain $[E_G:F] = 1$, so $E_G = F$.

→ $\boxed{\text{Recall}}$ the proof (5) on p.4 : If E is a splitting field of $f \in F[x]$, ~~then~~ separable, then $[E:F] = \underbrace{|Gal(E/F)|}_{G}$.

$$\begin{tikzcd}
E \arrow[d, dash] & & & E \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
K = F(u) \arrow[d, dash] & & F(u) \arrow[dr, dash] & F(\sigma(u)) \arrow[d, dash] & \cdots \arrow[dl, dash] & \forall \sigma \in G \arrow[dll, dash] \\
F & & & F & &
\end{tikzcd}$$

Galois $\sim G$ (E over F); Galois $\sim H$ (E over K)

Galois ? $\Leftrightarrow$ p splits in $K[x]$ $\Leftrightarrow X \subset F(u)$

- $f = pq$ in $F[x]$, p irreducible, $\deg p \geq 2$; $p(u) = 0$
- $Gal(E/F(u)) = H < G = Gal(E/F)$
- $X = \{\sigma(u) : \sigma \in G\} = \{u \in E : p(u) = 0\}$

  $|X| = \deg p = [F(u) : F]$

* Claim : $|G/H| = |X|$

i.e. # of roots of p equals # of cosets of $H < G$

Recall : $\rho : G \longrightarrow X :: \sigma \longmapsto \sigma(u)$ is surjective.

Q : What is $\rho^{-1}(v)$ for any root $v \in X$ of p ?

$$\sigma(u) = \tau(u) \Leftrightarrow \tau^{-1}\sigma(u) = u \Leftrightarrow \tau^{-1}\sigma \in H \Leftrightarrow \sigma H = \tau H$$

$\Rightarrow \tilde{\rho} : G/H \longrightarrow X :: \sigma H \mapsto \sigma(u)$

is well defined and bijective

Q: When is $H \trianglelefteq G$? [Answer: when K/F is a Galois extension]

To answer this, start w/ the question

- Q: What is $\mathrm{Gal}(E/F(\sigma(u)))$?

Notice that

$$F(\sigma(u)) = \sigma F(u) = \sigma K$$

<u>Fact</u> $\mathrm{Gal}(E/\sigma K) = \sigma H \sigma^{-1}$

<u>Pf</u> $\forall\, \tau \in G$:

$$\begin{aligned}
& \tau(b) = b \quad \forall\, b \in \sigma K \\
\Leftrightarrow\ & \tau(\sigma a) = \sigma a \quad \forall\, a \in K \\
\Leftrightarrow\ & \sigma^{-1}\tau\sigma a = a \quad \forall\, a \in K \\
\Leftrightarrow\ & \sigma^{-1}\tau\sigma \in H \\
\Leftrightarrow\ & \tau \in \sigma H \sigma^{-1}
\end{aligned}$$

<u>So</u> The Galois groups of the "conjugates" σK of K are the conjugate subgroups $\sigma H \sigma^{-1}$ of $H < G$.

<u>Thus</u>
$$\begin{aligned}
H \trianglelefteq G \ \Leftrightarrow\ & \sigma H \sigma^{-1} = H \quad \forall\, \sigma \in G. \\
\Leftrightarrow\ & \sigma K = K \quad \forall\, \sigma \in G \\
\Leftrightarrow\ & F(\sigma(u)) = F(u) \quad \forall\, \sigma \in G \\
\Leftrightarrow\ & X \subset F(u) \\
\Leftrightarrow\ & p \text{ splits in } F(u) \ (\text{so } K \text{ is spl. fld of } p) \\
\Leftrightarrow\ & K/F \text{ is a Galois extension.}
\end{aligned}$$

Assume now that $H \triangleleft G$, so $\sigma K = K$ $\forall\, \sigma \in G$.

This means that $\forall\, \sigma \in G$, $\sigma|_K \in Gal(K/F)$.

Thus we have a homomorphism

$$G \longrightarrow Gal(K/F) \;::\; \sigma \longmapsto \sigma|_K$$

This is <u>surjective</u> because each automorphism of K that fixes F can be extended to an automorphism of the splitting field E of f.

The kernel of this homomorphism ~~is~~ consists of all $\sigma \in G = Gal(E/F)$ such that $\sigma|_K = \varepsilon \in Gal(K/F)$, that is, all $\sigma \in G$ such that σ fixes K. But these σ exactly comprise $G(E/K) = H$.

The first isomorphism theorem then yields

$$Gal(K/F) \cong G/H$$

and the isomorphism is by restriction of elements of σH to K.