Wed, Nov 15, 2017

A minor digression on separability:

Defn ① $g \in K[x]$ is separable if each of its irreducible factors is.

Defn ② $g \in K[x]$ is separable if $\deg(g) = \#\mathrm{Roots}_{\overline{K}}(g)$.

How do these compare?

Prop Fix $f_1, f_2 \in K[x]$ irreducible. TFAE:

(1) $(f_1) = (f_2) \subset K[x]$

(2) $\mathrm{Roots}_{\overline{K}}(f_1) = \mathrm{Roots}_{\overline{K}}(f_2)$

(3) $\mathrm{Roots}_{\overline{K}}(f_1) \cap \mathrm{Roots}_{\overline{K}}(f_2) \neq \emptyset$.

Pf (1) $\Rightarrow$ (2) b/c $(f_1) = (f_2) \Rightarrow f_1 = a f_2$, $a \in K$.

(2) $\Rightarrow$ (3) obvious.

(3) $\Rightarrow$ (1). If α is in the intersection, we have

$$K[x] \xrightarrow{x \mapsto \alpha} \overline{K}$$

whose kernel is prime, hence maximal in $K[x]$. Both $f_1, f_2 \in$ Kernel, so $(\gcd(f_1, f_2)) = (f_1, f_2) \subset$ Kernel. Since f_i irreducible, unless $(f_1) = (f_2)$, $\gcd(f_1, f_2) =$ units $\subset K^\times$, contradicting properness of kernel. //

Cor For any $g \in K[x]$, the irreducible factorization

$$g = a f_1^{n_1} \cdots f_k^{n_k}, \quad n_i \geq 1,\ a \in K,\ f_i \text{ monic irreducible}$$

has $\mathrm{Roots}_{\bar{K}}(f_i) \cap \mathrm{Roots}_{\bar{K}}(f_j) = \emptyset$ when $i \neq j$.

So if g satisfies Defn①, we can reduce g to obtain a new polynomial

$$g_0 = a f_1 \cdots f_k$$

which fits Defn②. Moreover, the splitting fields of g_0 and g are obviously equal.

(The reason (g fits Defn①) $\Rightarrow$ (g_0 fits Defn②) is because each irred f_i separable $\Leftrightarrow$ $\deg f_i = \#\mathrm{Roots}_{\bar{K}}(f_i) \underset{\text{Cor.}}{\Longrightarrow} \#\mathrm{Roots}_{\bar{K}}(g) = \sum \#\mathrm{Roots}_{\bar{K}} f_i = \sum \deg f_i = \deg(g_0)$.)

We'll use Defn② from now on. The difference is the fuzziness, or nilpotence, of g.

Back to stream of lectures:

Thm Let $[L:K] < \infty$, $G := \mathrm{Gal}(L/K)$.
TFAE:
(1) $L^G = K$
(2) L is separable + satisfies $(*)$ (over K)
(3) L is splitting field of separable $g \in K[x]$.

Recall: (*) means if $\alpha \in L$, f min polyn of α, $\mathrm{Roots}_{\bar{K}}(f) \subset L$.

Pf: (1) $\Rightarrow$ (2) $\forall \alpha \in L$, set $g = \prod_{\beta \in G\alpha} (x - \beta)$. Then $\forall \sigma \in G$, $\sigma(g) = g$, so $g \in K[x]$. Then $\deg(g) = |G\alpha|$ and $\#\mathrm{Roots}_L(g) \leq \#\mathrm{Roots}_{\bar{K}}(g) \leq \deg g$.

$\deg g = \#G\alpha$

(2) $\Rightarrow$ (3) Let $L = K[\alpha_1, \dots, \alpha_n]$, and set $g = \prod f_i$ where each f_i is min polyn of α_i. Then reduce g to g_0; g_0 is separable since each f_i is (by (2)) and L is splitting field (b/c roots are in L by (2), and L is gen by roots).

(3) $\Rightarrow$ (1) Given any $\alpha \in L \setminus K$, WTS $\exists\, \sigma \in G$ st $\sigma(\alpha) \neq \alpha$. Let g_0 be separable polyn s.t. $L = K[\mathrm{Roots}_{\bar{K}}(g_0)]$. Let $f \in K[x]$ be minimal polynomial for α.

HW: f is separable since $\alpha \in K[\mathrm{Roots}_{\bar{K}}(g)]$ for g separable.

Then since $\alpha \notin K$, $\deg(f) \geq 2$, so f separable $\Rightarrow \exists\, \alpha \neq \alpha' \in \mathrm{Roots}_{\bar{K}}(f) \Rightarrow \exists\, \alpha \neq \alpha' \in \mathrm{Roots}_L(f)$ since L satisfies (*). (The miracle of splitting fields.) We thus have

$$\begin{tikzcd}
K \arrow[r, phantom, "\subset"] \arrow[d, equal] & K[\mathrm{Roots}_{\bar{K}}(f)] \arrow[r, phantom, "\subset"] \arrow[d, "\exists \sigma_0 \quad ⓐ"] & L \arrow[d, "\exists \sigma \quad ⓑ"] \\
K \arrow[r, phantom, "\subset"] & K[\mathrm{Roots}_{\bar{K}}(f)] \arrow[r, phantom, "\subset"] & L
\end{tikzcd}$$

ⓐ $\exists\, \sigma_0$ taking α to α' since Gal acts transitively on roots of an irred. polynomial in a splitting field. ⓑ σ_0 extends to σ by extension lemma for splitting fields: since g_0 is a polyn w/ coeff in K, $\sigma_0(g_0) = g_0$, so lemma applies b/c L is splitting field of $g_0 \in (K[\mathrm{Roots}_{\bar{K}}(f)])[x]$, too. //

Defn Let $[L:K]<\infty$. We say $K\subset L$ is a *Galois extension* if any (hence all) of conditions (1)~(3) is satisfied.

Rmk We'll see that there's another equivalent condition:

$$|Gal(L/K)| = [L:K] \text{ iff } K\subset L \text{ is Galois}$$

Here's an immediate corollary:

Cor Let $K\subset K_1\subset L$. If $K\subset L$ is Galois, so is $K_1\subset L$.

Pf: Let $g\in K[x]$ be separable polyn s.t. $L = K[Roots_{\overline{K}}(g)]$. Thinking of g as an element of $K_1[x]$, we have

$$L = K_1\left[Roots_{\overline{K_1}}(g)\right]$$

and g is obviously separable over K_1 if it's separable over K. (# roots, and deg(g), don't change). So $K_1\subset L$ satisfies (3). //

Cor Let $K \subset L$ be Galois.
Then
$$\text{Subfields}_K(L) = \text{Fix}.$$

Rmk Recall
- $\text{Subfields}_K(L) = \{ K \subset K_1 \subset L \}$.
- $\text{Fix} = \{ K_1 \text{ st } \exists\ H \subset Gal(L/K) \text{ for which } K_1 = L^H \}$.
  (ie, fixed fields of some subgp of $Gal(L/K)$.)

Pf: Given $K \subset K_1 \subset L$, previous corollary says
$$K_1 = L^{Gal(L/K_1)}$$
but $Gal(L/K_1) \subset Gal(L/K)$. //

We now make our way tw'd proving that $\text{Subgps}(G) = \text{Gal}$.

Goal: If $[L:K] < \infty$, $K \subset L$ Galois, then
$$\text{Subgps}(G) = \text{Gal}.$$

This goal then implies:

Thm $[L:K] < \infty$, $K \subset L$ Galois. Then
$$L^{\bullet} : \text{Subgps}(Gal(L/K)) \rightleftarrows \text{Subfields}_K(L) : Gal(L/\cdot)$$
are mutually inverse bijections

This theorem is part of the fund. thm. of Galois theory.

To work toward goal, we pass through two surprising theorems:

<u>Thm</u> (Artin's Thm) Let $K \subset L$ be an extension of finite degree. Then $L = K[\alpha]$ iff $\text{Subfields}_K(L)$ is finite.

<u>Thm</u> (Primitive element theorem). Let $K \subset L$ be finite and separable. Then $\exists\, \alpha \in L$ st $L = K[\alpha]$.

<u>Defn</u> Any $\alpha \in L$ st $K[\alpha] = L$ is called a primitive element, and L is called a primitive extension (of K).

Let's assume Artin's thm for now.

<u>Pf</u> (of primitive elt thm). Since $K \subset L$ is separable and finite, we write

- $L = K[\alpha_1, \ldots, \alpha_n]$ $\quad$ ($[L:K]$ finite)

- $g = f_1 \cdots f_n$, each f_i min polyn of α_i

- g_0 reduced form of g, so g_0 separable.

Then we have $K \subset L \subset \mathbb{L}$, $\mathbb{L}$ = splitting field of g_0 over K (and L). We've already shown that

$$\text{Subfields}_K(\mathbb{L}) = \mathbb{F}\text{ix} \cong \text{Subgps}(\text{Gal}(\mathbb{L}/K))$$

but the right hand side is finite — for example, writing

$$\mathbb{L} = K[\beta_1, \ldots, \beta_m],$$

and

$$\Omega = \bigcup_{\beta_i} \mathrm{Roots}_{\mathbb{L}}(h_i) \quad , \quad h_i \text{ min polyn of } \beta_i$$

we know that the map

$$\mathrm{Gal}(\mathbb{L}/K) \longrightarrow \mathrm{Aut}_{Set}(\Omega)$$

is an injection b/c $\mathbb{L}$ is generated by β_i. Since Ω is finite, so is $\mathrm{Gal}(\mathbb{L}/K)$. This means $\exists$ only finitely many subgps.

To finish: if there are only finitely many K_1 st $K \subset K_1 \subset \mathbb{L}$, in particular, " " " " " " " $K \subset K_1 \subset L$, because $L \subset \mathbb{L}$. By Artin's theorem, a primitive element exists. //

We now use the primitive element theorem, leaving Artin for another day:

Thm $K \subset L$ finite. Then $K \subset L$ is Galois iff:

(4) $|Gal(L/K)| = [L:K]$.

Pf $K \subset L$ Galois $\Rightarrow$ $K \subset L$ separable
$\Rightarrow L = K[\alpha]$ (prim. elt. thm.)

Now let $G = Gal(L/K)$ and consider

$$g(x) := \prod_{\beta \in G\alpha} (x - \beta).$$

We have that $\forall \sigma \in G$, $\sigma(g) = g$ again, so $g \in K[x]$, because $K \subset L$ Galois. We conclude g is min polyn of α using same inequalities as before.

$$\left(\deg(\text{min polyn}) \leq \deg(g) = |G\alpha| \leq \# Roots_{\overline{K}}(\text{min polyn}) \leq \deg(\text{min polyn}) \right).$$

Since $L = K[\alpha]$, σ is determined by $\sigma(\alpha)$. On the other hand, since g is irreducible, Gal acts transitively on $Roots_L(g) = G\alpha$. Hence

$$\begin{aligned} Gal(L/K) &\longrightarrow Roots_L(g) \\ \sigma &\longmapsto \sigma(\alpha) \end{aligned}$$

is both an injection and a surjection. We conclude by noting

$$\# Roots_L(g) = \# Roots_{\overline{K}}(g) = \deg(g) = [L:K].$$

Before proving the converse, a general idea: Set $G = \mathrm{Gal}(L|K)$ and consider

$$K_1 := L^G$$

so $K \subset K_1 \subset L$. Then $G = \mathrm{Gal}(L/K_1)$, so $K_1 \subset L$ is Galois. By previous part, we conclude

(*)
$$[L:K] = [L:K_1][K_1:K] = |\mathrm{Gal}(L/K)|\,[K_1:K].$$

If $[L:K] = |\mathrm{Gal}(L|K)|$, we must have $[K_1:K] = 1$, which means

$$K = K_1 = L^G. \quad //$$

How cool is that?

<u>Rmk</u> So $|\mathrm{Gal}(L|K)| = [L:K]$ iff $K \subset L$ Galois. What kinds of non-equality are possible? Well, we can see that $|\mathrm{Gal}(L|K)| \leq [L:K]$ because the former always <u>divides</u> the latter! This is the content of (*) above.