(1)

My condensation of Galois Theory from the textbook

§10.1 Galois groups and field/polynomial separability

- Given a field extension E of F, its Galois group is

$$G(E/F) = \mathrm{gal}(E:F) := \{\sigma \in \mathrm{Aut}(E) : \sigma(a) = a \ \forall a \in F\},$$

~~with closure~~ and we have $G(E/F) \subset \mathrm{Aut}(E) \subset S_E$

with closure under composition. So $G(E/F) \underset{\uparrow \text{subgroup}}{<} S_E$.

- Galois groups act on roots of polynomials:

Let $E \supset F$ be a field extension, $p \in F[x]$,

$$X := \{v \in E : p(v) = 0\}$$

Fact $\forall \sigma \in G(E/F)$ and $v \in X$, $\sigma(v) \in X$.
Pf $p(\sigma(v)) = \sum_{i=0}^{n} a_i (\sigma(v))^i = \sigma \sum_{i=0}^{n} a_i v^i = p(v) = 0$.

This implies that $G(E/F)|_X = \{\sigma|_X : \sigma \in G(E/F)\} \subset S_X$.

The map $\rho : G(E/F) \to S_X :: \sigma \mapsto \sigma|_X$ is a homomorphism

- Case $E = F(u)$, u algebraic over F, m = min polyn of u over F.
$X = \{v \in F(u) : m(v) = 0\}$

Fact $\forall v \in X$, $\exists! \ \sigma \in G(F(u)/F) : \sigma(u) = v$.

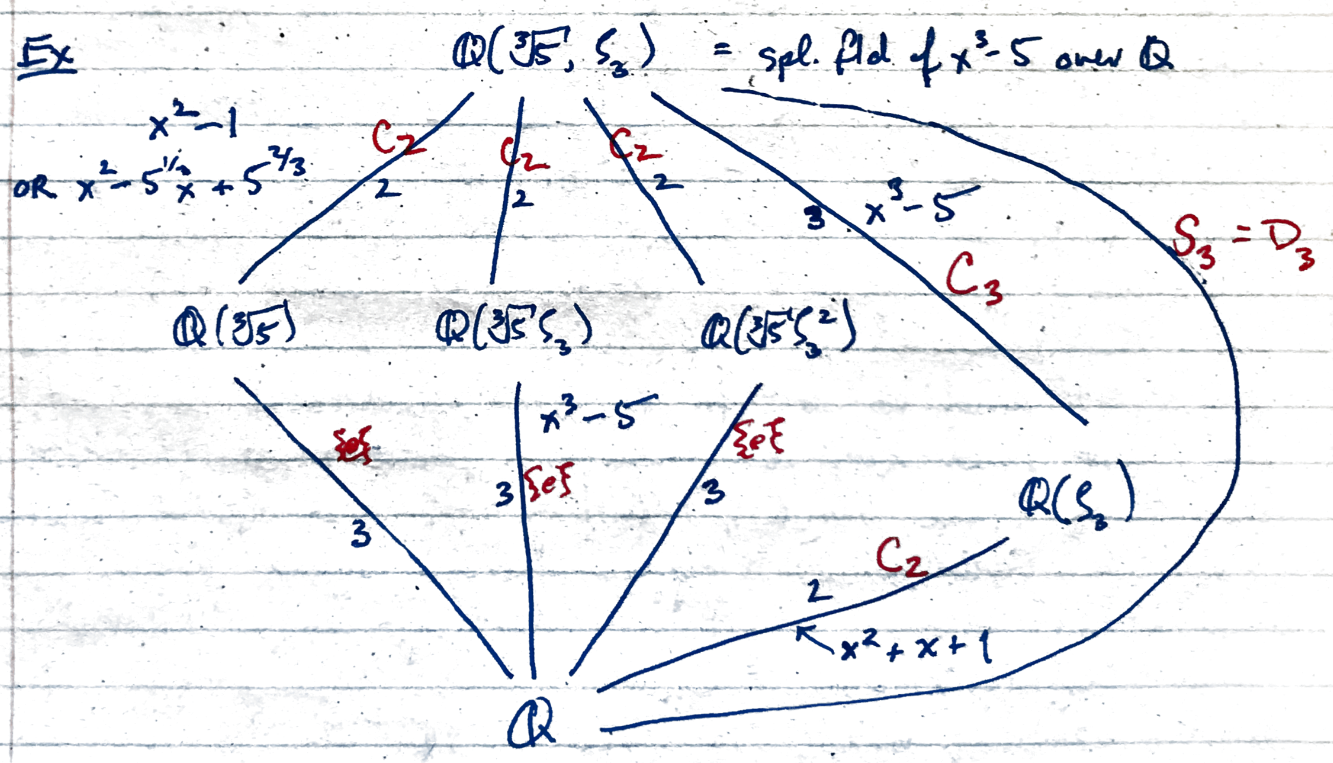
* existence ~~Under~~ The ~~automorphism~~ isomorphism
$F(u) \to F[x]/\langle m(x) \rangle \to F(v)$ is onto $F(u)$ since $F(v) < F(u)$ and this is a linear map of vector spaces of finite dimension.

* uniqueness. Recall that $F(u) = \{f(u) : f \in F[x]\}$.
Given $\sigma \in Gal(F(u)/F)$ such that $\sigma(u) = v$,
$\sigma(f(u)) = f(\sigma(u)) = f(v)$, so σ is (uniquely) determined.

Lesson: existence is due to irreducibility of m;
uniqueness is due to minimality of $F(u)$ (smallest fld w F & u)

- Consequences:
  * $\rho : G(F(u)/F) \longrightarrow S_X$ is injective, so G acts as a subgroup of permutations of X
  * If m splits in $F(u)$, then $|G(F(u)/F)| = \deg m = [F(u):F]$

- Ex



Degrees of field extensions are blue integers
Galois groups are in red.

Notice $\sigma : \sqrt[3]{5} \mapsto \sqrt[3]{5}\zeta_3$ has order ~~2~~ 3
$\tau : \zeta_3 \mapsto \zeta_3^2$ has order ~~3~~ 2 $\Big\} \Rightarrow D_3$
$\sigma\tau\sigma = \tau$

- $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = C_{p-1}$, $\zeta_p = e^{2\pi i/p}$, p prime.

Steps of the proof:

* $x^{p-1} + x^{p-2} + \dots + x + 1$ is irreducible over $\mathbb{Q}$, and its roots are $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$, all in $\mathbb{Q}(\zeta_p)$.
* $\mathbb{Z}_p^*$ is cyclic since it is a finite ~~subgroup of the~~ group of units of a field.
* Let $m \in \mathbb{Z}$ be s.th. $\bar{m} \in \mathbb{Z}_p^*$ is a generator of $\mathbb{Z}_p^*$.
* $\exists\, \sigma \in G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ s.th. $\sigma(\zeta_p) = \zeta_p^m$.
* $\sigma^k(\zeta_p) = \zeta_p^{m^k}$, so

$$\begin{aligned}
&\sigma^k(\zeta_p) = \sigma^l(\zeta_p) \\
\iff\ & \zeta^{m^k} = \zeta^{m^l} \\
\iff\ & \zeta^{m^k - m^l} = 1 \\
\iff\ & \bar{m}^k - \bar{m}^l = 0 \text{ in } \mathbb{Z}_p \\
\iff\ & \bar{m}^k (1 - \bar{m}^{l-k}) = 0 \text{ in } \mathbb{Z}_p \\
\iff\ & \bar{m}^{l-k} = 1 \quad \text{in } \mathbb{Z}_p \text{ (or in } \mathbb{Z}_p^* \cong C_{p-1}) \\
\iff\ & l - k \equiv 0 \pmod{p-1}
\end{aligned}$$

Thus $\sigma^k(\zeta_p) \neq \sigma^l(\zeta_p)$ for $k \neq l$ and $0 \leq k, l < p-1$ and so σ^k for $k = 0, 1, \dots, p-1$ are distinct.

Thus $\langle\sigma\rangle$ has order $p-1$,

* Since $|G(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p-1$ and $\langle\sigma\rangle \subset G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p-1$.

- $G(GF(p^n)/\mathbb{Z}_p) \cong C_n$

Steps of proof:

* The Frobenius automorphism $\sigma: w \mapsto w^p$ is in the Gal. grp G, so $\langle\sigma\rangle < G$
* $|G(GF(p^n)/\mathbb{Z}_p)| \leq n$
* For $k \in \mathbb{N}_0$, $\sigma^k = \varepsilon \to w^{p^k} - w = 0 \ \forall\, w \in GF(p^n)$ $\longrightarrow p^k \geq p^n$, so $k \geq n$. Thus $|\langle\sigma\rangle| \geq n$.
* $G(GF(p^n)/\mathbb{Z}_p) = \langle\sigma\rangle \cong C_n$

- Let E be a splitting field of f over F.
  * $G(E/F)$ is isomorphic to a subgroup of S_X, where $X = \{u \in E : f(u) = 0\}$.
  * f irred. over F $\Rightarrow$ G acts transitively on X
  * G acts transitively on X and f has no repeated roots $\Rightarrow$ f irred. over F

- Defn A polynomial $p(x) \in F[x]$ is separable (over F) if each of its irreducible factors has only simple roots {in any field extension of F.
  E is a separable extension of F if $\forall u \in E$ the minimal polynomial ~~over F~~ of u over F is separable.

- Let $p(x) \in F[x]$ be irreducible (over F).
  p is separable if and only if $p' \neq 0$ in $F[x]$.

- Let f be irreducible over F
  * $\mathrm{char}\, F = 0 \Rightarrow f$ is separable.
  * $\mathrm{char}\, F = p \Rightarrow$ (f not separable $\Leftrightarrow \exists g : f(x) = g(x^p)$)

- Let E be a splitting field of a separable polynomial $f \in F[x]$. Then

(*) $$|G(E/F)| = [E:F].$$

Steps of the proof:
* Let p be an irreducible factor of f w/ $\deg p \geq 2$, and let $u \in E$ be a root of p.
* To proceed by induction, consider $F \subset F(u) \subset E$:
  $[F(u):F] = k$; $[E:F(u)] = [E:F]/k \overset{\text{induction}}{=} |G(E/F(u))|$
* Set $X := \{v \in E : p(v) = 0\}$; $|X| = k \geq 2$
* $\forall \sigma \in G(E/F)$, $\{\tau \in G(E/F) : \tau(u) = \sigma(u)\} = \sigma G(E/F(u))$
* $\forall v \in X$, $\exists \sigma \in G(E/F) : \sigma(u) = v$
* $|G(E/F)| = \bigcup_{v \in X} \{\sigma \in G(E/F) : \sigma(u) = v\} = k\,|G(E/F(u))| = [E:F]$

(5)

- E = ~~splitting field of a separable polyn in $F[x]$~~ separable extension of F with $|F| = \infty$.

$\underline{E = F(u)}$ $\Longrightarrow$ E is a **simple** algebraic extension of F.

Proof Let's do the case that $E = F(v, w)$ (and then use induction).

candidate for u: linear comb of v and w

p = min polyn of v over F; V = roots of p in E
q = min polyn of w over F; W = roots of q in E

For any $a \in F^*$, set $u = v + aw$.
m = min polyn of w over $F(u)$, $m \in F(u)[x]$.

WTS deg $m = 1$

Set $g(x) := p(u - ax)$, $g \in F(u)[x]$.
Since $g(w) = p(v) = 0$ and $q(w) = 0$,
$m \mid q$ and $m \mid g$.

$* \rightarrow$ Thus each root of m is a root of q and a root of g.
But ~ we can choose a so that g has only the root w in common with q. To wit:

~~$\forall z \in W$ $g(z) = p(u - az) = 0$ $\Longleftrightarrow$ $u - az \in V$ $\Longleftrightarrow$ $v + a(w - z) \in V$ $\Longleftrightarrow$ $a \in$~~

$\forall\, w' \in W' = W \setminus \{w\}$,

$$g(w') = p(u - aw') = 0$$
$$\Longleftrightarrow u - aw' \in V$$
$$\Longleftrightarrow v + a(w - w') \in V$$
$$\Longleftrightarrow a \in (w - W')^{-1}(V - v)$$

So $g(w') \neq 0$ $\forall\, w' \in W'$
$\Longleftrightarrow$ $a \notin (w - W')^{-1}(V - v)$, which is a finite set.

Since F is infinite, such a exists.