Example Let $f = x^3 - 2$ and $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ be the splitting field of f over $\mathbb{Q}$.

$$e^{2\pi i/3} = \frac{-1}{2} + \frac{i\sqrt{3}}{2} = \rho.$$

Hence $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$

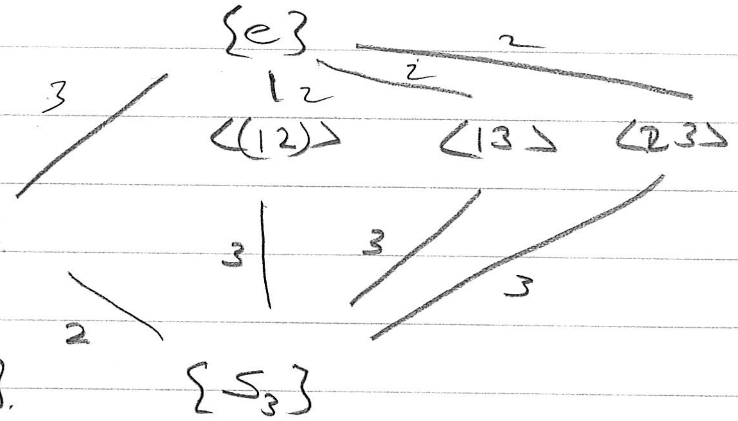
Any $\mathbb{Q}$-autom of L will send $\sqrt[3]{2} \to \sqrt[3]{2} =: r_1$ or $\sqrt[3]{2}\rho =: r_2$, or $\sqrt[3]{2}\rho^2 =: r_3$.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}, \rho) \arrow[d, dash, "2"'] \arrow[dd, dash, bend left, "6"] \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "3"'] \\
\mathbb{Q}
\end{tikzcd}$$

Since $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}] = 6$ and $[L : \mathbb{Q}]$ is a Galois extension, $Gal(L : \mathbb{Q})$ is a group of order 6

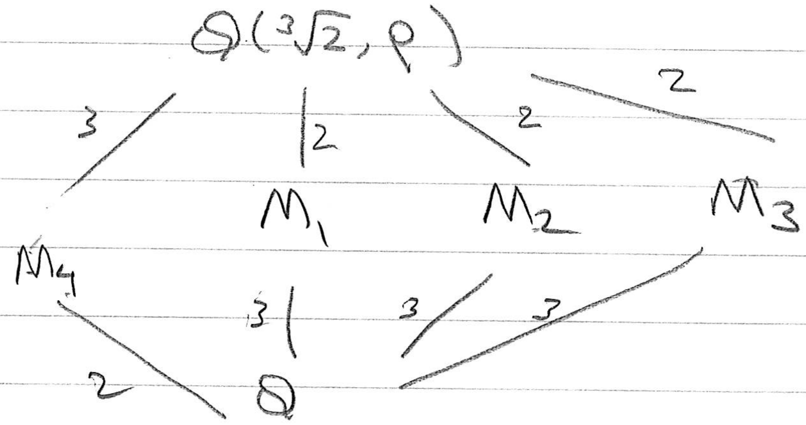
Any $\sigma \in G = Gal(L : \mathbb{Q})$ is determined by its effect on the 3 roots and there are at most 6 permutations of these 3 roots. On the other hand $|G| = 6$, so $G \cong S_3 = \{e, (12), (13), (23), (123), (132)\}$.

There are 4 proper s/gps of S_3



$\langle(123)\rangle = A_3$
$\langle(132)\rangle$
$= \{e, (123), (132)\}$.

Hence the subfields of $\mathbb{Q}(\sqrt[3]{2}, \rho)$ should look similar.



labeling the 3 roots as $\underset{\sqrt[3]{2}}{\overset{1}{\shortparallel}}$, $\underset{\sqrt[3]{2}\rho}{\overset{2}{\shortparallel}}$, $3 = \rho^2\sqrt[3]{2}$

Then (12) fixes 3, hence $\mathrm{Fix}(12) \supset \mathbb{Q}(\rho^2\sqrt[3]{2})$
The subgroup (12) has index 3 in S_3
and $[\mathbb{Q}(\rho^2\sqrt[3]{2}) : \mathbb{Q}]$ has degree 3 so

$M_1 = \mathbb{Q}(\rho^2\sqrt[3]{2})$ is the full fixed field of $\langle(12)\rangle$

Similarly (13) has fixed field $\mathbb{Q}(\rho\sqrt[3]{2}) = M_2$

and (23) has fixed field $\mathbb{Q}(\sqrt[3]{2}) = M_3$

Note (123) is the autom $\sigma: \sqrt[3]{2} \to \sqrt[3]{2}\rho$

$$\sqrt[3]{2}\rho \to \rho^2\sqrt[3]{2}$$

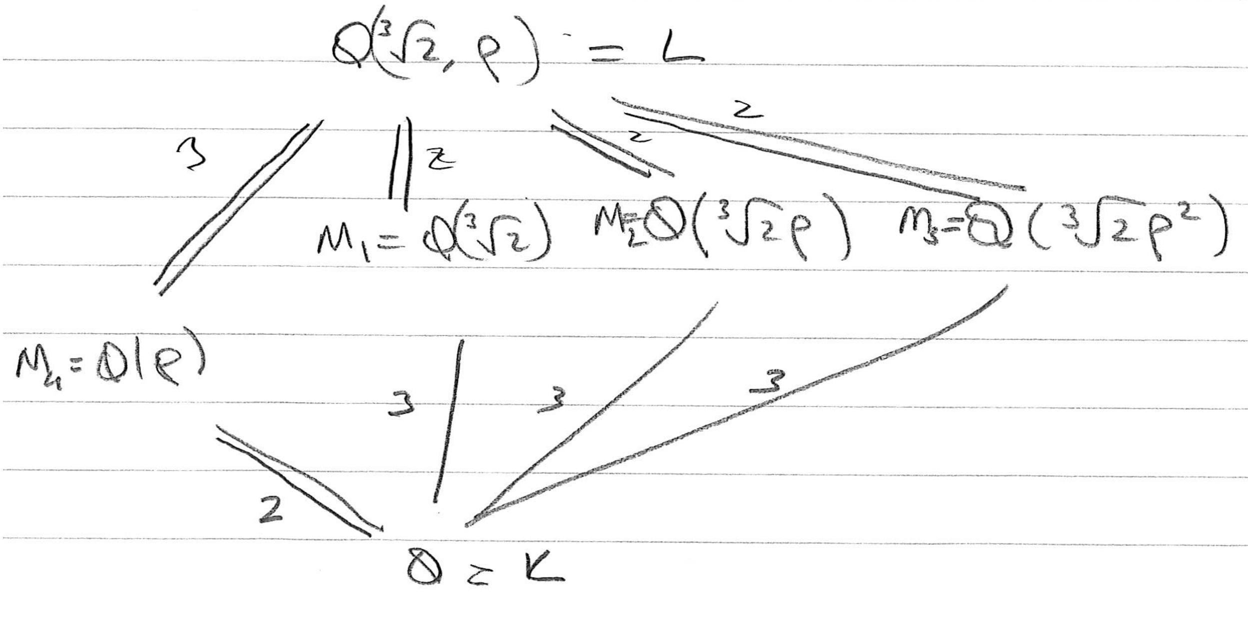
$$\rho^2\sqrt[3]{2} \to \sqrt[3]{2}$$

Hence $\sigma\left(\frac{\sqrt[3]{2}\rho}{\sqrt[3]{2}}\right) = \sigma(\rho) = \frac{\rho^2\sqrt[3]{2}}{\rho\sqrt[3]{2}} = \rho$

Hence (123) fixes ρ. Since $[\mathbb{Q}(\rho):\mathbb{Q}] = 2$
($\rho^3 = 1 \Rightarrow (\rho - 1)(\rho^2 + \rho + 1) = 0$
$x^2 + x + 1$ is the minimal poly of
ρ over $\mathbb{Q}$).

And $[S_3 : A_3] = 2$ we have that

$M_4 = \text{Fix}(123) = \mathbb{Q}(\rho)$. Hence the field structure is



Note non of the extenhions $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ are nome
$\mathbb{Q}(\sqrt[3]{2}\rho) : \mathbb{Q}$
$\mathbb{Q}(\sqrt[3]{2}\rho^2) : \mathbb{Q}$

But we do here that $[M_i : \mathbb{Q}] = 3 = |G| / [L : M_i] = \frac{6}{2}$

Where as the extenhions $\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2}\rho)$
$\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2}\rho^2)$

are all normal.
Their Galois groups are isomorphic to $\mathbb{Z}_2$

The extenhions $L : M_4$ are $M_4 : K$ are both normal.

$[L : M_4] = 3 = Gal(L : M_4) \cong \mathbb{Z}_3$

$[M_4 : K] = 2 = |G| / |\gamma(M_4)| = 6/3 = 2.$

$Gal(M_4 : K) \cong G / Gal(L : M_4) = S_3 / \mathbb{Z}_3 \cong \mathbb{Z}_2$

§6. Galois groups of polynomials

We've seen before that if $R(f)$ is the zero set of a polynomial $f \in K[x]$ then the Galois group of $L_f : K$ permutes the roots of f.

Here $L = L_f$ is the splitting field of f over K

We also saw that

$Gal(f) := Gal(L_f : K)$ is isomorphic to a subgroup of $S_{R(f)}$

(Lemma 3.2, 3.2'.)

If $f = f_1 \cdot \ldots \cdot f_k$ is a product of irreducible polynomials f_i of degree n_i,

then,

Since the Galois group permutes the roots of irreducible factors among themselves, we have in fact that

$$Gal(f) \leq S_{n_1} \times \ldots \times S_{n_k}$$

If f is irreducible then we've have also seen that given any 2 roots α, β of f, there is an element $\sigma \in Gal(f)$ s.t $\sigma(\alpha) = \beta$ (Prop 4.5)

Such a group is said to be <u>transitive</u> on the roots

ie given any 2 roots, $\exists\, \sigma \in G$ s.t $\sigma(\alpha) = \beta$

Rmk In general if $f = f_1 f_2$, f_i irred Then $Gal(f)$ will be transitive on blocks of roots, namely the roots of Irred. factors f_1, f_2.

Eg. $f = (x^2-2)(x^2-3)$

$$Gal\, f = \{e, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

where $\sigma : \sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to \sqrt{3}$ $\quad$ $\tau : \sqrt{3} \to -\sqrt{3}$, $\sqrt{2} \to \sqrt{2}$

$\sigma\tau : \sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$

The fact that $Gal(f)$ of an irred poly f has to be transitive on roots can restrict the possibilities for Galois gps quite a lot for degree 3 polynomials.
Suppose f is separable irred of degree 3 w/ roots $\alpha_1, \alpha_2, \alpha_3$ in a splitting field L_f

$Gal(f) \leq S_3$.
The s/gps of S_3 are $A_3 = \langle (123) \rangle$
$H_1 = \langle (12) \rangle$ $\quad H_2 = \langle 13 \rangle$, $H_3 = \langle 2, 3 \rangle$ and $\{e\}$

The only s/gps of S_3 that are transitive are S_3, and A_3

for example note in H_1, there is no elt which sends α_1 to α_3.

Hence $Gal(f)$ for a cubic irreducible poly is either S_3 or $A_3 \cong \mathbb{Z}_3$.

We have seen if $f = x^3 - 2 \in \mathbb{Q}[x]$ then $Gal(f) \cong S_3$

<u>When is it A_3?</u>

This question can be answered by looking at a general poly f of degree n.
Say $\alpha_1, \dots \alpha_n$ are roots of f repeated according to multiplicity in a splitting field $L_f : K$.

Set $\delta = \left(\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) \right)$, $D = \delta^2$

D is called the <u>discriminant of f</u>
Note if $\delta = 0$ then f has repeated roots.
In fact using Galois theory one can prove

<u>Thm 6.1</u> Suppose char $K \neq 2$, $f \in K[x]$
$D = disc(f)$, $L_f : K$ a splitting field extension for f. Then

(1) If $D = 0$ then f has a repeated root in L_f

(2) If $D \neq 0$, and D has a square root in K then $G = Gal(L_f : K) \subseteq A_n$

(3) If D has no square root in K, it has a square root δ in L, $G = Gal(L_f : K) \not\subseteq A_n$

and $K(\delta)$ is the fixed field of $G \cap A_n$.

Proof Exercise.

Defn. A poly $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ is called reduced if $a_{n-1} = 0$.
If f is monic of degree n, its corresponding reduced polynomial $\tilde{f}$ that obtained from $f(x)$ by change of variable $y = x - \frac{a_{n-1}}{n}$.

Thm 6.2 (1) A poly f and its corresponding reduced poly $\tilde{f}$ have the same discriminant

(2) The disc. of a reduced cubic $\tilde{f}(x) = x^3 + qx + r$ is

$$D = -4q^3 - 27r^2.$$

Pf. See Rotman p. 57

Combining Thm 6.1, 6.2 we have

Thm 6.3 Let $f \in \mathbb{Q}[x]$ be an irred cubic w/ Galois gp G, disc D. Then

1) $f(x)$ has exactly one real root $\iff D<0$, in which case $G \cong S_3$

2) f has 3 real roots $\iff D>0$.
In this case either $\sqrt{D} \in \mathbb{Q}$ and $G \cong \mathbb{Z}_3 = A_3$
or $\sqrt{D} \notin \mathbb{Q}$ and $G = S_3$

eg. $x^3 - 3x - 1$ has disc 81 which is a square. Hence $Gal(f) = A_3$.

To determine Galois group of an irred. sep. quartic is more involved. One first notes that there are the following transitive s/gps of S_4 : S_4, A_4

3 transitive s/gps isomorphic to D_4
$\langle (1234), (13) \rangle$, $\langle (1324), (12) \rangle$, $\langle (1243), (14) \rangle$

3 transitive s/gps isom to $\mathbb{Z}/4\mathbb{Z}$
$\langle (1234) \rangle$, $\langle (1243) \rangle$, $\langle (1324) \rangle$

1 transitive s/gp isom to $\mathbb{Z}_2 \times \mathbb{Z}_2$
$\{1, (12)(34), (13)(24), (14)(23)\}$

Galois gp of irred cubic is determined in $K[x]$ whether the quadratic poly $x^2 - D$ having a root in K or not.

For quartics, there is a cubic polynomial $R_3(x)$ called the cubic resolvent and the thm similar to Thm 6.3 in this case we have for a separable irred quartic.

Thm 6.4 (a)

D_f in K	$R_3(x) \in K[x]$	Gal(f)
$\neq \square$ in K	irred	S_4
$= \square$ "	irred	A_4
$\neq \square$ "	red	D_4 or $\mathbb{Z}/4\mathbb{Z}$
$= \square$ "	red	V

(b) $Gal(f) = V \iff R_3(x)$ splits completely over K
$Gal(f) = D_4$ or $\mathbb{Z}/4\mathbb{Z} \iff R_3(x)$ has a unique root in K

(c) If $D \neq \square$ and $R_3(x)$ is reducible in $K[x]$ so that $G_f = D_4$ or $\mathbb{Z}/4\mathbb{Z}$. Then

1. If $f(x)$ is irred over $K(\sqrt{D})$ then $G_f = D_4$
2. If " is red over $K(\sqrt{D})$ then $G_f = \mathbb{Z}/4\mathbb{Z}$

Cf: I. Kaplansky Fields and rings (p. 51ff)
Rotman Prop A-5.76
D. Dummit, R. Foote Abstract Algebra (p 527 ff)

An important class of polynomials whose Galois groups are abelian is given by

Cyclotomic polynomials and extensions

A cyclotomic extension of a field K is a field $K(\xi)$ where $\xi^n = 1$

Let $\mu_{n,K}$ denote the set of roots of $x^n - 1 = f$ (n-th roots of unity over K)

We'll restrict ourselves to $\mathbb{Q}$.

Then the set $\mu_n = \mu_{n,\mathbb{Q}}$ has n elements and $L := \mathbb{Q}(\mu_n)$ is a splitting field for $f(x)$

Since the n-th roots of 1 form a group under multiplication of $L^\times$, it is a cyclic group of size n.

If ξ_n is a primitive n-th root of 1, ie a generator of μ_n, then

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n$$
$$k \mapsto \xi_n^k$$ is an isomorphism

The primitive n-th roots of unity are given by residue classes prime to n. Hence there are $\varphi(n) = \#\{1 \leq k < n \mid (k, n) = 1\}$ primitive n-th roots of unity.

Note that since ξ_n generates μ_n

$\mathbb{Q}(\xi_n) = \mathbb{Q}$ is a splitting field of $X^n - 1$

To determine the degree of this extension and the minimal polynomial of ξ_n we note ① if $d \mid n$ and $\alpha \in \mu_d$ then $\alpha \in \mu_n$
since $\alpha^n = (\alpha^d)^{n/d} = 1$
Hence $\mu_d \subseteq \mu_n \quad \forall\, d \mid n$

② Conversely $\alpha \in \mu_n$ then its order is a divisor of n. Hence if $\alpha \in \mu_n$ and $\alpha \in \mu_d$ then $d \mid n$

We have
$$X^n - 1 = \prod_{\substack{\alpha^n = 1 \\ \text{ie } \alpha \in \mu_n}} (X - \alpha) = \prod_{d \mid n} \prod_{\substack{\alpha \in \mu_d \\ \alpha \text{ primitive}}} (X - \alpha)$$

we group together the factor $X - \alpha$ where α is an elt of order d in μ_n.
ie. a primitive d-th root of 1.

Defn The n-th cyclotomic polynomial $\Phi_n(x)$ is the polynomial whose roots are primitive n-th roots of 1

$$\boxed{\Phi_n(x) = \prod_{\substack{\xi \in \mu_n \\ \text{primitive}}} (x - \xi) = \prod_{\substack{1 \leq a < n \\ (a,n)=1}} (1 - \xi_n^{\,a})}$$

Hence

$$\boxed{x^n - 1 = \prod_{d \mid n} \Phi_d(x)}$$

This formula allows one to compute $\Phi_n(x)$ recursively

$$\Phi_1(x) = x - 1 \quad , \quad \Phi_2(x) = x + 1$$

$$x^3 - 1 = \Phi_1(x)\,\Phi_3(x) = (x-1)\,\Phi_3(x)$$

Hence $\Phi_3(x) = x^2 + x + 1$

$$x^4 - 1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_4(x) = (x-1)(x+1)\,\Phi_4(x)$$

Hence $\Phi_4(x) = x^2 + 1$

Also note for $n = p$ $\quad \Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$