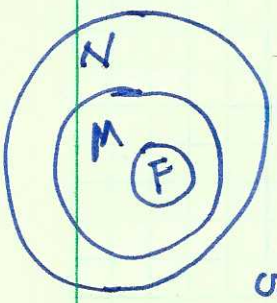
3 More on Galois groups

⊛ Fundamental theorem of Galois extension

Galois group of an equation $f(x)=0$ defined on the field F. Its root field is N. Then $Gal(N/F) = \{\sigma \in Aut(N) \mid \forall a \in F,\ \sigma(a)=a\}$.



Now consider M is a normal extension of F, and N is also a normal extension of M. (Recall that for a normal extension from the field A to B and an equation defined on A, if one of its roots is in B, then all of its roots are in B.) We can define $Gal(N/M)$ and $Gal(M/F)$. Then what's the relation among these three Galois groups?

⊛ If $\sigma \in Gal(N/F)$, then $\sigma(M) = M$, i.e. $\forall a \in M \Leftrightarrow \sigma(a) \in M$

Proof: ① if $a \in F$, then $\sigma(a) = a \in M$. If $a \notin F$ and $a \in M$, and assume that "a" satisfies $g(x)=0$ defined on F. Then $\sigma(g(x)) = g(\sigma(x))$

Because M is a normal extension of F, hence $\sigma(a) \in M$.

Conversely, if $\sigma(a) \in M$, $\Rightarrow \sigma^{-1}(\sigma(a)) = a \in M$.

Comment: This is the reason why we are interested in normal extension

For example, Consider $x^3-2=0$. $Q(\sqrt[3]{2})$ is not a normal extension, since $\sqrt[3]{2}\,\omega$ and $\sqrt[3]{2}\,\omega^2$ are not included. Then $N = Q(\sqrt[3]{2}, \omega)$, there exists $\sigma \in Gal(N/Q)$, which does not keep $Q(\sqrt[3]{2})$ invariant.

but $Q(\omega)$ is a normal extension. It's much better than $Q(\sqrt[3]{2})$.

We remember $\forall\ \sigma \in Gal(N/Q)$, it has $\sigma(\omega) = \omega$, or $\sigma(\omega) = \omega^2$, hence it leaves $Q(\omega)$ invariant!

(*) We prove that $Gal(N/M)$ is a normal subgroup of $Gal(N/F)$.

Let's denote $H = Gal(N/M)$, apparently $H \subset Gal(N/F)$. Consider an operation $h \in H$, and another element $g \in Gal(N/F)$. We consider $h' = g^{-1} h g$. Take $\forall\ a \in M$, then since $g(a) \in M$, we have $h(g(a)) = g(a)$ since H leaves M invariant. $\Rightarrow h'(a) = g^{-1} g(a) = a$!

$\Rightarrow h' \in H$. Hence, $Gal(N/M)$ is a normal subgroup of $Gal(N/F)$.

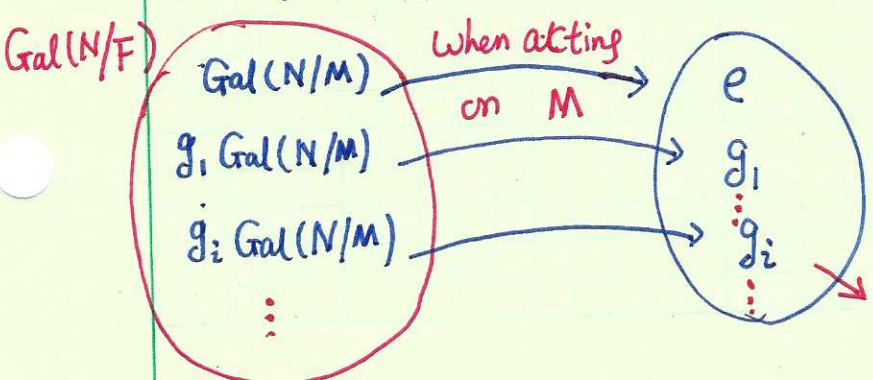
$\Rightarrow$ $\boxed{Gal(N/F) \triangleright Gal(N/M)}$

(*) The quotient group $Gal(N/F)/Gal(N/M) \sim Gal(M/F)$

Since $Gal(N/F)$ leaves M invariant, it can also be viewed automorphism of M. But many operations are the same. For example, $\forall\ h \in Gal(N/M)$, we have if $a \in M$, $h(a) = a$, i.e $Gal(N/M) \longrightarrow \{e\}$. We can use $Gal(N/M)$ as the Kernel and construct cosets. Say, $\forall$ operation in $g_1 Gal(N/M)$, we have

$g_1 h(a) = g_1(a) \in M$.

$\boxed{\text{we arrive at } Gal(M/F)}$



✡ Again we use $x^3-2=0$ to illustrate the above processes

$N = Q(\sqrt[3]{2}, \omega)$

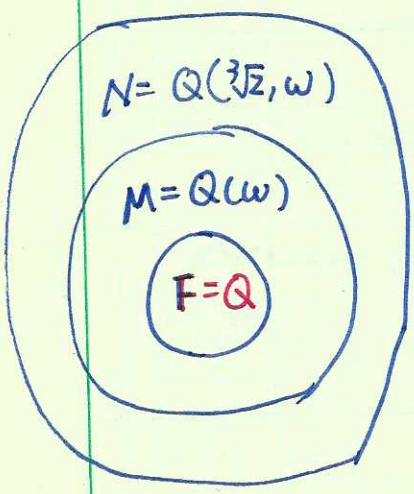
	E	f	f^2	g	fg	fg^2
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
ω	ω	ω	ω	ω^2	ω^2	ω^2

$S_3 = Gal(N/Q)$

$M = Q(\omega)$

	E	f	f^2
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$

$C_3 = Gal(N/M)$



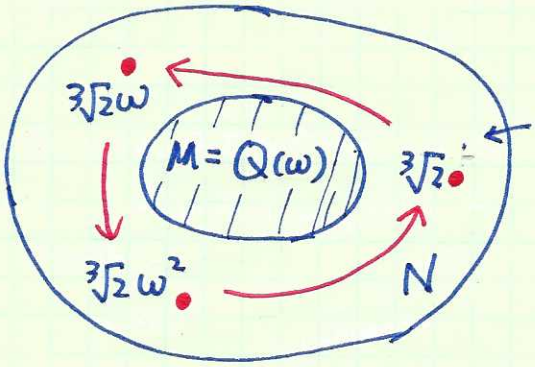
$1 = Gal(N/N)$

$\downarrow$

$C_3 = Gal(N/M) = Gal(Q(\sqrt[3]{2}, \omega)/Q(\omega))$

$\downarrow$

$S_3 = Gal(N/F) = Gal(Q(\sqrt[3]{2}, \omega)/Q)$



① C_3 applies on N/M

$Gal(N/M)$: M fixed,

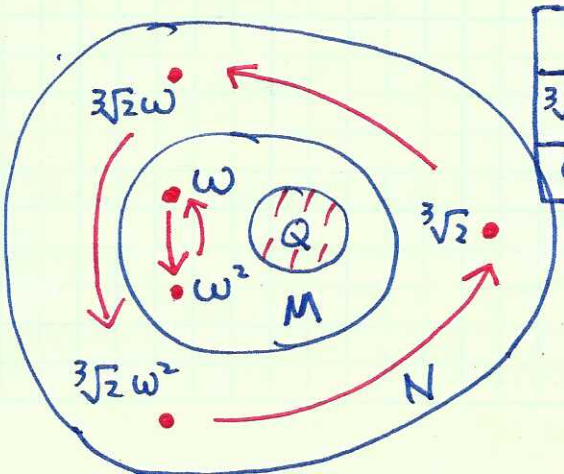
$\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$ rotate

② $S_3 = Gal(N/F)$ applies on N/F

↓ when S_3 only applies on M,

it's reduced to $S_3/C_3 = C_2$

$= Gal(M/Q)$.



	fg
$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$
ω	ω^2

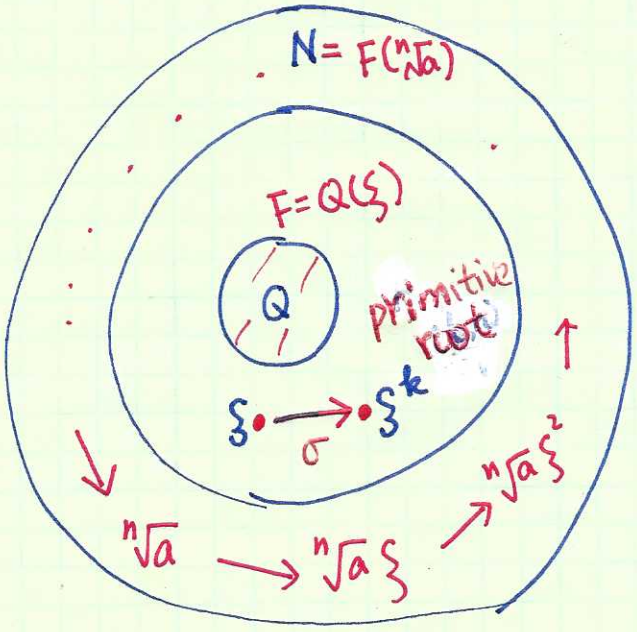
✱ Galois group of $x^n - a$ on the field $F = Q(\xi)$, $\xi = e^{i\frac{2\pi}{n}}$.

We have figured out that $Gal(F/Q) = (\mathbb{Z}/n\mathbb{Z})^*$, i.e. all the mapping ξ to a primitive root, which is an Abelian group. Now add $\sqrt[n]{a}$ into F, then $N = F(\sqrt[n]{a})$, and we ask $Gal(N/F) = ?$

We have roots $\{b = \sqrt[n]{a},\ b\xi,\ \cdots\ b\xi^{n-1}\}$, these roots are outside F, but in N. A mapping $\sigma_i \in Gal(N/F)$ changes $b \to b\xi^i$, then

$$\boxed{\sigma_i(b) = b\xi^i, \text{ and } \sigma_i(b\xi^j) = b\xi^{i+j}.}$$

This defines a n-th order cyclic group.



① $Gal(F/Q) = (\mathbb{Z}/n\mathbb{Z})^*$ ← Abliean but not neccesary cyclic

$\{k \pmod n\}$, $(k, n) = 1$ form a group under "product".

② $Gal(N/F) = \mathbb{Z}/n\mathbb{Z}$

Cyclic group

(*) A systemetic method

An equation $f(x)=0$ (is) defined in the field F, and N is its root field $F(u_1, \cdots u_n)$. G is the Galois group of $f(x)=0$. Any transformation T in G leaves $f(x)=0$ invariant, hence a root u after transformation remains a root of $f(x)=0$, i.e. $Tf(u) = f(T(u)) = 0$. More precisely,

$$T(u_1) = u_{\alpha 1},\quad T(u_2) = u_{\alpha 2},\quad \cdots \quad T(u_n) = u_{\alpha n},$$

hence T corresponds to a permutation among roots. But it's not necessary that every permutation corresponds to an automorphism transformation.

* Consider a polynomial $h = h(u_1, \cdots u_n)$ defined on F. If the value $h \in F$, then any $T \in Gal(N/F)$ also leaves h invariant. If the value $h \notin F$, then there must exist an operation T in $Gal(N/F)$, which changes the value of h. Otherwise the invariant part becomes $F(h)$.

Example: Galois group of $x^2+3x+1=0$. (define on Q)

Since there are only x_1 and x_2, $Gal(N/Q)$ is a subgroup of S_2.

consider $x_1 - x_2 = \sqrt{(x_1+x_2)^2 - 4x_1x_2} = \sqrt{5}$, and $\sqrt{5} \notin Q$, hence there must be an operation which changes $x_1 - x_2$. This is $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, which changes $x_1 - x_2 \to x_2 - x_1 = -\sqrt{5}$. Hence $Gal(N/Q) = S_2$.

If we view $x^2+3x+1=0$ as an equation defined on R, then $x_1 - x_2 = \sqrt{5} \in R$. Then only $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ leaves it invariant, its Galois group $G(N/R) = S_1$.

Example: $x^3 - 3x + 1 = 0$ on Q

- There are three roots $x_{1,2,3}$, hence, the Galois group is a subgroup of S_3.

Consider $h = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. For $x^3 + px + q = 0$, it can be proved

$$\Delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = -\frac{1}{108}(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = \left(\frac{1}{2}\right)^2 + (-1)^3 = -3/4$$

$$\Rightarrow h = \sqrt{108 \times 3/4} = \sqrt{81} = 9 \in Q$$

hence, $Gal(N/Q)$ leaves h invariant. Only the $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ leave h invariant. But $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ changes $h \to -h$.

$Gal(N/Q) = C_3$.

Example $x^3 - 2 = 0$ on Q

S_3 has the following subgroups

$G_1: \{E\}$, $G_2 = \left[E, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right]$, G_3, G_4

$G_5: \left\{E \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$, S_3

① Consider a polynomial $x_1 = \sqrt[3]{2} \notin Q$. There must be one operation in $Gal(N/Q)$ that changes $x_1 \to x_{2,3}$, hence G_1 and G_2 are not!

Similarly, G_3, G_4 cannot be.

② Consider $h = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = 6\sqrt{-3} \notin Q$

And there must be one operation in $Gal(N/Q)$ change h, hence G_5 cannot!

$\Rightarrow$ The only possibility is that $Gal(N/Q) = S_3$.

✱ Galois group of an equation with general coefficients

Consider $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ defined on field K, i.e. $a_1, \cdots a_n \in K$. The root field $N = K(x_1, \cdots x_n)$, then what's the Galois group $Gal[N/K] = ?$

Proof:

$$x_1 + \cdots x_n = -a_1 \qquad (1)$$

$$\begin{cases} \sum_{i<j} x_i x_j = a_2 & (2) \\ \vdots & \vdots \\ \sum_{i_1<\cdots<i_l} x_{i_1} \cdots x_{i_l} = (-)^l a_l \\ \vdots \\ x_1 \cdots x_n = (-)^n a_n & (n). \end{cases}$$

① $\forall\ \sigma \in Gal[N/K]$, Since $\sigma(x_i)$ also satisfies the equation. Hence $\sigma(x_1) \cdots \sigma(x_n)$ must be a permutation among roots. Hence $Gal[N/K] \subseteq S_n$.

② On the other hand, since the coefficients are general, we should also allow each root x_i can be mapped to any other root x_j. In other words, for any $\sigma \in S_n$, it obviously leaves all the symmetric polynominals invariant, i.e. $a_1 \cdots a_n$ invariant. Hence σ leaves K invariant, if $\in Gal[N/K]$, $\Rightarrow$ $Gal[N/K] = S_n$.

then $S_n \subseteq Gal[N/K]$.

Question: Why the $Gal[N/K]$ can be smaller for a concrete equation?

Consider $x^2 - 3x + 2 = 0$. Since $x_1 = 1, x_2 = 2 \in \mathbb{Q}$, they cannot be changed, hence its Galois group is trivial. The root field is still $\mathbb{Q}$.

The reason is Δ is a perfect square, i.e. $\sqrt{\Delta} \in \mathbb{Q}$. In other words, for $x^2 + ax + \frac{1}{4}(a^2 - c^2) = 0$. The Galois group is trivial, no square root is needed!

And also for the example $x^3-3x+1=0$. It's

$h=(x_1-x_2)(x_2-x_3)(x_3-x_1)\in\mathbb{Q}$, which cannot be changed! Hence its Galois group can only be C_3 but not S_3.

In other words, when we consider an equation with general coefficients, we do not put any extra constraint except the Viéta theorem, such that any permutation is in principle allowed!

(*) Discriminant: For an equation $x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots a_n=0$,

define $D=\prod_{i<j}(x_i-x_j)=\begin{vmatrix}1 & 1 & & 1\\ x_1 & x_2 & \cdots & x_n\\ \vdots & & & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1}\end{vmatrix}$.

* If $a_1,\cdots a_n$ are given #'s, and if $D\in K$, then $Gal(K(x_1\cdots x_n)/K)$ is a subgroup of A_n. If not, it must contain an odd permutation.

* $D^2=\begin{vmatrix}1 & 1 & & 1\\ x_1 & x_2 & \cdots & x_n\\ \vdots & & & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1}\end{vmatrix}\begin{vmatrix}1 & x_1 & \cdots & x_1^{n-1}\\ 1 & x_2 & & \vdots\\ \vdots & \vdots & & \\ 1 & x_n & & x_n^{n-1}\end{vmatrix}=\begin{vmatrix}S_0 & S_1 & \cdots & S_{n-1}\\ S_1 & S_2 & \cdots & S_n\\ \vdots & \vdots & & \vdots\\ S_{n-1} & S_n & \cdots & S_{2n-2}\end{vmatrix}$

$S_k=\sum_{i=1}^{n}r_i^k$

For quadratic case $D^2=\begin{vmatrix}S_0 & S_1\\ S_1 & S_2\end{vmatrix}=\begin{vmatrix}2 & -a_1\\ -a_1 & a_1^2-2a_2\end{vmatrix}=a_1^2-4a_2$

For the cubic case $D^2=4p^3+27q^2$ for $x^3+px+q=0$.

Theorem: Assume that the field F contains all the p-th order unit roots (p is a prime #). If N is a p-th order cyclic extension of F, then $N = F(\alpha)$ where α is a root of $x^p - a = 0$, with $a \in F$. $\neq 0$.

Proof: We denote $1, \xi, \xi^2, \cdots \xi^{p-1}$ as the p-th order unit roots.

$Gal(N/F)$ is a p-th order cyclic group: $= \{\tau, \tau^2, \cdots \tau^{p-1}, \tau^p = e\}$.

Pick up a number $\theta \in N$, but $\theta \notin F$, we find it's mappings

$\theta, \tau(\theta), \tau^2(\theta), \cdots \tau^{p-1}(\theta)$. Then we organize them with powers of the unit roots. We define

$$\begin{cases} a_1 = \theta + \xi\tau(\theta) + \xi^2\tau^2(\theta) + \cdots \xi^{p-1}\tau^{p-1}(\theta) \\ a_2 = \theta + \xi^2\tau(\theta) + \xi^4\tau^2(\theta) + \cdots \xi^{2(p-1)}\tau^{p-1}(\theta) \\ \vdots \\ a_j = \theta + \xi^j\tau(\theta) + \xi^{2j}\tau^2(\theta) + \cdots \xi^{j(p-1)}\tau^{p-1}(\theta) \\ \vdots \\ a_p = \theta + \tau(\theta) + \tau^2(\theta) + \cdots + \tau^p(\theta) \end{cases} \Rightarrow \sum_{j=1}^{p} a_j = p\theta$$

hence $\theta = \frac{1}{p}\sum_{j=1}^{p} a_j$

At least on $a_j \notin F$ otherwise $\theta \in F$.

($\tau(a_p) = a_p \in F$, hence it does work)

Assume $a_i = \theta + \xi^i\tau(\theta) + \xi^{2i}\tau^2(\theta) + \cdots + \xi^{(p-1)i}\tau^{p-1}(\theta) \notin F$,

Then $\tau(a_i) = \tau(\theta) + \xi^i\tau^2(\theta) + \cdots \xi^{(p-1)i}\theta$

$= \xi^{i(p-1)}(\theta + \xi^i\tau(\theta) + \xi^{2i}\tau^2(\theta) + \cdots \xi^{(p-1)i}\tau^{p-1}(\theta)) = \xi^{i(p-1)}a_i$

$\tau(a_i^p) = [\tau(a_i)]^p = a_i^p$ hence a_i^p is invariant under τ.

$\Rightarrow$ $a_i^p \in F$, Hence a_i is a root of $x^p - a = 0$ by setting $a = a_i^p$.

We take $\alpha = a_i$, then $N = F(\alpha)$.