2 Automorphism and Galois group

For a number field F, if there exists a mapping onto itself, such that $\forall \alpha, \beta \in F$, their images $S(\alpha)$ and $S(\beta)$ satisfy

$$S(\alpha)+S(\beta)=S(\alpha+\beta), \quad S(\alpha)S(\beta)=S(\alpha\beta),$$

then S is an automorphism mapping.

A field F's all automorphism transformations form a group, which is called "Automorphism group", denoted as Aut(F).

* For Q, the only possible automorphism operation is the identity mapping

Check S(0) and S(1): $S(0)+S(\beta)=S(\beta) \Rightarrow S(0)=0$

$S(1)S(\beta)=S(\beta) \Rightarrow S(1)=1$

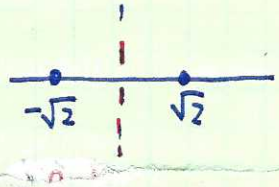
Based on S(0) and S(1), we can prove $\forall \alpha \in Q$, we have $S(\alpha)=\alpha$.

$\Rightarrow$ Aut(Q) = {e}.

* Aut($Q(\sqrt{2})$) — root field of $x^2-2=0$.

$x^2-2=0$ is invariant under automorphism, hence

$[S(\sqrt{2})]^2=2 \Rightarrow S(\sqrt{2})=\sqrt{2}$ or $-\sqrt{2}$. $\Rightarrow$ Aut($Q\sqrt{2}$) = S_2



* Galois group: If F has a subfield K, the automorphsim leaving K invariant also form a group, called the automorphism group F on K.

Consider an equation defined on F, $f(x)=0$. Its root field is N. The

automorphism group of N in F is defined as the Galoi's group of $f(x)=0$, denoted as $Gal(N/F)$.

(*) $Gal(N/F)$ is a subgroup of $Aut(N) = Gal(N/Q)$, since all operations leaving F invariant also leaves Q invariant.

(*) If u satisfies an irreducible equation $x^n + b_{n-1}x^{n-1} + \cdots b_0 = 0$ on K. Then $S(u)$ also satisfies this equation, i.e. $S(u)$ is a conjugation of u.

Proof: $S(u^n + b_{n-1}u^{n-1} + \cdots b_0) = 0 \Rightarrow$

$$[S(u)]^n + b_{n-1}[S(u)]^{n-1} + \cdots b_0 = 0. \quad \checkmark$$

(*) Example: $Gal(F/Q) = D_2$

An irreducible equation on Q: $x^4 - 2x^2 + 9 = 0 \Rightarrow$ roots $\pm(\sqrt{2} \pm i)$.

Its root field $F = Q(\sqrt{2}, i)$. Since $Gal(Q(\sqrt{2})/Q) = Z_2$, and

$Gal(F/Q(\sqrt{2})) = Z_2$, hence

$$\boxed{Gal(F/Q) = D_2 = Z_2 \otimes Z_2}$$

one Z_2 maps: $\sqrt{2} \leftrightarrow -\sqrt{2}$

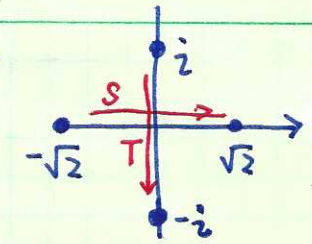
one Z_2 maps $i \leftrightarrow -i$.

The D_2 group has two generators

	E	S	T	ST
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
i	i	i	$-i$	$-i$

D_2 is also the symmetry of the root distribution.

or C_{2v}.



Comment: We cannot map $S(\sqrt{2}) \to i$ otherwise $\sqrt{2}\cdot\sqrt{2} = 2 \to i^2 = -1$, but Q should be map to itself.

(*) An example of $Gal(F/Q) = D_4$

Consider the root field of $x^4 - 3 = 0$. Its roots $\pm\sqrt[4]{3}, \pm\sqrt[4]{3}\,i$. Hence,

$F = Q(\sqrt[4]{3}, i)$. Then $[Q(\sqrt[4]{3}) : Q] = 4$, $[Q(\sqrt[4]{3}, i) : Q(\sqrt[4]{3})] = 2$

Hence $[F : Q] = 8$.

- A number in F can be expressed $u = a_1 + a_2\sqrt[4]{3} + a_3\sqrt{3} + a_4\sqrt[4]{27}$
$+ a_5 i + a_6\sqrt[4]{3}\,i + a_7 i\sqrt{3} + a_8 i\sqrt[4]{27}$.

where $a_{1\sim 8} \in Q$.

Its Galois group / automorphism group has two generators

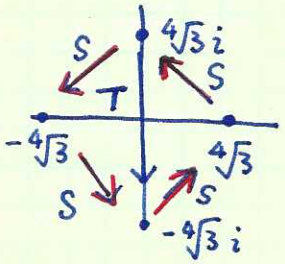
$$S: \begin{cases} S(\sqrt[4]{3}) = i\sqrt[4]{3} \\ S(i) = i \end{cases} \qquad T: \begin{cases} T(\sqrt[4]{3}) = \sqrt[4]{3} \\ T(i) = -i \end{cases}$$

only need to consider the mappings of $\sqrt[4]{3}$ and "i".

$Gal(F/Q) = \{E, S, S^2, S^3, T, TS, TS^2, TS^3\}$

Since automorphism makes $x^4 - 3 = 0$ invariant, hence, it makes

$\sqrt[4]{3}$ into $\pm\sqrt[4]{3}$, $\pm i\sqrt[4]{3}$.



$$S(u) = a_1 - a_6\sqrt[4]{3} - a_3\sqrt{3} + a_8\sqrt[4]{27}$$
$$+ a_5 i + a_2\sqrt[4]{3}\,i - a_7 i\sqrt{3} - a_4 i\sqrt[4]{27}$$

$T(u)$ is obvious

	E	S	S^2	S^3	T	TS	TS^2	TS^3
$\sqrt[4]{3}$	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Comment: since $i^2 = -1 \in Q$, hence $S^2(i) = T^2(i) = -1$, hence i can only be mapped to $\pm i$. Also since $(\sqrt[4]{3})^4 = 3 \in Q$, hence it's mapped to one of 4 roots. Hence, we have $2 \times 4 = 8$ different mappings, which can generated by R and T as above.

⊛ An example of $Gal(F/Q) = S_3$

Consider the root field N of $x^3 - 2 = 0$, whose roots are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$.

Its root field can be simply expressed as $Q(\sqrt[3]{2}, \omega)$. (comment: ω is in N since $\omega = \frac{1}{2}(\sqrt[3]{2})^2(\sqrt[3]{2}\,\omega)$. And once $\sqrt[3]{2}$ and ω are included, the three roots are automatically included.)

The automorphism group of $Q(\sqrt[3]{2})$ is trivial since $\sqrt[3]{2}$ can only be mapped to itself. $[S(\sqrt[3]{2})]^3 = 2$ and $S(\sqrt[3]{2})$ is real $\Rightarrow S(\sqrt[3]{2}) = \sqrt[3]{2}$.

Now consider the Galois group $Gal(Q(\sqrt[3]{2}, \omega))$: Any number in $Q(\sqrt[3]{2}, \omega)$ can be expressed as

$$u = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4\omega + a_5\sqrt[3]{2}\omega + a_6\sqrt[3]{4}\omega$$

$\omega^2 = -(1+\omega)$ is not independent

We only need to check the mapping of the generators $\sqrt[3]{2}$ and ω.

since $[S(\sqrt[3]{2})]^3 = S(2) = 2 \Rightarrow \sqrt[3]{2}$ can only be mapped to $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$

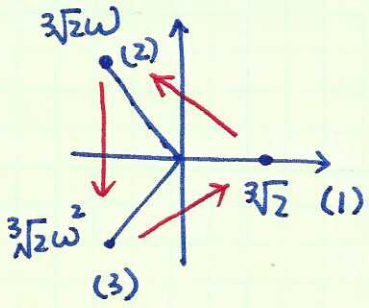
$[S(\omega)]^3 = S(\omega^3) = S(1) = 1$, and $S(\omega) \neq 1$, hence ω can only be mapped to ω, ω^2

Hence, we have 6 possible mapping

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

This is S_3 or D_3 or C_{3v} group!!!

We denote the three roots as 1, 2 and 3.



$E: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$f: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\sqrt[3]{2} \to \sqrt[3]{2}\omega$ $\to \sqrt[3]{2}\omega^2 \to \sqrt[3]{2}$

$f^2: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$g: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\sqrt[3]{2} \to \sqrt[3]{2}$, $\sqrt[3]{2}\omega \to \sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega^2 \to \sqrt[3]{2}\omega$

$fg: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $f^2g: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Hence,

$Gal(Q(\sqrt[3]{2}, \omega)/\cdot)$

becomes the symmetric group of the roots.

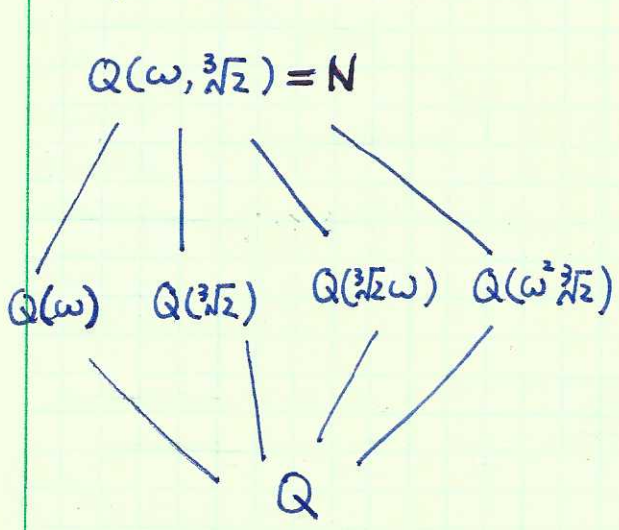
We can also check $Gal[Q(\sqrt[3]{2}, \omega)/Q(\omega)] = \{E, f, f^3\}$, since ω is fixed

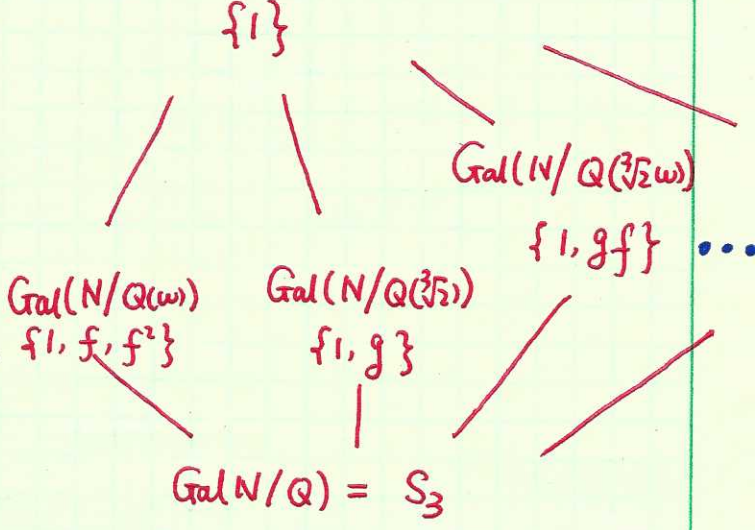
$Gal[Q(\sqrt[3]{2}, \omega)/Q(\sqrt[3]{2})] = \{E, g\}$, only those maintains $\sqrt[3]{2}$ invariant.

Similarly $Gal[Q(\sqrt[3]{2}, \omega)/Q(\omega\sqrt[3]{2})] = \{E, f^2g = gf\}$,

$Gal[Q(\sqrt[3]{2}, \omega)/Q(\omega^2\sqrt[3]{2})] = \{E, fg = gf^2\}$.

This procedure can be summerized as





(*) $Gal(Q(\xi)/Q)$ $\xi = e^{2\pi i/p}$ where p is a prime number

The root field of the irreducible polynomial $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ on the field Q is $Q(\xi)$. Consider $Aut(Q(\xi))$, or, $Gal(Q(\xi)/Q)$.

We have roots $\xi, \cdots \xi^{p-1}$. Once $\sigma(\xi)$ is determined, we have $\sigma(\xi^s) = (\sigma(\xi))^s$. Hence we define the mapping $\sigma_l(\xi) = \xi^l$, $(1 \le l \le p-$

① This is a automorphism since $\sigma_l(\xi^s) = \xi^{ls}$, and

$ls \pmod p$ runs over $1, \cdots p-1$ as s runs from $1, \cdots p-1$.

② Different σ_l form a $p-1$-order cyclic group

$$\sigma_{l_1}\sigma_{l_2}(\xi) = \sigma_{l_1}(\xi^{l_2}) = \xi^{l_1 \cdot l_2} = \sigma_{l_1 l_2}(\xi).$$

This is a product group defined on Z/pZ excluding those divided by p, denoted as $(Z/pZ)^*$. For example

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

σ_l

#'s in this table are the l's of σ_l.

⊛ primitive roots, Galois group of $X^n - 1 = 0$

If n is composite, i.e $n = p_1^{k_1} p_2^{k_2} \cdots p_e^{k_e}$, then not all of the n-th order unit roots are at equal footing. For those ω, whose powers, $\{\omega, \omega^2, \ldots\}$ can run over the entire series of $\{\xi, \xi^2, \cdots \xi^{n-1}, 1\}$, $\xi = e^{i\frac{2\pi}{n}}$, they are called primitive roots. For example, $X^4 = 1$: $X = -1$ is not primiti but $X = \pm i$ are. Consider a concrete example $n = 12$: four primitive root $(\xi, \xi^5, \xi^7, \xi$

	ξ	ξ^2	ξ^3	ξ^4	ξ^5	ξ^6	ξ^7	ξ^8	ξ^9	ξ^{10}	ξ^{11}
σ_1	ξ	ξ^2	ξ^3	ξ^4	ξ^5	ξ^6	ξ^7	ξ^8	ξ^9	ξ^{10}	ξ^{11}
σ_5	ξ^5	ξ^{10}	ξ^3	ξ^8	ξ^1	ξ^6	ξ^{11}	ξ^4	ξ^9	ξ^2	ξ^7
σ_7	ξ^7	ξ^2	ξ^9	ξ^4	ξ^{11}	ξ^6	ξ^1	ξ^8	ξ^3	ξ^{10}	ξ^5
σ_{11}	ξ^{11}	ξ^{10}	ξ^9	ξ^8	ξ^7	ξ^6	ξ^5	ξ^4	ξ^3	ξ^2	ξ^1

$\rightarrow (\mathbb{Z}/n\mathbb{Z})^*$

* Only when we map $\sigma(\xi)$ to a primitive root, such that $\sigma(\xi^l)$ can general an automorphism of $\mathbb{Q}(\xi)$. (k coprime with n)

* The primitive roots are those ξ^k, that $(k, n) = 1$. The # in this set is determined by the Euler function, $\varphi(n) = n(1-1/p_1)\cdots(1-1/p_e)$.

For $n = 12 = 2^2 \cdot 3$, $\varphi(n) = 12(1-1/2)(1-1/3) = 4$.

* The above mappings $\begin{cases} \sigma_l(\xi) = e^{i\frac{2\pi}{n}l} & \text{with } (l, n) = 1 \\ \sigma_l(\xi^s) = (\xi^s)^l \end{cases}$ form an

Abelian group, since $\sigma_{l_1}(\sigma_{l_2}(\xi^s)) = (\xi^s)^{l_1 l_2}$ and $(l_1 l_2, n) = 1$. hence $\xi^{l_1 l_2}$ remains primitive. — For $n = 12$, it's D_2.

* The Galois group $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$, for a general n.