A Galois Extension is a finite separable normal extension.

Theorem: a finite extension K/F is Galois if $|Aut(K/F)| = [K:F]$.

Proof: Aut-sms of K/F are embeddings $K/F \to K/F$, and

$\#$ embeddings $\leq [K:F]$, with equality iff

$\exists\, \alpha_1, \dots, \alpha_k \in K$ s.t. $K = F(\alpha_1, \dots, \alpha_k)$, α_i are

separable over F, and K contains all their conjugates

iff $\forall \alpha \in K$, α is separable and K contains all

its conjugates, That is, K is Galois.

Theorem K/F is Galois iff K is a splitting field of a separable polynomial from $F[x]$.

---

if K/F is Galois, then $Gal(K/F) := Aut(K/F)$.

If K is a spl. field of a separable $f \in F[x]$, $Gal(f) := Gal(K/F)$.

Examples

(1) Non-Galois extension: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. trivial

Examples

① Non-Galois extension: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

trivial group

$$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3, \quad \text{but } \operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$$

② $\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}$ is Galois.

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = V_4$$

③ $\mathbb{Q}(\alpha,\omega)/\mathbb{Q}$ (where $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3} = \sqrt[3]{1}$) is Galois.

splitting field of x^3-2. $\quad |\operatorname{Aut}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})| = 6$ since $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}] = 6$.

$\omega \mapsto \omega$ or ω^2, $\quad \alpha \mapsto \alpha$, $\alpha\omega$ or $\alpha\omega^2$ $\quad$ every choice is ok

So $\operatorname{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q}) \cong \mathbb{Z}_6$ or S_3 ...

take $\varphi_1 : \begin{matrix}\omega \mapsto \omega^2 \\ \alpha \mapsto \alpha\omega\end{matrix}$, $\quad \varphi_2 : \begin{matrix}\omega \mapsto \omega \\ \alpha \mapsto \alpha\omega\end{matrix}$.

Then $\varphi_1 \circ \varphi_2 : \begin{matrix}\omega \mapsto \omega \mapsto \omega^2 \\ \alpha \mapsto \alpha\omega \mapsto \alpha\omega\cdot\omega^2 = \alpha\end{matrix}$

$\varphi_2 \circ \varphi_1 : \begin{matrix}\omega \mapsto \omega^2 \mapsto \omega^2 \\ \alpha \mapsto \alpha\omega \mapsto \alpha\omega^2 \neq \alpha\end{matrix}$

So $\operatorname{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$ is not commutative,

So $\operatorname{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q}) \cong S_3$.

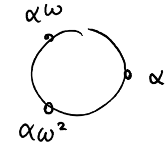
$$\| $$

$$\langle \tau : \omega \mapsto \omega^2,\ \varphi : \alpha \mapsto \alpha\omega \rangle$$

by the way, $\mathbb{Q}(\alpha,\omega) = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$

$\alpha\omega$

by the way, $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$



$$|Gal(\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)/\mathbb{Q})| = 6,$$

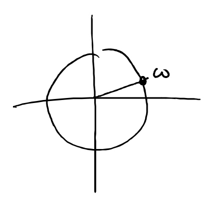
and it's a subgroup of S_3 since each aut-sm permutes the roots.

so it's equal to S_n.

(assume K/F is Galois)

If $K = F(\alpha_1, \dots, \alpha_k)$, A is the set of all conjugates of $\alpha_1, \dots, \alpha_k$, then $Gal(K/F) \leq S_A$

④ $K = \mathbb{Q}(\omega)$, $\omega = e^{2\pi i/n} = \sqrt[n]{1}$



This is normal b.c. all conjugates of ω are its powers.

$$|Gal(K/\mathbb{Q})| = \varphi(n) \quad \text{since} \quad [K : \mathbb{Q}] = \varphi(n).$$

conjugates of ω are ω^k, $(k, n) = 1$.

$\forall \varphi \in Gal(K/\mathbb{Q})$, $\varphi : \omega \longmapsto \omega^k$ for some $(k, n) = 1$.

Let $\varphi_k : \omega \mapsto \omega^k$. Then $Gal(K/\mathbb{Q}) = \{\varphi_k : (k, n) = 1\}$.

$(\varphi_k \circ \varphi_l)(\omega) = \omega^{l \cdot k} = \varphi_{k \cdot l}(\omega)$. So $\varphi_k \longleftrightarrow k$ is an isomorphism $Gal(K/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.

⑤ $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois.

$|Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. $\quad \Phi$ - Frobenius aut-sm $\in Gal$.

order of Φ is n, so $Gal = \langle \Phi \rangle \cong \mathbb{Z}_n$.

Theorem

(a) if K/F is Galois and $F \subseteq L \subseteq K$,

then K/L is Galois.

(b) if L_1/F, L_2/F are Galois extensions & $L_1, L_2 \subseteq K$,

then $(L_1 \cap L_2)/F$ is Galois.

(c) if L_1/F, L_2/F are Galois and $L_1, L_2 \subseteq K$,

then $(L_1L_2)/F$ is Galois.

Proof of (c) L_1L_2 is generated by elements of L_1 & L_2, which are separable and "normal" over F (i.e. all conjugates over F appear).

If K/F is finite & separable separable, then the normal closure

E/F of K/F is called the Galois Closure of K/F.

(E/F is Galois).

E/F is generated by conjugates of K/F.

If K/F is Galois, then $\forall \alpha \in K$,

$\mathrm{Gal}(K/F)$ acts transitively on the set of conjugates of α (any conjugate can be sent to any other conjugate).

If K/F is Galois, $F \subseteq L \subseteq K$, then any embedding $L/F \longrightarrow K/F$ is given by $\varphi|_L$ for some element $\varphi \in \mathrm{Gal}(K/F)$.