which implies $h|\sigma(\beta)| = \sigma(\beta)$ and

thus $\sigma(\beta) \in E^{Gal(E|B)} = B$. ∎

Example IV.17.

Let $f(X) = X^3 - 2 \in \mathbb{Q}(X)$ and

E its splitting field.

First we observe that f is irreducible:

[indeed otherwise it would have a

root $\frac{p}{q} \in \mathbb{Q}$; say p, q coprime. But

then $p^3 = 2q^3 \Rightarrow 2|p \Rightarrow 8|2q^3 \Rightarrow$

$4|q^3 \Rightarrow 2|q$ contr.]

Let $\beta = \sqrt[3]{2} \in \mathbb{R}$, $\omega = e^{\frac{2\pi i}{3}}$.

Then the roots of f are

$$\alpha_1 = \beta, \quad \alpha_2 = \beta\omega, \quad \alpha_3 = \beta\omega^2.$$

4.5.18

Now $[E:\mathbb{Q}] = [E:\mathbb{Q}(\beta)]\underbrace{[\mathbb{Q}(\beta):\mathbb{Q}]}_{3}$

and since $E \not\subset \mathbb{R}$, we have

$$[E:\mathbb{Q}] \geq 2 \cdot 3 = 6.$$

Since $Gal(E/\mathbb{Q}) \hookrightarrow S_3$ we get

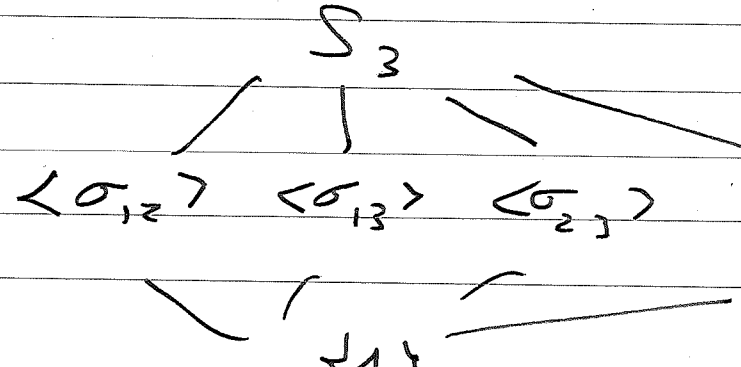
$$Gal(E/\mathbb{Q}) = S_3.$$

Thus any permutations of $\{\alpha_1, \alpha_2, \alpha_3\}$ is induced by a (unique) element in $Gal(E/\mathbb{Q})$.

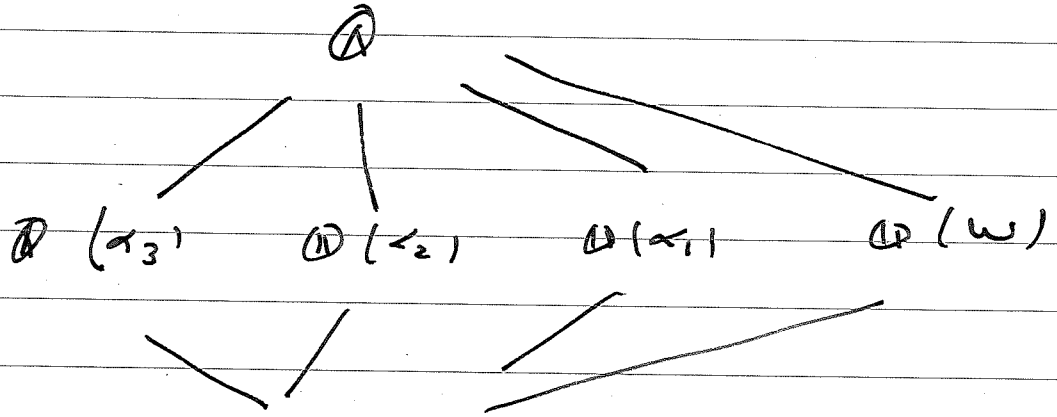
Let σ_{ij} correspond to the automorph. $\alpha_i \leftrightarrow \alpha_j$, and fixing α_k

and let τ: $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_1$.

The lattice of subgroups of S_3 is (exercise)



We claim that the corresponding lattice of fixed fields is:



For instance: $\sigma_{12}(\alpha_3) = \alpha_3$ hence

$E^{\langle\sigma_{12}\rangle} \supset \Phi(\alpha_3)$; but $[E : E^{\langle\sigma_{12}\rangle}] = 2$

hence $[E^{\langle\sigma_{12}\rangle} : \Phi] = 3$ which implies

$$E^{\langle\sigma_{12}\rangle} = \Phi(\alpha_3).$$

Next: $\tau(w) = \tau\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\alpha_3}{\alpha_2} = \frac{\beta w^2}{\beta w} = w.$

Hence $E^{\langle\tau\rangle} \supset \Phi(w) \supsetneq \Phi$

and since $[E : E^{\langle \tau \rangle}] = 3$ this implies $E^{\langle \tau \rangle} = \mathbb{Q}(w)$.

Now we'll examine a certain number of consequences of the Galois correspondence. The most straightforward is:

Corollary IV.18. A (finite) Galois extension has only finitely many intermediate subfields.

Proof: $G = Gal(E/k)$ is finite and has therefore only finitely many subgroups. ∎

Def. IV.19: An extension E/k is simple if there is $u \in E$ with $E = k(u)$.