Definition 1. Let F/K be an extension of fields. Then an intermediate field $K \subseteq E \subseteq F$ is *stable* if $\sigma(E) = E$ for all $\sigma \in \mathrm{Aut}_K(F)$.

Lemma 1. *(i) If E is stable, then $E' = \mathrm{Aut}_E(F)$ is a normal subgroup of $\mathrm{Aut}_K(F)$.*

(ii) If $H \leq \mathrm{Aut}_K(F)$ is normal, then $H' = \mathrm{Aut}_K(F)'$ is stable.

Proof. (i) Suppose that E is stable, and let $\tau \in E'$ and $\sigma \in \mathrm{Aut}_K(F)$. If $\alpha \in E$, then $\sigma(\alpha) \in E$, and so $\tau\sigma(\alpha) = \sigma(\alpha)$, and thus, $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. As α was arbitrary, so $\sigma^{-1}\tau\sigma \in E'$, and $E' \lhd \mathrm{Aut}_K(F)$.

(ii) Suppose that H is a normal subgroup of $\mathrm{Aut}_K(F)$. Let $\sigma \in \mathrm{Aut}(F/K)$ and $\tau \in H$. Then $\sigma^{-1}\tau\sigma \in H$ since H is a normal subgroup of $\mathrm{Aut}_K(F)$. Thus, for any $\alpha \in H'$, we have $\sigma^{-1}\tau\sigma(\alpha) = \alpha$, and as H' is the fixed field, $\tau\sigma(\alpha) = \sigma(\alpha)$ for all $\tau \in H$. Thus, $\sigma(\alpha) \in H'$ for any $\alpha \in H'$ and $\sigma \in \mathrm{Aut}_K(F)$, so H' is stable. □

Lemma 2. *If F/K is Galois and E is a stable intermediate field of the extension, then E is Galois over K.*

Proof. If $\alpha \in E \setminus K$, then there exists $\sigma \in \mathrm{Gal}(F/K)$ such that $\sigma(\alpha) \neq \alpha$. But $\sigma(E) = E$, so $\sigma|_E \in \mathrm{Aut}_K(E)$. So α is not fixed by some element of $\mathrm{Aut}_K(E)$ and as α was arbitrary, $\mathrm{Aut}_K(E)' = K$. □

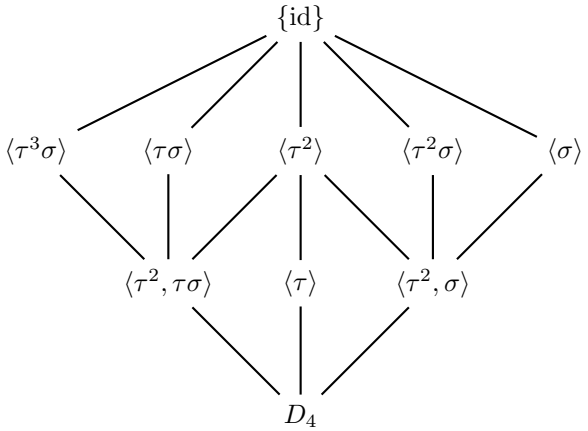
Note if F/K is a finite Galois extension, restriction gives a homomorphism $\mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ if $K \subseteq E \subseteq F$ is stable. This is also onto, so an isomorphism $\sigma \in \mathrm{Aut}(E)$ can be extended to a finite extension. Thus,

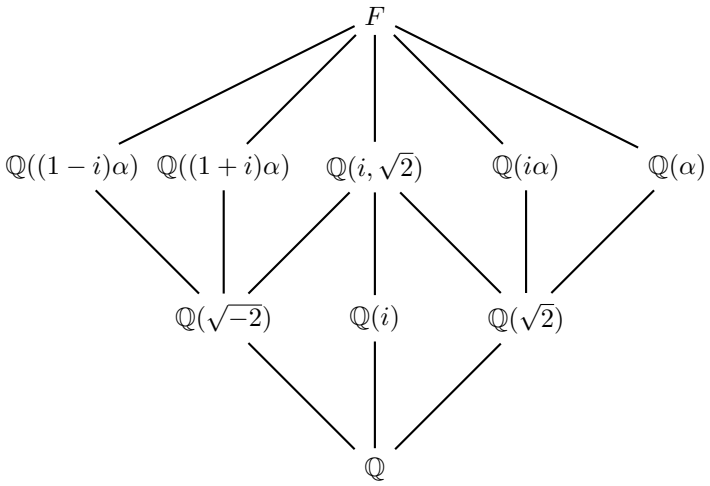
$$\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(F/K)/\mathrm{Gal}(F/E)$$

Lemma 3. *Let F/K be Galois, and suppose that the intermediate field E is algebraic and Galois. Then it is stable over K.*

Example 1. Let $F = \mathbb{Q}(i, \sqrt[4]{2})$ and let $\alpha = \sqrt[4]{2}$. Consider this as an extension of $\mathbb{Q}$. We first claim that there exists automorphisms $\sigma, \tau \in \mathrm{Aut}(\mathbb{Q}(i, \sqrt[4]{2}))$ with $\sigma(i) = -i$, $\sigma(\alpha) = \alpha$, $\tau(i) = i$, and $\tau(\alpha) = i\alpha$. The identity function $\mathrm{id} : \mathbb{Q}(i) \to \mathbb{Q}(i)$ can be extended to an isomorphism $\tau : \mathbb{Q}(i, \alpha) \to \mathbb{Q}(i, i\alpha) = \mathbb{Q}(i, \alpha)$ with $\tau(\alpha) = i\alpha$. Observe that here, for $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(F)$, we have $\sigma^2 = \tau^4 = \mathrm{id}$ and $\sigma^{-1}\tau\sigma(i) = i$ and $\sigma^{-1}\tau\sigma(\alpha) = i^3\alpha$. Therefore, $\sigma^{-1}\tau\sigma(x) = \tau^3(x)$ for $x = i$ and $x = \alpha$. Furthermore, $\sigma^{-1}\tau\sigma = \tau^{-1}$. In particular, $\langle \sigma, \tau \rangle \leq \mathrm{Aut}_{\mathbb{Q}}(F)$. In fact, this is a dihedral group D_4, and $\langle \sigma, \tau \rangle \simeq D_4$. In fact, $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq D_4$.

We are then able to consider the following lattice diagrams.





Definition 2. F/K is said to be a *splitting field* of $f(x) \in K[x]$ if

1. $f(x) = \alpha(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in F[x]$ for some $\alpha, \alpha_i \in F$, i.e. f splits over F
2. $F = K(\alpha_1, ..., \alpha_n)$, where $\alpha_1, ..., \alpha_n$ are the roots of f in F.

Let $\mathcal{P}(K)$ be the set of polynomials of positive degree in $K[x]$. An extension F/K is a *splitting field* over K of the set $\mathcal{P}(K)$ of polynomials if every polynomial in $\mathcal{P}(K)$ splits in $F[x]$ and F is generated over K by the roots of all the polynomials in $\mathcal{P}(K)$.

Note that every polynomial $f(x) \in K[x]$ has a splitting field F/K with $[F:K] \leq \deg(f)!$.

Definition 3. Let $f(x) \in K[x]$ be irreducible. Then $f(x)$ is *separable* if in some splitting field, every root of f is simple, that is, the linear factors are distinct.

Definition 4. An element $\alpha \in F$ is separable over K if its minimal polynomial over K is separable; F/K is separable if and only if every element is separable.

Example 2. Let $K = \mathbb{F}_p(t)$ be the field with p elements with indeterminate t, and let $f(x) = x^p - t$, which is irreducible by Eisenstein's criterion. Let F be a splitting field and $f(s) = 0$ for $s \in F$. Then $s^p = t$ and so $f(x) = x^p - t = x^p - s^p = (x-s)^p$, so s is the only root in $f(x)$.