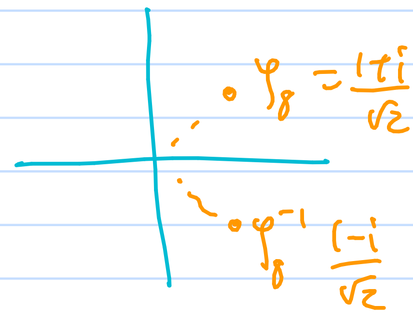
2) $[\mathbb{Q}(\zeta_8):\mathbb{Q}] = \varphi(8) = 4$




$\Phi_8(x) = x^4+1$

$\zeta_8^2 = i \Rightarrow \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_8)$

$\zeta_8 + \zeta_8^{-1} = \sqrt{2} \Rightarrow \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

More about simple extensions: $\begin{pmatrix} K = F(\alpha) \\ | \\ F \end{pmatrix}$

Thm: If $K$ is finite then any field ext. $K/F$ is simple.

(We proved this in the section on finite fields)

Thm: Suppose $K/F$ is a field extension, $[K:F]<\infty$, and $\operatorname{char} F = 0$. Then it is a simple extension.

Pf: Since $K$ is obtained from $F$ by adjoining a finite # of elements (since $[K:F]<\infty$), it suffices by an inductive argument to consider the case when $K = F(\alpha_1, \alpha_2)$.

Let $f_i(x) = \min_F(\alpha_i)$, $i = 1, 2$. In appropriate splitting fields, these polys. factor as

$$f_1(x) = \prod_{i=1}^{n} (x - \beta_i), \quad f_2(x) = \prod_{j=1}^{m} (x - \gamma_j).$$

Suppose $\beta_1 = \alpha_1$, $\gamma_1 = \alpha_2$.

(*) Lemma: If $F$ is any field of charac. 0, every irred. poly. in $F[x]$ is separable.

Pf: Suppose $f \in F[x]$ is irred., write

$$f(x) = \sum_{i=0}^{n} a_i x^i. \quad \text{Then} \quad D_x(f)(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

(w.l.o.g. assume $a_n = 1$)

Since char $F = 0$, $n a_n \neq 0 \Rightarrow \deg(D_x f) = n-1$.

For any root $\alpha$ of $f$, $\min_F(\alpha) = F$

$\Rightarrow D_x(f)(\alpha) \neq 0$.

Therefore $f$ is separable. ■

Back to main proof, since char $F = 0$, all roots of $f_1$ are distinct and all roots of $f_2$ are distinct. It follows that, $\forall 1 \leq i \leq n$ and $\forall 2 \leq j \leq m$, there is at most one value of $x \in F(\alpha_1, \alpha_2)$ for which $\beta_i + x\gamma_j = \beta_1 + x\gamma_1$.

Since $|F| = \infty$, (char $F = 0 \Rightarrow \mathbb{Q} \subseteq F$)

$$\begin{aligned} &\beta_i + x\gamma_j = \beta_1 + x\gamma_1 \\ -&(\beta_i + x'\gamma_j = \beta_1 + x'\gamma_1) \\ \hline &\cancel{(x-x')}\gamma_j = \cancel{(x-x')}\gamma_1 \end{aligned}$$

$\exists c \in K(\alpha_1, \alpha_2)$ s.t.

$\beta_i + c\gamma_j \neq \beta_i + c\gamma_1$, $\forall 1 \leq i \leq n$, $2 \leq j \leq m$.

Now set $\theta = \beta_1 + c\gamma_1 = \alpha_1 + c\alpha_2$.

Claim: $\alpha_2 \in F(\theta)$.

To see this, define $g \in (F(\theta))[x]$ by $g(x) = f_1(\theta - cx)$. Since $g(\alpha_2) = 0$ we have that $\min_{F(\theta)}(\alpha_2) \mid g(x)$.

Similarly, since $f_2 \in (F(\theta))[x]$ and $f_2(\alpha_2) = 0$, we have $\min_{F(\theta)}(\alpha_2) \mid \gcd(g, f_2)$.

Let $h(x) = \gcd(g, f_2)$. If $\delta$ were a root of $h$ different from $\alpha_2$ (in some algebraic closure) then we would have:

(i) $\delta$ is a root of $f_2 \Rightarrow \delta = \gamma_j$ for some $2 \leq j \leq m$

(ii) $\theta - c\delta$ is a root of $f_1$

$\Rightarrow \theta - c\delta = \beta_i$ for some $1 \leq i \leq n$

$\Rightarrow \theta = \beta_i + c\gamma_j \Rightarrow \alpha_1 + c\alpha_2 = \beta_i + c\gamma_j$.

Contradiction $\Rightarrow h(x)$ is linear

$\Rightarrow \alpha_2 \in F(\theta)$.

$\Rightarrow \alpha_1 \in F(\theta)$

$\Rightarrow F(\alpha_1, \alpha_2) = F(\theta)$. ∎

Def: An ext. $K/F$ with $[K:F] < \infty$ is <u>separable</u> if $\forall \alpha \in K$, $\min_F(\alpha)$ is separable.

Primitive Element Theorem: If $K/F$ is a separable field ext., $[K:F] < \infty$, then it is simple.

Pf: follows from exactly the same arguments used to prove the previous two thms. ∎

# Field automorphisms

**Defs:** Suppose $K/F$ is a field extension.

$\mathrm{Aut}(K)$ = group of all field automorphisms of $K$, under composition

$\mathrm{Aut}(K/F)$ = subgroup of all $\sigma \in \mathrm{Aut}(K)$ which fix $F$

$\sigma \in \mathrm{Aut}(K)$ fixes $F$ if $\sigma|_F = $ identity.

Equiv. $\forall a \in F$, $\sigma(a) = a$.

**Lemma:** Any element of $\mathrm{Aut}(K)$ fixes the prime subfield of $K$.

Pf: $\forall \sigma \in \mathrm{Aut}(K)$, $\sigma(1) = 1$, so

$$\sigma\left(\frac{a}{b}\right) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b}, \quad \forall a, b \in \mathbb{Z}, \quad b \neq 0 \quad \blacksquare$$