Content:

Theorem If E/F is an extension of fields such that $[E:F] < \infty$, then E is a simple extension $\Leftrightarrow$ there are a finite number of intermediate fields between F and E.

Corollary $F \lhd E \Rightarrow E$, is a simple extension.

Definition We say $\alpha \in F$ is separable if $\min(\alpha, F)$ is separable.

Corollary If $E = F(a_1, \ldots, a_n)$ such that $a_i \in E$ is separable $\forall\, i$, then $\exists\, \theta \in E$ such that $E = F(\theta)$.

Example $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.

Theorem** If $F \lhd E$ and $F \subseteq K \subseteq E$, then $F \lhd K \Leftrightarrow \mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$.

Theorem

If E/F is an extension of fields such that $[E:F] < \infty$, then E is a simple extension $\Leftrightarrow$ there are a finite number of intermediate fields between F and E.

Proof:

Assume $E = F(\alpha)$ for some $\alpha \in E$. Since $[E:F] < \infty$, we know α is algebraic.

Let $p(x) = \min(\alpha, F)$. Let B be an intermediate field, then $F \subseteq B \subseteq E$.

Let $g(x) = \min(\alpha, B)$. *Note that $E = B(\alpha)$.

Let $g(x) = b_0 + b_1 x + \cdots + b_{m-1}x^{m-1} + x^m$, $b_i \in B$.

So $[E:B] = \deg g(x) = m$. Define $B' = F(b_0, \ldots, b_{m-1})$. Then $F \subseteq B' \subseteq B \subseteq E$.

Since $g(x) \in B'[x]$ and g is irreducible over B, then g is irreducible over B'.

Similarly to *, $E = B'(\alpha)$.

Thus $[E:B'] = \deg g(x) = m$. And since $B' \subseteq B$ we have $B' = B$.

So then any intermediate field is completely determined by the $\min(\alpha, B)$.

We need only show there are finitely many $\min(\alpha, B)$.

Since $\min(\alpha, B)$ is monic and must divide $p(x)$ which is also monic, there are only finitely many possibilities for the $\min(\alpha, B)$.

$\therefore$ There are a finite number of intermediate fields between F and E.

Conversely, assume there are finitely many intermediate fields.

Since $[E:F] < \infty$, then $|F| < \infty \Rightarrow |E| < \infty$.

So $E^* = \langle \alpha \rangle$, for some $\alpha \in E$. We have proven previously $E = F(\alpha)$.

Assume $|F| = \infty$. Then $|E| = \infty$.

Claim: For each $\alpha, \beta \in E$, $\exists\, \gamma \in E$ such that $F(\alpha, \beta) = F(\gamma)$.

Let $T = \{\alpha + c\beta \mid c \in F\}$. Since $|F| = \infty$, $|T| = \infty$.

Consider $F(\alpha + c\beta)$. Since there are only finitely many intermediate fields there must exist $c_1, c_2 \in F$, $c_1 \neq c_2$ such that $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$.

Clearly $F(\alpha + c_1\beta) \subseteq F(\alpha, \beta)$.

And $\alpha + c_2\beta \in F(\alpha + c_2\beta)$ so $\alpha + c_1\beta - \alpha + c_2\beta = (c_1 - c_2)\beta$.

So $\beta = 1/(c_1 - c_2)\,(c_1 - c_2)\beta \in F(\alpha + c_1\beta)$ as $c_1 \neq c_2$. It follows that $\alpha \in F(\alpha + c_1\beta)$.

Thus, if any two elements are adjoined, we can express it as a simple extension.

Consider all simple extensions in E.

Since $[E:F] < \infty$, I can choose $\eta \in E$ such that $[F(\eta):F]$ is maximal with respect to all simple extensions.

Suppose it's not. Then $\exists\, r \in E$ such that $r \notin F(\eta)$.

Consider all $F(r, \eta)$. By the above claim $\exists\, \gamma \in E$ such that $F(r, \eta) = F(\gamma)$.

$[F(\gamma):F] = [F(\gamma):F(\eta)][F(\eta):F]$.

Since $r \notin F(\eta)$, then $[F(\gamma):F(\eta)] \neq 1$.

So $[F(\gamma):F] > [F(\eta):F]$.

Thus $E = F(\eta)$, a simple extension.

Corollary If E/F is an extension of fields and $F \lhd E$, then E is a simple extension.

Proof:
$F \lhd E \Rightarrow$ there are finitely many intermediate fields between F and E.
And by the above theorem, E is a simple extension.

Example $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Definition We say $\alpha \in F$ is *separable* if $\min(\alpha, F)$ is separable.

Corollary If $E = F(a_1, \ldots, a_n)$ such that $a_i \in E$ is separable $\forall\, i$, then $\exists\, \theta \in E$ such that $E = F(\theta)$.

Proof:
Let $p_i(x) = \min(\alpha_i, F)$,
Define $f(x) = p_1(x)p_2(x)\cdots p_n(x)$.
α_i is separable, thus $p_i(x)$ is separable for each i, so f is separable.
Let B be a splitting field for f over F.
So $F \lhd B$. So there are finitely many fields between F and E.
So $\exists\, \theta \in E$ such that $E = F(\theta)$.

Example $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Theorem** If $F \lhd E$ and $F \subseteq K \subseteq E$, then $F \lhd K \Leftrightarrow \mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$.

Proof:

Assume $F \lhd K$.

We know $\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$.

Let $\varphi \in \mathrm{Gal}(E/K)$ and $\sigma \in \mathrm{Gal}(E/F)$.

We need to show $\sigma^{-1}\varphi\sigma \in \mathrm{Gal}(E/K)$.

Clearly $\sigma^{-1}\varphi\sigma$ is an isomorphism. We only need to show $\sigma^{-1}\varphi\sigma$ fixes K.

Claim: $\sigma(K) = K$.

Since $F \lhd K$, K is a splitting field for some separable polynomial $f \in F[x]$.

Let $\alpha_1, \ldots, \alpha_n$ be roots of f so then we have $K = F(\alpha_1, \ldots, \alpha_n)$.

We know σ must permute $\alpha_1, \ldots, \alpha_n$.

Thus, $\sigma(\alpha_i) \in K$ and $\sigma(F) \subseteq K$, so $\sigma(K) = K$.

Thus $\forall\ c \in K$, $\sigma^{-1}\varphi\sigma(c) = \sigma^{-1}(\sigma(c))$ since φ fixes K and $\sigma(c) \in K$.

And $\sigma^{-1}(\sigma(c)) = c$ as σ is a bijection.

So $\sigma^{-1}\varphi\sigma$ fixes K, hence $\sigma^{-1}\varphi\sigma \in \mathrm{Gal}(E/K)$.

Conversely, assume $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$.

Claim: $\sigma(K) = K$.

Let $\varphi \in \mathrm{Gal}(E/K)$ and $\sigma \in \mathrm{Gal}(E/F)$.

$\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F) \Rightarrow \sigma^{-1}\varphi\sigma \in \mathrm{Gal}(E/K)$.

So $\forall\ c \in K$, $c = \sigma^{-1}\varphi\sigma(c) = \sigma^{-1}(\sigma(c))$.

Thus $\varphi\sigma(c) = \sigma(c)\ \forall\ \varphi \in \mathrm{Gal}(E/K)$.

Since σ is injective, then $\ker \sigma = \{0\}$, hence $K \cong \sigma(K)$.

Then $[K:F] = [\sigma(K):F]$.

But $[K:F] = [K:\sigma(K)]\,[\sigma(K):F]$. Thus $[K:\sigma(K)] = 1$.

So $K = \sigma(K)$.

Need to show $F \lhd K$.

Since $F \lhd E$, there are finitely many intermediate fields between F and E.

Since $F \subseteq K \subseteq E$, there are finitely many intermediate fields between F and K.

So $K = F(\alpha)$ for some $\alpha \in K$. Let $f = \min(\alpha, E)$.

Since $F \lhd E$, we know E contains all the roots of f and they are distinct.

So f is separable.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f.

Then $\exists\ \sigma_i \in \mathrm{Gal}(E/F)$ such that $\sigma_i(\alpha) = \alpha_i$.

So $\sigma_i(K) = K$ by the above claim.

Thus, $\alpha_1, \ldots, \alpha_n \in K$. Thus K is a splitting field for f.

$\therefore F \lhd K$.