Prop 24: K/F finite. Then,

K/F simple $\iff$ $\exists$ finitely many int. fields $F \subseteq E \subseteq K$.

Pf: $\Rightarrow$: done

$\Leftarrow$: If F finite, done (Prop 17), so assume F infinite.

If $K = F(\alpha, \beta)$, then finitely many int. fields $\Rightarrow$ $\exists c \neq c' \in F$ s.t. $F(\alpha + c\beta) = F(\alpha + c'\beta)$. But then

$\beta \in \frac{1}{c-c'}(\alpha + c\beta - \alpha - c'\beta) \in F(\alpha + c\beta)$, and so

$F(\alpha, \beta) = F(\alpha + c\beta)$ simple.

General K follows by induction. $\square$

E.g.: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Thm 25 (Primitive Element Theorem):

K/F finite, sep. $\Rightarrow$ K/F simple

In particular K/F finite, char 0 $\Rightarrow$ simple since irred. polys in char 0 are sep.

Pf: Let L be the Galois closure of K over F.

$\mathrm{Gal}(L/F)$ finite $\Rightarrow$ finitely many subgps. of $\mathrm{Gal}(L/F)$

$\Rightarrow$ finitely many int. fields $F \subseteq E \subseteq L$

$\Rightarrow$ finitely many int. fields $F \subseteq E \subseteq K$

$\Rightarrow$ K/F simple

Prop 24

---

§14.5 Cyclotomic Ext'ns & abelian ext'ns / $\mathbb{Q}$

Thm 26: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$

Pf: Let $\sigma_a(\zeta_n) = \zeta_n^a$ (and σ_a fixes $\mathbb{Q}$). Then,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_a \mid 0 \le a < n,\ \gcd(a,n)=1\}$$

Now, $(\mathbb{Z}/n\mathbb{Z})^\times = \{b \mid 0 \le b < n,\ \gcd(b,n)=1\}$, so the map $a \pmod n \mapsto \sigma_a$ is a bijection. It is a group homom. since $\sigma_a\sigma_b(\zeta_n) = \sigma_a(\zeta_n^b) = \zeta_n^{ab} = \sigma_{ab}(\zeta_n)$.

$\square$

Def: K/F is an abelian ext'n if K/F is Galois and $\mathrm{Gal}(K/F)$ is an abelian gp.

Cor: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian.

Cor 27 (Ridulous pf of the Chinese Remainder Thm, 孫子 (Sun Tzu), 3rd c. CE)
(not that one!)

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, p_i distinct. Then,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times$$

Pf: $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{a_1}}, \ldots, \zeta_{p_k^{a_k}}) = \underbrace{\mathbb{Q}(\zeta_{p_1^{a_1}}) \cdots \mathbb{Q}(\zeta_{p_k^{a_k}})}_{\text{composite}}$,

and since $p_i \neq p_j$ when $i \neq j$, $\mathbb{Q}(\zeta_{p_i^{a_i}}) \cap \mathbb{Q}(\zeta_{p_j^{a_j}}) = \mathbb{Q}$.
By Cor 22,

$$\begin{array}{ccccc} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \cong & \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) & \times \cdots \times & \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q}) \\ (\mathbb{Z}/n\mathbb{Z})^\times & \cong & (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times & \times \cdots \times & (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times \end{array}$$

Let's explore abelian ext'ns a bit more.

Subgps., quotients, direct prods. of abelian gps. are abelian so Galois subext'ns, composites of abelian ext'ns are abelian ext'ns

Open question: which finite groups are Galois groups?

Cor 28: Every abelian gp. is a Galois gp. over $\mathbb{Q}$ of a subfield of a cyclo. ext'n.

Pf: Let $G \cong \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k}$ $\qquad \mathbb{Z}_a := \mathbb{Z}/a\mathbb{Z}$

Dirichlet: $\forall m$, infinitely many primes $p \equiv 1 \pmod m$.

If $n = p_1 \cdots p_k$, p_i distinct, then by the Chinese Remainder Thm,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times$$

$$\cong \mathbb{Z}_{p_1 - 1} \times \cdots \times \mathbb{Z}_{p_k - 1}$$

By Dirichlet, can choose $p_1 \equiv 1 \pmod{n_1}, \cdots p_k \equiv 1 \bmod n_k$, so $n_i \mid p_i - 1$, so $\mathbb{Z}_{p_i - 1}$ has a subgp. H_i of order $\frac{p_i - 1}{n_i}$.

$H_i \triangleleft \mathbb{Z}_{p_i - 1}$, so $H_1 \times \cdots \times H_k \triangleleft (\mathbb{Z}/n\mathbb{Z})^\times$, and

$$(\mathbb{Z}/n\mathbb{Z})^\times / (H_1 \times \cdots \times H_k) \cong \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k} \cong G$$

is the Galois gp. of a subfield of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$. $\square$

Kronecker-Weber Thm: Let K be a finite abelian ext'n of $\mathbb{Q}$. Then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.

Pf: "Class field theory"

Example: (see other example in D&F for help w/ project)

$G := \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$, $\zeta := \zeta_5$

$$G = \{\sigma_1 : \zeta \mapsto \zeta,\ \sigma_2 : \zeta_5 \mapsto \zeta^2,\ \sigma_4 : \zeta_5 \mapsto \zeta^4 = \zeta^{-1},\ \sigma_3 : \zeta_5 \mapsto \zeta^3\}$$

Let $H = \{\sigma_1, \sigma_4\}$

Let $\alpha = \zeta + \sigma_4 \zeta = \zeta + \zeta^{-1}$

Then, $\sigma_4 \alpha = \zeta^{-1} + \zeta = \alpha$, so $\text{Fix } H = \mathbb{Q}(\alpha)$

What is this field?

$$\alpha^2 + \alpha - 1 = \zeta^2 + 2 + \zeta^3 + \zeta + \zeta^4 - 1 = 0$$

Quad. formula $\Rightarrow \alpha = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

In general, if p is an odd prime,

$$\begin{cases} \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p), & \text{if } p \equiv 1 \bmod 4 \\ \mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p), & \text{if } p \equiv 3 \bmod 4 \end{cases}$$