Recall: L/K is Galois if $|\operatorname{Aut}_K(L)| = [L:K]$. L/K is separable if $|\operatorname{Hom}_K(L,M)| = [L:K]$ for some field $M \supseteq K$.

L/K is Galois $\implies$ L/K is separable.

L/K is Galois $\iff$ $L =$ splitting field over K of some separable $f(X) \in K[X]$ $\iff$ L/K is separable and $\operatorname{Hom}_K(L,M) = \operatorname{Aut}_K(L), \forall M \supseteq L$.

If L/K is separable, let N be the Galois closure of L/K.

Define $G := \operatorname{Gal}(N/K), H := \operatorname{Gal}(N/L)$. Then, fields between L and K correspond to groups between G and H.

Given a separable extension L/K, we can write $L = L_n - L_{n-1} - \ldots - L_1 - K = L_0$ where there is no field between L_i and L_{i-1}. This is a powerful approach enabling one to study arbitrary L/K be induction, where the induction step addresses a *minimal extension*.

useful because: Galois groups (closures) of minimal separable extensions are massively restricted. Define such a Galois group to be a primitive permutation group.

Facts: If G is a primitive subgroup of S_n, then either

- $L \times L \times \ldots \times L \leq G \leq \operatorname{Aut}(L^k) = \operatorname{Aut}(L)^k \rtimes S_k$
- $n = p^k$, p prime, $(C_p)^k \leq G \leq \operatorname{AGL}_k(\mathbb{F}_p) = (\mathbb{F}_p)^k \rtimes \operatorname{GL}_k(\mathbb{F}_p)$ in usual action on $(\mathbb{F}_p)^k$.

Also: for 100% of positive integers n, the only primitive subgroups of S_n are A_n and S_n.

Also: if n is prime then every transitive subgroup of S_n is:

- S_n or A_n
- groups between $\mathbb{F}_n$ and $\operatorname{AGL}_1(\mathbb{F}_n)$.
- if $n = \frac{q^k-1}{q-1}$ with $k \geq 2$ and q prime, then $\operatorname{PGL}_k(\mathbb{F}_q) \leq G \leq \operatorname{P\Gamma L}_k(\mathbb{F}_q)$ acting on $P^{k-1}(\mathbb{F}_q)$.
- $n = 23$, M_{23} "Mathieu sporadic group"
- $n = 11$, M_{11} and $\operatorname{PSL}_2(\mathbb{F}_n)$.

Solvability by radicals:

Given $f(X) \in \mathbb{Q}[X]$, when can all roots of $f(X)$ be expressed in terms of nested radicals e.g. $\sqrt[3]{57\sqrt{31} - 1000\sqrt[5]{21+\sqrt{3}}}$

Concretely: an element $\alpha \in \mathbb{C}$ is expressible in terms of nested radicals iff $\alpha \in K_n$ for some field K_n $s.t.$ $K_n \supseteq K_{n-1} \supseteq \ldots \supseteq K_0 = \mathbb{Q}$ where $K_i = K_{i-1}(\alpha_i)$ with $d_i \in K_{i-1}$ for some positive integer d_i.

Theorem. *For any separable $f(X) \in \mathbb{Q}[X]$, $f(x)$ is "solvable by radicals" meaning that all its complex roots are expressible as above if and only if the Galois group G of $f(X)$ over $\mathbb{Q}$ is "solvable", i.e. $\exists G \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_k = 1$ where G_{i-1} is normal in G, and G_i/G_{i-1} is cyclic of prime order.*

Corollary. *All polynomials in $\mathbb{Q}[X]$ of degree ≤ 4 are solvable by radicals, but $\forall n \geq 5$, $\exists$ degree-n irreducible $f(x) \in \mathbb{Q}[x]$ which are NOT solvable (since $\exists$ polynomials with groups S_n, which is not solvable when $n \geq 5$)*

Key lemma

Lemma. *If a field K contains n n-th roots of unity, and L/K is Galois with $\mathrm{Gal}(L/K) \cong C_n$, then $L = K(\alpha)$ where $\alpha^n \in K$.*

Converse is easy: if K contains n-th roots of unity ζ and $L = K(\alpha)$ where $\mathrm{minpol}_K(\alpha) = x^n - c$, then L/K is Galois and $\mathrm{Gal}(L/K) \cong C_n$.

For: the roots of $x^n - c$ are $\alpha\phi^i$, $0 \leq i \leq n-1$, which are all in $K(\alpha) = L$. SO $L =$ splitting field of $x^n - c$ over $K \implies L/K$ is Galois of degree n, $\mathrm{Gal}(L/K) = \{\sigma_i i\alpha \mapsto \alpha\phi^i, i \in \mathbb{Z}/n\mathbb{Z}\} \implies \mathrm{Gal}(L/K) = \langle\sigma_1\rangle \cong C_n$