## Solvable Groups

Defn A finite group $G$ is solvable if there are subgroups

$$1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

s.t. for $i = 1, \ldots, n$ we have

(a) $G_i \trianglelefteq G_{i-1}$

(b) $[G_{i-1} : G_i]$ is prime. (so $G_i / G_{i-1} \cong C_p$)

e.g. · The chain $1 \leq A_3 \leq \Sigma_3$ exhibits $\Sigma_3$ as solvable.

· All finite abelian groups are solvable (soon).

· $A_n, \Sigma_n$ are nonsolvable for $n \geq 5$ (later).

Prop Every subgp of a finite solvable gp is solvable.

Pf Let $\{G_i\}_{i=0}^n$ be a chain witnessing solvability of $G$.

For $H \leq G$ define $H_i = H \cap G_i$ and note $H_0 = H \cap G_0 = H \cap G = H$

$H_n = H \cap 1 = 1$.

Let $\pi$ be the composite $H_{i-1} \hookrightarrow G_{i-1} \to G_{i-1}/G_i$.

Then $\ker \pi = \{ h \in H_{i-1} \mid hG_i = G_i \}$

$= H_{i-1} \cap G_i = (H \cap G_{i-1}) \cap G_i$

$= H \cap G_i = H_i \trianglelefteq H_{i-1}$.

By the first isomorphism thm,

$$H_{i-1}/H_i \cong \mathrm{im}(\pi) \leq G_{i-1}/G_i$$

so $H_{i-1}/H_i \cong 1$ or $C_p$.

$\Updownarrow$

$H_i = H_{i-1}$

So discarding duplicates we get a chain witnessing solvability of $H$. $\square$

Thm $H \trianglelefteq G$ finite. Then $G$ is solvable iff $H$ and $G/H$ are solvable.

Pf First suppose $G$ solvable. Then $H$ is solvable by the prop. Let $\pi: G \to G/H$ be the quotient hom. and set $\tilde{G}_i = \pi(G_i)$. Exc After discarding duplicates, $\tilde{G}_i$ give a chain witnessing solvability of $G/H$.

Now suppose $H$, $G/H$ solvable with

$$1 = H_\ell \leq H_{\ell-1} \leq \cdots \leq H_0 = H$$
$$1 = \tilde{G}_m \leq \cdots \leq \tilde{G}_0 = G/H$$

witnessing solvability. Then

$$1 = H_\ell \leq \cdots \leq H_0 = H \leq \pi^{-1}\tilde{G}_m \leq \cdots \leq \pi^{-1}\tilde{G}_0 = G$$

witnesses solvability of $G$. (check). $\square$

Prop Every finite abelian group $G$ is solvable.

Pf by strong induction on $n = |G|$. The case $n=1$ is trivial. Assume $G$ abelian of order $n > 1$ and the result is true $\forall$ abelian gps of order $< n$.

Let $p$ be a prime divisor of $n$. If $p = n$, $G \cong C_p$ solvable. If $p < n$, Cauchy's thm says there is $\langle g \rangle \leq G$, $\langle g \rangle \cong C_p$. This is solvable & normal since $G$ abelian. $|G/\langle g \rangle| < n$ so $G/\langle g \rangle$ solvable, so the prop follows from the theorem. $\square$.

e.g. $\mathbb{F}_p \cong T \trianglelefteq AGL_1(\mathbb{F}_p)$ with $AGL_1(\mathbb{F}_p)/T \cong \mathbb{F}_p^\times$. Both $\mathbb{F}_p, \mathbb{F}_p^\times$ abelian, hence solvable, so $AGL_1(\mathbb{F}_p)$ is solvable.

Rmk Feit-Thompson theorem: Every gp of odd order is solvable. Pf 255pp. $\square$

## Radical & Solvable Extensions

<u>Defn</u> A field extension $L/F$ is <u>radical</u> if there are fields
$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$ where for $i = 1, \ldots, n$ $\exists \gamma_i \in F_i$ s.t. $F_i = F_{i-1}(\gamma_i)$ and $\gamma_i^{m_i} \in F_{i-1}$ for some integer $m_i > 0$.

Note if $b_i = \gamma_i^{m_i}$ then $F_i = F_{i-1}(\sqrt[m_i]{b_i})$, i.e. radical extns arise by adjoining successive radicals.

<u>e.g.</u> $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{2+\sqrt{2}}) = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ witnesses $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ as a radical extn.

<u>Defn</u> A field extn $L/F$ is <u>solvable</u> (by radicals) if there is a field extn $M/L$ s.t. $M/F$ is radical.

<u>e.g.</u> The splitting field of $x^3 + x^2 - 2x + 1$ $/\mathbb{Q}$ is solvable but not radical.

<u>Defn</u> Suppose $K_1, K_2 \subseteq L$ subfields. The <u>compositum</u> $K_1K_2$ of $K_1$ & $K_2$ is the smallest subfield of $L$ containing $K_1, K_2$.

$$\begin{tikzcd}
 & L \arrow[d, dash] & \\
 & K_1K_2 & \\
K_1 \arrow[ur, dash] \arrow[uur, dash] & & K_2 \arrow[ul, dash] \arrow[uul, dash]
\end{tikzcd}$$

Existence: Fields are closed under arbitrary intersection.

<u>Prop</u> $M/L/F$ with $M/F$ Galois. Then the compositum of all conjugate fields of $L$ in $M$ is the Galois closure of $L/F$.

<u>Lemma</u> $M/L_1, L_2/F$ with $M/F$ Galois, then

$\cancel{\mathrm{Gal}(L_1L_2/F) = \mathrm{Gal}(L_1/F) \cap \mathrm{Gal}(L_2/F)}$

$\mathrm{Gal}(M/L_1L_2) = \mathrm{Gal}(M/L_1) \cap \mathrm{Gal}(M/L_2)$.

**Pf Lemma** If $\sigma$ fixes $L_1L_2$ then it fixes $L_1, L_2$ so

$$Gal(M/L_1L_2) \subseteq Gal(M/L_1) \cap Gal(M/L_2)$$

Suppose $\sigma \in Gal(M/L_1) \cap Gal(M/L_2)$. Suppose for $\Rightarrow\Leftarrow$ that $\sigma x \neq x$ for some $x \in L_1L_2$. Then $M^{\langle\sigma\rangle} \cap L_1L_2 \subsetneq L_1L_2$ with $L_1, L_2 \subseteq M^{\langle\sigma\rangle} \cap L_1L_2$, $\Rightarrow\Leftarrow$. □

**Pf Prop** Compositum of the $\sigma L$, $\sigma \in Gal(M/F)$ has Galois gp $\bigcap_{\sigma \in Gal(M/F)} \sigma\, Gal(M/L)\, \sigma^{-1}$, which is clearly normal in $Gal(M/F)$ so $\mathrm{Comp}_{\sigma \in Gal(M/F)}(\sigma L)/F$ is Galois and contains ~~all Galois conjugates of~~ $L$. Now check that any Galois extn containing $L$ contains all $\sigma L$ (exc). □

Properties of radical & solvable extns

**Lemma** (a) If $L/F$, $M/L$ are radical, so is $M/F$.

(b)
$$\begin{tikzcd} & L \arrow[d, dash] & \\ & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\ K_1 \arrow[dr, dash, "\text{radical}"'] & & K_2 \arrow[dl, dash] \\ & F & \end{tikzcd} \implies K_1K_2/K_2 \text{ radical}.$$

(c) $K_1/F, K_2/F$ radical $\implies K_1K_2/F$ radical

**Pf** (a) follows from defns & (c) $\Leftarrow$ (b).

For (b), the idea is to adjoin the same roots to $K_2$ (check details). □

**Thm** If $L/F$ is separable and radical, then the Galois closure of $L$ is also radical.

**Pf** The Galois conjugates of $L$ are radical. □

**Cor** Solvable extns of char 0 fields have solvable Galois closure.