Random Krull-Zassenhaus

Suppose $|G|$ divisible by p but $p \nmid |\mathrm{Aut}\, G|$

then $G \simeq C_p \times H$ for some H, $p \nmid |H|$

<u>Pf:</u> $P \in \mathrm{Syl}_p G$ <u>Claim</u>: P central. $x \in P$

$$P \to \mathrm{Aut}(G) \qquad \mathrm{inn}_x : G \to G$$
$$x \mapsto \mathrm{inn}_x \qquad g \mapsto xgx^{-1}$$

$\Rightarrow \mathrm{inn}_x = (e)$. $\Rightarrow x \in Z(G)$.

$P \subset Z(G)$.

$P \triangleleft G \Rightarrow$ Schur-Zassenhaus has a complement

$G = P \rtimes H$. H acts on P inner auts.

$P \subset Z(G) \Rightarrow G = P \times H$.

$\mathrm{Aut}\, G > \mathrm{Aut}\, P \times \mathrm{Aut}\, H > \mathrm{Aut}\, P$

$P \simeq C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_r}}$

$$\mathrm{Aut}\, P > \mathrm{Aut}\,(C_{p^{n_i}})$$
$$\| $$
$$(\mathbb{Z}/p^{n_i}\mathbb{Z})^* = p^{n_i} - p^{n_i - 1}$$

if $n_i > 1$ then $p \mid |\mathrm{Aut}\, P|$

$n_i = 1$ all i $\quad P \simeq (C_p)^r \simeq \mathbb{F}_p^r \quad \mathrm{Aut}(P) = GL_r(\mathbb{F}_p)$

$\cup$

$$U = \left\{ \begin{pmatrix} 1 & & a \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_{=T_a} \middle| a \in \mathbb{F}_p \right\}$$

$p \mid |\mathrm{Aut}\, GL_r(\mathbb{F}_p)|$ if $r > 1$.

$\mathbb{F}_p \simeq U < GL_r(\mathbb{F}_p)$

$T_a T_b = T_{a+b}$

Since $p \nmid |\mathrm{Aut}\, G| \Rightarrow P \simeq C_p$. $\square$

$$1 \to C_p \to P \to P/C_p \to 1$$

<u>Def</u> Let X be a set, an X-group is a group G together w/ a map $X \xrightarrow{\varphi} \mathrm{End}(G)$.

notation $x \cdot g \equiv \varphi(x)(g)$ $\quad x(gh) = x(g)x(h)$.

<u>Def</u> X-group homomorphisms $\left(\begin{array}{l} f : G \to H \text{ s.t. } \\ f(x \cdot g) = x \cdot f(g) \end{array} \right)$ gp. hom.

X-subgroup $H < G$ $\quad$ (i.e. H an X gp and inclusion $H \hookrightarrow G$ an X-hom).
$(H <_X G)$

<u>Lem</u> The first iso. thm (& rest) hold for X gps.

i.e. if $\varphi : G \longrightarrow H$ an X-gp hom then

$\ker\varphi$, $\operatorname{im}\varphi$ are X-groups.

and $\ker\varphi \trianglelefteq_X G$

normal subgp & an X-subgp.

get an iso

$$G/\ker\varphi \cong \operatorname{im}\varphi$$

in particular also have if $N \trianglelefteq_X G$ then G/N has an X-gp structure via

$$x.(gN) = (x.g)N$$

ex: $X = \underset{R}{\text{ring}}$ then R-modules are Abelian X-groups.

given R-modules M, N then X-homs are the same as R-homs

X subgps same as R-submodules.

$X = R$

X-gp = gp M together w/ arb. map $R \to \operatorname{End}_{gp} M$

R-module = Ab gp M " " $R \to \operatorname{End}_{Ab\,gp} M$

s.t. $(r_1 + r_2) \cdot m = r_1 m + r_2 m$

$(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$

$1 \cdot m = m$

Ex: $X = \emptyset$ gps = X gps

Ex: fix G consider $X = G$ via conjugation.

G-subgps = normal subgps.

$$H <_G G \iff H \lhd G$$
$$\Updownarrow$$
$$H \lhd_G G$$

---

from now on: $< \, = \, <_X$, $\lhd \, = \, \lhd_X$

Def an X-gp is simple (aka irreducible) if it has no proper $\boxed{\text{normal}}$ X-subgps and $\neq (e)$

Def A sequence of X-subgps of an X-gp G

$$\mathcal{H}: (e) = H_0 \lhd H_1 \lhd \cdots \lhd H_h = G$$

is called a <u>composition series</u> if H_i / H_{i-1} is simple all i.

(via corresp thm
$H_{i-1} \lhd H_i$ is max'l normal proper)

Def H_i / H_{i-1} are called the composition factors of G.

Q: How unique are comp. factors?

Def we say two comp. series

$$\mathcal{H}: (e) = H_0 \lhd H_1 \lhd \dots \lhd H_h = G$$

$$\mathcal{K}: (e) = K_0 \lhd \dots \lhd K_k = G$$

are equivalent ($\mathcal{H} \sim \mathcal{K}$) if $h = k$ & $\exists$ a permutation $\sigma \in S_h$

s.t. $H_i / H_{i-1} \cong K_{\sigma(i)} / K_{\sigma(i)-1}$

$G = C_2 \times C_3$

$$\mathcal{H} \quad (e) \lhd \overset{H_1}{C_2} \lhd \overset{H_2}{C_2 \times C_3}$$

$$\mathcal{K} \quad (e) \lhd \underset{K_1}{C_3} \lhd \underset{K_2}{C_2 \times C_3}$$

$H_1/H_0 \cong K_2/K_1$

$H_2/H_1 \cong K_1/K_0$

Def we say an X-gp G has finite length if it has a comp. series.

Def an X-gp G has infinite length if we can form a nonending seq.

$$(e) = H_0 \lhd H_1 \lhd H_2 \lhd \dots \quad \text{(non terminating)}$$

H_i / H_{i-1} simple.

Theorem (Jordan-Hölder)

If an X-gp G has finite length then any two comp. series for G are equivalent & G doesn't have infinite length.

Ex: if $X=\emptyset$

X-comp series = comp. series. (solvable $\Leftrightarrow$ comp series w/ cyclic factors)

if $X=G$

X-comp series = Chief series (solvable $\Leftrightarrow$ comp series w/ Abelian factors)

Pf Induct on length of $\mathcal{H}$ (h)

if $h=1$ then $\mathcal{H}: (e)=H_0 \triangleleft H_1 = G$

$\Rightarrow G = H_1/H_0$ simple. $\Rightarrow \mathcal{K}=\mathcal{H}$ ✓

induction step:

$$\mathcal{H}: \overbrace{(e)=H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft \overset{H}{\overset{\shortparallel}{H_{h-1}}}}^{\overline{\mathcal{H}}} \triangleleft H_h = G$$

$$\mathcal{K}: \underbrace{(e)=K_0 \triangleleft \cdots \triangleleft \underset{K}{\underset{\shortparallel}{K_{k-1}}}}_{\overline{\mathcal{K}}} \triangleleft K_k = G$$

Case 1: $H=K$

then by induction $\overline{\mathcal{H}} \sim \overline{\mathcal{K}}$

but $G/H = G/K$ simple.

Case 2: $H \neq K$

strategy: construct new series for H & K

$$\mathcal{U}: (e) = \overbrace{\overbrace{U_0 \lhd \cdots \lhd U_{u-2} = N}^{\bar{\bar{\mathcal{U}}}} \lhd H}^{\overline{\mathcal{U}}} \lhd G$$

$$\mathcal{V}: (e) = \underbrace{\overbrace{V_0 \lhd \cdots \lhd V_{v-2}}^{\bar{\bar{\mathcal{V}}}} = N \lhd K}_{\overline{\mathcal{V}}} \lhd G$$

if could do this then by induction

$\overline{\mathcal{U}} \sim \overline{\mathcal{H}}$ but then $G/H \cong G/H = G/H_{h-1}$

$\Rightarrow \mathcal{U} \sim \mathcal{H}$

Claim $\mathcal{U} \sim \mathcal{V}$