Semidirect products

Note: $k \in K \leq G$ and $H \trianglelefteq G \Rightarrow khk^{-1} \in H$

$h \mapsto khk^{-1}$ is an automorphism $\varphi_k : H \to H$

Def: Fix a homomorphism $K \to \operatorname{Aut} H$, $k \mapsto \varphi_k$. The semidirect product of H and K is

$H \rtimes K = (H \times K, \cdot)$ with $(h,k)\cdot(h',k') = (h\varphi_k(h'), kk')$

The point: $kh'k^{-1} = \varphi_k(h') \Rightarrow h(k\,h')k' = h\,\underbrace{k\,h'k^{-1}}_{\varphi_k(h')}\,k\,k'$.

Lemma: $H \trianglelefteq H \rtimes K$ and $khk^{-1} = \varphi_k(h)$ $\forall k \in K$ and $h \in H$. $\square$

E.g. $|G| = 21$ $\quad p = 7,\ m = 3 \Rightarrow s \mid 3$ and $s \equiv 1 \pmod 7 \Rightarrow s = 1$

$\Rightarrow$ Sylow 7-subgroup $H \trianglelefteq G$

$p = 3,\ m = 7 \Rightarrow s \mid 7$ and $s \equiv 1 \pmod 3 \Rightarrow s = \{1, 7\}$

$\Rightarrow$ Sylow 3-subgroup K might be normal in G or not.

$K \trianglelefteq G \Rightarrow G \cong C_3 \times C_7 \cong C_{21}$ as in $|G| = 15$ case.

$K \not\trianglelefteq G \Rightarrow G$ not abelian, but still $H \cap K = \{1\} \Rightarrow |HK| = |H|\cdot|K| = 7\cdot 3 = 21 = |G|$

$\Rightarrow G = HK$. $H \trianglelefteq G \Rightarrow G \cong H \rtimes K$, but for which $\varphi : K \to \operatorname{Aut} H$?
$k \mapsto \varphi_k$

$H = \{1, h, h^2, \ldots, h^6\}$. $\operatorname{Aut} H \cong C_6 \Rightarrow \varphi_k : x \mapsto x^a$ for $a \in \{2, 4\}$ since $\varphi_k(h)^3 = h^{a^3} = h$
$2^3 = 7+1,\ 4^3 = 63+1$

$\Rightarrow khk^{-1} = h^2$ or h^4.

But these yield isomorphic semidirect products under $k \mapsto k^2$.

$\therefore |G| = 21 \Rightarrow G \cong C_{21}$ or $G \cong C_7 \rtimes C_3$ (and there's only one such $\rtimes$)

Proofs of the Sylow thms

setup: p prime, $|G| = n = p^e m$, $p \nmid m$, $e \geq 1$

Sylow 1: $\exists\, H \leq G$ with $|H| = p^e$.

Lemma: $p \nmid \binom{n}{p^e} = \dfrac{n(n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots 1}$. ($n$ → m)

Pf: Given $1 \leq k \leq p^e - 1$, write $k = p^f l$ with $p \nmid l$. Then

$$\left.\begin{aligned} n-k &= p^e m - p^f l = p^f(p^{e-f}m - l) \\ p^e - k &= p^e - p^f l = p^f(p^{e-f} - l) \end{aligned}\right\} \Rightarrow \operatorname{ord}_p\left(\frac{n-k}{p^e-k}\right) = \operatorname{ord}_p\left(\frac{p^{e-f}m - l}{p^{e-f} - l}\right) = 0. \quad \square$$

Pf of Sylow 1: $G \curvearrowright \binom{G}{p^e}$ = union of orbits $\mathcal{O}$

$\Rightarrow \binom{G}{p^e} = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}|$

Lemma $\Rightarrow$ $\not\equiv 0 \pmod p$ $\Rightarrow$ $|\mathcal{O}| \not\equiv 0 \pmod p$ for some $\mathcal{O}$. Let $U \in \mathcal{O}$.

Then $|G_U| \cdot |\mathcal{O}| = |G| = p^e m \Rightarrow p^e \mid |G_U|$.

But $|G_U| \mid |U| = p^e$ by Prop p. 23. Set $H = G_U$. $\square$

Sylow 2: Fix $K \leq G$ with $p \mid |K|$. Sylow p-subgroup $H \leq G \Rightarrow$ Sylow p-subgroup $(gHg^{-1}) \cap K$.

Pf: $G \curvearrowright X = G/H$. $|X| = m \not\equiv 0 \pmod p \Rightarrow \exists$ K-orbit $\mathcal{O}$ with $p \nmid |\mathcal{O}|$.

$x \in \mathcal{O} \Rightarrow x = gH$ for some $g \in G$. $G_x = ?$ gHg^{-1} $\quad agH = gH \Leftrightarrow g^{-1}ag \in H \Leftrightarrow a \in gHg^{-1}$

$\Rightarrow K_x = (gHg^{-1}) \cap K$

$[K : (gHg^{-1}) \cap K] = [K : K_x] = |\mathcal{O}|$ prime to p.

$|gHg^{-1}| = p^e \Rightarrow (gHg^{-1}) \cap K$ is a p-group.

$\Rightarrow$ $|K| / |(gHg^{-1}) \cap K|$ has no p

$|(gHg^{-1}) \cap K|$ is all p (p-group)

$\Rightarrow (gHg^{-1}) \cap K \leq K$ is a Sylow p-subgroup. $\square$

Sylow 3: #Sylow p-subgroups of G divides m and $\equiv 1 \ (p)$.

Pf: $G \curvearrowright X$ transitive by Cor 2 of Sylow 2

$\Rightarrow |X| = [G : N]$ for $N = N_G(H)$, where $H \in X$ is arbitrary.

$H \leq N \Rightarrow [G : N] \mid [G : H] = m$. ✓

$H \curvearrowright X$. Q. When does H stabilize $H' \in X$?

A. $\Leftrightarrow hH'h^{-1} = H' \ \forall \ h \in H$

$\Leftrightarrow H \leq N_G(H')$.

But $H' \trianglelefteq N_G(H')$ is a normal Sylow p-subgroup of $N_G(H')$.

Since $H \leq N_G(H')$, it is also a Sylow p-subgroup.

Thus $H = H'$, since all Sylow p-subgroups are conjugate (Cor 2 of Sylow 2).

Conclusion: $H \curvearrowright X$ with only one orbit of size 1, and

$p \mid |\mathcal{O}| \ \forall$ other orbits $\mathcal{O} \neq \{H\}$

$\Rightarrow |X| \equiv 1 \ (p)$. $\square$