# Algebra I Lecture 11: More on $\rtimes$, finitely gen. abelian gps.

**Ex**: $p$ odd prime. Last day of new material before exam!

We ~~find~~ build 2 different non-abelian gps of order $p^3$.

1). $H = \mathbb{Z}_p \times \mathbb{Z}_p$, $K = \mathbb{Z}_p$.

~~Aut(H)~~ Think of $H$ as 2-dim$^{\underline{\text{al}}}$ vectorspace over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

By Lin. alg, $\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_p)$ (invertible matrices sending basis elts to $\binom{1}{0}, \binom{0}{1}$)

$|GL_2(\mathbb{F}_p)|$: $p^2-1$ choices ~~for~~ top row (avoid $(0,0)$)
$p^2-p$ choices bottom (avoid multiples of top row)

$\rightsquigarrow (p^2-1)(p^2-p)$ choices.

thus, $p \mid |\mathrm{Aut}(H)|$. Cauchy $\Rightarrow$ $H$ has an automorphism of order $p$.
(e.g.: $\begin{pmatrix}1&0\\1&1\end{pmatrix} \in GL_2(\mathbb{F}_p)$).

$\Rightarrow \exists$ non-trivial hom $\varphi: K \to \mathrm{Aut}(H)$. (send generator ~~to~~ of $K$ to this aut.).

and then $H \rtimes_\varphi K$ is non-ab of order $p^3$.

---

Explicitly: Write
$H = \langle a \rangle \times \langle b \rangle$ ~~(gps of order $p^2$ are abelian + recognition thm)~~
$K = \langle x \rangle$.

$\begin{pmatrix}1&0\\1&1\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$, $\begin{pmatrix}1&0\\1&1\end{pmatrix}\cdot\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$

~~K $\circlearrowleft$~~ $K \circlearrowleft H$ by $x \cdot a = ab$, $x \cdot b = b$ ~~(Stagger...)~~

gp. order $p^2$ ab

Then $G_1 = H \rtimes K \cong \langle x, a, b \mid x^p = a^p = b^p = 1,\ ab = ba,\ xax^{-1} = ab,\ xbx^{-1} = b \rangle$

This is the Heisenberg gp. over $\mathbb{Z}/p\mathbb{Z}$.

2) Take $H = \mathbb{Z}/p^2\mathbb{Z}$, $K = \mathbb{Z}/p$ (by pow)

$\mathrm{Aut}(H) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}_{p(p-1)}$ ← true for prime powers, if odd power $\Rightarrow \exists!$ subgp. of order $p$ in $\mathrm{Aut}(H)$

($p^2 - p$ rel. prime to $p$ in $1, \dots, p^2$)

So $\exists$ non-~~trivial~~ hom. $\varphi : K \to \mathrm{Aut}(H)$

$\rightsquigarrow$ ~~$G \cong H$~~ $G = H \rtimes_\varphi K$ non-ab. of order $p^3$.

Explicitly, If $H = \langle y \rangle$, $K = \langle x \rangle$, $x \cdot y = y^{p+1}$

$\boxed{\text{~~Fermat~~: Freshman Dream: order of aut } \leftrightarrow p+1 : \; p+1 \not\equiv 0 \bmod p^2,\ (p+1)^p \equiv p^p + 1 \equiv 1 \bmod p.}$

$G_2 \cong \langle x, y \mid x^p = y^{p^2} = 1,\ xyx^{-1} = y^{p+1} \rangle$.

This ~~has~~ has an elt of order $p^2$, & the Heisenberg does not;

~~Only~~ Only ~~one~~ (will return to this)

~~(by)~~ Lemma: If $K$ is cyclic, $H$ is any gp, $\varphi_1, \varphi_2 : K \hookrightarrow \mathrm{Aut}(H)$ are homs s.t. $\varphi_1(K), \varphi_2(K)$ conjugate then

$$H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K.$$

Similar to HW problem

$G_1, G_2$ only non-ab. ones.

~~This~~ Don't give rigorous pf for lack of time, similar to hw. problem you did (maybe follows)?

Thus, $G_1 \not\cong G_2$, Except if $p = 2$. then $G_1 \cong G_2 \cong D_8$.

Classification thm:

- $|G| = p \to$ cyclic
- $|G| = p^2 \to \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$ (using Fund. Th. of Ab. gps + gps of order $p^2$ are abelian)
- $|G| = pq$, $p < q$ (WLOG)
  $p \nmid q-1 \Rightarrow G$ cyclic, if $p \mid q-1 \to$ 2 gps: Cyclic + the non-ab. one [Class eq?] (we saw)

$|G| = p^3$ ~~$p \neq 2$~~ $\Rightarrow$ Proposition (too far a field, uses $p$-power map hom: $G \to G$)

$p \neq 2$: $|G| = p^3 \overset{\Rightarrow}{p \neq 2} \Rightarrow \exists H \leq G$, $|H| = p^2$, $K \leq G$ $|K| = p$ s.t. $H \cap K = 1$.

See Book!

Not on Comp Exam Syllabus!

Abelian: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

Non-abelian: 2 choices for $G$:

$\exists$ a subgp $H$ of order $p^2$ and it must be normal (index = smallest prime divisor of $|G|$.)

So $H \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Case 1): $\mathbb{Z}/p^2\mathbb{Z} \rightsquigarrow G \cong G_2$ (we saw).

Case 2): $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ $\quad \mathrm{Aut}(H) \cong GL_2(\mathbb{F}_p)$.

Sylow $p$-subgp. of $\mathrm{Aut}(H)$ has order $p$.

$\Rightarrow$ all subgps of order $p$ in $\mathrm{Aut}(H)$ are conjugate.

$\Rightarrow \exists !$ semi-direct product (by the lemma before).

$\Rightarrow$ 5 gps of size $p^3$.

N.B.: If $p = 2$, $G_1 \cong G_2$, but there is a new gp of quaternions, $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

$\boxed{p \nmid q : p \nmid (q-1) \to \text{cyclic}}$ (true? mention?)

$i^2 = j^2 = k^2 = -1$,

$ij = k$

$ji = -k$

$jk = i$ ---

Start here

Read also: $|G| = 12, 30$ in book

---

## Finitely Generated Abelian gps.

$G$ is finitely generated if $G = \langle g_1, \dots, g_n \rangle$.

If $G$ abelian, write additively. Let $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{n \text{ times}}$.

Lemma: An ab. gp. $G$ is f.g. iff $\exists$ a surj. hom. $\varphi: \mathbb{Z}^n \twoheadrightarrow G$

Pf: $\Leftarrow$: Given $\varphi$, set $\varphi(e_i) = g_i$ what else?
If $g \in G$, let $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n$ s.t. $\varphi(m) = g$.
(surjective)
Then $m = m_1 e_1 + \cdots + m_n e_n \Rightarrow g = \varphi(m) = m_1 g_1 + \cdots m_n g_n$
(std. basis vectors) $\Rightarrow g \in \langle g_1, \ldots, g_n \rangle$.

$\Rightarrow$: Given $g_1, \ldots, g_n$ generators,
define $\varphi$ by $\varphi(e_i) = g_i$.

Then $\varphi(m_1 e_1 + \cdots + m_n e_n) = m_1 g_1 + \cdots + m_n g_n$
Easy check: $\varphi$ is a hom. and its surjective.

Def: A gp. $\cong$ to $\mathbb{Z}^n$ is called a free abelian gp. of rank $n$.

Free ab. gps. are very similar to vector spaces, but with only integers allowed as scalars.

N.B: Finite gps. are finitely generated.

Fundamental Thm of F.g. Ab. Gps:

Let $G$ be a f.g. ab. gp. Then

1). $G \cong \mathbb{Z}^r \times \boxed{\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}}$ $\leftarrow$ torsion (saw in HW).

integers ~~$\forall$,~~ $r, n_1, \ldots, n_k$ s.t.

a). $r \geq 0$ $n_j \geq 2$ $\forall j$.

b). $n_{i+1} \mid n_i$, $1 \leq i \leq s-1$

invariant factors

2). The expression in (1) is unique (if it satisfies a), b).)

Pf: The proper place for this is module theory (Ch. 12).
(like vector spaces but weird!)