Last time: Given two groups $H, N$ and a homomorphism $\mu: H \to Aut(N)$ 20.1
constructed a new group $N \rtimes_\mu H$ so that
- $H, N$ are (isomorphic to) subgroups of $N \rtimes H$
- $N \triangleleft (N \rtimes H)$
- $\forall a \in h, \forall n \in N \quad ana^{-1} = (\mu(a))(n)$.

---

Definition Let $H$ be a subgroup of a group $G$. The normalizer of $H$ in $G$ is
$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$
One can check directly:
- $N_G(H)$ is a subgroup of $G$ [not hard; but see below].
- $H < N_G(H)$ (easy, since $\forall a \in H \quad aHa^{-1} \subseteq H$)
- $H \triangleleft N_G(H)$. (easy, since $\forall g \in N_G(H), \ gHg^{-1} = H$)

Another way to see that $N_G(H)$ is a subgroup of $G$:
Since $G$ acts on itself by conjugation, it acts on the set $\mathcal{P}(G)$ of all subsets of $G$
$$g \bullet S := c_g(S) = \{gsg^{-1} \mid s \in S\}$$
(recall: $c_g: G \to G, \ c_g(x) = gxg^{-1}$)

$$N_G(H) = \{g \in G \mid g \bullet H = H\} = Stab(H) \text{ for the action of } G \text{ on } \mathcal{P}(G).$$
Hence $N_G(H)$ has to be a subgroup.

---

Definition Let $G$ be a finite group and $p$ a prime with $p \mid |G|$.
Then $\exists! \, n, m \in \mathbb{N}$ st $|G| = p^n \cdot m$ and $\gcd(p, m) = 1$
A subgroup $P$ of $G$ is a Sylow $p$-subgroup if $|P| = p^n$
A subgroup $H$ of $G$ is a $p$-subgroup if $|H| = p^k$, $1 \le k \le n$.

Ex $G = S_3 \quad |G| = 3! = 6 \quad \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$ are Sylow 2-subgr
$\langle(123)\rangle$ is a Sylow 3-subgroup of $S_3$.

**Note:** A Sylow p-subgroup is a largest p-subgroup, in the sense that no p-subgroup can have more elements than a Sylow p-subgroup.

**Note:** Sylow p-subgroups are not unique.

**Theorem** (Sylow theorems #1, 2, 3) Let $G$ be a finite group, $p$ a prime with $p \mid |G|$.

1) If $p^k \mid |G|$ then there is a subgroup $H$ of $G$ with $|H| = p^k$. In particular p-Sylow subgroups exist.

2) Let $H < G$ be a p-subgroup, $P < G$ a Sylow p-subgroup. Then $\exists a \in G$ st $aHa^{-1} \leq P$.

In particular any two Sylow p-subgroups are conjugate.

3) Let $n_p$ = # of p-Sylow subgroups, let $P$ be a p-Sylow subgroup (which exists by (1)). Then
   - (i) $n_p \mid |G/P| = |G|/|P|$
   - (ii) $n_p \equiv 1 \mod p$
   - (iii) $n_p = |G| / |N_G(P)|$ where $N_G(P)$ is the normalizer of $P$ in $G$.

---

<no proof>

**Lemma 20.1** Suppose $p, q$ are two primes with $p > q$. Then

(i) If $q \nmid (p-1)$, then any group of order $pq$ is cyclic, ie isomorphic to $\mathbb{Z}_{pq}$

(ii) if $q \mid (p-1)$, then any group of order $pq$ is either cyclic or is a semi-direct product $\mathbb{Z}_p \rtimes_\mu \mathbb{Z}_q$ (for some homomorphism $\mu: \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$.)

**Proof** Let $G$ be a group of order $pq$, ie $|G| = pq$.

By Cauchy's theorem $G$ has elements of order $p$ and of order $q$
$\Rightarrow \exists$ subgroups $P, Q$ of $G$ with $|P| = p$, $|Q| = q$.
Since $P \cap Q$ is a subgroup of $P$ and of $Q$
$|P\cap Q| \mid p$ and $|P \cap Q| \mid q$. $\Rightarrow |P \cap Q| \mid \gcd(p,q) = 1$
$\Rightarrow P \cap Q = \{e\}$

$n_p \mid |G|/|P| = pq/p = q$ by one of Sylow's Theorems $\Rightarrow n_p = q$ or $1$
Since $n_p \equiv 1 \mod p$ and since $q < p$, $n_p = 1$.
Hence $P$ is a <u>unique</u> $p$-Sylow subgroup of $G$
On the other hand, $\forall g \in G$ $gPg^{-1}$ is also a $p$-Sylow subgroup.
$\Rightarrow gPg^{-1} = P \quad \forall g \in G$
$\Rightarrow P \lhd G$

Consider $f: P \times Q \to G \quad f(a,b) = ab$.
<u>Claim:</u> $f$ is a bijection.
<u>Proof of claim</u> Since $|G| = pq = |P \times Q|$ enough to show that $f$ is injective.
Suppose $a_1 b_1 = a_2 b_2$. Then $a_2^{-1} a_1 = b_2 b_1^{-1}$.
Since $a_2^{-1}a_1 \in P$, $b_2 b_1^{-1} \in Q$, $a_2^{-1}a_1 \in P \cap Q = \{e\}$. $\Rightarrow a_2 = a_1$
$\Rightarrow b_2 = b_1$. $\square$

Recall from lecture 18: If $G$ is a group, $H, N < G$, $N \lhd G$ and $f: N \times H \to G$, $f(a,b) = ab$ is a bijection, then $G \simeq N \rtimes H$
Hence in our case $G \simeq \mathbb{Z}_p \rtimes_\mu \mathbb{Z}_q$ for some $\mu: \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$

<u>Exercise</u> For any $n > 1$, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to the group
$\mathbb{Z}_n^\times = \{[k] \in \mathbb{Z}_n \mid [k][\ell] = [1]$ for some $[\ell] \in \mathbb{Z}_n\}$
$\mathbb{Z}_n^\times$ is a group under multiplication, $e_{\mathbb{Z}_n^\times} = [1]$

Back to $G = \mathbb{Z}_p \rtimes_\mu \mathbb{Z}_q$. The multiplication of $G$ depends on $\mu$. Since $\ker\mu < \mathbb{Z}_q$, $|\ker \mu| \mid q = |\mathbb{Z}_q|$
Since $q$ is prime, $\ker\mu = \{[0]\}$ or $\ker \mu = \mathbb{Z}_q$.

If $\ker\mu = \mathbb{Z}_q$, then $\mu(a) = id \in Aut(\mathbb{Z}_p) \quad \forall a \in \mathbb{Z}_q$

And then $a \cdot x = x \quad \forall a \in \mathbb{Z}_q,\ x \in \mathbb{Z}_p$

$\Rightarrow \quad \mathbb{Z}_p \rtimes \mathbb{Z}_q \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}.$

Otherwise $\ker\mu = \{[0]\}$ and $\mu: \mathbb{Z}_q \to Aut(\mathbb{Z}_p) = \mathbb{Z}_p^\times$

is injective. $\mathbb{Z}_q \simeq \mu(\mathbb{Z}_q) < \mathbb{Z}_p^\times$

$\mathbb{Z}_p^\times = \{[1], \dots [p-1]\}$ as a set, since $\forall k \in \mathbb{N},\ 1 \le k < p,\ \gcd(k,p) = 1$

$\Rightarrow \exists x, y \in \mathbb{Z}$ s.t. $kx + yp = 1 \Rightarrow [k][p] = [1]$ in $\mathbb{Z}_p \Rightarrow [k] \in \mathbb{Z}_p^\times$

In particular $|\mathbb{Z}_p^\times| = p-1.$

Therefore, if $q \nmid (p-1)$, $\mu: \mathbb{Z}_q \to Aut(\mathbb{Z}_p)$ is not injective

$\Rightarrow \ker\mu = \mathbb{Z}_q$ and $G \simeq \mathbb{Z}_{pq}$.

$\square$

---

Next time: back to rings