Theorem 1. Every $G$-set is a disjoint union of "transitive $G$-sets."

2. If $X$ is a transitive $G$-set and $x \in X$, then $X \cong G/\text{stab}_G(x)$. (So $|X| = |G|/|\text{stab}_G(x)|$)

Theorem. If $X$ is a $G$-set and $x_i$ are representatives of the orbits, then

$$|X| = \sum_i \frac{|G|}{|\text{stab}_G(x_i)|}$$

Example. If $G$ is a $p$-group, the Centre of $G$ is not empty.

**THE SYLOW THEOREMS.**

Let $G$ be a $p$-group, $p$ prime, $p < m$. \ $\text{Syl}_p(G) = \{P \leq G : |P| = p^m \}$

are "Sylow $p$-subgroups of $G". A "p-subgroup" in general is any subgroup of $G$ of order a power of $p$.

Sylow 1 \ $\text{Syl}_p(G) \neq \emptyset$. Also see comment at bottom.

Proof. By induction on $|G|$, if $G$ has a normal subgroup of order $p^m$ (or $p^n$) or if $G$ has a subgroup of order divisible by $p^m$, we are done. The existence of one of the said types follows from the class equation:

$$\text{The centre of } G \text{, the centralizer of } y \text{ in } G$$

\[ \gamma \text{ Either both are divisible by } p, \]
\[ |G| = |\mathbb{Z}(G)| + \sum \left( G : C_G(y_i) \right) \]

Either both are divisible by \( p \), or neither. Do 2nd case first.

Where \( y_i \) are representatives from the non-central conjugacy classes of \( G \).

\[ \square \]

**Theorem.** If \( G \) is a finite Abelian group of order divisible by a prime \( p \), then \( G \) contains an element of order \( p \). "Cauchy's Theorem" D&F pp 102

**Proof.** Enough to find an element of order divisible by \( p \): if \( p \) is of order \( p \cdot n \), \( 2^n \) would be of order \( p \).

Pick \( x \in G, x \neq 1 \). If \( p \mid |x| \), we're done. Otherwise \( p \mid |G/<x>| \), so by induction, \( \exists y \in G \) s.t. \( |G/<x>| = p \) in \( G/<x> \). So \( y^p \in <x> \) i.e., \( y^p = x^k \) for some \( k \). Write \( |y| = pk + r \) with \( 0 \leq r < p \), get \( e = y^{pk+r} = x^{kr}y^r \) so \( y^r \in <x> \Rightarrow r = 0 \), as \( |G| = p \).

So the order of \( y \) is divisible by \( p \). \( \square \)

(A) would have been better to state and prove:

claim: if \( \phi : G \to H \) is a morphism \& \( y \in G \), then \( |\phi(y)| \mid |y| \).

Proof. If \( |\phi(y)| = n \), \( |y| = m \), \( m = nq + r \). Then \( e = \phi(y^n) = \phi(y^{nq})\phi(y^r) = (\phi(y))^q \phi(y)^r = \phi(y)^r \).

So \( r = 0 \).

**Theorem.** 1. Sylow p-groups always exist: \( \text{Syl}_p(G) \neq \emptyset \).

2. Every p-group is contained in a Sylow-p group.
3. All Sylow-$p$ subgroups of $G$ are conjugate, and

$$N_p(G) = \{ Syl_p(G) \} \equiv 1 \mod p \quad \& \quad |N_p(G)| \mid |G|$$

**Groups of order 15.**

$P_5$ is normal in $G$, $P_3$ is

normal in $G$. Any $y \in P_3$ commutes

with $P_5$ [otherwise $\exists y \mid \text{Aut} P_5 \neq 1$],

$P_5 = \{ y \mid \text{otherwise} \} \mid \text{Aut} P_5 = 1 \}$

**Preliminary Lemma.**

A group of

order $p$ is $\mathbb{Z}/p$.

Aside. $N_p \mid |G| \Rightarrow n_p \mid n_1 \quad \& \quad n_1 = 1 \mod p \Rightarrow \frac{n_1}{n_p} = 1 \mod \frac{p}{q-1}$

$(\text{Aside. Aut} \left( \mathbb{Z}/p \right) = \left( \mathbb{Z}/p \right)^* \quad \text{so } |\text{Aut} \left( \mathbb{Z}/p \right)| = \phi(p))$

$x = x^y = y^x \quad \text{for generators } x \in P_5, y \in P_3.$

**Aside.** If $G = \left< a, b \right>$, $G_1 \cap G_2 = \left< c \right>$, $[G_1, G_2] = \left< c \right>$, then

$G = G_1 \times G_2$

**Aside.** $\mathbb{Z}/p \times \mathbb{Z}/q = \mathbb{Z}/pq$

This also works for order $pq$, $p \neq q$ primes, $pq-1$.  

**Groups of order 21.** $P_7$ is normal, $P_3$ might not be.

$P_3$ may act on $P_7$. If $P_7 = \langle x \rangle$, $P_3 = \langle y \rangle$, we

have $x^y = x^q$ or $x^y = x^q$.  

**Aside.** Aut($\mathbb{Z}/7$) is cyclic; $A = \{ 1, 2, 3, 4, 5 \}$

$\text{Ded. What does this mean?}$

This also works for order $pq$, $p \neq q$ primes, $pq-1$. 

Also did the “extension lemma”.

**Lemma.** If $P \leq \text{Syl}_p(G)$ & $H \triangleleft \text{N}_p(G)$ is a $p$-group,

then $H \leq P$.

2. If $P \leq \text{Syl}_p(G), \langle x \rangle = \langle p \rangle$, $x \in \text{N}_p(G)$, then $x \in P$.

Reformulation: $P \leq \text{Syl}_p(G), |H| = p^\beta \Rightarrow H \triangleleft \text{N}_p(G)$

**Stronger Sylow 1.** If $p^\beta \mid |G|$, then $G$

has a subgroup of order $p^\beta$.  

11-1100 Page 3
Proof: Let \( \mathcal{X} = \{ \mathcal{S} \subseteq G : |S| = p^k \} \), and write

\[ |\mathcal{X}| = p^{k+1} m \]

with maximal \( \chi \). By counting and binomial nonsense, \( p^k |\chi| \) yet \( p^{k+1} |\chi| \).

\( G \) acts on \( \mathcal{X} \) by translations, so there must be \( s_0 \in \mathcal{X} \) such that \( p^{k+1} |G : s_0|\), hence \( p^B |H = \text{stab}_G(s_0)| \). Yet if \( x \in s_0 \) then \( g \mapsto gx \) is an injection \( H \to s_0 \), so \( |H| \leq |s_0| = p^B \), so \( |H| = p^B \).