Content:

Theorem	Cauchy's Theorem, Let G be a finite group whose order is divisible by p, a prime. Then G has an element of order p.
Definition	p-group
Theorem	If G is a p-group, then $Z(G) \neq \{e\}$.
Definition	Conjugate
Theorem	All groups of order p^2 are Abelian.
Theorem	Let G be an Abelian group. G is simple if and only if $\|G\| = p$, p a prime.
Theorem	There are no non-abelian p-groups that are simple.
Theorem	A_n is simple for $n \geq 5$.
Lemma	All 3-cycles in A_5 are conjugate.

Exam 2 will be moved to November 9.

Theorem Cauchy's Theorem

Let G be a finite group whose order is divisible by p, a prime. Then G has an element of order p.

Proof:

We already proved the result for Abelian groups.

Let $|G| = pm$, p, a prime, $m \in \mathbb{Z}$. We will induct on m.

$m = 1\surd$ (i.e. If $|G| = p$, then we already know G has an element of order p.)

We state our induction hypothesis as "Assume any group of order pk where $k < m$ has an element of order p, (p prime)."

Assume G is non-abelian.

Let $x \in G$ such that $x \notin Z(G)$

(We know we can do this as G is not Abelian).

Then $\exists\ g \in G$ such that $gxg^{-1} \neq x$, hence $|x^G| = [G:C_G(x)] \geq 2$.

So $C_G(x)$ is a proper subgroup of G.

If $p|\ |C_G(x)|$, then by our induction hypothesis, $C_G(x)$ contains an element of order p.

And since $C_G(x) \leq G$, then G has an element of order p.

So we may assume $p \nmid |C_G(x_i)|$ for all non-central x_i.

But, for all i, $|G| = [G:C_G(x_i)] \bullet |C_G(x_i)|$.

Since $p \mid |G|$ and $p \nmid |C_G(x_i)|$, then, by Euclid's lemma, $p \mid [G:C_G(x_i)]$ for all non-central i.

$\therefore\ p \mid \sum_i [G : C_G(x_i)]$.

And since $|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$ and $p \mid |G|$, then $p \mid |Z(G)|$.

Since $Z(G)$ is Abelian, then $Z(G)$ has an element of order p. Hence G has an element of order p.

Example Prove all groups of order 42 are not simple.

Proof:
By Cauchy's theorem, G has an element of order 7, call it a. Let $H = \langle a \rangle$.
Then $[G{:}H] = 6$. And $42 \nmid 6!$.
So G is not simple by the Index Factorial theorem.

Note: This is HW #98 done, just generalize.

Example If G is a group, $|G| = 6$, then $G \cong \mathbb{Z}_6$ or $G \cong S_3$.

Proof (Alternate to proof given in text, mentioned in Lecture Notes 10/7/09): By Cauchy's theorem, G contains an element of order 2 and an element of order 3.
Let $a, b \in G$ such that $\circ(a) = 2$ and $\circ(b) = 3$.
We can show e, a, b, b^2, ab, ab^2 are all distinct elements of G.
Consider ba.

$ba = e \Rightarrow b = a^{-1} = a \quad \Rightarrow\Leftarrow$
$ba = a \Rightarrow b = e \quad \Rightarrow\Leftarrow$
$ba = b \Rightarrow a = e \quad \Rightarrow\Leftarrow$
$ba = b^2 \Rightarrow a = b \quad \Rightarrow\Leftarrow$

So either $ba = ab$ or $ba = ab^2$.

If $ba = ab$, then it can be easily checked that is Abelian.
Hence $\circ(ab) = 6$, by Prop 2.82 (If $a, b \in G$ are commuting elements of orders m, n respectively, and $(m, n) = 1$, then $\circ(ab) = mn$.)
$\therefore\ |G| = |\langle ab \rangle| = 6$.
$\therefore\ G \cong \mathbb{Z}_6$.

If $ba = ab^2$, then $a^{-1}ba = b^2 = aba$ (since $\circ(a) = 2$).
$D_6 = \langle x, y \mid x^2 = 1 = y^3, xy\,x = y^{-1} = y^2 \rangle$.
Define $\phi: D_6 \to G$ by $\phi(x) = a$, $\phi(y) = b$.
Checking well-defined comes down to checking that the relations are preserved.

$\therefore\ G \cong D_6 = S_3$.

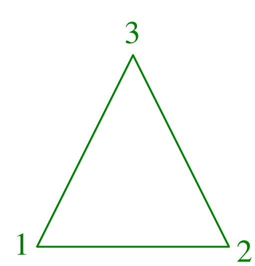
Aside Here is why $D_6 = S_3$. Consider the triangle whose vertices are numbered.

We know $D_6 = \{r_0, r_1, r_3, f_1, f_2, f_3\}$.

$r_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$



Definition Let G be a finite group of order p^k where p is prime, then G is called a *p-group*.

Theorem If G is a p-group, then $Z(G) \neq \{e\}$.

Proof:

By the class equation, $|G| = |Z(G)| + \sum_i \underbrace{[G:G_{x_i}]}$ where one x_i is chosen from each orbit with more than 1 element.

Can't be 1 as $|\mathcal{O}(x)| = [G:G_x]$ and each orbit has more than 1 element.

By Lagrange's theorem, $[G:G_{x_i}] \mid |G|$ for each i.

Since each $[G:G_{x_i}] \neq 1$, then $p \mid [G:G_{x_i}]$, so $p \mid \sum_i [G:G_{x_i}]$.

Since G is a p-group, then $p \mid |G|$, so $p \mid |Z(G)| + \sum_i [G:G_{x_i}]$,

hence $p \mid |Z(G)|$. $\therefore$ $Z(G) \neq \{e\}$.

Theorem All groups of order p^2 are Abelian.

Proof:

$Z(G) \leq G$, so $|Z(G)| = 1, p$, or p^2.

By the previous theorem, $|Z(G)| \neq 1$.

If $|Z(G)| = p$, then $|G/Z(G)| = p^2/p = p$, hence $G/Z(G)$ is cyclic.

And by Exercise 2.69, G is Abelian. But if $|Z(G)| = p$, then $G \neq Z(G)$.

$\therefore$ G cannot be Abelian, a contradiction, hence $|Z(G)| \neq p$.

If $|Z(G)| = p^2$, then $|G/Z(G)| = p^2/p^2 = 1$, hence $Z(G) = G$. $\therefore$ G is Abelian.

Theorem Let G be an Abelian group. G is simple if and only if $|G| = p$, p a prime.

Proof (from lecture notes):

Any subgroup is normal.

The only groups with only trivial subgroups are the $\mathbb{Z}_p$'s.

Proof (from text):

If G is finite of prime order p, then G has no subgroups H other than $\{1\}$ and G, otherwise Lagrange's theorem would show that $|H|$ is a divisor of p. $\therefore$ G is simple.

Conversely, assume G is simple. Since G is Abelian, every subgroup is normal, and so G has no subgroups other than $\{1\}$ and G. Choose $x \in G$ with $x \neq 1$. Since $\langle x \rangle$ is a subgroup, we have $\langle x \rangle = G$. If x has infinite order, then all the powers of x are distinct, and so $\langle x^2 \rangle \leq \langle x \rangle$ is a forbidden proper subgroup of $\langle x \rangle$, a contradiction. $\therefore$ Every $x \in G$ has finite order. If $\circ(x) = m < \infty$ and if m is composite, say $m = kn$, then $\langle x^k \rangle$ is a proper nontrivial subgroup of $\langle x \rangle$, a contradiction. $\therefore$ $G = \langle x \rangle$ has prime order.

Theorem There are no non-abelian p-groups that are simple.

Proof:
Let G be a non-abelian p-group. Then $Z(G) \neq G$.
By previous theorem, $Z(G) \neq \{e\}$.
Since the center of a group is always a normal subgroup of the group, then $Z(G)$ is a non-trivial normal subgroup of G.

Theorem A_n is simple for $n \geq 5$.

To prove this we need the next 2 lemmas.

Question Let G act on itself by conjugation. Let $H \leq G$. Then H can act on itself by conjugation. Let $x, y \in H$. If $y \in \mathcal{O}(x)$ for G, then is $y \in \mathcal{O}(x)$ for H?
That is, if $y = gxg^{-1}$ for some $g \in G$ is $y = hxh^{-1}$ for some $h \in H$?
Not necessarily. See #89 (iii).
(There are two conjugacy classes of 5-cycles in A_5, each of which has 12 elements, while there is only one conjugacy class of 5-cycles in S_5.)
So, we don't get the following lemma for free, we have to prove it.

Lemma All 3-cycles in A_5 are conjugate.

Proof:
Let $\alpha = (123) \in S_5$. By Thm 2.9 (All permutations γ and σ in S_n have the same cycle structure iff $\exists\ \alpha \in S_n$ with $\sigma = \alpha\gamma\alpha^{-1}$.) we know all 3-cycles are conjugate to (123) in S_5. $\therefore\ |\alpha^{S_5}| = (5 \cdot 4 \cdot 3)/3 = 20$.

And by Thm 2.98 ($|\mathcal{O}(x)| = [G:G_x]$), $|\alpha^{S_5}| = \dfrac{|S_5|}{|C_{S_5}(\alpha)|} = \dfrac{120}{|C_{S_5}(\alpha)|}$.

$\therefore\ |C_{S_5}(\alpha)| = 6$.
We can easily find these 6 elements.
It's a subgroup, so it must contain (1).
Since $\alpha\alpha\alpha^{-1} = \alpha$, then $\alpha \in C_{S_5}(\alpha)$. So $\alpha^{-1} = (132) \in C_{S_5}(\alpha)$.
Any cycle γ, disjoint to α will give us $\gamma\alpha\gamma^{-1} = \alpha$, so $(45) \in C_{S_5}(\alpha)$.
Since $C_{S_5}(\alpha)$ is a group, then (123)(45) and (132)(45) are in $C_{S_5}(\alpha)$.

$$C_{S_5}(\alpha) = \{\underbrace{(1)}_{\text{even}}, \underbrace{(123)}_{\text{even}}, \underbrace{(132)}_{\text{even}}, \underbrace{(45)}_{\text{odd}}, \underbrace{(123)(45)}_{\text{odd}}, \underbrace{(132)(45)}_{\text{odd}}\}$$

$C_{A_5}(\alpha) = A_5 \cap C_{S_5}(\alpha)$, so $C_{A_5}(\alpha) = \{(1), (123), (132)\}$,
hence $|C_{A_5}(\alpha)| = 3$.

Since $\left|\alpha^{A_5}\right| = \dfrac{|A_5|}{|C_{A_5}(\alpha)|}$, and $|A_5| = (1/2)5! = 60$, then $\left|\alpha^{A_5}\right| = 20$.

Thus $\left|\alpha^{S_5}\right| = \left|\alpha^{A_5}\right|$, which implies all 3-cycles are conjugate to (123) in A_5.
Note: This lemma can be generalized from A_5 to A_n for $n \leq 5$.

Lemma Each element in A_n, for $n \geq 3$ is either a 3-cycle or a product of 3-cycles.

Proof:
Let $\alpha \in A_n$, $n \geq 3$. Then $\alpha = \tau_1\tau_2\cdots\tau_{2k-1}\tau_{2k}$ for some positive integer k.
We may assume that adjacent τ's are distinct, otherwise their product is (1). As the transposition can be grouped in pairs, then we only need to prove that a product of 2 transpositions is a 3-cycle. So consider τ and τ'.
If $\tau = (i\ j)$ and $\tau' = (j\ k)$, then $\tau\tau' = (\ i\ j\ k)$.
If $\tau = (i\ j)$ and $\tau' = (k\ n)$, then $\tau\tau' = (i\ j)(j\ k)(j\ k)(k\ n) = (i\ j\ k)(j\ k\ n)$.
$\therefore$ α is either a 3-cycle or a product of 3-cycles.

On Monday we will prove A_5 is simple, and A_6 is simple. We will also discuss finite Abelian groups. You can read about it in 5.1 if you want.