Content:

Proposition	Let $G = \langle a \rangle$ and $\circ(a) = n$. Then a^k is a generator of $G \Leftrightarrow \gcd(k, n) = 1$.
Proposition	All subgroups of a cyclic group are cyclic.
Proposition	If G is a cycle group, then G has a *unique* subgroup of order d for all divisors d of n.
Claim	Let G be a group and $H \leq G$, $a, b \in G$. Define the relation $a \sim b$ if $a^{-1}b \in H$. This is an equivalence relation.
Definition	Left Coset
Lemma	Since $a^{-1}b \in H$ is an equivalence relation with equivalence classes aH, we get the following: Let G be a group, $H \leq G$, $a, b \in G$. 1) $b \in aH \Leftrightarrow a^{-1}b \in H$. 2) $aH = bH \Leftrightarrow a^{-1}b \in H$. 3) $aH = H \Leftrightarrow a \in H$. 4) $aH \cap bH \neq \varnothing \Leftrightarrow aH = bH$.
Definition	Alternating Group
Theorem	**Lagrange's** Let $H \leq G$, G a finite group, then $\lvert H \rvert \mid \lvert G \rvert$.
Definition	Index
Corollaries	of Lagrange Let G be a finite group. **1)** $\circ(a) \mid \lvert G \rvert$, $\forall\, a \in G$. **2)** $a^{\lvert G \rvert} = 1$. **3)** Every group of order p (prime) is cyclic. **4)** Every group of order 4 is Abelian.
Theorem	(Fermat) Let p be prime and $a \in \mathbb{Z}$, then $a^p \equiv a \bmod p$.
Theorem	(Euler) If $\gcd(r, m) = 1$, then $r^{\phi(m)} \equiv 1 \bmod m$, where $\phi(m)$ = the number of integers k with $1 \leq k \leq m$ and $\gcd(k, m) = 1$.
Theorem	(Wilson's) An integer p is prime iff $(p-1)! \equiv -1 \bmod p$.

From Monday, **Lemma** G is a group and $a \in G$. If $\circ(a) = n < \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ where $e, a, a^2, \ldots, a^{n-1}$ are n distinct elements in G.
The order of a group = the number of elements in the group, $|G|$. So the lemma gives us that $\circ(a) = |\langle a \rangle|$. We will prove this on Wednesday.

Wednesday,
Theorem/Lemma (take your pick) restated:

If $\circ(a) = n < \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ where $e, a, a^2, \ldots, a^{n-1}$ are all disjoint.

Proof:
Let $H = \{e, a, a^2, \ldots, a^{n-1}\}$. We will show $H = \langle a \rangle$.
$\subseteq$: Recall that $\langle a \rangle$ is the smallest subgroup of G containing a.
$H \subseteq \langle a \rangle$ as $\langle a \rangle$ must contain every integral power of a, and every element of H is an integral power of a.
$\supseteq$: Let $a^k \in \langle a \rangle$ for some $k \in \mathbb{Z}$. By the division algorithm, $k = nq + r$, hence $a^k = a^{nq+r} = a^{nq}\, a^r = a^r \in H$, where $n = \circ(a)$ and $0 \leq r < n$.
$\therefore\ \langle a \rangle \subseteq H$.

Distinct elements: Assume $a^i = a^j$, $i, j \in \{1, 2, \ldots, n-1\}$.

Then
$$a^i \bullet (a^j)^{-1} = a^j \bullet (a^j)^{-1}$$
$$a^i \bullet a^{-j} = e$$
$$a^{i-j} = e$$

$\therefore\ i - j \in \{0, 1, 2, \ldots, n-1\}\ \therefore\ i - j < n$.
Since $\circ(a) = n$, then $i - j = 0$, hence $i = j$.

Example $\mathbb{Z}_{12}$ $= \langle [1] \rangle = \{ [1]n \mid n \in \mathbb{Z}\} = \{[0], [1], [2], \ldots, [11]\}$
$= \langle [5] \rangle = \{[5]n \mid n \in Z\} = \{[5], [10], [3], [8], [1], \ldots, [0]\}$
$= \langle [7] \rangle = \{[7]n \mid n \in Z\} = \{[7], [2], [9], [4], [11]\ldots, [0]\}$
$= \langle [11] \rangle = \{[11]n \mid n \in Z\} = \{[11], [10], [9], [8], \ldots, [0]\}$

Proposition Let $G = \langle a \rangle$ and $\circ(a) = n$. Then a^k is a generator of $G \Leftrightarrow \gcd(k, n) = 1$.
Proof:
Since $|G| = n$, then

$$\begin{aligned} & G = \langle a^k \rangle \\ \Leftrightarrow \quad & \circ(a^k) = n \quad \text{(by lemma at top of page)} \\ \Leftrightarrow \quad & \frac{n}{\gcd(n,k)} = n \quad \text{(by gcd theorem given 9/14/09)} \\ \Leftrightarrow \quad & \gcd(n,k) = 1. \end{aligned}$$

Example Find all subgroups of $\mathbb{Z}_{12}$.
1) $\langle [0] \rangle = \{[0]\}$,
2) $\langle [1] \rangle = \{[0], [1], [2], \ldots, [11]\} = \mathbb{Z}_{12}$,
3) $\langle [2] \rangle = \{[2], [4], [6], [8], [10], [0]\} = \langle [10] \rangle$,
4) $\langle [3] \rangle = \{[3], [6], [9], [0]\} = \langle [9] \rangle$,
5) $\langle [4] \rangle = \{[4], [8], [0]\} = \langle [8] \rangle$,
6) $\langle [6] \rangle = \{[6], [0]\}$,
7) $\langle [5] \rangle = \mathbb{Z}_{12}$, 8) $\langle [7] \rangle = \mathbb{Z}_{12}$, 9) $\langle [11] \rangle = \mathbb{Z}_{12}$.

Proposition All subgroups of a cyclic group are cyclic.
Proof: Homework, #34.

Proposition If G is a cycle group, then G has a *unique* subgroup of order d for all divisors d of n.
Proof: Homework, #35.

Let G be a group and $H \leq G$, $a, b \in G$. Define the relation $a \sim b$ if $a^{-1}b \in H$.
Claim: This is an equivalence relation.
Proof:
Reflexivity: Since $a^{-1}a = 1_G = 1_H \in H$, then $a \sim a$.
Symmetry: Since $H \leq G$, then $a^{-1}b \in H$ implies that $(a^{-1}b)^{-1} = b^{-1}a \in H$.
$\therefore a \sim b \Rightarrow b \sim a$.
Transitivity: Suppose $a \sim b \Rightarrow b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$,
then $(a^{-1}b)(b^{-1}c) = a^{-1}(b \bullet b^{-1})c = a^{-1}c \in H$.
$\therefore$ If $a \sim b \Rightarrow b \sim c$, then $a \sim c$.
$\therefore a \sim b$ is an equivalency relation.

Question What do the equivalence classes look like?
$\forall\, a, b \in G, a^{-1}b \in H \Rightarrow a^{-1}b = h$ for some $h \in H$.
$\therefore \qquad b = ah$

Definition Let $H \leq G$. The *left coset* of a in G is $aH = \{ah \mid h \in H\}$.

Note: The set of cosets are the equivalence classes from above.

Example $Q = (\pm 1, \pm i, \pm j, \pm k\}$.
Let $H = \{\pm 1\}$, then
$1H = H = -1H$.
$iH = \{\pm i\} = -iH$.
$jH = \{\pm j\} = -jH$.
$kH = \{\pm k\} = -kH$.

These cosets are mutually disjoint and cover all of Q.

Example Let group $G = \mathbb{R}$, $H = \mathbb{Z}$.
$0.5 + \mathbb{Z} = 1.5 + \mathbb{Z}$.
What can a complete, non-redundant set of representatives come from?
$[0, 1)$.

Example Let group $G = S_3$, $H = \{(1), (12)\}$.
$(13)H = \{(13), (123)\} \neq \{(13), (132)\} = H(13)$.
So left cosets are not always equal to right cosets, even though there is the same number of each of them for any group.

Lemma Since $a^{-1}b \in H$ is an equivalence relation with equivalence classes aH, we get the following:
Let G be a group, $H \leq G$, $a, b \in G$.
1) $b \in aH \Leftrightarrow a^{-1}b \in H$.
($\Leftarrow$: $a^{-1}b \in H \Rightarrow aa^{-1}b = b = ah$ where $h \in H$, hence $b \in aH$.)
2) $aH = bH \Leftrightarrow a^{-1}b \in H$.
($\Leftarrow$: $(a^{-1}b)^{-1} = b^{-1}a \in H \Rightarrow bb^{-1}a = a = bh$ where $h \in H$, hence $a \in bH$.)
3) $aH = H \Leftrightarrow a \in H$.
($\Rightarrow$: Since if $aH = H$, then $ah \in H$ and $ahh^{-1} = a \in H$.)
4) $aH \cap bH \neq \varnothing \Leftrightarrow aH = bH$.
($ah \in aH \cap bH \Rightarrow ah \in bH \Rightarrow a \in bH \Rightarrow a^{-1}b \in H \Rightarrow aH = bH$.)

Throwing in groups means we now get the following:
1) $aH \leq G \Leftrightarrow a \in H$.
(Since $aH \leq G$, then $ah \in aH \Rightarrow (ah)^{-1} = h^{-1}a^{-1} \in aH \Rightarrow a^{-1} \in H$
$\Rightarrow a \in H$.)
2) $|aH| = |H|$.
(We can show there is a bijection ϕ: $H \rightarrow aH$. Let $\phi(h) = ah$. To show 1-1, suppose $\phi(h) = \phi(g)$, then $ah = ag$. Since $a, h, g \in G$ then cancellation holds and $h = g$. To show onto, let $y \in aH$, then $a^{-1}y \in H$, hence $\exists\ h \in H$ such that $\phi(h) = y$.)

Definition The *alternating group* A_n is the set of all even permutations in S_n.

$A_n \trianglelefteq S_n$.

Proof:

By definition $A_n \subseteq S_n$. Now we apply the subgroup test.

Let $\alpha, \beta \in A_n$ where $\alpha = \tau_1\tau_2\cdots\tau_{2k}$ and $\beta = \gamma_1\gamma_2\cdots\gamma_{2j}$ are products of transpositions, $k, j \in \mathbb{Z}$. Then $\alpha\beta^{-1} = \tau_1\tau_2\cdots\tau_{2k}\,\gamma_{2j}^{-1}\cdots\gamma_2^{-1}\gamma_1^{-1}$, which is an even product of transpositions. Hence $\alpha\beta^{-1} \in A_n$. $\therefore$ $A_n \trianglelefteq S_n$.

Question How many distinct cosets are there? 2, even permutations and odd

Let $\alpha \in S_n - A_n$. Thus, α is odd, hence $(12)\alpha$ is even.
$\therefore$ $(12)\alpha \in A_n$. Since $(12)\alpha = (12)^{-1}\alpha$, then we can apply property (1), $b \in aH \Leftrightarrow a^{-1}b \in H$ to get $\alpha \in (12)A_n$. So $S_n = A_n \cup (12)A_n$.

Thus $|S_n| = |A_n \cup (12)A_n|$
$= |A_n| \cup |(12)A_n|$ (Since A_n and $(12)A_n$ are disjoint).
$= 2\,|A_n|$.

So $(1/2)|S_n| = |A_n|$.

Theorem **Lagrange's Theorem**

Let $H \trianglelefteq G$, G a finite group, then $|H| \,\big|\, |G|$.

Proof:

Let $a_1H, a_2H, \ldots, a_nH$ be a list of all distinct cosets.

Then $G = \bigcup_{i=1}^{n} a_iH$ since $\forall\ g \in G$, $g \in gH = a_iH$ for some i.

And since $\forall\ a, b \in G$, $aH \cap bH \neq \varnothing \Leftrightarrow aH = bH$, we have that the cosets partition G into pairwise disjoint subsets.

Thus, $|G| = \sum_{i=1}^{n} |a_iH| = n|H|$, hence $|H| \,\big|\, |G|$ as desired.

Definition The *index* of H in G, denoted $[G:H]$ is the number of distinct left cosets of H in G.

The index $[G:H]$ is the number n in the formula $|G| = n|H|$ used in the proof of Lagrange, thus $|G| = [G:H] \cdot |H|$.

Corollaries of Lagrange

Let G be a finite group.

1) $\circ(a) \mid |G|$, $\forall\ a \in G$.

Proof: $\circ(a) = |\langle a \rangle|$ by previous lemma.
$|\langle a \rangle| \mid |G|$ by Lagrange's Theorem.

2) $a^{|G|} = 1$.

Proof: By (1), $\circ(a) \mid |G|$. By Theorem 2.24, $a^{|G|} = 1$.

3) Let p be a prime. Then every group of order p is cyclic.

Proof: Let $a \in G$, $a \neq 1$, $\circ(a) = d$, $|G| = p$, p a prime integer. Since $\circ(a) \mid |G|$, then $d \mid p$.
We have proven previously that $\circ(a) = |\langle a \rangle|$, hence $|\langle a \rangle| = p$.
Since $\langle a \rangle \leq G$ and $|\langle a \rangle| = |G|$, then $\langle a \rangle = G$.

4) Every group of order 4 is Abelian.

Proof: Let G be a group of order 4.
If G is cyclic, then we're done (since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$).
Assume G is not cyclic and let $x \in G$, $x \neq 1$.
Then $\circ(x) \mid |G|$ by (1), so $\circ(x) \mid 4$.
This implies that $\circ(x) \in \{1, 2, 4\}$.
But $\circ(x) \neq 4$, as $4 = \circ(x) = |\langle x \rangle| = |G| \Rightarrow \langle x \rangle = G$, which contradicts our assumption. And $\circ(x) \neq 1$, by assumption. $\therefore$ $\circ(x) = 2$. $\therefore$ $x^2 = e$.
We now show this implies G is Abelian.
Let $a, b \in G$, then $ab \in G$ and $e = (ab)^2 = (ab)(ab) = a(ba)b$.
Thus $a^{-1}b^{-1} = a^{-1}eb^{-1} = a^{-1}a(ba)bb^{-1} = ba$.
Since $a^2 = e \Rightarrow a = a^{-1}$, then we have $a^{-1}b^{-1} = ab = ba$.
$\therefore$ G is Abelian.

Klein 4 Group

There are only 2 groups of order 4, the Klein 4 Group and the cyclic $\mathbb{Z}_4$.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Number Theory Corollaries

$U(\mathbb{Z}_m) = \{[r] \mid \gcd(r, m) = 1\}$. This is a group with respect to multiplication.
Can use $ra + mb = 1$ to find inverses. If p is prime, then $|U(\mathbb{Z}_p)| = p - 1$.
$\mathbb{Z}_p = \{[0], [1], [2], \ldots, [p-1]\}$. Proof is on p. 70.

Theorem (Fermat)
Let p be prime and $a \in \mathbb{Z}$, then $a^p \equiv a \bmod p$.

Proof:
$a^p \equiv a \pmod p \Leftrightarrow [a]^p = [a]$ in $U(\mathbb{Z}_p)$. $[a]^{p-1} = [1]$ since $|U(\mathbb{Z}_p)| = p - 1$.
$\therefore$ $[a]^p = [a]$.

Theorem (Euler)

If gcd $(r, m) = 1$, then $r^{\phi(m)} \equiv 1 \bmod m$, where
$\phi(m)$ = the number of integers k with $1 \le k \le m$ and $\gcd(k, m) = 1$.

Proof:
Suppose gcd $(r, m) = 1$. Since $U(\mathbb{Z}_m) = \{[r] \mid \gcd(r, m) = 1\}$, then
$|U(\mathbb{Z}_m)| = \phi(m)$.
$\therefore\ [r]^{\phi(m)} = [1]$ since $a^{|G|} = 1$.
This is equivalent to $r^{\phi(m)} \equiv 1 \bmod m$.

Theorem (Wilson's)
An integer p is prime iff $(p - 1)! \equiv -1 \bmod p$.

Proof:
$\Rightarrow$: Let p be a prime number. We want to show $[(p - 1)!] = [-1]$ in $\mathbb{Z}_p$.
We know $[(p - 1)!] = [2][3]\cdots[p - 1]$ in $U(\mathbb{Z}_p)$.
If an element is not its own inverse, it will cancel with its inverse in this product. The remaining factors will each have order 2.
Let $[a] \in U(\mathbb{Z}_p)$ where $[a] \ne 1$ and $[a]^2 = [1]$.
Then $p \mid a^2 - 1 \Rightarrow p \mid (a - 1)(a + 1) \Rightarrow p \mid a - 1$ or $p \mid a + 1$.
Since $[a] \ne [1]$, then $[a] = [-1]$. $\therefore\ [(p - 1)!] = [-1]$ as desired.

$\Leftarrow$: We'll prove the contrapositive. Assume m is composite.
Then $\exists\ a, b \in \mathbb{Z}$ such that $m = ab$ and $1 < a \le b < m$.
If $a < b$, then $m = ab$ is a divisor of $(m - 1)!$, and so $(m - 1)! \equiv 0 \bmod m$.
If $a = b$, then $m = a^2$. If $a = 2$, then $(a^2 - 1)! = 3! = 6 \equiv 2 \bmod 4$ and $\sim(2 \equiv -1 \bmod 4)$.
If $2 < a$, then $2a < a^2$, and so a and $2a$ are factors of $(a^2 - 1)!$; thus, $(a^2 - 1)! \equiv 0 \bmod a^2$.
$\therefore\ \sim[(m - 1)! \equiv -1 \bmod m]$.

Hand in #35 Monday.

On Monday, we will cover 2.5 and 2.6 jointly. We will start with
$G/H = \{aH \mid a \in G\}$
$(aH) * (bH) = abH$ Is this well-defined?
Yes, if it has normality.