MATH 110B - GROUP THEORY

MATTHEW GHERMAN

These notes are based on Hungerford, *Abstract Algebra* 3rd edition.

Contents

1. Groups

1.1. Definition of a group.

Definition 1.1. A *group* is a non-empty set G closed under a binary operation $\cdot$ that satisfies the following three axioms.

(1) (Associativity) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(2) (Identity) There is an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
(3) (Inverses) For each $a \in G$, there is some $b \in G$ such that $a \cdot b = b \cdot a = e$.

Definition 1.2. A group is *abelian* if the binary operation is commutative. In other words, $a \cdot b = b \cdot a$ for all $a, b \in G$.

Example 1.1. Every ring under addition is an abelian group. For instance, $(\mathbb{Z}, +)$ or $(\mathbb{Q}, +)$. However, $(\mathbb{Z}, \cdot)$ is not a group since there is no multiplicative inverse to $\frac{1}{2}$. We can make $(\mathbb{Q}, \cdot)$ into a group by removing zero.

Example 1.2. Let R be a ring. Recall that a unit in R is an element that has a multiplicative inverse. The set of units $R^\times$ of R is a group under multiplication.

The quintessential example is $(\mathbb{Z}/n\mathbb{Z})^\times$. From Math 110A, we know that an equivalence class $\overline{a}$ is invertible in $\mathbb{Z}/n\mathbb{Z}$ if and only if a and n are relatively prime as integers. Thus the number of elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ is the Euler totient function $\varphi(n)$.

The multiplication table for $(\mathbb{Z}/8\mathbb{Z})^\times$ is the following.

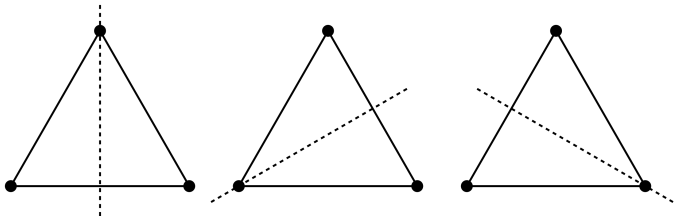
$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

We find that each non-identity element is its own inverse. Further, the symmetry along the left to right diagonal reveals that $(\mathbb{Z}/8\mathbb{Z})^\times$ is an abelian group.

Since each element has an inverse, each row and column of a group multiplication table will contain one and only one copy of each element of the group. The group multiplication table is much like a Sudoku puzzle.

Example 1.3. Let $GL_n(F)$ be invertible $n \times n$ matrices with coefficients in a field F. We can likewise classify $GL_n(F)$ by the $n \times n$ matrices A with $\det(A) \neq 0$. The common choices for F are $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}/p\mathbb{Z}$ for p a prime integer. Except for $n = 1$, these are non-abelian groups.

Example 1.4. Many groups arise as symmetries of shapes. Take an equilateral triangle with labeled vertices 1, 2, and 3. We can reflect the triangle about any axis through one of the vertices.



Likewise, we can rotate by an angle of $\frac{2\pi}{3}$ counterclockwise. The set of these symmetries form a group under composition called a *dihedral group*. We can replace the equilateral triangle with any regular n-gon to obtain a dihedral group denoted D_n. Let r represent rotation by $\frac{2\pi}{3}$ and s represent a reflection. The elements of D_3 are $\{e, r, r^2, s, sr, sr^2\}$. This is another example of a non-abelian group since the element rs is not the same as sr.

Example 1.5. Let $X_n = \{1, 2, \ldots, n\}$. The set S_n of bijections of X_n under composition is a group called the *symmetric group* on n elements. For $n \geq 3$, S_n will be non-abelian.

As an example, take $n = 3$. The permutation

$$1 \to 2$$
$$2 \to 3$$
$$3 \to 1$$

is denoted (123). Each number is sent to the number on its right while the rightmost number is sent to the first. Another permutation is (12). Reading left to right,

$$1 \to 2$$
$$2 \to 1$$
$$3 \to 3.$$

The set S_3 is $\{e, (12), (13), (24), (123), (132)\}$ where e is the identity element that keeps each number fixed. We compose permutations as functions compose or, in other words, we read right to left. For example, (123)(12) is the permutation

$$1 \to 2 \to 3$$
$$2 \to 1 \to 2$$
$$3 \to 3 \to 1$$

so $(123)(12) = (13)$. The permutation (12)(123) is

$$1 \to 2 \to 1$$
$$2 \to 3 \to 3$$
$$3 \to 1 \to 2$$

so $(12)(123) = (23)$.

With some more machinery, we will show that S_3 is the same as the dihedral group of the equilateral triangle. For $i, j, k \in \{1, 2, 3\}$, an element of the form (ijk) is a rotation while an element of the form (ij) is a reflection about the axis through vertex k. For larger n, however, the group S_n is much larger than D_n.

End of lecture 1

1.2. **Basic properties of groups.**

Proposition 1.1. Let G be a group and $a, b, c \in G$.

(1) G has a unique identity element.
(2) If $ab = ac$ or $ba = ca$, then $b = c$.
(3) Each element of G has a unique inverse.

Proof. (1) Let e and e' be two elements such that $ae = ea = a$ and $ae' = e'a = a$ for all $a \in G$. Then $e = ee' = e'$ so there is exactly one identity element.
(2) Let $ab = ac$. Multiply both sides by a^{-1} on the left to obtain $a^{-1}(ab) = a^{-1}(ac)$. By associativity, $(a^{-1}a)b = (a^{-1}a)c$ or $eb = ec$. We conclude that $b = c$. The other claim can be shown via right multiplication.
(3) Suppose d and d' are inverse of a. Then $ad = e = ad'$. By (2), $d = d'$ as desired.

□

The result of Proposition 1.1 allows us to denote the unique inverse of $a \in G$ by a^{-1}.

Corollary 1.1. Let G be a group with $a, b \in G$.

(1) $(ab)^{-1} = b^{-1}a^{-1}$
(2) $(a^{-1})^{-1} = a$

Proof. (1) We want to show $b^{-1}a^{-1}$ is the inverse of ab. By associativity,

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b \\ &= b^{-1}eb \\ &= b^{-1}b \\ &= e.\end{aligned}$$

A similar argument can be made to show $(ab)(b^{-1}a^{-1}) = e$. The uniqueness of the inverse proves $(ab)^{-1} = b^{-1}a^{-1}$.
(2) We want to show that a is the inverse of a^{-1}. We have

$$\begin{aligned}aa^{-1} &= e \\ a^{-1}a &= e\end{aligned}$$

so a is the inverse of a^{-1}.

□

For a positive integer n and $a \in G$, we will denote by a^n the product of n copies of a. We will denote a^{-n} to be the product of n copies of a^{-1}. For convenience, we may write $a^0 = e$.

Remark 1.1. For a non-abelian group G, note that $(ab)^n$ might not be equal to $a^n b^n$.

The following exponent rules do hold, however.

Proposition 1.2. Let G be a group with $a \in G$. For all $m, n \in \mathbb{Z}$,

$$\begin{aligned}a^m a^n &= a^{m+n} \\ (a^m)^m &= a^{mn}.\end{aligned}$$

Proof. We will prove the result for $n \geq 0$ inductively. The other cases will be left as an exercise.

As a base case, let $n = 0$. Then $a^m a^0 = a^m = a^{m+0}$. As the inductive step, assume that $a^m a^k = a^{m+k}$ for all $0 \leq k \leq n-1$. We want to show, $a^m a^n = a^{m+n}$. Via associativity and the

inductive hypothesis,

$$\begin{aligned} a^m a^n &= (a^m a^{n-1})a \\ &= a^{m+n-1}a \\ &= a^{m+n}. \end{aligned}$$

As a base case, let $n = 0$. Then $(a^m)^0 = e = a^{m\cdot 0}$. Assume that $(a^m)^k = a^{mk}$ for all $0 \leq k \leq n-1$. By the inductive hypothesis and the above result,

$$\begin{aligned} (a^m)^n &= (a^m)^{n-1}a^m \\ &= a^{m(n-1)}a^m \\ &= a^{m(n-1)+m} \\ &= a^{mn}. \end{aligned}$$

□

Remark 1.2. Let G be an abelian group with $a \in G$. The group operation will sometimes be denoted by $+$ instead of $\cdot$. In these cases, the identity element will be denoted 0 and the inverse of $a \in G$ will be $-a$. Further, na is the sum of n copies of a and $-na$ is the sum of n copies of a^{-1}. We will call G an *additive group*.

Definition 1.3. Let G be a group with $a \in G$. If $a^M = e$ for a positive integer M, then the *order* of a is the smallest positive integer k for which $a^k = e$. If no such M exists, then a is said to have *infinite order*. We denote by $|a|$ the order of a.

Definition 1.4. The size of a group G will also be called the *order* of G. We will use the notation $|G|$ to denote the order of the group G.

The connection between order of elements and order of groups will be explored next chapter.

Example 1.6. What is the order of the element (123) in S_3? The element $(123)^2$ is

$$\begin{aligned} 1 &\to 2 \to 3 \\ 2 &\to 3 \to 1 \\ 3 &\to 1 \to 2 \end{aligned}$$

so $(123)^2 = (132)$. Then $(123)^3 = (123)(123)^2 = (123)(132)$ is

$$\begin{aligned} 1 &\to 3 \to 1 \\ 2 &\to 1 \to 2 \\ 3 &\to 2 \to 3. \end{aligned}$$

We conclude that $(123)^3 = e$ and $|(123)| = 3$. Further, we can show $|(132)| = 3$ and $|(ij)| = 2$ for any distinct $i, j \in \{1, 2, 3\}$.

In general, the order of S_n is $n!$ since there are $n!$ different ways of permuting a set of size n.

Example 1.7. In the additive group $\mathbb{Z}/12\mathbb{Z}$, the element $\overline{8}$ has order 3.

$$\begin{aligned} \overline{8} + \overline{8} &= \overline{4} \\ \overline{8} + \overline{8} + \overline{8} &= \overline{8} + \overline{4} = \overline{0} \end{aligned}$$

Proposition 1.3. Let G be a group with $a \in G$.

(1) If $a^i = a^j$ with $i \neq j$, then a has finite order.
(2) If a has infinite order, then the elements a^k for $k \in \mathbb{Z}$ are distinct.

Proof. (1) Assume $a^i = a^j$ for $i \neq j$. Without loss of generality, assume that $i > j$. Multiply both sides by a^{-j}. Then $a^{i-j} = e$ and a has finite order.
(2) The statement is the contrapositive of (1) and, thus, equivalent.

□

We can reduce many group theory problems to matters of elementary number theory via the following result.

Proposition 1.4. Let G be a group with $a \in G$ an element of finite order n.
(1) $a^k = e$ if and only if $n|k$
(2) $a^i = a^j$ if and only if $i \equiv j \pmod{n}$
(3) If $n = td$ with $d \geq 1$, then a^t has order d

Proof. (1) ($\Rightarrow$) Suppose $a^k = e$. By the division algorithm, $k = nq + r$ with $0 \leq r < n$. Thus

$$\begin{aligned} a^k &= a^{nq+r} \\ &= (a^n)^q a^r \\ &= e^q a^r \\ &= a^r. \end{aligned}$$

Since $a^k = e$, we conclude $a^r = e$. The order of a is n so n is the smallest positive integer for which $a^n = e$. Since r is strictly less than n, we have $r = 0$.
($\Leftarrow$) Assume $k = nt$. Then $a^k = a^{nt} = (a^n)^t = e^t = e$. End of lecture 2
(2) Equivalenty, we will prove that $a^{i-j} = e$ if and only if $i - j \equiv 0 \pmod{n}$. By (1), $a^{i-j} = e$ if and only if n divides $i - j$. This is equivalent to $i \equiv j \pmod{n}$.
(3) We have $(a^t)^d = a^{td} = a^n = e$. We want to prove that d is the smallest such positive exponent. Let k be a positive integer such that $(a^t)^k = e$. Then $a^{tk} = e$ and n divides tk by (1). We can write $tk = nr = (td)r$ for some integer r. We have $k = dr$. Since k and d are positive and $d|k$, we have $d \leq k$.

□

Lemma 1.1. Let G be a group. Let $a, b \in G$ be elements of finite order such that $ab = ba$. If $\gcd(|a|, |b|) = 1$, then $|ab| = |a||b|$.

Proof. Let $m = |a|$, $n = |b|$, and $k = |ab|$. We have

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e_G^n e_G^m = e_G$$

so k divides mn by Proposition 1.4(1).
Next,

$$e_G = e_G^n = ((ab)^k)^n = (ab)^{kn} = a^{kn}b^{kn} = a^{kn}(b^n)^k = a^{kn}e_G = a^{kn}$$

so Proposition 1.4(1) implies that m divides kn. Since m and n are relatively prime, m divides k. The same argument with m and n swapped proves that n divides k as well. Since m and n are relatively prime, mn divides k and $k = mn$. □

Lemma 1.2. Let G be a group. Let $a, b \in G$ be elements of finite order such that $ab = ba$. Let $m = |a|$ and $n = |b|$. Then $|ab|$ divides $\operatorname{lcm}(m, n)$.

Proof. We have $\ell = \operatorname{lcm}(m, n)$ where $\ell = rm$ and $\ell = sn$ for some integers $r, s \in \mathbb{Z}$. Since a and b commute,

$$(ab)^\ell = a^\ell b^\ell = a^{rm}b^{sn} = (a^m)^r(b^n)^s = e_G.$$

Therefore, $|ab|$ divides ℓ by Proposition 1.4(1). □

Note that the $|ab|$ is not necessarily $\operatorname{lcm}(|a|, |b|)$ when $b = a^{-1}$ for instance.

1.3. **Subgroups.**

Definition 1.5. A non-empty subset H of G is a *subgroup* of G if the following hold.

(1) (Closure under group operation) For each $a, b \in H$, $ab \in H$.
(2) (Closure under inverse) For each $a \in H$, $a^{-1} \in H$.

Every non-trivial group G has at least two subgroups: the trivial subgroup $\{e\}$ and G itself. All other groups are called *proper* subgroups.

Proposition 1.5. Let H be a finite non-empty subset of a group G. If H is closed under the group operation in G, then H is a subgroup of G.

Proof. We only need to check that H is closed under inverse. If $a \in H$, then closure under the group operation implies $a^k \in H$ for all positive integers k. Since H is finite, a is an element of finite order. Let $|a| = n$. If $n = 1$, then $a = e$ and we are done. Assume $n > 1$. Since $n - 1 \equiv -1 \pmod{n}$, Proposition 1.4 implies that $a^{n-1} = a^{-1}$. □

Example 1.8. The subset

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\}$$

is a subgroup of $GL_2(\mathbb{R})$. We have

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \in H$$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in H$$

Example 1.9. Recall the dihedral group D_3 has elements $\{e, r, r^2, s, sr, sr^2\}$ where r represents a rotation of an equilateral triangle by an angle of $\frac{2\pi}{3}$ counterclockwise and s represents reflection about an axis through a vertex of the equilateral triangle. The subset $H = \{e, r, r^2\}$ is the subgroup of rotations of D_3. Likewise, $K = \{e, sr^i\}$ is a subgroup of D_3 containing one of the reflections for each $0 \leq i \leq 2$.

Example 1.10. Let S_4 be the symmetric group containing all permutations of $X_4 = \{1, 2, 3, 4\}$. The subset H of all permutations that fix 4 is a subgroup. In fact, this subgroup is basically the same as S_3 since it contains all possible permutations of the subset $\{1, 2, 3\}$ in X_4.

Definition 1.6. The *quaternion group* is the set $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ where $-i$ is the inverse of i, $-j$ is the inverse of j, and $-k$ is the inverse of k. Further,

$$\begin{aligned} (-1)^2 &= 1 \\ i^2 = j^2 = k^2 &= -1 \\ ij &= k \\ ji &= -k. \end{aligned}$$

The quaternion group is inspired by the standard unit vectors, $\{i, j, k\}$, of $\mathbb{R}^3$ where we operate via the cross-product. Right-hand rule implies that $i \times j = k$ and $j \times i = -k$. Q_8 is a helpful example of a small non-abelian group.

Example 1.11. The subsets $\{1, -1\}$ and $\{1, i, i^2 = -1, i^3 = -i\}$ are subgroups of Q_8.

If we want a subgroup H to contain $\{i, j\}$, then it must contain the inverses $\{-i, -j\}$ and be closed under multiplication. Thus $ij = k \in H$, and we conclude $H = Q_8$.

1.3.1. *Center of a group.*

Definition 1.7. The *center* of a group G is

$$Z(G) = \{h \in G : gh = hg \text{ for all } g \in G\}.$$

In other words, an element of G is in the center if and only if it commutes with all other elements of G. If G is an abelian group, then $Z(G) = G$. If G is not abelian, then $Z(G)$ will be a proper subset of G.

End of lecture 3

Proposition 1.6. The center of G is a subgroup of G.

Proof. The identity of G is always in the center so $Z(G)$ is non-empty.

Let $h_1, h_2 \in Z(G)$. Then $(h_1h_2)g = h_1gh_2 = g(h_1h_2)$ for all $g \in G$. Thus $h_1h_2 \in Z(G)$.

Let $h \in G$. For each $g \in G$, we have $gh^{-1} = (hg^{-1})^{-1} = (g^{-1}h)^{-1} = h^{-1}g$. Thus $h^{-1} \in Z(G)$. □

Example 1.12. We will compute the center of $GL_2(\mathbb{R})$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of the center of $GL_2(\mathbb{R})$. Take $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then

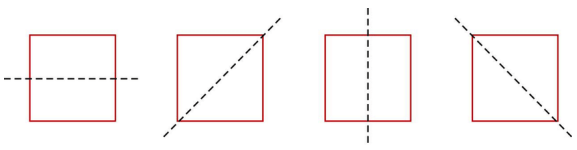
$$AB = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$
$$BA = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

are equal so $a = d$ and $b = c$. Take $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then

$$\begin{aligned} AC &= \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \\ &= \begin{pmatrix} a & a+b \\ b & a+b \end{pmatrix} \\ CA &= \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} a+b & a+b \\ b & a \end{pmatrix} \end{aligned}$$

are equal so $b = c = 0$. We conclude that $Z(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}^\times \right\}$ is the subset of invertible scalar matrices.

Example 1.13. The elements of D_4 are symmetries of the square. We can rotate by a multiple of $\frac{\pi}{2}$ or reflect about one of the axes pictured below.



Let r be a rotation by $\frac{\pi}{2}$ counterclockwise and s be a reflection. Then the elements of D_4 are $\{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. We find

$$rs = sr^3$$
$$r^3 s = sr$$

so r, r^3, and s are not elements of the center. Further,

$$r(sr^i) = sr^{i+3}$$
$$(sr^i)r = sr^{i+1}$$

where $i + 3 \not\equiv i + 1 \pmod 4$. Thus sr^i is not an element of the center for each $0 \leq i \leq 3$. We can show that r^2 does commute with each element so $Z(D_4) = \{e, r^2\}$.

Example 1.14. We will show that $Z(S_3) = \{e\}$. Let $i, j, k \in \{1, 2, 3\}$ be distinct. Then

$$(ij)(ijk) = (jk)$$
$$(ijk)(ij) = (ik)$$

proves that no non-trivial element can be in the center of G. By a similar argument, we can show that $Z(S_n) = \{e\}$ for all $n \geq 3$. We can interpret the result as symmetric groups are as far from abelian as possible.

Example 1.15. Since $ij = k \neq -k = ji$ and $jk = i \neq -i = kj$, the center of the quaternion group does not contain $\{\pm i, \pm j, \pm k\}$. We can show that $Z(Q_8) = \{1, -1\}$.

1.3.2. *Cyclic subgroups.*

Proposition 1.7. If G is a group and $a \in G$, then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Proof. Let $H = \langle a \rangle$. Each element of H is a^k for some $k \in \mathbb{Z}$. Then

$$a^{-k} \in H$$
$$a^k a^\ell = a^{k+\ell} \in H.$$

□

Definition 1.8. The group $\langle a \rangle$ is the *cyclic subgroup generated by* a. If $G = \langle a \rangle$, then G is a *cyclic group*. Note that every cyclic group is abelian since $a^k a^\ell = a^{k+\ell} = a^\ell a^k$.

Some of the most useful examples of groups are cyclic. We will be able to describe a large class of groups by their cyclic subgroups.

Example 1.16. The group $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$ is a cyclic group generated by 2. However, the element 8 is order 2 and does not generated the group.

Proposition 1.8. Let G be a group with $a \in G$.

(1) If a has infinite order, then $\langle a \rangle$ is an infinite subgroup consisting of the distinct elements a^k for $k \in \mathbb{Z}$.
(2) If a has finite order n, then $\langle a \rangle$ is a subgroup of order n and $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Proof. The result follows from Proposition 1.3. □

Remark 1.3. There is an additive version of Proposition 1.8. Let a have finite order n of an additive group G. Then $\langle a \rangle = \{0, a, 2a, \ldots, (n-1)a\}$.

Example 1.17. The group $\mathbb{Z}$ is an infinite cyclic group generated by 1.

Example 1.18. The group $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group generated by $\overline{1}$ for each n.

Example 1.19. For $G = D_4$, examples of cyclic subgroups of D_4 are $\langle r \rangle$ or $\langle sr^i \rangle$ for $0 \leq i \leq 3$. The subgroup $H = \langle r^2, s \rangle$ is a non-cyclic subgroup.

Proposition 1.9. Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ and H a subgroup of G. If $H = \langle e \rangle$, then H is the cyclic subgroup generated by e. If $H \neq \langle e \rangle$, then there is some non-identity element a^i. By possibly taking an inverse, we may assume i is positive. Let k be the smallest positive integer for which $a^k \in H$. We will prove that $H = \langle a^k \rangle$. Let $h \in H$ so $h = a^m$ for some m. By the division algorithm, $m = kq + r$ for $0 \leq r < k$. Thus

$$a^r = a^{m-kq} = a^m a^{-kq} = a^m (a^k)^{-q} \in H.$$

Since k is the smallest positive integer, $r = 0$ and $h = a^m = (a^k)^q$ as desired. □

End of lecture 4

1.3.3. *Generators of a group.* Cyclic subgroups are the easiest groups to describe. It turns out we can describe groups as products of cyclic subgroups. Often large groups can be described with only a small set of fundamental elements.

Definition 1.9. Let S be a non-empty subset of a group G. Let $\langle S \rangle$ be the subset of all possible finite products of integer powers of elements of S. We will refer to $\langle S \rangle$ as the *subgroup generated by* S.

If $S = \{a\}$, then $\langle S \rangle$ is the cyclic subgroup generated by a. If $G = \langle S \rangle$, then we say that G is *generated* by S. The next result proves that $\langle S \rangle$ is the smallest subgroup of G containing the subset S.

Proposition 1.10. (1) $\langle S \rangle$ is a subgroup of G that contains S.
(2) If H is a subgroup of G that contains the set of S, then H contains the subgroup $\langle S \rangle$.

Proof. (1) $\langle S \rangle$ is non-empty because the set S is non-empty and every element of S (considered as a one-element product) is an element of $\langle S \rangle$. If $a, b \in \langle S \rangle$, then

$$a = a_1 a_2 \cdots a_k$$

where $k \geq 1$ and each a_i is either an element of S or the inverse of an element of S. Similarly,

$$b = b_1 b_2 \cdots b_t$$

with $t \geq 1$ and each b_j is either an element of S or the inverse of an element of S. Therefore, the product

$$ab = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_t$$

consists of elements of S or inverses of elements of S. Hence, $ab \in \langle S \rangle$ and $\langle S \rangle$ is closed under products. Further,

$$a^{-1} = a_k^{-1} \cdots a_2^{-1} a_1^{-1}$$

is in $\langle S \rangle$ so $\langle S \rangle$ is closed under inverses.

(2) Any subgroup that contains the set S must include the inverse of every element of S. By closure, this subgroup must also contain all possible products, in every order, of elements of S and their inverses. Therefore, every subgroup that contains S must also contain the entire group $\langle S \rangle$.

□

Example 1.20. The group D_n is generated by the set $S = \{r, s\}$ where r is the rotation by $\frac{2\pi}{n}$ counterclockwise and s is a reflection.

Example 1.21. As we noted in Example 1.11, Q_8 is generated by $\{i, j\}$.

Definition 1.10. Let G_1 and G_2 be two groups. The *Cartesian product* is the set of ordered pairs

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

with the operation $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$.

We will be able to describe many groups as the Cartesian product of the above group examples.

Example 1.22. Let $G = \langle S \rangle$ and $H = \langle T \rangle$ be two groups. Then the Cartesian product $G \times H$ is generated by the set of ordered pairs $(S \times \{e_H\}) \cup (\{e_G\} \times T)$.

Once we determine a set of generators for a group, much of the information of the group can be determined by checking only on the generators. For instance, the next result shows that we can check that a group is abelian on its generators.

Proposition 1.11. Let $G = \langle S \rangle$. If $ab = ba$ for any two $a, b \in S$, then G is abelian.

Proof. Let $x, y \in G$. Then $x = a_1 a_2 \cdots a_k$ for $a_i \in S$ and $y = b_1 b_2 \cdots b_\ell$ for $b_j \in S$. Since each a_i commutes with each b_j,

$$\begin{aligned} ab &= (a_1 a_2 \cdots a_k)(b_1 b_2 \cdots b_\ell) \\ &= (a_1 a_2 \cdots a_{k-1})(b_1 b_2 \cdots b_\ell) a_k \\ &\vdots \\ &= (b_1 b_2 \cdots b_\ell)(a_1 a_2 \cdots a_k) \\ &= ba. \end{aligned}$$

□

1.4. **Isomorphisms and Homomorphisms.** There are many examples of groups that use different symbols to represent the same underlying structure. These groups will be referred to as isomorphic groups. In practice, we will treat isomorphic groups as the same. Once we identify elements properly, there is no discernible difference except in the symbols we use to represent them.

Example 1.23. Below are the multiplication tables of $(\mathbb{Z}/5\mathbb{Z})^\times$ and $\mathbb{Z}/4\mathbb{Z}$.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Via the identification

$$1 \mapsto \overline{0}$$
$$2 \mapsto \overline{1}$$
$$3 \mapsto \overline{3}$$
$$4 \mapsto \overline{2},$$

we can see that the two groups have the same underlying structure since the product of any two elements in $(\mathbb{Z}/5\mathbb{Z})^\times$ corresponds to the product of the corresponding elements in $\mathbb{Z}/4\mathbb{Z}$. In fact, we will prove in Proposition 1.16 that any two cyclic groups of the same order will be isomorphic by identifying a generator of one with a generator of the other.

Writing down multiplication tables is not an effective technique for large finite or infinite groups. Thus we will want a simpler formal process for finding when two groups are the same. In short, a group homomorphism is a function that preserves the multiplication structure on groups. This should remind you of the definition of a ring homomorphism except with only one operation involved.

Definition 1.11. Let G and H be groups. A function $f : G \to H$ is a *group homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Proposition 1.12. Let $f : G \to H$ be a group homomorphism.

(1) $f(e_G)$ is the identity of H.
(2) $f(a^{-1}) = f(a)^{-1}$ for every $a \in G$.

Proof. (1) For $g \in G$, we have $f(g) = f(ge_G) = f(g)f(e_G)$. Multiply on the left by $f(g)^{-1}$ to prove that $e_H = f(e_G)$.

(2) By (1),
$$f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H.$$
Thus $f(a^{-1})$ is the inverse of $f(a)$.

□

The other piece of an isomorphism is that there is a one-to-one correspondence between the elements of the respective groups.

Definition 1.12. Let A and B be sets. A function $f : A \to B$ is *injective* if $f(x) = f(y)$ implies $x = y$. The function is *surjective* if for each $z \in B$, there is some $x \in A$ for which $f(x) = z$. The function is a *bijection* if f is both injective and surjective. Equivalently, a function is bijective if it has an inverse.

Definition 1.13. Let G and H be groups. A function $f : G \to H$ is a *group isomorphism* if f is a bijective group homomorphism. We write $G \simeq H$ when there is a group isomorphism $f : G \to H$.

Example 1.24. Let $E = 2\mathbb{Z}$ be the additive group of even integers. Define $f : \mathbb{Z} \to E$ as $f(n) = 2n$. We claim that f is a group isomorphism. Note that

$$f(m+n) = 2(m+n) = 2m + 2n = f(m) + f(n)$$

so f is a group homomorphism. If $f(m) = f(n)$, then $2m = 2n$ and $m = n$ by dividing by 2. Thus f is injective. Since E is the set of even integers, f is surjective. We conclude that f is an isomorphism and $\mathbb{Z} \simeq E$. This is another example of two isomorphic cyclic groups.

Example 1.25. Let K be the multiplicative group of positive real numbers. Define $f : \mathbb{R} \to K$ as $f(r) = 10^r$. We claim that f is a group isomorphism. Then

$$f(r+s) = 10^{r+s} = 10^r 10^s = f(r)f(s)$$

so f is a group homomorphism. If $f(r) = f(s)$, then $10^r = 10^s$ and $r = s$ by taking $\log_{10}$ of both sides. Thus f is injective. For each $k \in K$, we find

$$f(\log_{10}(k)) = 10^{\log_{10}(k)} = k$$

so f is surjective. We conclude that f is a group isomorphism and $R \simeq K$.

Example 1.26. The function $f : \mathbb{R}^\times \to \mathbb{R}^\times$ given by $f(r) = r^2$ is a group homomorphism since

$$f(rs) = (rs)^2 = r^2 s^2 = f(r)f(s).$$

However, $f(-1) = f(1) = 1$ so f is not injective. Further, f is not surjective since $f(r) = r^2 \geq 0$.

Example 1.27. The function $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $f(a) = \overline{a}$ is a homomorphism of additive groups since

$$f(a+b) = \overline{a+b} = \overline{a} + \overline{b} = f(a) + f(b).$$

The function is surjective but not injective. For $a \equiv b \pmod{n}$, we have $f(a) = f(b)$.

Example 1.28. Let G and H be groups. The function $f : G \times H \to G$ given by $f(g,h) = g$ is projection onto the first coordinate. The function f is a surjective group homomorphism that is not injective for non-trivial H.

Example 1.29. A bijection between finite sets implies that the sets have the same size. Thus two finite groups of different order cannot be isomorphic. It is not generally true that two finite groups of the same size are isomorphic, however.

End of lecture 5

Proposition 1.13. If G is abelian and H is non-abelian, then G and H are not isomorphic.

Proof. We will prove the contrapositive. Assume that $f : G \to H$ is an isomorphism and G is abelian. For each $h_1, h_2 \in H$, there exist $g_1, g_2 \in G$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. Then

$$h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1) = f(g_2)f(g_1) = h_2 h_1.$$

We conclude that H is abelian. □

Note that in the proof of the above result we only use the surjectivity of f. Thus we can relax the assumption to any surjective group homomorphism.

Example 1.30. The groups $\mathbb{Z}/6\mathbb{Z}$ and S_3 have the same order but are not isomorphic by Proposition 1.13.

Proposition 1.14. If $f : G \to H$ is an isomorphism, then $a \in G$ and $f(a) \in H$ have the same order.

Proof. Let n be the order of a and k the order of $f(a)$. Then

$$f(a)^n = f(a^n) = f(e_G) = e_H$$

by Proposition 1.12(1) so $k \leq n$. Further,

$$f(a)^k = f(a^k) = e_H.$$

Since $f(e_G) = e_H$ and f is injective, $a^k = e_G$. Thus $k \geq n$. □

Note that we only needed f to be injective in the above argument. Thus the same result is true for any injective group homomorphism. We state and prove a generalization for general group homomorphisms.

Proposition 1.15. Let $a \in G$ be an element of finite order. If $f : G \to H$ is a homomorphism, then $|f(a)|$ divides $|a|$.

Proof. Let $n = |a|$. Then $f(a)^n = f(a^n) = f(e_G) = e_H$ by Proposition 1.12(1). Thus Proposition 1.4(1) implies that $|f(a)|$ divides $n = |a|$. □

Example 1.31. The groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are not isomorphic by Proposition 1.14. Every element of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order at most 2 while $\overline{1}$ and $\overline{3}$ have order 4 in $\mathbb{Z}/4\mathbb{Z}$.

Example 1.32. Let c be a fixed element of a group G. Define the function $f : G \to G$ as $f(a) = cac^{-1}$. This is called *conjugation by c*. For $a, b \in G$,

$$f(ab) = c(ab)c^{-1} = ca(c^{-1}c)bc^{-1} = (cac^{-1})(cbc^{-1}) = f(a)f(b)$$

so f is a group homomorphism. The function $g : G \to G$ given by $g(a) = c^{-1}ac$ is inverse to f so f is an isomorphism.

An isomorphism from a group to itself is an *automorphism*. An automorphism defined by conjugation by an element of G is an *inner automorphism*.

Proposition 1.16. Let G be a cyclic group.

(1) If G is infinite, then G is isomorphic to the additive group $\mathbb{Z}$.
(2) If G is finite of order n, then G is isomorphic to the additive group $\mathbb{Z}/n\mathbb{Z}$.

Proof. (1) Suppose $G = \langle a \rangle$ is an infinite cyclic group. Define the function $f : G \to \mathbb{Z}$ as $f(a^k) = k$. Then f is a homomorphism since

$$f(a^i a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j).$$

If $f(a^i) = f(a^j)$, then $i = j$ and f is injective. For each $i \in \mathbb{Z}$, the element $a^i \in G$ satisfies $f(a^i) = i$ so f is bijective. Therefore, $G \simeq \mathbb{Z}$.

(2) Suppose $G = \langle b \rangle$. Define the function $f : G \to \mathbb{Z}/n\mathbb{Z}$ as $f(b^k) = \overline{k}$. Since there are multiple ways of writing an element of G, we need to check that f is well-defined. Let $b^k = b^\ell$. Then $f(b^k) = \overline{k} = \overline{\ell} = f(b^\ell)$ by Proposition 1.4(2). Further, f is a homomorphism since

$$f(b^i b^j) = f(b^{i+j}) = \overline{i+j} = \overline{i} + \overline{j} = f(b^i) + f(b^j)$$

If $f(b^i) = f(b^j)$, then $i \equiv j \pmod{n}$. By Proposition 1.4, $b^i = b^j$ when $i \equiv j \pmod{n}$. Thus f is an injection and f is a bijection since G and $\mathbb{Z}/n\mathbb{Z}$ have the same order.

□

Much like Math 110A, we will define the kernel and image of a group homomorphism. In the best case scenario, knowledge of these two subgroups will give a nearly complete picture of the group homomorphism.

Definition 1.14. Let $f : G \to H$ be a group homomorphism. Define the *kernel of* f and *image of* f respectively as

$$\ker(f) = \{a \in G : f(a) = e_H\}$$
$$\text{im}(f) = \{b \in H : b = f(a) \text{ for some } a \in G\}.$$

Proposition 1.17. The kernel of f is a subgroup of G and the image of f is a subgroup of H.

Proof. The identity of G is an element of $\ker(f)$ so $\ker(f)$ is non-empty.

Let $a, b \in G$ be elements of the kernel of f. Then

$$f(ab) = f(a)f(b) = e_H e_H = e_H$$

so $ab \in \ker(f)$.

By Proposition 1.12(2),

$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$$

so $\ker(f)$ is a subgroup of G.

Since $f(e_G) = e_H$, the identity element of H is always an element of $\text{im}(f)$. Thus $\text{im}(f)$ is non-empty.

Let $c, d \in H$ be elements of the image of f. Then there are $a, b \in G$ for which $f(a) = c$ and $f(b) = d$. Thus

$$f(ab) = f(a)f(b) = cd$$

and $cd \in \text{im}(f)$.

Again by Proposition 1.12(2),

$$f(a^{-1}) = f(a)^{-1} = c^{-1}$$

so $c^{-1} \in \text{im}(f)$. We conclude that $\text{im}(f)$ is a subgroup of H. □

For now, we will work with the image. We will generalize the next result in the First Isomorphism Theorem once we have the notion of a quotient group.

Proposition 1.18. Let $f : G \to H$ be a group homomorphism. If f is injective, then $G \simeq \text{im}(f)$.

Proof. Any group homomorphism $f : G \to H$ can be regarded as a surjective group homomorphism $f : G \to \text{im}(f)$. If f is injective, then f is an isomorphism onto $\text{im}(f)$ and $G \simeq \text{im}(f)$. □

Example 1.33. Define $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ as $f(\overline{k}) = \overline{2k}$. Then

$$f(\overline{k} + \overline{\ell}) = f(\overline{k+\ell}) = \overline{2(k+\ell)} = \overline{2k} + \overline{2\ell} = f(\overline{k}) + f(\overline{\ell})$$

and f is a group homomorphism. We can see that f is injective since $f(\overline{0}) = \overline{0} \neq \overline{2} = f(\overline{1})$. Proposition 1.18 implies that $\mathbb{Z}/2\mathbb{Z} \simeq \text{im}(f) = \langle\overline{2}\rangle$. In other words, a copy of $\mathbb{Z}/2\mathbb{Z}$ sits inside $\mathbb{Z}/4\mathbb{Z}$ as the subgroup generated by $\overline{2}$.

Example 1.34. Recall Example 1.27 where we define the surjective group homomorphism

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

as $f(k) = \overline{k}$. Since f is surjective, $\text{im}(f) = \mathbb{Z}/n\mathbb{Z}$. Let $k \in \ker(f)$ so $f(k) = \overline{0}$. Then $k \equiv 0 \pmod{n}$ or $n|k$. In other words, $\ker(f) \subset n\mathbb{Z}$. To prove the reverse containment, take $a \in n\mathbb{Z}$. Then $a = nk$ for some $k \in \mathbb{Z}$ and $f(nk) = \overline{nk} = \overline{0}$. Therefore, $\ker(f) = n\mathbb{Z}$. We can rephrase this as multiples of n are the elements that map to $\overline{0}$ under f.

Example 1.35. Let G and H be groups. Recall Example 1.28 where we define projection onto the first coordinate $f : G \times H \to G$ as $f(g, h) = g$. Since f is a surjective group homomorphism, $\text{im}(f) = G$. The elements that map to e_G will be of the form $\ker(f) = \{(e_G, h) : h \in H\}$. We can identify this set with H via $(e_G, h) \mapsto h$. With some work, we can show that $\ker(f) \simeq H$. Therefore, there is an isomorphic copy of H in the Cartesian product $G \times H$.

What happens if we instead project onto the second coordinate?

End of lecture 6

2. Normal Subgroups and Quotient Groups

2.1. **Congruence and Lagrange's Theorem.** Recall that two integers are congruent modulo n if $a - b$ is divisible by n. The set $n\mathbb{Z}$ in $\mathbb{Z}$ is the subgroup of multiples of n. We can translate the congruence into multiplicative notation as ab^{-1} is an element of $n\mathbb{Z}$. The following definition generalizes the notion of congruence to an arbitrary subgroup of any group.

Definition 2.1. Let K be a subgroup of a group G. Let $a, b \in G$. Then a is *congruent to b modulo K* if $ab^{-1} \in K$.

Much as in the case of $\mathbb{Z}/n\mathbb{Z}$, our goal is to partition G so that any two elements in a grouping are congruent modulo K. Each piece of the partition will then be treated as a single element in the quotient. For instance, any two integers that are 1 modulo n are elements of the equivalence class $\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.1. For K a subgroup of G, congruence modulo K is an equivalence relation.

Proof. Let $a, b, c \in G$.

Reflexivity: $aa^{-1} = e \in K$ since K is a subgroup of G. Thus a is congruent to a modulo K.

Symmetry: Assume a is congruent to b modulo K. We want to show that b is congruent to a modulo K. We have $ab^{-1} \in K$ so $(ab^{-1})^{-1} \in K$ since K is a subgroup. Then $ba^{-1} \in K$ and b is congruent to a modulo K.

Transitivity: Assume that a is congruent to b modulo K and b is congruent to c modulo K. We want to show that a is congruent to c modulo K. We know that $ab^{-1} \in K$ and $bc^{-1} \in K$. The product of two elements of K is another element of K so $(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = ac^{-1} \in K$. Thus a is congruent to c modulo K. □

For a subgroup K of G and an element $a \in G$, define the *congruence class of a modulo K* to be the set of all elements of G that are congruent to a modulo K. In other words,

$$\overline{a} = \{b \in G : ba^{-1} \in K\}.$$

Let $k = ba^{-1} \in K$ for some $b \in G$. Then $b = ka$ so we can rewrite

$$\overline{a} = \{ka : k \in K\}.$$

As a result, we will adopt the notation Ka for the congruence class of a modulo K.

Definition 2.2. A *right coset* of K in G is a congruence class of some $a \in G$ modulo K. We will denote the right coset Ka.

In the next section, we introduce left cosets aK. We can rephrase everything in this section via left cosets. For non-abelian groups, the left and right cosets might contain different elements, but there will always be the same number of left and right cosets of a subgroup.

Example 2.1. Let $G = D_4$ and $K = \langle s \rangle = \{e, s\}$. The subgroup K is a right coset. We also have the right cosets $Kr = \{r, sr\}$ and $Kr^2 = \{r^2, sr^2\}$. The remaining right coset is $Kr^3 = \{r^3, sr^3\}$. Note that each element of D_4 appears in one and only one right coset of K.

Let $G = D_4$ and $N = \langle r \rangle$. The subgroup N is a right coset. The only other right coset is $Ns = \{s, rs = sr^3, r^2s = sr^2, r^3s = sr\}$. Once again, each element of D_4 appears in one and only one right coset of K.

Proposition 2.2. Let K be a subgroup of G and $a, c \in G$. Then a is congruent to c modulo K if and only if $Ka = Kc$.

Proof. ($\Rightarrow$) Assume a is congruent to c modulo K. Then $ac^{-1} \in K$ and $a = kc$ for some $k \in K$. Then $Ka = K(kc) \subset Kc$. Further, $c^{-1} = a^{-1}k$ for some $k \in K$ or $c = k^{-1}a$ by taking the inverse of both sides. Then $Kc = K(k^{-1}a) \subset Ka$ and $Ka = Kc$.

($\Leftarrow$) Assume that $Ka = Kc$. Then $ea = a \in Kc$ and $a = kc$ for some $k \in K$. Thus $ac^{-1} = k \in K$ by multiplying by c^{-1} on the right. We conclude that a is congruent to c modulo K. □

Corollary 2.1. Let K be a subgroup of G. Two right cosets of K in G are either disjoint or identical.

Proof. Let Ka and Kb be two right cosets of K in G. If $Ka \cap Kb$ is non-trivial, then there are $k_1, k_2 \in K$ for which $k_1a = k_2b$. Then $ab^{-1} = k_1^{-1}k_2 \in K$. By Proposition 2.2, $Ka = Kb$. □

2.1.1. *Lagrange's Theorem.* In this subsection, we will develop our first powerful theorem for dealing with groups. Lagrange's Theorem will reduce some of our group questions to a question about divisibility of integers.

Proposition 2.3. Let K be a subgroup of G.

(1) G is the union of the right cosets of K, $G = \bigcup_{a \in G} Ka$.
(2) For each $a \in G$, there is a bijection of sets $f : K \to Ka$. If K is finite, any two right cosets contain the same number of elements.

Proof. (1) Since Ka is a subset of G, we have $\bigcup_{a \in G} Ka \subset G$. Let $b \in G$, then $b = eb \in Kb$ and $b \in \bigcup_{a \in G} Ka$. Thus $G \subset \bigcup_{a \in G} Ka$ and $G = \bigcup_{a \in G} Ka$.

(2) Define the set function $f : K \to Ka$ as $f(k) = ka$ for each $k \in K$. By definition of Ka, f is surjective. Assume $f(x) = f(y)$ for $x, y \in K$. Then $xa = ya$ and $x = y$ by right multiplication by a^{-1}. Thus f is injective and, hence, bijective.

If K is finite, every coset Ka has the same number of elements as K. Thus Ka and Kb have the same number of elements for any $a, b \in G$.

□

Definition 2.3. Let H be a subgroup of G. Then the *index of H in G* is the number of distinct right cosets of H in G, denoted $[G : H]$.

If G is finite, then the index of any subgroup is finite. If G is infinite, the index of a subgroup could be finite or infinite.

Example 2.2. Let $n\mathbb{Z}$ be the subgroup of $\mathbb{Z}$ containing multiples of n. Then $[\mathbb{Z} : n\mathbb{Z}] = n$ since there are n distinct congruence classes.

Example 2.3. Let $\mathbb{Z}$ be the integral subgroup of the additive group $\mathbb{Q}$. For $a, b \in \mathbb{Q}$, the cosets $\mathbb{Z} + a$ and $\mathbb{Z} + b$ are equal if and only if $a - b \in \mathbb{Z}$. Each coset has a unique representative $x \in \mathbb{Z} + a$ for which $0 \leq x < 1$. If $0 \leq x < y < 1$, then $\mathbb{Z} + x \neq \mathbb{Z} + y$. Thus $[\mathbb{Q} : \mathbb{Z}]$ is infinite.

Theorem 2.1 (Lagrange's Theorem)**.** Let K be a subgroup of a finite group G. Then the order of K divides the order of G. Further,

$$|G| = |K|[G : K].$$

Proof. Suppose that $[G : K] = n$ and denote the n distinct cosets of K in G by $Kc_1, \ldots, Kc_n$ for each $c_i \in G$. By Proposition 2.3(1), $G = \bigcup_{i=1}^{n} Kc_i$. The cosets are distinct so, by Corollary 2.1, the cosets are pairwise disjoint. Thus $|G| = \sum_{i=1}^{n} |Kc_i| = \sum_{i=1}^{n} |K|$ by Proposition 2.3(2). We conclude that $|G| = |K|[G : K]$. □

Corollary 2.2. Let G be a finite group.

(1) If $a \in G$, then the order of a divides the order of G.

(2) If $|G| = k$, then $a^k = e$ for every $a \in G$.

Proof. (1) The cyclic subgroup $\langle a \rangle$ of G has order $|a|$ by Proposition 1.8(2). By Lagrange's Theorem, $|a|$ divides $|G|$.

(2) If $|G| = k$ and $|a| = n$, then $n|k$ by (1). Thus $k = nt$ for some $t \in \mathbb{Z}$ and

$$a^k = a^{nt} = (a^n)^t = e^t = e.$$

□

Example 2.4. Let p be a prime integer. Every group G of order p is cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Let $a \in G$. Then $|a|$ divides p by Corollary 2.2. Since p is prime, $|a| = 1$ or $|a| = p$. If $|a| = 1$, then a is the identity of G. If $|a| = p$, then $\langle a \rangle = G$ and G is cyclic of order p. By Proposition 1.16(2), $G \simeq \mathbb{Z}/p\mathbb{Z}$.

End of lecture 7

Example 2.5. Every group of order 4 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $a \in G$. By Lagrange's Theorem, $|a|$ divides 4 so $|a| = 1$, $|a| = 2$, or $|a| = 4$. If G has an element of order 4, then $G \simeq \mathbb{Z}/4\mathbb{Z}$ by Proposition 1.16(2).

Suppose that G does not contain an element of order 4. Then each non-identity element of G has order 2. Let $G = \{e, a, b, c\}$. We can fill in the multiplication table as follows.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

If $ab = e$, then $b = a^{-1} = a$, a contradiction. If $ab = a$, then $b = e$, a contradiction. If $ab = b$, then $a = e$, a contradiction. Thus $ab = c$. We obtain the multiplication table below by filling in the grid like a Sudoku puzzle.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This is the multiplication table for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ via the following identification

$$e \mapsto (\overline{0}, \overline{0})$$
$$a \mapsto (\overline{1}, \overline{0})$$
$$b \mapsto (\overline{0}, \overline{1})$$
$$c \mapsto (\overline{1}, \overline{1}).$$

2.2. **Normal Subgroups.** We would like the set of cosets of a subgroup K in a group G to form a group. For $a, b \in G$ obvious multiplication would be $(Ka)(Kb) = K(ab)$. However, the elements of $(Ka)(Kb)$ have the form k_1ak_2b while the elements of $K(ab)$ have the form k_1ab for $k_1, k_2 \in K$. For non-abelian groups, these two descriptions can be quite different. A normal subgroup will be one for which the set of right cosets is a group under the desired operation.

Definition 2.4. Let K be a subgroup of G and $a \in G$. A *left coset* is $aK = \{ak : k \in K\}$.

Definition 2.5. A subgroup N of G is *normal* if $aN = Na$ for all $a \in G$. In other words, the left coset containing a coincides with the right coset containing a. We write $N \triangleleft G$.

Example 2.6. Recall Example 2.1 where $G = D_4$ with subgroups $K = \langle s \rangle$ and $N = \langle r \rangle$. The left coset $rK = \{r, rs = sr^3\}$ while the right coset $Kr = \{r, sr = r^3s\}$. Thus K is not normal.

However, $sN = Ns$ and $rN = N = Nr$ so N is a normal subgroup. Note that we only need to check the normality condition on the generators of the group.

Example 2.7. Let G be an abelian group with subgroup N. Since $an = na$ for all $a \in G$ and $n \in N$, N is a normal subgroup of G. We conclude that every subgroup of an abelian group is normal.

Example 2.8. Let G be a group with subgroup N. Recall that the center $Z(G)$ of G from Definition 1.7 is the subgroup of elements that commute with all elements of G. Let $N \subseteq Z(G)$. Take $a \in G$ and $n \in N$. Then $an = na$ so any subgroup of $Z(G)$ is always a normal subgroup of G. In particular, this implies that $Z(G)$ is always normal.

Remark 2.1. It is important to note that the condition $aN = Na$ does not imply that $an = na$ for each $n \in N$. The equality $aN = Na$ only requires that $an_1 = n_2a$ for some possibly distinct $n_1, n_2 \in N$. We can think of this as a relaxed commutativity condition.

The following result is the motivation for normal subgroups. We will be able to define an intuitive multiplication on the right (or left) cosets of normal subgroups.

Proposition 2.4. Let N be a normal subgroup of G with $a, b, c, d \in G$. If $Na = Nb$ and $Nc = Nd$, then $N(ac) = N(bd)$.

Proof. There are elements $m, n \in N$ for which $ab^{-1} = m$ and $cd^{-1} = n$. Since N is normal, $an = n_1a$ for some $n_1 \in N$. Then

$$\begin{aligned}(ac)(bd)^{-1} &= acd^{-1}b^{-1} \\ &= a(cd^{-1})b^{-1} \\ &= anb^{-1} \\ &= n_1ab^{-1} \\ &= n_1m \in N.\end{aligned}$$

Therefore, $N(ac) = N(bd)$ by Proposition 2.2. □

The following result lists equivalent properties of a normal subgroup. There are scenarios where one of the properties will be easier to check than the others.

Proposition 2.5. Let N be a subgroup of G with $aNa^{-1} = \{ana^{-1} : n \in N\}$ for $a \in G$. The following are equivalent.

(1) N is a normal subgroup of G.
(2) $aNa^{-1} \subset N$ for all $a \in G$.
(3) $aNa^{-1} = N$ for all $a \in G$.

Proof. (1) $\Rightarrow$ (2): If N is normal, then $aN = Na$ for all $a \in G$. Fix $a \in G$. Then for each $n \in N$, $an = n_1 a$ for some $n_1 \in N$. Thus $ana^{-1} = n_1 \in N$ by multiplying on the right by a^{-1}. We have $aNa^{-1} \subset N$ for all $a \in G$.

(2) $\Rightarrow$ (3): Assume that $aNa^{-1} \subset N$ for each $a \in G$. Let $n \in N$. Then $a^{-1}na = n_1$ so $n = an_1a^{-1}$ for some $n_1 \in N$. Thus $N \subset aNa^{-1}$ and $aNa^{-1} = N$ for each $a \in G$.

(3) $\Rightarrow$ (1): If $aNa^{-1} = N$ for each $a \in G$, then each $n \in N$ satisfies $ana^{-1} = n_1$ for some $n_1 \in N$. Thus $an = n_1 a$ via right multiplication by a. We conclude that $aN \subset Na$. Each $n \in N$ also satisfies $an_2a^{-1} = n$ for some $n_2 \in N$. Then $an_2 = na$ via right multiplication by a. Thus $aN \supset Na$ and $aN = Na$. □

Example 2.9. Let $G = S_3$ and $N = \{e, (123), (132)\}$. For $n \in N$, we always have nNn^{-1}. We only need to check conjugation by $a \in G$ for transpositions a. Then

$$(12)(123)(12) = (132)$$
$$(12)(132)(12) = (123).$$

We can do the same computation for (13) and (23). We don't need to check conjugation by elements that are in the subgroup since any product of elements in N will remain in N We conclude that $aNa^{-1} = N$ for each $a \in G$ so N is normal.

End of lecture 8

Remark 2.2. It is sufficient to check normality on a set of generators of G. Let $G = \langle S \rangle$ and $g \in G$. Then $g = s_1 \cdots s_k$ for some $s_i \in S$. For each $n \in N$, we have

$$\begin{aligned} gng^{-1} &= (s_1 \cdots s_k)n(s_1 \cdots s_k)^{-1} \\ &= (s_1 \cdots (s_{k-1}(s_k n s_k^{-1})s_{k-1}^{-1}) \cdots s_1). \end{aligned}$$

We can inductively prove that $gng^{-1} \in N$ if $s_i n s_i^{-1} \in N$ for each $s_i \in S$.

Further, we can check normality on a set of generators for N. Let $N = \langle T \rangle$. For each $n \in N$, we can write $n = t_1 \cdots t_k$ for some $t_i \in S$. Then

$$\begin{aligned} gng^{-1} &= g(t_1 \cdots t_k)g^{-1} \\ &= gs_1(g^{-1}g)t_1(g^{-1}g) \cdots (g^{-1}g)t_k g^{-1} \\ &= (gt_1g^{-1}) \cdots (gt_k g^{-1}). \end{aligned}$$

If $gt_ig^{-1} \in N$ for each $t_i \in S$, then $gng^{-1} \in N$ for all $n \in N$. Therefore, N is normal.

Lemma 2.1. Let H be a subgroup of G with $[G : H] = 2$. Then H is normal.

Proof. Let $\{H, Ha\}$ be the set of right cosets of H. Then $a \notin H$ and the left cosets aH and H are not equal. Since $[G : H] = 2$, the set of left cosets is $\{H, aH\}$. We conclude that $aH = Ha$. □

2.3. **Quotient Groups.**

Definition 2.6. Let N be a normal subgroup of G. We will denote the sets of right cosets of N in G by G/N. We will call G/N the *quotient of G by N*.

The following result partially motivates the fraction notation.

Proposition 2.6. Let N be a normal subgroup of G with $a, b \in G$.

(1) G/N is a group via the operation $(Na)(Nb) = N(ab)$.
(2) If G is finite, then $|G/N| = |G|/|N|$.
(3) If G is abelian, then G/N is abelian.

Proof. (1) The operation is well-defined by Proposition 2.4. Let $a, b, c \in G$. The coset $N = Ne$ is the identity element since

$$(Ne)(Na) = N(ea) = Na$$
$$(Na)(Ne) = N(ae) = Na.$$

The inverse of Na is Na^{-1} since

$$(Na)(Na^{-1}) = N(aa^{-1}) = Ne = N$$
$$(Na^{-1})(Na) = N(a^{-1}a) = Ne = N.$$

The operation is associative since

$$\begin{aligned}((Na)(Nb))(Nc) &= N(ab)Nc \\ &= N((ab)c) \\ &= N(a(bc)) \\ &= Na(N(bc)) \\ &= Na((Nb)(Nc)).\end{aligned}$$

(2) The order $|G/N|$ is $[G : H]$ which, by Lagrange's Theorem, is $|G|/|N|$.
(3) Let $a, b \in G$. Then $(Na)(Nb) = N(ab) = N(ba) = (Nb)(Na)$.

□

Example 2.10. Let $G = D_4$ and $N = \langle r \rangle$. Then G/N is a group of order $|G|/|N| = 2$ by Proposition 2.6(2). The only group of order 2 by Example 2.4 is $\mathbb{Z}/2\mathbb{Z}$. Thus $G/N \simeq \mathbb{Z}/2\mathbb{Z}$.

Example 2.11. Let $G = D_4$ and $K = Z(G)$. By Example 1.13, $Z(G) = \langle r^2 \rangle$, and $Z(G)$ is normal by Example 2.8. Proposition 2.6 implies that $|G/K| = 4$. The cosets are $K = \{e, r^2\}$, $Kr = \{r, r^3\}$ $Ks = \{s, r^2s = sr^2\}$, and $K(sr) = \{sr, r^2sr = sr^3\}$. We have the following multiplication table.

$\cdot$	K	Kr	Ks	$K(sr)$
K	K	Kr	Ks	$K(sr)$
Kr	Kr	K	$K(sr)$	Ks
Ks	Ks	$K(sr)$	K	Kr
$K(sr)$	$K(sr)$	Ks	Kr	K

By Example 2.5, G/K is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The multiplication table is that of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since every non-identity element has order 2. Therefore, $G/K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 2.12. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $N = \langle (1,2) \rangle$. Since G is abelian, N is normal. The order of N is 2 so Proposition 2.6 implies $|G/N| = |G|/|N| = 4$. The cosets are

$$\begin{aligned} N &= \{(0,0),(1,2)\} \\ N + (1,0) &= \{(1,0),(0,2)\} \\ N + (0,1) &= \{(0,1),(1,3)\} \\ N + (1,1) &= \{(1,1),(0,3)\}. \end{aligned}$$

The element $N + (0,1)$ generates G/N so $G/N \simeq \mathbb{Z}/4\mathbb{Z}$.

Example 2.13. The additive group $\mathbb{Q}$ is abelian so the subgroup $\mathbb{Z}$ is normal. The quotient group $\mathbb{Q}/\mathbb{Z}$ is an infinite group by Example 2.3. An element $\left[\frac{r}{s}\right]$ has order dividing s. Thus every element of $\mathbb{Q}/\mathbb{Z}$ has finite order. Interestingly, the group has at least one element of each finite order.

2.3.1. *The Structure of Groups.* The general method for studying a group G is first find normal subgroups N of G. If we know information about N and the quotient G/N, we can often learn information about the group G.

Proposition 2.7. Let N be a normal subgroup of G. Then G/N is abelian if and only if

$$aba^{-1}b^{-1} \in N$$

for all $a, b \in G$.

Proof. ($\Rightarrow$) Assume that G/N is abelian. Let $a, b \in G$. Then $(Na)(Nb) = N(ab)$ is equal to $(Nb)(Na) = N(ba)$ so $ab(ba)^{-1} \in N$. Thus $aba^{-1}b^{-1} \in N$ for every $a, b \in G$.

($\Leftarrow$) Assume that $aba^{-1}b^{-1} \in N$ for every $a, b \in G$. We can rewrite $aba^{-1}b^{-1} = (ab)(ba)^{-1}$. Then $(Na)(Nb) = N(ab) = N(ba) = (Nb)(Na)$ for every $a, b \in G$. We conclude that G/N is abelian. □

Definition 2.7. The *commutator subgroup* of a group G is $[G,G] = \langle aba^{-1}b^{-1} : a, b \in G \rangle$.

Proposition 2.7 proves that every normal subgroup for which the quotient group is abelian must contain the commutator subgroup. Thus the commutator subgroup will play a significant role in studying almost every non-abelian group.

End of lecture 9

Proposition 2.8. The subgroup $[G,G]$ of G is normal.

Proof. Let $g \in G$. We have

$$\begin{aligned} g(aba^{-1}b^{-1})g^{-1} &= gaba^{-1}(g^{-1}g)b^{-1}g^{-1} \\ &= (ga)b(a^{-1}g^{-1})gb^{-1}g^{-1} \\ &= (ga)b(ga)^{-1}(b^{-1}b)gb^{-1}g^{-1} \\ &= ((ga)b(ga)^{-1}b^{-1})(bgb^{-1}g^{-1}) \in [G,G]. \end{aligned}$$

The conjugation of every generator of $[G,G]$ is an element of $[G,G]$. Remark 2.2 implies that $[G,G]$ is normal. □

Example 2.14. Let G be an abelian group. Then $[G,G] = \{e\}$. In fact, G is abelian if and only if $[G,G] = \{e\}$.

The following result is another useful tool in classifying groups.

Proposition 2.9. If G is a group for which $G/Z(G)$ is cyclic, then G is abelian.

Proof. Note that $Z(G)$ is a normal subgroup of G by Example 2.8. Let $Z(G)a \in G/Z(G)$ be a generator where $a \in Z(G)a$ is an element of G. Then we can write every element of G as na^i for some $n \in Z(G)$. For $n_1, n_2 \in Z(G)$,

$$\begin{aligned}(n_1a^i)(n_2a^j) &= a^in_1a_jn_2\\ &= a^ia^jn_1n_2\\ &= a^{i+j}n_1n_2\\ &= a^j(a^in_1)n_2\\ &= (a^jn_2)(a^in_1).\end{aligned}$$

Every element of G commutes with every other element of G so G is abelian. □

2.4. **Isomorphism Theorems.** There is a close connection between normal subgroups, quotient groups, and surjective group homomorphisms. Recall the definition of the kernel of a group homomorphism $f : G \to H$ from Definition 1.14. In Proposition 1.17, we prove that the kernel is a subgroup of G.

Proposition 2.10. Let $f : G \to H$ be a group homomorphism. Then $\ker(f)$ is a normal subgroup of G.

Proof. Let $g \in G$ and $k \in \ker(f)$. Then

$$\begin{aligned} f(gkg^{-1}) &= f(g)f(k)f(g^{-1}) \\ &= f(g)e_G f(g)^{-1} \\ &= f(g)f(g)^{-1} \\ &= e_G. \end{aligned}$$

Thus $gkg^{-1} \in \ker(f)$ and $\ker(f)$ is a normal subgroup of G. □

As the next result shows, the kernel measures how far a group homomorphism is from being injective.

Proposition 2.11. Let $f : G \to H$ be a group homomorphism with $K = \ker(f)$. Then $K = \{e_G\}$ if and only if f is injective.

Proof. ($\Rightarrow$) Assume $K = \{e_G\}$. Then $f(a) = f(b)$ implies

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e_H.$$

We have $ab^{-1} = e_G$ so $a = b$ and f is injective.

($\Leftarrow$) Assume f is injective. Since $f(e_G) = e_H$, we conclude that $f(a) = e_H$ implies $a = e_G$. Thus $K = \{e_G\}$. □

The following result develops a one-to-one correspondence between normal subgroups of G and kernels of homomorphisms out of G. We have already seen in Proposition 2.10 that any kernel is a normal subgroup. Every normal subgroup is also the kernel of some group homomorphism.

Proposition 2.12. If N is a normal subgroup of G, the function $\pi : G \to G/N$ given by $\pi(a) = Na$ is a surjective group homomorphism with kernel N.

Proof. Let $a, b \in G$. Then $\pi(ab) = N(ab) = (Na)(Nb) = \pi(a)\pi(b)$ so π is a group homomorphism.

Given some right coset Na, the element $a \in G$ satisfies $\pi(a) = Na$. Thus π is surjective.

Let $a \in \ker(f)$. Then $f(a) = Na = N$, which is equivalent to $a \in N$. Therefore, $\ker(f) = N$. □

Definition 2.8. We call $\pi : G \to G/N$ a *quotient group homomorphism*.

The following are some of the most useful results in our study of groups. The Correspondence Theorem will relate the subgroups of G to that of a quotient G/N. In most situations, we will have information about the structure of either G or G/N. The Correspondence Theorem often allows us to translate that information to the other setting. The Isomorphism Theorems provide tools for describing groups as the quotient of a possibly more familiar group.

Theorem 2.2 (Correspondence Theorem)**.** Let N be a normal subgroup of G. Then there is a bijection between the set of all subgroups of G that contain N and the set of subgroups of G/N.

Proof. Assume that K is a subgroup of G that contains N. Since N is a normal subgroup of G, N is also a normal subgroup of K. Then $K/N = \{Nk : k \in K\}$ is a non-empty subset of G/N that is closed under the operation and inverses. Thus K/N is a subgroup of G/N.

Assume that $\overline{K}$ is a subgroup of G/N. Define $K = \{k \in G : \pi(k) \in \overline{K}\}$, and we want to show that K is a subgroup of G that contains N. Clearly, K is not empty since $\pi(e_G) \in \overline{K}$. Given $k_1, k_2 \in K$, we have $\pi(k_1k_2) = \pi(k_1)\pi(k_2) \in \overline{K}$ since $\overline{K}$ is closed under the group operation. Thus $k_1k_2 \in K$. We have $\pi(k_1^{-1}) = \pi(k_1)^{-1} \in \overline{K}$ since $\overline{K}$ is closed under inverses. Thus $k_1^{-1} \in K$. We conclude that K is a subgroup of G. For any $n \in N$, $\pi(n)$ is the identity of G/N so $n \in K$. Therefore, K is a subgroup of G that contains N.

The two operations described are inverse to one another, producing the desired bijection. □

End of lecture 10

Corollary 2.3 (Correspondence Theorem for Normal Subgroups)**.** Let N be a normal subgroup of G. Then there is a bijection between the set of all normal subgroups of G that contain N and the set of normal subgroups of G/N.

Proof. The Correspondence Theorem proves the bijection for subgroups. We need only show that normal subgroups map to normal subgroups under the correspondence.

Let K be a normal subgroup of G that contains N. Then for $Nk \in K/N$ and $Ng \in G/N$, we have $(Ng)(Nk)(Ng)^{-1} = N(gkg^{-1}) \in K/N$. Thus K/N is a normal subgroup of G/N.

Let K/N be a normal subgroup of G/N. For $k \in K$ and $g \in G$, we have $(Ng)(Nk)(Ng)^{-1} \in K/N$ so $gkg^{-1} \in K$. Thus K is a normal subgroup of G. □

Example 2.15. Let $G = \mathbb{Z}$ and $N = n\mathbb{Z}$. Since G is abelian, N is automatically normal in G. Any subgroup of $\mathbb{Z}$ containing $n\mathbb{Z}$ will be of the form $m\mathbb{Z}$ for $m|n$. The corresponding subgroup of $\mathbb{Z}/n\mathbb{Z}$ will be $m\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + h : h \in m\mathbb{Z}\}$.

Take, for example, $n = 6$ and $m = 2$. Then the subgroup $2\mathbb{Z}$ of $\mathbb{Z}$ contains $6\mathbb{Z}$ and corresponds to $2\mathbb{Z}/6\mathbb{Z} = \{\mathbb{Z} + 0, \mathbb{Z} + 2, \mathbb{Z} + 4\} \simeq \mathbb{Z}/3\mathbb{Z}$. Visually, we reduce the fraction $2/6$ to $1/3$. This intuition is a bit dangerous, however.

Lemma 2.2. Let $f : G \to H$ be a group homomorphism with kernel K. Let $a, b \in G$. Then $f(a) = f(b)$ if and only if $Ka = Kb$.

Proof. ($\Rightarrow$) Assume $f(a) = f(b)$. Then

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) = e_H.$$

so $ab^{-1} \in K$. We conclude $Ka = Kb$.

($\Leftarrow$) Assume $Ka = Kb$. Then $ab^{-1} \in K$ so $f(ab^{-1}) = e_H$. We have $f(a) = f(b)$ by a similar argument as above. □

Theorem 2.3 (First Isomorphism Theorem)**.** Let $f : G \to H$ be a group homomorphism with kernel K. Then the quotient group G/K is isomorphic to $\text{im}(f)$.

Proof. We want to define $\varphi : G/K \to \text{im}(f)$ by $\varphi(Ka) = f(a)$, but cosets can have different labels. We need to show that each label results in the same image under φ. Suppose $Ka = Kb$ for $a, b \in G$. Then $f(a) = f(b)$ by Lemma 2.2 so $\varphi(Ka) = \varphi(Kb)$. Therefore, φ as written is well-defined.

The function φ is a group homomorphism since

$$\varphi((Ka)(Kb)) = \varphi(K(ab)) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb).$$

Suppose $h \in \text{im}(f)$. Then there is some $g \in G$ for which $f(g) = h$ by f surjective. Thus

$$\varphi(Kg) = f(g) = h$$

and φ is surjective. Suppose $\varphi(Ka) = \varphi(Kb)$ for $a, b \in G$. Then $f(a) = f(b)$ so $Ka = Kb$ by Lemma 2.2. We conclude that φ is injective and, as a result, an isomorphism. □

The First Isomorphism Theorem will allow us to describe a group H by finding a group G and a surjective homomorphism $f : G \to H$. Then $G/\ker(f) \simeq H$.

Example 2.16. Define projection onto the first coordinate $f : G \times H \to G$ as $f(g, h) = g$. The group homomorphism is surjective by Example 1.28. With $\overline{H} = \ker(f) = \{(e_G, h) : h \in H\}$, the First Isomorphism Theorem implies $(G \times H)/\overline{H} \simeq G$. We can show that $\overline{H} \simeq H$ via the identification $(e_G, h) \mapsto h$.

Example 2.17. Let $f : \mathbb{C}^\times \to \mathbb{R}^\times$ be $f(a + bi) = a^2 + b^2$. We have

$$\begin{aligned} f((a+bi)(c+di)) &= f((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= f(a+bi)f(c+di) \end{aligned}$$

so f is a group homomorphism. Let $K = \text{im}(f)$ be the subgroup of all positive real numbers. Since 1 is the identity of $\mathbb{R}^\times$, $N = \ker(f) = \{a + bi : a^2 + b^2 = 1\}$ is the circle of radius 1 in the complex plane. The First Isomorphism Theorem implies $\mathbb{C}^\times/N \simeq K$.

Example 2.18. The function $f : \mathbb{R}^\times \to \mathbb{R}^\times$ where $f(r) = r^2$ is a group homomorphism by Example 1.26. We have $\ker(f) = \{1, -1\}$ since these are the real numbers that square to 1. Let $K = \text{im}(f)$ be the subgroup of all positive real numbers. The First Isomorphism Theorem implies $\mathbb{R}^\times/\{1, -1\} \simeq K$.

Lemma 2.3. Let K and N be subgroups of G with N normal in G. Then

$$NK = \{nk : n \in N, k \in K\}$$

is a subgroup of G that contains N and K.

Proof. The identity element of NK is $e_G e_G$. Let $n_1k_1, n_2k_2 \in NK$. Since N is normal, $k_1n_2 = n_3k_1$ for some $n_3 \in N$. Thus

$$\begin{aligned} (n_1k_1)(n_2k_2) &= n_1(k_1n_2)k_2 \\ &= n_1(n_3k_1)k_2 \\ &= (n_1n_3)(k_1k_2) \in NK. \end{aligned}$$

Further, N normal implies that $(n_1k_1)^{-1} = k_1^{-1}n_1^{-1} = n_4k_1^{-1} \in NK$ for some $n_4 \in N$. For any $n \in N$ and $k \in K$, we have $n = ne_G \in NK$ and $k = e_Gk \in NK$. Therefore, NK is a subgroup of G that contains N and K. □

Of particular interest is the case when $G = NK$. Then we can build the group G out of possibly more recognizable subgroups.

Theorem 2.4 (Second Isomorphism Theorem)**.** Let K and N be subgroups of G with N normal in G. Then $N \cap K$ is a normal subgroup of K and $NK/N \simeq K/(N \cap K)$.

Proof. Let $a \in N \cap K$ and $k \in K$. Then $kak^{-1} \in K$ since $k, a, k^{-1} \in K$. Since N is normal in G, $ka = a_1k$ for some $a_1 \in N$. Thus $kak^{-1} = a_1kk^{-1} = a_1 \in N$. We conclude that $kak^{-1} \in N \cap K$ so $N \cap K$ is a normal subgroup of K.

Define the function $f : NK \to K/(N \cap K)$ as $f(nk) = (N \cap K)k$. There could be multiple ways of writing elements of NK so we need to check if f is well-defined. Let $n_1k_1 = n_2k_2$ for $n_i \in N$ and

$k_j \in K$. Then $f(n_1k_1) = (N \cap K)k_1$ while $f(n_2k_2) = (N \cap K)k_2$. However, $k_2k_1^{-1} = n_2^{-1}n_1 \in N \cap K$ so $(N \cap K)k_1 = (N \cap K)k_2$. Thus f is well-defined. Let $n_1k_1, n_2k_2 \in NK$. Since N is normal, $(n_1k_1)(n_2k_2) = nk_1k_2$ for some $n \in N$. Then

$$f((n_1k_1)(n_2k_2)) = f(nk_1k_2) = (N \cap K)k_1k_2 = f(n_1k_1)f(n_2k_2)$$

and f is a group homomorphism. Given some $(N \cap K)k$, we have $f(e_Gk) = (N \cap K)k$ so f is surjective. For $n \in N$, we have $f(ne_G) = (N \cap K)$ so $N \subset \ker(f)$. If $f(nk) = (N \cap K)$, then $k \in N \cap K$ which implies $nk \in N$. Thus $\ker(f) = N$. The First Isomorphism Theorem implies that $NK/\ker(f) = NK/N \simeq K/(N \cap K)$. □

End of lecture 11

Often, we will use a special case of the Second Isomorphism Theorem where $N \cap K = \{e_G\}$.

Corollary 2.4. Let K and N be subgroups of G with $N \triangleleft G$. If $N \cap K = \{e_G\}$, then $NK/N \simeq K$.

The Second Isomorphism Theorem produces a useful order argument for finite groups G.

Corollary 2.5. Let K and N be subgroups of G with $N \triangleleft G$. If G is a finite group, then $|NK||N \cap K| = |N||K|$.

Proof. By the Second Isomorphism Theorem, $NK/N \simeq K/(N \cap K)$. Thus $|NK/N| = |K/(N \cap K)|$. We have $|NK/N| = |NK|/|N|$ and $|K/(N \cap K) = |K|/|N \cap K|$. By clearing denominators, $|NK||N \cap K| = |N||K|$. □

Example 2.19. Let $G = D_n$, $K = \langle s \rangle$, and $N = \langle r \rangle$. By Lemma 2.1, the index 2 subgroup N is normal. Lemma 2.3 proves that NK is a subgroup of G. In this case, every element of G can be written as r^is^j for $0 \leq i \leq n-1$ and $0 \leq j \leq 1$ so $G = NK$. Further, $N \cap K = \{e_G\}$. The Second Isomorphism Theorem implies $G/N = NK/N \simeq K$. In other words, the cosets $\{Ne_G, Ns\}$ under multiplication behave the same way as the elements $\{e_G, s\}$ of G.

The Third Isomorphism Theorem is a particularly useful case of the Correspondence Theorem when K is also a normal subgroup of G.

Theorem 2.5 (Third Isomorphism Theorem)**.** Let K and N be normal subgroups of G with $N \subset K \subset G$. Then K/N is a normal subgroup of G/N, and the quotient group $(G/N)/(K/N)$ is isomorphic to G/K.

Note that the cancellation of N in $(G/N)/(K/N)$ motivates the fraction notation for quotients. However, we have to be careful because this only works when K is also a normal subgroup of G.

Proof. The Correspondence Theorem for Normal Subgroups proves $K/N \triangleleft G/N$.

Define the function $f : G/N \to G/K$ as $f(Ng) = Kg$. We need to check whether f is well-defined. Let $Ng_1 = Ng_2$ for $g_i \in G$ so $g_2g_1^{-1} \in N$. Then $f(Ng_1) = Kg_1$ and $f(Ng_2) = Kg_2$. Since $N \subset K$, we have $g_2g_1^{-1} \in K$ and f is well-defined. For $Ng_1, Ng_2 \in G/N$, we have

$$f((Ng_1)(Ng_2)) = f(N(g_1g_2)) = K(g_1g_2) = (Kg_1)(Kg_2) = f(Ng_1)f(Ng_2)$$

so f is a group homomorphism. Given $Kg \in G/K$, we have $f(Ng) = Kg$ so f is surjective. If $f(Ng) = Kg = K$, then $g \in K$ and $Ng \in K/N$. Thus $\ker(f) \subset K/N$. For $Nk \in K/N$, $f(Nk) = Kk = K$ so $K/N \subset \ker(f)$ and $\ker(f) = K/N$. The First Isomorphism Theorem implies $(G/N)/(K/N) \simeq G/K$. □

Example 2.20. Let m and n be integers such that $n|m$. Since $\mathbb{Z}$ is abelian, we have a chain of normal subgroups $m\mathbb{Z} \subset n\mathbb{Z} \subset \mathbb{Z}$. The Third Isomorphism Theorem gives an isomorphism

$$f : (\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$$

where $f(n\mathbb{Z}/m\mathbb{Z} + (m\mathbb{Z} + k)) = n\mathbb{Z} + k$. In other words, if you reduce modulo m and then modulo n, it is the same thing as reducing modulo n to begin with.

2.4.1. *Simple Groups.* The techniques developed in this section often require normal subgroups of a group G. A particularly interesting and tricky example of groups are those without any normal subgroups.

Definition 2.9. Let G be a group. Then G is *simple* if its only normal subgroups are $\{e\}$ and G.

Example 2.21. Let p be prime. By Example 2.4, a group G of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Any subgroup of G will have order 1 or p by Lagrange's Theorem. In other words, the element is either the identity or a generator. Thus $\mathbb{Z}/p\mathbb{Z}$ is simple.

Proposition 2.13. A group G is simple abelian if and only if G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proof. ($\Rightarrow$) Suppose G is a simple abelian group. Since G is abelian, every subgroup of G is normal. Thus G has no non-trivial subgroups so $\langle a\rangle = G$ for a non-identity element $a \in G$. If $\langle a\rangle$ is not finite, then $\langle a\rangle \simeq \mathbb{Z}$ by Proposition 1.16(1). The group $\mathbb{Z}$ is not simple so $\langle a\rangle$ is finite. Let $|a| = n$ and $n = td$. Then $\langle a^t\rangle$ is a subgroup of G of order d by Proposition 1.4(3). Therefore, G is a cyclic group of order p or $G \simeq \mathbb{Z}/p\mathbb{Z}$.

($\Leftarrow$) See Example 2.21. □

Example 2.22. Let G be a simple group. Let $f : G \to H$ be a group homomorphism. We know that $\ker(f)$ is normal in G by Proposition 2.10. By simplicity of G, $\ker(f) = \{e_G\}$ or $\ker(f) = G$. Thus f is injective by Proposition 2.11 or $f(a) = e_H$ for all $a \in G$. A kernel of a group homomorphism out of a simple group is all or nothing.

2.5. **The Symmetric and Alternating Groups.** Group theory began with the study of permutations and groups of permutations. The abstract definition of a group came later and may appear to be far more general than the concept of a group of permutations. The next theorem shows that this is not the case, however.

Let $A(G)$ be the set of bijective functions from G to G. These functions need not be homomorphisms. On the homework, we proved that $A(G)$ is group under composition. The proof of Cayley's Theorem is based on an injection from G to $A(G)$.

Theorem 2.6 (Cayley's Theorem)**.** Every group G is isomorphic to a group of permutations

Proof. Let $a \in G$. Define the set map $\varphi_a : G \to G$ as $\varphi_a(x) = ax$. Since a has an inverse, $\varphi_{a^{-1}} \circ \varphi_a = \varphi_a \circ \varphi_{a^{-1}}$ is the identity set map. Thus φ_a is a bijection of sets and, thus, an element of $A(G)$.

Define $f : G \to A(G)$ as $f(a) = \varphi_a$. For $a, b \in G$, we have $f(ab) = \varphi_{ab}$. We have

$$\varphi_{ab}(x) = (ab)x = a(bx) = \varphi_a(\varphi_b(x))$$

so $\varphi_{ab} = \varphi_a \circ \varphi_b$. Then $f(ab) = f(a)f(b)$ and f is a group homomorphism. Suppose $f(a) = f(b)$ for $a, b \in G$ so $\varphi_a(x) = \varphi_b(x)$ for all $x \in G$. Thus $ax = bx$. Multiply on the right by x^{-1} to obtain $a = b$. Therefore, f is an injective group homomorphism. By the First Isomorphism Theorem, $G \simeq \mathrm{im}(f) \subset A(G)$. □

Corollary 2.6. Every finite group G of order n is isomorphic to a subgroup of S_n.

Proof. By Cayley's Theorem, G is isomorphic to a subgroup of $A(G)$. Since G is a set of n elements, $A(G) \simeq S_n$. □

Definition 2.10. We refer to an element $(a_1 a_2 \dots a_k) \in S_n$ as a *k-cycle*. Two cycles σ_1 and σ_2 are *disjoint* if they have no elements in common.

Example 2.23. The cycles (12) and (34) are disjoint in S_4.

Example 2.24. The inverse of a k-cycle $(a_1 a_2 a_3 \dots a_{k-1} a_k)$ is $(a_1 a_k a_{k-1} \dots a_3 a_2)$.

Proposition 2.14. Let $\sigma = (a_1 \dots a_k)$ and $\tau = (b_1 \dots b_\ell)$ be disjoint cycles of S_n. Then $\sigma\tau = \tau\sigma$.

Proof. Let $c \in X_n$. Then $\sigma(c) = c$ or $\tau(c) = c$. Without loss of generality, assume $\tau(c) = c$. Then $(\sigma\tau)(c) = \sigma(c)$. Since σ and τ are disjoint, $\tau(\sigma(c)) = \sigma(c)$. Thus $(\sigma\tau)(c) = (\tau\sigma)(c)$ for all $c \in X_n$. □

Proposition 2.15. Every permutation of S_n is the product of disjoint cycles.

Proof. Let $\sigma \in S_n$. For each element $c \in X_n$, trace where c goes via powers of σ to produce the k-cycle $\tau = (c\ \sigma(c)\ \sigma^2(c)\ \dots\ \sigma^{k-1}(c))$. For each element of X_n that is not in τ, perform the same process. Eventually each element of X_n is in one and only one of the cycles. Then σ is the product of these disjoint cycles. □

End of lecture 12

Proposition 2.16. The order of the permutation τ in S_n is the least common multiple of the lengths of the disjoint cycles whose product is τ.

Proof. Let $\tau = \prod_{i=1}^{\ell} \sigma_i$ for disjoint k_i-cycles σ_i and $m = \mathrm{lcm}(k_1, \dots, k_\ell)$. We have $\sigma_i^m = e$ for all $1 \le i \le \ell$. Since the σ_i are disjoint, they will commute by Proposition 2.14. Thus

$$\tau^m = \left(\prod_{i=1}^{\ell} \sigma_i\right)^m = \prod_{i=1}^{\ell} \sigma_i^m = e.$$

Assume that $\tau^M = e$. Then $\tau^M = \prod_{i=1}^{\ell} \sigma_i^M$. The σ_i are disjoint so σ_i^M must be the identity for each $1 \le i \le \ell$. By Proposition 1.4(1), k_i divides M for each $1 \le i \le \ell$. Thus $m|M$ and $|\tau| = m$. □

2.5.1. *Alternating Groups.*

Definition 2.11. A 2-cycle of S_n is called a *transposition*.

Proposition 2.17. Every element of S_n is a product of (not necessarily disjoint) transpositions.

Proof. By Proposition 2.15, every element of S_n is a product of disjoint cycles. Thus we only need to show that a k-cycle is a product of transpositions:

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k).$$

□

Definition 2.12. A permutation is *even* if it can be written as a product of an even number of transpositions. Likewise, a permutation is *odd* if it can be written as a product of an odd number of transpositions.

Strictly from the definitions, a permutation could be both even and odd at this point. We will prove that this cannot occur in the following results.

Lemma 2.4. The identity element is even but not odd.

Proof. We can write the identity permutation as $(12)(12)$ so it is even. Assume $e = \tau_k \cdots \tau_2 \tau_1$ for transpositions τ_i and k odd. Let $c \in X_n$ and τ_r be the lowest index transposition for which c appears. Write $\tau_r = (cd)$ for $d \in X_n$. If $r = k$, then e does not fix c, a contradiction. Thus $r < k$.

Let c, d, x, y be distinct elements of X_n. Then τ_{r+1} has one of the following forms.

(1) (xy)
(2) (xd)
(3) (cy)
(4) (cd)

In Case (1), Proposition 2.14 implies that $(xy)(cd) = (cd)(xy)$ so we can move τ_r to the left one position. In Case (2), $(xd)(cd) = (xc)(xd)$ so the first appearance of c can be moved to the left one position. In Case (3), $(cy)(cd) = (cd)(dy)$ so the first appearance of c can be moved to the left one position. By repeated use of Cases (1)-(3), we will eventually be in Case (4). Then $\tau_{r+1}\tau_r = (cd)(cd)$ is the identity. We can write the identity with two fewer transpositions. Repeat this procedure for any element of X_n to eventually reduce to a single transposition. This is a contradiction since the identity fixes each element of X_n. Therefore, the identity is an even permutation. □

Proposition 2.18. Each permutation in S_n is exclusively even or odd.

Proof. Assume $\alpha \in S_n$ can be written as a product of transpositions $\sigma_1 \cdots \sigma_k$ and transpositions $\tau_1 \cdots \tau_\ell$. Then

$$e = \alpha\alpha^{-1} = (\sigma_1 \cdots \sigma_k)(\tau_1 \cdots \tau_\ell)^{-1} = \sigma_1 \cdots \sigma_k \tau_\ell^{-1} \cdots \tau_1^{-1}$$

is a description of the identity with $k + \ell$ transpositions. Lemma 2.4 implies that $k + \ell$ is even so k and ℓ are either both even or both odd. □

Definition 2.13. The *alternating group* A_n is the subset of all even permutations of S_n.

Proposition 2.19. A_n is a group of order $\frac{n!}{2}$ (for $n \geq 2$).

Proof. By Lemma 2.4, $e \in A_n$ so A_n is non-empty. Let $\alpha, \beta \in A_n$. Then $\alpha = \sigma_1 \cdots \sigma_{2k}$ can be written as a product of $2k$ transpositions and $\beta = \tau_1 \cdots \tau_{2\ell}$ can be written as a product of 2ℓ transpositions by Proposition 2.17. We conclude that

$$\begin{aligned} \alpha\beta &= (\sigma_1 \cdots \sigma_{2k})(\tau_1 \cdots \tau_{2\ell}) \\ &= \sigma_1 \cdots \sigma_{2k} \tau_1 \cdots \tau_{2\ell} \end{aligned}$$

is a product of $2(k+\ell)$ transpositions. Thus A_n is closed under the group operation. The inverse of α can be written $\alpha^{-1} = \sigma_{2k}^{-1} \cdots \sigma_1^{-1}$ so A_n is closed under inverses.

In the case that $n = 1$, $A_1 = S_1$ is trivial. Let $n \geq 2$. Define $f : A_n \to B_n$ by $f(\alpha) = (12)\alpha$ where B_n is the set of odd permutations of S_n. Assume $f(\alpha) = f(\beta)$ so $(12)\alpha = (12)\beta$. Multiply on the left by (12) to obtain $\alpha = \beta$. Thus f is injective. For $\gamma \in B_n$, the permutation is $(12)\gamma \in A_n$. Then $f((12)\gamma) = (12)(12)\gamma = \gamma$ so f is surjective. Therefore, $|A_n| = |B_n|$. Each permutation is either even or odd so $|S_n| = |A_n| + |B_n|$ and $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. □

End of lecture 13

2.5.2. *The Simplicity of the Alternating Group.*

Example 2.25. The group A_4 is not simple. We will prove on the homework that the subgroup $\{e, (12)(34), (13)(24), (14)(23)\}$ is normal in A_4.

Theorem 2.7. For $n \neq 4$, the group A_n is simple.

Corollary 2.7. For $n \geq 5$, the only normal subgroups of S_n are $\{e\}$, A_n, and S_n.

Section 8.5 of Hungerford has the whole proof of the theorem. In the interest of time, we will only prove two helpful lemmas.

Lemma 2.5. Every element of A_n for $n \geq 3$ is a product of 3-cycles.

Proof. Let $\alpha \in A_n$. Then α can be written as a product of transpositions by Proposition 2.17. Let $a, b, c, d \in X_n$. A pair of transpositions has the form $(ab)(ac)$ or $(ab)(cd)$.

$$(ab)(ac) = (acb)$$
$$(ab)(cd) = (adb)(adc)$$

Since there are an even number of transpositions in the description of α, we pair them up and follow the above formulas to write α as a product of 3-cycles. □

Lemma 2.6. Let $n \geq 3$. If N is a normal subgroup of A_n and N contains a 3-cycle, then $N = A_n$.

Proof. Without loss of generality, assume $(123) \in N$. Then $(123)^2 = (132) \in N$ as well. Let $x = (12)(3k)$ for $k \in X_n$ and $k > 3$. Since N is normal, $x(123)x^{-1} \in N$. We have

$$(12)(3k)(123)(3k)(12) = (1k2) \in N.$$

The inverse of $(1k2) = (12k) \in N$ as well. Thus N contains all 3-cycles of the form $(1k2)$ and $(12k)$. For $a, b, c \in X_n$ with $a, b, c \geq 3$, every 3-cycle is either of the form or inverse to one of the form $(1a2)$, $(1ab)$, $(2ab)$, or (abc).

$$(1ab) = (12b)(1a2) \in N$$
$$(2ab) = (1b2)(12a) \in N$$
$$(abc) = (1a2)(12c)(1b2)(12a) \in N$$

Thus N contains all 3-cycles of S_n, and Lemma 2.5 proves that $N = A_n$. □

End of midterm material

3. Topics in Group Theory

3.1. **Direct Products.** If G and H are groups, then their Cartesian product $G \times H$ is also a group, with the operation defined coordinate-wise. In this section we extend this notion to more than two groups. Then we examine the conditions under which a group is isomorphic to a direct product of certain of its subgroups. We will then define a more general product structure called the semi-direct product. The semi-direct product can simplify the classification of finite groups of small order.

Definition 3.1. If $G_1, \ldots, G_n$ are groups, then the Cartesian product $G_1 \times \cdots \times G_n$ is a group under coordinate-wise multiplication. For $a_i, b_i \in G_i$,

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

The identity element is $(e_{G_1}, \ldots, e_{G_n})$ and the inverse of $(a_1, \ldots, a_n)$ is $(a_1^{-1}, \ldots, a_n^{-1})$. We call the group $G_1 \times \cdots \times G_n$ the *direct product*.

Example 3.1. Note that G_i is not directly a subgroup of the direct product $G = G_1 \times \cdots \times G_n$. However, there is a subgroup of the direct product that is isomorphic to G_i. Define the inclusion $\iota_i : G_i \to G$ as $\iota_i(a_i) = (0, \ldots, a_i, \ldots, 0)$ where $a_i \in G_i$ is placed in the ith component of the direct product. The inclusion is an injective group homomorphism so the First Isomorphism Theorem implies that $G_i \simeq \mathrm{im}(\iota_i)$, which is a subgroup of the direct product. In particular, $\mathrm{im}(\iota_i) = (0, \ldots, G_i, \ldots, 0)$.

Example 3.2. If $G_1, \ldots, G_n$ are finite groups, then $|G_1 \times \cdots \times G_n| = \prod_{i=1}^n |G_i|$ and the direct product is finite.

Example 3.3. The direct product $G_1 \times \cdots \times G_n$ is abelian if and only if G_i is abelian for each $1 \leq i \leq n$.

Example 3.4. Let $G = \mathbb{Z}/6\mathbb{Z}$. Then $M = \langle \overline{3} \rangle$ and $N = \langle \overline{2} \rangle$ are normal subgroups of G since G is abelian. The direct product $M \times N$ is cyclic generated by $(\overline{3}, \overline{2})$ so $M \times N \simeq \mathbb{Z}/6\mathbb{Z}$ by Proposition 1.16. Note also that every element in $\mathbb{Z}/6\mathbb{Z}$ can be written uniquely as a sum of an element in M and an element in N. Consequently, we can describe $\mathbb{Z}/6\mathbb{Z}$ internally as a product of subgroups without making use of the externally defined direct product.

The following lemma will help to prove in which scenarios a group is isomorphic to a direct product of subgroups.

Lemma 3.1. Let M and N be normal subgroups of G with $M \cap N = \{e\}$. If $a \in M$ and $b \in N$, then $ab = ba$.

Proof. Consider $aba^{-1}b^{-1}$. Since M is normal, $bab^{-1} \in M$ so $aba^{-1}b^{-1} \in M$. Similarly, $aba^{-1} \in N$ so $aba^{-1}b^{-1} \in N$. Since $M \cap N$ is trivial, we conclude that $aba^{-1}b^{-1} = e$ or $ab = ba$. □

Recall that a product of subgroups is given by $MN = \{mn \in G : m \in M, n \in N\}$.

Proposition 3.1. Let $N_1, \ldots, N_k$ be normal subgroups of a group G such that $G = N_1 \cdots N_k$ and $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) = \{e_G\}$ for each $1 \leq i \leq k$. Then G is isomorphic to the direct product $N_1 \times \cdots \times N_k$.

Proof. Define $f : N_1 \times \cdots \times N_k \to G$ as $f(a_1, \ldots, a_k) = a_1 \cdots a_k$. Let $a_i, b_i \in N_i$. By Lemma 3.1,

$$\begin{aligned} f((a_1, \ldots, a_k)(b_1, \ldots, b_k)) &= f(a_1 b_1, \ldots, a_k b_k) \\ &= (a_1 b_1) \cdots (a_k b_k) \\ &= (a_1 \cdots a_k)(b_1 \cdots b_k) \\ &= f(a_1, \ldots, a_k) f(b_1, \ldots, b_k). \end{aligned}$$

Thus f is a homomorphism. Assume $f(a_1, \ldots, a_k) = e_G$. Then $a_1 \cdots a_k = e_G$ or

$$a_i = a_1^{-1} \cdots a_{i-1}^{-1} a_k^{-1} \cdots a_{i+1}^{-1}.$$

Since $a_i \in N_i$ and $a_1^{-1} \cdots a_{i-1}^{-1} a_k^{-1} \cdots a_{i+1}^{-1} = a_1^{-1} \cdots a_{i-1}^{-1} a_{i+1}^{-1} \cdots a_k^{-1} \in (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k)$ by Lemma 3.1, we conclude $a_i = e_G$ for each $1 \leq i \leq k$. Thus f is injective. Since $G = N_1 \cdots N_k$, f is surjective. Therefore, f is an isomorphism. □

End of lecture 14

Corollary 3.1. Let G be a group with normal subgroups M and N such that $M \cap N = \{e_G\}$ and $MN = G$. Then $G \simeq M \times N$.

Example 3.5. The multiplicative group $G = (\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ can be written as a direct product of two cyclic groups. Let $M = \langle 11 \rangle = \{1, 11\}$ and $N = \langle 2 \rangle = \{1, 2, 4, 8\}$. Since G is abelian, M and N are normal. Further, $M \cap N = \{1\}$. Corollary 3.1 implies

$$(\mathbb{Z}/15\mathbb{Z})^\times \simeq M \times N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

3.1.1. *Semi-direct Product.* Many group examples cannot be written as a direct product of subgroups. The semi-direct product will allow us to describe a larger number of groups in terms of subgroups.

Example 3.6. Every proper subgroup of D_4 has order 1, 2, or 4 by Lagrange's Theorem. Thus every subgroup is abelian by Examples 2.4 and 2.5. Since D_4 is not abelian, D_4 cannot be a direct product of subgroups.

Recall that in homework problem Section 7.4 # 36, we prove the following result.

Proposition 3.2. For a group G, an *automorphism* of G is a group isomorphism $f : G \to G$. The set of all automorphisms of G, denoted $\mathrm{Aut}(G)$, is a group under composition.

Definition 3.2. Let H and N be groups. Let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism. Then the semi-direct product $N \rtimes_\varphi H$ is the set $N \times H$ with the following operation

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2).$$

Proposition 3.3. The semi-direct product $N \rtimes_\varphi H$ is a group with identity (e_N, e_H) and

$$(n, h)^{-1} = (\varphi(h)^{-1}(n^{-1}), h^{-1}) = (\varphi(h^{-1})(n^{-1}), h^{-1}).$$

Proof. The multiplication is associative. The identity element satisfies

$$\begin{aligned}
(n, h)(e_N, e_H) &= (n\varphi(h)(e_N), h) \\
&= (ne_N, h) \\
&= (n, h) \\
(e_N, e_H)(n, h) &= (e_N \varphi(e_H)(n), h) \\
&= (e_N \mathrm{id}_N(n), h) \\
&= (n, h).
\end{aligned}$$

The inverse element satisfies

$$\begin{aligned}(n,h)(\varphi(h)^{-1}(n^{-1}),h^{-1}) &= (n\varphi(h)(\varphi(h)^{-1}(n^{-1})),e_H)\\ &= (nn^{-1},e_H)\\ &= (e_N,e_H)\\ (\varphi(h)^{-1}(n^{-1}),h^{-1})(n,h) &= (\varphi(h)^{-1}(n^{-1})\varphi(h^{-1})(n),e_H)\\ &= (\varphi(h^{-1})(n^{-1})\varphi(h^{-1})(n),e_H)\\ &= (\varphi(h^{-1})(n^{-1}n),e_H)\\ &= (\varphi(h^{-1})(e_N),e_H)\\ &= (e_N,e_H).\end{aligned}$$

□

Example 3.7. We will write D_4 as a semi-direct product of subgroups. Let $N=\langle r\rangle$ and $H=\langle s\rangle$. The group homomorphism $h: N\to N$ defined by $h(r)=r^3$ is an automorphism of N. Define $\varphi: H\to \mathrm{Aut}(N)$ as $\varphi(s)=h$. The multiplication in $N\rtimes_\varphi H$ works as follows.

$$\begin{aligned}(r,e_H)(e_N,s) &= (r\varphi(e_H)(e_N),s)\\ &= (r\mathrm{id}_N(e),s)\\ &= (r,s)\\ (e_N,s)(r,e_H) &= (e_N\varphi(s)(r),s)\\ &= (e_Nh(r),s)\\ &= (r^3,s).\end{aligned}$$

By identifying $(a,b)\in N\rtimes_\varphi H$ with $ab\in D_4$, we can prove that $N\rtimes_\varphi H\simeq D_4$.

The symbol $\rtimes$ is a combination of the direct product symbol and the normal subgroup symbol. The next result motivates the notation since N is isomorphic to a normal subgroup of the semi-direct product.

Proposition 3.4. The subgroup $\{(n,e_H): n\in N\}$ is a normal subgroup of $N\rtimes_\varphi H$.

Proof. Let $k,n\in N$ and $h\in H$. Then

$$\begin{aligned}(k,h)(n,e_H)(k,h)^{-1} &= (k\varphi(h)(n),h)(\varphi(h)^{-1}(k^{-1}),h^{-1})\\ &= (k\varphi(h)(n)\varphi(h)(\varphi(h)^{-1}(k^{-1})),e_H)\\ &= (k\varphi(h)(n)k^{-1},e_H).\end{aligned}$$

Since k and $\varphi(h)(n)$ are elements of N, we conclude that the desired subgroup is normal in $N\rtimes_\varphi H$. □

Remark 3.1. There is some intuition for building a group out of the semi-direct product of subgroups. Take a normal subgroup N and a subgroup H of G. As motivation, observe

$$\begin{aligned}(e_N,h)(n,e_H)(e_N,h)^{-1} &= (\varphi(h)(n),h)(\varphi(h)^{-1}(e_N^{-1}),h^{-1})\\ &= (\varphi(h)(n)\varphi(h)(\varphi(h)^{-1}(e_N^{-1})),e_H)\\ &= (\varphi(h)(n),e_H).\end{aligned}$$

The element $\varphi(h)\in\mathrm{Aut}(N)$ represents how the conjugation by h behaves in G.

Proposition 3.5. Let H be a subgroup of G and N a normal subgroup of G. If $G=NH$ and $N\cap H=\{e_G\}$, then $G\simeq N\rtimes_\varphi H$ for some $\varphi: H\to\mathrm{Aut}(N)$.

Proof. Let $\varphi : H \to \mathrm{Aut}(N)$ be the group homomorphism $\varphi(h) = (n \mapsto hnh^{-1})$. Define

$$f : N \rtimes_\varphi H \to G$$

as $f(n,h) = nh$. We have

$$\begin{aligned} f((n_1,h_1)\cdot(n_2,h_2)) &= f(n_1\varphi(h_1)(n_2), h_1h_2) \\ &= f(n_1h_1n_2h_1^{-1}, h_1h_2) \\ &= (n_1h_1n_2h_1^{-1})(h_1h_2) \\ &= n_1h_1n_2h_2 \\ &= f(n_1,h_1)f(n_2,h_2) \end{aligned}$$

so f is a group homomorphism. Let $f(n,h) = e_G$ so $nh = e_G$. Then $h = n^{-1} \in N \cap H$. We conclude that $h = n = e_G$ and f is injective. Since $G = NH$, f is surjective. Therefore, $G \simeq N \rtimes_\varphi H$. □

The following shows that the semi-direct product is a generalization of the usual direct product.

Example 3.8. Let $\varphi : H \to \mathrm{Aut}(N)$ be the group homomorphism $\varphi(h) = \mathrm{id}_N$. The multiplication in the semi-direct product is

$$\begin{aligned} (n_1,h_1)\cdot(n_2,h_2) &= (n_1\varphi(h_1)(n_2), h_1h_2) \\ &= (n_1\mathrm{id}_N(n_2), h_1h_2) \\ &= (n_1n_2, h_1h_2). \end{aligned}$$

Thus $N \rtimes_\varphi H \simeq N \times H$ and the semi-direct product is the usual direct product.

Example 3.9. Let $N = \mathbb{Z}/5\mathbb{Z}$ and $H = \mathbb{Z}/6\mathbb{Z}$. We want to find all possibilities for $N \rtimes_\varphi H$. As we know from the homework, $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times = \{1,2,3,4\}$. The automorphism that $i \in (\mathbb{Z}/5\mathbb{Z})^\times$ represents is the unique group isomorphism $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ defined by sending $\overline{1}$ to $\overline{i}$. A generator of H has order 6 so $\varphi(\overline{1})$ must have order 1, 2, 3, or 6. The elements 2 and 3 are order 4 in $(\mathbb{Z}/5\mathbb{Z})^\times$ so $\varphi(\overline{1}) = 1$ or $\varphi(\overline{1}) = 4$. In the first case, $\varphi(\overline{1}) = 1$ represents the identity automorphism. We obtain $N \rtimes_\varphi H = N \times H$ by Example 3.8. In the second case, $\varphi(\overline{1}) = 4$ represents the automorphism of N where $\overline{1}$ maps to $\overline{4}$. We have a multiplication example

$$\begin{aligned} (\overline{0},\overline{1})\cdot(\overline{2},\overline{5}) &= (\overline{0} + \varphi(\overline{1})(\overline{2}), \overline{0}) \\ &= (\overline{3},\overline{1}) \\ (\overline{2},\overline{5})\cdot(\overline{0},\overline{1}) &= (\overline{2} + \varphi(\overline{5})(\overline{0}), \overline{0}) \\ &= (\overline{2},\overline{0}) \end{aligned}$$

so $N \rtimes_\varphi H$ is a non-abelian group of order 30.

End of lecture 15

3.2. **Finite Abelian Groups.** We have the tools to classify all finite abelian groups. We will prove that every finite abelian group is isomorphic to a direct product of cyclic groups.

Definition 3.3. If G is an abelian group and p is a prime integer, let $G(p)$ be the set of all elements whose order is some power of p. In other words,

$$G(p) = \{a \in G : |a| = p^k \text{ for some } k \geq 0\}.$$

We call $G(p)$ the *p-primary subgroup of* G.

Proposition 3.6. The subset $G(p)$ of an abelian group G is a subgroup.

Proof. The identity has order $1 = p^0$ so $G(p)$ is non-empty. Let $a, b \in G(p)$ with $|a| = p^k$ and $|b| = p^\ell$. Then $(ab)^{p^{k+\ell}} = a^{p^{k+\ell}} b^{p^{k+\ell}} = e_G e_G = e_G$ since G is abelian. We conclude $|ab|$ divides $p^{k+\ell}$ by Proposition 1.4(1) so $|ab|$ is a power of p since p is prime. Thus $ab \in G(p)$, and $G(p)$ is closed under the group operation. The inverse a^{-1} to $a \in G(p)$ satisfies $(a^{-1})^{p^k} = (a^{p^k})^{-1} = e_G^{-1} = e_G$ so $|a^{-1}|$ divides p^k and $a^{-1} \in G(p)$. Therefore, $G(p)$ is a subgroup of G. □

Example 3.10. If $G = \mathbb{Z}/12\mathbb{Z}$, then $G(2) = \{0, 3, 6, 9\}$ and $G(3) = \{0, 4, 8\}$.

If $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then $G(3) = G$ since every element has order a power of 3.

Lemma 3.2. Let G be an abelian group with $a \in G$ an element of finite order. Let $\{p_i\}_{i=1}^t$ be the distinct primes that divide $|a|$. Then $a = a_1 \cdots a_t$ for some $a_i \in G(p_i)$.

Proof. We will proceed by induction on the number t of distinct primes that divide $|a|$. If $t = 1$, then $a \in G(p_1) = G$ and the result holds. Assume the result holds for $t \leq k-1$, and we will prove it for $t = k$. We have $|a| = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and $r_i > 0$. Let $m = p_2^{r_2} \cdots p_k^{r_k}$ and $n = p_1^{r_1}$. We have $\gcd(m, n) = 1$ so $1 = mu + nv$ for some $u, v \in \mathbb{Z}$. Then

$$a = a^{mu+nv} = a^{mu} a^{nv}.$$

Since $|a| = mn$, $a^{mu} \in G(p_1)$. Define $a_1 = a^{mu}$. Similarly, $|a^{nv}|$ is divisible by only the distinct primes $p_2, \ldots, p_k$. By the inductive hypothesis, $a^{nv} = a_2 \cdots a_k$ for $a_i \in G(p_i)$. Therefore, $a = a_1 a_2 \cdots a_k$ as desired. □

Proposition 3.7. If G is a finite abelian group, then

$$G \simeq G(p_1) \times \cdots \times G(p_t)$$

where $p_1, \ldots, p_t$ are the distinct primes that divide $|G|$.

Proof. By Lemma 3.2, $G = G(p_1) \cdots G(p_t)$. We will now show that

$$G(p_i) \cap (G(p_1) \cdots G(p_{i-1}) G(p_{i+1}) \cdots G(p_k)) = \{e_G\}$$

for each $1 \leq i \leq k$. Let $H = G(p_1) \cdots G(p_{i-1}) G(p_{i+1}) \cdots G(p_t)$. Let $a \in G(p_i) \cap H$ so $|a| = p_i^{r_i}$ for some $r_i \geq 0$. Further, $a = a_1 \cdots a_{i-1} a_{i+1} \cdots a_t$ for $a_j \in G(p_j)$. By Lemma 1.2, $|a|$ divides $\operatorname{lcm}(|a_1|, \ldots, |a_{i-1}|, |a_{i+1}|, \ldots, |a_t|)$, which is a product of powers of $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_t$. The only way this is possible is if $|a| = 1$ and $a = e_G$. Apply Proposition 3.1 to complete the proof. □

Definition 3.4. A group G of order p^k is a *finite p-group.*

An *element of maximal order* a in a finite p-group G is one for which $|b| \leq |a|$ for all $b \in G$.

Lemma 3.3. Let G be a finite abelian p-group and a an element of maximal order in G. Then there is a subgroup K of G such that $G \simeq \langle a \rangle \times K$.

The proof of Lemma 3.3 is technical and too long for lecture. We will outline the proof, and the rest can be found as Hungerford Lemma 9.6.

Proof. Consider the set S of all subgroups H of G for which $\langle a\rangle \cap H = \{e_G\}$. S is non-empty since $\langle e_G\rangle \in S$. With G finite, there is a maximal element $K \in S$. If we show $\langle a\rangle K = G$, then Corollary 3.1 would imply that $G \simeq \langle a\rangle \times K$.

Assume $\langle a\rangle K \neq G$. Then there is some non-identity $b \in G$ for which $b \notin \langle a\rangle K$. Since G is a p-group, there is some p^j for which $b^{p^j} = e_G \in \langle a\rangle K$. Let k be the smallest positive integer for which $b^{p^k} \in \langle a\rangle K$. Then $c = b^{p^{k-1}} \notin \langle a\rangle K$ but $c^p \in \langle a\rangle K$. With some work and the maximality of a, we can show that $c \in \langle a\rangle K$, contradicting the choice of c. Therefore, $\langle a\rangle K = G$. □

Theorem 3.1 (Fundamental Theorem of Finite Abelian Groups)**.** Every finite abelian group G is the direct product of cyclic groups, each of prime power order.

Proof. By Proposition 3.7, G is isomorphic to the direct product of its subgroups $G(p_i)$, one for each p_i dividing $|G|$. To complete the proof, we need to show that each finite abelian p-group is a direct product of finite cyclic p-groups.

We proceed by induction on $|H|$. If $|H| = p$, then $H \simeq \mathbb{Z}/p\mathbb{Z}$ by Example 2.4. Assume the result holds for every finite abelian p-group of order less than that of H. Let $a \in H$ be an element of maximal order p^k in H. Then Lemma 3.3 implies there is a subgroup K of H for which $H \simeq \langle a\rangle \times K$. By the inductive hypothesis, K is isomorphic to a direct product of finite cyclic p-groups. Therefore, H is isomorphic to a direct product of finite cyclic p-groups. □

End of lecture 16

Definition 3.5. The order of the cyclic factors in the Fundamental Theorem of Finite Abelian Groups are the *elementary divisors* of a finite abelian group G.

A corollary to Lagrange's Theorem states that the order of each element divides the order of a finite group. When k divides the order of a finite group, do we have an element of that order? Cauchy's Theorem for Finite Abelian Groups provides a partial converse to the corollary to Lagrange's Theorem when a group is finite abelian. We will eventually extend this result to all finite groups.

Corollary 3.2 (Cauchy's Theorem for Finite Abelian Groups)**.** If G is a finite abelian group G and p is a prime dividing the order of G, then G contains an element of order p.

Proof. By the Fundamental Theorem of Finite Abelian Groups, we can write G as a product of cyclic groups

$$G \simeq G_1 \times \cdots \times G_m.$$

There is some cyclic component $\mathbb{Z}/p^k\mathbb{Z}$, say G_1 without loss of generality, that contains an element a of order p. Then $(a, e_{G_2}, \ldots, e_{G_m})$ is an element of order p in G. □

The Fundamental Theorem of Finite Abelian Groups reduces the description of finite abelian groups to a question of elementary number theory.

Example 3.11. Let G be an abelian group of order 36. We can factor $36 = 2^2 \cdot 3^2$. By the Fundamental Theorem of Finite Abelian Groups, G is isomorphic to one of the following.

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

We can verify that no two of the groups are isomorphic by counting elements of certain orders.

Note that one of the groups in the list of Example 3.11 must be cyclic of order 36. The next result will help us determine which groups in such a list are cyclic.

Lemma 3.4. If $\gcd(m,n)=1$, then $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/(mn)\mathbb{Z}$.

Proof. The order of $(\overline{1},\overline{1})$ in $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/(mn)\mathbb{Z}$ is the smallest $t\in\mathbb{Z}$ such that

$$t(1,1)=(\overline{t},\overline{t})=(\overline{0},\overline{0}).$$

Then $t\equiv 0 \pmod m$ and $t\equiv 0 \pmod n$. We have $m|t$ and $n|t$. Since $\gcd(m,n)=1$, $(mn)|t$. The order of $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ is mn so $(\overline{1},\overline{1})$ generates the group and $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ is cyclic. Therefore, $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/(mn)\mathbb{Z}$. □

Proposition 3.8. Let $n=p_1^{n_1}\cdots p_k^{n_k}$ with the p_i distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/p_1^{n_1}\times\cdots\times\mathbb{Z}/p_k^{n_k}\mathbb{Z}.$$

Proof. We will proceed by induction on n. By Example 2.4, the result holds for $n=2$. Assume that the result holds for all groups of order less than n. Apply Lemma 3.4 to $p_1^{n_1}$ and $m=p_2^{n_2}\cdots p_k^{n_k}$. Then $\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/p_1^{n_1}\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. The inductive hypothesis provides the result. □

Example 3.12. Consider the group $G=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$. Arrange the prime powers of the cyclic factors by size where each prime has a row as follows.

2	4	4
	3	3
		5

Reorganize by multiplying the elements in each column.

2	4	4
	3	3
		5
2	12	60

Via this procedure, each number will divide the next as we move left to right. By Proposition 3.8, we have

$$G\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/60\mathbb{Z}.$$

Theorem 3.2 (Invariant Factors)**.** Every finite abelian group is the direct product of cyclic groups of orders $m_1,\ldots,m_t$ where m_{i-1} divides m_i for each $2\le i\le t$.

Definition 3.6. The $m_1,\ldots,m_t$ from a finite abelian group G are the *invariant factors* of G.

In order to prove the uniqueness of our elementary divisor and invariant factor descriptions of finite abelian groups, we prove the following lemma.

Lemma 3.5. Let G and H be abelian groups.

(1) The subset $pG=\{x^p : x\in G\}$ is a subgroup of G.
(2) If G and H are isomorphic, $pG\simeq pH$.
(3) If G is a finite abelian p-group, then $pG\neq G$.

Proof. (1) The element $e_G^p=e_G$ so G^p is non-empty. Let $a,b\in pG$. Then $a=x^p$ and $b=y^p$ and $ab=x^py^p=(xy)^p$. Thus pG is closed under the group operation. For $a=x^p$, we have $a^{-1}=(x^p)^{-1}=(x^{-1})^p$ so pG is closed under inverses. Therefore, pG is a subgroup of G.

(2) Let $f:G\to H$ be a group isomorphism. Then $f(x^p)=f(x)^p$ so $f(pG)\subset pH$. Since f is surjective, every element $h\in pH$ satisfies $h=y^p=f(x)^p=f(x^p)$. Therefore, $f(pG)=pH$, and f injective implies $pG\simeq pH$.

(3) Assume, first, that $G = \langle a \rangle$ is cyclic. Then $pG = \langle a^p \rangle$ and $pG \neq G$. By the Fundamental Theorem of Finite Abelian Groups, a general finite abelian group G is isomorphic to a direct product of cyclic groups C_i. For each cyclic component, $pC_i \neq C_i$ so $pG \neq G$ by (2). □

End of lecture 17

Theorem 3.3 (Uniqueness of Elementary Divisors)**.** Let G and H be finite abelian groups. Then G is isomorphic to H if and only if G and H have the same elementary divisors up to reordering.

Proof. ($\Rightarrow$) Assume $f : G \to H$ is a group isomorphism. Then a and $f(a)$ have the same order for each $a \in G$ so $f(G(p)) = H(p)$. Thus $G(p) \simeq H(p)$ via f, and we need only prove the result when G and H are p-groups.

Assume G and H are isomorphic p-groups. We will proceed by induction on the order of G to prove that G and H have the same elementary divisors. When $|G| = 2$, all groups of order 2 will have the same elementary divisors. Assume the result holds for all groups of order less than $|G|$. Suppose the elementary divisors of G and H are respectively

$$p^{n_1}, p^{n_2}, \ldots, p^{n_t}, p, \ldots, p$$
$$p^{m_1}, p^{m_2}, \ldots, p^{m_k}, p, \ldots, p$$

with each $m_i, n_j > 1$, r copies of p at the end of the list for G, and s copies of p at the end of the list for H. By Lemma 3.5, the elementary divisors of pG and pH are respectively

$$p^{n_1-1}, p^{n_2-1}, \ldots, p^{n_t-1}$$
$$p^{m_1-1}, p^{m_2-1}, \ldots, p^{m_k-1}.$$

By Lemma 3.5(3), $|pG| < |G|$ and $|pH| < |H|$. Apply the inductive hypothesis so $t = k$ and $n_i - 1 = m_i - 1$ or $n_i = m_i$. Since $|G|$ and $|H|$ are the products of the respective elementary divisors, $r = s$, and G and H have the same elementary divisors.

($\Leftarrow$) If G and H have the same elementary divisors, then $G \simeq H$ up to possibly rearranging cyclic factors. □

Theorem 3.4 (Uniqueness of Invariant Factors)**.** Let G and H be finite abelian groups. Then G is isomorphic to H if and only if G and H have the same invariant factors.

Example 3.13. We will classify up to isomorphism all the finite abelian groups of order 72 with elementary divisors. The prime factorization is $72 = 2^3 \cdot 3^2$. The possibilities for the 2-primary part are $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The possibilities for the 3-primary part are $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Thus a finite abelian group of order 72 is isomorphic to one of the following.

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

The following table shows how to obtain invariant factors for the last element on the list.

2	2	2
	3	3
2	6	6

The classification of finite abelian groups of order 72 via invariant factors is as follows.

$$\mathbb{Z}/72\mathbb{Z}$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$$
$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

3.3. **The Sylow Theorems.** Finite non-abelian groups are much more complicated than finite abelian groups. The Sylow Theorems provide the most useful tools for studying non-abelian finite groups. We will not prove the results in this section but, instead, focus on applications. The proofs can be found in the next section.

Let G be a group with subgroup H. Lagrange's Theorem shows that $|H|$ divides $|G|$. Sylow's First Theorem provides a partial converse.

Theorem 3.5 (Sylow's First Theorem)**.** Let G be a finite group and p a prime. If p^k divides $|G|$, then G has a subgroup of order p^k.

Example 3.14. The symmetric group S_6 has order $6! = 720 = 2^4 \cdot 3^2 \cdot 5$. Thus S_6 has subgroups of order 2, 4, 8, 16, 3, 9, and 5. The other two Sylow theorems will help us prove how many distinct subgroups of these orders exist in a group.

Corollary 3.3 (Cauchy's Theorem)**.** If G is a finite group whose order is divisible by p, then G contains an element of order p.

Proof. Let p divide $|G|$. Then Sylow's First Theorem implies that G has a subgroup H of order p. Since $|H| = p$, H is cyclic generated by some order p element of G. □

Definition 3.7. Let G be a finite group and p a prime. If p^n is the largest power of p that divides $|G|$, then a subgroup of G of order p^n is called a *Sylow p-subgroup*. The existence of such a subgroup is guaranteed by Sylow's First Theorem.

Example 3.15. Since S_4 has order $4! = 24 = 2^3 \cdot 3$, a subgroup of order 8 will be a Sylow 2-subgroup. The Sylow 2-subgroups of S_4 are

$$\{e, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$$
$$\{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$$
$$\{e, (14), (23), (12)(34), (13)(24), (14)(23), (1243), (1342)\}.$$

The Sylow 3-subgroups of S_4 are order 3 and, thus, cyclic. The order 3 elements of S_4 are 3-cycles.

Example 3.16. Let p be a prime and G a finite abelian group of order $p^n m$ where p does not divide m. Then $G(p)$ is a Sylow p-subgroup of G. In fact, we will show that $G(p)$ is the unique Sylow p-subgroup of G.

End of lecture 18

In Example 1.32, we showed that the homomorphism $f : G \to G$ defined by $f(a) = xax^{-1}$ is an isomorphism. We referred to f as conjugation by x. Let K be a subgroup of G. Then the image of K under f, denoted xKx^{-1}, is isomorphic to K. In particular, $|xKx^{-1}| = |K|$ for all $x \in G$. If K is a Sylow p-subgroup of G, then so is xKx^{-1}.

Sylow's Second Theorem provides a relationship among the Sylow p-subgroups of a group.

Theorem 3.6 (Sylow's Second Theorem)**.** If P and K are Sylow p-subgroups of a group G, then there is some $x \in G$ for which $P = xKx^{-1}$.

Any two Sylow p-subgroups of a group are isomorphic by Sylow's Second Theorem.

Corollary 3.4. Let G be a finite group and K a Sylow p-subgroup of G for some prime p. Then K is normal if and only if K is the unique Sylow p-subgroup of G.

Proof. ($\Rightarrow$) Assume that K is normal so $xKx^{-1} = K$ for all $x \in G$. By Sylow's Second Theorem, any two Sylow p-subgroups are conjugate. Thus K is the unique Sylow p-subgroup of G.

($\Leftarrow$) For each $x \in G$, xKx^{-1} is a Sylow p-subgroup of G. Since K is the unique Sylow p-subgroup, we conclude that $xKx^{-1} = K$ for all $x \in G$. Thus K is normal. □

Sylow's Third Theorem helps count the number of Sylow p-subgroups in a group G.

Theorem 3.7 (Sylow's Third Theorem)**.** The number m_p of Sylow p-subgroups of a finite group G divides $|G|$ and $m_p \equiv 1 \pmod{p}$.

3.3.1. *Applications of Sylow Theorems.* Simple groups are the basic building blocks of all groups. We will use Sylow theorems to determine when groups of a certain order are not simple.

Example 3.17. Let G be a group of order $63 = 3^2 \cdot 7$. By Sylow's Third Theorem, the number of Sylow 7-subgroups m_7 divides 63 and $m_p \equiv 1 \pmod{7}$. The only number that satisfies both properties is $m_7 = 1$. By Corollary 3.4, we conclude that the unique Sylow 7-subgroup of G is normal. Therefore, there are no simple groups of order 63.

Example 3.18. We will show that there are no simple groups of order 56. Let G be a group of order $56 = 2^3 \cdot 7$. The number of Sylow 7-subgroups m_7 divides 56 and $m_7 \equiv 1 \pmod{7}$. We conclude $m_7 = 1$ or $m_7 = 8$. If $m_7 = 1$, then the unique Sylow p-subgroup is normal by Corollary 3.4 and G is not simple.

Assume $m_7 = 8$. Each Sylow 7-subgroup is a cyclic group of order 7. Let P_1 and P_2 be two distinct Sylow 7-subgroups. Then $|P_1 \cap P_2|$ divides $|P_1| = 7$ so $|P_1 \cap P_2| = 1$ or $|P_1 \cap P_2| = 7$. Since P_1 and P_2 are distinct, $|P_1 \cap P_2| = 1$. Therefore, each Sylow 7-subgroup provides 6 elements of order 7 so G has $8 \cdot 6 = 48$ elements of order 7. By Lagrange's Theorem, the intersection of a Sylow 2-subgroup and a Sylow 7-subgroup is trivial. Since the order of a Sylow 2-subgroup is 8, we have $m_2 = 1$ so G has a normal subgroup by Corollary 3.4. We conclude that there are no simple groups of order 56.

We can also use the Sylow theorems to classify finite groups.

Proposition 3.9. Let G be a group of order pq for primes $p > q$. If q does not divide $p - 1$, then $G \simeq \mathbb{Z}/(pq)\mathbb{Z}$.

Proof. By Sylow's Third Theorem, the number m_p of Sylow p-subgroups must divide $|G| = pq$. Thus m_p is 1, q, p, or pq. Further, $m_p \equiv 1 \pmod{p}$ by Sylow's Third Theorem. Since $p > q$, $q \not\equiv 1 \pmod{p}$ and $m_p \neq q$. Clearly, $p \equiv 0 \pmod{p}$ and $pq \equiv 0 \pmod{p}$ so $m_p = 1$. Therefore, there is exactly one Sylow p-subgroup P, which is normal by Corollary 3.4.

By Sylow's Third Theorem, the number m_q of Sylow q-subgroups must divide $|G| = pq$. Thus m_q is 1, q, p, or pq. Further, $m_q \equiv 1 \pmod{q}$ by Sylow's Third Theorem. By assumption, $p \not\equiv 1 \pmod{q}$. Clearly, $q \equiv 0 \pmod{q}$ and $pq \equiv 0 \pmod{q}$ so $m_q = 1$. Therefore, there is exactly one Sylow q-subgroup K, which is normal by Corollary 3.4.

Since $P \cap K$ is a subgroup of P and K, its order must divide $|P| = p$ and $|K| = q$ by Lagrange's Theorem. Thus $P \cap K = \{e_G\}$. The Second Isomorphism Theorem implies $|PK| = \frac{|P||K|}{|P \cap K|} = pq$ so $G = PK$. Corollary 3.1 and Proposition 3.8 imply

$$G \simeq P \times K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/(pq)\mathbb{Z}.$$

□

Example 3.19. To obtain the result of Proposition 3.9, we need the assumption that q does not divide $p - 1$. However, we can obtain a result in the general case too.

Let G be a group of order pq for distinct primes $p > q$. Following the proof of Proposition 3.9, if $m_q = 1$, $G \simeq \mathbb{Z}/(pq)\mathbb{Z}$. If $m_q = p$, let K be a Sylow q-subgroup. We can still argue that $P \cap K = \{e_G\}$ and $G = PK$. Proposition 3.5 implies that $G \simeq P \rtimes_\varphi K$ for some $\varphi : K \to \mathrm{Aut}(P)$.

End of lecture 19

3.4. **Conjugacy and the Proof of Sylow's Theorems.**

Definition 3.8. Let G be a group with $a, b \in G$. We say that a is conjugate to b if there exists $x \in G$ for which $b = xax^{-1}$.

Proposition 3.10. Conjugacy is an equivalence relation on G.

Proof. The relation is reflexive. Choose $x = e_G$. We have $e_G a e_G^{-1} = a$ and a is conjugate to itself.

The relation is symmetric. If a is conjugate to b, then $b = xax^{-1}$ or $x^{-1}bx = a$. Thus b is conjugate to a.

The relation is transitive. Assume a is conjugate to b and b is conjugate to c. Then $b = xax^{-1}$ and $c = yby^{-1}$ for $x, y \in G$. We have $c = (yx)a(yx)^{-1}$ and a is conjugate to c. □

Definition 3.9. The *conjugacy class* of $a \in G$ is the set of all elements conjugate to a.

By Proposition 3.10, G is partitioned into conjugacy classes. In other words, G is the disjoint union of conjugacy classes of G where each element is in one and only one conjugacy class. Since $\{e_G\}$ is a conjugacy class, each conjugacy class of a non-trivial group will satisfy $|C_i| < |G|$.

Example 3.20. We will determine the conjugacy classes of S_3. The identity element is always in its own conjugacy class. We have

$$(13)(12)(13)^{-1} = (123)(13) = (23)$$
$$(23)(12)(23)^{-1} = (132)(23) = (13).$$

Conjugation by an element of S_3 will not change whether an element is even or odd. The remaining elements (123) and (132) are even while any conjugate of (12) is odd. Thus $\{(12), (13), (23)\}$ is one conjugacy class. Finally,

$$(12)(123)(12)^{-1} = (23)(12) = (132).$$

The final conjugacy class $\{(123), (132)\}$.

We can write each element of S_n uniquely up to rearrangement as a product of disjoint cycles. The *cycle type* is the list of cycle lengths for a given element of S_n. In general, each conjugacy class of S_n contains only the elements of a certain cycle type and contains all elements of a certain cycle type.

Definition 3.10. Let G be a group and $a \in G$. The *centralizer* of a is the set of all elements of $g \in G$ that commute with a,

$$C_G(a) = \{g \in G : ga = ag\}.$$

Proposition 3.11. For a group G and $a \in G$, the centralizer $C_G(a)$ is a subgroup of G.

Proof. The identity $e_G \in C_G(a)$ since $e_G a = a e_G$. Let $g, h \in C_G(a)$. Then

$$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$$

so $gh \in C_G(a)$. For $g \in C_G(a)$, we also have $a^{-1}g = ga^{-1}$. Thus

$$g^{-1}a = (a^{-1}g)^{-1} = (ga^{-1})^{-1} = ag^{-1}$$

so $g^{-1} \in C_G(a)$. □

Example 3.21. The element $(12) \in S_4$ commutes with itself, disjoint elements, and products thereof. Thus $C_G((12)) = \{e_G, (12), (34), (12)(34)\}$.

Proposition 3.12. Let G be a finite group with $a \in G$. The number of elements in the conjugacy class of a is the index $[G : C_G(a)]$. The number of elements in the conjugacy class of a divides $|G|$.

Proof. Let S be the set of distinct right cosets of $C = C_G(a)$ in G. Let T be the conjugacy class of a in G. Define the function $f : S \to T$ as $f(Cx) = xax^{-1}$. We will show that f is a bijection of sets. First, we need to show that f is well-defined. Assume $Cx = Cy$ for $x, y \in G$. Then $x^{-1}y \in C_G(a)$ and $(x^{-1}y)a = a(x^{-1}y)$ for all $a \in G$. We rearrange to obtain $yay^{-1} = xax^{-1}$ or $f(Cx) = f(Cy)$. To show f is injective, assume $f(Cx) = f(Cy)$ for $x, y \in G$. The previous argument backward proves that $Cx = Cy$. For each element $b \in T$, we have $b = xax^{-1}$ for some $x \in G$. Thus $f(Cx) = b$ and f is surjective.

The number of elements in S is $[G : C_G(a)]$ and the number of elements of T is the number of distinct conjugates of a. By Lagrange's Theorem, $[G : C_G(a)]$ divides $|G|$. □

Proposition 3.13 (Class Equation)**.** Let G be a group with distinct conjugacy classes $C_1, \ldots, C_t$ with representatives $a_i \in C_i$. The *class equation* states

$$|G| = \sum_{i=1}^{t} [G : C_G(a_i)].$$

Further,

$$|G| = |Z(G)| + \sum_{j=1}^{r} |C_j|$$

for each C_j containing more than one element.

Proof. We have $|G| = \sum_{i=1}^{t} |C_i|$. Apply Proposition 3.12.

If C_i has only one element $a \in C$, then $ag = ga$ for all $g \in G$ and $a \in Z(G)$. Thus the center $Z(G)$ is the union of all the one-element conjugacy classes of G. □

End of lecture 20

Example 3.22. The class equation applied to $G = S_3$ shows that

$$\begin{aligned} |G| &= |Z(G)| + |(12)| + |(123)| \\ 6 &= 1 + 3 + 2. \end{aligned}$$

The class equation applied to $G = S_4$ shows that

$$\begin{aligned} |G| &= |Z(G)| + |(12)| + |(12)(34)| + |(123)| + |(1234)| \\ 24 &= 1 + 6 + 3 + 8 + 6. \end{aligned}$$

Note that the size of each conjugacy class divides the order of the group.

Sylow's First Theorem (Theorem 3.5) takes a finite group G and a prime p. If p^k divides $|G|$, then G has a subgroup of order p^k.

Proof of Sylow's First Theorem. We will proceed via induction on the order of G. If $|G| = 1$, then the G has a subgroup of order p^0. Assume that the statement is true for all groups of order less than $|G|$. By the class equation,

$$|G| = |Z(G)| + \sum_{j=1}^{r} [G : C_G(a_j)]$$

for some elements $a_j \in G$. We have $[G : C_G(a_j)] > 1$ and $|Z(G)| \geq 1$ since $e_G \in Z(G)$. Suppose there is some j for which p does not divide $[G : C_G(a_j)]$. By Lagrange's Theorem,

$$|G| = |C_G(a_j)|[G : C_G(a_j)].$$

Thus p^k divides $|C_G(a_j)|$. The inductive hypothesis implies that $C_G(a_j)$ and, thus, G has a subgroup of order p^k, completing the proof.

If p divides $[G : C_G(a_j)]$ for each $1 \leq j \leq r$, then p divides $|G| - \sum_{j=1}^{r} |C_G(a_j)| = |Z(G)|$. Since $Z(G)$ is abelian, Cauchy's Theorem for Abelian Groups implies there is an element c of order p in $Z(G)$. Let $N = \langle c \rangle$. Since $c \in Z(G)$, N is a normal subgroup of G of order p. Then p^{k-1} is the largest power of p that divides G/N. By the inductive hypothesis, G/N has a subgroup T of order p^{k-1}. The Correspondence Theorem implies that there is a subgroup H of G containing N such that $H/N \simeq T$. By Lagrange's Theorem, $|H| = |N||T| = p^k$. □

In order to prove the remaining two Sylow theorems, we will introduce a subgroup notion of conjugacy.

Definition 3.11. Let A, B, H be subgroups of G. Then A is *H-conjugate* to B if there exists an $x \in H$ such that $B = xAx^{-1}$. In the special case that $H = G$, we say that A and B are *conjugate*.

Proposition 3.14. Let H be a subgroup of G. Then H-conjugacy is an equivalence relation on the set of all subgroups of G.

Proof. Refer to the proof of Proposition 3.10 using subgroups A, B, C in place of a, b, c. □

Definition 3.12. Let A be a subgroup of G. The *normalizer* of A in G is

$$N_G(A) = \{g \in G : gAg^{-1} = A\}.$$

Proposition 3.15. For a subgroup A of G, the normalizer $N_G(A)$ is a subgroup of G. Further, A is a normal subgroup of $N_G(A)$.

Proof. Since $e_G A e_G^{-1} = A$, $e_G \in N_G(A)$ and $N_G(A)$ is non-empty. Let $x, y \in N_G(A)$. Then

$$(xy)A(xy)^{-1} = x(yAy^{-1})x^{-1} = xAx^{-1} = A$$

and $xy \in N_G(A)$. For each $a \in A$, $xbx^{-1} = a$ for some $b \in A$. Thus $x^{-1}ax \in A$ for all $a \in A$. Conjugation by x^{-1} is an isomorphism so $x^{-1}Ax = A$ and $x^{-1} \in N_G(A)$. By definition, $xAx^{-1} = A$ so A is normal in $N_G(A)$. □

Example 3.23. Let $A = \langle (12) \rangle$ in S_4. The elements that fix A under conjugation would be $\{e, (12), (34), (12)(34)\}$. Looking back at Example 3.21, we notice that $C_G(a) = N_G(A)$ when A is cyclic generated by a. In general, though, centralizers fix elements via conjugation while normalizers fix subgroups via conjugation.

If we instead take $A = \{e, (12)(34), (13)(24), (14)(23)\}$, we find $N_G(A) = G$ since $A \triangleleft S_4$.

Proposition 3.16. Let A and H be subgroups of a finite group G. The number of elements in the equivalence class of A under H-conjugacy is $[H : H \cap N_G(A)]$ and, therefore, divides $|H|$.

Proof. Refer to the proof of Proposition 3.12 where G is replaced by H, a is replaced by A, and $C_G(a)$ is replaced by $H \cap N_G(A)$. □

Lemma 3.6. Let Q be a Sylow p-subgroup of a finite group G. If $x \in G$ has order a power of p and $xQx^{-1} = Q$, then $x \in Q$.

Proof. Proposition 3.15 implies that Q is normal in $N_G(Q)$. By assumption, $x \in N_G(Q)$. Since $|x|$ is a power of p, the order of Qx in $N_G(Q)/Q$ is a power of p. Denote by T the cyclic subgroup of $N_G(Q)/Q$ generated by Qx. By the Correspondence Theorem, there is some subgroup H of G containing Q for which $T = H/Q$. Lagrange's Theorem implies that $|H| = |T||Q|$ is a power of p. However, $Q \subset H$ with $|Q|$ the largest power of p dividing the order of G. Thus $Q = H$ and T is the trivial subgroup of $N_G(Q)/Q$. Therefore, $Qx = Q$ or $x \in Q$. □

End of lecture 21

Sylow's Second Theorem (Theorem 3.6) takes a finite group with Sylow p-subgroups P and K. There is some $x \in G$ for which $P = xKx^{-1}$.

Proof of Sylow's Second Theorem. Let $|G| = p^n m$ where p does not divide m. Then $|K| = p^n$. Let $K = K_1, \ldots, K_t$ be the distinct conjugates of K in G. By Proposition 3.16, $t = [G : N_G(K)]$. Since K is a subgroup of $N_G(K)$, we have p^n divides $|N_G(K)|$. By Lagrange's Theorem,

$$|G| = |N_G(K)|[G : N_G(K)] = |N_G(K)|t$$

so p does not divide t. We want to show that P is one of the K_i.

The set $S = \{K_1, \ldots, K_t\}$ is a union of distinct equivalence classes under P-conjugacy. By Proposition 3.16, the number of elements P-conjugate to some K_i is $[P : P \cap N_G(K_i)]$, which is a divisor of $|P| = p^n$ by Lagrange's Theorem. The number of subgroups in each equivalence class is a power of p so t is a sum of powers of p. Since p does not divide t, at least one of the powers of p in the sum is $p^0 = 1$. Therefore, there is some i for which $xK_ix^{-1} = K_i$ for all $x \in P$. By Lemma 3.6, $x \in K_i$ for each $x \in P$. Thus $P \subset K_i$ and, by order considerations, $P = K_i$. □

Sylow's Third Theorem (Theorem 3.7) states that the number of Sylow p-subgroups t divides $|G|$ and is congruent to 1 modulo p.

Proof of Sylow's Third Theorem. Let $S = \{K_1, \ldots, K_t\}$ be the set of all Sylow p-subgroups of G. By Sylow's Second Theorem, these are all conjugates of K_1. The proof of Sylow's Second Theorem shows $t = [G : N_G(K_1)]$, and t divides the order of G by Lagrange's Theorem.

Let $P = K_j$ for some $1 \leq j \leq t$. The only P-conjugate of P is P. Lemma 3.6 shows that the only equivalence class consisting of a single element is the class consisting of P. Further, S is the disjoint union of distinct equivalence classes, and each equivalence class has order a power of p. Only the class containing P has order $p^0 = 1$. Hence, $t \equiv 1 \pmod{p}$. □

3.5. **The Structure of Finite Groups.** We will apply the results of this chapter to the classification of finite groups. In particular, we will classify all groups of order up to 15. We begin the section with helpful results about p-groups.

Proposition 3.17. If G is a group of order p^n with p prime and $n \geq 1$, then the center $Z(G)$ contains more than one element. In particular, $|Z(G)| = p^k$ for $1 \leq k \leq n$.

Proof. By Lagrange's Theorem, $|Z(G)| = p^k$ for $0 \leq k \leq n$. The class equation implies

$$|Z(G)| = |G| - \sum_{j=1}^{r} |C_j|$$

where each $|C_j|$ is a number larger than 1 that divides $|G|$. Thus each $|C_j|$ is divisible by p. Since $|G|$ is divisible by p, the righthand side of the equation is divisible by p. Therefore, p divides $|Z(G)|$ and $1 \leq k \leq n$. □

Corollary 3.5. If p is prime and $n > 1$, then there is no simple group of order p^n.

Proof. By Proposition 3.17, a group G of order p^n has non-trivial center. The center $Z(G)$ is normal. If $Z(G) \neq G$, then G is not simple. If $Z(G) = G$, then G is abelian and G is not simple by Proposition 2.13. □

End of lecture 22

Corollary 3.6. If G is a group of order p^2 for p prime, then G is abelian. Hence, G is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. Note that $Z(G)$ is normal so $G/Z(G)$ is a group. By Proposition 3.17, the order of $Z(G)$ is either p or p^2. If $Z(G)$ has order p^2, then G is abelian. If $Z(G)$ has order p, then $|G/Z(G)| = p$ and $G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$ by Example 2.4. Since $G/Z(G)$ is cyclic, G is abelian by Proposition 2.9. We draw a contradiction because $Z(G) = G$ has order p^2. Thus G is abelian of order p^2, and the Fundamental Theorem of Finite Abelian Groups completes the proof. □

Proposition 3.18. Let p and q be distinct primes such that $q \not\equiv 1 \pmod{p}$ and $p^2 \not\equiv 1 \pmod{q}$. If G is a group of order p^2q, then G is isomorphic to $\mathbb{Z}/(p^2q\mathbb{Z})$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Proof. By Sylow's Third Theorem, the number m_p of Sylow p-subgroups must divide p^2q so the only options are 1, p, p^2, q, pq, and p^2q. Further, $m_p \equiv 1 \pmod{p}$ so $m_p = 1$ or $m_p = q$. Since $q \not\equiv 1 \pmod{p}$ by assumption, $m_p = 1$ and the Sylow p-subgroup P is normal by Proposition 3.4.

By Sylow's Third Theorem, m_q can only be 1, p, or p^2. Since $p^2 \not\equiv 1 \pmod{q}$ by assumption, neither p nor p^2 is an option so $m_q = 1$. The Sylow q-subgroup Q is normal.

The order of $P \cap Q$ must divide $|P| = p^2$ and $|Q| = q$ so $P \cap Q = \{e_G\}$. Thus

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^2q = |G|$$

by the Second Isomorphism Theorem. Corollary 3.1 implies $G \simeq P \times Q$. Finally, Corollary 3.6 provides the possibilities for P, and Example 2.4 provides the possibilities for Q. □

Example 3.24. The group A_4 has order $12 = 2^2 \cdot 3$. However, A_4 cannot be written as a direct product of abelian groups because A_4 is not abelian.

Proposition 3.19. If p and q are distinct primes, then there is no simple group of order p^2q.

Proof. Suppose $|G| = p^2q$. If either $q \not\equiv 1 \pmod{p}$ or $p^2 \not\equiv 1 \pmod{q}$, then the proof of Proposition 3.18 proves that G has a non-trivial normal subgroup.

Assume $q \equiv 1 \pmod{p}$ and $p^2 \equiv 1 \pmod{q}$. Then $p|(q-1)$ and $p \leq q-1$. Since q is prime and $p^2 - 1 = (p-1)(p+1)$, q divides $p-1$ or $p+1$. However, q cannot divide $p-1$ since $p \leq q-1$. Thus $q = p+1$. Since p and q are prime, the only possibility is $p = 2$ and $q = 3$.

We will now prove that no group of order 12 is simple. Sylow's Third Theorem implies that $m_3 = 1$ or $m_3 = 4$. If $m_3 = 1$, then the Sylow 3-subgroup is normal by Corollary 3.4. Assume $m_3 = 4$. Each Sylow 3-subgroup is cyclic of order 3. There are 8 elements of order 3 in G. Every non-trivial element of a Sylow 2-subgroup must have even order so there can only be one Sylow 2-subgroup. By Corollary 3.4, G has a normal Sylow 2-subgroup. □

3.5.1. *Dihedral Groups.*

Definition 3.13. Let the *dihedral group* D_n of order $2n$ be the group generated by $\{r, s\}$ where $|r| = n$, $|s| = 2$, and $sr = r^{-1}s$.

Note that one of the first dihedral group defined, D_4, satisfies the above criteria. As mentioned, the dihedral group represents the symmetries of a regular n-gon. We can write the elements as

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

where $sr^i = r^{n-i}s$ for $0 \leq i < n$.

Proposition 3.20. If $|G| = 2p$ for $p \neq 2$ a prime, then G is isomorphic to $\mathbb{Z}/(2p)\mathbb{Z}$ or D_p.

Proof. By Cauchy's Theorem, G contains an element a of order p and an element b of order 2. Then $b^2 = e_G$ implies $b^{-1} = b$. The index 2 subgroup $H = \langle a \rangle$ is normal in G by Lemma 2.1. Thus $bab^{-1} = bab \in H$ so $bab = a^t$ for some $0 \leq t \leq p-1$. We have

$$a^{t^2} = (a^t)^t = (bab)^t = (bab)\cdots(bab) = ba^tb = b(bab)b = a$$

so $t^2 \equiv 1 \pmod{p}$ by Proposition 1.4(2). Since p divides $t^2 - 1$, p divides $t-1$ or $t+1$. Rewriting this, $t \equiv 1 \pmod{p}$ or $t \equiv -1 \pmod{p}$.

Assume $t \equiv 1 \pmod{p}$. Then $bab = a$ or $ba = ab$. By Proposition 1.1, $|ab| = |a||b| = 2p$ and G is cyclic generated by ab. Therefore, $G \simeq \mathbb{Z}/(2p)\mathbb{Z}$ by Proposition 1.16.

End of lecture 23

Assume $t \equiv -1 \pmod{p}$. Then $bab = a^{-1}$. Define $f : D_p \to G$ by $f(r^is^j) = a^ib^j$. Note that $|a| = |r|$, $|b| = |s|$, and $bab = a^{-1}$ while $srs = r^{-1}$. We can thus show that f is well-defined. Further, f is a group homomorphism via

$$\begin{aligned} f((r^is^j)(r^ks^\ell)) &= f(r^{i-k}s^{j+\ell}) \\ &= a^{i-k}b^{j+\ell} \\ &= (a^ib^j)(a^kb^\ell) \\ &= f(r^is^j)f(r^ks^\ell). \end{aligned}$$

Let $K = \langle b \rangle$. By Lagrange's Theorem, $H \cap K = \{e_G\}$. Then $|HK| = 2p$ by the Second Isomorphism Theorem so $G = HK$. Every element can be written as a^ib^j, which implies that f is surjective. Since $|D_p| = |G|$, f is an isomorphism. □

Example 3.25. The symmetric group S_3 is not abelian of order $6 = 2 \cdot 3$. Proposition 3.20 implies that $S_3 \simeq D_3$. Is this true for other symmetric groups S_n?

3.5.2. *Groups of Small Order.* The table below contains the finite groups of order at most 15 that we have classified thus far. We will fill in rows 8 and 12 in this section.

Order	Groups	Proof
1	$\{e\}$	
2	$\mathbb{Z}/2\mathbb{Z}$	Example 2.4
3	$\mathbb{Z}/3\mathbb{Z}$	Example 2.4
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	Example 2.5
5	$\mathbb{Z}/5\mathbb{Z}$	Example 2.4
6	$\mathbb{Z}/6\mathbb{Z}$, D_3	Proposition 3.20
7	$\mathbb{Z}/7\mathbb{Z}$	Example 2.4
8	?	
9	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	Corollary 3.6
10	$\mathbb{Z}/10\mathbb{Z}$, D_5	Proposition 3.20
11	$\mathbb{Z}/11\mathbb{Z}$	Example 2.4
12	?	
13	$\mathbb{Z}/13\mathbb{Z}$	Example 2.4
14	$\mathbb{Z}/14\mathbb{Z}$, D_7	Proposition 3.20
15	$\mathbb{Z}/15\mathbb{Z}$	Proposition 3.9

Example 3.26. Let G be a non-abelian group of order 8. In particular, G is not cyclic. Thus every non-identity element must have order 2 or 4 by Lagrange's Theorem. If every non-identity element of G has order 2, then every element of G is its own inverse so

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

for all $a, b \in G$ and G is abelian. We conclude there is some element $a \in G$ of order 4. Let $b \in G$ be such that $b \notin \langle a \rangle$. Any two elements in $\{e_G, a, a^2, a^3, b, ab, a^2b, a^3b\}$ are distinct since $a^i = a^jb$ implies $b \in \langle a \rangle$. Thus $G = \{e_G, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

By Lemma 2.1, the index 2 subgroup $\langle a \rangle$ is normal. The conjugation group homomorphism $f : G \to G$ defined as $f(a) = bab^{-1}$ is an isomorphism. Thus element bab^{-1} has order $|a| = 4$ and $bab^{-1} \in \langle a \rangle$ by normality. Then $bab^{-1} = a$ or $bab^{-1} = a^3$ by order considerations. However, $bab^{-1} = a$ would imply G is abelian so $bab^{-1} = a^3$ or $ba = a^3b$. We can produce the following part of the multiplication table of G.

$\cdot$	e_G	a	a^2	a^3	b	ab	a^2b	a^3b
e_G	e_G	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e_G	ab	a^2b	a^3b	b
a^2	a^2	a^3	e_G	a	a^2b	a^3b	b	ab
a^3	a^3	e_G	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab				
ab	ab	b	a^3b	a^2b				
a^2b	a^2b	ab	b	a^3b				
a^3b	a^3b	a^2b	ab	b				

End of lecture 24

In order to complete the table, we want to find b^2. Since $b^2 = a^ib$ implies $b \in \langle a \rangle$, we conclude that $b^2 \in \langle a \rangle$. If $b^2 = a$, then

$$ab = b^2b = bb^2 = ba$$

and G is abelian. Similarly, $b^2 = a^3$ implies

$$ab = (a^3)^{-1}b = b^{-2}b = bb^{-2} = b(a^3)^{-1} = ba$$

and G is abelian. Therefore, $b^2 = e_G$ or $b^2 = a^2$. In the first case, the multiplication table will be that of D_4. In the second case, the multiplication table is that of Q_8.

Definition 3.14. The *quaternion group* is the set $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ with relations

$$(-1)^2 = 1$$
$$i^2 = j^2 = k^2 = -1$$
$$ijk = -1.$$

Proposition 3.21. If G is a non-abelian group of order 8, then $G \simeq D_4$ or $G \simeq Q_8$.

Proof. It remains to show that D_4 and Q_8 are not isomorphic. We see that D_4 has two elements of order 4, $\{r, r^3\}$ while Q_8 has six elements of order 4, $\{i, -i, j, -j, k, -k\}$. Thus D_4 and Q_8 are not isomorphic. □

Example 3.27. Let G be a non-abelian group of order 12. As a result, G cannot be cyclic and every non-identity element of G has order 2, 3, 4, or 6 by Lagrange's Theorem. By Proposition 3.19, either a Sylow 2-subgroup P is normal or a Sylow 3-subgroup Q is normal. Example 2.4 implies $Q \simeq \mathbb{Z}/3\mathbb{Z}$. Example 2.5 shows $P \simeq \mathbb{Z}/4\mathbb{Z}$ or $P \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Lagrange's Theorem implies $P \cap Q = \{e_G\}$ so $|PQ| = 12$ by Second Isomorphism Theorem and $G = PQ$.

Case 1: Assume that $m_2 = 1$ so P is normal. Assume that P is not cyclic. Then $P = \langle a_1, a_2 \rangle$ for $|a_i| = 2$ and $a_1 a_2 = a_2 a_1$. Let $Q = \langle b \rangle$. Since P is normal, order considerations imply $ba_1b^{-1} = a_1$, $ba_1b^{-1} = a_2$, or $ba_1b^{-1} = a_1a_2$. The same can be said for conjugating a_2 by b. If $ba_ib^{-1} = a_i$, then $ba_jb^{-1} = a_j$ for $j \neq i$ and G is abelian. Assume $ba_1b^{-1} = a_2$. Then $ba_2b^{-1} = a_1$ would imply $b^2a_2b^{-2} = a_2$ and $b^3a_2b^{-3} = a_1$. We need $a_2 = b^3a_2b^{-3}$, which is a contradiction. Thus $ba_2b^{-1} = a_1a_2$. If $ba_1b^{-1} = a_1a_2$, a similar argument shows that $ba_2b^{-1} = a_1$. In either case, a relabeling results in the same multiplication table. We can show that G is isomorphic to A_4.

Assume that P is cyclic so $P = \langle a \rangle$. G is generated by $\{a, b\}$. Since P is normal, order considerations imply $bab^{-1} = a$ or $bab^{-1} = a^3$. If $bab^{-1} = a$, then G is abelian. If $bab^{-1} = a^3$, then $b^2ab^{-2} = a$ and, since $b^3 = e_G$,

$$a = b^3ab^{-3} = bab^{-1} = a^3,$$

which contradicts $|a| = 4$. Therefore, G does not have a normal cyclic subgroup of order 4.

Case 2: Assume that $m_3 = 1$ so Q is normal. Let $Q = \langle b \rangle$. At first, assume P is not cyclic so $P = \langle a_1, a_2 \rangle$ for $|a_i| = 2$ and $a_1a_2 = a_2a_1$. Then $a_1ba_1^{-1} = b$ or $a_1ba_1^{-1} = b^2$ since order is preserved and Q is normal. The same can be said of conjugation by a_2. If $a_1ba_1^{-1} = b$, then $a_2ba_2^{-1} = b^2$ since G is not abelian. If $a_1ba_1^{-1} = b^2$ and $a_2ba_2^{-1} = b^2$, then $(a_1a_2)b(a_1a_2)^{-1} = b$. By possibly relabeling, we can assume $a_1ba_1^{-1} = b$ and $a_2ba_2^{-1} = b^2$. Then a_1 and b commute so Lemma 1.1 implies $|a_1b| = \text{lcm}(|a_1|, |b|) = 6$. We can write

$$G = \{(a_1b)^i, a_2(a_1b)^j\}$$

for $0 \leq i, j \leq 6$. Further,

$$a_2(a_1b)a_2^{-1} = a_1(a_2ba_2^{-1}) = a_1b^2 = (a_1b)^{-1}.$$

We can show that $G \simeq D_6$.

Assume that $P = \langle a \rangle$ is cyclic. Once again, take $Q = \langle b \rangle$ to be normal in G. G is generated by $\{a, b\}$. If $aba^{-1} = b$, then a and b commute and G is abelian. Thus $aba^{-1} = b^2$ since b^2 is the only other order 3 element in Q. We can write out a unique multiplication table. Denote the group T.

Proposition 3.22. If G is a non-abelian group of order 12, then G is isomorphic to A_4, D_6, or T.

Proof. It remains to check that no two of the groups are not isomorphic. A_4 does not have an element of order 6 while D_6 has two elements of order 6. Additionally, the group T has an element of order 6, namely a^2b in the notation of Example 3.27. The groups D_6 and T are not isomorphic since T has an element of order 4. □

We can now complete the table.

Order	Groups	Proof
1	$\{e\}$	
2	$\mathbb{Z}/2\mathbb{Z}$	Example 2.4
3	$\mathbb{Z}/3\mathbb{Z}$	Example 2.4
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$	Example 2.5
5	$\mathbb{Z}/5\mathbb{Z}$	Example 2.4
6	$\mathbb{Z}/6\mathbb{Z}$, D_3	Proposition 3.20
7	$\mathbb{Z}/7\mathbb{Z}$	Example 2.4
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, Q_8	Proposition 3.21
9	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	Corollary 3.6
10	$\mathbb{Z}/10\mathbb{Z}$, D_5	Proposition 3.20
11	$\mathbb{Z}/11\mathbb{Z}$	Example 2.4
12	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, A_4, D_6, T	Proposition 3.22
13	$\mathbb{Z}/13\mathbb{Z}$	Example 2.4
14	$\mathbb{Z}/14\mathbb{Z}$, D_7	Proposition 3.20
15	$\mathbb{Z}/15\mathbb{Z}$	Proposition 3.9

End of material covered on the final
End of lecture 25

4. Applications of Group Theory

4.1. **Group Actions.** Loosely speaking, a group action will be a permutation of a set by a group. In other areas of mathematics, groups arise mostly as the objects that act on a set. In combinatorics, groups act on finite sets of objects. In topology, groups like the fundamental group act on topological spaces. In Galois theory, groups arise as automorphisms of fields.

Definition 4.1. Let G be a group and X a set. G *acts on* X if there is an operation $g \cdot x$ such that the following properties hold.

(1) For every $g, h \in G$ and $x \in X$, $(gh) \cdot x = g \cdot (h \cdot x)$.
(2) For every $x \in X$, $e_G \cdot x = x$.

We have already seen numerous examples of group actions.

Example 4.1. The group S_n acts on $X_n = \{1, 2, \ldots, n\}$.

Example 4.2. The group D_n acts on the set of vertices of the regular n-gon.

Example 4.3. Let G be the group of the Rubik's cube, which is all sequences of motions on the cube (keeping center colors in fixed locations). The group acts on two different sets: the 12 edge cubelets and the 8 corner cubelets. We could further let G act on the set of all 20 non-center face cubelets together.

Example 4.4. The proof of Cayley's Theorem, Theorem 2.6, relied on a group action. We let the group G act on the set G by left multiplication. In other words $g \cdot x = gx$ for $g \in G$ and $x \in X$.

We have a generalization of Cayley's Theorem for every group action. Cayley's Theorem produces an injective group homomorphism, but that need not be the case in general.

Proposition 4.1. The group G acts on a set X if and only if there exists a group homomorphism $\varphi : G \to A(X)$ where $A(X)$ is the group of set bijections of X.

Proof. ($\Rightarrow$) Assume that G acts on X. Let $g \in G$. Define $\varphi(g)$ as the bijection $\varphi(g)(x) = g \cdot x$ for $x \in X$. Then $\varphi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \varphi(g)(\varphi(h)(x))$. We conclude that $\varphi(gh) = \varphi(g) \circ \varphi(h)$ so φ is a group homomorphism.

($\Leftarrow$) Assume that $\varphi : G \to A(X)$ is a group homomorphism. Define the group action $g \cdot x = \varphi(g)(x)$. Then $e_G \cdot x = \varphi(e_G)(x) = x$ since $\varphi(e_G)$ is the identity set bijection. Further, $(gh) \cdot x = \varphi(gh)(x) = \varphi(g)(\varphi(h)(x)) = g \cdot (h \cdot x)$. □

We can use this equivalent condition of a group action to prove the following generalization of index 2 subgroups being normal. The result can be very useful for future group classification.

Corollary 4.1. Let p be the smallest prime divisor of $|G|$ for a finite group G. A subgroup H of G with $[G : H] = p$ is normal in G.

Proof. Let G act on the left cosets G/H by left multiplication. There is some group homomorphism $\varphi : G \to A(G/H)$ by Proposition 4.1. The homomorphism is non-trivial since H is not all of G. With $|G/H| = [G : H] = p$, we can identify $A(G/H) \simeq S_p$. Note that $\operatorname{im}(\varphi)$ is a subgroup of S_p so $|\operatorname{im}(\varphi)|$ divides $|S_p| = p!$ by Lagrange's Theorem. In order for $\varphi(g) = \mathrm{id}_X$, we need $g \cdot H = H$ or $g \in H$. Thus $H \subset \ker(\varphi)$.

The First Isomorphism Theorem implies that $G/\ker(\varphi) \simeq \operatorname{im}(\varphi)$. In particular, $|G/\ker(\varphi)| = |G|/|\ker(\varphi)|$ divides $p!$. The only factor that $|G|$ and $p!$ share is p since p is the smallest prime dividing $|G|$. We conclude that $|G/\ker(\varphi)|$ is 1 or p. With φ non-trivial, $|G/\ker(\varphi)| = p$. Therefore, $|\ker(\varphi)| = \frac{|G|}{p} = |H|$ and $H = \ker(\varphi)$. By Proposition 2.10, H is a normal subgroup of G. □

Example 4.5. In the proof of Sylow's Theorems, we made use of a different group action of the group G on itself. A group G can act on the set G via conjugation. In other words, $g \cdot x = gxg^{-1}$.

End of lecture 26

Definition 4.2. Let G be a group that acts on a set X. For $x \in X$, the *stabilizer of x in G*, written $\text{Stab}_G(x)$, is the set of elements such that $g \cdot x = x$.

$$\text{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

Note that $\text{Stab}_G(x)$ is a subset of G.

Definition 4.3. Let G be a group that acts on a set X. For $x \in X$, the *orbit of x under G*, written $\text{Orb}_G(x)$ is the set of all elements in X of the form $g \cdot x$ for $g \in G$.

$$\text{Orb}_G(x) = \{y \in Y : g \cdot x = y\}$$

Note that $\text{Orb}_G(x)$ is a subset of X.

Proposition 4.2. Let G be a group that acts on the set X. For $x, y \in X$, the relation $x \sim y$ if and only if $g \cdot x = y$ is an equivalence relation. We can partition X into a disjoint union of orbits.

Proof. Reflexivity: $x \sim x$ since $e_G \cdot x = x$.
Symmetry: Let $x \sim y$. Then $g \cdot x = y$ and $x = g^{-1} \cdot y$ so $y \sim x$.
Transitivity: Let $x \sim y$, $y \sim z$. Then $g \cdot x = y$ and $h \cdot y = z$. We have $(hg) \cdot x = z$. □

Example 4.6. Let $1 \in X_3$ and $G = S_3$. Then $\text{Stab}_G(1) = \{e, (23)\}$ and $\text{Orb}_G(1) = \{1, 2, 3\} = X_3$.

Definition 4.4. A group action is *transitive* if for any pair $x, y \in X$, there is some $g \in G$ for which $y = g \cdot x$. In other words, the group action only has one orbit.

Example 4.7. Let G be a group that acts on the set G by conjugation. The orbit of some $a \in G$ is the conjugacy class of a. The stabilizer of $a \in G$ is the centralizer $C_G(a)$.

Proposition 4.3 (Cauchy's Theorem)**.** Let G be a finite group with prime p dividing $|G|$. Then G has an element of order p.

Proof. Let $X = \{(x_1, \ldots, x_p) \in G^p : x_1 \cdots x_p = e_G\}$. Each element in the p-tuple is an independent choice except for the last element $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$. Thus $|X| = |G|^{p-1}$ and p divides $|X|$. Let $\mathbb{Z}/p\mathbb{Z}$ act on X by cyclically permuting the elements of each tuple. In particular,

$$\overline{1} \cdot (x_1, \ldots, x_{p-1}, x_p) = (x_p, x_1, \ldots, x_{p-1}).$$

The action sends an element of X to another element of X since

$$e_G = x_1 \cdots x_{p-1} x_p = (x_1 \cdots x_{p-1})(x_1 \cdots x_{p-1})^{-1} = (x_1 \cdots x_{p-1})^{-1}(x_1 \cdots x_{p-1}) = x_p(x_1 \cdots x_{p-1})$$

in G. The orbit of each point is either size 1 or p. The orbit of an element $x \in X$ is size 1 if and only if $x = (a, \ldots, a)$ or $a^p = e_G$. Partition X into a disjoint union of orbits. Thus

$$(\#\text{ orbits of size 1}) = |X| - p \cdot (\#\text{ orbits of size } p) \equiv 0 \pmod{p}.$$

Since $(e_G, \ldots, e_G) \in X$ is an element with orbit size 1, there must be at least $p - 1$ other elements with an orbit of size 1. □

Proposition 4.4. Let the group G act on X. For each $x \in X$, $\text{Stab}_G(x)$ is a subgroup of G.

Proof. We have $e_G \in \text{Stab}_G(x)$ by property (2) of the group action definition. Let $g, h \in \text{Stab}_G(x)$. Then $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ by property (1) of the group action definition. Further, $x = e_G \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. □

We now find a generalization of Proposition 3.12. There is an inverse relationship between elements that fix $x \in X$, the stabilizer, and all the elements one can obtain as $g \cdot x$, the orbit. With the orbit and stabilizer, we often get a complete picture of the group action.

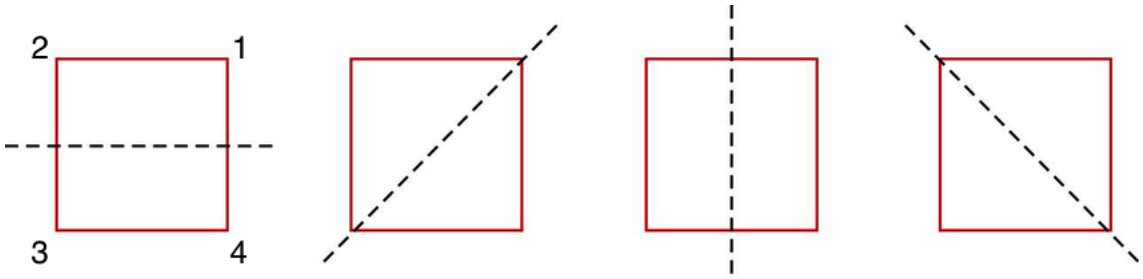
Theorem 4.1 (Orbit-Stabilizer)**.** Suppose G is a finite group that acts on the set X. For any $x \in X$, then $|G| = |\mathrm{Stab}_G(x)||\mathrm{Orb}_G(x)|$.

Proof. Let S be the set of right cosets of $\mathrm{Stab}_G(x)$ in G. Let $T = \mathrm{Orb}_x(G)$. Define the set map $f : T \to S$ such that $f(g{\cdot}x) = \mathrm{Stab}_G(x)g$. We need to check that f is well-defined. Given $g{\cdot}x = h{\cdot}x$, then $h^{-1}g \in \mathrm{Stab}_G(x)$. Thus $\mathrm{Stab}_G(x)g = \mathrm{Stab}_G(x)h$. We want to show that f is injective. Assume $f(g \cdot x) = f(h \cdot x)$. Then $\mathrm{Stab}_G(x)g = \mathrm{Stab}_G(x)h$ which implies $h^{-1}g \in \mathrm{Stab}_G(x)$. As a result, $g \cdot x = h \cdot x$. To show f is surjective, let $\mathrm{Stab}_G(x)g$ be a right coset. Then $f(g \cdot x) = \mathrm{Stab}_G(x)g$. We conclude that f is a set bijection. □

Example 4.8. Let the group $G = S_3$ act on $X_3 = \{1, 2, 3\}$. Pick $1 \in X_3$ so $\mathrm{Orb}_G(1) = \{1, 2, 3\}$ and $\mathrm{Stab}_G(1) = \{e, (23)\}$. We confirm Orbit-Stabilizer below.

$$\begin{aligned} |G| &= |\mathrm{Stab}_G(x)||\mathrm{Orb}_G(x)| \\ 6 &= 2 \cdot 3 \end{aligned}$$

Example 4.9. Let $G = D_4$ act on the vertices $V = \{1, 2, 3, 4\}$ of a square.



Define r as counterclockwise rotation of the square by $\frac{\pi}{2}$ and s the leftmost reflection. Pick $1 \in V$ so $\mathrm{Orb}_G(1) = \{1, 2, 3, 4\}$ and $\mathrm{Stab}_G(1) = \{e, rs\}$. We once again confirm Orbit-Stabilizer.

Example 4.10. Let $G = \mathrm{GL}_n(\mathbb{R})$ act on the set $\mathbb{R}^n$ where $A \cdot v$ is the matrix multiplication Av. The stabilizer $\mathrm{Stab}_G(v)$ is the non-trivial subgroup of matrices that have invariant subspace $\mathrm{Span}(v)$. The orbit of some v is the entirety of $\mathbb{R}^n$ so the group action is transitive. Note that Orbit-Stabilizer does not apply since G is not a finite group.

4.1.1. *Burnside's Lemma.* We can rearrange the result of Orbit-Stabilizer to obtain a sometimes more useful result. Burnside's Lemma usually is applied to problems in combinatorics.

Definition 4.5. Let the group G act on a set X. A *fixed point* of $g \in G$ is an element $x \in X$ for which $g \cdot x = x$. Denote by $\mathrm{Fix}(g)$ the subset of fixed points of g in X.

Definition 4.6. Let the group G act on a set X. Denote by X/G the set of orbits of X with respect to the group action.

Lemma 4.1 (Burnside's Lemma)**.** Let the group G act on the set X. Then

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Proof. We can write the sum in two different ways

$$\begin{aligned}\sum_{g\in G}|\mathrm{Fix}(g)| &= \sum_{g\in G}|\{x\in X : g\cdot x = x\}| \\ &= |\{(g,x)\in G\times X : g\cdot x = x\}| \\ &= \sum_{x\in X}|\{g\in G : g\cdot x = x\}| \\ &= \sum_{x\in X}\mathrm{Stab}_G(x).\end{aligned}$$

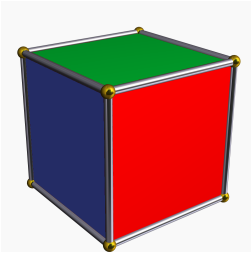
In $|X/G|$, each orbit provides 1 to the sum. The size of each orbit is $|\mathrm{Orb}_G(x)|$ so we can view each $x\in X$ as contributing $\frac{1}{|\mathrm{Orb}_G(x)|}$ to the sum $|X/G|$. Thus $|X/G| = \sum_{x\in X}\frac{1}{|\mathrm{Orb}_G(x)|}$.

By Orbit-Stabilizer and the above results, we have

$$\begin{aligned}|X/G| &= \sum_{x\in X}\frac{1}{|\mathrm{Orb}_G(x)|} \\ &= \sum_{x\in X}\frac{|\mathrm{Stab}_G(x)|}{|G|} \\ &= \frac{1}{|G|}\sum_{x\in X}|\mathrm{Stab}_G(x)| \\ &= \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.\end{aligned}$$

□

Example 4.11. We can use Burnside's Lemma to count the number of rotationally different 3-colorings of the cube.



Let X be the set of colorings of a cube with fixed orientation so $|X| = 3^6$. The group G is the rotational symmetry group of a cube. Each rotation of a cube has an axis of rotation through the center of two opposite faces, edges, or vertices. We organize the 24 distinct rotations below.

- The identity element of G
- The six 90-degree face rotations
- The three 180-degree face rotations
- The eight 120-degree vertex rotations
- The six 180-degree edge rotations

Two colorings belong to the same orbit when one coloring can be obtained from another by rotating the cube. We want to count the number of orbits, $|X/G|$.

- The identity element of G leaves all 3^6 elements of X fixed.
- The six 90-degree face rotations each leave 3^3 of the elements of X fixed.
- The three 180-degree face rotations each leave 3^4 of the elements of X fixed.
- The eight 120-degree vertex rotations each leave 3^2 of the elements of X fixed.

- The six 180-degree edge rotations each leave 3^3 of the elements of X fixed.

Burnside's Lemma implies the number of rotationally distinct 3-colorings of the cube is

$$|X/G| = \frac{1}{24}(3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2 + 6 \cdot 3^3) = 57.$$

4.2. **Solvable and Nilpotent Groups.** The Classification of Finite Abelian groups allows us to easily list all finite abelian groups of any order up to isomorphism. In this section, we will define more general classes of groups called nilpotent and solvable groups that can be approximated well by abelian groups. We hope that the power of the Classification of Finite Abelian Groups can be extended to such a class of groups.

4.2.1. *Nilpotent groups.*

Definition 4.7. Let G be a group. A *central series* is a sequence of subgroups

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_{n-1} \triangleright H_n = \{e_G\}$$

such that, for each $0 \leq i \leq n-1$, H_{i+1} is normal in G and H_i/H_{i+1} is a subgroup of $Z(G/H_{i+1})$. The condition implies H_i/H_{i+1} is abelian for each $0 \leq i \leq n-1$.

A group does not necessarily have a central series. However, there is a minimal choice at each step in the construction of such a sequence. In order for H_i/H_{i+1} to be in the center of G/H_{i+1}, we need elements of H_i to commute with elements of G modulo H_{i+1}. Defining $H_{i+1} = [G, H_i]$ where $[G, H_i]$ is the subgroup of G generated by $\{ghg^{-1}h^{-1} : g \in G, h \in H_i\}$ could produce a central series.

Definition 4.8. Let G be a group. A *lower central series* is a sequence of subgroups

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n \triangleright \dots$$

such that $H_{i+1} = [G, H_i]$ for $0 \leq i \leq n-1$.

Definition 4.9. A *nilpotent* group is one that has a central series. Equivalently, a *nilpotent* group is one that has a lower central series that terminates to the trivial subgroup in finitely many steps. We write

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_{n-1} \triangleright H_n = \{e_G\}$$

such that $H_{i+1} = [G, H_i]$ for $0 \leq i \leq n-1$.

We can think of central series as approximating a nilpotent group G by abelian groups. We hope that many of the techniques used to study abelian groups can be extended to the study of nilpotent groups. The following examples will illustrate that nilpotent groups really do extend the notion of an abelian group.

Example 4.12. Abelian groups are nilpotent. Let G be an abelian group. To construct a lower central series, $H_0 = G$ and $H_1 = [G, G] = \{e_G\}$.

Example 4.13. The quaternion group Q_8 is nilpotent. The commutator subgroup

$$[Q_8, Q_8] = \{\pm 1\}$$

by computing all products similar to $iji^{-1}j^{-1} = kk = -1$. Thus we have the following finite lower central series.

$$G = H_0 \triangleright \{\pm 1\} \triangleright \{1\}$$

Example 4.14. The direct product of two nilpotent groups is nilpotent. Let G_1 and G_2 be nilpotent groups. We have the following two lower central series where, without loss of generality, $m \leq n$.

$$G_1 = H_{10} \triangleright H_{11} \triangleright \cdots \triangleright H_{1n} = \{e_{G_1}\}$$
$$G_2 = H_{20} \triangleright H_{21} \triangleright \cdots \triangleright H_{2m} = \{e_{G_2}\}$$

Then the center $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$. One can check that the following sequence is a lower central series for $G_1 \times G_2$.

$$G_1 \times G_2 = H_{10} \times H_{20} \triangleright H_{11} \times H_{21} \triangleright \cdots \triangleright H_{1m} \times H_{2m} \triangleright \cdots \triangleright H_{1n} \times \{e_{G_2}\} = \{e_{G_1}\} \times \{e_{G_2}\}$$

Proposition 4.5. All finite p-groups are nilpotent.

Proof. We will proceed via induction on the order of G. As a base case, the trivial group is nilpotent. If $Z(G) = G$, then G is abelian and nilpotent by Example 4.12. Assume without loss of generality that G is not abelian. Then Proposition 3.17 implies that $Z(G)$ is non-trivial. The group $G/Z(G)$ is a p-group of order less than $|G|$ so the inductive hypothesis implies that $G/Z(G)$ is nilpotent. We can build the following central series for $G/Z(G)$ where $H_{i+1} \triangleleft G/Z(G)$ and H_i/H_{i+1} is a subgroup of $Z((G/Z(G))/H_{i+1})$ for each $0 \leq i \leq n-1$.

$$G/Z(G) = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_{n-1} \triangleright H_n = \{e_{G/Z(G)}\}$$

By the Correspondence Theorem for Normal Subgroups, we can lift to the following sequence where $\widetilde{H_i} \triangleleft G$ and, by the Third Isomorphism Theorem, $\widetilde{H_i}/\widetilde{H_{i+1}}$ is a subgroup of $Z(G/\widetilde{H_{i+1}})$ for each $0 \leq i \leq n-1$.

$$G = \widetilde{H_0} \triangleright \widetilde{H_1} \triangleright \cdots \triangleright \widetilde{H_{n-1}} \triangleright \widetilde{H_n} = Z(G)$$

Since $Z(G)$ is abelian, we can construct the central series.

$$G = \widetilde{H_0} \triangleright \widetilde{H_1} \triangleright \cdots \triangleright \widetilde{H_{n-1}} \triangleright \widetilde{H_n} \triangleright \widetilde{H_{n+1}} = \{e_G\}$$

Therefore, G is nilpotent. □

Corollary 4.2. Any finite direct product of finite p-groups is nilpotent.

Proof. Proceed by induction on the number of components in the direct product. Proposition 4.5 is the base case. Example 4.14 completes the inductive step. □

Theorem 4.2. A finite group G is nilpotent if and only if G is a direct product of p-groups. Equivalently, a finite group G is nilpotent if and only if each of the Sylow p-subgroups of G is normal.

Although the class of nilpotent groups generalizes the class of abelian groups, Theorem 4.2 proves that it is not a novel enough definition. In the next section we introduce solvable groups, a sufficiently distinct generalization of abelian groups to encompass what we need in future studies like Galois theory.

4.2.2. *Solvable groups.*

Definition 4.10. A *subnormal series* of a group G is a sequence of subgroups

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_{n-1} \triangleright H_n = \{e_G\}$$

such that $H_{i+1} \triangleleft H_i$ and H_i/H_{i+1} is an abelian group for each $0 \leq i \leq n-1$. Note that H_n need not be normal in G.

Definition 4.11. Let G be a group and define $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Then the sequence of subgroups

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots$$

is a *derived series*.

Definition 4.12. A group is *solvable* if it has a subnormal series. Equivalently, a group is *solvable* if it has a derived series that terminates to $\{e_G\}$ in finitely many steps.

The next example shows that solvable groups extend the idea of nilpotent, and thus abelian, groups.

Example 4.15. A central series is an example of a subnormal series. The condition that H_{i+1} is normal in G and H_i/H_{i+1} is contained in $Z(G/H_{i+1})$ implies that H_{i+1} is normal in H_i and H_i/H_{i+1} is abelian. Thus nilpotent groups are solvable.

$$\text{cyclic groups } \subset \text{ abelian groups } \subset \text{ nilpotent groups } \subset \text{ solvable groups}$$

Example 4.16. In order to prove that not all solvable groups are nilpotent, take $G = S_3$. We can show that $[S_3, S_3] = A_3$. Since $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ is abelian, $[A_3, A_3] = \{e\}$. The derived series of S_3 is

$$S_3 \triangleright A_3 \triangleright \{e\}.$$

Thus S_3 is solvable. However, S_3 does not have a normal Sylow 2-subgroup. Theorem 4.2 implies S_3 is not nilpotent.

Example 4.17. S_5 is not solvable. We can show that the commutator subgroup $[S_5, S_5] = A_5$. Since A_5 is simple and non-abelian, $[A_5, A_5] = A_5$. The derived series of S_5 does not terminate to the trivial subgroup.

In general, S_n is not solvable for $n \geq 5$. This is a key step in the proof of Abel–Ruffini Theorem that there are polynomials of each degree $n \geq 5$ that are not solvable by radicals.

Theorem 4.3 (Feit-Thompson)**.** Every finite group of odd order is solvable.

Corollary 4.3. If a finite group is simple, it is either cyclic of prime order or of even order.

Proof. If G is simple abelian, then $G \simeq \mathbb{Z}/p\mathbb{Z}$ for prime p by Proposition 2.13. Assume G is non-abelian. If G is solvable, then

$$\{e_G\} \subset [G, G] \subset G.$$

Feit-Thompson implies that a non-abelian simple group G is even order. □