INTRODUCTION TO GROUP THEORY

LECTURE NOTES BY STEFAN WANER

Contents

Date: July 2003.

1. Complex Numbers: A Sketch

A **complex number** is just a pair, $z = (a, b)$ of real numbers. We usually write this pair in the form $z = a + ib$, where the "+" and "i" are just decorations (for now). The number a is called the **real part** of z, while b is called the **imaginary part** of z. We denote the set of all complex numbers by $\mathbb{C}$. Note that we can represent any complex number $z = a + ib \in \mathbb{C}$ by a point in the plane.

Examples 1.1. In class of complex numbers and their locations in the plane

Definition 1.2. We define addition and multiplication of complex numbers as follows:

(1) $(a + ib) + (c + id) = (a + c) + i(b + d)$
(2) $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$

In other words, we add complex numbers by adding their real and imaginary parts, and multiply them by treating i as a square root of -1.

Notation 1.3. We use the following shorthand notation:

$a + i \cdot 0 = a$ (That is, $(a, 0) = a$)
$0 + ib = ib$ (That is, $(0, b) = ib$)
$0 + i1 = i$ (That is, $(0, 1) = i$)

Then we see that the sum of a and ib is indeed the single complex number $a + ib$. In other words, we can now think of $a + ib$ as a sum rather than as a wild and crazy way of writing (a, b).

Notes 1.4.

(1) $i^2 = -1$ (Check it and see; remember that i is just shorthand for the complex number $+i1$)
(2) For every complex number z, we have $1 \cdot z = z \cdot 1 = z$
(3) Addition and multiplication of complex numbers obey the same rules (commutativity, associativity, distributive laws, additive identity, multiplicative identity) as the real numbers. We'll see in a minute that there are also inverses.

Examples 1.5. Illustrating the geometry of addition and multiplication: In class.

Definition 1.6. The **magnitude** of the complex number $z = a+ib$ is given by the formula

$$|z| = \sqrt{a^2 + b^2}$$

(This is just its distance from the origin) Also, we define:

$$\bar{z} = a - ib,$$

called the complex conjugate of z.

Examples in class

Now we notice that:

$$z\bar{z} = |z|^2$$

In other words:

$$z \cdot \frac{\bar{z}}{|z|^2} = 1$$

But this says that $\bar{z}/|z|^2$ is the multiplicative inverse of z. In other words,

$$\boxed{z^{-1} = \frac{\bar{z}}{|z|^2}}$$

Examples in class

We now look at the polar form, and we can write

$$z = r\cos\theta + ir\sin\theta = r(\cos\theta + i\sin\theta)$$

We also write this as $re^{i\theta}$. (Explanation in class)

Notes 1.7.

(1) If $z = re^{i\theta}$, then $r = |z|$.
(2) the identity $[r(\cos\theta + i\sin\theta)][s(\cos\phi + i\sin\phi)] = rs(\cos(\theta+\phi) + i\sin(\theta+\phi)$ translates to $re^{i\theta} + re^{i\phi} = re^{i(\theta+\phi)}$, which is what we expect from the laws of exponents.
(3) Addition and multiplication of complex numbers. Also, this gives us the key to the geometric meaning of multiplication.
(4) If we multiply a complex number by itself repeatedly, we now get:

$$[r(\cos\theta + i\sin\theta)]^n = r^n(\cos n\theta + i\sin n\theta),$$

which is known as **De Moivrés formula**. We can use it to find nth roots of any complex number: take the nth root of the magnitude, and divide the angle θ by n. We can also divide $\theta + 2\pi$ by n to get another nth root, and $\theta + 4\pi$, $\theta + 6\pi$, etc. They start repeating when we get to $\theta + 2n\pi$. In other words:

There are $n-1$ different nth roots of any complex number.

Examples 1.8.

A. Find all the 4th roots of i.
B. Find all the 5th roots of $32e^{i\pi/3}$.
C. Find all the roots of the equation $z^3 = i$.

If we choose $r = 1$ in De Moivrés formula, this places us on the unit circle, and we find all kinds of nth roots of 1.

Definition 1.9. The **primitive** nth **root of unity** is the complex number $\omega = e^{2\pi i/n}$. Note that all the other nth roots of unity are powers of ω. In other words, the n nth roots of unity are:

$$1 = \omega^0, \omega, \omega^2, \ldots, \omega^{n-1}.$$

Note This gives us another (easy) way of getting all the nth roots of any complex number: Find one of them, and then multiply it by the different nth roots of unity above!

Exercise Set 1.

1. Find all the 8th roots of unity, sketch their position on the unit circle, and represent them both in Cartesian form ($x + iy$) and polar form ($re^{i\theta}$).Which of them are real, and which pure imaginary?

2. Find all the 5th roots of $32e^{i\pi/3}$

3. (a) Show that, if z is a complex number, then $\bar{z}^n = \overline{z^n}$ for all integers n (including negative ones).

(b) Show that, if ω is an nth root of unity, then so are $\overline{\omega}$ and ω^r for every integer r.

(c) Show that, if ω is an nth root of unity, then $\omega^{-1} = \omega^{n-1}$.

4. (a) The set of **Gaussian integers** is defined as the set $\mathbb{Z}[i]$ of all complex numbers of the form $m_0 + m_1 i$, where m_0 and m_1 are integers. Prove that products of Gaussian integers are Gaussian integers.

(b) If ω is an nth root of unity, define $\mathbb{Z}[\omega]$, the set of **generalized Gaussian integers** to be the set of all complex numbers of the form $m_0 + m_1\omega + m_2\omega^2 + \cdots + m_{n-1}\omega^{n-1}$,where n and m_i are integers. Prove that products of generalized Gaussian integers are generalized Gaussian integers.

2. Sets, Equivalence Relations and Functions

A **set** is an undefined "primitive" notion. Intuitively, it refers to a collection of things called elements. If a is an element of the set S, we write $a \in S$. If a is not an element of the set S, we write $a \notin S$. Some important sets are:

$\mathbb{Z}$, the set of all integers
$\mathbb{N}$, the set of all natural numbers (including 0)
$\mathbb{Z}^+$, the set of all positive inegers
$\mathbb{R}$, the set of all rational numbers
$\mathbb{R}$, the set of all real numbers
$\mathbb{C}$, the set of all complex numbers

We can describe a set in several ways:

(1) by listing its elements; e.g.. $S = \{6, 66, 666\}$
(2) in the form $\{\, x \mid P(x)\}$, where $P(x)$ is a predicate in x, for instance

$$S = \{\, x \mid x \text{ is a real number other than } 6\}$$

or

$$T = \{\, x \in \mathbb{Z} \mid x \text{ odd}\}$$

Note: Two sets are equal if they have the same elements. That is,

$$\boxed{A = B \text{ means } x \in A \Leftrightarrow x \in B}$$

Definitions 2.1. Let A and B be sets.

We say that A is a **subset** of B and write $A \subset B$ if $x \in A \Rightarrow x \in B$.

$A \cap B$ is the intersection of A and B, and is given by
$$A \cap B = \{\, x \mid x \in A \text{ and } x \in B\}$$

$A \cup B$ is the union of A and B, and is given by
$$A \cup B = \{\, x \mid x \in A \text{ or } x \in B\}$$

$\emptyset$ is the empty set; $\emptyset = \{\, x \mid F(x)\}$, where $F(x)$ is any false predicate in x, such as "$x = 3$ and $x \neq 3$" or "Your math instructor drives a red mustang with x doors."

$A - B$ is the complement of B in A, and is given by
$$A - B = \{\, x \mid x \in A \text{ and } x \notin B\}$$

$A \times B$ is the set of all ordered pairs,
$$A \times B = \{\, (a, b) \mid a \in A, b \in B\}$$

If $\{\, A_\alpha \mid \alpha \in \Omega\}$ is any collection of sets indexed by Ω, then:

$\bigcap_{\alpha\in\Omega} A_\alpha$ is the **intersection** of the A_α and is given by
$$\bigcap_{\alpha\in\Omega} A_\alpha = \{\, x \mid x \in A_\alpha \text{ for all } \alpha \in \Omega\}$$

$\bigcup_{\alpha\in\Omega} A_\alpha$ is the **union** of the A_α and is given by

$$\bigcup_{\alpha\in\Omega} A_\alpha = \{\, x \mid x \in A_\alpha \text{ for some}^1\, \alpha \in \Omega\}$$

Note: To prove that two sets A and B are equal, we need only prove that $x \in A \Leftrightarrow x \in B$. In other words, we must prove two things:

(a) $A \subset B$ (ie., $x \in A \Rightarrow x \in B$)
(b) $B \subset A$ (ie., $x \in B \Rightarrow x \in A$)

Lemma 2.2. *The following hold for any three sets A, B and C and any indexed collection of sets B_α ($\alpha \in \Omega$):*

(1) *Associativity:*
$$A \cup (B \cup C) = (A \cup B) \cup C \qquad A \cap (B \cap C) = (A \cap B) \cap C$$
(2) *Commutativity:*
$$A \cup B = B \cup A \qquad A \cap B = B \cap A$$
(3) *Identity and Idempotent*
$$A \cup A = A, \qquad A \cap A = A$$
$$A \cup \emptyset = A, \qquad A \cap \emptyset = \emptyset$$
(4) *De Morgan's Laws:*
$$A-(B\cup C) = (A-B)\cap(A-C), \quad A-(B\cap C) = (A-B)\cup(A-C)$$
Fancy Form:
$$A - \bigcup_{\alpha\in\Omega} B_\alpha = \bigcap_{\alpha\in\Omega}(A - B_\alpha), \quad A - \bigcap_{\alpha\in\Omega} B_\alpha = \bigcup_{\alpha\in\Omega}(A - B_\alpha)$$
(5) *Distributive Laws:*
$$A\cup(B\cap C) = (A\cup B)\cap(A\cup C), \quad A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$$
Fancy Form:
$$A\cup\Big(\bigcap_{\alpha\in\Omega} B_\alpha\Big) = \bigcap_{\alpha\in\Omega}(A\cup B_\alpha), \quad A\cap\Big(\bigcup_{\alpha\in\Omega} B_\alpha\Big) = \bigcup_{\alpha\in\Omega}(A\cap B_\alpha)$$

Proof We prove (1), (2), (3) and a bit of (4) in class. The rest you will prove in the exercise set. □

Definition 2.3. A **partitioning** of a set S is a representation of S as a union of disjoint subsets S_α, called **partitions**:
$$S = \bigcup_{\alpha\in\Omega} S_\alpha$$
where $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$.

Examples 2.4.

A. The set $\mathbb{Z}$ can be partitioned into the odd and even integers.
B. $\mathbb{Z} = 3\mathbb{Z} \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z})$, where $m + 3\mathbb{Z} = \{\, m + 3n \mid n \in \mathbb{Z}\}$. (You will spell this out in more detail in the exercise set.)
C. The set of $n \times n$ matrices can be partitioned into subsets each of which contains matrices with the same determinant.

Definition 2.5. A **relation** on a set S is a subset R of $S \times S$. If $(a, b) \in R$, we write $a\,R\,b$, and say that a **stands in the relation R to b.**

[1] That is, at least one

Examples 2.6.

A. Equality on any set A
B. $\neq$ on any set A
C. $<$ on $\mathbb{Z}$
D. $m \approx n$ if $m - n \in 3\mathbb{Z}$, on $\mathbb{Z}$
E. Row equivalence on the set of $m \times n$ matrices
F. Any partitioning of a set S gives one: Define $a\,R\,b$ if a and b are in the same partition.

Definition 2.7. An **equivalence relation** on a set S is a relation $\approx$ on S such that, for all a, b and $c \in S$:

(1) $a \approx a$ (Reflexivity)
(2) $a \approx b \Rightarrow b \approx a$ (Symmetry)
(3) $(a \approx b$ and $b \approx c) \Rightarrow a \approx c$ (Transitivity)

Examples 2.8.

A. Equality on any set
B. Equivalence mod k on $\mathbb{Z}$ (in class)
C. Row equivalence on the set of $m \times n$ matrices
D. Any partition on S yields an equivalence relation

Definition 2.9. If $\approx$ is an equivalence relation on S, then the **equivalence class** of the element $s \in S$ is the subset

$$[s] = \{\, t \in S \mid t \approx s\}$$

Lemma 2.10. *Let $\approx$ be any equivalence relation on S. Then*

(a) *If $s, t \in S$, then $[s] = [t]$ iff $s \approx t$.*
(b) *Any two equivalence classes are either disjoint or equal.*
(c) *The equivalence classes form a partitioning of the set S.* □

Theorem 2.11. Equivalence Relations "are" Partitions
There is a one-to-one correspondence between equivalence relations on a set S and partitions of S. Under this correspondence, an equivalence class corresponds to a set in the partition. □

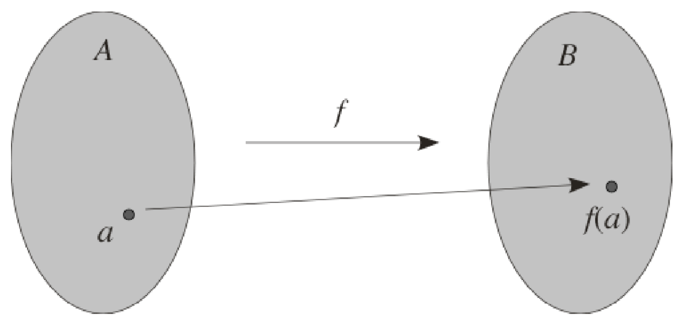
Examples 2.12.

A. $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes of integers mod n. [r] = [s] iff $r - s \in nZ$. We look at these equivalence classes explicitly in class.
B. **Construction of the rationals** Define a relation on $\mathbb{Z} \times \mathbb{Z}^*$ by $(m, n) \sim (k, l)$ iff $ml = nk$. The quotient $\frac{m}{n}$ is defined to be the equivalence class of (m, n). (Exercise set)

Definition 2.13. Let A and B be sets. A **map** or **function** $f\colon A \to B$ is a triple (A, B, f) where f is a subset of $A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ (that is, one and only one $b \in B$) with $(a, b) \in f$. We refer to this element b as $f(a)$. A is called the **domain** or **source** of f and B is called the **codomain** or **target** of f.

Notes:

(1) We think of f a rule which assigns to every element of A a unique element $f(a)$ of B, and we can picture a function $f\colon A \to B$ as shown in the figure.



(2) The codomain of f is not the "range" of f; that is, not every element of B need be of the form $f(a)$.

(3) The sets A and B are *part of the information* of f. For instance, specifying f by saying only "$f(x) = 2x - 1$" is not sufficient because we have not specified the domain and codomain. We should instead say something like this:

"Define $f\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = 2x - 1$."

Examples 2.14. Some in class, plus:

A. If A is any set, we have the identity map $1_A\colon A \to A$; $1_A(a) = a$ for every $a \in A$.

B. If $B \subset A$, then we have the inclusion map $\iota\colon B \to A$; $\iota(b) = b$ for all $b \in B$

C. The empty map $\emptyset\colon \emptyset \to A$ for any set A.

Definition 2.15. Let $f\colon A \to B$ be a map. Then f is **injective** (or **one-to-one**) if

$$f(x) = f(y) \Rightarrow x = y$$

In other words, if $x \neq y$, then $f(x)$ cannot equal $f(y)$.

Examples 2.16.

A. $f\colon \mathbb{R} \to \mathbb{R}$; $f(x) = 2x - 1$ is injective.

B. $f\colon \mathbb{R} \to \mathbb{R}$; $f(x) = x^2 + 1$ is not.

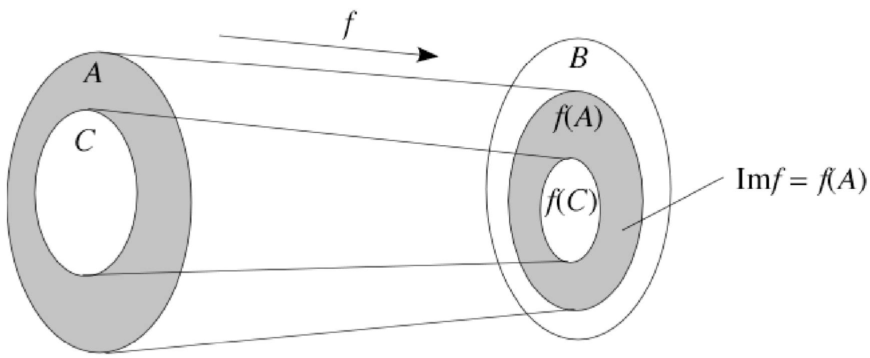
C. The identity $1_A\colon A \to A$ is injective for every set A.

D. The inclusion $\iota\colon B \to A$ is injective for every set A and every subset $B \subset A$.

Definitions 2.17. Let $f\colon A \to B$ be a map, and let $C \subset A$. Then the **image** of C under f is the subset

$$\boxed{f(C) = \{\, f(c) \mid c \in C\}}$$

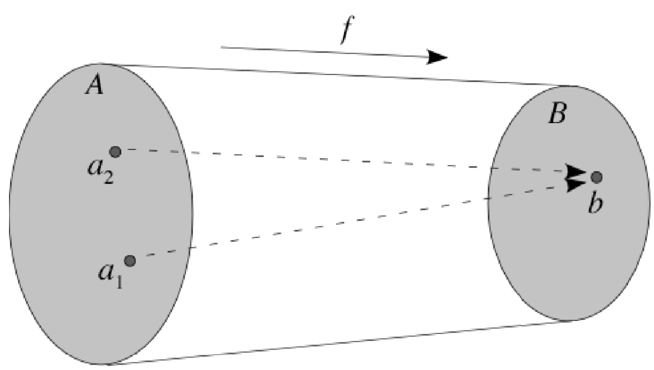
(See the figure.)



The **image** of f is defined as
Im $f = f(A)$.
f is **surjective** (or **onto**) if Im $f = B$. In other words,

$$\boxed{b \in B \Rightarrow \exists a \in A \text{ such that } f(a) = b}$$

Thus, f "hits" every element in B (see figure).



f is surjective iff Im $f = B$

Note: If $f\colon A \to B$, then $f(A)$ is sometimes called the **range of** f.

Examples 2.18.

A. $f\colon \mathbb{R} \to \mathbb{R}; f(x) = x^2 + 1$. Find $f(\mathbb{R})$ and $f[0, +\infty)$.
B. Identity maps are always surjective.
C. The inclusion $\iota\colon C \to B$ is surjective iff $C = B$.

D. The canonical projections of a (possibly infinite) product.
E. Let S be any set and let $\approx$ be an equivalence relation on S. Denote the set of equivalence classes in S by $S/\approx$. Then there is a natural surjection $\nu\colon S \to S/\approx$.

Lemma 2.19. *Let $f\colon A \to B$. Then:*

(a) $f^{-1}(f(C)) \supset C$ *for all* $C \subset A$ *with equality iff* f *is injective;*
(b) $f(f^{-1}(D)) \subset D$ *for all* $D \subset B$ *with equality iff* f *is surjective;*

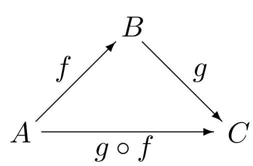
Proof Exercise Set 2. We'll prove (a) in class. □

Definition 2.20. $f\colon A \to B$ is **bijective** if it is both injective and surjective.

Examples 2.21.

A. Exponential map $\mathbb{R} \to \mathbb{R}^+$
B. Square root function
C. Inverse Trig functions
D. Multiplication by a non-zero real number
E. The identity map on any set

Definition 2.22. If $f\colon A \to B$ and $g\colon B \to C$, then their **composite,** $g \circ f\colon A \to C$, is the function specified by $g \circ f(a) = g(f(a))$.



(Example in class.)

Lemma 2.23. *Let $f\colon A \to B$ and $g\colon B \to C$. Then:*

(a) *If f and g are injective, then so is $g \circ f$.*
(b) *If f and g are surjective, then so is $g \circ f$.*
(c) *If $g \circ f$ is injective, then so is f.*
(d) *If $g \circ f$ is surjective, then so is g.* □

Definition 2.24. $f\colon A \to B$ and $g\colon B \to A$ are called **inverse maps** if $g \circ f = 1_A$ and $f \circ g = 1_B$. In this event, we write $g = f^{-1}$ (and say that g **is the inverse of** f) and $f = g^{-1}$. If f has an inverse, we say that f is **invertible.**

Theorem 2.25 (Inverse of a Function)**.**

(a) *$f\colon A \to B$ is invertible iff f is bijective*
(b) *The inverse of an invertible map is unique.*

We prove (a) in class and leave (b) as an exercise. □

Exercise Set 2.

1. Prove Lemma 2.2 (4) and (5).

2. Prove that
$$A \times \bigcup_{\alpha\in\Omega} S_\alpha = \bigcup_{\alpha\in\Omega}(A \times S_\alpha)$$
and
$$A \times \bigcap_{\alpha\in\Omega} S_\alpha = \bigcap_{\alpha\in\Omega}(A \times S_\alpha)$$

3. (cf. Example 2.4[B]) Prove that $\mathbb{Z}$ can be partitioned as $\mathbb{Z} = 3\mathbb{Z} \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z})$, where $m + 3\mathbb{Z} = \{m + 3n \mid n \in \mathbb{Z}\}$. (You must show that $\mathbb{Z}$ is indeed the union of the three sets shown. [Hint: consider the remainder when an arbitrary integer is divided by 3.]

4. Give an example of a relation on $\mathbb{Z}$ which is:
- **a.** reflexive and symmetric but not transitive;
- **b.** transitive and reflexive but not symmetric;
- **c.** transitive and symmetric but not reflexive.

5. Verify that the relation on $Z \times Z^*$ given by $(m, n) \approx (k, l)$ iff $ml = nk$ is an equivalence relation.

6. **a.** Let $M(n)$ be the set of $n \times n$ matrices, let P be some fixed $n \times n$ matrix, and define $f : M(n) \to M(n)$ by $f(A) = PA$. (f is called "left translation by P.") Show that f is injective iff P is invertible.
- **b.** Let f be as in (a). Show that f is surjective iff P is invertible.

7. Prove Lemma 2.19.

8. **a.** Give an example of a map $f : A \to B$ and a map $g : B \to C$ with $g \circ f$ injective but g not injective. (See Lemma 2.23.)
- **b.** Give an example of a map $f : A \to B$ and a map $g : B \to C$ with $g \circ f$ surjective but f not surjective. (See Lemma 2.23.)

9. **a.** By citing appropriate results in these notes, give a two-line proof that if $f : A \to B$ and $g : B \to C$ are bijective, then so is $g \circ f$.
- **b.** Give an example of a map $f : A \to B$ and a map $g : B \to C$ with $g \circ f$ bijective, but with neither f nor g bijective.

10. Prove Theorem 2.25(b).

11. Prove that composition of functions is associative: $(f \circ g) \circ h = f \circ (g \circ h)$ and **unital**: $f \circ 1_A = 1_B \circ f = f$ for all $f : A \to B$.

12. Let $f : A \to B$, and define a relation on A by $a \approx a$ if $f(a) = f(a')$. Show that $\approx$ is an equivalence relation on A.

3. Mathematical Induction and Properties of the Integers

The *Axiom of Mathematical Induction* is one of the central axioms of arithmetic. Here is one of the forms it can take:

Axiom of Mathematical Induction
If S is any subset of N such that:
(a) $0 \in S$;
(b) $n \in S \;\Rightarrow\; n+1 \in S$,
then $S = \mathbb{N}$.

The following is a theorem in "meta-mathematics":

Theorem 3.1 (Principle of Mathematical Induction)**.**
If $P(n)$ is any proposition about the natural number n such that:
(a) *$P(0)$ is true;*
(b) *If $P(n)$ is true, then $P(n+1)$ is true,*
then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof: Let $S = \{\, n \in N \mid P(n) \text{ is true}\} \ldots$ □

Corollary 3.2 (General Principle of Mathematical Induction)**.**
If $P(n)$ is any proposition about the natural number $n \geq k$ such that:
(a) *$P(k)$ is true;*
(b) *If $P(n)$ is true, then $P(n+1)$ is true,*
then $P(n)$ is true for all $n \geq k$.

Proof: Let $Q(n)$ be the proposition "$P(n+k)$ is true," and apply the theorem to Q. □

Examples 3.3. We prove the following by induction:

A. $1 + 2 + \cdots + n = n(n+1)2$ for all $n \geq 1$.
B. De Morgan's Law for finite unions: If $A,\ B_i$ $(i = 1, 2, \ldots)$ are any sets, then:
$$A - \bigcup_{i=1}^{n} B_i = \bigcap_{i=1}^{n} (A - B_i)$$
C. Every polynomial over $\mathbb{Z}$ factors as a product of irreducible polynomials over $\mathbb{Z}$.

Definition 3.4. The integer a **divides** the integer b if there exists an integer k such that $b = ak$. When this is the case, we write $a|b$.

Definition 3.5. The positive integer h is the **greatest common divisor** (gcd) or **highest common factor** (hcf) of a and b if

(a) h is a divisor of a and b; (we write $h|a$ and $h|b$)
(b) If d is a divisor of a and b, then d is a divisor of h. That is,
$$d|a \text{ and } d|b \Rightarrow d|h$$

We denote the hcf h of a and b by (a, b).

Note: The hcf is always positive, so that $(\pm a, \pm b) = (a, b)$.

Proposition 3.6 (Existence and Properties of the hcf)**.**
If a and b are integers, not both 0, then (a, b) exists. Moreover, there exist integers m and n such that

$$ma + nb = (a, b)$$

Proof: Here is the very elegant proof in Herstein: Let

$$M = \{ ma + nb \mid m, n \in \mathbb{Z}\}$$

Then M certainly contains positive integers (since a and b are not both zero), so let h be the smallest positive element of M. We claim that h is the hcf, which not only proves existence, but also the property
$h = ma + nb.$
Indeed, we need to show properties (a) and (b) above.

Property (a): Let us prove that h is a divisor of a. If $a = 0$, then h is certainly a divisor of a. If $a \neq 0$, then by the division algorithm we can divide a by h to obtain

$$a = ph + r \text{ with } 0 = r < h$$

(that's even true is a is negative!) Hence

$$\begin{aligned} r &= a - ph \\ &= a - p(ma + nb) \\ &= (1 - pm)a + (-pn)b \in M. \end{aligned}$$

But now $r \in M$ is non-negative, and is smaller than the smallest positive element, which forces it to be zero. In other words, h is a divisor of a, as claimed.

Property (b): If d is a common divisor of a and b, we must show that d is also a divisor of h. But the hypothesis implies that

$$a = kd \text{ and } b = ld$$

for some k and l. Hence

$$\begin{aligned} h &= ma + nb \\ &= m(kd) + m(ld) = d(mk + ml), \end{aligned}$$

showing that h is divisible by d, as required. □

Definition 3.7. The integers a and b are **relatively prime** if $(a, b) = 1$.

Corollary 3.8 (Relatively Prime Integers)**.**
If a and b are relatively prime, then there exist integers m and n such that

$$ma + nb = 1.$$

□

Example in class

Definition 3.9. The integer $p > 1$ is **prime** if its only divisors are ± 1 and $\pm p$. It follows that p is prime iff $(n, p) = 1$ or p for every integer n.

Lemma 3.10.
If $(a, b) = 1$ *and* $a \mid bc$, *then* $a \mid c$.

Proof: Choose m and n such that $ma + nb = 1$. Multiplying by c gives

$$mac + nbc = c.$$

Since a divides both terms on the left (the second term by hypothesis), it must divide the term on the right. □

Corollary 3.11.

(a) *If* p *is prime, and* $p \mid bc$, *then* $p \mid b$ *or* $p \mid c$. More generally,

(b) *If* p *is prime, and* p *divides any product of integers, then it divides at least one of them.*

Proof: For part (a), assume $p \mid bc$ but $p \nmid b$. Then $(p, b) = 1$, so by the lemma, $p|c$. Part (b) follows by an inductive argument. □

Extra Reading: Unique factorization of integers into primes

Exercise Set 3.

Prove the the statements in Exercises 1 to 3 by induction:

1. $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$ for $n \geq 1$

2. $1^3 + 2^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$ for $n \geq 1$

3. $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for $n \geq 1$

4. Let $R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$. Prove by induction that $R^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$ for all $n \geq 1$.

The following are taken from Herstein's *Topics in Algebra* (p. 23):

5. Prove: If $a \mid b$ and $b \mid a$, then $a = \pm b$.

6. Prove: If $a \mid x$ and $b \mid x$, and $(a, b) = 1$, then $ab \mid x$.

7. (A step-by-step approach to Herstein's starred problem) Let p be a prime number.

(a) Use the binomial theorem to show that $(n+1)^p - (n^p + 1)$ is divisible by p for all $n \geq 1$.

(b) Use part (a) and induction to prove that, for all positive integers a, $a^p - a$ is divisible by p.

(c) Deduce that (b) is true for all integers a.

Note: You have proved that $a^p - a$ is divisible by p for every prime p. That is, $a^p - a \equiv 0 \mod p$, as stated in Herstein's problem.

4. Groups

Definition 4.1. A **binary operation** on a set S is a map $*\colon S \times S \to S$. In other words, the operation $*$ assigns to each pair (s, t) of elements in S an element $*(s, t)$, which we shall write as $s * t$, of S.

Examples 4.2.

A. Addition, subtraction and multiplication on $\mathbb{R}$
B. Division and multiplication in $\mathbb{Q}^*$
C. Composition in $Map(X, X)$, the set of maps $X \to X$
D. Multiplication of $n \times n$ matrices
E. Concatenation of strings in a given set of symbols
F. $\mathbb{N}$ is not closed under subtraction; hence subtraction is not a binary operation on $\mathbb{N}$.
G. The quotient a/b is not defined for every pair of real numbers (a, b), Hence division is not a binary operation on $\mathbb{R}$.

Recall that $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes of integers modulo n.

Lemma 4.3 (Addition modulo n)**.**
The operation $+\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *given by* $[m] + [n] = [m + n]$ *is a well defined binary operation.* □

Some of these operations have the nice properties we ascribe to a *group*:

Definition 4.4. A **group** $(G, *)$ is a set G together with a binary operation $*$ on G such that:

(a) $*$ is associative.
(b) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
(c) There is an element $e \in G$ called an **identity element** such that $e * g = g * e = g$ for every $g \in G$.
(d) For every $g \in G$, there exists an element $g' \in G$, called an **inverse** of g such that $g * g' = g' * g = e$.

Examples 4.5.

A. $(\mathbb{Z}, +)$
B. $(\mathbb{Q}^*, \times)$
C. $(M(m, n), +)$
D. $(GL(n; \mathbb{Q}), \times)$, $(GL(n; \mathbb{R}), \times)$, and $(GL(n; \mathbb{C}), \times)$
E. The set
$$C_n = \{\, \omega^0, \omega, \omega^2, \ldots, \omega^{n-1} \,\} \subset \mathbb{C}$$
of nth roots of unity, under multiplication.
F. $(\mathbb{Z}/n\mathbb{Z}, +)$ Compare its group structure with that of C_n.
G. The set of all invertible maps $\mathbb{R} \to \mathbb{R}$ under composition
H. The set S_A of all bijections of a set A, under composition
I. The unit circle,
$$S^1 = \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$$
under multiplication

J. $\mathbb{Z}$ is not a group under subtraction.
K. $\mathbb{Z}$ is not a group under multiplication.
L. $\mathbb{Q}$ is not a group under multiplication

Note: When we do not want to be explicit about the group operation $*$, we shall leave it out, and write $a * b$ as ab or sometimes as $a + b$ when appropriate. Similarly, we shall write a group as G rather than $(G, *)$ when the group operation is understood.

Lemma 4.6 (Cancellation Law, Uniqueness of Identity and Inverses)**.** *If G is a group, then the following are true:*

(a) Left Cancellation: *If g, h and k have the property that $gh = gk$, then $h = k$.*
(b) Right Cancellation: *If g, h and k have the property that $hg = kg$, then $h = k$.*
(c) Uniqueness of the Identity: *If e and e' are both identities in G, then $e = e'$.*
(d) Uniqueness of Inverses: *If g' and g'' are both inverses of $g \in G$, then $g' = g''$.* □

Note: As a consequence of part (d) of the lemma, we shall speak of *the* inverse of g and write it as g^{-1}. Similarly, we shall speak of *the* identity element of a group.

Lemma 4.7 (Product of Inverses)**.** *If G is a group and $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.*

The proof is in the exercise set. □

Definition 4.8. An **abelian group** is a group G satisfying the commutative law:

$$ab = ba \text{ for all } a, b \in G.$$

Examples 4.9. Spot which of the above examples of groups are abelian.

Further Important Examples of Groups 4.10.

A. **The Dihedral groups D_n**
D_n is the set of symmetries of the regular n-gon (n rotations and n reflections). Illustrated in class. If a is rotation through $2\pi/n$, and if b is reflection in the x-axis, then we can write D_n as:

$$D_n = \{\, e, a, a^2, \ldots, a^{n-1},\ b, ba, ba^2, \ldots, ba^{n-1} \,\}$$

Checking that this indeed gives us a group is tedious, but we shall see in the exercises how to avoid this by realizing D_n as a group of 2×2 matrices. We can multiply elements according to the rule: $ba = a^{-1}b$. In terms of "generators and relations" we can also describe D_n as:

$$D_n = \langle\, a, b \mid a^n = b^2 = e,\ bab^{-1} = a^{-1} \,\rangle$$

B. **The Symmetric groups S_n**
S_n is defined to be the group of permutations (self-bijections) of the set $\{1, 2, 3, \ldots, n\}$. In other words, $S_n = S_{\{1,2,3,\ldots,n\}}$. We look at the examples S_2 and S_3 and their multiplicative structure in class.

C. **The Quaternion group Q_8**
Q_8 is defined by

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \right\}$$

The group operation is matrix multiplication, and i is the familiar complex number. We abbreviate these elements as follows:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

In class, we verify the following:

$$i^2 = j^2 = k^2 = -1, \text{ and } ij = k = -ji, jk = i = -kj, ki = j = -ik$$

Exercise Set 4.

1. List all six elements of D_3, together with its multiplication table.
2. Show that,if G is a group and g and g' are such that $gg' = e$, then $g' = g^{-1}$.

Hand In:

1. Show that the operation $\cdot : \mathbb{Z}/n\mathbb{Z} \times Z/n\mathbb{Z} \to Z/n\mathbb{Z}$ given by $[m] \cdot [k] = [mk]$ is a well defined binary operation.
2. (a) Prove Lemma 4.7.
(b) Show that, if G is abelian, then $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.
(c) Give an example to show that $(ab)^{-1} \neq a^{-1}b^{-1}$ in general.
3. Show that, if G is a group and $g \in G$ is such that $g^n = g^m$ for some $m \neq n$, then there exists an integer r with $g^r = e$.
4. Show that, if G is a finite group and $g \in G$, then there exists a positive integer r with $g^r = e$.
5. Prove that, in any finite group G, the inverse of each element is a power of itself.
6. Recall from the exercises on induction that if $R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$, then one has $R^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$ for all $n \geq 1$.
(a) Let $\theta = 2\pi/n$. Show that $R^n = I$, the identity matrix, and that $\{I, R, R^2, \ldots, R^{n-1}\}$ is a group under matrix multiplication. Which group does it remind you of?
(b) Let R and θ be as above, and let $T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Show that $T^2 = I$, and that $TRT^{-1} = R^{-1}$. Deduce that

$$\{ I, R, R^2, \ldots, R^{n-1}\, T, TR, TR^2, \ldots, TR^{n-1} \}$$

is a realization of D^n, and use this to construct the multiplication table for D_3.

7. Product Groups If G and G' are groups, define an operation on $G \times G'$ by $(a, a')(b, b') = (ab, a'b')$. Show that this turns $G \times G'$ into a group.

5. Subgroups

First, some comments and definitions.

Remark The notation + for the group operation will only be used for abelian groups, and then only for groups in which it stands for what is commonly thought of as the sum. Such a group will be called **additive** and its identity element will be written as 0 rather than e.

Definitions 5.1.

(1) The **order** of the finite group G is the cardinality of G as a set, and will be denoted by $|G|$.
(2) If S is a subset of G such that for every s and $t \in S$, one has $st \in S$, then we shall say that S is **closed** under the group operation in G. Note that S then inherits a binary operation from G. If S is a subset of G which is closed under the group operation, we refer to the resulting binary operation on S as the **induced operation on** S .

Examples 5.2.

A. $2\mathbb{Z} \subset Z$ is closed under the group operation (+) of $\mathbb{Z}$.
B. $\mathbb{N} \subset \mathbb{Z}$ is also closed under addition.
C. The set of odd numbers is not a closed subset of $\mathbb{Z}$ under addition.

Definition 5.3. A **subgroup** of G is a subset $H \subset G$ such that:

(a) H is closed under the group operation;
(b) H is a group in its own right under the induced operation. If H is a subgroup of G, we shall write $H < G$.

Examples 5.4.

A. Every group is a subgroup of itself.
B. The subset $\{e\} \subset G$ is a subgroup.
C. $2\mathbb{Z} \subset \mathbb{Z}$ is a subgroup because it is a group in its own right.

Note: A subgroup H of G must be a non-empty subset of G, since being a group in its own right implies that it contains the identity.

In practice, the following criterion is extremely useful in checking that a given subset of G is a subgroup:

Proposition 5.5 (Test for a Subgroup)**.** *A subset $H \subset G$ is a subgroup of G iff:*

(a) *H is non empty and closed under the group operation*
(b) *H is closed under inverses: if $h \in H$, then $h^{-1} \in H$.* □

In words, this tells us that for a subset to be a subgroup, it must be nonempty and contain the products and inverses of all its elements. It also gives us the following mechanical test:

How to check that H is a subgroup of G

(a) Show that $H \neq \emptyset$, and if a and $b \in H$, then $ab \in H$
(b) Show that, if $h \in H$, then $h^{-1} \in H$.

We can now give many more examples of subgroups.

Examples 5.6.

A. The subgroup $SL(n)$ of $GL(n)$ consisting of $n \times n$ matrices with determinant $+1$
B. $G = GL(n)$; H the set of upper triangular matrices
C. Find all the subgroups of C_6.
D. Find all the subgroups of D_2.
E. Some finite subgroups of the circle group
F. Subgroups of $\mathbb{Z}$
G. The continuous functions in $(\mathbb{R}^{\mathbb{R}}, +)$

Definition 5.7. A group G is called **cyclic** if it contains an element g such that every element of G is a (possibly negative) power of g. We refer to g as a **generator** of G.

Examples 5.8.

A. Generators of C_n; for $g = \omega^r$ to be a generator, some power of it must be ω. This translates to an interesting requirement on r.
B. Generators of $\mathbb{Z}$
C. Generators of $m\mathbb{Z}$
D. D_n is not cyclic.
E. $\mathbb{Q}$ is not cyclic under $\times$

Definition 5.9. A **proper subgroup** of G is a subgroup $H < G$ such that $H \neq G$.

Definition and Proposition 5.10. *If $g \in G$, let $\langle g \rangle$ denote the subset $\{ g^n \mid n \in \mathbb{Z} \}$. Then $\langle g \rangle$ is a subgroup of G, called the* **cyclic subgroup generated by** *g.* □

Examples 5.11.

A. Look at various such subgroups of C_n
B. $\langle a \rangle$ and $\langle b \rangle$ are subgroups of D_n.
C. The subgroup of $GL(n)$ generated by a rotation matrix
D. Cyclic subgroups of $\mathbb{Z}$

Theorem 5.12 (Subgroups of Cyclic Groups)**.**
Every subgroup of a cyclic group is cyclic.

Proof: Let G be a cyclic group, so that $G = \langle g \rangle$, say, and let $H < G$. Then H is a set of powers of g. Choose n to be the smallest positive exponent of elements in H;

$n = \min\{\, i \in N \mid i > 0 \text{ and } g^i \in H \,\}$.
Then I claim that every element of H is a power of $a = g^n$, giving the result. Indeed, if $h \in H$ is not the identity, then either h or h^{-1} is of the form g^m with $m > 0$, so that $m = n$. Dividing m by n gives
$m = qn + r$
with $r < n$ or $r = 0$, whence
$g^m = (g^n)^q g^r$, giving
$g^r = g^m (g^{-n})^q$,
a product of elements of H, showing that $g^r \in H$. By the choice of m, we must have $r = 0$, giving
h (or h^{-1}) $= g^m = (g^n)^q$,
proving the result. □

Corollary 5.13 (Classification of subgroups of $\mathbb{Z}$)**.**
Every subgroup of $\mathbb{Z}$ is cyclic and of the form $n\mathbb{Z}$. □

Exercise Set 5.

1. Which of the following are closed under the group operation?
  (a) The set of upper-triangular $n\times n$ matrices as a subset of $(M(n,n),+)$
  (b) The set of upper-triangular $n\times n$ matrices as a subset of $(GL(n,\mathbb{R}),\times)$
  (c) The set of pure rotations in D_n
  (d) The set of transpositions in S_n

2. Which of the following are subgroups of $(\mathbb{C},+)$?
  (a) $\mathbb{R}$
  (b) $7\mathbb{Z}$
  (c) $i\mathbb{R}$ (the set of pure imaginary numbers including 0)
  (d) $3\mathbb{Q}$

Hand In:

1. Which if the following are subgroups of $GL(n,\mathbb{R})$? Justify your answer in in each case.
  (a) $n \times n$ matrices with determinant 2
  (b) $n \times n$ matrices with determinant 1
  (c) $n \times n$ matrices with determinant a power of 3
  (d) $n \times n$ matrices with determinant ± 1
  (e) $n \times n$ matrices A with $AA^T = I$

2. (a) Prove that, if H and K are subgroups of G, then $H \cap K$ is also a subgroup of G.
  (b) Show that the intersection of any collection of subgroups of a group G is a subgroup of G.
  (c) True or false? The union of any two subgroups of a group is again a subgroup. Prove or give a counterexample.

3. One-Step Test for Subgroups
Prove that a subset $H \subset G$ is a subgroup of G iff H is nonempty, and $hk^{-1} \in H$ whenever h and $k \in H$.

4. Describe the cyclic subgroups of $GL(2,\mathbb{R})$ generated by:

(a) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$

5. Show that a cyclic group with only one generator has order at most two. [Hint: consider the inverse of a generator ...]

6. Prove that every cyclic group is abelian.

7. (a) Show that any group G with no proper subgroups other than $\{e\}$ is cyclic.

(b) Now deduce that, in fact, such a group must be finite of prime order.

8. Order of an Element of G

If G is a group and $g \in G$, the **order of** g is the smallest positive integer k with the property that $g^k = e$. If no such k exists, we say that g **has infinite order.**

(a) Find the order of ω^3 in C_{666}

(b) If $g \in G$, show that g has order k iff $|\langle g \rangle| = k$

9. Conjugate Subgroups

Let $H < G$ be a subgroup, and let $g \in G$. Define:

$gHg^{-1} = \{\, ghg^{-1} \mid h \in H \,\}$

Show that gHg^{-1} is a subgroup of G. We call this subgroup the **conjugate of H under g.**

6. The Permutation Groups

Recall that S^n is the group of all permutations of the set $\{1, 2, \ldots, n\}$.

Definition 6.1. The **cycle** $(n_1, n_2, \ldots, n_m)$ of distinct integers $n_i \leq n$ is the element σ of S_n defined by:

$$\sigma(j) = \begin{cases} n_{i+1} & \text{if } j = n_i \text{ and } i \leq m-1 \\ n_1 & \text{if } j = n_m \\ j & \text{otherwise} \end{cases}$$

We call m the **length** of the cycle.

Examples 6.2. In class; including 1-cycles, 2-cycles, etc.

Notes

(a) $(n_1, n_2, \ldots, n_m) = (n_m, n_1, n_2, \ldots, n_{m-1}) = \ldots$
(b) $(n_1, n_2, \ldots, n_m)^{-1} = (n_m, n_{m-1}, \ldots, n_1)$

Multiplying Cycles Practice examples in class, and specifically $(1, 2, 3, 4)(4, 5, 6, 7)$

Examples 6.3. Some Permutation Groups

A. S_3
B. S_4
C. D_n for various n may be represented as a group of permutations—namely, what the rotations and reflections do to the vertices
D. Rigid motions of the cube

Definition 6.4. The two cycles $(n_1, n_2, \ldots, n_m)$ and $(r_1, r_2, \ldots, r_s)$ are **disjoint** if $\{n_1, n_2, \ldots, n_m\}$ and $\{r_1, r_2, \ldots, r_s\}$ are disjoint as sets.

Note: Multiplication of disjoint cycles is commutative.

If $\sigma \in S_n$, define an equivalence relation on $\{1, 2, \ldots, n\}$ by $a \approx b$ if there exists an $r \geq 0$ with $\sigma^r(a) = b$.

Lemma 6.5. *The relation defined above is indeed an equivalence relation. (Proof in the Exercise set)* □

Definition 6.6. The equivalence classes of the relation defined above are called the **orbits** in $\{1, 2, \ldots, n\}$ under σ.

Lemma 6.7. *Each orbit in $\{1, 2, \ldots, n\}$ under $\sigma \in S_n$ has the form*

$$\{k, \sigma(k), \sigma^2(k), \ldots, \sigma^{j-1}(k)\}$$

for some $k \in \{1, 2, \ldots, n\}$.

Proof: Let $\mathcal{O}$ be any orbit under σ, and choose $k \in \mathcal{O}$. Consider the subset $\mathcal{S} = \{k, \sigma(k), \sigma^2(k), \ldots\} \subset \{1, 2, \ldots, n\}$. By definition of the equivalence relation, every element of the orbit containing k must be a power of σ applied to k, and hence in $\mathcal{S}$. Conversely, every element of $\mathcal{S}$ must be in the same orbit as k. It follows that the orbit of $\mathcal{O}$ of k is exactly the set $\mathcal{S}$. That is, $\mathcal{O} = \mathcal{S}$.

What, exactly, does $\mathcal{S}$ look like? Since $\mathcal{S}$ cannot have more than n elements, we must have repetitions; that is, $\sigma^i(k) = \sigma^j(k)$ for some $i < j < n$. Let j be the smallest integer ≥ 1 such that $\sigma^i(k) = \sigma^j(k)$ for some $i < j$. Claim: $i = 0$; that is, $\sigma^j(k) = 1$. Indeed, if $i > 0$, (so that $j \geq 2$) then apply σ^{-1} to both sides of the equation $\sigma^i(k) = \sigma^j(k)$, getting $\sigma^{i-1}(k) = \sigma^{j-1}(k)$, with $j - 1 \geq 1$, contradicting the fact that j was the smallest such integer. Because of the claim, it also follows that $k, \sigma(k), \sigma^2(k), \ldots, \sigma^{j-1}(k)$ are all distinct. Hence, $\mathcal{O}$ is the set described. □

Theorem 6.8 (Disjoint Cycle Representation)**.**
Every permutation of n letters is a product of disjoint cycles. Further, any two decompositions of into such a product give the same disjoint cycles.

Proof: If σ is a permutation of $N = \{1, 2, \ldots, n\}$, then N is a disjoint union of equivalence classes. Each of these classes is of the form $\{k, \sigma(k), \sigma^2(k), \ldots, \sigma^{j-1}(k)\}$ by the lemma. Let the disjoint equivalence classes be $\{k_1, \sigma(k_1), \sigma^2(k_1), \ldots, \sigma^{r_1}(k_1)\}$, $\{k_2, \sigma(k_2), \sigma^2(k_2), \ldots, \sigma^{r_2}(k_2)\}$, $\ldots$, $\{k_q, \sigma(k_q), \sigma^2(k_q), \ldots, \sigma^{r_q}(k_q)\}$.We now observe that

$$\sigma = (k_1, \sigma(k_1), \sigma^2(k_1), \ldots, \sigma^{r_1}(k_1))(k_2, \sigma(k_2), \sigma^2(k_2), \ldots, \sigma^{r_2}(k_2)) \\ \ldots (k_q, \sigma(k_q), \sigma^2(k_q), \ldots, \sigma^{r_q}(k_q)),$$

a product of disjoint cycles. □

Examples 6.9. Express the following as products of disjoint cycles:

A. $(1, 2, 3)(3, 4, 5)$
B. $(1, 2)(2, 1, 3)(4, 3, 1)$
C. $(1, 2, 3)^{-1}(3, 5, 6)(2, 1)$
D. $(a, b)(b, c)(c, d)(e, f)(f, g)$

Definition 6.10. A cycle of length 2 is called a **transposition.**

Theorem 6.11 (Everything is 2-Cycles)**.**
Every permutation of $\{1, 2, \ldots, n\}$ is a product of (not necessarily disjoint) transpositions. □

Note: We can ignore cycles of length 1 in such a decomposition, or we can write, for example, (1) = (1, 2)(1, 2).

Lemma 6.12 (Effect of a 2-Cycle on the Number of Orbits)**.**
If τ is a transposition and σ is any permutation in S_n, then the number of disjoint orbits in $\tau\sigma$ and σ differ by 1. (Note that disjoint orbits include those of length 1.)

Proof: Let $\tau = (a, b)$. We look at two cases:

Case 1: a is in one of the disjoint cycles of σ and b is in another.
Then we see in class how to glue τ to the three cycles involved to get a single

disjoint one. In other words, multiplication by τ has decreased the number of disjoint cycles by 1.

Case 2. a and b are in the same cycle of σ.
Then we observe that

$$(a, b)(a, x, y, z, \ldots, q, b, r, s, t, ,, , k) = (a, x, y, z, \ldots, q)(b, r, s, t, \ldots, k).$$

In other words, it breaks up that cycle into two disjoint ones, thereby increasing the number of disjoint cycles by 1. □

Theorem 6.13 (Parity is Well-Defined)**.**
Any two decompositions of σ as a product of transpositions have the same parity. (That is, the number of transpositions is either odd for both or even for both.)

Proof: Suppose that the permutation $\sigma \in S_n$ can be expressed in two ways as product of 2-cycles:
$\sigma = \tau_1\tau_2 \ldots \tau_s = \epsilon_1\epsilon_2 \ldots \epsilon_t$.
We must show that $s \equiv t \mod 2$. But
$\sigma = \tau_1\tau_2 \ldots \tau_s\iota$
where ι is the identity; $\iota = (1)(2)...(n)$. By the lemma, the number of disjoint cycles in σ must therefore be congruent to $n + s \mod 2$. Similarly, applying this fact to the second decomposition gives
$n + s \equiv n + t \mod 2$,
whence $s \equiv t \mod 2$, as required. □

Definition 6.14. A permutation that can be expressed as an even number of transpositions is called an **even permutation.** Otherwise, it is called an **odd permutation.** We write

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Definition and Proposition 6.15.

(a) *The set of even permutations in S_n is a subgroup, called A_n, the* **alternating group on n letters.**

(b) $|A_n| = \dfrac{|S_n|}{2}$ □

Exercise Set 6.

1. Prove Lemma 6.5.

2. Write down cycle decompositions of all 24 of the rigid motions of the cube by regarding each rigid motion as a permutation of the 6 faces. The set of these permutations is a subgroup of S_6 which we shall call S_{CUBE}. Prove or disprove: S_{CUBE} is a subgroup of A_6.

3. Represent the complete group of rigid motions of the regular tetrahedron as a subgroup of S_4. (Consider rotations about all possible axes...) Deduce that this group is just A_4.

4. (a) Prove that sgn: $S_n \to C_2$ is a group homomorphism.

(b) Show that parity is not affected by conjugation; that is, if $\sigma, \rho \in S_n$, then $\operatorname{sgn}(\sigma^{-1}\rho\sigma) = \operatorname{sgn}(\rho)$.

5. (a) Let $x = (1,2)(3,4) \in S_8$. Find an element $a \in S_8$ such that $a^{-1}xa = (5,6)(1,3)$.

(b) Show that there is no element $a \in S_8$ with $a^{-1}(1,2,3)a = (1,3)(5,7,8)$. [Hint: see Exercise 4(b).]

6. (Herstein, p. 81 #11) Prove that the smallest subgroup of S_n containing $(1,2)$ and $(1,2,\ldots,n)$ is S_n. (In other words, these generate S_n.)

7. Cosets and Lagrange's Theorem

We now define a most peculiar relation on the elements of a group, arising from a given subgroup:

Definition 7.1. If G is a group and $H \subset G$ is a subgroup, define a relation on G by

$$a \approx_H b \Leftrightarrow a^{-1}b \in H$$

We say that a is **congruent to b mod H.**

Now, saying that $a^{-1}b \in H$ is the same as saying that $a^{-1}b = h$ for some $h \in H$. In other words, $b = ah$ for some $h \in H$. Thus:

$$\begin{aligned} a \approx_H b &\Leftrightarrow a^{-1}b \in H \\ &\Leftrightarrow b = ah \text{ for some } h \in H \end{aligned}$$

Lemma 7.2. *Congruence mod H is an equivalence relation.* □

What do the equivalence classes look like?

Definition 7.3. If $H \subset G$ and $g \in G$, then define the **left coset of H containing g** as

$$gH = \{ gh \mid h \in H \}$$

Proposition 7.4 (Congruence mod H and Cosets)**.**

(a) *The following are equivalent:*
   - (i) $a \approx_H b$
   - (ii) $a^{-1}b \in H$
   - (iii) $b = ah$ *for some* $h \in H$
   - (iv) $b \in aH$
   - (v) $bH \subset aH$
   - (vi) $bH = aH$

(b) *The left cosets aH are the equivalence classes of equivalence mod H. Thus, two left cosets are either equal or disjoint (this being true of equivalence classes in general).*

Proof: We prove (a) in class. For part (b), denote the equivalence class of $a \in G$ by $[a]$. One has

$$\begin{aligned} b \in [a] &\Longleftrightarrow a \approx_H b && \textit{Definition of equivalence classes} \\ &\Longleftrightarrow b \in aH && \textit{By part (a), (i)} \Rightarrow \textit{(iv)} \end{aligned}$$

whence $[a] = aH$. That is, the equivalence classes are just the left cosets, as required. □

Examples 7.5.

A. Cosets of $2\mathbb{Z}$ in $\mathbb{Z}$

B. Cosets of $3\mathbb{Z}$ in $\mathbb{Z}$
C. Cosets of $n\mathbb{Z}$ in $\mathbb{Z}$
D. $G = C_6;\ H = C_3$
E. $G = C_{mn};\ H = C_m$
F. $G = D_n;\ H = C_n$
G. $G = \mathbb{Z}/6\mathbb{Z};\ H = \{0, 3\}$
H. $G = S^1;\ H = C_3$

Lemma 7.6. *If G is a finite group and $H < G$, then any two left cosets of H have the same cardinality.*[2] □

Theorem 7.7 (Lagrange)**.**
Let G be any finite group and $H < G$. Then $|H| \,\Big|\, |G|$. □

Note The "converse" is not true; if G is a group, and m is a divisor of $|G|$, then there need not exist a subgroup of order m. (See the exericse set.)

Corollary 7.8.
(a) *Every group of prime order is cyclic.*
(b) *The order of every element of a finite group divides the order of the group.*
(c) (a consequence of (b)) *If G is a finite group, and $g \in G$ has the property that $g^k = e$, then the order*[3] *of g divides k.*
(d) *If G is a finite group, and $g \in G$, then $g^{|G|} = e$.* □

Definition 7.9. If $H < G$, then define G/H to be the set of left cosets of H in G. If G is finite, then **the index of H in G** is defined as the number of left cosets of H in G, and written as $[G : H]$. That is,

$$[G : H] = |G/H|$$

Consequences: (1) $|G/H| = \dfrac{|G|}{|H|}$; (2) $|G| = [G : H] \cdot |H|$.

Exercise Set 7.
1. Prove that A_4 has no subgroup of order 6, thus contradicting the "converse" of Lagrange's theorem.
2. (a) List all the left cosets of $C_{333} = \langle \omega^2 \rangle \subset C_{666}$.
(b) List all the left cosets of $H = \langle b \rangle \subset D_8$.
(c) List all the left cosets of $H = \langle a \rangle \subset D_8$.
3. Let $H < G$. Define a relation $\approx^H$ on the elements of G by $a \approx^H b$ iff $ab^{-1} \in H$.
(a) Show that this is an equivalence relation.
(b) Show that the equivalence classes are the **right cosets**, $Hg = \{\, hg \mid h \in H \,\}$.

[2] Two sets are defined to have the same cardinality if there is a bijection from one to the other. (Notice that "having the same cardinality" is an equivalence relation on the class of all sets.)

[3] See Exercise Set 4 # 8.

(c) Show that, if G is finite and $H < G$, then every right coset of H in G has the same number of elements every left coset of H in G.
(d) Show that the number of right cosets of H in G is equal to the number of left cosets of H in G.
(e) Show that if G is abelian, then every left coset is a right coset.
(f) Give an example to show that, in general, a left coset need not equal any right coset. [Hint: Look at Exercise 2(b) above.]

4. Describe the set of left cosets of $S^1 \times \{1\}$ in $T = S^1 \times S^1$, where the group structure on T is given by $(s, r) \cdot (s', r') = (ss', rr')$.

5. Recall that two integers m and n are relatively prime if there exist integers r and s such that $rn + sm = 1$. If m and n are relatively prime, we write $(m, n) = 1$. Show that $C_n = \langle \omega \rangle$ is generated by ω^m iff $(m, n) = 1$.

6. (a) If H is a subgroup of G, its **normalizer** is

$$N(H) = \{ a \in G \mid aHa^{-1} = H \}$$

(See Footnote.[4]) Prove that N(H) is a subgroup of G and contains H.

(b) If H is a subgroup of G, its **centralizer** is

$$C(H) = \{ a \in G \mid ah = ha \text{ for every } h \in H \}.$$

Prove that $C(H)$ is a subgroup of G.

(c) Is one of $N(H)$ and $C(H)$ contained in the other?

7. If $H < G$, let $N = \bigcap_{x \in G} xHx^{-1}$. Prove that N is a subgroup of G with the property that $aNa^{-1} = N$ for every $a \in G$.

8. (One of Herstein's starred problems: p. 48 #24, but with hints supplied to assist you. It is suggested that you challenge yourself and avoid looking at the hints.)

Suppose G is a finite group with $|G|$ not divisible by 3.

(a) Show that for every $g \in G$, there exists $y \in G$ such that $g = y^3$. (That is, each element has a cube root!)
(b) Suppose now that G also has the property that $(ab)^3 = a^3b^3$ for every $a, b \in G$. Show that, for all a and $g \in G$, one has $ga^2 = a^2g$. [Hint: Choose y as in part (a), and consider the expression $(aya^{-1})^3$.]
(c) Deduce that, under the assumption given in part (b), G is abelian. [Hint: Use the property $(ab)^3 = a^3b^3$ to conclude that $(ba)^2 = a^2b^2$, and then apply part (b).]

9. Suppose G is a finite group with $|G|$ not divisible by the prime p. Prove that there exists an integer M such that $g^{(p^M)} = g$ for every $g \in G$, as follows:

---

[4] aHa^{-1} is defined to be $\{ aha^{-1} \mid h \in H \}$

(a) Show that, for every $g \in G$, there exists a positive integer m such that $g^{(p^m)} = g$. [Hint: Consider the elements $g, g^p, g^{(p^2)}, \ldots$]

(b) Now prove that, if $g^{(p^m)} = g$, then $g^{(p^{km})} = g$ for every positive integer k. Then use the fact that G is finite to obain the result.

8. Normal Subgroups and Quotient Groups

Definition 8.1. A subgroup $H < G$ is a **normal** subgroup of G if $ghg^{-1} \in H$ for every $g \in G$. We write $H \lhd G$.

Examples 8.2.

A. All subgroups of abelian groups are normal.
B. A_n is a normal subgroup of S_n.
C. $\langle a \rangle$ is a normal subgroup of D_n, whereas $\langle b \rangle$ is not.

Lemma 8.3 (Equivalent Definition of a Normal Subgroup)**.**
The subgroup H of G is normal iff $gHg^{-1} = H$ for every $g \in G$.

Proof:

$\boxed{\Rightarrow}$ If H is normal, then, by definition,

$$gHg^{-1} \subset H$$

for every $g \in G$. Multiplying both sides by g and its inverse gives

$$H \subset g^{-1}Hg$$

for every g. Since this holds for every $g \in G$, we can replace g by its inverse to obtain

$$H \subset gHg^{-1}$$

for every g. Putting these two inclusions together gives the result.

$\boxed{\Leftarrow}$ If $gHg^{-1} = H$, then every element of the left-hand side is an element of the right-hand side, showing the result. $\square$

Note By the proof of the above lemma, $H < G$ iff $gH = Hg$ for every $g \in G$. In fact:

Lemma 8.4 (Another Equivalent Definition of a Normal Subgroup)**.**
The subgroup H of G is normal iff every right coset of H in G is also a left coset.

Proof:

$\boxed{\Rightarrow}$ If H is normal, then, by the preceding lemma, $gHg^{-1} = H$, whence $gH = Hg$, so that the left coset gH is equal to the right coset Hg.

$\boxed{\Leftarrow}$ Now suppose every left coset of H is also right coset. To show that H is normal, choose $g \in G$. Then gH is a right coset. Since $g \in gH$, it must also be an element of that right coset. But only one right coset can contain g, namely Hg. Hence, $gH = Hg$, whence $gHg^{-1} = H$, as required. $\square$

Definition 8.5. If A and B are arbitrary subsets of G, define their **product,** AB**,** by

$$AB = \{\, ab \mid a \in A, b \in B \,\}.$$

Of course, this product is associative: $(AB)C = A(BC)$, so we shall simply write ABC for a product of three subsets of G.

Examples 8.6.

A. If $H < G$, then $HH = H$.
B. If $H < G$ and $g \in G$, then $\{g\}H = gH$. We shall drop the set braces for single elements, and write, say aHb instead of $\{a\}H\{b\}$.
C. If $H < G$, and $a, b \in G$, then

$$\begin{aligned}(aH)(bH) &= a(Hb)H \\ &= a(bH)H && \text{(since } H \text{ is normal)} \\ &= abH && \text{(since } HH = H\text{)}\end{aligned}$$

Thus, the product of two left cosets is another left coset:

$$(Ha)(Hb) = Hab.$$

In fact:

Lemma 8.7 (Multiplying the Cosets of a Normal Subgroup).
The subgroup H of G is normal iff the product of two left cosets of H is always a left coset.

Proof:

$\boxed{\Rightarrow}$ We just proved this part.
$\boxed{\Leftarrow}$ In the exercise set. □

Recall that, if $H < G$, then G/H is the set of all left cosets gH of H in G.

Lemma 8.8 (The Quotient Group).
If $H < G$, then the multiplication of left cosets turns G/H into a group, called the **quotient group.**

Proof: We just check the axioms! □

Note It follows from the last section that the order of the quotient group G/H is the quotient, $|G|/|H|$.

Examples 8.9.

A. $G = \mathbb{Z}$; $H = n\mathbb{Z}$ (This explains the notation $\mathbb{Z}/n\mathbb{Z}$!)
B. G any abelian group
C. S_n/A_n
D. $\mathbb{Z}[x]/\ker\varepsilon$
E. $G/\{e\}$ is just a copy of G. We write $G/\{e\} \cong G$
F. $G/G \cong \{e\}$.
G. $C_6/\{1, \omega^2, \omega^4\}$
H. $(\mathbb{Z}/6\mathbb{Z})/\{[0], [2], [4]\}$
I. $GL(n, \mathbb{R})/SL(n, \mathbb{R})$
J. $D_n/\langle a\rangle \cong C_2$
K. $(G \times G)/(G \times e)'$

Exercise Set 8.

1. Find all the normal subgroups of D_{18}. Justify your assertions.

2. (a) If G is a group and H is a subgroup of index 2 in G, prove that $H \triangleleft G$.
(b) Is the corresponding result still true for subgroups of index 3? Give a proof or counterexample.

3. Show that the intersection of normal subgroups of G is a normal subgroup of G.

4. Give an example of a non-abelian group all of whose subgroups are normal. [Hint: A certain group we have studied has this property.]

5. Suppose H is the only subgroup of order $|H|$ in the group G. Show that $H \triangleleft G$.

6. Suppose that M and N are normal subgroups with the property the $M \cap N = \{e\}$. Show that, for any $m \in M, n \in N$ one has $mn = nm$.

7. Complete the proof of Lemma 8.7: The subgroup H of G is normal iff the product of two left cosets of H is always a left coset.

8. Prove that every quotient of a cyclic group is cyclic.

9. Write down the multiplication tables for the following quotient groups, and identify each as a familiar group:
(a) C_6/C_3
(b) C_{15}/C_5
(c) $Q_8/\{\pm 1\}$
(d) $Q_8/\{\pm 1, \pm i\}$

10. (a) Prove that, if $H < G$, then $H \triangleleft N(H)$. (See Exercise Set 7 for the definition of $N(H)$.)
(b) Prove that the subgroup H of G is normal iff $N(H) = G$.
(c) Prove that, if $H \triangleleft G'$, then $G' < N(H)$. (In other words, $N(H)$ is the maximal subgroup of G in which H is normal.)

9. Homomorphisms

Definition 9.1. Let G and G' be groups. A map $f\colon G \to G'$ is a **homomorphism** if, for every pair of elements $a, b \in G$, one has $f(ab) = f(a)f(b)$.

Examples 9.2.

A. G any group; $1_G\colon g \to G$; $1_G(g) = g$ (identity map)
B. G and G' any groups, $f_e\colon G \to G'$; $f_e(g) = e$ (trivial map)
C. $f\colon \mathbb{Z} \to \mathbb{Z}$; $f(n) = mn$
D. $f\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$; $f(n) = [n]$ (canonical quotient map)
E. $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$; $f[n] = [3n]$
F. G any group; $f\colon G \to G$; $f(g) = aga^{-1}$ for a fixed element $a \in G$. (conjugation by a)
G. $\det\colon GL(n, \mathbb{R}) \to \mathbb{R}$
H. $\rho\colon C_n \to GL(2, \mathbb{R})$; $\rho(e^{2\pi i/n}) = \begin{bmatrix} \cos(2\pi i/n) & -\sin(2\pi i/n) \\ \sin(2\pi i/n) & \cos(2\pi i/n) \end{bmatrix}$
I. $\operatorname{sgn}\colon S_n \to \{-1, 1\}$; $\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$
J. $\varepsilon\colon \mathbb{R}[x] \to \mathbb{R}$; $\varepsilon(p(x)) = p(1)$ (evaluation at 1)
K. $\rho\colon C_3 \to S_3$; $\rho(\omega^r) = (1, 2, 3)^r$
L. If $H < G$, then the **inclusion** map $\iota\colon H \to G$; $\iota(h) = h$ is a group homomorphism.
M. The **canonical projections** $\pi_1\colon G \times G' \to G$; $\pi_1(a, a') = a$, and $\pi_2\colon G \times G' \to G'$; $\pi_2(a, a') = a'$.

Lemma 9.3 (Elementary Properties of Homomorphisms)**.**
If $f\colon G \to G'$ is any homomorphism, then:

(a) $f(e_G) = e_{G'}$
(b) $f(a^{-1}) = f(a)^{-1}$ *for every* $a \in G$.
(c) *If $H \subset G$ is a subgroup, then $f(H) \subset G'$ is also a subgroup.*
(d) *If $K \subset G'$ is a subgroup, then $f^{-1}(K) \subset G$ is also a subgroup.* □

Definition 9.4. If $f\colon G \to G'$ is a group homomorphism, define:

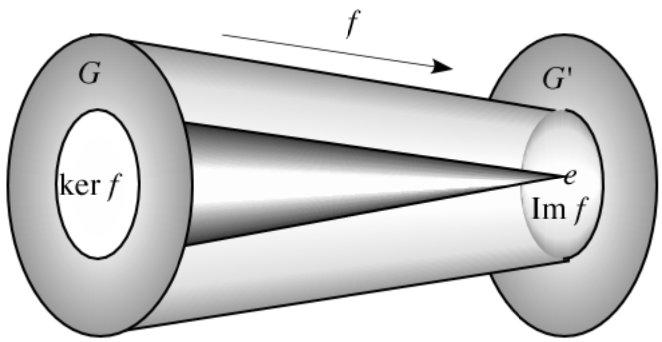
$$\operatorname{Ker} f = \{\, g \in G \mid f(g) = e \,\} = f^{-1}(e)$$
$$\operatorname{Im} f = \{\, f(g) \mid g \in G \,\} = f(G)$$

Ker f is called the **kernel of** f, and Im f is called the **image of** f. (See the figure.)

Corollary 9.5. $\operatorname{Ker} f$ *and* $\operatorname{Im} f$ *are subgroups of G and G' respectively.*

Examples 9.6. We look at the kernels and images of all the homomorphisms given in the above examples.

Definition 9.7. Let $f\colon G \to G'$ be a homomorphism. We say that f is a **monomorphism** (**injective**) if f is 1-to-1. That is, $f(a) = f(b) \Rightarrow a = b$. f is an **epimorphism** (**surjective**) if f is onto; that is, $\operatorname{Im} f = G'$. f is an **isomorphism** (**bijective**) if it is both monic and epic.



Note If $f\colon G \to G'$ is an isomorphism, then, by Theorem 2.25, f is invertible as a map of sets.

Lemma 9.8 (Criterion for a Monomorphism)**.**
$f\colon G \to G'$ is a monomorphism iff $\mathrm{Ker} f = \{e\}$*.* □

Examples 9.9 (of monomorphisms and epimorphisms)**.**

A. If $H < G$, then the inclusion $\iota\colon H \to G$ is a monomorphism. (Sub-examples in class)
B. If $H \lhd G$, then the natural projection $\nu\colon G \to G/H$ is an epimorphism. (Sub-examples in class)

Theorem 9.10 (Inverse of a Homomorphism)**.**
If $f\colon G \to G'$ is an isomorphism, then $f^{-1}\colon G' \to G$ is also a group homomorphism.

Proof: All we need to show is that $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ for every $a, b \in G$. But, since f is a homomorphism, applying f to each side of this equation yields the same result: ab. Thus, since f is monic, the two sides of the equation must be equal as claimed. □

Definition 9.11. The groups G and G' are **isomorphic** if there exists an isomorphism $\phi\colon G \to G'$. We write $G \cong G'$.

More Terminology: An **endomorphism** on a group G is a homomorphism $G \to G'$; an **automorphism** on G is an isomorphism $G \to G$.

Examples 9.12.

A. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong C_n$
B. $M(n, m) \cong \mathbb{R}^{mn}$
C. $S_3 \cong D_3$
D. $\mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
E. Is $\mathbb{Z} \cong \mathbb{Q}$ under addition?
F. If G is any group, define $\mathrm{Aut}(G)$, the **automorphism group of** G to be the set of automorphisms $G \to G$. Then $\mathrm{Aut}(G)$ is a group under composition.

Proposition 9.13 (Kernels are Normal).
If $f\colon G \to G'$ is a homomorphism, then $\operatorname{Ker} f \lhd G$. □

Proposition 9.14 (Preservation of Normalcy).
If $f\colon G \to G'$ is a homomorphism, then:

(a) *If $H < J < G$, then $H \lhd J$ implies $f(H) \lhd f(J)$.*
(b) *If $K < L < G'$, then $K \lhd L$ implies $f^{-1}(K) \lhd f^{-1}(L)$.* □

We now prove the very important

Theorem 9.15 (Fundamental Homomorphism Theorem).
Let $f\colon G \to G'$ be any homomorphism. Then there is a natural isomorphism

$$\phi\colon G/\operatorname{Ker} f \xrightarrow{\cong} \operatorname{Im} f$$

□

Examples 9.16.

A. $\operatorname{sgn}\colon S_n \to \{-1, 1\}$
B. $f\colon \mathbb{Z} \to C_n;\ f(m) = \omega^m$
C. $f\colon S^1 \to S^1;\ f(z) = z^2$
D. $f\colon \mathbb{R} \to S^1;\ f(x) = e^{ix}$
E. $f\colon \mathbb{R}^2 \to S^1 \times S^1;\ f(\theta, \phi) = (e^{i\theta}, e^{i\phi})$
F. $f\colon D_n \to C_2; f(a^r b^s) = b^s$
G. $\det\colon GL(n, \mathbb{R}) \to \mathbb{R}^*$

Definition 9.17. A group G is **simple** if it has no normal subgroups except G and $\{e\}$.

Examples 9.18.

A. C_p for primes p
B. S_n is not simple for any $n \geq 2$.
C. A_n is simple if n exceeds 5 (Exercise set).

Exercise Set 9.

1. Let G be any abelian group. Show that the map $f\colon G \to G;\ f(g) = g^2$ is a group homomorphism.
2. Which of the following are group homomorphisms. Justify your claims
  (a) $f\colon (\mathbb{R}, +) \to (\mathbb{R}^*, \times);\ f(x) = e^x$
  (b) $f\colon C_n \to D_n;\ f(\omega^r) = a^r$
  (c) $f\colon Q_8 \to \mathbb{C}^*;\ f(\pm i) = \pm i, f(\pm 1) = \pm 1, f(\pm j) = \pm i, f(\pm k) = \pm i$.
  (d) $f\colon GL(n; \mathbb{R}) \to GL(n; \mathbb{R});\ f(A) = P^{-1}AP$ for a fixed $P \in GL(n; \mathbb{R})$.
  (e) Let G be arbitrary with $a \in G$. Define $\tilde{a}\colon G \to G$ by $\tilde{a}(g) = aga^{-1}$.
3. Prove that the composite of any two homomorphisms (monomorphisms, epimorphisms, isomorphisms) is a homomorphism (monomorphism, epimorphism, isomorphism).

4. Let V be a vector space over $\mathbb{C}$, and let $Aut(V)$ be the set of linear isomorphisms $V \xrightarrow{\cong} V$.
(a) Verify that $Aut(V)$ is a group under composition of functions.
(b) Assume that $\{ e_1, e_2, \ldots, e_n \}$ is a basis for V, and let $[f]$ denote the matrix of the linear map f with respect to this basis. Show that the map $\phi\colon Aut(V) \to GL(n;\mathbb{C})$ given by $\phi(f) = [f]$ is an isomorphism of groups. [You may quote any result from linear algebra you like if you remember any! If not, seek help.]

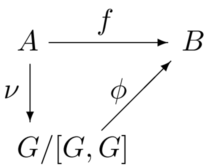
5. Calculate $Aut(\mathbb{Z}/3\mathbb{Z})$ and $Aut(\mathbb{Z}/6\mathbb{Z})$. In general, what can you say about $Aut(\mathbb{Z}/n\mathbb{Z})$?

6. **Cayley's Theorem** Let G be a finite group of order n, and define a homomorphism $\phi\colon G \to Sn$ as follows.
(a) Let $g \in G$. Define $\tilde{g} : G \to G$ by $\tilde{g}(a) = ga$. Verify that $\tilde{g}$ is bijective for every choice of g.
(b) Show that the map $\theta\colon G \to S_G$ given by $\theta(g) = \tilde{g}$ is a monomorphism.
(c) Show that for each choice of numbering of the elements of G, we have an isomorphism $\tau\colon S_G \xrightarrow{\cong} S_n$.
(d) Now let ϕ be the composite $\tau \circ \theta$. Then ϕ is a monomorphism $G \hookrightarrow S_n$. Deduce: **Cayley's Theorem:** *Every finite group of order n is isomorphic to a subgroup of S_n.*

7. Use Theorem 9.15 to produce isomorphisms as shown:
(a) $C_6/C_3 \cong C_2$
(b) $C_{pq}/C_p \cong C_q$
(c) $Q_8/\{\pm 1, \pm i\} \cong C_2$

8. Prove that the following statements are equivalent for the finite group G:
(1) G is simple.
(2) There is no epimorphism from G onto any group G' with $0 < |G'| < |G|$.
(3) If $f\colon G \to G'$ is any homomorphism, then f is either trivial or injective.

9. The **commutator** of the elements a and b of the group G is the element $aba^{-1}b{-}^{1} \in G$. The **commutator subgroup** $[G, G]$ **of** G is the subgroup generated by all the commutators of elements of G. Prove:
(a) $[G, G] \triangleleft G$
(b) $G/[G, G]$ is abelian. It is called the **abelianization** of Ga.
(c) If $f\colon G \to A$ is a homomorphism with A abelian, then here exists a unique homomorphism $\phi\colon G/[G, G] \to A$ such that the diagram



commutes (that is, $\phi \circ \nu = f$). This property is called the **universal property of the commutator subgroup.**

10. Prove that any homomorphism $f\colon G \to G'$ can be expressed as a composite $\iota \circ \phi \circ \nu$ of three homomorphisms, where ι is a monomorphism, ϕ is an isomorphism and ν is an epimorphism.

11. An (additive) abelian group G is called a **torsion group** if, for every $g \in G$, one has $ng = 0$ for some $g \in G$. (0 is the identity in G.) In other words, every element of G has finite order. (See the first section on groups.) Prove that $\mathbb{Q}/\mathbb{Z}$ is a torsion group, and illustrate this by finding an element of order 666 in $\mathbb{Q}/\mathbb{Z}$.

12. If we have an infinite sequence of homomorphisms $f_i\colon G_i \to G_{i-1}$, $(i \geq 1)$ of groups, define the **inverse limit** of the G_i by

$$\overleftarrow{\lim}\, G_i = \{\, (g_0, g_1, \dots, g_n, \dots) \mid g_i \in G_i \text{ and } f_i(g_i) = g_{i-1} \,\}.$$

(a) Show that $\overleftarrow{\lim}\, G_i$ is a group.

(b) Show that the maps $\pi_i\colon \overleftarrow{\lim} G_i \to G_i$ given by $\pi_i((g_0, g_1, \dots, g_n, \dots)) = g_i$ is a group homomorphism.

(c) Show that the group $\overleftarrow{\lim}\, (\mathbb{Z}/p^i\mathbb{Z})$, where $f_i : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^{i-1}\mathbb{Z}$ is given by the natural projection, is **torsion free** (that is, every element has infinite order).

13. Prove that A_n is simple if n exceeds 5 by doing the following exercise from Fraleigh, p. 153.

(a) Show that A_n contains every 3-cycle if $n \geq 3$.

(b) Show that A_n is generated by 3-cycles if $n = 3$. [Hint: Compute $(a, b, c)(b, c, d)$ and $(a, b)(b, c)$]

(c) Fix r and s in $\{1, 2, \dots, n\}$. Show that A_n is generated by the particular 3-cycles (r, s, i) for $1 \leq i \leq n$. [Hint: Compute $(r, s, i)^2$, $(r, s, j)(r, s, i)^2$, $(r, s, j)^2(r, s, i)$, and $(r, s, i)^2(r, s, k)(r, s, j)^2(r, s, i)$]

(d) Let N be a normal subgroup of A_n for $n \geq 3$. Show that if N contains a 3-cycle, then $N = A_n$. [Hint: Show that $(r, s, i) \in N$ implies $(r, s, j) \in N$ by computing $((r, s)(i, j))(r, s, i)^2((r, s)(i, j))^{-1}$.]

(e) Let N be a nontrivial normal subgroup of A_n for $n \geq 5$. Show that one of the following cases must hold, and conclude in each case that $N = A_n$:

Case 1: N contains a 3-cycle.

Case 2: N contains a product of disjoint cycles, at least one of which has length greater than 3. [Hint: If N contains the disjoint product $\sigma = \mu(a_1, a_2, \dots, a_r)$, show that $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it.]

Case 3: N contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$. [Hint: Show that $\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}$ is in N, and compute it.]

Case 4: N contains a disjoint product of the form $\sigma = (a_1, a_2, a_3)$, where μ is a product of disjoint 2-cycles. [Hint: Show $\sigma^2 \in N$, and compute it.]

Case 5: N contains a disjoint product of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$, where μ is a product of an even number of disjoint 2-cycles. [Hint: Show that $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it to deduce that $\alpha = (a_2, a_4)(a_1, a_3)$ is in N. Using $n \geq 5$ for the first time, choose $i \in \{1, 2, \dots, n\}$ with $i \neq a_1, a_2, a_3, a_4$. Let $\beta = (a_1, a_3, i)$. Show that $\beta^{-1}\alpha\beta\alpha \in N$, and compute it.]

14. (Optional; Harder) **Semidirect Products** Let G and G' be groups, and let $\phi\colon G \to Aut(G')$ be a homomorphism. Define a new group $G \times_\phi G'$ as follows. As a set, $G \times_\phi G'$ is just the Cartesian product $G \times G'$. Multiplication is given by the following strange formula:

$$(a, a')(b, b') = (ab, (\phi(b^{-1})(a'))(b')).$$

(a) Verify that $G \times_\phi G'$ is a group with identity $(e_G, e_{G'})$ and $(a, a')^{-1} = (a^{-1}, \phi(a)(a'^{-1}))$.

(b) Show that, if $\phi(g) = 1\colon G' \to G'$, then $G \times_\phi G'$ coincides with $G \times G'$.

(c) Let $G = C_p$; p prime, and let $G' = C_p \times C_p$, the usual product. Define $\phi\colon C_p \to C_p \times C_p$ by $\phi(\omega^r)(\omega^s, \omega^t) = (\omega^s, \omega^{rs+t})$. Show that ϕ is indeed a homomorphism, and that $G \times_\phi G'$ is a non-abelian group of order p^3. [Write $a = (\omega, 1, 1), b = (1, \omega, 1), c = (1, 1, \omega)$. Show that $a^p = b^p = c^p = e, bc = cb,\ ac = ca$, and $aba^{-1} = bc$.]

10. Some Structure Theorems

This section summarizes some results about homomorphisms and what they preserve.

Lemma 10.1. *If $\phi\colon G \xrightarrow{\cong} G'$ is an isomorphism, then ϕ induces a one-to-one correspondence between subgroups of G and subgroups of G'. Moreover, this correspondence preserves normalcy.* □

Lemma 10.2. *Let K be normal in G, and let $\nu\colon G \to G/K$ be the natural epimorphism. Then ν induces a one-to-one correspondence between subgroups of G containing K and subgroups of G/K. Moreover, this correspondence preserves normalcy.*

Outline of Proof: Let $\mathcal{S}$ be the collection of subgroups of G containing K, and let $\mathcal{T}$ be the collection of subgroups of G/K. Define $\psi\colon \mathcal{S} \to \mathcal{T}$ by $\psi(H) = \nu(H)$, and $\theta\colon \mathcal{T} \to \mathcal{S}$ by $\theta(L) = \nu^{-1}(L)$. Then we check that ψ and θ are inverses. In checking this, note that $\nu^{-1}\nu(H) \supset H$ in general, but if $H \supset K$, then

$$\begin{aligned} g \in \nu^{-1}\nu(H) \Rightarrow & \nu(g) \in \nu(H) \\ \Rightarrow & \nu(g) = \nu(h) \text{ for some } h \in H \\ \Rightarrow & \nu(h^{-1}g) = e \text{ for some } h \in H \\ \Rightarrow & h^{-1}g \in \operatorname{Ker}\nu = K \text{ for some } h \in H \\ \Rightarrow & g \in hK \text{ for some } h \in H. \end{aligned}$$

But, since $H \supset K$ and H is a subgroups, $hK \subset H$, and so $g \in H$, showing $\nu^{-1}\nu(H) \subset H$ as well. We already know that ψ and θ preserve normalcy. □

Theorem 10.3 ("Second Homomorphism Theorem")**.**
Let $f\colon G \to G'$ be any homomorphism with image I and kernel K. Then f induces a one-to-one correspondence between subgroups of G containing K and subgroups of I. Moreover, this correspondence preserves normalcy.

Proof: We can write f as a composite

$$G \xrightarrow{\nu} G/K \xrightarrow[\cong]{\phi} I \xrightarrow{\iota} G'$$

By Lemmas 10.1 and 10.2, both ν and ϕ induce normalcy-preserving one-to-one correspondences of the appropriate type, so the result follows. □

Lemma 10.4. *If $\phi\colon G \xrightarrow{\cong} G'$ is an isomorphism, then the one-to-one correspondence in Lemma 10.1 induces isomorphisms between respective quotients. That is, if $H \triangleleft K < G$, then ϕ induces an isomorphism $K/H \cong \phi(K)/\phi(H)$.* □

Lemma 10.5. *Let K be normal in G, and let $\nu\colon G \to G/K$ be the natural epimorphism. Then the one-to-one correspondence in Lemma 10.2 induces isomorphisms between respective quotients. That is, if $K < H \triangleleft J < G$,* *then* ϕ *induces an isomorphism* $J/H \cong \nu(J)/\nu(H) = (J/K)/(H/K)$. *In particular, if* $H \lhd G$, *then* $G/H \cong (G/K)/(H/K)$. $\square$

Theorem 10.6 ("Third Homomorphism Theorem")**.**
Let $f\colon G \to G'$ *be any homomorphism with image* I *and kernel* K. *Then the one-to-one correspondence of the Second Homomorphism Theorem induces isomorphisms between respective quotients. That is, if* $K < H \lhd J < G$, *then* ϕ *induces an isomorphism* $J/H \cong f(J)/f(H) = (J/K)/(H/K)$. $\square$

11. Group Actions

From now on, we shall always write groups multiplicatively.

Definition 11.1. Let G be a group and X be a set. Then a **left action of G on X** is a map

$$\alpha\colon G \times X \to X$$

with the following properties for all $g, h \in G$ and $x \in X$ (where we write $\alpha(g,x)$ as simply $g.x$ or gx):

(1) $(gh).x = g.(h.x)$
(2) $e.x = x$

If X has a given (left) action by a group G, we refer to X as a (left) **G-set.**

Examples 11.2.

A. Trivial action on any set X
B. G acting on G by multiplication
C. G acting on G/H for $H < G$
D. C_3 acting on $\mathbb{C}$ by rotation
E. C_n acting on $\mathbb{C}$ by rotation
F. C_n acting on $\mathbb{C}$ by the clockwise rotation
G. C_2 acting in $\mathbb{R}$ by flipping
H. C_n acting on $\{ e^{2k\pi i/n} \}$ by multiplication
I. D_n acting on $\mathbb{C}$ by rotation and reflection
J. S_n acting on $\{ 1, 2, \ldots, n \}$ in the natural way
K. $O(n, \mathbb{R})$ acting on S^n by multiplication
L. Disjoint unions of copies of G/H's

Definition 11.3. If X and Y are G-sets, then define the **product** G-set $X \times Y$ as the Cartesian product of X and Y with the G-action specified by $g.(x,y) = (gx, gy)$.

Definition 11.4. If X is a G-set and $x \in X$, then define

$$G_x = \{ g \in G \mid g.x = x \},$$

the **stabilizer of x.**

Lemma 11.5 (Stabilizers are Subgroups)**.**
Let X be a G-set and $x \in X$. Then G_x is a subgroup of G. □

Note: The first example below will show that G_x need not be normal, but in fact can be an arbitrary subgroup of G.

Examples 11.6.

A. $X = G/H, x = eH$
B. $G = C_3, X = \{ e^{2n\pi i/3} \}, x = e^{2\pi i/3}$
C. $X = G$, $x =$ any $g \in G$
D. $G = S_n, X = \{ 1, 2, \ldots, n \}, x = 1$
E. The trivial G-action on a set X.

F. C_3 acting on $\mathbb{C}$ by rotation, $x = 0, x = 1$.

Definition 11.7. If $G_x = e$ for every $x \in X$, then we say that X is a **free** G**-set**, or that G **acts freely** on X.

Examples 11.8. Look at our list of G-actions and decide which are free ones.

Definition 11.9. Let G act on X. Then the **orbit of** $x \in X$ is the subset of X given by

$$G.x = \{\, g.x \mid x \in X \,\}$$

The G-set X is called **transitive** if it is an orbit. In other words, if $X = G.x$ for some $x \in X$.

Examples 11.10. Look at the orbits of some elements in our examples of group actions.

Proposition 11.11 (Orbits are Equivalence Classes)**.**
Let X be a G-set. The relation $x \approx y$ if $y = g.x$ for some $g \in G$ is an equivalence relation. The corresponding equivalence classes are the orbits in X; that is, $[x] = G.x$ for every $x \in X$. □

Corollary 11.12 (Decomposition of G-sets)**.**
It follows that every G-set is a disjoint union of orbits. □

We'll see what the orbits look like a little later on.

Examples 11.13 (of Orbits)**.**

A. G/H
B. Look at the orbits of all the elements in the previous collection of examples.
C. $G = C_3, X = \{\, e^{2n\pi i/6}, 0 \,\}$. Write this set as a disjoint union of orbits.

Definition 11.14. Let X and Y be G-sets. Then a map $f\colon X \to Y$ is called a G**-map,** a G**-equivariant map,** or just an **equivariant map** if

$$f(g.x) = g.f(x)$$

for every $x \in X$ and $g \in G$. (Note the analogy with scalar multiplication of vectors and linear maps.)

Examples 11.15.

A. The identity map on any G-set
B. X any G-set and $: X \to \{\, * \,\}$
C. $G = \{e\}$. Then any map $X \to Y$ is automatically a G-map.
D. $G = C_3, X = \{\, e^{2n\pi i/6} \,\}, Y = \{\, e^{2n\pi i/3} \,\}$. What G-maps are possible?
E. $H < G,\ \nu\colon G \to G/H$ the natural projection
F. $K < H < G,\ \nu\colon G/K \to G/H$ the natural projection

Lemma 11.16 (Determining a G-map on an Orbit)**.** *If X is a transitive G-set, then any G-map $f\colon X \to Y$ is completely determined by its value on any single point $x \in X$.* □

Proposition 11.17 (What Orbits Look Like)**.**
Let X be any G-set, and let $x \in X$. Then there is an invertible G-map

$$f\colon G/G_x \to G.x$$

given by $f(gG_x) = g.x$. □

Definition 11.18. A G**-equivalence** is a G-map $f\colon X \to Y$ which happens to be invertible.

Proposition 11.19 (Inverses of G-maps)**.**
The inverse of a G-equivalence is a G-equivalence. (Proved in Exercises) □

It follows that the map f in Proposition 11.17 is a G-equivalence.

Definition 11.20. Two G-sets X and Y are G**-equivalent** if there exists a G-equivalence $f\colon X \to Y$. We write $X \cong_G Y$. (Note that it is an equivalence relation on the class of all G-sets—see the Exercises)

Note It follows from Proposition 11.17 that the orbit of any $x \in X$ is G-equivalent to G/Gx. It now follows form Corollary 11.12 that *every G-set is G-equivalent to a disjoint union of G-spaces of the form G/H for various subgroups $H < G$.* Thus we now know what all G-sets "look like." In other words, we have *classified* all G-sets.

We now look at how the various G/H are related to each other; for instance, you might ask: When is $G/H \cong_G G/K$?

Definition 11.21. Let $H < G$ and let X be a G-set. Define the H**-fixed set,** $X^H \subset X$ as:

$$X^H = \{\, x \in X \mid h.x = x \text{ for each } h \in H \,\}$$

Examples 11.22.

A. $eH \in (G/H)^H$
B. $(G/H)^H = NH/H$
C. If $H < K$, then $X^H \supset X^K$.
D. $x \in X^{G_x}$ for every $x \in X$.

(This is as far as we have to go for the Sylow theorems.)

Notation If X and Y are G-sets, denote the set of all G-maps $X \to Y$ by $G\mathcal{M}(X, Y)$. (In other words, $f \in G\mathcal{M}(X, Y)$ iff f is a G-map $X \to Y$. Similarly, if $H < G$, then the set of all H-maps $X \to Y$ is denoted by $H\mathcal{M}(X, Y)$. (This makes sense if X and Y are H-spaces.) Finally, if $H = \{\, e \,\}$, we write $\{\, e \,\}\mathcal{M}(X, Y)$ as $\mathcal{M}(X, Y)$.

Notes 11.23.

(a) $\mathcal{M}(X, Y)$ is just the set of all maps $f\colon X \to Y$.

(b) $f \in H\mathcal{M}(X,Y)$ iff $f(h.x) = h.f(x)$ for each $x \in X$ and $h \in H$.

Proposition 11.24 (Fixed Points are Just G-maps)**.**
Let Y be a G-space. One has the following bijection of sets:

$$G\mathcal{M}(G/H, Y) \cong_G \mathcal{M}(*, Y^H) \cong Y^H,$$

where $*$ denotes a single-point set. In other words, G-maps $G/H \to Y$ are in 1-1 correspondence with the points in Y^H. □

Note: This implies that, to specify a G-map $G/H \to Y$, all we need do is pick a point in Y^H, and *vice-versa*.

Corollary 11.25. *If $Y^H = \emptyset$, then there are no G-maps $G/H \to Y$.* □

Corollary 11.26. *There exists a G-map $G/K \to G/H$ iff K is conjugate to a subgroup of H. Further, any G-map $f\colon G/K \to G/H$ has the form $f(gK) = gaH$, for every $g \in G$, where $a \in G$ is such that $a^{-1}Ka \subset H$. We say that a* **normalizes** *K in H. Conversely, every such $a \in G$ determines a G-map of the above form.* □

Corollary 11.27. *G-maps $G/H \to G/H$ are in 1-1 correspondence with elements of NH/H.* □

Corollary 11.28 (Classification of Orbits up to G-Equivalence)**.**
There is a G-equivalence $G/H \to G/K$ iff K is conjugate to H in G. □

Note: We now have the following sharper classification of finite G-sets: *Any finite G-set is equivalent to a disjoint union of G/H's, where any two such G/H's are equivalent to each other iff the corresponding subgroups are conjugates of each other.*

Lemma 11.29 (Burnside)**.**
Let G act on the finite set X. For each $g \in G$, let $|X^g|$denote the number of elements fixed by g. Then the number of orbits in X is given by:

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof: Let $D = \{\, (g,x) \in G \times X \mid g.x = x \,\}$. Look at the projection $\pi_2\colon D \to X$. Then the preimage of any point x is its stabilizer G_x. Further, the preimage of every point in the *orbit* of $x \in X$ is a conjugate of G_x, and thus has the same number of elements. The preimage of the orbit of $x \in X$ therefore has

Number in preimage $\times$ number in orbit $= |Gx||G/Gx| = |G|$ elements!
Thus, the total number of elements in D is

Number of orbits in G $\times$ number of elements per orbit $= N|G|$,
so

$$N = \frac{1}{|G|}|D| \qquad \ldots \qquad (1)$$

Now look at the other projection, $\pi_1\colon D \to G$. The preimage of $g \in G$ under this projection is just X^g. Hence,

$$|D| = \sum_{g\in G} |X^g| \qquad \dots \qquad (2)$$

Putting (1) and (2) together gives the result. $\square$

Note In the above proof, $X^g = X^{\langle g\rangle}$. (Why?)

Example 11.30. Let us compute the number of 2-color paintings (red, green) of the faces of a regular tetrahedron. Here, X is the set of all of those paintings: $\binom{4}{2} = 6$ altogether. For a given rotation g of the tetrahedron, X^g consists of those paintings that are left fixed by g.

Exercise Set 10.

1. Find G_x in each of the following cases:
   (a) $X = \mathbb{C}$, $G = C_2$ acting by reflection in the y-axis, $x = 0, x = i, x = 1$.
   (b) $X = G/H$, $x = gH$ for some $g \in G$.
   (c) $X = \{\, gHg^{-1} \mid g \in G \,\}$, G acting by conjugation: $g.(aHa^{-1}) = gaH(ga)^{-1}; x = H$.
2. Show that, if X is a G-space, $x \in X$, and $H < G_x$, then $x \in X^H$.
3. Prove that the relation $X \cong_G Y$ (of G-equivalence) is an equivalence relation on the class of all G-sets.
4. Prove Proposition 11.19.
5. Prove or disprove each of the following claims:
   (a) $(X \times Y)^H = X^H \times Y^H$ for X and Y be two G-sets
   (b) $(X \cup Y)^H = X^H \cup Y^H$ for X and Y sub-G-sets of some G-set Z
   (c) $(X \cap Y)^H = X^H \cap Y^H$ for X and Y sub-G-sets of some G-set Z
   (d) $(G/K)^H = G^H/K$ where G acts by multiplication on the left
6. Show that $G\times G \cong_G G \coprod G \coprod \cdots \coprod G$ ($|G|$ times; $\coprod$ denotes disjoint union.)
7. Show that $G \times (G/H)$ is G-equivalent to a disjoint union of $|G/H|$ copies of G.
8. Represent the S_n-set $\{\, 1, 2, \dots, n \,\}$ as a disjoint union of S_n-orbits of the form S_n/H for certain $H < S_n$.
9. **A Consequence for p-Groups.** Let p be a prime number. A **p-group** is a finite group of order p^n for some n. Let G be any p-group, and let G act on itself by conjugation: $g.a = gag^{-1}$.
   (a) Show that the orbit of any element has cardinality a power of p (possibly $p^0 = 1$. Use Lagrange's Theorem)
   (b) By thinking of G as a disjoint union of orbits and counting, deduce that center of G is nontrivial.
10. If α is an action of G on X, then we get an associated map $\rho(g)\colon X \to X$ for each $g \in G$ given by

$$\rho(g)(x) = g.x$$

Prove: If α is an action of G on X, then:

(a) The associated map $\rho(g)\colon X \to X$ is invertible for each $g \in G$, with $\rho(g^{-1}) = \rho(g)^{-1}$.

(b) Denote by $\mathrm{Bij}(X)$ the group, under composition, of invertible maps on X. The function $\rho\colon G \to \mathrm{Bij}(X)$ defined above is a group homomorphism.

(c) The assignment $\alpha \mapsto \rho$ is a 1-1 correspondence between actions of G in X and homomorphisms $G \to \mathrm{Bij}(X)$. (In other words, an action of G on X "is" precisely a homomorphism $G \to \mathrm{Bij}(X)$.)

(d) Let $x \in X$, and let $\mathrm{Bij}_x(X) = \{ f \in \mathrm{Bij}(X) \mid f(x) = x \}$. Show that $\mathrm{Bij}_x(X)$ is a subgroup of $\mathrm{Bij}(X)$. To what subgroup of G does $\mathrm{Bij}(X)$ correspond?

11. Let X be an H-set for some $H < G$, and define a corresponding G-set as follows: Let $G \times_H X$ be the set of equivalence classes of pairs (g, x) with $g \in G$ and $x \in X$, where

$$(a, x) \approx (b, y) \text{ iff } a = bh \text{ and } y = h.x \text{ for some } h \in H.$$

(In other words, we are defining $(bh, x) \approx (b, hx)$ for every $h \in H$.) We call $G \times_H X$ the **G-set induced by the H-action on** X. Prove the following:

(a) The relation $\approx$ is an equivalence relation.

(b) $G \times_H X$ is a G-set via the action $g.[a, x] = [ga, x]$. (Show that this action is well defined.)

(c) There is a natural G-surjection $p : G \times_H X \to G/H$.

(d) $G \times_H \{*\} \cong_G G/H$ and $G \times_H H \cong_G G$

(e) If X is a G-set, then $G \times_H X \cong_G (G/H) \times X$, with the product G-action.

(f) If $f\colon Y \to G/H$ is any G-surjection, then $Y \cong_G G \times_H X$ for some H-set X. (Note: This result gives us a **classification of all surjections onto G-orbits.**)

12. (Difficult) **A decomposition of $(G/H) \times (G/K)$ into G-orbits** If H and K are subgroups of G, define

$$HgK = \{ hgk \mid h \in H \text{ and } k \in K \}$$

This is called the **double coset** associated with H and K.

(a) Prove that two double cosets are either equal or disjoint.

(b) Prove that $(G/H) \times (G/K)$ is a disjoint union of G-orbits of the form $G/(H^g \cap K)$, where H^g denotes gHg^{-1}.

(c) Deduce that $(G/H) \times (G/K) \cong_G \bigcup_{HgK} G/(H^g \cap K)$.

13. Compute the number of 6-color paintings of the faces of a cube (that is, the number of possible configurations of the numbers on a die.)

14. Compute the number of 3-color paintings of the faces of a cube.

12. The Sylow Theorems

Definition 12.1. A p**-group** is a group of order p^n for some prime p.

Lemma 12.2 (A Counting Result)**.**
Let G be a p-group and let X be a finite G-set. Then

$$|X| \equiv |X^G| \mod p$$

□

Theorem 12.3 (Cauchy)**.**
Let G be any finite group such that $|G|$ is divisible by the prime p. Then G has an element of order p (and hence a subgroup of order p).

Proof: Let $X = \{ (g_1, g_2, \dots, g_p) \mid g_i \in G, g_1 g_2 \dots g_p = e \}$. So X is the set of p-tuples in G with product e. Then we can say several things about X:

(a) $|X| = |G|^{p-1}$. Why? Because there is a 1-1 correspondence between elements of X and the se of all $(p-1)$-tuples of elements of G; you fill in the last element of G by the constraint $g_p = (g_1 g_2 \dots g_{p-1})^{-1}$.
(b) Let σ be the cycle $(1, 2, \dots, p) \in S_p$. Then $\langle \sigma \rangle$ acts on X by permuting the indices;

$$\begin{aligned} \sigma(g_1, g_2, \dots, g_p) &= (g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(p)}) \\ &= (g_2, g_3, \dots, g_p, g_1) \end{aligned}$$

(c) $(g_1, g_2, \dots, g_p)$ is fixed by $\langle \sigma \rangle$ iff $g_1 = g_2 = \dots = g_p$. For example, the element $(e, e, \dots, e)$ is fixed by $\langle \sigma \rangle$.
(d) If any other element is fixed by $\langle \sigma \rangle$, then it has the form $(a, a, \dots, a)$ with $a \neq e$, and so $a^p = e$, so a must be an element of order p, giving us what we are seeking.

Thus, it suffices to show that $X^{\langle \sigma \rangle}$ has more than one element in it. But, by the lemma, since $\langle \sigma \rangle$ is definitely a p-group, we have

$$|X| \equiv |X^{\langle \sigma \rangle}| \mod p.$$

That is,

$$|G|^{p-1} \equiv |X^{\langle \sigma \rangle}| \mod p$$

by fact (a). Since $|G| = k.p$, this gives:

$$(kp)^{(p-1)} \equiv |X^{\langle \sigma \rangle}| \mod p.$$

But $p-1$ is positive (p is at least 2), so that the left-hand side is divisible by a positive power of p, making it $0 \mod p$. Thus the right-hand side, $|X^{\langle \sigma \rangle}|$, is also divisible by p. Since $X^{\langle \sigma \rangle}$ has at least one element in it—namely $(e, e, \dots, e)$— it must therefore have order a positive power of p. Done. □

Corollary 12.4. *G is a p-group iff every element of G has order a power of p.* □

Recall that G acts on G/H via left multiplication: $g(g'H) = (gg')H$. We also saw that

$$|G/H^H| = |NH/H|$$

Now suppose H happens to be a p-group. Look at G/H as an H-set decomposed into H-orbits. We have

$$G/H = O_1 \coprod O_2 \coprod \cdots \coprod O_r \coprod (G/H)^H,$$

where the O_i are orbits of magnitude > 1. But we know how big they must be: $|H/J|$ for appropriate subgroups J of H. Since H is a p-group we must have, by Lagrange, that each J is a p-group also, and so each $|O_i|$ must be a non-zero power of p. In other words,

$$\boxed{|G/H^H| = |NH/H| \equiv |G/H| \mod p}$$

In particular, $|NH/H|$ can't be 1, since 1 is not divisible by p. Thus, $NH \neq H$.

Theorem 12.5 (Sylow's First Theorem)**.**
Let G be a finite group of order $p^n m$, where m is not divisible by p. Then:

(a) *G contains a subgroup of order p^i for every $i \leq n$.*
(b) *Every subgroup H of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.*

Proof:

(a) By Cauchy's theorem, G contains a subgroup of order p. We now do induction on i, the start of induction $i = 1$ being true. Thus assume there is a subgroup of order p^j for every $j \leq i$. We must now produce a subgroup of order p^{i+1}. Let H be a subgroup of order i and look at G/H. Since $|G/H| = |G|/|H|$, it is still divisible by p, so by the above boxed formula, $|NH/H|$ is also divisible by p. By Cauchy's theorem, the quotient group NH/H also has an element of order p, and hence a subgroup K of order p. Look at $J = \nu^{-1}(K)$, where $\nu \colon NH \to NH/H$ is the natural quotient. But J contains H and is a subgroup of NH. Further, $\nu| \colon J \to K$ is epic with kernel H, so that $J/H \cong K$. Since $|H| = p^i$ and $|K| = p$, we must have $|J| = p^{i+1}$. Done.
(b) If H has order p^i with $1 \leq i < n$, then we can get $K < NH/H$ as above, and find that $J = \nu^{-1}(K)$ has order p^{i+1} and, being contained in the normalizer of H, must normalize H. □

Definition 12.6. If G has order $p^n m$ where m is not divisible by p, we call any subgroup of order p^n a **Sylow-p-subgroup** of G. Thus Sylow-p-subgroups are maximal p-subgroups of G, and always exist by the theorem.

Theorem 12.7 (Sylow's Second Theorem)**.**
Let G be finite. Then any two Sylow p-subgroups of G are conjugate.

Proof: Let H and K be two Sylow p-subgroups of G, and let H act on G/K by left multiplication. Then, by Lemma 12.2,

$$|(G/K)^H| \equiv |G/K| \mod p.$$

But $|G/K|$ is not divisible by p (since K is Sylow) and thus neither is $|(G/K)^H|$. In particular, $(G/K)^H \neq \emptyset$. This means that there is a $g \in G$ such that

$$hgK = gK$$

for all $h \in H$. But this means that $g^{-1}Hg \subset K$. Since $|H| = |K|$, this must be an equality, and we are done. □

Theorem 12.8 (Third Sylow Theorem)**.**
Let G be a finite group such that p divides $|G|$, and let n_p be the number of p-Sylow subgroups of G. Then:

(a) *n_p divides G.*
(b) *$n_p \equiv 1 \mod p$.*

Proof:

(a) By Theorem 12.7, all the Sylow p-subgroups are conjugate. In other words, if G acts on the set of all Sylow p-subgroups by conjugation, then there is a single orbit. The number of things in the orbit is n_p. Further, if H is a Sylow p-subgroup, then G_H (the stabilizer of H) is NH. Hence:
$$n_p = |G/NH|,$$
which certainly divides $|G|$.

(b) Now let H be a Sylow subgroup, and let H now act on the set X of all Sylow p-subgroups by conjugation. Then H fixes itself.
Claim: H fixes nothing else. Indeed, if H did fix another beast, K, say, then $H < NK$, making both H and K p-subgroups of NK. But then they must be Sylow p-subgroups of NK , making them conjugate in NK. But all conjugates of K by elements of NK are the same as K by definition! In other words, $H = K$ as claimed. The upshot of this is that there is only one fixed point under this action. Thus, by Lemma 12.2 again:
$$n_p = |X| \equiv |X^H| \equiv 1 \mod p.$$
Done. □

Examples 12.9.

A. All Sylow subgroups of D_3
B. No group of order 15 is simple, since it has only one Sylow-5 subgroup, which must therefore be normal.