Math 375
Week 1

1.1 Introduction to Groups

Introduction

Abstract algebra is the study of *structures* that certain collections of 'objects' or 'sets' possess. You have already had a taste of this in Math 204, linear algebra, or in CS 221, discrete structures. In Math 204 you studied a single structure in some depth, the vector space structure. At first you proceeded quite informally—you treated vectors as something quite geometric. Vectors were 'objects' that had both a direction and a magnitude, in other words, 'arrows.' However, you soon realized that you could perform certain operations on these arrows—you could add two of them, you could multiply one by a scalar—and still have a vector. We described this by saying the set was **closed** under these operations.

Very quickly you began to focus on the operational aspects of dealing with vectors. Does the addition commute? Is there an additive identity? Are there additive inverses for each vector? And so on. This activity was formalized in the definition of a *vector space* with its eight or so axioms. The preciseness of the definition turned out to be quite a liberating thing: you soon begin to spot vector spaces everywhere! The set of n-tuples form the vector space $\mathbf{R}^n$ when component addition and scalar multiplication are used. The set of $n \times m$ matrices form a vector space if the usual addition and scalar multiplication are used. The set of continuous functions form a vector space using the ordinary definitions of addition and scalar multiplication of functions. So does the set of all polynomials or the set of all polynomials of degree less than or equal to n. Notice that in each case two things are required: a set of objects and two operations on this set.

The vector space structure is just one of many possible algebraic structures that a set may have. It is not the simplest structure, nor is it the most complicated. We probably won't study vector spaces very much this term. In Math 331 (if you have taken it) the idea of closure occurs in several places. For example, functions that were differentiable, integrable, continuous, or had limits were closed under addition and scalar multiplication. Moreover, we defined fields like **R**, and **Q** which had additional structure to them, including a multiplication with identities and inverses and a distributive law which showed how multiplication interacts with addition.

In Math 375, we'll start with a much simpler structure, the sort of structure exhibitted by the most familiar mathematical objects such as the integers and the rational numbers. What 'operations' can you perform on **N**, **Z**, **Q**, and **R**? Are all of these sets closed under all of these operations? We see that the more 'structure' we impose on the set and operations, the fewer the number of sets that will satisfy the conditions. So if we want to study lots of sets, we should not impose too much structure—just enough to be useful! This is what groups are all about.

1.2 Preliminary Discussion on Groups

A crucial part of the vector space axiom system concerned the notion of the two operations on the set involved. In particular: given $v, w \in V$ (V a vector space) $v + w \in V$, where 'addition' was an operation that took two elements of V and produced a third element of V.

Stripped down to its basic elements, this operation takes two elements of the set and produces a third. In general, the order in which the elements appear can be important.

When ordering is important, we often speak of **ordered pairs** or even **ordered n-tuples**. Usually these are denoted (a, b). Generally:

$$(a, b) \neq (b, a).$$

When would this equality be valid?

Definition 1 *A **binary operation** $*$ on a set S is a function that associates to each ordered pair (a, b) of elements of S an element of S which we denote by $a * b$ or simply ab.*

Example 1 Ordinary addition, multiplication, subtraction on **Z**, **Q**, **R**. What about division? What about division on $\mathbf{Z}^+$, $\mathbf{Q}^+$, $\mathbf{R}^+$? □

The basic algebraic structure that we'll study this term is that of a group. Groups appear not only in the context of mathematics, but in physics, chemistry, coding theory, kinship systems, design and architecture. For example, it turns out there are only seventeen different patterns of wallpaper that are possible (up to change of design element) and each of these patterns is described by a group. So what is a group?

Definition 2 *Suppose that:*

*i) G is a set and that $*$ is a binary operation on G (i.e., G is **closed** under $*$);*

ii) $*$ is associative: $(a * b) * c = a * (b * c)$;

*iii) there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (i.e., the existence of an **identity**; the same identity for all $a \in G$);*

*iv) for each $X \in G$ there exists $y \in G$ so that $a * b = b * a = e$, where e is the identity element from (iii) (i.e., **inverses** exist).*

*Then G with its binary operation $*$ is a **group** and is denoted by $(G, *)$.*

Notice that emptyset cannot be a group because (iii) fails. Notice that the group operation need not be commutative.

Example 2 Provide me with two examples of groups and two non-examples.

You are probably familiar with modular arithmetic; in fact you use something like it to tell time. Ordinarily the hours of the day are given 'modulo 12' more or less, while military time is given 'modulo 24.'

Definition 3 ***(Arithmetic Modulo** n**)*** *Let n be a fixed positive integer. For any integers a and b, $(a + b) \bmod n$ is the remainder upon dividing $a + b$ by n; similarly, $(a \cdot b) \bmod n$ is the remainder upon dividing $a \cdot b$ by n.*

Example 3 $(6 + 3) \bmod 4 = 1$; $(6 \cdot 3) \bmod 4 = 2$.

Definition 4 ***(Modular Equations)*** *Let n be a fixed positive integer. For any integers a and b, we write $a = b \bmod n$ if n divides $b - a$.*

Example 4 $19 = 4 \bmod 5$, $22 = -8 \bmod 10$, and $67 = 34 \bmod 11$.

Notice that after dividing by n, the only poosible remainders are: $\{0, 1, 2, \ldots, n - 1\}$. (This is, in fact, a consequence of the division algorithm that we will prove next time.) We can make this set of remainders into a group in the following way.

Definition 5 *If n is a positive integer, then the set $\mathbf{Z}_n = \{0, 1, 2, \ldots, n - 1\}$ is called the **integers modulo** n or the integers mod n.*

This set can be made into a group using addition mod n start by looking at $\mathbf{Z}_4$. This is summarized in the **Cayley table** that follows.

$\oplus$ mod 4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Notice that the set is closed. What is the identity element? Locate the inverses of each element. Verify associativity on your own! Is this operation commutative? How can you easily tell from the Cayley table?

More generally, $\oplus$, addition mod n is certainly a binary operation on $\mathbf{Z}_n$. Further, if $j \in \mathbf{Z}_n$, its inverse is $n - j$. 0 is the identity. Only associativity needs ot be checked. For now we'll assume it.

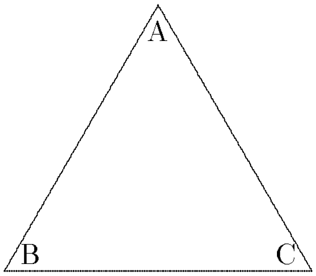
Example 5 Assume that we are given an equlateral triangle, ABC. Find all of the rigid motions which 'map' the triangle to itself.

SOLUTION Observe that the final position of the triangle is completely determined by two things:

i. the location of a single vertex (say A);

ii. the orientation of the triangle (face up or face down).

There are three possible locations for vertex A and each with two possible orientations, so there is a total of $3\times 2 = 6$ rigid motions mapping this triangle to itself.



These motions have simple geometric descriptions. We have three different counterclockwise rotations of 0, 120, and 240 degrees: r_0, r_{120}, and r_{240} (which preserve orientation). We also have three reflections through the lines which bisect the angles (these change orientation). We denote these reflections by a, bh, and c, where the line of reflection passes through the corresponding vertex of the triangle. We can define an operation '$*$' (followed by) this set of motions:

We say a motion r *followed by* s (denoted $r * s$ or rs) is equal to a motion t if first doing r and then s to the figure is the same as performing the motion t alone.

We can fill in the Cayley table for our set of motions with this operation.

$*$	r_0	r_{120}	r_{240}	a	b	c
r_0	r_0	r_{120}	r_{240}	a	b	c
r_{120}	r_{120}	r_{240}	r_0	b	c	a
r_{240}	r_{240}	r_0	r_{120}	c	a	b
a	a	c	b	r_0	r_{240}	r_{120}
b	b	a	c	r_{120}	r_0	r_{240}
c	c	b	a	r_{240}	r_{120}	r_0

This set of motions is usually called D_3, the dihedral group of order 6. Observe that we have

i. a binary operation (closure) where
ii. r_0 acts like the identity;
iii. every element has an inverse: r_{120} and r_{240} are inverses of each other, while all other elements are their own inverses.
iv. $*$ is associative. This can be verified directly by using the table, though this is quite tedious.

Therefore $(D_3, *)$ is a group. Notice that it is *not* commutative (abelian). For example:

$$r_{120} * a = b \qquad \text{but} \qquad a * r_{120} = c.$$

Example 6 $(D_n, *)$ is the group of motions of a regular n-gon. It is the **Dihedral Group** of order $2n$. It contains $2n$ elements: n rotations and n reflections for a total of $2n$ elements.

More on Binary Operations

Recall that:

Definition 6 *A* ***binary operation*** *$*$ on a set S is a function that associates to each ordered pair (a, b) of elements of S an element of S which we denote by $a * b$ or simply ab.*

Example 7 From set theory both union and intersection are binary operations: let X be a set and let $S = \{A|\ A \subseteq X\}$. Define $A * B = A \cup B$. Is there an identity element for $\cup$? What if $A * B = A \cap B$. Is there an identity element? □

The operations of addition and multiplication of real numbers are associative and commutative. Recall that

Definition 7 *If $*$ is a binary operation on S, then*

a) *$*$ is* ***associatative*** *if $(a * b) * c = a * (b * c)$ for all $a,\ b,\ c \in S$.*

b) *$*$ is* ***commutative*** *if $a * b = b * a$ for all $a,\ b \in S$.*

Example 8 Division is not commutative on $\mathbf{Q}^+$ or $\mathbf{R}^+$. (When does $a/b = b/a$?) Subtraction is not associative on $\mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{R}$. Is it commutative? Matrix addition is both associative and commutative.

Example 9 Let M_{22} be the set of all 2×2 matrices. Matrix multiplication is not commutative

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1/2 & 1 \end{pmatrix}.$$

but it is associative. □

Example 10 Are the operations $\cap$ and $\cup$ commutative on our previous set example?

Example 11 Which of the following are binary operations on $\mathbf{Z}$? Commutative? Associative?

a) $m * n = 2^{mn}$.

b) $m * n = \sqrt{mn}$.

c) $m * n = m^n$. Is there an identity? Inverses?

Example 12 On $\mathbf{R}$ is $a * b = a^b$ a binary operation? Associative? Commutative?

1.3 The Well-Ordering Principle

One of the goals of this course is to become better at writing proofs, continuing the process begun in Math 204, 331, and CS 221. One of the basic tools that we will require in this course is call the Well-Ordering Principle. You are familiar with one of its consequences, the method of proof by mathematical induction.

The Well-Ordering Principle: Every non-empty subset of $\mathbf{Z}^+$ has a smallest element.

This seems quite reasonable. We will accept this statement as an axiom; it's not something that we will try to prove. It is an assumption that we make about $\mathbf{Z}^+$. (Must there be a greatest element?)

Example 13 What are the smallest elements of these sets?

d) $E = \{\text{even positive integers}\}$.

e) $\{n! |\ n \in \mathbf{Z}^+\}$.

f) $\{n |\ n > \pi\}$.

g) $\{n |\ n \text{ is prime}\}$.

The Division Algorithm and Its Consequences

Definition 8 *Given $d \neq 0$. We say that d* **divides** *a (is a* **divisor** *of a) if there's an integer q so that $dq = a$. (This is denoted by $d|a$. If d does not divide a this is indicated by $d \not| a$.)*

Example 14 $6|18$ because $6 \cdot 3 = 18$; however $7 \not| 15$; notice $5|0$.

Theorem 9 ***(The Division Algorithm)*** *If a and b are integers with $b > 0$, then there exist unique integers q (quotient) and r (remainder) such that*

$$a = bq + r, \qquad \text{where } 0 \leq r < b.$$

Why is this geometrically obvious? Just divide the number line into multiples of b units.

Example

a) If $a = 39,\ b = 5$ then $q = 7,\ r = 4$.

b) If $a = -16,\ b = 5$ then $a = -3 \cdot 5 - 1$; but r is supposed to be non-negative! Intstead, use $a = -16 = -4 \cdot 5 + 4$, then $q = -4,\ r = 4$.

PROOF To prove that there are *unique* integers r and q with the required properties means that we have to show that:

i. There exists at least one integer q and at least one integer r with the desired properties (Existence);

ii. No other integers have these properties (Uniqueness).

EXISTENCE *We will assume that $a > 0$.* A similar proof works for $a < 0$. Consider the set

$$S = \{a - bk \mid k \text{ is an integer and } a - bk \geq 0\}.$$

If $0 \in S$, then b divides a. The result follows by letting $q = a/b$ and $r = 0$.

If $0 \notin S$, then notice that $a \in S$ (since $a = a - b \cdot 0 \in S$), so $S \neq \emptyset$. By Well-Ordering, there is a smallest element, say $r = a - bq \in S$. Then $a = bq + r$ and $r \geq 0$. Next we show that $r < b$; we use a proof by contradiction for that.

Assume instead that $r \geq b$, then:

$$0 \leq r - b = (a - bq) - b = a - (bq + b) = a - b(q + 1) \in S.$$

So $r - b \in S$ and smaller than r. But r is the *smallest* element of S. Contradiction. So we must have $r < b$.

UNIQUENESS Suppose that we had some other pair of integers q' and r' which satisfied the required conditions. Then

$$a = bq + r = bq' + r',$$

where $0 \leq r < b$ and $0 \leq r' < b$. WMA (we may assume) $r' \geq r$. Then

$$0 \leq r' - r < b. \qquad (*)$$

But

$$r' - r = a - bq' - (a - bq) = b(q - q').$$

So $r' - r$ is a multiple of b. By equation $(*)$, that multiple must be 0. So

$$q - q' = 0 \Rightarrow q = q'$$

and

$$r - r' = 0 \Rightarrow r = r'. \blacksquare$$

EXAMPLE 16 Several states encode information into drivers' licenses. In Florida for males: last 3 digits are $40(m-1)+b$ where m is month of birth and b is the date. If the last 3 digits were 146, then

$$146 = 40(3) + 26 = 40(4-1) + 26$$

so the person's birth date is April 26. They do this to help prevent forgery.

DEFINITION 10 *If a and b are integers, at least one of which is nonzero, the* ***greatest common divisor*** *of a and b is largest positive integer d that divides both a and b and is denoted by $\gcd(a,b)$. When $\gcd(a,b) = 1$, we say that a and b are* **relativley prime**.

EXAMPLE

a) $\gcd(8,12) = 4$

b) $\gcd(3,6) = 3$

c) $\gcd(-3,-6) = 3$

d) $\gcd(5,18) = 1$

e) $\gcd(6,0) = 6$

f) $\gcd(6120,4862) = ?$

How do we find the gcd for a pair of large numbers? Well Euclid managed to prove the following the following.

THEOREM 11 *The so-called the* ***Euclidean Algorithm*** *will produce $\gcd(a,b)$ in a finite number of steps.*

PROOF Clearly $\gcd(a,b) = \gcd(|a|,|b|)$. WMA the integers involved are nonnegative. In particular, WMA $0 \le b \le a$. Then the division algorithm implies:

$$a = bq_1 + r_1 \qquad \text{where } 0 \le r_1 < b.$$

Then $d|a$ and $d|b$ iff $d|b$ and $d|r_1$. So

$$\gcd(a,b) = \gcd(b,r_1).$$

The good thing about this is that we have replaced the pair (a,b) by a smaller pair (b,r_1) which should be easier to solve! (Remember that $r_1 < b \le a$.) Repeat this process using the division algorithm until the answer becomes obvious:

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{k-1},r_k) = \gcd(r_k,0).$$

From the last equality we have $\gcd(a,b) = r_k$.

Why must the last remainder in this proces equal 0? The sequence of remainders r_i is strictly decreasing and always nonnegative, so it can't go on forever. It must terminate at 0. ∎

EXAMPLE 18 Find $(1155, 756)$.

SOLUTION

$$\begin{aligned} 1155 &= 756 \cdot 1 + 399 \\ 756 &= 399 \cdot 1 + 357 \\ 399 &= 357 \cdot 1 + 42 \\ 357 &= 42 \cdot 8 + 21 \\ 42 &= 21 \cdot 2 + 0 \end{aligned}$$

So, $\gcd(1155, 756) = 21$.

EXAMPLE 19 Find $\gcd(6120, 4862)$.

SOLUTION

$$\begin{aligned} 6120 &= 4862 \cdot 1 + 1258 \\ 4862 &= 1258 \cdot 3 + 1088 \\ 1258 &= 1088 \cdot 1 + 170 \\ 1088 &= 170 \cdot 6 + 68 \\ 170 &= 68 \cdot 2 + 34 \\ 68 &= 34 \cdot 2 + 0 \end{aligned}$$

So $\gcd(6120, 4862) = 34$.

Notice that this process can be reversed. That is, we can write the greatest common divisor of two numbers as an integral linear combination of the two numbers.

THEOREM 12 *For any non-zero integers a and b, there are integers s and t such that* $\gcd(a,b) = as + bt$. *That is, the gcd is a linear combination of a and b. Moreover, it is the* ***smallest*** *positive integer of the form $as + bt$.*

PROOF One way to actually do it is to work through Euclidean Algorithm backwards. But I want to give a general proof that uses the Well-Ordering Principle.

Consider the set $S = \{am + bn | m, n \in \mathbf{Z};\ am + bn > 0\}$. S is not empty (use $am + b0 < 0$, with m being the same sign as a. Well-ordering implies S has a smallest element, say, $d = as + bt$.

We first show $d = \gcd(a,b)$. From the division algoritm:

$$a = dq + r, \qquad 0 \leq r < d.$$

If $r > 0$, then

$$r = a - dq = a - (as + bt)q = a(1 - sq) - b(tq) < d,$$

that is, r is a smaller linear combination of a and b than d contradicting our choice of d from the well-ordering principle. So we must have $r = 0$, so $d = aq$, i.e., $d|q$. Similarly, $d|b$. So d is a common divisor of a and b.

To show d is the gcd, let e be any other common divisor of a and b. Then $a = em$ and $b = en$. So

$$d = as + bt = ems + ent = e(ms + nt),$$

that is, $e|d$. So $d \geq e$, i.e., d is at least as large as any other common divisor of of a and b. So $d = \gcd(a,b)$. ■

COROLLARY 13 *Suppose that $d = \gcd(a,b)$. If $e|a$ and $e|b$, then $e|d$. That is, any divisor of both a and b is a divisor of* $\gcd(a,b)$.

EXAMPLE 20 $6 \mid 24$ and $6 \mid 36$. Also $6 \mid \gcd(24, 36) = 12$.

EXTRA CREDIT Write a program to express $\gcd(a,b)$ as a linear combination of a and b. You can't use the proof above, you must work backwards through the Euclidean algorithm.

EXAMPLE 21 $2 = \gcd(14, 10) = -2 \cdot 14 + 3 \cdot 10$. Or $1 = \gcd(9, 16) = -7 \cdot 9 + 4 \cdot 16$.

EXAMPLE 22 We saw that $21 = \gcd(1155, 756)$. Find integers s and t so that $14 = 1155s + 756t$.

SOLUTION Simply work backwards through the chain of equalities in the Euclidean algorithm.

$$\begin{aligned}
21 &= 357 - 8 \cdot 42 && \text{now eliminate 42}\\
&= 357 - 8(399 - 357) = -8 \cdot 399 + 9 \cdot 357 && \text{now eliminate 357}\\
&= -8 \cdot 399 + 9(756 - 399) = 9 \cdot 756 - 17 \cdot 399 && \text{now eliminate 399}\\
&= 9 \cdot 756 - 17(1155 - 756)\\
&= -17 \cdot 1155 + 26 \cdot 756. \ \square
\end{aligned}$$

Definition 14 *If $gcd(a, b) = 1$, then a and b are* ***relatively prime****.*

When integers are relatively prime, we obtain a nice factorization result.

Theorem 15 ***(Euclid's Lemma)*** *If r, a, and b are integers such that r divides ab and $\gcd(r, a) = 1$, then r divides b.*

PROOF Since $\gcd(r, a) = 1$, there are integers s and t so that

$$rs + at = 1.$$

Multiply both sides by b:

$$rsb + atb = b.$$

Now $r \mid rsb$ and $r \mid atb$ since $r \mid ab$, so $r \mid rsb + atb = b$. $\blacksquare$

Example 23 Let $r = 7$, $a = 9$ and $b = 35$. Then $7 \mid 315 = 9 \cdot 35$ and $\gcd(7, 9) = 1$. Notice that $7 \mid 35$.

Euclid's Lemma is most often used in the following form.

Corollary 16 *If p is a prime and $p|ab$, then $p|a$ or $p|b$.*

If $p \not| a$, then $\gcd(p, a) = 1$ since p is prime. By Euclid's Lemma, $p|b$. $\blacksquare$

Example 24 Let $p = 11$ and $ab = 220 = 5 \cdot 44$. Then $11 \not| 5$, but $11 \mid 44$.

Example 25 The prime hypothesis cannot be dropped: $8|24 = 2 \cdot 12$, but $8 \not| 2$ and $8 \not| 12$.

An allied notion to $\gcd(a, b)$ is $\mathrm{lcm}(a, b)$. Recall that:

Definition 17 *A non-zero integer r is a common multiple of two non-zero integers a and b if both $r \mid a$ and $r \mid b$. The* ***least common multiple*** *of two non-zero integers a and b is the smallest positive integer that is a mulitple of both a and b.*

Example 26 $\mathrm{lcm}(8, 12) = 124$. Note that it is easy to compute $\mathrm{lcm}(m, n)$. Let $d = \gcd(m, n)$. Then $m = pd$ and $n = qd$ so $\mathrm{lcm}(m, n) = pqd$. Here $\gcd(8, 12) = 4$ and $8 = 4 \cdot 2$ and $12 = 4 \cdot 3$ so $\mathrm{lcm}(8, 12) = 4 \cdot 2 \cdot 3 = 24$.

EXTRA CREDIT Show that $ab = \gcd(a, b)\cdot\mathrm{lcm}(a, b)$. Hint: Use the Fundamental Theorem of Arithmetic: the unique factorization of integers into primes.

1.4 Induction

One the most important consequences of the Well-Ordering Principle is the Principle of Mathematical Induction. You should be familiar with the following form.

THEOREM 18 ***Induction (First Form).*** *Let S be a set of positive integers containing 1. Suppose that S has the property that whenever $n \geq 1$ belongs to S, then so does $n+1$. Then S also contains all positive integers greater than 1.*

Note: 1 may be replaced wih any integer a.

PROOF By contradiction. Assume that S does not contain all positive integers. Let S' be the set of all positivie integers not in S. Then $S' \neq \emptyset$ so the Well-Ordering Principle implies that S' has a smallest element k. Now $k \neq 1$ because $1 \in S$. So $k > 1$ which means that $k-1$ is a positive integer. But $(k-1) \in S$ because because k is the smallest positive integer no in S is false. But then by hypothesis $(k-1)+1 \in S$. Contradiction. ∎

EXAMPLE 27 Assume you know the product rule for derivatives but not the power rule. Show that for all $n \in \mathbf{Z}^+$:

$$\frac{d}{dx}(x^n) = nx^{n-1}.$$

PROOF Let S be the set of all positive integers for which the statement is true. Induct: (i) $1 \in S$ because: $\frac{d}{dx}(x) = 1 = 1x^0$.

(ii) Assume $n \in S$ Show $n+1 \in S$. That is, assume $\frac{d}{dx}(x^n) = nx^{n-1}$ Show that $\frac{d}{dx}(x^{n+1}) = (n+1)x^n$. But

$$\begin{aligned}
\frac{d}{dx}(x^{n+1}) = \frac{d}{dx}(x \cdot x^n) = \frac{d}{dx}(x)\cdot x^n + x \cdot \frac{d}{dx}(x^n) & \qquad \text{product rule} \\
1 \cdot x^n + x \cdot nx^{n-1} & \qquad \text{since } 1,\, n \in S \\
= x^n + nx^n & \\
= (n+1)x^n. \ \square & \qquad \text{So } (n+1) \in S.
\end{aligned}$$

EXAMPLE 28 Use induction to prove that $2^n < n!$ for every positive integer $n \geq 4$.

PROOF Basis Step: First show that the inequality is true when $n = 4$. But

$$2^4 = 16 < 24 = 4!,$$

so the basis step holds.

Inductive Step: Assume that the statement is true for n and show that it is true for $n+1$. That is, given $2^n < n!$, show that $2^{n+1} < (n+1)!$ (where $n \geq 4$). But

$$\begin{aligned} 2^{n+1} = 2 \cdot 2^n &< (n+1)2^n && \text{since } n \geq 4 \\ &< (n+1)n! && \text{inductive step hypothesis} \\ &= (n+1)! \end{aligned}$$

Example 29 Suppose that T_n is a set with n elements. Show that T_n has 2^n subsets (including the empty set).

Induct on n. Notice this time that we can start with $n = 0$, where $T_0 = \emptyset$. Basis Step: Show $n = 0$ satisfies the formula, i.e., show that the empty set has $2^0 = 1$ subset. But the only subset of T_0 is $\emptyset$.

Inductive Step: Show that $n \in S \Rightarrow n+1 \in S$. That is, if T_n has 2^n subsets, show that T_{n+1} has 2^{n+1} subsets. Let $T_n = \{a_1, a_2, \ldots, a_n\}$ and $T_{n+1} = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$. What do the subsets of T_{n+1} look like and how do they compare to the subset of T_n? Well, there are two types of subsets of T_{n+1}: those that contain a_{n+1} and those that do not. The first group is just the collection of subsets of T_n and so it numbers 2^n by indcution. Notice that if we take a subset from the second group—one that contains a_{n+1}—and simply remove a_{n+1} from this set, then we have another subset of T_n. So there must be 2^n of the second type of subsets as well. Therefore, the number of subsets of T_{n+1} is: $2^n + 2^n = 2^{n+1}$. ▯

Theorem 19 ***Induction (Second Form).*** *Let S be a set of (positive) integers containing a. Suppose that S has the property that $n+1$ belongs to S, whenever all the integers from a to n belong to S. Then S contains all positive integers greater than or equal to a.*

EXTRA CREDIT Provide a proof (similar to the first version of induction).

This version of induction is useful as the following example from Math 331 illustrates.

Theorem 20 ***Fundamental Theorem of Arithmetic*** *(First Part) Let $a > 1$. Then there are primes $p_1, \ldots, p_r$ such that*

$$a = p_1 p_2 \cdots p_r.$$

'Every positive integer can be factored (uniquely) into primes.'

Example 30 $84 = 2 \cdot 2 \cdot 3 \cdot 7$.

PROOF Basis Step. Start with $a = 2$. 2 is prime so $2 = 2$ gives the prime factorization.

Inductive Step: Assume the integers 2 to n are in S. Show $n+1 \in S$. There are two cases: Case 1) $n+1$ is prime, then $a = n+1 = p_1$ is the factorization.

Case 2) If $n+1$ is not prime, then $n+1 = ab$ where a and b are positive integers and a and b are greater than 1 and less than $n+1$. That is $2 \leq a, b$ and $a, b \leq m$. Then by the induction hypothesis there are prime factorizations:

$$a = p_1 p_2 \cdots p_r$$

and similarly

$$b = q_1 q_2 \cdots q_s$$

So

$$n+1 = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

which gives the factorization. ∎

We need this version of induction: we can't say that $a = n$ or $b = n$, only that $a \leq n$ and $b \leq n$.