Chapter 1

$\mathbb{N} = \{1, 2, 3, \dots\}$
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$
$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0 \right\}$
$\mathbb{R}$ = real numbers
$\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \ \&\ i^2 = -1\}$

Hernstein uses $A \subset B$ to mean A is a subset of B, not the standard "proper subset" meaning. !!

Basic Sets

Let $n\mathbb{Z}$ denote the set $\{nm : m \in \mathbb{Z}\}$ where $n \in \mathbb{Z}$. Let's prove
$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$

Suppose $x \in 6\mathbb{Z}$. Prove $x \in 2\mathbb{Z} \cap 3\mathbb{Z}$. We show $x \in 6\mathbb{Z} \Rightarrow x \in 2\mathbb{Z} \wedge x \in 3\mathbb{Z}$

$x \in 6\mathbb{Z}$
$\Rightarrow x = 6m \quad m \in \mathbb{Z}$
$\Rightarrow x = 3(2m),\ 2m \in \mathbb{Z} \quad \&\quad x = 2(3m),\ 3m \in \mathbb{Z}$
$\Rightarrow x \in 3\mathbb{Z} \ \&\ x \in 2\mathbb{Z}$
$\Rightarrow x \in 3\mathbb{Z} \cap 2\mathbb{Z}$
$\Rightarrow x \in 2\mathbb{Z} \cap 3\mathbb{Z}$

$x \in 2\mathbb{Z} \cap 3\mathbb{Z}$
$\Rightarrow x \in 2\mathbb{Z} \ \&\ x \in 3\mathbb{Z}$
$\Rightarrow x = 2a \quad x = 3b$ for $a, b \in \mathbb{Z}$
$\Rightarrow x = 2a = 3b$ for $a, b \in \mathbb{Z}$, is this too much of a jump
$\Rightarrow x = 2(3c) = 3(2c)$
$\Rightarrow x = 6c$ for $c \in \mathbb{Z}$
$\Rightarrow x \in 6\mathbb{Z}$

Set Operations

- $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- $A \cup B = \{x \mid x \in A \vee x \in B\}$
- $A \setminus B = A - B = \{x \in A \mid x \notin B\} = \{x \mid x \in A \wedge x \notin B\}$
- $A' = A^c = \{x \mid x \notin A\}$
- $A \times B = \{(a, b) \mid a \in A, b \in B\}$

Induction

We will use induction in this course by assuming the well-ordering-principle rather than the principle of mathematical induction. These are equivalent axioms.

We will be painfully explicit in this class, explicitly defining proposition P_i for $i \in \mathbb{N}$, proving it true for n_0 (i.e. P_{n_0} is true), showing P_{i+1} is true if P_i is true for $i > n_0$.

Example:
Prove 3 divides $4^n - 1$ for $n \in \mathbb{Z}$ $n \geq 0$. Equivalently

Equivalently, we show $\exists k \in \mathbb{Z}$ s.t. $3k = 4^n - 1$ $\forall n \in \mathbb{Z}, n \geq 0$. This is our proposition P_n.

We show P_0 holds: $3k_0 = 4^0 - 1 = 1 - 1 = 0$ where $k_0 = 0 \in \mathbb{Z}$ & $k_0 \geq 0$.

Now, assume P_i is true. We show P_{i+1} is true.

$3k_i = 4^i - 1$ for some $k_i \in \mathbb{Z}$, $\forall$ assumed
$4(3k_i) = 4^{i+1} - 4$
$4(3k_i) + 3 = 4^{i+1} - 1$
$3(4k_i) + 3 = 4^{i+1} - 1$
$3(\underbrace{4k_i + 1}_{k_{i+1}}) = 4^{i+1} - 1$

We have just shown P_{i+1} holds given P_i holds, in particular where $k_{i+1} = 4k_i + 1$.

By the PMI (principle of mathematical induction), $\exists k \in \mathbb{Z}$ s.t. $3k = 4^n - 1$ $\forall n \in \mathbb{Z}$, $n \geq 0$. Thus 3 divides $4^n - 1$ for $n \in \mathbb{Z}$ $n \geq 0$.

Def: Prime
A prime is any integer which has exactly 2 (unique) natural number factors. (1 & itself)

Thm: Fundamental Theorem of Arithmetic
Every positive integer $n \geq 2$ is a product of 1 or more primes.

That is if $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ where p_i & q_i are primes, then $s = t$ & after rearrangement $p_i = q_i$ $i = 1, \ldots, t$. (or $\{p_i\} = \{q_i\}$).

pf:
Let our proposition be r_n (not p b/c we're already using that for primes).

Let m be an integer $m \geq 2$ such that r_m is true. We show r_{m+1} is true.

$m = p_1 \cdots p_s$ where $p_1, \ldots, p_s$ are primes
$m + 1 = p_1 \cdots p_s + 1$

Case $m+1$ is prime:
Trivially r_{m+1} is true.

Case $m+1$ is not prime:
Tough! We'll get to in a bit

Def: Well-Ordering Principle
Any non-empty subset of $\mathbb{N}$ has a smallest element s_0, that is $\forall s \in S \subseteq \mathbb{N}.\ s_0 \leq s$.

This is equivalent to the Principle of Mathematical Induction.

Def: Extended Well-Ordering Principle
This is the same as the well-ordering principle except on $\mathbb{N} \cup \{0\}$.

This is equivalent b/c if $0 \in S$ then 0 is the smallest element. Otherwise the well-ordering principle applies

With the well-ordering principle, let's return to the Fundamental theorem of arithmetic

Pf: cont.
We prove that given $m \in \mathbb{Z}, m \geq 2$ & r_m holds, we show $m+1$ holds in the case where $m+1$ is not prime.

We prove this by contradiction by assuming that there is indeed a positive integer $n \geq 2$ but n is not a product of one or more primes.

Let $S = \{x \in \mathbb{N} \mid x \geq 2$ & x is not a product of 1 or more primes$\}$.
By definition $S \subseteq \mathbb{N}$ & $S \neq \emptyset$ b/c we assume some n is in S.

By the well-ordering principle, S has a smallest element m.
Since $m \in S$, m is not a prime. Since m is not a p
Since m is not a prime, there are some integers $1 < a < m$, $1 < b < m$ such that $m = ab$.
Since m is the smallest element of S, $a \notin S$ & $b \notin S$.
This means a & b are the products of 1 or more primes.
That means $m = ab$ is the product of 1 or more primes.
Therefore $m \notin S$. Contradiction!

Sorry for making this so wordy. I was following her.

Division

Thm: Division Algorithm (for Integers)
Let $a, b \in \mathbb{Z}$ where $b \neq 0$. Then $\exists q, r \in \mathbb{Z}$ s.t.
$a = bq + r$ & $0 \leq r < |b|$

We're computing a/b; where q is the quotient & r is the remainder

q & r are also unique but we won't show that now.

When we use $b = 2$, then we get even/odd integers. That is every integer k has $a \in \mathbb{Z}$ s.t. $k = 2a$ or $k = 2a+1$

We call it the extended division algorithm

Examples:
Let $a = 20$ & $b = 3$. $q = 6$, $r = 2$. $\quad 20 = 3(6) + 2$ (a b q r)

Let $a = -20$ & $b = 3$. $q = -7$, $r = 1$. $\quad 20 = 3(-7) + 1$ (a b q r)

We'd want $q = -6$ & $r = -2$, but r needs to be positive so you "wrap around" r forward causing you to push q back

$$20 = 3(-6) - 2 = 3(-6) - 2 + 3 - 3 = 3(-7) + 1$$

Let $a = -20$ & $b = -3$. $q = 7$, $r = 1$.

Pf:
Let's consider where $b > 0$ (or $b \geq 1$ bc integers). Let $S = \{a - bq : q \in \mathbb{Z} \text{ \& } a - bq \geq 0\}$. We show $S \neq \emptyset$. We show $S \neq \emptyset$ to be able to use the well-ordering principle (only non-negative elements).

If $a \geq 0$, then $a - b \cdot 0 \in S$, so $S \neq \emptyset$.
If $a < 0$, $a - ba = a(1-b) \geq 0 \in S$ since $a < 0$ & $1 - b \leq 0$, so $S \neq \emptyset$.
$a - ba = a(1-b) \geq 0$ since

Since S is a non-empty subset of $\mathbb{N} \cup \{0\}$, we can use the extended well ordering principle. Let r be the smallest element of S.

Since $r \in S$, there exists an integer q such that $r = a - bq \geq 0$, so $a = bq + r$ where $q, r \in \mathbb{Z}$ & $r \geq 0$.

We still need to show $r < |b| = b$ (bc $b > 0$).

~~ignore me~~

To show this, assume for contradiction that $r \geq b$. In that case $r - b \geq 0$. Moreover $r - b < r$ since $b > 0$.
Since $r = a - bq$ for some q, $r - b$
$r - b = (a - bq) - b = a - b(q+1)$.

Since $q \in \mathbb{Z}$, $q + 1 \in S$. Therefore $r - b \in S$, but $r - b < r$ & we said r is the smallest element. Therefore $r < |b|$ must be true.

Now consider wher $b < 0$. Then $-b$ is a positive integer. By the above proof, there exist integers q & r s.t. $a = (-b)q + r$ where $0 \leq r < -b = |b|$.
Then $a = b(-q) + r$ where $-q$ & r are integers & $0 \leq r < |b|$.

We have thus show the divisoon algorithm holds when $b < 0$ & $b > 0$, so we have proved the theorem.

We can use the division algorithm to get other algorithms such as the greatest common divisor.

Def: Greatest Common Divisor (GCD)
Let $a, b \in \mathbb{Z}$. An integer d is said to be the greatest common divisor iff

(i) $d > 0$,

(ii) d divides a & d divides b, &

(iii) if c is a non-zero integer that divides a & b, c divides d.

We denote d by $d = \gcd(a, b)$.

Rem: This division algorithm generalizes to other algebraic systems

Thm:
Let $a, b \in \mathbb{Z}$ & not both $= 0$. Then
i) the greatest common divisor of a & b $\gcd(a, b)$ exists
ii) there exists integers s & t s.t. $\gcd(a, b) = as + bt$

Pf:
We again use the well ordering principle.

Let $S = \{ a\hat{s} + b\hat{t} : \hat{s}, \hat{t} \in \mathbb{Z} \text{ \& } a\hat{s} + b\hat{t} > 0 \}$.

We show $S \neq \emptyset$.
If $a \neq 0$, $a(1) + b(0) = a > 0$ when $a > 0$ & $a(-1) + b(0) = -a > 0$ when $a < 0$.
Likewise for b.
Therefore $S \neq \emptyset$.

By the well-ordering-principle S has a smallest element we denote d.
So $d > 0$ $\exists s, t \in \mathbb{Z}$ s.t. $d = as + bt$

Trivially $d > 0$ (i).

We show (iii).
Let $c \in \mathbb{Z}$ s.t. c divides a & c divides b.

By def $\exists x, y \in \mathbb{Z}$ s.t. $a = cx$ & $b = cy$
$\Rightarrow d = as + bt = cxs + cyt = c(xs + yt)$
Since $xs + yt \in \mathbb{Z}$, c divides d.

We now show (ii), that is d divides a & d divides b. The method below can be done equivalently for a & b, even tho only a is shown.

By the division algorithm, $\exists q, r \in \mathbb{Z}$ s.t. $a = qd + r$ $0 \leq r < |d| = d$ ← recall $d > 0$
To show d divides a, we show $r = 0$.

Assume for contradiction that $r \neq 0$ so $0 < r < d$.
$r = a - dq$
$= a - (as + bt)q$
$= a - asq - btq$
$= a(1 - sq) + b(-tq)$
Therefore $r \in S$, but $r < d$ & d is the smallest element of S.
Therefore $r = 0$.
Therefore (ii).

We have thus shown (i), (ii), & (iii).

This isn't normally how we calculate gcd(a, b). Instead we use the Euclidean algorithm.

Thm:
gcd(0, 0) is undefined.

Pf:
This proof comes b/c all integers divide 0 & 0.
Suppose $d = \gcd(0, 0)$ exists.
Let $c = d + 1$. c divides 0 & 0 but not d, thus (iii) is violated.
∴ No d exists.

Should formally show $c = d + 1$ doesn't divide d.

Thm:
If $a = 0$ & $b > 0$ then $\gcd(a, b) = b$.

Let $d = b$. We show $d = \gcd(a, b)$.

Since $b > 0$, $d > 0$. Thus (i).

$d = b$ divides $a = 0$ where $a = d(0)$ & divides b where $b = d(1)$. Thus (ii).

Let c be a non-zero integer that divides a & b. c divides $d = b$ trivially b/c c divides b. Thus (iii).

Therefore, when $a = 0$ & $b > 0$ $b \in \mathbb{Z}$, $\gcd(a, b) = b$.

Thm:
Let $a = 0$ & $b < 0$. $\gcd(a, b) = -b$. This falls from the previous theorem.

We have thus shown $\forall n \in \mathbb{Z}$ $n \neq 0$, $\gcd(n, 0) = \gcd(0, n) = n$.

Example:
Let $s, t \in \mathbb{Z}$ be such that $\gcd(123456, 1000) = 123456s + 1000t$

$\gcd(123456, 1000) = 123456(s+1000) + 1000(t - 123456)$ also holds
$\gcd(123456, 1000) = 123456(s-2000) + 1000(t - 2 \cdot 123456)$ also holds

In general, when $a, b, s, t \in \mathbb{Z}$ where not both $a=0$ & $b=0$.
$\gcd(a, b) = a(s+bn) + b(t-an) \quad \forall n \in \mathbb{Z}$
This is equivalent to $\gcd(a, b) = as' + bt'$ for some $s', t' \in \mathbb{Z}$ but it uses some fixed s & t. In fact, from some fixed s & t you can get all possible s' & t'.

Def:
Two integers a & b are <u>relatively prime</u> or <u>coprime</u> iff $\gcd(a, b) = 1$

Example:
2 & 3 are relatively prime. 2 & 4 are not.

Example:
Let p be a prime & a be an integer. What is the GCD of p & a?

If p divides a, $\gcd(p, a) = p$

If p does not divide a, $\gcd(p, a) = 1$ & p & a are relatively prime
This means $1 = ps + at$ for some $s, t \in \mathbb{Z}$

Thm:
Let $a, b \in \mathbb{Z}$ be both not zero. $1 = as + bt$ for some $s, t \in \mathbb{Z}$ iff a & b are relatively prime.

pf: a, b coprime $\Rightarrow \exists s, t \in \mathbb{Z}$ s.t. $1 = as + bt$
We show a & b coprime $\Rightarrow 1 = as + bt$ for some $s, t \in \mathbb{Z}$

This falls from the definition of a, b coprime ($\gcd(a, b) = 1$) & the theorem $\gcd(a, b) = as + bt$ for some $s, t \in \mathbb{Z}$

pf: $\exists s, t \in \mathbb{Z}$ s.t. $1 = as + bt \Rightarrow a, b$ coprime
Suppose $1 = as + bt$ for some $s, t \in \mathbb{Z}$. We show $\gcd(a, b) = 1$ so a & b are relatively prime. The Roman numerals are the parts of the definition of GCD.

Trivially $1 > 0$. (i)

1 divides a where $a = 1(a)$ & 1 divides b $b = 1(b)$. (ii)

Let c divide a & b, so $a = q_a c$ & $b = q_b c$ for some $q_a, q_b \in \mathbb{Z}$
$1 = as + bt = q_a cs + q_b ct = c(q_a s + q_b t)$, so c divides 1. (iii) □

Thm:
Let $a, b, c \in \mathbb{Z}$ s.t. $a \neq 0$, a divides bc, & a, b coprime.
Then a divides c.

Pf:
Since a, b coprime, then $\exists s, t \in \mathbb{Z}$ s.t. $1 = as + bt$,
Since a divides bc, $bc = aw$ for some $w \in \mathbb{Z}$

$c = 1 \cdot c = (as + bt)c = asc + btc = asc + (bc)t = asc + awt = a(sc + wt)$

Therefore, a divides c.

Thm:
Suppose that p is a prime & p divides bc where $b, c \in \mathbb{Z}$.
Then p divides b or p divides c

Pf:
We split this into two cases.

If p divides b, then the theorem holds trivially. □

If p doesn't divide b, then p & b are relatively prime, so
$\gcd(p, b) = 1 = ps + bt$ for some $s, t \in \mathbb{Z}$ ← unnecessary
By the earlier theorem p divides c. □

In both cases, p divides b or p divides c.

This does not hold for non-primes.

Cor:
Suppose p is a prime, k is a positive integer, & $b_1, \ldots, b_k$ are integers such that p divides $b_1 \cdots b_k$

Then there exists an integer i $1 \leq i \leq k$ such that p divides b_i.
Basically p divides at least one b_i.

This can be shown easily w/ induction.

Thm:
Let n be a positive integer & $p_1, \ldots, p_n$ be primes. Let $M = p_1 \cdots p_n + 1$

Then M is relatively prime with all primes p_i.

Let $i \in \mathbb{Z}$ $1 \leq i \leq n$. $M + (-p_1 \cdots p_{i-1} p_{i+1} \cdots p_n) = 1$ by rearranging the above eqn.
Therefore, $\forall i \in \mathbb{Z}$ $1 \leq i \leq n$, M, p_i coprime. □

This works similarly for all subsets of $p_1, \ldots, p_n$

Def: Function Composition

Let $f: A \to B$, $g: B \to C$ be functions.

The composition $g \circ f: A \to C$ is

$$(g \circ f)(x) = g(f(x))$$

Note that $Rng(f) = Dom(g) = B$ might not always be true. You're only guaranteed $Rng(f) \subseteq Dom(g)$.

Example:

Let $f(x) = \sqrt{x}$ & $g(x) = \begin{cases} x+1 & x \geq 4 \\ -x & x < 4 \end{cases}$

$Dom(f) = [0, \infty)$

$Dom(g) = \mathbb{R}$

Let's find $Dom(g \circ f)$. & the domain of

$$\begin{aligned} Dom(g \circ f) &= \{ a \in Dom(f) \mid f(a) \in Dom(g) \} \\ &= \{ a \in [0, \infty) \mid \sqrt{a} \in \mathbb{R} \} \\ &= [0, \infty) \end{aligned}$$

The functional rule of a function just says how to evaluate the function.

Let's find the functional rule for $g \circ f$

$$(g \circ f)(x) = g(f(x)) \quad x \in [0, \infty)$$

$$= g(\sqrt{x}) \quad x \in [0, \infty)$$

$$= \begin{cases} \sqrt{x} + 1 & x \geq 16 \\ -\sqrt{x} & x < 16 \end{cases}$$

$x \geq 16 \leftarrow f(16) = 4 \Leftrightarrow f^{-1}(4) = 16$ } f^{-1} exists b/c $Dom(f) = [0, \infty)$

$x < 16 \leftarrow f(16) = 4 \Leftrightarrow f^{-1}(4) = 16$ }

Thm:

Let $f: A \to B$, $g: B \to C$, $h: C \to D$ be functions where A, B, C, D are non-empty sets. Then

i) $h \circ (g \circ f) = (h \circ g) \circ f$,

ii) $f \circ i_A = f$ where i_A is identity for A

iii) $i_B \circ f = f$ " i_B " " " B

We show (i)

$$\begin{aligned} (h \circ (g \circ f))(a) \\ &= h[(g \circ f)(a)] \\ &= h(g(f(a))) \end{aligned}$$

$$\begin{aligned} ((h \circ g) \circ f)(a) &= \\ &= (h \circ g)(f(a)) \\ &= h(g(f(a))) \end{aligned}$$

Def:
$f: A \to B$ is said to be <u>surjective / onto / a surjection</u> iff $Rng(f) = B$.

This means that
i) $\forall a \in A$, $f(a) \in B$ &
ii) $\forall b \in B$, $\exists a \in A$ s.t. $f(a) = b$.

Example
$f: \mathbb{R} \to \mathbb{R}$ $f(x) = x^2$ is not surjective.

Consider $b = -3 \in \mathbb{R}$. Assume for contradiction that $b = -3 \in Rng(f)$.
That means $\exists a \in A$ s.t. $-3 = f(a) = a^2$. However $a^2 \geq 0$, but $b = -3 < 0$. Thus $b = -3 \notin Rng(f)$
Thus f is not surjective.

The differentiation b/w range & codomain is a fine one. All functions are onto some codomain, namely their range.

Example:
Let $f: \mathbb{R} \to \mathbb{R}$ $f(x) = e^x$. Let's show f is onto $(0, \infty)$.

To prove f is onto $(0, \infty)$, we prove $Rng(f) = (0, \infty)$. We do this by double set inclusion.

We show that $(0, \infty) \subseteq Rng(f)$.
Let $b \in (0, \infty)$. & $a = \ln(b)$. a is a real number b/c $b > 0$.
Moreover $f(a) = e^a = e^{\ln(b)} = b$.
So $b \in Rng(f)$ & $(0, \infty) \subseteq Rng(f)$.

We show $Rng(f) \subseteq (0, \infty)$.
Let $a \in \mathbb{R}$. We show $f(a) \in (0, \infty)$.
$f(a) = e^a > 0$ for $a \in \mathbb{R}$.
So $f(a) \in (0, \infty)$ & $Rng(f) \subseteq (0, \infty)$

Thus $Rng(f) = (0, \infty)$ & f is onto $(0, \infty)$.

Def:
$f: A \to B$ is said to be injective/ one-to-one/ an injection iff $u = v$ whenever $f(u) = f(v)$

In terms of ordered pairs,
$u = v$ whenever $(u, b) \in f$ & $(v, b) \in f$.

Essentially every output is only mapped to by one input.

Example:
Let S be a non-empty set. The identity function i_S is injective.

Example:
We define an $f: \mathbb{N} \to \mathbb{N}$ s.t. f is surjective but not injective
$f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ n & \text{if } n \text{ odd} \end{cases}$

f is not injective b/c $f(1) = f(2) = 1$.

To show f is surjective, we show $Rng(f) = \mathbb{N}$ by double set inclusion. ← left as exercise

Thm:
Let $f: A \to B$ & $g: B \to C$ be injections. $g \circ f$ is an injection

Pf:
Suppose $(g \circ f)(u) = (g \circ f)(v)$. We show $u = v$.

$(g \circ f)(u) = (g \circ f)(v)$
$\Rightarrow g[f(u)] = g[f(v)]$

Since g is one-to-one, $f(u) = f(v)$.
Since f is one-to-one, $u = v$.

Thus $g \circ f$ is injective iff $f: A \to B$, $g: B \to C$ is injective.

Def:
If f is any function, we may define the <u>inverse of f</u> as f^{-1} defined as
$(a, b) \in f^{-1}$ iff $(b, a) \in f$

f^{-1} itself is a function iff
$(a, c) \in f^{-1}$ & $(a, b) \in f^{-1} \Rightarrow b = c$.

We rewrite this in terms of f
$(c, a) \in f$ & $(b, a) \in f \Rightarrow b = c$.
<u>In other words, f^{-1} is a function iff f is injective.</u>

Since we derive f^{-1} by switching coordinates, if f & f^{-1} are functions, then
$f^{-1}(a) = b \iff f(b) = a$

$\text{Dom}(f^{-1}) = \text{Rng}(f)$
$\text{Rng}(f^{-1}) = \text{Dom}(f)$

Thm:
Suppose $f: A \to B$ is a one-to-one function w/ $B' = \text{Rng}(f) \subseteq B$. Then
$f^{-1} \circ f = id_A$ & $f \circ f^{-1} = id_B$

Pf:
Let $a \in A$ & $b = f(a)$. Then $f^{-1}(b) = a$ by def.
So
$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = id_A(a)$.
We have shown $f^{-1} \circ f = id_A$.

$g \circ f = id_B$ follows similarly. □

Def:
Let $f: A \to B$ be a function where A & B are nonempty.

f is called <u>injective / an injection / a one-to-one correspondance b/w A & B</u> iff f is injective/one-to-one & surjective/onto.

Example:
Let's define a bijection $f: \mathbb{N} \cup \{0\} \to \{z \in \mathbb{Z} \mid z < 0\}$. That is a bijection b/w the non-negative integers & the negative integers.

Let $f(n) = -n-1$. f is a function, we show it is onto & one-to-one.

Let $a, b \in \mathbb{N} \cup \{0\}$ where $f(a) = f(b)$. We show $a = b$. That is f is one-to-one.
$f(a) = f(b) \Rightarrow -a-1 = -b-1 \Rightarrow -a = -b \Rightarrow a = b$.
Thus f is one-to-one.

To show f is onto, we show $Rng(f) = \{z \in \mathbb{Z} \mid z < 0\}$ by double set inclusion

We show $Rng(f) \subseteq \{z \in \mathbb{Z} \mid z < 0\}$.
If $n \in \mathbb{N} \cup \{0\}$, then $n \geq 0$ & $-n \leq 0$.
Therefore, $-n-1 \leq 0-1 \Rightarrow -n-1 \leq 1$
So $f(n) \in \{z \in \mathbb{Z} \mid z < 0\}$ & $Rng(f) \subseteq \{z \in \mathbb{Z} \mid z < 0\}$.

We show $\{z \in \mathbb{Z} \mid z < 0\} \subseteq Rng(f)$.
Let $z \in \mathbb{Z}$ where $z < 0$. We show $z = f(a)$ for some $a \in \mathbb{N} \cup \{0\}$
Let $a = -z-1$. $f(a) = -a-1 = -(-z-1)-1 = z+1-1 = z$
We now show $a \in \mathbb{N} \cup \{0\}$. (should do after $a \in \mathbb{N} \cup \{0\}$)
By def, $z < 0$. So $-z > 0$ & $-z-1 > 0-1 \Leftrightarrow -z-1 > -1$.
Therefore $a = -z-1 \in \mathbb{N} \cup \{0\}$.

$z = -a-1$
$-z = a+1$
$a = -z-1$

Since z is integer, $a = -z-1$ is an integer

Thm: Given a finite set S, the number of possible bijections f is $n!$ where $n = |S|$.

Pf:

We can describe each bijection as a permutation of S, where the i-th element in S maps to the i-th element in the permutation.

If $S = \{1, 2, 3\}$

f_1	f_2	f_3	f_4	f_5	f_6
$1 \to 1$	$1 \to 1$	$1 \to 2$	$1 \to 2$	$1 \to 3$	$1 \to 3$
$2 \to 2$	$2 \to 3$	$2 \to 1$	$2 \to 3$	$2 \to 1$	$2 \to 2$
$3 \to 3$	$3 \to 2$	$3 \to 3$	$3 \to 1$	$3 \to 2$	$3 \to 1$

Thm: Suppose $f: A \to B$, $g: B \to C$ are bijections where A, B, C non-empty sets,

i) $g \circ f: A \to C$ is a bijection

ii) $f^{-1}: B \to A$ is a bijection

Pf:

i) We know the composition of surjections is a surjection & the composition of injections is an injection. Thus $g \circ f: A \to C$ is a bijection. □

ii) We first prove f^{-1} is one-to-one.
We show that $f^{-1}(d) = f^{-1}(e)$ implies $d = e$.
Suppose $f^{-1}(d) = f^{-1}(e)$.

$d = f(f^{-1}(d)) = f(f^{-1}(e)) = e$ since $f^{-1}(d) = f^{-1}(e)$ & f is a function. □

OR

Let $k = f^{-1}(d) = f^{-1}(e)$. Since $f^{-1}(d) = k$, $d = f(k)$. Since $f^{-1}(e) = k$, $e = f(k)$.
Since f is a function, $d = e$. □

Now let's talk about all bijections. Like we were w/ the theorem at top.
Let S be a non-empty set.
Let $A(S) = \{f: S \to S \mid f \text{ bijective}\}$ be the set of all bijections w/in S.

Thm:
Let S be a non-empty set.

i) If $f, g \in A(S)$, $g \circ f \in A(S)$

ii) If $f, g, h \in A(S)$, $h \circ (g \circ f) = (h \circ g) \circ f$

iii) i_S (identity on S) is an element of $A(S)$. If $f \in A(S)$, $f \circ i_S = i_S \circ f = f$.

iv) If $f \in A(S)$, $\exists f^{-1} \in A(S)$ s.t. $f \circ f^{-1} = f^{-1} \circ f = i_S$.

Notation:
If $f: A \to B$ & $g: B \to C$ are functions, $g \circ f = gf$

Def:
Let $f \in A(S)$ where S is a non-empty set.

i) $f^0 = i_S$

ii) $f^1 = f$ ← technically unnecessary but good to see

iii) $f^n = f f^{n-1}$ where $n \in \mathbb{N}$ ← f composed n times

iv) $f^{-n} = f^{-1} f^{-n+1} = (f^{-1})^n$ where $n \in \mathbb{N}$ ← f^{-1} composed n times

Note: $f^{-1}: S \to S$ is a bijection b/c inverse of bijection is bijection

Prop:
Many of our power rules were used to hold.
Let $f, g \in A(S)$ where S is a non-empty set. Let $n, m \in \mathbb{Z}$

i) $f^n f^m = f^{n+m}$

ii) $(f^n)^m = f^{nm}$

iii) $(fg)^n \neq f^n g^n$ in general

Example:
Let $f, g \in S_3$ where $f(1)=1$, $f(2)=3$, $f(3)=2$ & $g(1)=3$, $g(2)=1$, $g(3)=2$

Recall: $S_n = \{1, \dots, n\}$

Consider f^2, g^2, $f^2 \circ g^2$, $f \circ g$, $(f \circ g)^2$

i) f^2: $1 \to 1$, $2 \to 2$, $3 \to 3$

ii) g^2: $1 \to 2$, $2 \to 3$, $3 \to 1$

iii) $f^2 \circ g^2$: $1 \to 2$, $2 \to 3$, $3 \to 1$

iv) $f \circ g$: $1 \to 2$, $2 \to 1$, $3 \to 3$

v) $(f \circ g)^2$: $1 \to 1$, $2 \to 2$, $3 \to 3$

Note: $f^2 \circ g^2 \neq (f \circ g)^2$

Thm:
Let $f, g \in A(S)$ where S is a non-empty set.
Then
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Pf:

Let $s_1 \in S$, $s_2 = g^{-1}(s_1)$, & $s_3 = f^{-1}(s_2)$. Since
Since $s_2 = g^{-1}(s_1)$, $g(s_2) = s_1$. Like wise $f(s_3) = s_2$.

$$(f^{-1} \circ g^{-1})(s_1) = f^{-1}(g^{-1}(s_1)) = f^{-1}(s_2) = s_3$$
$$(g \circ f)(s_3) = g(f(s_3)) = g(s_2) = s_1$$

$\therefore (g \circ f)^{-1} = f^{-1} \circ g^{-1}$ □

#(Equivalence) Relations

Def:
A relation on a set S is a subset $R \subseteq S \times S$.

More intuitively, it is a function $R: S \times S \to \{T, F\}$ that decides if two sets are related. $(s,t) \in R \Leftrightarrow sRt$.

Def:
Let S be a non-empty set & R be a relation on S.

i) R is <u>reflexive</u> iff $\forall s \in S$. $(s,s) \in R$ (or sRs)

ii) R is <u>symmetric</u> iff $\forall s,t \in S$ $(s,t) \in R \Leftrightarrow (t,s) \in R$

iii) R is <u>transitive</u> iff $\forall s,t,u \in S$ $(s,t) \in R \wedge (t,u) \in R \Rightarrow (s,u) \in R$

Def:
Let S be a non-empty set & R be a relation on S.
R is an <u>equivalence</u> relation iff it is reflexive, symmetric, & transitive.

Let $s,t \in S$. We say s is equivalent to t & write $s \sim t$ iff $(s,t) \in R$

Using tilde $\sim$ notation, we get
Reflexive: $\forall s \in S$ $s \sim s$
Symmetric: $\forall s,t \in S$ $s \sim t \Leftrightarrow t \sim s$
Transitive: $\forall s,t,u \in S$ $s \sim t \wedge t \sim u \Rightarrow s \sim u$.

Example:
Let S be a non-empty set.
Let $I_S = \{(s,t) \in S \times S \mid s = t\}$.

I_S is an equivalence relation. I won't write the proof b/c I'm behind.

Def: Congruence Modulo n
Let $n \in \mathbb{N}$ & $a, b \in \mathbb{Z}$. We define relation
We define relation $\sim$ on $\mathbb{Z}$ by
$a \sim b$ iff n divides $a-b$.

In other words,
$a \sim b \Leftrightarrow \exists c \in \mathbb{C}$ s.t. $a-b = cn$ or equivalently $a = cn+b$

Iff $a \sim b$, we say a is congruent to b mod(ulo) n.

Notation:
To emphasize the dependence on the dependence of n, many people write
$a \equiv b \pmod{n}$
iff $a \sim b$.

Thm:
Congruence modulo n is an equivalence relation

Reflexivity:
Let $a \in \mathbb{Z}$. We show $a \sim a$.

$a \sim a$ holds b/c $a - a = cn$ for all n when $c = 0 \in \mathbb{Z}$.

Symmetry:
Let $a, b, n \in \mathbb{Z}$. Assume $a \sim b$. We show $b \sim a$.

$a \sim b \Rightarrow a - b = cn$ for some $c \in \mathbb{Z}$

Multiplying both sides by -1 gives us
$-a + b = -cn = (-c)n$ where $-c \in \mathbb{Z}$
$\Rightarrow b \sim a$.

Thus $\sim$ is reflexive.

Transitivity:
Let $a, b, c, n \in \mathbb{Z}$. Assume $a \sim b$ & $b \sim c$. We show $a \sim c$.

$a \sim b \Rightarrow a - b = c_1 n$ for some $c_1 \in \mathbb{Z}$.
$b \sim c \Rightarrow b - c = c_2 n$ for some $c_2 \in \mathbb{Z}$.

Adding the equations gives us
$a - c = c_1 n + c_2 n = (c_1 + c_2)n$
Since $c_1 + c_2$ is an integer,
$a \sim c$
when $a \sim b$ & $b \sim c$. s.

Thus congruence mod n is transitive.
Congruence mod n is an equivalence relation.

Def:

Let $\sim$ be an equivalence relation on S.
The equivalence class of $a \in S$ is
$E = \{b \in S : a \sim b\}$.

Def:

We know congruence mod n is an equivalence relation on S.
Given $a \in \mathbb{Z}$ the congruence/equivalence class of a is

$$[a_n] =$$
$$= \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$$
$$= \{b \in \mathbb{Z} \mid n \text{ divides } b-a\}$$
$$= \{b \in \mathbb{Z} \mid b - a = nc \text{ for some } c \in \mathbb{Z}\}$$
$$= \{b \in \mathbb{Z} \mid b = nc + a \text{ for some } c \in \mathbb{Z}\}.$$

Example:

Let $n = 1$ & $a \in \mathbb{Z}$. Find $[a]_1$.

$$[a]_1 = \{b \in \mathbb{Z} \mid b = a + c \text{ for some } c\}.$$
$$= \{\ldots, a-2, a-1, a, a+1, a+2, \ldots\}$$
$$= \mathbb{Z}$$

Example:

Let $n = 1$.

$$[0]_3 = \{b \in \mathbb{Z} \mid b \equiv 0 \pmod{3}\}$$
$$= \{b \in \mathbb{Z} \mid 3 \text{ divides } b - 0\}$$
$$= \{b \in \mathbb{Z} \mid b = 3c\}$$
$$= \{0, \pm 3, \pm 6, \ldots\}$$

$$[1]_3 = \{1, 1 \pm 3, 1 \pm 6, \ldots\} = \{\ldots, -5, -2, 1, 4, \ldots\}$$

$$[2]_3 = \{2, 2 \pm 3, 2 \pm 6, \ldots\} = \{\ldots, -4, -1, 2, 5, \ldots\}$$

$$[3]_3 = [0]_3$$

$$[-1]_3 = [2]_3$$

N.B. Note that these partition $\mathbb{Z}$.

Thm:
Let R be an equivalence relation on a non-empty set S.

i) The union of all the equivalence classes is S.

ii) If $a, b \in S$ & $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$ & aRb.

Equivalently, if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.

iii) If $a, b \in S$, then $[a] = [b]$ iff $(a, b) \in R$.

Pf:
Let's prove only part iii.

Suppose $[a] = [b]$.
$(a, a) \in R$ holds since R is reflexive.
Since $(a, a) \in R$, $a \in [a]$
Since $[a] = [b]$, $a \in [b]$.
Thus $(a, b) \in R$.

Suppose $(a, b) \in R$. We show $[a] \cap [b] \neq \emptyset$ thus by ii $[a] = [b]$.
We know $(a, b) \in R$, so $a \in [b]$.
Since $(b, a) \in R$ (by reflexivity) $a \in [a]$.
Since $a \in [b]$ & $a \in [a]$, $[a] \cap [a] \neq \emptyset$.
Therefore $[a] = [b]$.

Example:
Let $n = 3$. How do we show $[-16]_3 = [2]_3$ w/o calculating their equivalence classes.

We show
$-16 \equiv -2 \pmod 3$.
$\Leftrightarrow -16 - 2 = -18$ is a multiple of 3

$-18 = -6(3)$, so -18 is a multiple of 3 & $[-16] = [2]_3$.

Thm:
Suppose $n \in \mathbb{N}$. Then
$[a]_n \in \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ $\forall a \in \mathbb{Z}$.
Moreover, if $i, j \in \mathbb{Z}$ b/w 0 & $n-1$ such that $i \neq j$, then
$[i]_n \neq [j]_n$

Pf:
Let $a \in \mathbb{Z}$.
By the division algorithm, $\exists q, r \in \mathbb{Z}$ where $0 \leq r < |n| = n$ s.t.
$a = qn + r$.
The restrictions on r mean
$r \in \{0, 1, \ldots, n-1\}$.

Since $a = qn + r$
$a - r = qn$.
Therefore
$a \equiv r \pmod n$

By iii from the above, $[a]_n = [r]_n \in \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Let's talk about doing math on equivalence classes, in particular wrt congruence mod n.

Def:
Let $n \in \mathbb{N}$.
$\mathbb{Z}_n = \{[0]_n, \ldots, [n-1]_n\}$
is called a <u>ring of integers mod n</u>.

Def:
Let $n \in \mathbb{N}$.
Let's define addition $\oplus$ & multiplication $\otimes$ on $\mathbb{Z}_n$.

$$[a]_n \oplus [b]_n = [a+b]_n$$

$$[a]_n \otimes [b]_n = [a \cdot b]_n$$

(We often drop circles)

We need to show $\oplus$ & $\otimes$ are well defined.

Pf:
To show $\oplus$ is well defined, we need for $a, b, c, d \in \mathbb{Z}$
$[a]_n = [c]_n$ & $[b]_n = [d]_n$
$\Rightarrow [a]_n + [b]_n = [c]_n + [d]_n$.

$[a]_n = [c]_n \Leftrightarrow a \equiv c \pmod n$
$[b]_n = [d]_n \Leftrightarrow b \equiv d \pmod n$
$[a+b]_n$ $[c+d]_n$
To get $[a]_n + [b]_n = [c]_n + [d]_n$, we need to show
$(a+b) \pmod n = (c+d) \pmod n$
$\Leftrightarrow a+b \equiv (c+d) \pmod n$

Since $a \equiv c \pmod n$ & $b \equiv d \pmod n$, $\exists s, t \in \mathbb{Z}$ s.t.
$a - c = sn$
$b - d = tn$

We try to write $(a+c)-(b+d)$ in terms of n to show
$a+b \equiv (c+d) \pmod n$
$(a+b) - (c+d)$
$= a - c + b - d$
$= sn + tn$
$= (s+t)n$

Since $s, t \in \mathbb{Z}$, $s+t \in \mathbb{Z}$. Thus we have just written n divides $(a+b) - (c+d)$.

Thus
$$a+b \equiv (c+d) \pmod{n}$$
$\therefore \oplus$ is well defined.

Pf:
The proof that $\otimes$ is well defined follows a similar proof.

Example:

Find $([a]_{16}+[10]_{16})[6]_{16}$ writing our final answer as $[a]_{16}$ where $0 \le a < 16$.

$$([a]_{16}+[10]_{16})[6]_{16} = [14]_{16}[6]_{16} = [3]_{16}[6]_{16} = [18]_{16} = [2]_{16}$$

Prop:
Many of our normal additive & multiplicative properties hold for $\oplus$ & $\otimes$

i) $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$

ii) $[a]_n + [b]_n = [b]_n + [a]_n$

iii) $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$

iv) $[a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$

v) $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$

vi) $([a]_n[b]_n)[c]_n = [a]_n([b]_n[c]_n)$

vii) $[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$

Not Properties:
Notably, a few properties fail for $\oplus$ & $\otimes$.

i) $[a]_n[b]_n = [0]_n \not\Rightarrow ab = 0$ (i.e. a or b are zero).

Example: $[3]_6[4]_6 = [12]_6 = [0]_n$ but $3 \cdot 4 \neq 0$ & $3 \neq 0$ & $4 \neq 0$

Sometimes Properties:
Let $n \in \mathbb{N}$.
Let $a \in \mathbb{Z}$. Does there exist $b \in \mathbb{Z}$ s.t.
$[a]_n[b]_n = [1]_n$.
In other words, for what n is there a multiplicative inverse.

Suppose there is such a b. Then
$$[a]_n[b]_n = [ab]_n = [1]_n$$
so
$$ab \equiv 1 \pmod{n}$$

This means
$$ab - 1 = cn \quad \text{for some } c \in \mathbb{Z}$$
Thus
$$ab + n(-c) = 1 \quad \text{for some } c \in \mathbb{Z}.$$

Since b & $-c$ are some integers, we know $\gcd(a, n) = 1$ & thus a & n are coprime.

Let's try to show that if a & n are coprime then there is a multiplicative inverse of a.

Suppose a & n are relatively prime. That is
$\gcd(a,n)=1 \Leftrightarrow ab+nt=1$ for some $b, t\in\mathbb{Z}$

Then
$$[1]_n=[ab+nt]_n=[a]_n[b]_n+[n]_n[t]_n$$
$$=[a]_n[b]_n+[0]_n[t]_n$$
$$=[a]_n[b]_n.$$

Thus there does exist some $b\in\mathbb{Z}$ s.t.
$[a]_n[b]_n=[1]_n$.

Thus
$[a]_n[b]_n=[1]_n$ for some $b\in\mathbb{Z}$
iff a & n are relatively prime.

Chapter 2

Binary Operations/Operators

We also say

Def:

Let S be a non-empty set.
A binary operation on S is a function $f: S \times S \to S$.

Notation:

We write $f((a,b)) = a * b$ unless f is known (e.g. $f = +$).
We say S is closed under the binary operation $*$.

Examples:

i) Multiplication on natural numbers $\times: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a binary operation.

ii) Subtraction on natural numbers $-: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is not a binary operator. $1 - 1 = 0 \notin \mathbb{N}$.

iii) Composition of bijections $\circ: A(S) \times A(S) \to A(S)$ is a binary operation b/c
$g \circ f \in A(S) \quad \forall f, g \in A(S)$

iv) Matrix addition $+: \mathbb{R}^{m \times n} \times \mathbb{R}^{m \times n} \to \mathbb{R}^{m \times n}$ is a binary operation

v) Matrix multiplication on square matrices $\times: \mathbb{R}^{n \times n} \times \mathbb{R}^{n \times n} \to \mathbb{R}^{n \times n}$ is a binary operation.

Example:

Let $n \in \mathbb{N}$.
Let $GL_{n \times n}(\mathbb{R}) = \{ X \in \mathbb{R}^{n \times n} \mid \det(X) \neq 0 \}$ be the general linear group of $\mathbb{R}^{n \times n}$.

$$GL_{2 \times 2}(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \text{ where } ad - bc = 0 \right\}$$

Is $+$ a binary operator? No!

$$I + (-I) = [0]$$

but

$\det(I) = 1 \neq 0 \iff I \in GL_{2 \times 2}(\mathbb{R})$,
$\det(-I) = (-1)^n \neq 0 \iff -I \in GL_{2 \times 2}(\mathbb{R})$, &
$\det([0]) = 0 \iff [0] \in GL_{2 \times 2}(\mathbb{R})$.

Example:
Is $*$ defined on $\mathbb{Q}^+$ a binary operation on $\mathbb{Q}^+$.
$\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b+d}$ $\forall a,b,c,d \in \mathbb{N}$.

No b/c $*$ is not well defined
$\frac{1}{2} * \frac{1}{3} = \frac{2}{5} \neq \frac{3}{8} = \frac{1}{2} * \frac{2}{6}$

Example:
Suppose $p \in \mathbb{N}$ is a prime. We show all elements $n \in \mathbb{Z}_p$ where $n \neq 0$ have a multiplicative inverse.

Groups

Def:
Let G be a nonempty set & let $*$ be a binary operation on G.
$(G,*)$ is a group or G is said to be a group (under $*$) iff

i) Closure: $a*b \in G$ $\forall a,b \in G$

ii) Associative Law: $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$

iii) Existence of Identity: $\exists e \in G$ s.t. $a*e = e*a = a$. e is the identity (or unit)

iv) Existence of Inverses: $\forall a \in G$ $\exists b \in G$ $a*b = b*a = e$. We say $a = b^{-1}$ & $b = a^{-1}$.

We call a group an abelian group (under $*$) iff i-iv hold & also the following holds. Opposite is non-abelian.

Comes from mathematician Abel.

v) Commutative Laws: $a*b = b*a$ $\forall a,b \in G$

We call a group infinite if it has infinitely many elements. Opposite is finite.

Examples:
i) $\mathbb{Q}$ under $+$ is an infinite abelian group.
ii) $\mathbb{Q}$ under $\cdot$ (multiplication) is not a group b/c there is no inverse for 0.
iii) we "fix" this by excluding 0 or only looking at positive rationals.
$\mathbb{Q} \setminus \{0\}$ under multiplication $\cdot$ is an infinite abelian group.
$\mathbb{Q}^+$ under multiplication $\cdot$ is also an infinite abelian group.

Example:
Let $n \in \mathbb{N}$. Consider $M_{n\times n}(\mathbb{R})$ ($n \times n$ matrices over $\mathbb{R}$).
$M_{n\times n}(\mathbb{R})$ is a group under what binary operations.

$M_{n\times n}(\mathbb{R})$ is a group under $+$.

i) $A+B \in M_{n\times n}(\mathbb{R})$ $\forall A,B \in M_{n\times n}(\mathbb{R})$

ii) $(A+B)+C = A+(B+C)$ $\forall A,B,C \in M_{n\times n}(\mathbb{R})$

iii) $[0] \in$ b/c $\forall A \in M_{n\times n}(\mathbb{R})$ $A+[0] = [0]+A = A$

iv) $\forall A \in M_{n\times n}(\mathbb{R})$ $A+(-A) = (-A)+A = [0]$

(v) also holds, so $M_{n\times n}(\mathbb{R})$ is an infinite abelian group under $+$.

$M_{n\times n}(\mathbb{R})$ is not a group under $\cdot$ b/c $[0]\in M_{n\times n}(\mathbb{R})$ but $[0]$ has no inverse.

Consider $GL_{n\times n}(\mathbb{R}) = \{A\in\mathbb{R}^{n\times n} : \det(A)\neq 0\}$. This is an infinite group. It is abelian iff $n=1$ & non-abelian o/w.

i) $AB\in GL_{n\times n}(\mathbb{R})$ b/c $\det(AB)=\det(A)\det(B)\neq 0$ b/c $\det(A)\neq 0$ & $\det(B)\neq 0$.

ii) $(AB)C=A(BC)$ $\forall A,B,C\in GL_{n\times n}(\mathbb{R})$

iii) $I=e$ b/c $AI=IA=A$ $\forall A\in GL_{n\times n}(\mathbb{R})$

iv) $\exists A^{-1}$ s.t. $AA^{-1}=A^{-1}A=I$ $\forall A$ iff $\det(A)\neq 0$. Since $A\in GL_{n\times n}(\mathbb{R})$, we know $\det(A)\neq 0$.

Example:

Let $n\in\mathbb{N}$.

$\mathbb{Z}_n$ is a finite abelian group under $+$.

Note: We should show numbers going together into $[\dots]_n$

i) $[a]_n+[b]_n=[a+b]_n\in\mathbb{Z}_n$ $\forall [a]_n,[b]_n\in\mathbb{Z}_n$

ii) $([a]_n+[b]_n)+[c]_n=[a]_n+([b]_n+[c]_n)$ $\forall [a]_n,[b]_n,[c]_n\in\mathbb{Z}_n$

iii) $[a]_n+[0]_n=[0]_n+[a]_n=[a]_n$ $\forall [a]_n\in\mathbb{Z}$ & $[0]_n$

iv) $[a]_n+[-a]_n=[0]_n$ $\forall [a]_n\in\mathbb{Z}_n$ b/c $[-a]_n\in\mathbb{Z}_n$

v) $[a]_n+[b]_n=[b]_n+[a]_n$ $\forall [a]_n,[b]_n\in\mathbb{Z}_n$

Example:

Let $n\in\mathbb{N}$.

Let $\mathbb{Z}_n^* = \{[k]_n\in\mathbb{Z}_n \mid k,n \text{ coprime}\}$ is a finite abelian group. That is throw out all elements that share a factor w/ n.

i) Closure: If a,n coprime & b,n coprime, then ab,n coprimes. We won't prove now.

ii) Associative: Falls from mult.

iii) 1 coprime w/ everything & 1 is identity

iv) a,n coprime $\Leftrightarrow 1=as+nt \Leftrightarrow [1]_n=[as+nt]_n=[a]_n[s]_n+[nt]_n$

Thus $\exists [s]_n\in\mathbb{Z}_n$. s,n coprime w/ n b/c o/w $[a]_n$ not coprime.

Example:
Let S be a nonempty set. $A(S)$ (set of bijections on S) is a group under composition $\circ$.

Examples:
Let $n \in \mathbb{N}$. Let S_n denote bijections from $\{1, \dots, n\}$ onto itself. By the above S_n is a group under composition.

If $n=1$, $S_1 = \{i\}$ is an abelian group b/c $i \circ i = i \circ i$.

If $n=2$, $S_2 = \{i, f\}$ is an abelian group. $i^{-1}=i$. $f^{-1}=f$
$i \circ i = i = i \circ i$
$f \circ i = f = i \circ f$
$f \circ f = i = f \circ f$

If $n \geq 3$, then S_n is non-abelian, as done in HW.

Def:
Let G_1 & G_2 be groups under $*_1$ & $*_2$ resp.
Let $G = G_1 \times G_2$. Define $*$ as
$(a, b) * (c, d) = (a *_1 c, b *_2 d)$.

We call $*$ the direct product.

G is a group under $*$ & abelian iff both G_1 & G_2 are & finite likewise.

Pf:
i) Closure: Trivial by def

ii) Associative: Trivial by def

iii) Identity: $e = (e_1, e_2)$

iv) Inverse: $(a, b)^{-1} = (a^{-1}, b^{-1})$

Def:
Let G be a group under $*$.
Let $n \in \mathbb{Z}$ $n \geq 0$ & $a \in G$.

We define the power of a as
$a^0 = e$ where e is the identity
$a^{n+1} = a * a^n$

We often elide the $*$ for brevity (unless the op is standard).

We often write the power as a subscript to avoid ambiguity.

Prop:
i) $a^{-n} = (a^n)^{-1} = (a^{-1})^n$ ← Recall we're reversing & inverting the ops (like a stack)

Example:
$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$7[2]_3 = [14]_3 = [2]_3$

$\to [2]_3 = [-14]_3 = [1]_3$ OR $-7[2]_3 = -(7[2]_3) = -([2]_3) = [-2]_3 = [1]_3$

Thm:
Let G be a group (under $*$) & $a, b \in G$.
All the following hold

proof here:
i) The identity e of G is unique.
ii) The inverse of a is unique
iii) $(a^{-1})^{-1} = a$
iv) $(a*b)^{-1} = b^{-1} * a^{-1}$

homework:
v) $\forall u, v \in G$
$a * u = a * v \Rightarrow u = v$
$u * a = v * a \Rightarrow u = v$
vi) $e^n = e \quad \forall n \in \mathbb{Z}$

tough:
vii) Let $m, n \in \mathbb{Z}$.
$a^m a^n = a^{m+n}$
$(a^m)^n = a^{mn}$

pf:

i) Let $e, e' \in G$ be identities of G.
By the properties of identities
$e = e' * e = e * e' = e'$
$\therefore e = e'$ □

ii) Let $a \in G$. Let $u, v \in G$ be inverses of a.
By the properties of inverses (& the identity)
$(u*a)*v = e*v = v$
$u*(a*v) = u*e = u$
Since $*$ is associative by def so
$(u*a)*v = u*(a*v)$
$\therefore v = u$ □

iii) Let $a \in G$. By def $a * a^{-1} = a^{-1} * a = e$, where a^{-1} is the inverse of a.
Here, using the definition of inverse, a is the inverse of a^{-1}.
$\therefore (a^{-1})^{-1} = a$ □

iv) Let $a, b \in G$. We show $(a*b) * (b^{-1} * a^{-1})$
$(a*b) * (b^{-1} * a^{-1})$
$= (a * (b * b^{-1})) * a^{-1}$ associative property
$= (a * e) * a^{-1}$
$= a * a^{-1}$
$= e$
Now we do the other direction b/c we don't know commutativity
$(b^{-1} * a^{-1}) * (a*b) = (b^{-1} * (a^{-1} * a)) * b = (b^{-1} * e) * b = b^{-1} * b = e$.
$\therefore (a*b)^{-1} = b^{-1} * a^{-1}$

Thm:
Let G be an abelian group.
$(a*b)^n = a^n * b^n \quad \forall a, b \in G. \ \forall n \in \mathbb{Z}.$

This is b/c commutativity
$(a*b)^n = \underbrace{(a*b)\cdots(a*b)}_{n} = \underbrace{(a*\cdots*a)}_{n} * \underbrace{(b*\cdots*b)}_{n} = a^n * b^n$

Subgroups

Def:
A subgroup S of group G under $*$ is a subset $S \subseteq G$ where S itself is a group under $*$.

Example:
Consider the abelian group $\mathbb{Z}_{10}$ under $+$. Let $A = \{[0]_{10}, [5]_{10}\}$ & $B = \{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$.

$A+B = \{a+b \mid a \in A \ \& \ b \in B\} = \{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}, [7]_{10}, [9]_{10}, [1]_{10}, [3]_{10}\}$

Example:
Consider group $\mathbb{R}$ under $+$.

$\mathbb{Z}$ is a subgroup of $\mathbb{R}$ under $+$.
$\mathbb{Q}$ is a subgroup of $\mathbb{R}$ under $+$.
$\{0\}$ is a subgroup.
$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ where $n \in \mathbb{N}$ is a subgroup.
$\mathbb{Z}_{10}$ is not a subgroup b/c its elements are equivalence classes.
$G = \{x \text{ is irrational or } 0\}$ is not a subgroup b/c $\sqrt{2} + (1-\sqrt{2}) = 1 \notin G$

Rem:
Suppose G is a group w/ non-empty subset $H \subseteq G$.

The associative law must hold for $a, b, c \in H$, that is
$(ab)c = a(bc)$
↑ we ellide the operation $*$

Rem:
Suppose H is a subgroup of G. Let $e \in G$ be the identity of G & $e' \in H$ be the identity of H. Then $e' = e$.

That is $\forall h \in H \ e'*h = h*e' = h$.

Since $e' \in G$ & e identity of G, $e*e' = e'$
Likewise $e'*e' = e'$, so
$e*e' = e'*e'$
We "multiply" by $(e')^{-1}$ on the right
$e*e'*(e')^{-1} = e'*e'*(e')^{-1}$
$\therefore e = e'$.

Thm:
Let G be a group & H be a subset of G.
H is a subgroup of H iff
i) $\forall h_1, h_2 \in H \quad h_1 h_2 \in H$ ← *elided
ii) $e \in H$ where e identity of G ← Can replace w/ $H \neq \emptyset$ b/c $hh^{-1} = e \in H$ (i) & (iii) def of identity
iii) $\forall h \in H \quad h^{-1} \in H$

Basically, we get associativity for free!

Remark:
Let G be a group. The subset $\{e\} \subseteq G$ where e identity is a subgroup. It is one of the trivial subgroups.

We prove all properties
i) $ee = e \in \{e\}$ $\forall$ elem $\in \{e\}$
ii) $e \in \{e\}$
iii) $e^{-1} = e \in \{e\}$

Thus $\{e\} \subseteq G$ is a subgroup of G.

Likewise $G \subseteq G$ is a subgroup of G.

We call $\{e\}$ & G the trivial subgroups of G.

Note: H is a ~~proper~~ subgroup of G iff H is a subgroup & $H \neq G$
↕
Hernstein calls these improper

Example:
Let $n \in \mathbb{Z}$. The set
$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} = H$$
is a subgroup of $\mathbb{Z}$ under $+$
3
We show the properties hold.

Let $h_1, h_2 \in H = n\mathbb{Z}$. We show $h_1 + h_2 \in H$.
Since $h_1, h_2 \in H$,
$h_1 = nz_1$ & $h_2 = nz_2$ for some $z_1, z_2 \in \mathbb{Z}$.
So
$$h_1 + h_2 = nz_1 + nz_2 = n(z_1 + z_2)$$
Since $z_1 + z_2 \in \mathbb{Z}$, $h_1 + h_2 \in H$, so (i) holds.

We show $0 \in H$ is the identity. Let $h \in H$ where $h = nz$
$$h + 0 = nz + 0 = nz \in H$$
So (ii) holds.

Let $h \in H$ where $h = n\mathbb{Z}$. We show $h^{-1} = -n\mathbb{Z} \in H$.

$h + h^{-1} = n\mathbb{Z} - n\mathbb{Z} = 0$

$h^{-1} = -n\mathbb{Z} = n(-\mathbb{Z}) \in H$ b/c $-\mathbb{Z} \in \mathbb{Z}$

Thus $h^{-1} = -n\mathbb{Z} \in H$, so (iii) holds.

Thus $H = n\mathbb{Z}$ is a subgroup.

Example:

Let $G = S_3$ be a group under composition.

Let $H = \{i, f\} \subseteq G$ where i is the identity & f is defined by

$f(1) = 1$

$f(2) = 3$

$f(3) = 2$

Is $H \subseteq G$ a subgroup?

It is & we prove it now.

First, (ii) trivially holds b/c $i \in H$.

To prove (i), we enumerate all possible compositions

$i \circ i = i \in H$ $\quad f \circ i = f \in H$

$i \circ f = f \in H$ $\quad f \circ f = i \in H$

$f(f(1)) = f(1) = 1$

$f(f(2)) = f(3) = 2$

$f(f(3)) = f(2) = 3$

Now, to show (iii) we find a^{-1} $\forall a \in H$.

$i^{-1} = i$ b/c $i \circ i = i$ (above)

$f^{-1} = f$ b/c $f \circ f = i$ (above)

Thus $H = \{i, f\}$ is a subgroup of $G = S_3$.

Example:

Let $G = S_3$ be a group under $\circ$.

Let $H = \{i, f\} \leq G$ where i identity & f

$f(1) = 2$

$f(2) = 3$

$f(3) = 1$

H is not a subgroup b/c $f \circ f \notin H$ b/c

$(f \circ f)(1) = 3$

$(f \circ f)(2) = 1$

$(f \circ f)(3) = 2$

Example:

Let $G = GL_{2\times 2}(\mathbb{R})$ be a group under multiplication where $GL_{2\times 2}(\mathbb{R}) = \{A \in \mathbb{R}^{2\times 2} \mid \det(A) \neq 0\}$ (general linear group)

Consider the subset $H = SL_{2\times 2}(\mathbb{R})$ where

$SL_{2\times 2}(\mathbb{R}) = \{A \in G \mid \det(A) = 1\}$. ← special linear group

We show $SL_{2\times 2}(\mathbb{R})$ subgroup of $GL_{2\times 2}(\mathbb{R})$.

i) $AB \in SL_{2\times 2}(\mathbb{R})$ b/c $\det(AB) = \det(A)\det(B) = 1$ iff $A, B \in SL_{2\times 2}(\mathbb{R})$

ii) $I \in SL_{2\times 2}(\mathbb{R})$ b/c $\det(I) = 1$

iii) $A^{-1} \in SL_{2\times 2}(\mathbb{R})$ b/c $\det(A) \neq 0 \Rightarrow A^{-1}$ exists & $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1$.

Def:

Let G be a group. Define the center of G $Z(G)$ by
$Z(G) = \{g \in G \mid gb = bg \ \forall b \in G\}$.
$Z(G)$ is a subgroup of G.

Intuitively, $Z(G)$ is the set of all elements of G that commute.

By definition, $Z(G) \subseteq G$. We now show the subgroup properties hold.

$eb = b = be \ \forall b \in G$. (ii)

Let $g_1, g_2 \in Z(G)$. Let $b \in G$.
We show $(g_1 g_2) \in Z(G)$.

$$\begin{aligned}(g_1 g_2)(b) &= g_1(g_2 b) \\ &= (g_2 b) g_1 \\ &= g_2(b g_1) \\ &= (b g_1) g_2 \\ &= b(g_1 g_2) \quad \text{(i)}\end{aligned}$$

Let $g \in Z(G)$. Let $b \in G$. We show $g^{-1} \in Z(G)$
$gb = bg$ b/c $g \in Z(G)$.
Thus
$$\begin{aligned} g^{-1}(gb)g^{-1} &= g^{-1}(bg)g^{-1} \\ \Rightarrow bg^{-1} &= g^{-1}b \quad \text{(iii)}\end{aligned}$$
So $g^{-1} \in Z(G)$ when $g \in Z(G)$. (iii)

Thus $Z(G)$ subgroup of G. ∎ that is everything commutes

Furthermore, the center $Z(G)$ is an abelian group ↓ & G is an abelian group iff $Z(G) = G$.

Cyclic Subgroups & Groups

Thm:

Let G be a group w/ $a \in G$.
Let $H = \{a^n \mid n \in \mathbb{Z}\}$. H is a subgroup of G.

First, we show $H \subseteq G$. To show this we split a^n into cases
$a^0 = e \in G$
$a^n = a^{n-1}a \in G$ if $a^{-1} \in G$. Since $a^0 \in G$, $a^n \in G \ \forall n \in \mathbb{Z}, n \geq 0$
$a^n = (a^{-1})^n \in G$ by above.

Next we show the 3 subgroup properties.

Let $a^m, a^n \in H$ w/ $m, n \in \mathbb{Z}$. We show $a^m a^n \in H$.

$a^m a^n = a^{m+n} \in H$

b/c $m+n \in \mathbb{Z}$ since $m, n \in \mathbb{Z}$. (i)

By def $a^0 = e \in H$. (ii)

Let $a^n \in H$ w/ $n \in \mathbb{Z}$. We show $(a^n)^{-1} \in H$.

$(a^n)^{-1} = a^{-n} \in \mathbb{Z}$

b/c $-n \in \mathbb{Z}$ since $n \in \mathbb{Z}$. (iii)

Thus H is a subgroup of G.

Here, H is called the cyclic subgroup of G generated by a

Def:

Let G be a group w/ $a \in G$.

The <u>cyclic subgroup of G generated by a</u> $\langle a \rangle$ is

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ We call <u>a the generator of G.</u>

This is proved above.

Why is this called cyclic? B/c eventually you roll around & get $e \in G$.

Example:

Let $G = S_3$ be a group under $\circ$. Let $f \in G$ be

$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1$

Let's look at f^k for some k's

$f^0 = i$

$f^{-1} = f^2$ b/c $f^2 \circ f = f^3 = i$

$f^2 = 1 \to 3, \ 2 \to 1, \ 3 \to 2$

$f^3 = 1 \to 1, \ 2 \to 2, \ 3 \to 3 = i$

$f^4 = f^3 \circ f = f$

$f^5 = f^3 \circ f^2 = f^2$

This looks a lot like congruence mod 3!

note: this doesn't have to be 3 for S_3.

We show $\langle f \rangle = \{i, f, f^2\}$.

Let $f^n \in \langle f \rangle$. We know there exists $q, r \in \mathbb{Z}$ s.t.

$n = 3q + r$ where $0 \le r < 3$

So:

$f^n = f^{3q} \circ f^r = (f^3)^q \circ f^r = f^r \in \{f^0, f^1, f^2\} = \{i, f, f^2\}$

Thus $\{i, f, f^2\} \leq (f)$ (by def of (f)) & $(f) \leq \{i, f, f^2\}$ (by above), so

$(f) = \{i, f, f^2\}$

Example:

Let $G = \mathbb{Z}_{10}$ be a group under $+$. Let $H = ([2]_{10})$. Find H.

look like arithmetic powers

Since superscripts $([2]_{10})^3$ are confusing in this case, we write $3 \cdot [2]_{10}$.

$0 \cdot [2]_{10} = [0]_{10} = e$ $\quad 1 \cdot [2]_{10} = [2]_{10}$ $\quad 2 \cdot [2]_{10} = [4]_{10}$

$3 \cdot [2]_{10} = [6]_{10}$ $\quad 4 \cdot [2]_{10} = [8]_{10}$ $\quad 5 \cdot [2]_{10} = [10]_{10} = [0]_{10} = e$

$6 \cdot [2]_{10} = 5 \cdot [2]_{10} + 1 \cdot [2]_{10} = [2]_{10}$

We conjectecture $H = \{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$.

This is true, but to show it we would do double set inclusion & the division algorithm (by 5). Like we did earlier

Why 5? $|H| = 5 \Leftrightarrow 5 \cdot [2]_{10} = [0]_{10} = e$

$0 \cdot [1]_n = [0]_n$
$1 \cdot [1]_n = [1]_n$
$2 \cdot [1]_n = [2]_n$
$10 \cdot [1]_n = [0]_n$

Example:

Let $G = \mathbb{Z}_{10}$ again be a group under $+$.
$H = ([1]_{10}) = \mathbb{Z}_{10}$, which is shown similar to the above.

In fact $\mathbb{Z}_n = ([k]_n)$ where k, n coprime (i.e. $\gcd(k, n) = 1$).

Def:

A group G is called cyclic if $\exists a \in G$ s.t. $\langle a \rangle = G$.
Here a is called a generator of G.

As you can see $\mathbb{Z}_{10}$ is a cyclic group generated by $[1]_{10}$ b/c $([1]_{10}) = \mathbb{Z}$. (Likewise for the numbers coprime to 10: 1, 3, 7, 9)

Example:

$\mathbb{Z}$ is a cyclic group under $+$.

1 & -1 are generators for G b/c $(1) = (-1) = \mathbb{Z}$.

Example:
Let $n \in \mathbb{N}$. $\mathbb{Z}_n$ is a cyclic group under $+$ generated by $[1]_n$.

Further $[a]_n$ generates $\mathbb{Z}_n$ where a, n coprime & in fact these are all the generators of $\mathbb{Z}_n$. (I think & sketched a proof)

Thm:
Let G be a group & $a \in G$.

i) The cyclic subgroup $\langle a \rangle \leq G$ generated by a is abelian

ii) If G is a cyclic group, then G is abelian. ← The converse is not true

PF:
i) Let $H = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$. Let $h_1, h_2 \in H$, where $h_1 = a^b$ & $h_2 = a^c$ for some $b, c \in \mathbb{Z}$. Then $h_1 h_2 = a^b a^c = a^{b+c} = a^{c+b} = a^c a^b = h_2 h_1$

Thus $\langle a \rangle \leq G$ is abelian.

ii) Since G is cyclic $\exists a \in G$ s.t. $\langle a \rangle = G$. Since $\langle a \rangle \leq G$ is a cyclic subgroup it is abelian. Thus $G = \langle a \rangle$ is abelian.

We often use the contrapositive to show a group is not cyclic

Lagrange's Theorem

Let's talk about equivalence classes in terms of groups.

Recall:
Let S be a non-empty set w/ relation $\sim$. $\sim$ is an equivalence relation if it is reflexive, transitive, & symmetric.

Let $a \in S$. The equivalence class of a $[a]$ is $[a] = \{ b \in S \mid a \sim b \}$.

Further, these equivalence classes partition S. That is
i) $\bigcup_{a \in S} [a] = S$

ii) $\forall a, b \in S$ $[a] \cap [b] = \emptyset$ or $[a] = [b]$

iii) $\forall a, b \in S$ $[a] = [b] \iff a \sim b$

Now we'll apply this to groups

Let $H \leq G$ be a subgroup of G. We'll define $\sim$ on G as $a \sim b \iff ab^{-1} \in H$. $\forall a, b \in G$

$\sim$ is reflexive b/c $aa^{-1} = e \in H$ b/c H is a subgroup which necessarily has the identity.

$\sim$ is symmetric b/c $a \sim b \iff b \sim a$. We show this by showing $ab^{-1} \in H \iff ba^{-1} \in H$.
Suppose $a \sim b$ where $a, b \in G$. Then $ab^{-1} \in H$. By the inverse property $(ab^{-1})^{-1} = ba^{-1} \in H$, so $\sim$ is symmetric.

Finally, $\sim$ is transitive.
Let $a, b, c \in G$ where $a \sim b$ & $b \sim c$. We show $a \sim c$.
$a \sim b \Rightarrow ab^{-1} \in H$ & $b \sim c \Rightarrow bc^{-1} \in H$
Since H is a subgroup (i.e. closed)
$(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = ac^{-1} \in H$
Thus $a \sim c$ & $\sim$ is transitive.

Thus $\sim$ is an equivalence relation on G.

Let's write the equivalence classes.

$$\begin{aligned}[a] &= \{ b \in G \mid b \sim a \} \\ &= \{ b \in G \mid ba^{-1} \in H \} \\ &= \{ b \in G \mid \exists h \in H \text{ s.t. } ba^{-1} = h \} \\ &= \{ b \in G \mid \exists h \in H \text{ s.t. } b = ah \} \\ &= \{ ha \mid h \in H \} \\ &= Ha\end{aligned}$$

Note: $He = \{ he \mid h \in H \} = H$

Def:
Let $H \leq G$ be a subgroup of group G. Let $a \in G$.
The set Ha is called the right coset of H in G determined by a.

$$Ha = \{ ha \mid h \in H \} = [a]$$ under earlier $a \sim b \Leftrightarrow ab^{-1} \in H$ equivalence relation.

Def:
Let $H \leq G$ be a subgroup of group G.
The number of distinct cosets of H in G is called the index of H in G. We denote this by

$$i_G(H) = [G : H]$$

Prop: (Right) Cosets
i) $G = \bigcup_{a \in G} Ha$

ii) $\forall a, b \in G$ $Ha = Hb$ or $Ha \cap Hb = \emptyset$

iii) $\forall a, b \in G$ $Ha = Hb$ iff $ba^{-1} \in H \Leftrightarrow ab^{-1} \in H$

iv) $\forall a \in G$ $Ha = He \Leftrightarrow ae^{-1} = a \in H$

v) $\forall a \in G$ $|Ha| = |H|$

vi) $|G| = |H| \cdot i_G(H)$ index of H or # distinct cosets from i, ii, & v

Lagrange's Theorem! More on that later

Suppose $a \in H$. Define $f: H \to Ha$ by $f(h) = ha$ $\forall h \in H$.

We show f is surjective & injective.

To show f injective, let $h_1, h_2 \in H$ where $f(h_1) = f(h_2)$. We show $h_1 = h_2$

$h_1 a = h_2 a$ b/c $f(a_1) = f(a_2)$

$\Rightarrow (h_1 a)a^{-1} = (h_2 a)a^{-1}$

$\Rightarrow h_1(aa^{-1}) = h_2(aa^{-1})$

$\Rightarrow h_1 = h_2$ □

f is trivially surjective b/c

$Ha = \{ha \mid h \in H\}$

$Rng(f) = \{f(h) = ha \mid h \in H\}$

Since $Ha = Rng(f)$, f is surjective.

Thm: Lagrange's Theorem

Let G be a finite group w/ subgroup H

i) $|G| = |H|\,[G:H] = |H|\,id_G(H)$

ii) The order of H divides the order of G.

Example:

Let S_3 be the group under composition $\circ$.

Let $f \in S_3$ where $f(1) = 2$, $f(2) = 1$, $f(3) = 3$.

Let $H = \langle f \rangle$ be the cyclic subgroup of S_3 generated by H.

$f^0 = i$, $f^1 = f$, $f^2 = i$.

$\Rightarrow H = \{i, f\}$.

We find the index of H in S_3 $[S_3 : H]$ using Lagrange's theorem.

$|G| = |H|\,[G:H]$

$3! = 2\,[G:H]$

$6 = 2\,[G:H]$

$[G:H] = 3$

Thus there are 3 distinct right cosets

$Hi = H = \{i, f\}$ Note: $Hf = H = \{i \circ f = f,\ f \circ f = i\}$

Let $g \in S_3$ where $g(1) = 1$, $g(2) = 3$, $g(3) = 2$.

$Hg = \{g, f \circ g\}$ $f \circ g: 1 \to 2,\ 2 \to 3,\ 3 \to 1$

Note: $H(f \cdot g) = Hg$

Let $v \in S_3$ where $v = g \circ f$ $v(1) = 3$, $v(2) = 1$, $v(3) = 2$

$Hv = \{v, f \circ v\}$ $f \circ v: 1 \to 3,\ 2 \to 2,\ 3 \to 1$

Cor: Lagrange's
Suppose G is a finite group of order p where p is a prime. The G is cyclic. ← & thus abelian.

Pf:
Let $a \in G$ st $a \neq e$. This exists b/c $|G| = p > 1$.
Let $H = \langle a \rangle$ be a cyclic subgroup.
By Lagrange's theorem $|H$ divides $|G| = p$.
Since p is prime $|H| = 1$ or p.
Since $a \in H \neq e$, $|H| > 1$.
Thus $|H| = |G| = p$.
Since $H \leq G$ & $|H| = |G|$, $H = G$.
Thus G is cyclic. □

Remarks:
i) Our initial $\sim$ was $a \sim b \Leftrightarrow ab^{-1} \in H$. ← inverse property

We could define it $a \sim b \Rightarrow a^{-1}b \in H$ (b/c $(ab^{-1})^{-1} = a^{-1}b \in H$).

ii) Under this new definition of $\sim$, we get the equivalence class for each $a \in G$ is aH.

We call aH the <u>left coset</u> of H in G determined by a.

iii) For <u>finite groups</u>, the number of distinct right cosets is equal to the number of distinct left cosets.

Note: We don't know every left coset is a right coset.

Def:
Let G be a group w/ $a \in G$.
The <u>order of a</u> $o(a)$ is the number of elements in the cyclic subgroup generated by a. That is
$$\therefore o(a) = |\langle a \rangle|$$

a is of finite order if $o(a)$ is finite.

Cor:
Let G be a group w/ $a \in G$.
$$o(a) = 1 \Leftrightarrow a = e$$

Proof next page.

Pf:

$o(a)=1 \Rightarrow a=e$

Suppose $o(a)=1$ & $a \neq e$.

$e=a^0 \in \langle a \rangle$ & $a=a^1 \in \langle a \rangle$. Since $a \neq e$, $\langle a \rangle$ has at least 2 distinct elements.

Thus $o(a) \neq 1$. Thus $a=e$ must be true. □

$a=e \Rightarrow o(a)=1$

$e^n=e \ \forall n \in \mathbb{Z}$ (shown in homework).

Thus $\langle a \rangle = \langle e \rangle = \{e^n \mid n \in \mathbb{Z}\} = \{e\}$.

Thus $o(e)=o(a)=1$. □

Example:

Let $G=S_3$ be a group under $\circ$. How do we show that there is no $f \in G$ s.t. $o(f)=6$.

If $o(f)=6$, then $\langle f \rangle = G$ b/c $|G|=|S_3|=3!=6$. Thus $G=S_3$ is cyclic.

If G is cyclic then $G=S_3$ is abelian. We have shown on HW that $G=S_3$ under $\circ$ is non-abelian. Thus there is no such f. □

Example:

Let $G=S_3$ be a group under $\circ$,

Let $f \in S_3$ be $f: 1 \to 1,\ 2 \to 3,\ 3 \to 2$

By Lagrange's theorem, $o(f)=|\langle f \rangle|$ divides $|S_3|$ (since $\langle f \rangle \leq S_3$ as $f \in S_3$.

Since S_3 isn't cyclic (non-abelian) $o(f) \neq 6$. ← helpful in some cases, not here

Since $f \neq e$, $o(f) \neq 1$.

Thus $o(f)=2$ or $o(f)=3$.

Let's find $\langle f \rangle$ directly.

$f^0 = i$ $\quad f^1 = f$ $\quad f^2: \begin{matrix} 1 \to 1 = i \\ 2 \to 2 \\ 3 \to 3 \end{matrix}$

Let $n \in \mathbb{Z}$ & $f^n \in \langle f \rangle$. By division algorithm $n = 2q+r$ for some $q, r \in \mathbb{Z}$ $0 \leq r < |2| = 2$.

Thus

$$f^n = f^{2q+r} = (f^2)^q f^r = i^q f^r = f^r \in \{f^0, f^1\} = \{i, f\}.$$

Thus $\langle f \rangle = \{i, f\}$ & $o(f)=2$.

Thm:

Let G be a group w/ $a \in G$ of finite order. Thus $\langle a \rangle$ is finite.

Let $o(a)=m$. thus $\langle a \rangle$ has m elements. Then $\langle a \rangle = \{a^0, \dots, a^{m-1}\}$.

Pf:

Consider $\underbrace{a^0, \dots, a^m}_{m+1 \text{ elem}} \in \underbrace{\langle a \rangle}_{m \text{ elem}}$. By the pigeonhole principle $a^u = a^v$ for some $u \neq v$ $0 \leq u \leq m$ & $0 \leq v \leq m$. Rewrite u & v s.t. $u<v$ for simplicity.

Since $a^u = a^v$, $a^{-u} a^u = a^{-u} a^v \Rightarrow e = a^{v-u}$ where $v-u > 0$ (since $u<v$).

Additionally $v-u \in \mathbb{N}$ so $0 < v-u \leq m$.

Let k be the smallest positive integer s.t. $a^k = e$. We show k exists.

Let $S = \{n \in \mathbb{N} \mid a^n = e\}$. Since $v-u > 0$ & $a^{v-u} = e$ so $S \neq \emptyset$ & k exists.

Thus $\{a^0, \dots, a^{k-1}\} \subseteq \langle a \rangle$. Let's show $a^0, \dots, a^{k-1}$ are distinct.

Suppose for contradiction that $a^0, \dots, a^{k-1}$ contains some duplicate.

That is $\exists s,t \in \mathbb{Z}$ $0 \le s \le k-1$ $0 \le t \le k-1$ $s \neq t$ where $a^s = a^t$.
We rewrite s & t st $s<t$ for simplicity.

$e = a^0 = a^{-s}a^s = a^{-s}a^t = a^{t-s}$ where $t-s \le t < k$. We assume k was the smallest positive integer st $a^k = e$. However $a^{t-s} = e$ & $t-s$. This is a contradiction.

Thus $a^0, \dots, a^{k-1}$ are distinct.

We now show $\langle a \rangle \subseteq \{a^0, \dots, a^{k-1}\}$.
Let $n \in \mathbb{Z}$ & $a^n \in \langle a \rangle$. By the division algorithm $n = qk + r$ where $q, r \in \mathbb{Z}$ $0 \le r < k$.

$$a^n = a^{qk+r} = (a^k)^q a^r = e^q a^r = a^r \in \{a^0, \dots, a^{k-1}\}.$$

Since $\{a^0, \dots, a^{k-1}\} \subseteq \langle a \rangle$ & $\langle a \rangle \subseteq \{a^0, \dots, a^{k-1}\}$, $\langle a \rangle = \{a^0, \dots, a^{k-1}\}$.
Since $o(a) = m$ (i.e. $\langle a \rangle$ has m distinct elements) & $\{a^0, \dots, a^{k-1}\}$ is k distinct elements, $k = m$.

Therefore
$\langle a \rangle = \{a^0, \dots, a^{m-1}\}$. □

Coro:
Let G be a group w/ $a \in G$. Then
i) a is of finite order iff $\exists k \in \mathbb{N}$ st $a^k = e$
ii) If a is of finite order, then the order of a $o(a)$ is the smallest positive integer m st $a^m = e$.

PF:
i) Suppose $a \in G$ where $a^k = e$. What is the order of a?
We now $o(a) \le k$ by our some logic in the proof above. We say less than or equal to b/c we might have some multiple of the smallest possible k.

ii) Again, if you look at the above proof we directly showed this (if you rename m to k).

Coro:
Let G be a finite group of order n. Let $a \in G$ be an element of G w/ $m = o(a)$.

By Lagrange's theorem, we get
$|G| = |\langle a \rangle| [G : \langle a \rangle] \Rightarrow o(a)[G : \langle a \rangle] \Rightarrow n = m[G : \langle a \rangle]$
That is m divides n.

Example:

Consider group S_4 under $\circ$. The order of S_4 is $|S_4| = 4! = 24$.
If $f \in S_4$ then the order of f is
$o(f) \in \{1, 2, 3, 4, 6, 8, 12, 24\}$ ← factors of 24

What are the elements of order 1? Only the identity $i \in S_4$.

What are the elements of order 24? There are none b/c S_4 is non-abelian. If $\exists f \in S_4$ st $o(f) = 24$ then $\langle f \rangle = S_4$, meaning S_4 would be cyclic & thus abelian.

Let $f \in S_4$ be defined as $f: 1 \to 2, 2 \to 3, 3 \to 4, 4 \to 1$ (rotate 1 left/up).
What is the order of f?

$f^0 = i$

$f^1 = f$

f^2: $1 \to 3, 2 \to 4, 3 \to 1, 4 \to 2$

f^3: $1 \to 4, 2 \to 1, 3 \to 2, 4 \to 3$

f^4: $1 \to 1, 2 \to 2, 3 \to 3, 4 \to 4 = i$

Since 4 is the smallest positive integer m st $f^m = i$, we know
$o(f) = 4$ & $\langle f \rangle = \{f^0, f^1, f^2, f^3\}$.

Example:

Consider group $\mathbb{Z}_{10}$ under $+$. The order of $\mathbb{Z}_{10}$ is $|\mathbb{Z}_{10}| = 10$.

Consider $[3]_{10}$. Find the order of $[3]_{10}$. We know $o([3]_{10}) \in \{1, 2, 5, 10\}$.

To find the order of $[3]_{10}$, we go over the possibilities of $o([3]_{10})$ m & pick the smallest m such that $m \cdot [3]_{10} = [0]_{10} = e$.

$1 \cdot [3]_{10} = [3]_{10} \neq [0]_{10}$

$2 \cdot [3]_{10} = [6]_{10} \neq [0]_{10}$

$5 \cdot [3]_{10} = [15]_{10} = [5]_{10} \neq [0]_{10}$

$10 \cdot [3]_{10} = [30]_{10} = [0]_{10}$

$m = 10$ is the smallest m st $m \cdot [3]_{10} = [0]_{10}$. Therefore the order of $[3]_{10}$ is $o([3]_{10}) = 10$.

Thm:
Let G be a finite group of order n. Let $a \in G$. Then we know $a^n = e$

pf:
Let m denote the order of a, which is finite b/c G is finite.

We know m divides n, that is $n = mc$ for some $c \in \mathbb{Z}$. Therefore
$a^n = a^{mc} = (a^m)^c = e^c = e$

Essentially all possible orders of a converge at n since $o(a) \in \{$factors of $n\}$.

Let's actually generalize the above theorem to apply to any integer k.

Thm:
Let G be a group where $|G| = n$ w/ $a \in G$ where $o(a) = m$. For all $k \in \mathbb{Z}$
$a^k = e \iff m$ divides k

Pf:

i) m divides $k \Rightarrow a^k = e$

Suppose m divides k. Then by the definition of divides, $k = mc$ for some $c \in \mathbb{Z}$. Then

$$a^k = a^{mc} = (a^m)^c = e^c = e. \quad \square$$

↑ Recall m is smallest positive integer st $a^m = e$

ii) $a^k = e \Rightarrow m$ divides k

Suppose $a^k = e$. By the division algorithm $\exists q, r \in \mathbb{Z}$ where $0 \le r < m$ st $k = qm + r$. Using this breakdown of k we have

$$a^k = a^{qm+r} = (a^m)^q a^r = e^q a^r = a^r$$

& $a^k = e$

$\Rightarrow a^r = e$

Since $0 \le r < m$ & a^m is the smallest positive integer st $a^m = e$. Since $r < m$, we have $r \le 0$. Thus $r = 0$.

Therefore $k = qm$ for some $q \in \mathbb{Z}$. Thus m divides k. $\square$

Recall:

For set $\mathbb{Z}_n$, an element $[a]_n \in \mathbb{Z}_n$ has a multiplicative inverse only when a & n are coprime (i.e. $\gcd(a, n) = 1$).

Suppose $\gcd(a, n) = 1$. Then $\exists s, t \in \mathbb{Z}$ st $as + nt = 1$. Thus

$$[as + nt]_n = [1]_n$$
$$[as]_n + [nt]_n = [1]_n$$
$$[a]_n[s]_n + [n]_n[t]_n = [1]_n$$
$$[a]_n[s]_n + [0]_n[t]_n = [1]_n$$
$$[a]_n[s]_n = [1]_n$$

Therefore $[a]_n$ has multiplicative inverse $[s]_n$.

Def:

Consider $U_p = \{[a]_p \in \mathbb{Z}_p \mid [a]_p \neq [0]_p\} = \{[1]_p, \ldots, [p-1]_p\}$ where p is a prime. U_p can also be characterized by elements w/ a multiplicative inverse or elements coprime to p.

Thm:

U_p is a group under multiplication.

Pf:

First let's show closure. Let $[a]_p, [b]_p \in U_p$.

Then $[a]_p[b]_p = [ab]_p$.

Since p is prime, we know $\gcd(ab, p) = 1$ or $\gcd(ab, p) = p$.

We want $\gcd(ab, p) = 1$ for U_p to be a group.

Suppose for contradiction that $\gcd(ab, p) = p$.
Then p divides a or b since p is prime. This violates our assumption that $[a]_p, [b]_p \in U_p$. Thus U_p is closed.

The associative property falls from associativity of multiplication.

The identity property holds w/ $[1]_p$ being the identity. $[1]_p \in U_p$ b/c $[1]_p \neq [0]_p$ & & $p \geq 2$ as a prime.

The inverse property holds b/c a, p coprime for all $[a]_p \in U_p$ by definition. By our earlier theorem this implies the existence of a multiplicative inverse for $[a]_p$.

Coro: where p is prime
i) Suppose $a \in \mathbb{Z}$ is relatively prime to p. Then $[a]_p \in U_p$.
Since $|U_p| = p-1$, we have
$([a]_p)^{p-1} = e \Rightarrow [a^{p-1}]_p = e$ (b/c multiplication is our operation.)

ii) By the above corollary, $a^{p-1} \equiv 1 \bmod p \Leftrightarrow a^{p-1} = qp+1$ for some $q \in \mathbb{Z}$

Thm: Fermat's Little Theorem
Let p be a prime & let $a \in \mathbb{Z}$ be relatively prime to p. Thus

$$a^{p-1} \equiv 1 \pmod p$$

Coro:
Let p is a prime & let $a \in \mathbb{Z}$. Then

$$a^p = a \pmod p$$

Group Homomorphisms

Def:
Let G & G' be groups & $\varphi: G \to G'$ be a function.

i) φ is a homomorphism iff $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$

ii) φ is a monomorphism iff φ is a homomorphism & φ is injective.

iii) φ is an isomorphism iff φ is a homomorphism & φ is bijective.

iv) φ is an automorphism iff φ is a isomorphism & $G = G'$

Def:
Let G & G' be groups. We say G & G' are isomorphic iff $\exists$ an isomorphism φ from G to G'.

Example:
Let G be a group w/ $g \in G$. Define $\varphi: G \to G$ by $\varphi(a) = gag^{-1}$

a) Let's show φ is a homomorphism.
$\varphi(a)\varphi(b) = (gag^{-1})(gbg^{-1}) = ga(g^{-1}g)bg^{-1} = g(ab)g^{-1} = \varphi(ab)$
$\therefore \varphi$ is a homomorphism.

b) Let's show φ is a monomorphism. We already know φ is a homomorphism, so we show φ is injective.
Suppose $\varphi(a) = \varphi(b)$. We show $a = b$.

$\varphi(a) = \varphi(b)$
$\Rightarrow gag^{-1} = gbg^{-1}$
$\Rightarrow g^{-1}(gag^{-1})g = g^{-1}(gbg^{-1})g$
$\Rightarrow (g^{-1}g)a(g^{-1}g) = (g^{-1}g)b(g^{-1}g)$
$\Rightarrow a = b$

$\therefore$ g is a monomorphism

c) Let's show φ is a isomorphism. We know φ is a monomorphism (i.e. homomorphic & bijective) so we must show it's surjective.

Let $y \in G$. We find $a \in G$ s.t. $\varphi(a) = y$.
Let $a = g^{-1}yg$. We know $a = g^{-1}yg \in G$ b/c $g \in G$, $g^{-1} \in G$, $y \in G$, & G is closed under product. We now show $\varphi(a) = y$.
$\varphi(a) = gag^{-1} = g(g^{-1}yg)g^{-1} = (gg^{-1})y(gg^{-1}) = y$
$\therefore$ g is an isomorphism.

d) Since φ is an isomorphism & since $\text{Dom}(\varphi) = \text{Codom}(\varphi)$ b/c $\varphi: G \to G$, we know φ is an automorphism.

(In particular, an inner automorphism!)

Example:
Let G be the group $\mathbb{Z}$ under $+$.
Let G' be the group $\mathbb{Z}_2$ under $+$.
Define $\varphi: G \to G'$ by $\varphi(a) = [a]_2$.

We show φ is a homomorphism. Let $a, b \in G = \mathbb{Z}$.
$\varphi(a+b) = [a+b]_2 = [a]_2 + [b]_2 = \varphi(a) + \varphi(b)$ ← use $+$ b/c operation is addition

φ is however not a monomorphism b/c it is not one-to-one
$\varphi(0) = [0]_2 = [2]_2 = \varphi(2)$ but $0 \neq 2$.

Example:
Consider group $\mathbb{R}$ under $+$ & group $\mathbb{R}^{2\times 2}$ under $+$.
Define $\varphi: \mathbb{R} \to \mathbb{R}^{2\times 2}$ by
$$\varphi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}.$$

We show φ is a homomorphism. Let $a, b \in \mathbb{R}$
$$\varphi(a+b) = \begin{bmatrix} a+b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \varphi(a) + \varphi(b).$$

If we replace $\mathbb{R}^*$ w/ $GL_{2\times 2}(\mathbb{R})$ under matrix multiplication, we don't get a homomorphism. That is b/c φ becomes not well-defined.
$\varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \notin GL_{2\times 2}(\mathbb{R})$. b/c $\det\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0$

General linear group $\{X \in \mathbb{R}^{2\times 2} \mid \det(X) \neq 0\}$

Example:
Consider group $\mathbb{R}^* = \{a \in \mathbb{R} \mid a \neq 0\}$ & group $GL_{2\times 2}(\mathbb{R})$.
Define $\varphi: \mathbb{R}^* \to GL_{2\times 2}(\mathbb{R})$ by
$\varphi(a) = \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix}$

We show φ is a homomorphism
$\varphi(ab) = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = \varphi(a)\varphi(b)$

Further we actually get a monomorphism.

Thm: Properties of Homomorphisms
Let G_1, G_2, G_3 be groups. Let $\alpha: G_1 \to G_2$ & $\beta: G_2 \to G_3$ be homomorphisms. Let $e_1 \in G_1$ be the identity of G_1 & $e_2 \in G_2$ that of G_2.

i) $\alpha(e_1) = e_2$

ii) $\beta \circ \alpha$ homomorphism

iii) $\beta \circ \alpha$ monomorphism if α, β monomorphisms

iv) $\beta \circ \alpha$ isomorphism if α, β isomorphisms.

Pf:
i) $\alpha(e_1 e_1) = \alpha(e_1)$ b/c $e_1 e_1 = e_1$
$\alpha(e_1 e_1) = \alpha(e_1)\alpha(e_1)$ by α homomorphism
$\alpha(e_1 e_1) = \alpha(e_1)\alpha(e_1) = \alpha(e_1)$
$\Rightarrow \alpha(e_1)\alpha(e_1)\alpha(e_1)^{-1} = \alpha(e_1)\alpha(e_1)^{-1}$
$\Rightarrow \alpha(e_1) = e_2$

ii) Let $a, b \in G_1$. We show $(\beta\circ\alpha)(ab) = ((\beta\circ\alpha)(a))((\beta\circ\alpha)(b))$
$(\beta\circ\alpha)(ab) = \beta(\alpha(ab))$
$= \beta(\alpha(a)\alpha(b))$
$= \beta(\alpha(a))\,\beta(\alpha(b))$
$= ((\beta\circ\alpha)(a))((\beta\circ\alpha)(b))$

Thm:
Let G_1 & G_2 be groups & let α be a homomorphism $G_1 \to G_2$. Then

i) If H is a subgroup of G_1, then $\varphi(H) = \{\varphi(h) \mid h \in H\}$ is a subgroup of H_2.

ii) If α is an isomorphism, then α^{-1} is a isomorphism $G_2 \to G_1$

Pf:
i) On HW !!

ii) We know the inverse of a bijection is a bijection. So let's show α^{-1}

is a homomorphism when α^{-1} is isomorphic.

To do this, we need to show that $\forall c, d \in G_2$
$$\alpha^{-1}(cd) = \alpha^{-1}(c)\alpha^{-1}(d)$$

Let $a, b \in G_1$ st $\alpha^{-1}(c) = a$ & $\alpha^{-1}(d) = b$, that is $c = \alpha(a)$ & $d = \alpha(b)$.
Since α is a homomorphism,
$$\alpha(ab) = \alpha(a)\alpha(b) = cd$$
Therefore
$$\alpha^{-1}(cd) = ab = \alpha^{-1}(c)\alpha^{-1}(d)$$
Therefore α^{-1} is a homomorphism.

Note: We assume that α is isomorphism

Since α^{-1} is a bijection & homomorphism when α isomorphism, we know α^{-1} isomorphism.

Kernel of Isomorphism

Def:
Let φ be a homomorphism $G \to G'$. Let $e \in G$ be the identity of G & $e' \in G'$ the identity of G'.
The kernel of φ $\ker(\varphi)$ is the set
$$\ker(\varphi) = \{ g \in G \mid \varphi(g) = e \}.$$

Example:
Consider $\mathbb{R}^+$ as a group under multiplication & $\mathbb{R}$ as a Group under addition.
Let $\varphi: \mathbb{R}^+ \to \mathbb{R}$ be the function
$$\varphi(a) = \ln(a).$$

We show φ is a homomorphism
$$\therefore \varphi(ab) = \ln(ab) = \ln(a) + \ln(b).$$

Let's find the kernel of φ.
$$\ker(\varphi) = \{ a \in \mathbb{R}^+ \mid \varphi(a) = 0 \}$$
$$\leq \{ a \in \mathbb{R}^+ \mid \ln(a) = 0 \}$$
$$= \{1\}.$$

This actually means that φ is a monomorphism (i.e. one-to-one/injective).

Thm:
Let φ be a homomorphism $G \to G'$. Let e be identity of G & e' of G'. We know

i) $\ker(\varphi)$ is a subgroup of G.

ii) $g\ker(\varphi)g^{-1} \subseteq \ker(\varphi)$ for all $g \in G$.

That is $gng^{-1} \in \ker(\varphi)$ $\forall g \in G$ & $n \in \ker(\varphi)$.

iii) φ is injective/one-to-one/a monomorphism iff $\ker(\varphi) = \{e\}$.

Pf:

i) $\ker(\varphi) = \{g \in G \mid \varphi(g) = e'\}$ is a subset of G by definition. Thus we show identity, closure, & inverses.

We already showed $\varphi(e) = e'$ for all homomorphisms, so $e \in \ker(f)$ & the identity property holds.

Let's show closure. Let $a, b \in \ker(\varphi)$. We show $ab \in \ker(\varphi)$, that is $\varphi(ab) = e'$.

$\varphi(ab) = \varphi(a)\varphi(b)$ (φ homomorphism)
$= e'e'$ ($a, b \in \ker(\varphi)$)
$= e'$

Thus $ab \in \ker(\varphi)$ & closure holds.

Let's show inverse property. Let $a \in \ker(\varphi)$, so $\varphi(a) = e'$.
We want to show $a^{-1} \in \ker(\varphi)$, that is $\varphi(a^{-1}) = e'$.

ii) Let $g \in G$ & $n \in \ker(\varphi)$. Then $\varphi(n) = e' \in G'$ by definition.
We show $\varphi(gng^{-1}) = e'$ to show $gng^{-1} \in \ker(\varphi)$.

$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1})$ (homomorphism)
$= \varphi(g)e'\varphi(g^{-1})$ ($n \in \ker(\varphi)$)
$= \varphi(g)\varphi(g)^{-1}$ ($\varphi(g) = \varphi(g)^{-1}$ ← shown later)
$= e'$

Thus $g(\ker(\varphi))g^{-1} \subseteq \ker(\varphi)$. □

iii) Assume φ is injective. We show $\ker(\varphi) = \{e\}$ by double set inclusion.

We know $e \in \ker(\varphi)$ so $\{e\} \subseteq \ker(\varphi)$.
We know $\varphi(e) = e'$. Let $a \in \ker(\varphi)$. Then we know
$\varphi(a) = e' = \varphi(e)$.
Since φ is injective, this means $a = e$. Thus $\ker(\varphi) \subseteq \{e\}$.

Consequently, $\ker(\varphi) = \{e\}$ given φ is injective.

Now the opposite direction. Suppose $\ker(\varphi) = \{e\}$.
Let $a, b \in G$ s.t. $\varphi(a) = \varphi(b)$.
Then $\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b)^{-1} = e'$ by the inverse property.
We use algebraic manipulation to show $a = b$

$\varphi(a)\varphi(b^{-1}) = e' \Rightarrow \varphi(a)\varphi(b^{-1}) = e'$ (internalize inverse shown below)
$\Rightarrow \varphi(ab^{-1}) = e'$ (def of homomorphism)
$\Rightarrow ab^{-1} = e$ ($\ker(\varphi) = \{e'\}$)

$\Rightarrow a = b$

Thus φ is injective given $\ker(\varphi) = \{e\}$.

Therefore, φ is injective iff $\ker(\varphi) = \{e\}$.

Thm: Cayley's Theorem
Let G be a group. G is isomorphic to a subgroup of $A(G)$.

Recall $A(G) = \{ f : G \to G \mid f \text{ bijective} \}$ is a group under $\circ$.

Let's define a function $\theta : G \to A(G)$ by
$\theta(g) = \varphi_g$ where $\varphi_g : G \to G$ is $\varphi_g(a) = ga$

Let's show that θ is a monomorphism. In HW 7 we showed
$\varphi_a \circ \varphi_b = \varphi_{ab}$.
Thus we show θ is a homomorphism b/c
$\theta(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \theta(a) \circ \theta(b)$.
We also showed in HW that $\varphi_g = i$ if & only if $g = e$.
Thus
$\ker(\theta) = \{ g \in G \mid \theta(g) = \varphi_g = i \} = \{ g \in G \mid g = e \} = \{e\}$.
By our earlier theorems, this means θ is injective.
Thus θ is a monomorphism.

Since $\theta : G \to A(G)$ is a monomorphism, by Cayley's theorem $\theta(G)$ is a subgroup of $A(G)$. Thus there exists an isomorphism b/w G & $A(G)$. ←?

TODO: Is this true?

Normal Subgroups

Def:
Let G be a group w/ subgroup N. N is a <u>normal subgroup</u> iff
$aNa^{-1} \subseteq N \quad \forall a \in G$. ← looks like kernels!

In other words, N is a normal subgroup of G iff
$ana^{-1} \in N \quad \forall a \in G, n \in N$

We denote this by $N \triangleleft G$. ← related to ideals

Thm:
From our earlier theorems (recent), we know $\ker(\varphi)$, where $\varphi : G \to G'$ is a homomorphism, <u>is a normal subgroup</u> of G.

Example:
Let G be a group w/ identity e. Then $\{e\} \trianglelefteq G$.

Let $a \in G$ & $n \in \{e\} \Leftrightarrow n = e$. Then
$ana^{-1} = aea^{-1} = aa^{-1} = e \in \{e\}$.
Thus $\{e\}$ is a normal subgroup of G.

Example:
Suppose G is an abelian group. What are the normal subgroups of G?

All subgroups N are normal groups of G!

Let $a \in G$ & $n \in N$. Then
$ana^{-1} = aa^{-1}n = n \in N$.
Thus N is a normal subgroup of G iff N is a subgroup of G, where G is an abelian group.

Example:
Let G be a group. The G is a normal subgroup of itself.

This is b/c $a \in G$, so $a^{-1} \in G$. Since G is closed under the group operator (closure property), we know
$aga^{-1} \in G \quad \forall a \in G \ \forall g \in G$.

Thm:
Suppose G is a group w/ subgroup N. We know

i) N is a normal subgroup of G iff $aNa^{-1} = N \ \forall a \in G$,

ii) N is a nomal subgroup of G iff $aN = Na \ \forall a \in G$.

Pf:
i) Suppose N is a normal subgroup of G. We show $aNa^{-1} = N$ for all $a \in G$.

We already know $aNa^{-1} \subseteq N \ \forall a \in G$ b/c N is normal.

To show $N \subseteq aNa^{-1} \ \forall a \in G$, we need to, given an $n \in N$, find $m \in N$ such that
$n = ama^{-1}$.

Take $m = a^{-1}na$. First $m \in N$. Since N is normal, we know $bdb^{-1} \in N$ if $b \in G$ & $d \in N$. Let $b = a^{-1} \in G$ & $d = n \in N$.
$ama^{-1} = a(a^{-1}na)a^{-1}$
$= n$.
Thus $\forall n \in N \ \exists m \in N$ st $n = ama^{-1}$. Thus $N \subseteq aNa^{-1} \ \forall a \in G$.
Th...

Now suppose $aNa^{-1} = N$. This is left as an exercise for HW.

Example:
Let G be a finite group w/ identity e. Let H be a subgroup of G w/ index 2.

How many right cosets of H in G are there? How many left?

There are 2 right cosets of H in G & likewise 2 left cosets.

Let $g \in G$. When are Hg & He equal? What about gH & eH?
$Hg = He$ iff $g \in H$. Likewise $gH = eH$ iff $g \in H$.

Recall cosets of H in G partition G. Further Hg & He are equivalence classes.

Let $g \in G$ st $Hg \neq He$. Since $Hg \neq He$, we know $Hg \cap He = \emptyset$. Likewise, we know $g \notin H$ b/c if $g \in H$, we'd have $Hg = He$.

Suppose $g \in G$ & $g \in H$. Then $Hg = H = gH$.

Suppose $g \in G$ but $g \notin H$. We know $Hg \neq He$ from above. Likewise we know $gH \neq eH$. But $He = H = eH$. Since there are only 2 distinct cosets we conclude
$Hg = gH = G \setminus H = H$, ← complement of H in G!

Recall:
It's been awhile since we talked about cosets.
Let H be a subgroup of group G.

Define the right coset Ha where $a \in G$ is the representative of Ha as
$Ha = \{ha \mid h \in H\}$.

Likewise the left coset is
$aH = \{ah \mid h \in H\}$.

Using our work in the above example, we conjecture that if the index of subgroup H in group G is 2, then H is a normal subgroup of G, $H \triangleleft G$.

Note that if the index of H is 1 then $H = G$ & G is always a normal subgroup of itself.

Example:
Consider the group S_3.
Let $f \in S_3$ defined by $f: 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1$.

What is the order of f in S_3: $o(f)$? We know it is one of 1, 2, 3, 6. This is b/c the order of f must divide its group.

Since $f \neq i$, we know $o(f) \neq 1$. [$f \neq i$]

Since S_3 is non-abelian, we know $o(f) \neq 6$. If $o(f)=6$ then S_3 would be a cyclic group generated by f, meaning it would be abelian (extension of power rules).

Thus $o(f)=2$ or $o(f)=3$. f

f^2: is defined by f^2: $1 \to 3$, $2 \to 1$, $3 \to 2$. Since $f^2 \neq i$, we know $o(f) \neq 2$. Thus $o(f)=3$.

Further, f^3: $1 \to 1$, $2 \to 2$, $3 \to 3$. Since...
3 is the smallest positive integer m st $f^m = i$. Thus $o(f)=3$.

Let $H=\langle f \rangle$. $|H|=3$ b/c $o(f)=3$. By Lagrange's theorem
$|S_3| = |H|\,[G:H]$
Thus we conclude the order of H in G $[G:H]=2$.

Thus we expect $|H|$ to be a normal subgroup.

Quotient / Factor Groups

Def:
Let N be a normal subgroup of group G.
Define the quotient group G/N (read: G mod N) as
$G/N = \{Na \mid a \in G\}$.

So for each $a \in G$, $Na = [a]$ under the equivalence relation
$x \sim y$ iff $xy^{-1} \in N$.

Define $*$ (the group operation) on G/N by
$(Na)*(Nb) = Nab$ for all $a, b \in G$

The following is a proof of the group properties

How do we know this group operation $*$ is well-defined? We need to show like inputs result in like outputs. ← closed

Suppose $Na = Nb$ & $Nc = Nd$ for some $a, b, c, d \in G$. We show $(Na)*(Nc) = (Nb)*(Nd)$, that is $Nac = Nbd$.

From our theorems of equivalence classes, we know two equivalence classes Nac & Nbd are equivalent iff their representatives are related, that is
$Nac = Nbd \iff ac \sim bd \iff (ac)(bd)^{-1} \in N$.

Since we assumed $Na = Nb$, we know $a \sim b$. Likewise $Nc = Nd$ gives us $c \sim d$.
By the definition of our relation we have $ab^{-1} \in N$ & $cd^{-1} \in N$.

Take the product $(ac)(bd)^{-1}$. We show this is an element of N.
$(ac)(bd)^{-1} = acd^{-1}b^{-1} = anb^{-1}$ for some $n \in N$ (b/c $c \sim d \iff cd^{-1} \in N$).

Now we try to find a $m \in N$ st $nb^{-1} = b^{-1}m$ b/c if there is then
$anb^{-1} = ab^{-1}m$
Must be in N b/c $ab^{-1} \in N$ & $m \in N$.

Proof: Let $n = bnb^{-1}$. We know $n \in N$ b/c $n \in N$, $b \in G$, & N is normal. Therefore

$$an b^{-1} = ab^{-1}n = ab^{-1}bnb^{-1}$$

Thus $(ac)(bd)^{-1} \in N$, so $ac \sim bd$. Thus $(Na)*(Nc) = Nac = Nbd = (Nb)*(Nd)$ given $Na = Nb$ & $Nc = Nd$. Therefore $*$ is well defined. □

What is the identity of G/N wrt $*$?

We guess that $Ne = N$ is the identity of G/N.
Let $a \in G$. Then

$$(Na)*(Ne) = Nae = Na \quad \& \quad (Ne)*(Na) = Nea = Na.$$

Thus $Ne = N$ is the identity of G/N.

This actually works for all $n \in N$ b/c $N = Ne = Nn$ b/c $nne \Rightarrow ne^{-1} \in N$.
Further $\forall n_1, n_2 \in N \quad Nn_1 = Nn_2$ b/c $n_1 \sim n_2 \Leftrightarrow n_1 n_2^{-1} \in N$.

Is $*$ associative? Yes. $(Na)*(Nb*Nc) = Na*Nbc = Nabc = Nab*Nc = (Na*Nb)*Nc$

Does $*$ have an inverse? Yes b/c $\forall a \in G \ \exists a^{-1} \in G$ s.t. $aa^{-1} = e$. Therefore it follows

$$(Na)*(Na^{-1}) = Naa^{-1} = Ne = N.$$

Therefore G/N is a group under $*$.

Example:
Let G denote the group of integers under $+$. Pick some $n \in \mathbb{N}$.
Let $N = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Consider G/N.

Pick some $a \in \mathbb{Z}$. We find $N+a$ is our familiar congruence mod n

$$N+a = \{nz + a \mid z \in \mathbb{Z}\} = [a]_n$$

What is the order of $N+2$ in G/N?
This is equivalent to asking what is the order of $[2]_n$ in $\mathbb{Z}_n$.
It depends on whether n is even or odd.

Example:
Consider the group S_3 w/ $f \in S_3$ defined by $f: 1 \to 2, 2 \to 3, 3 \to 1$
The order of f $o(f) = 3$ b/c $H = (f) = \{f^0, f^1, f^2\} = \{i, f, f^2\}$ where

$f^0 = i \Leftrightarrow f = 1,2,3$
$f^1 = f \Leftrightarrow f' = 2,3,1$
$f^2: 1 \to 3, \ 2 \to 1, \ 3 \to 2. \Leftrightarrow f^2 = 3,1,2$
$f^3 = i$

(right-side is permutation notation)

We know that there are exactly 2 (left/right) cosets of H in S_3 b/c $|S_3| = 3! = 6$ & $|H| = 3$, so by Lagrange's we know the index of H in G $[S_3 : H] = 2$

$|S_3| = |H|[S_3 : H]$

B/c there are exactly 2 (right) cosets, we know S_3/H has exactly two elements, in particular H & Hg where $g: 1\to 1, 2\to 3, 3\to 2 \Leftrightarrow g = 1, 3, 2$.

How do we know $Hg \neq H$? B/c $g \in Hg$ but $g \notin H$.

Note: H is a normal subgroup of S_3. How do we know that? The index of H in G is 2 & we showed earlier that all subgroups w/ index 2 are normal.

Let's compute all products in S_3/H. For example, what is $(Hg)*(Hg)$?

$Hi * Hi = Hii = Hi$

$Hi * Hg = Hig = Hg$ We could use that $H = Hi$ is the identity of group S_3/H.

$Hg * Hi = Hgi \neq Hg$

$Hg * Hg = Hgg = Hi$ & Note $gog = i$

Could we have gotten $Hg * Hg = Hg$? No b/c...

i) We know $Hg * Hi = Hg$ b/c Hi is the identity of S_3/H & we need an inverse of Hg

ii) If $Hg * Hg = Hg$, then Hg would be identity. Then $Hg = Hi$, which is a contradiction.

Thm: Properties of Normal Subgroups

Let G be a group w/ normal subgroup N.

i) If $n \in \mathbb{Z}$, then $(Na)^n = N(a^n)$. [Trivial $n=0$, inductive $n>0$, $(Na)^n = [(Na)^r]^{-1}$ for $n<0$].

ii) If G is finite, then $|G/N| = [G:N] = id_G(N) = \frac{|G|}{|N|}$. } Lagrange's

iii) If G is abelian, then G/N is abelian.

$Na * Nb = Nab = Nba = Nb * Na \quad \forall a, b \in G$.

iv) If G is cyclic, then G/N is cyclic. (Proof below)

v) The function $\varphi: G \to G/N$ defined by $\varphi(g) = Ng \ \forall g \in G$ is a homomorphism from G onto G/N w/ kernel $\ker(\varphi) = N$. (Proof below)

This is called the <u>canonical homomorphism.</u>

Pf:

iv) Assume G is a cyclic group. Let $a \in G$ be the generator of G, that is $G = (a) = \{a^z \mid z \in \mathbb{Z}\}$.

We show $G/N = (Na)$, that is G/N is cyclic w/ generator a. We do this w/ double set inclusion.

Trivially, $\{(Na)^z \mid z \in \mathbb{Z}\} \subseteq G/N$ holds b/c G/N is closed under $*$.

Let $x \in G/N$. By definition $x = Nb$ for some $b \in G$. Since $b \in G$, we know

$\exists k \in \mathbb{Z}$ st $b = a^k$. Thus $x = Nb = N(a^k)$ for some $k \in \mathbb{Z}$.

By (i), we thus know $x = N(a^k) = (Na)^k$. Therefore $\forall x \in G/N$
Therefore $\forall x \in G/N \ \exists k \in \mathbb{Z}$ st $x = (Na)^k$.
Thus $G/N \subseteq \langle Na \rangle$.

Since we have double set inclusion, we know $G/N = \langle Na \rangle$, so G/N is cyclic. □

v) • First, let's show such a φ is a homomorphism. Let $g, h \in G$.
$\varphi(gh) = Ngh = Ng * Nh = \varphi(g)\varphi(h)$

• Now let's show φ is onto G/N. Trivially $\text{Rng}(\varphi) \subseteq G/N$ b/c φ is well-defined. Let's show the reverse.

Let $x \in G/N$. Then $x = Na = \varphi(a)$ for some $a \in G/N$.
Thus $x \in \text{Rng}(\varphi)$ & so $G/N \subseteq \text{Rng}(\varphi)$.

Therefore $G/N = \text{Rng}(\varphi)$ & φ is onto.

• Now let's show $\ker(\varphi) = N$. Let e be the identity of G.
$\ker(\varphi) = \{ g \in G \mid \varphi(g) = Ne = N \}$
$= \{ g \in G \mid Ng = N \}$
$= \{ g \in G \mid g \in N \}$
$= N$ (since $N \subseteq G$).

Thus all parts hold.

First Homomorphism Theorem

The first homomorphism theorem is a big deal. Let's set the stage.

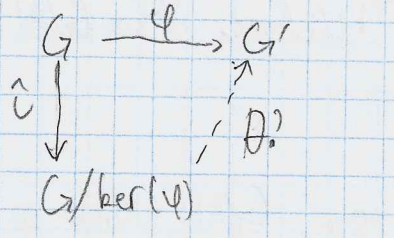
Let G & G' be groups. If $\varphi: G \to G'$ is a homomorphism, we know it's range $\text{Rng}(\varphi) = \varphi(G)$ is a subgroup of G'.

Let N be a normal subgroup of G. There must be a canonical homomorphism $\hat{\imath}$ from G onto G/N such that $\ker(\hat{\imath}) = N$. In particular
$\hat{\imath}(g) = Ng$.

• If $\varphi: G \to G'$ is a homomorphism, then its kernel $\ker(\varphi)$ is a normal subgroup of G, that is $\ker(\varphi) \triangleleft G$ $\forall$ homomorphism $\varphi: G \to G'$.

Consider the canonical homomorphism $\hat{i}$ from G' onto $G/\ker(\varphi)$.

Let's draw a diagram of this.



Is there a homomorphism θ st $\varphi = \theta \circ \hat{i}$? In other words we want for all $g \in G$ $(\theta \circ \hat{i})(g) = \varphi(g)$.

We rewrite $(\theta \circ \hat{i})(g)$ as $\theta(\hat{i}(g)) = \theta(\ker(\varphi)g)$. ← definition of $\hat{i}$

So we need to define $\theta(\ker(\varphi)g)$ to $\varphi(g)$ $\forall g \in G$.
Is this well defined? If $\ker(\varphi)g = \ker(\varphi)h$, is $\theta(\ker(\varphi)g) = \theta(\ker(\varphi)h)$?

Thm: First Homomorphism Theorem
Let G & G' be groups w/ homomorphism $\varphi: G \to G'$.
Let $\hat{i}$ denote the canonical homomorphism from G onto $G/\ker(\varphi)$.
Let $H' = \text{rng}(\varphi) = \varphi(G)$.

We know the following:

i) There is a monomorphism $\theta: G/\ker(\varphi) \to G'$ st $\theta \circ \hat{i} = \varphi$.

ii) The range of θ is H'. Thus $G/\ker(\varphi)$ is isomorphic to H'. (B/c θ then isomorphism from $G/\ker(\varphi)$ to H')

iii) If φ is onto G', then $G/\ker(\varphi)$ is isomorphic to G'.

PF:
Define θ by $\theta(\ker(\varphi)g) = \varphi(g)$. Since $\hat{i}(g) = \ker(\varphi)g$ $\forall g$, we know that indeed $\varphi = \theta \circ \hat{i}$. if θ is well defined.

Let's show that θ is well defined. Let $g, h \in G$ be elements of G such that $\ker(\varphi)g = \ker(\varphi)h$. We show $\theta(\ker(\varphi)g) = \theta(\ker(\varphi)h)$.

By the definition of equality of cosets, if $\ker(\varphi)g = \ker(\varphi)h$, then $gh^{-1} \in \ker(\varphi)$.

Since $gh^{-1} \in \ker(\varphi)$, we know $\varphi(gh^{-1}) = e'$ where e' is the identity of G'.
We now show $\theta(\ker(\varphi)g) = \theta(\ker(\varphi)h)$ by showing $\varphi(g) = \varphi(h)$.

$e' = \varphi(gh^{-1}) = \varphi(g)\,\varphi(h^{-1}) = \varphi(g)\,\varphi(h)^{-1}$
$\Rightarrow e'\varphi(h) = \varphi(g)\,\varphi(h)^{-1}\varphi(h)$
$\Rightarrow \varphi(h) = \varphi(g)$
$\Rightarrow \theta(\ker(\varphi)h) = \theta(\ker(\varphi)g)$

Thus θ is well-defined. (well-defined/closed)

(i) Now we show θ is indeed a homomorphism

Let $g, h \in G$. We show θ is a homomorphism, that is
$\theta(\ker(\psi)g * \ker(\psi)h) = \theta(\ker(\psi)g)\,\theta(\ker(\psi)h)$.
by the following algebra:

$\theta(\ker(\psi)g * \ker(\psi)h)$
$= \theta(\ker(\psi)gh)$
$= \psi(gh)$
$= \psi(g)\,\psi(h)$
$= \theta(\ker(\psi)g)\,\theta(\ker(\psi)h)$. (homomorphism)

Now let's show that θ is one-to-one/a monomorphism. To do this we show $\ker(\theta) = \{\ker(\psi)\}$ where $\ker(\psi)$ is the identity of $G/\ker(\psi)$. You could show the "more standard" way but it's harder.

$\ker(\theta) = \{\ker(\psi)g \in G/\ker(\psi) \mid \theta(\ker(\psi)g) = e' \in G'\}$
$= \{\ker(\psi)g \in G/\ker(\psi) \mid \psi(g) = e'\}$
$= \{\ker(\psi)g \in G/\ker(\psi) \mid g \in \ker(\psi)\}$
$= \{\ker(\psi)\}$.

(i) Since $\ker(\theta) = \{\ker(\psi)\}$ (identity of $G/\ker(\psi)$), θ monomorphism (monomorphism)

(ii) We won't show that the range of θ is H' here. b/c time.

Example:

Let G be all functions $f: \mathbb{R} \to \mathbb{R}$ under addition $+$ where
$(f+g)(x) = f(x) + g(x)$ $\forall f, g \in \mathbb{R} \to \mathbb{R}$ & $x \in \mathbb{R}$.
G is an abelian group. We show that partially here.

The identity of G is the zero function $z(x) = 0$.

The inverse of G is the negative of the given $f \in G$.
That is $f^{-1}(x) = -f(x)$ $\forall x \in \mathbb{R}$.

Consider $N = \{f \in G \mid f(\pi) = 0\}$. This is in fact a normal subgroup of G.

The identity $z(x) = 0$ is in N b/c $z(\pi) = 0$.

N is closed under the group operation $+$ b/c
$f(\pi) + g(\pi) = 0$ when $f(\pi) = 0$ & $g(\pi) = 0$ (i.e. $f, g \in N$)

N has the inverse property b/c $\forall f \in N$ $f^{-1} \in N$. That is b/c
$-f(\pi) = 0$ when $f(\pi) = 0$ (i.e. $f \in N$).

Thus N is a subgroup.

Since G is abelian, N is abelian. Further, since G is abelian N is a normal subgroup as all subgroups of an abelian group are normal.

We want to show that G/N is isomorphic to $\mathbb{R}$. We do this by finding a homomorphism φ from G to $\mathbb{R}$ where $\ker(\varphi) = N$. That is, we want $f \in N$ iff $\varphi(f) = f(\pi)$.

Define φ by the evaluation on π. That is
$\varphi(f) = f(\pi)$ $\forall f \in G \Leftrightarrow f: \mathbb{R} \to \mathbb{R}$.

We show φ is a homomorphism w/ our properties.
$\varphi(f) = f(\pi) = 0$ iff $f \in N \Leftrightarrow f(\pi) = 0$.
φ is a homomorphism b/c $\varphi(f+g) = (f+g)(\pi) = f(\pi) + g(\pi) = \varphi(f) + \varphi(g)$.

We now show φ is onto. Let $r \in \mathbb{R}$, we find a $f(x) \in G$ st $f(\pi) = r$.
Choose $f(x) = r$. Then $\varphi(f) = f(\pi) = r$. Then $r \in \text{Rng}(\varphi)$, so φ is onto.
(Formally, $\mathbb{R} \subseteq \text{Rng}(\varphi)$ as shown & $\text{Rng}(\varphi) \subseteq \mathbb{R}$ b/c $\varphi: G \to \mathbb{R}$ well-defined.)

Example:
Let $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. $\mathbb{R}^*$ is an abelian group under multiplication.
Consider the normal subgroup $(0, \infty) \subseteq \mathbb{R}^*$.
$\mathbb{R}^*/(0,\infty)$ has two elements, namely $(0,\infty)\cdot 1$ & $(0,\infty)\cdot -1$.
(if $a > 0$, $(0,\infty)\cdot a = (0,\infty)\cdot 1$ b/c $\exists n \in (0,\infty)$ st $an = 0$.)

What other groups have exactly 2 elements?
- $\{\pm 1\}$ under multiplication
- $\mathbb{Z}_2$ under $+$
- S_2 under $\circ$

Let's pick S_2 & show $\mathbb{R}^*/(0,\infty)$ is isomorphic to it.
We need to find a homomorphism $\varphi: \mathbb{R}^* \to S_2$ st $\ker(\varphi) = (0,\infty)$.
Recall $S_2 = \{i, f\}$ where $f: 1 \to 2, 2 \to 1$.

Define φ as
$$\varphi(r) = \begin{cases} i & r \in (0,\infty)\cdot 1 \\ f & r \in (0,\infty)\cdot -1 \end{cases}$$

If φ is a homomorphism, then $\ker(\varphi) = (0,\infty)$ clearly (b/c $\varphi(r) = i$ $\forall r \in (0,\infty)$).

Now we show φ is a homomorphism
$$\varphi(ab) = \begin{cases} i & ab > 0 \\ f & ab < 0 \end{cases} = \begin{cases} i \circ i & a>0 \ \& \ b>0 \\ i \circ f & a>0 \ \& \ b<0 \\ f \circ i & a<0 \ \& \ b>0 \\ f \circ f & a<0 \ \& \ b<0 \end{cases} = \varphi(a) \circ \varphi(b).$$
(really $ab = (0,\infty)\cdot \pm 1$ ← should be cosets)

Since φ is a homomorphism w/ $\ker(\varphi) = (0,\infty)$, we know φ is onto S_2 & by the 1st homomorphism theorem S_2 & $\mathbb{R}/(0,\infty)$ are isomorphic.

Chapter 3

We'll be dealing a lot w/ S_n, that is the set of bijections w/in $\{1, \dots, n\}$ or equivalently the permutations of $[1, \dots, n]$, so let's get a more compact notation.

Notation:

Let $n \in \mathbb{N}$. Consider S_n w/ $\sigma \in S_n$. Instead of writing
$\sigma(1) = a_1, \ \sigma(2) = a_2, \dots, \sigma(n) = a_n$
we write
$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & & a_n \end{pmatrix}$$

This notation also let's you visualize composition like $\tau \circ \sigma$ by "rearranging" the columns of τ so that the top numbers of τ align w/ the bottom numbers of σ.

Likewise visualize inverse as flipping the rows & reordering the columns in sorted order.

Def: Cycle

Let $n \in \mathbb{N}$ & $r \in \mathbb{N}$ where $r \leq n$.
Let $i_1, \dots, i_r$ be distinct integers in $1, \dots, n$.

Define σ in S_n by
$\sigma(j) = j$ where $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_r\}$
$\sigma(i_k) = i_{k+1}$ where $k < r$
$\sigma(i_r) = i_1$

Basically you rotate the i's to the right & leave the rest alone.

We call this permutation σ an r-cycle denoted $(i_1 i_2 \dots i_r)$ where r is the length of σ.
When $r = 2$, we call σ a transposition.

Def:

Two cycles $(i_1 \dots i_r)$ & $(j_1 \dots j_t)$ are disjoint iff
$\{i_1 \dots i_r\} \cap \{j_1 \dots j_t\} = \emptyset$

Example:

Let $\sigma = (1\ 2)$ in S_3. Write σ in our compact non-cyclic notation
$$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Example
Let $\sigma = (12)$ in S_3. Write σ more explicitly
$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Rem:
From the above examples you can see we need to know n to compute the functional value of σ.

We can compose $\circ$ cycles (note: we elide the $\circ$) like we do w/ mappings.

Example:
Consider $(1\,3\,4)(2\,3\,1)(1\,4\,5)$ in S_3. Write σ
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$

Thm:
1) Every 1-cycle is the identity permutation
2) If $i, j \in \mathbb{N}$, then $(i\,j)^{-1} = (j\,i) = (i\,j)$
3) If $\sigma = (i_1 \dots i_r)$, then $\sigma^{-1} = (i_r \dots i_1)$
4) The order of an r-cycle is r
5) If $\sigma = (i_1 \dots i_r)$ & $\rho \in S_n$, then $\rho\sigma\rho^{-1} = (\rho(i_1) \dots \rho(i_n))$.
6) Disjoint subgroups commute.
7) (my addition) If $\sigma = (i_1, i_2 \dots i_n)$, then $\sigma = (i_2 \dots i_n\, i_1)$

Thm:
Every permutation is a product of disjoint cycles.

We won't prove this theorem b/c it's tough. :

Transpositions & Alternating Groups

We want to show that you can write every permutation σ in S_n as a product of transpositions. First let's show you can write every r-cycle as a product of transpositions. We'll only be focusing on $n \geq 2$ b/c S_1 is boring.

Let σ be an r-cycle where $r \in \mathbb{N}$.

If $r = 1$, then σ is the identity, so $\sigma = (1\,2)(1\,2) = I$.

If $r > 1$, then where $\sigma = (i_1 \dots i_r)$ we can rewrite σ as product of $r-1$ transpositions
$\sigma = (i_1\, i_r)(i_1\, i_{r-1}) \dots (i_1\, i_3)(i_1\, i_2)$.
I'm behind on notes so you can check this yourself.

Example:
$(1\,2\,4\,5) = (1\,5)(1\,4)(1\,2)$
$(1\,2\,4\,5\,3) = (1\,3)(1\,5)(1\,4)(1\,2)$

Example:

$$\begin{aligned}&((1\,2\,3\,4)(5\,6)(7\,8))^{-1}\\ &= (7\,8)^{-1}(5\,6)^{-1}(1\,2\,3\,4)^{-1}\\ &= (8\,7)(6\,5)(4\,3\,2\,1)\\ &= (8\,7)(6\,5)(4\,1)(4\,2)(4\,3)\end{aligned}$$

Def:
Let $n \in \mathbb{N}$ where $n \geq 1$. Let $\sigma \in S_n$ be a permutation in S_n.

We say σ is <u>even</u> if σ can be written as the product of an even number of transpositions

We say σ is <u>odd</u> if σ can be written as the product of an odd number of transpositions.

Thm:
A permutation $\sigma \in S_n$ cannot be both even & odd, but it must be one of them.

We won't show that here. :)

Def:
Let $n \in \mathbb{N}$ where $n \geq 1$. Let $A_n = \{\sigma \in S_n \mid \sigma \text{ even}\}$.
A_n is called the <u>alternating group</u> of degree n.

Note that A_n is indeed a subgroup of S_n.

Example:
Consider S_2. We know $S_2 = \{i, (1\,2)\}$.
Since $i = (1\,2)(1\,2)$ is even & $(1\,2)$ is odd,
$A_2 = \{i\}$.

Example:
Consider S_3. We know $|S_3| = 3! = 6$ & in particular
$S_3 = \{i, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.
What is A_3?

$r = 3 \Rightarrow r-1$ products

$i = (1\,2)(1\,2) \in A_3$
$(1\,2) \notin A_3$
$(1\,3) \notin A_3$
$(2\,3) \notin A_3$

$(1\,2\,3) = (1\,3)(1\,2) \in A_3$
$(1\,3\,2) = (1\,2)(1\,3) \in A_3$

So $|A_3| = 3$.

Given the above two examples (& name of even & odd), we conjecture $|A_n| = |S_n|/2 \ \forall n \in \mathbb{N}, n > 1$.

Thm:
Consider r-cycle σ. σ is even if r is odd & odd if r is even.

This is b/c we showed we can write any r-cycle as a product of $r-1$ transpositions.

Thm:
Let $n \in \mathbb{N}$ where $n > 1$, then A_n is a normal subgroup of S_n & the index $[S_n : A_n]$ of A_n in S_n is 2 & thus $|A_n| = \frac{n!}{2}$ ← $|S_n|$ (From Lagranges)

Pf:
Define a function $f: S_n \to \mathbb{Z}_2$ by ← We consider S_n under $\circ$ & $\mathbb{Z}_2$ under $+$.

$$f(\sigma) = \begin{cases} [0]_n & \text{if } n \text{ is even} \\ [1]_n & \text{if } n \text{ is odd} \end{cases}$$

We show f is a homomorphism. Consider $\sigma_1, \sigma_2 \in S_n$. We have 4 cases.

σ_1 even & σ_2 even $\Rightarrow \sigma_1 \circ \sigma_2$ even b/c even + even = even.
$f(\sigma_1 \circ \sigma_2) = [0]_2$
✓ $f(\sigma_1) + f(\sigma_2) = [0]_2 + [0]_2 = [0]_2$

σ_1 odd & σ_2 odd $\Rightarrow \sigma_1 \circ \sigma_2$ even b/c odd + odd = even
$f(\sigma_1 \circ \sigma_2) = [0]_2$
✓ $f(\sigma_1) + f(\sigma_2) = [1]_2 + [1]_2 = [0]_2$

σ_1 odd & σ_2 even $\Rightarrow \sigma_1 \circ \sigma_2$ odd b/c odd + even = even
$f(\sigma_1 \circ \sigma_2) = [1]_2$
✓ $f(\sigma_1) + f(\sigma_2) = [1]_2 + [0]_2 = [1]_2$

✓ σ_1 even & σ_2 odd follows the same logic to above.

Note that in all cases if we can write σ_1 as a product of s transpositions & σ_2 is a product of t transpositions, then $\sigma_1 \circ \sigma_2$ can be written as the product of $s+t$ transpositions where you simply combine σ_1 & σ_2's two transpositions.

Thus f is a homomorphism.

By the way we defined f, we know
$A_n = \ker(f) = \{\sigma \in S_n \mid \sigma \text{ is even}\}$.
Thus we know A_n is a normal subgroup of S_n b/c all kernels are normal subgroup.

By the first homomorphism theorem S_n/A_n is isomorphic to $\mathbb{Z}_n$. Therefore $|S_n/A_n| = 2$, thus $[S_n : A_n] = 2$.
By Lagrange's theorem
$|S_n| = [S_n : A_n]\,|A_n| \Rightarrow |A_n| = |S_n|/[S_n : A_n] = n!/2$. □

Chapter 4

Here we'll talk about rings, which is like + & · on $\mathbb{Z}$.

Def:
Let R be a nonempty set w/ binary operations + & · on R. $(R, +, \cdot)$ is called a ring, specifically a ring under + & ·
iff
i) R is an abelian group under +
ii) $a \cdot b \in R \quad \forall a, b \in R$ (i.e. · is a well-defined binary op)
iii) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$ (i.e. · is associative)
iv) $(a+b) \cdot c = a \cdot c + b \cdot c$ & $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$
(i.e. · distributes over +)

Note that · doesn't need to be commutative

Rem:
(i) means
+ bin. op. over R,
+ associative & commutative, &
+ has identity & inverses

(iv) is called the distributive laws

The additive identity in R is denoted by 0 or 0_R

The additive inverse of $a \in R$ is denoted $-a$.

Def:
R is a commutative ring iff · is commutative on R
(& R is a ring).

R is called a ring w/ identity iff there is a · identity denoted 1 (or 1_R) in R such that $1 \neq 0$. (not included by everyone)

Rem:
If R is a ring w/ identity, the multiplicative inverse of $a \in R$ is denoted by a^{-1}. If a^{-1} exists, we say $a \in R$ is an invertible element.

If you let $1 = 0$, then $R = \{0\}$. This is b/c $0 \cdot a = 0$.
If $1 = 0$, then for all $a \in R$ $1 \cdot a = a$ & $0 \cdot a = 0$. If $0 \neq 1$ then $1 \cdot a = 0 \cdot a$, so $a = 0$ for all $a \in R$.

Example:
Consider $\mathbb{Z}$ under normal $+$ & $\cdot$. Then $\mathbb{Z}$ is a commutative ring w/ identity. $+1$ & 1 are the only invertible elements of $R=\mathbb{Z}$.

Example:
Let $n\in\mathbb{N}$ where $n>1$. Consider $\mathbb{Z}_n$.

$\mathbb{Z}_n$ is a commutative ring w/ identity $[1]_n$. Let's prove that.

As we've studied before, $\mathbb{Z}_n$ is an abelian group under $+$. Associativity & well-definedness of $\cdot$ is easy to show, so let's do distributivity.

Take some $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$.

$$\begin{aligned}[a]_n\cdot([b]_n+[c]_n) &= [a]_n\cdot[b+c]_n\\ &= [a(b+c)]_n\\ &= [ab+ac]_n\\ &= [ab]_n+[ac]_n\\ &= [a]_n[b]_n+[a]_n[c]_n.\end{aligned}$$

Since $\cdot$ is commutative, this shows both distributive laws. (distributivity)

(we haven't proven this yet)

We also haven't shown commutativity or identity of $\cdot$ but those are again easy.

Let's find when $[a]_n\in\mathbb{Z}_n$ is invertible. We know $[a]_n$ is invertible iff $\exists [b]_n\in\mathbb{Z}_n$ st $[a]_n[b]_n=[b]_n[a]_n=[1]_n$. Now $[a]_n[b]_n=[1]_n$ iff $ab\equiv 1 \pmod n$.

Let $a\in\mathbb{Z}$. $\exists b\in\mathbb{Z}$ st $ab\equiv 1 \pmod n$ iff n divides $ab-1$. n divides $ab-1$ iff $\exists c\in\mathbb{Z}$ st $ab-1=nc$. This holds iff $ab+n(-c)=1$. This is true iff n & c are relatively prime.

How do we find b? The euclidean algorithm. (find GCD)

Example:
Consider $R=\mathbb{R}^{n\times n}$. R is a ring w/ identity under standard addition & multiplication.

We know A invertible iff $\det(A)\neq 0$.

We know R commutative iff $n=1$. O/w it's non-commutative.

Example:
Let R denote the set of polynomials w/ real coefficients $\mathbb{R}[x]$.
R is a commutative ring under normal $+$ & $\cdot$. What are the invertible elements of R?

Thm:
Let R be a ring. $0a=a0=0$ $\forall a\in R$.

Pf:
Consider $a\in R$. Then
$$a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$$
Thus $$-(a\cdot 0)+(a\cdot 0) = -(a\cdot 0)+(a\cdot 0+a\cdot 0) = (-(a\cdot 0)+a\cdot 0)+a\cdot 0 = a\cdot 0$$

Since $-(a\cdot 0)+a\cdot 0 = a\cdot 0$ but also $-(a\cdot 0)+a\cdot 0 = 0$, we know
$a\cdot 0 = 0$

We show the same for $0\cdot a$. □

Thm:
Let R be a ring. Then
$a(-b) = (-a)b = -(ab) \quad \forall a, b \in R$

Pf:
Consider $a, b \in R$.

We show $a(-b) = -(ab)$.
$a(-b) + (ab) = a(-b+b) = a0 = 0$
Since $+$ is commutative, we also have
$(ab) + a(-b) = 0$
So $a(-b)$ is the additive inverse of (ab). Thus
$a(-b) = -(ab)$

$(-a)b = -(ab)$ follows similarly. □

Thm:
Let R be a ring.
$(-a)(-b) = ab \quad \forall a, b \in R$

Pf:
Consider $a, b \in R$. By our earlier theorem
$(-a)(-b) = -(a(-b)) = -(-(ab))$
Since this is a double inverse,
$-(-(ab)) = ab$
so we conclude
$(-a)(-b) = ab$.

Thm:
Let R be a ring w/ identity 1. Consider $a \in R$. If $b, c \in R$ are inverses of a that is
$ab = ba = 1$ & $ac = bc = 1$,
then $b = c$. In other words a^{-1} (multiplicative inverse of a) is unique if it exists.

We did this for groups by considering bac.

required for inverses

Thm:
Let R be a ring w/ identity. Consider $a, b \in R$. Then ab is invertible if a & b are invertible.

We again just show by associativity that $(ab)^{-1} = b^{-1}a^{-1}$ like we did w/ groups.
$(ab)(b^{-1}a^{-1}) = aa^{-1} = 1$

Rem:
The converse, that a & b are invertible is definitely true for commutative rings. It might be true in general but we haven't shown that here.

Notation:
Consider $a \in R$ where R is a ring. Let $n \in \mathbb{Z}$.

i) We denote the nth power of addition by na. So
$3a = a + a + a$

ii) We denote the nth power of multiplication by a^n. So
$a^3 = a \cdot a \cdot a$

If R is a ring w/ identity & $a \in R$ is invertible, then
$a^{-n} = (a^{-1})^n$
So
$a^{-3} = (a^{-1})^3 = a^{-1} \cdot a^{-1} \cdot a^{-1}$.
And trivially
$a^0 = 1$

Properties:
Consider $a, b \in R$ where R is a ring & $n, m \in \mathbb{Z}$.

i) $(n+m)a = na + ma$

ii) $n(a+b) = na + nb$

iii) $(a^n)^m = a^{nm}$

Special Rings

We'll talk about integral rings (rings like $\mathbb{Z}$) & rational rings (rings like $\mathbb{Q}$).

Def:
Consider $a \in R$ where $a \neq 0$ & R is a ring.
a is said to be a zero divisor or divisor of zero if $\exists b \in R$ where $b \neq 0$ such that
$ab = ba = 0$

Example:
Consider $\mathbb{Z}_4$ under standard $+$ & $\cdot$. Are there any zero divisors in $\mathbb{Z}_4$?
✗ $[0]_4 = 0 \in \mathbb{Z}_4$. ×
✗ $[1]_4 [a]_4 = [a]_4 \neq 0$ iff $[a] \neq 0$. ×
✓ $[2]_4 [2]_4 = [4]_4 = [0]_4 = 0$.
× $[3]_4 [1]_4 = [3]_4 \neq 0$, $[3]_4 [2]_4 = [6]_4 \neq 0$, $[3]_4 [3]_4 = [9]_4 \neq 0$

Only show one side b/c commutative here

We can see only $[2]_4$ is a zero divisor.

Example:
Consider $\mathbb{Z}_6$. Are there any zero divisors?
We claim & you can show that $[2]_6, [3]_6, [4]_6$ are the only zero divisors.

$[2]_6[3]_6 = [6]_6 = 0 \Rightarrow [2]_6$ & $[3]_6$ zero divisors
$[4]_6[3]_6 = [12]_6 = 0 \Rightarrow [4]_6$ & $[3]_6$ zero divisors.

Def:
Let R be a commutative ring w/ identity

1) R is an integral domain if R has no zero divisors
2) R is a field if all non-zero elements a in R are invertible in R.

Remark:
If R is a commutative ring w/ identity, then R is a field iff
$\{a \in R \mid a \neq 0\} = R \setminus \{0\}$
is a group under multiplication $\cdot$.

Pf:
This is trivial for the identity, inverse property, & associativity. We must only show closure.

Consider $a, b \in R \setminus \{0\}$. Is $a \cdot b \in R \setminus \{0\}$? That is does $a \cdot b \neq 0$?
Suppose for contradiction that $a \neq 0$ & $b \neq 0$ but $ab = 0$

$ab = 0 =$
$\Rightarrow a^{-1}(ab) = a^{-1}0 = 0$
$\Rightarrow b = 0$

This contradicts $b \neq 0$, thus $ab \neq 0$ & $ab \in R \setminus \{0\}$.
We have thus shown closure.

Thm:
If R is a field, then R is an integral domain. (The converse isn't true)

Pf:
Suppose for contradiction that R is a field but R is not an integral domain. Since R is not an integral domain, there is a divisor of zero.

Thus $\exists a, b \in R$ where $a \neq 0$ & $b \neq 0$, but $ab = ba = 0$.

Since R is a field, $R \setminus \{0\}$ forms a group under multiplication. By the closure property $ab \in R \setminus \{0\}$ $\forall a, b \in R \setminus \{0\}$. In other words $ab \neq 0$ $\forall a, b \in R$ where $a \neq 0$ & $b \neq 0$
But this contradicts our assumption that R is an integral domain.

Thus R is a field implies R is an integral domain. □

Example:
Consider $\mathbb{Z}$. It is an integral domain but not field.

$\mathbb{Z}$ is not a field b/c $2 \in \mathbb{Z}$, but $\frac{1}{2} \notin \mathbb{Z}$. However, $\mathbb{Z}$ is a commutative ring. Further if $ab = 0$, then $a = 0$ or $b = 0$. By contraposition if $a \neq 0$ & $b \neq 0$, then $ab \neq 0$. Thus $\mathbb{Z}$ has no divisors of zero & is an integral domain as such.

Example:
Consider $\mathbb{R}$. $\mathbb{R}$ is a field.

Let's go back to our divisors of zero for $\mathbb{Z}_n$

Example
We showed $\mathbb{Z}_4$ & $\mathbb{Z}_6$ have divisors of zero. You can check that $\mathbb{Z}_3$ & $\mathbb{Z}_5$ have no divisors of zero (i.e. are integral domains)

We conjecture that for all $n \in \mathbb{Z}$ where $n > 1$
$\mathbb{Z}_n$ has a divisor of zero iff n is not prime / is composite.
$\mathbb{Z}_n$ has no divisors of zero / is an integral domain iff n is prime.

This is true! (Not yet proven)

Thm:
If R is a ring w/ identity & $a \in R$ is an invertible element in R.
Then a is not a divisor of zero.

PF:
Suppose for contradiction that $a \in R$ is invertible & a is a divisor of zero, that is $\exists b \in R$ where $b \neq 0$ st $ab = ba = 0$.

Using a series of algebraic transformations we get
$0 = a^{-1} \cdot 0 = a^{-1}(ab) = b$
This contradicts $b \neq 0$, so $a \in R$ is not a divisor of zero.

This theorem lets us connect our earlier theorem that $[a]_n$ is invertible if & only if a & n are coprime.

Note that we haven't shown that all non-invertible elements of R are divisors of zero. This is true for some rings (e.g. $\mathbb{Z}_n$) but not for others (i.e. $\mathbb{Z}$).

Example:
Consider $\mathbb{Z}_p$ where p is prime. Then $\mathbb{Z}_p$ has no divisors of zero (i.e. it's an integral field) b/c all $[a]_p \in \mathbb{Z}_p$ are invertible since a & p are coprime, that is $\gcd(a, p) = 1$, b/c p is prime.

Conclusions:

Suppose $n \in \mathbb{Z}$ where $n > 1$. Then we say the following about $\mathbb{Z}_n$.

1) $\mathbb{Z}_n$ has no divisors of zero / $\mathbb{Z}_n$ is an integral field iff n is prime.

2) All $[a]_n \in \mathbb{Z}_n$ is invertible / $\mathbb{Z}_n$ is a field iff n is prime.

The following are about non-$\mathbb{Z}_n$ fields

3) $\mathbb{Q}$ has no divisors of zero b/c $\forall a \in \mathbb{Q}$ is invertible / $\mathbb{Q}$ is a field.

4) $\mathbb{Z}$ has no divisors of zero / $\mathbb{Z}$ is an integral field.

Example:

Consider $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ & $B = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}$. Can we show A is a divisor of zero only using B.

$$AB = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Since $AB \neq 0$ but $BA = 0$, we cannot conclude whether A is a divisor of zero or not. (In this case it is but we don't know that here.)

Subrings & Ideals

Def:

Let R be a ring & S a non-empty subset of R.

S is a <u>subring</u> of R iff S itself is a ring under the same binary operations as R.

A subring S of R is an <u>ideal</u> of R iff $ab \in S$ & $ba \in S$ for all $a \in S$ & $b \in R$. Intuitively, multiplying by an element of S collapses the result into S.

Example:

The even integers are an ideal of $\mathbb{Z}$. Further $n\mathbb{Z}$ ($n \in \mathbb{Z}$) is an ideal of $\mathbb{Z}$. (Won't show here)

Remark:
Suppose S is a non-empty subset of ring R. S is a subring of R iff
a) $0 \in S$
b) $a+b \in S \quad \forall a, b \in S$
c) $-a \in S \quad \forall a \in S$
d) $ab \in S \quad \forall a, b \in S$

Basically, we don't need to check commutativity, associativity, or distributivity b/c those are "inherited" from $+$ & $\cdot$ on R.

Remark:
Suppose S is a non-empty subset of ring R. S is an ideal of R iff
a) $0 \in S$
b) $a+b \in S \quad \forall a, b \in S$
c) $-a \in S \quad \forall a \in S$
d) $ab \in S$ & $ba \in S \quad \forall a \in S$ & $b \in R$ ← stronger than (d) for subrings

Notice that this is identical to the requirements for subrings except (d) is made stronger.

Example: (could just say ideal)
Let R be a ring. Then $\{0_R\}$ & R are both subrings & ideals of R.

Let's first show $\{0_R\}$ ideal (& thus subring) of R
a) $0_R \in \{0_R\}$
b) $0_R + 0_R = 0_R \in \{0_R\}$
c) $-0_R = 0_R \in \{0_R\}$
d) $0_R b = b 0_R = 0_R \in \{0_R\} \quad \forall b \in R$

Now we can very easily show R similarly. For brevity we skip this.

Example:
Let S be an ideal of $R = \mathbb{Z}$.

If $S = \{0\}$ then $S = 0\mathbb{Z}$.

If $S \neq \{0\}$, then $\exists s \in S$ st $s \neq 0$. We know $-s \in S$ & $-s > 0$ or $s > 0$. Thus S contains a positive integer.

By the well-ordering principle, we know there exists a smallest positive integer $n \in S$. We want to show $S = n\mathbb{Z}$, which we do by double set inclusion.

Since $n \in S$ & S is an ideal of $\mathbb{Z}$, $nz \in S \quad \forall z \in \mathbb{Z}$. Thus $n\mathbb{Z} \subseteq S$.

Let m be an element of S. By the division algorithm $\exists q, r \in \mathbb{Z}$ st $m = qn + r$ & $0 \leq r < n$.
To show $m \in n\mathbb{Z}$, we want $r = 0$. By the above equation, we get $r = m + (-q)n$.
We know $(-q)n \in S$ b/c $(-q) \in \mathbb{Z}$ & $n \in S$ & S is an ideal of $\mathbb{Z}$. Since $m \in S$ by assumption, we have $r \in S$. Since r is "smaller" than the smallest positive element of S, n, we know r is not positive. Thus $r = 0$.

We thus know $n = qr$ where $q \in \mathbb{Z}$ for all $m \in S$. Thus $S \subseteq r\mathbb{Z}$. ∎

By double set inclusion, $S = r\mathbb{Z}$.

Thm:
If you have an ideal S of the integers $\mathbb{Z}$, then $S = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

This was proven in our above example.

Thm:
If R is a commutative ring w/ identity & $a \in R$, then
$aR = \{ar \mid r \in R\}$
is an ideal containing a.

We know $a \in aR$ b/c R has an identity.

This is the generalization of our above theorem.

Suppose R is a commutative ring w/ no identity & $a \in R$.
What can we say about $aR = \{ar \mid r \in R\}$?

Let $b, c \in aR$. Then $b = ar_1$ & $c = ar_2$ for some $r_1, r_2 \in R$. So
$bc = ar_1 ar_2 = a(r_1 ar_2) \in aR$.
From this we conjecture aR is always a subring of R.
This is indeed true.

Example:
Consider subring $\mathbb{Q}$ of ring $\mathbb{R}$. Is $\mathbb{Q}$ an ideal of $\mathbb{R}$? No.
Consider $1 \in \mathbb{Q}$ & $\pi \in \mathbb{R}$.
$1 \cdot \pi = \pi \notin \mathbb{Q}$.

Thm:
Consider subring S of ring R where $1 \in S$ & $S \subset R$. Then S is <u>not</u> an ideal of R.

Pf:
Consider $1 \in S$. Take $r \in R$ st $r \notin S$. We know r exists b/c S is a proper subset of R. Thus
$1 \cdot r = r \in R$ but $1 \cdot r = r \notin S$.

Ring Homomorphisms

Like group homomorphisms which preserved the group properties, ring homomorphism preserve ring properties.

Def:
Let R & R' be rings & $\varphi: R \to R'$ be a function.

1) φ is a homomorphism iff $\varphi(a+b) = \varphi(a) + \varphi(b)$ & $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in R$
2) φ is a monomorphism iff φ is a homomorphism & injective
3) φ is an isomorphism iff φ is a homomorphism & bijective
4) Iff $R = R'$ & φ is an isomorphism, we call φ an automorphism.

Def:
Let R & R' be rings. We say R & R' are isomorphic & write $R \cong R'$ iff $\exists$ isomorphism $\varphi: R \to R'$.

Example:
Consider rings $R = \mathbb{Z}$ & $R' = \mathbb{Z}_n$ where $n \in \mathbb{N}$. Define $\varphi: R \to R'$ by $\varphi(a) = [a]_n$.

We claim φ is a (ring) homomorphism.

Take $a, b \in R = \mathbb{Z}$. Then
$\varphi(a+b) = [a+b]_n = [a]_n + [b]_n = \varphi(a) + \varphi(b)$ &

$\varphi(ab) = [ab]_n = [a]_n [b]_n = \varphi(a)\varphi(b)$
Thus φ is a (ring) isomorphism.

We claim φ is not injective. Consider $0, n \in R = \mathbb{Z}$. Then
$\varphi(0) = [0]_n = [n]_n = \varphi(n)$
but $0 \neq n$. Thus φ is not injective.

Example:
Consider rings $\mathbb{R}$ & $\mathbb{R}^{2\times 2}$. Define $\varphi: \mathbb{R} \to \mathbb{R}^{2\times 2}$ by

$$\varphi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}.$$

We show φ is a homomorphism. Let $a, b \in \mathbb{R}$. Then

$$\varphi(a+b) = \begin{bmatrix} a+b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \varphi(a)\varphi(b)$$

↑ check yourself

$$\begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

We show φ is a monomorphism by showing it is injective.
Take some $a, b \in \mathbb{R}$ such that $\varphi(a) = \varphi(b)$.

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow a = b.$$

Thus φ is a monomorphism.

We show it is not isomorphic b/c it isn't surjective.
Take $I \in R^{2\times 2}$. Suppose $I \in \text{Rng}(\varphi)$, that is $\exists a \in R$ st $\varphi(a) = I$.

$$\varphi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow 0 = 1.$$

This is a contradiction so φ is not an isomorphism.

Note: $\varphi(a) = \begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix}$ wouldn't be a homomorphism b/c

$$\varphi(a)\varphi(b) = \begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} = 0 \quad \forall a, b \in R.$$ Thus $\varphi(1\cdot 1) = \varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ but $\varphi(1)\cdot\varphi(1) = 0$

Def:
Take a ring homomorphism $\varphi: R \to R'$. The kernel of φ is thus
$\ker(\varphi) = \{ a \in R \mid \varphi(a) = 0_{R'} \}$ where
where $0_{R'}$ is the additive identity of R'.

Thm:
Suppose R & R' are rings & $\varphi: R \to R'$ is a homomorphism.

i) $\ker(\varphi)$ is an ideal of R.

ii) φ is injective (i.e. monomorphism) iff $\ker(\varphi) = \{0_R\}$.

iii) $\varphi(na) = n\varphi(a)$ $\forall a \in R$ & $n \in \mathbb{Z}$.

iv) $\varphi(a^n) = (\varphi(a))^n$ $\forall a \in R$ & $n \in \mathbb{N}$. We need $n > 0$ b/c we don't know that a multiplicative identity or inverse exists for a.

You could say this for all $n \in \mathbb{Z}$ if R is a field & $a \neq 0$.

Pf:
i) We know $\ker(\varphi) \leq R$ by definition.

Since φ is a homomorphism from $(R, +)$ to $(R', +)$, we know $\varphi(0_R) = 0_{R'}$. Thus $0_R \in \ker(\varphi)$.

By our work on group homomorphisms we also know $a + b \in R$ & $-a \in R$ for all $a, b \in \ker(\varphi)$.

Now we just show the ideal property, that is
$as \in R$ & $sa \in R$ $\forall a \in \ker(\varphi)$ & $s \in R$.

Take $a \in \ker(\varphi)$ & $s \in R$. We show $as, sa \in \ker(\varphi)$, that is $\varphi(as) = 0_{R'}$ & $\varphi(sa) = 0_{R'}$.
B/c φ is a ring homomorphism we know
$\varphi(as) = \varphi(a)\varphi(s) = 0_{R'}$ b/c $\varphi(a) = 0_{R'}$ & $\varphi(sa)$ likewise.

Thus $\ker(\varphi)$ is an ideal of R. □ (i)

Should name this proposition Ph.

LE: (iv)
We show inductively that $\varphi(a^n) = \varphi(a)^n$ for all $n \in \mathbb{N}$.

First we show this is true for $n=1$. Trivially $\varphi(a^1) = \varphi(a) = \varphi(a)^1$.
$\varphi(a^1) = \varphi(a) = \varphi(a)^1$

Now suppose this holds for some $m \in \mathbb{N}$. We show this holds for $m+1$.
$\varphi(a^{m+1}) = \varphi(a^m a) = \varphi(a^m)\varphi(a) = \varphi(a)^m \varphi(a) = \varphi(a)^{m+1}$
Thus our propositions holds for $m+1$ whenever it holds for m

By the principle of mathematical induction,
$\varphi(a^n) = \varphi(a)^n \quad \forall n \in \mathbb{N}$.

Example:
We want to find all ring homomorphisms $\varphi : \mathbb{Z} \to \mathbb{Z}$.

Suppose φ is a ring homomorphism. Then (1)
$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) = \varphi(1)^2$.
By the properties of powers (& multiplication), we know $\varphi(1) = 0$ or $\varphi(1) = 1$.

Suppose $\varphi(1) = 0$. Then for all $z \in \mathbb{Z}$
$\varphi(z) = \varphi(1 \cdot z) = \varphi(1)\varphi(z) = 0$.
So φ is the constant function 0.

Suppose $\varphi(1) = 1$. Then by (iii) in our earlier theorem
$\varphi(z) = \varphi(z \cdot 1) = z \cdot \varphi(1) = z$
So φ is the identity function.

Thus the constant function 0 & the identity function are the only ring homomorphisms on $\mathbb{Z}$ to $\mathbb{Z}$.

Let's cover the ring analog of the First homomorphism theorem.

Thm:
Let R & R' be rings & $\varphi : R \to R'$ be a (ring) homomorphism. Let $\hat{\imath}$ denote the canonical homomorphism $R \to R/\ker(\varphi)$. Let $H' = \text{Range}(\varphi)$.

1) There exists monomorphism $\theta : R/\ker(\varphi) \to R'$ such that $\theta \circ \hat{\imath} = \varphi$

2) The range of θ is H' so $R/\ker(\varphi)$ is isomorphic H'.

3) In particular, if φ is onto R', then $R/\ker(\varphi)$ is isomorphic to R'.

Let's recall the definition of a canonical homomorphism.

Def:
Let R be a ring & I be an ideal of R. Define $\hat{\imath} : R \to R/I$ by
$\hat{\imath}(a) = I + a \quad \forall a \in R$

$\hat{\imath}$ is a ring homomorphism from R onto R/I w/ kernel I.
As before we call $\hat{\imath}$ the <u>canonical homomorphism</u> from R onto R/I.

How do we define <u>quotient rings</u> like R/I? Like so

<u>Def:</u> Quotient Rings
Let R be a ring & I be an ideal of R.
Let R/I denote the right (or left) cosets of I in R, that is
$R/I = \{I+a \mid \forall a \in R\}$.

From our work on quotient groups we know
$(I+a)+(I+b) = I+(a+b)$
is well defined.

We'd like to define
$(I+a)(I+b) = I+(ab)$.

We want this to be well-defined so if $I+a=I+c$ & $I+b=I+d$ then
$(I+a)(I+b)=(I+c)(I+d) \iff I+(ab)=I+(cd)$
This is true iff $ab-cd \in I$ (given $a-c \in I$ & $b-d \in I$).

<u>Pf:</u> Product is Well-Defined
Let $a,b,c,d \in I$ where
$a-c \in I$ & $b-d \in I$
or equivalently
$I+a=I+c$ & $I+b=I+d$.

Let $s_1 = a-c \in I$ & $s_2 = b-d \in I$. Then
$ab-cd = a(s_2+d)-cd$ $\quad (b=s_2+d)$
$= as_2+ad-cd$
$= as_2+(a-c)d$
$= as_2+s_1d$ $\quad (s_1=a-c)$
We know $as_2 \in I$ & $s_1d \in I$ b/c I is an ideal in R & $s_1, s_2 \in I$. Since I is closed under $+$, we know
$ab-cd = as_2+s_1d \in I$.

Thus $(I+a)(I+b)=I+(ab)$ is well defined $\forall a,b \in R$

Thm:
Let R be a ring & I be an ideal of R. Then
1) R/I is a ring.
2) If R is a commutative ring, then so is R/I.
3) If R is a ring w/ identity, then so does R/I.

Given that $R \neq I$ that is. If $R=I$, then $R/I = \{I\}$, which means $0=1$, which we don't allow by definition of 1.

We call R/I the quotient ring of R mod I.