Math UA 343

Section 5

Spring 2025

Christiana Mavroyiakoumou (cm4291@nyu.edu)

1

A big part of abstract algebra involves properties of integers and sets. We now collect the properties we need for future reference.

Well Ordering Principle: Every nonempty set of positive integers contains a smallest member.

Note. We say a nonzero integer t is a divisor of an integer s if there is an integer u s.t. $\boxed{s = tu}$.
We write $t \mid s$ (i.e. "t divides s"). When t is not a divisor of s we write $t \nmid s$. A prime is a positive integer greater than 1 whose only positive divisors are 1 and itself.
We say that an integer s is a multiple of an integer t if there is an integer u such that $\boxed{s = tu}$.

multiple of t — divisor of s

SETS AND EQUIVALENCE RELATIONS

SET THEORY

A set is a well-defined collection of objects; defined in a way that we can determine for any given object x whether or not x belongs to the set.

The objects that belong to a set are called its elements (or members).

Notation: • Capital letters such as A or X for sets
• If a is an element of the set A we write $a \in A$.

Usual ways to specify a set.

① List all of its elements inside a pair of braces

e.g. $X = \{x_1, x_2, \ldots, x_n\}$

for a set containing elements $x_1, x_2, \ldots, x_n$

② State the property that determines whether or not an object x belongs to the set.

$$X = \{x : x \text{ satisfies } P\}$$

if each $x \in X$ satisfies a certain property P.

<u>Example</u>. If E is the set of even positive integers, we can describe E by writing

either $E = \{2, 4, 6, \ldots\}$

or $E = \{x : x \text{ is an even integer and } x > 0\}$

We write $2 \in E$ to mean 2 is in the set E

$-3 \notin E$ to mean -3 is <u>not</u> in the set E.

Important sets we will consider:

$\mathbb{N} = \{n : n \text{ is a natural number}\} = \{1, 2, 3, \ldots\}$

$\mathbb{Z} = \{n . n \text{ is an integer}\} = \{\ldots, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q} = \{r : r \text{ is a rational number}\} = \{p/q : p, q \in \mathbb{Z} \text{ where } q \neq 0\}$

$\mathbb{R} = \{x : x \text{ is a real number}\}$

$\mathbb{C} = \{z : z \text{ is a complex number}\}$

<u>Relations between sets</u>

A set A is a subset of B $(A \subset B)$ if every element of A is also an element of B

e.g $\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8\}$

and $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

- Each set is a subset of itself.

- A set B is a proper subset of a set A if $B \subset A$ but $B \neq A$.

- If A is not a subset of B we write $A \not\subset B$, e.g. $\{4, 7, 9\} \not\subset \{2, 4, 5, 8, 9\}$

- Two sets are equal ($A=B$) if we can show that $A \subset B$ and $B \subset A$
- An empty set is a set with no elements in it ($\emptyset$). The empty set is a subset of every set.

Operations

- The union $A \cup B$ of two sets A and B is $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- The intersection $A \cap B$ of A and B is $A \cap B = \{x : x \in A \text{ and } x \in B\}$

e.g. If $A = \{1,3,5\}$ and $B = \{1,2,3,9\}$ then $A \cup B = \{1,2,3,5,9\}$
$A \cap B = \{1,3\}$

- We take the union and intersection of more than two sets

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \dots \cup A_n$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \dots \cap A_n$$

- When two sets have no elements in common, we call them disjoint ($A \cap B = \emptyset$)
  e.g. if E is the set of even integers and O is the set of odd integers then E and O are disjoint.

Sometimes we'll work within one fixed set U ← universal set

For any set $A \subset U$, we define the complement of A (written as A') to be the set

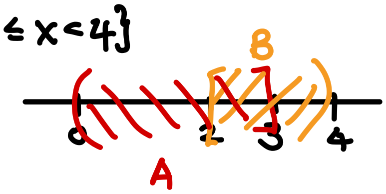
$$A' = \{x : x \in U \text{ and } x \notin A\}$$

The difference of two sets A and B is

$$A \setminus B = A \cap B' = \{x : x \in A \text{ and } x \notin B\}$$

Example. Let $\mathbb{R}$ be the universal set and suppose that

$$A = \{x \in \mathbb{R} : 0 < x \leq 3\} \text{ and } B = \{x \in \mathbb{R} : 2 \leq x < 4\}$$



Then
$$A \cap B = \{x \in \mathbb{R} : 2 \leq x \leq 3\}$$
$$A \cup B = \{x \in \mathbb{R} : 0 < x < 4\}$$
$$A \setminus B = \{x \in \mathbb{R} : 0 < x < 2\}$$
$$A' = \{x \in \mathbb{R} : x \leq 0 \text{ or } x > 3\}$$

Proposition 1 Let $A, B,$ and C be sets. Then

1. $A \cup A = A$, $\quad A \cap A = A$, $\quad A \setminus A = \emptyset$
2. $A \cup \emptyset = A$, $\quad A \cap \emptyset = \emptyset$
3. $A \cup (B \cup C) = (A \cup B) \cup C$, $\quad A \cap (B \cap C) = (A \cap B) \cap C$
4. $A \cup B = B \cup A$, $\quad A \cap B = B \cap A$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

In class we prove 1. and 3. and the rest will be given to you as exercises in your HW1

Proof 1.
$$A \cup A = \{x : x \in A \text{ or } x \in A\} = \{x : x \in A\} = A$$

and

$$A \cap A = \{x : x \in A \text{ and } x \in A\} = \{x : x \in A\} = A$$

$$A \setminus A = A \cap A' = \emptyset$$

Proof 3. For sets $A, B,$ and C

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x : x \in B \text{ or } x \in C\} \\ &= \{x : x \in A \text{ or } x \in B, \text{ or } x \in C\} \\ &= \{x : x \in A \text{ or } x \in B\} \cup C \\ &= (A \cup B) \cup C \end{aligned}$$

Similarly for $A \cap (B \cap C) = (A \cap B) \cap C$. $\square$

Theorem 1. De Morgan's laws

Let A and B be sets. Then

1. $(A \cup B)' = A' \cap B'$
2. $(A \cap B)' = A' \cup B'$

Proof. 1. If $A \cup B = \emptyset$ then the theorem follows immediately since both A and B are the empty set

Otherwise, we must show that $(A \cup B)' \subset A' \cap B'$ and $(A \cup B)' \supset A' \cap B'$

let $x \in (A \cup B)'$. Then $x \notin A \cup B$.

So x is neither in A nor in B, by the definition of the union of sets. By the definition of the complement, $x \in A'$ and $x \in B'$. Therefore, $x \in A' \cap B'$ and we have $(A \cup B') \subset A' \cap B'$

To show the reverse inclusion, suppose that $x \in A' \cap B'$. Then $x \in A'$ and $x \in B'$ $\Rightarrow$ $x \notin A$ and $x \notin B$. Thus $x \notin A \cup B$ and so $x \in (A \cup B)'$. Hence, this shows $(A \cup B)' \supset A' \cap B'$.

These two together imply $(A \cup B)' = A' \cap B'$.

$\square$

Cartesian products and mappings

Given two sets A and B we define a new set $A \times B$ $\leftarrow$ Cartesian product of A and B

as a set of ordered pairs.

That is:

$$\boxed{A \times B = \{(a, b) \quad a \in A \text{ and } b \in B\}}$$

Example. If $A = \{x, y\}$, $B = \{1, 2, 3\}$ and $C = \emptyset$ then

$$A \times B = \{(x,1), (x,2), (x,3), (y,1), (y,2), (y,3)\}$$

and $A \times C = \emptyset$

We define the Cartesian product of n sets to be

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) : a_i \in A_i \text{ for } i=1, \dots, n\}$$

Subsets of $A \times B$ are called relations.

We define a mapping or function $f \subset A \times B$ from a set A to a set B to be the special type of relation where each element $a \in A$ has a unique element $b \in B$ such that $(a,b) \in f$.

Equivalently, for every element in A, f assigns a unique element in B.

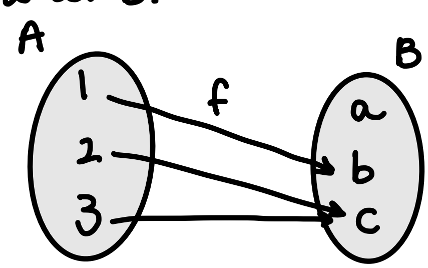
$f: A \to B$ or $A \xrightarrow{f} B$

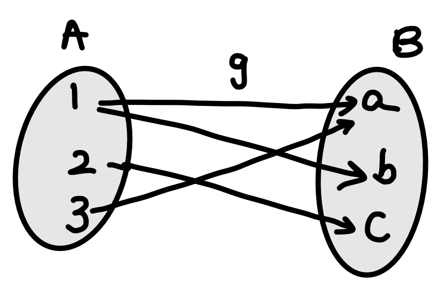
Instead of writing ordered pairs $(a,b) \in A \times B$ we write $f(a) = b$ or $f: a \mapsto b$.

The set A is called the domain of f and $\boxed{f(A) = \{f(a) : a \in A\} \subset B}$ is called the range or image of f.

[Note : We can think of the elements in the function's domain as input values and the elements in the function's range as output values.]

Example. Suppose $A = \{1,2,3\}$ and $B = \{a,b,c\}$. We define relations f and g from set A to set B.





The relation f is a mapping.

The relation g is not a mapping ← g is not because $1 \in A$ is not assigned to a unique element in B i.e. $g(1) = a$ & $g(1) = b$

Note. A relation is well-defined if each element in the domain is assigned to a unique element in the range.

- If $f: A \to B$ is a map and the image of f is B, i.e. $f(A) = B$ then f is said to be **onto** or **surjective**.

→ In other words, if $\exists$ an $a \in A$ for each $b \in B$ s.t. $f(a) = b$, then f is onto.

- A map is **one-to-one** or **injective** if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.

→ In other words, a function is one-to-one if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

ϕ is one-to-one ψ is not one-to-one ϕ is onto ψ is not onto

A map that is both onto and one-to-one is called **bijective**.

Example. Let $f: \mathbb{Z} \to \mathbb{Q}$ be defined as $\boxed{f(n) = n/1}$.

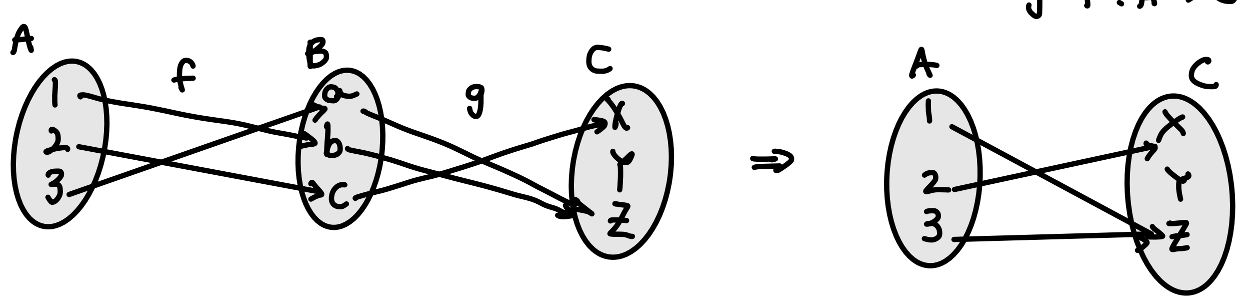
Then f is one-to-one but not onto   there is no n for which $f(n) = 3/4$ for example

Given two functions we can construct a new one by using the range of the first function as the domain of the second function. Let $f: A \to B$ and $g: B \to C$ be mappings. Define a new map, the **composition** of f and g from A to C by

$$\boxed{(g \circ f)(x) = g(f(x))}$$

Example. Composition of maps

$g \circ f : A \to C$



Example. let $f(x) = x^2$ and $g(x) = 2x + 5$ Then $(f \circ g)(x) = f(g(x)) = (2x+5)^2 = 4x^2 + 20x + 25$

and $(g \circ f)(x) = g(f(x)) = 2x^2 + 5$.

* The order matters! In most cases $f \circ g \neq g \circ f$

However, in some cases we could have $f\circ g = g\circ f$. Let $f(x)=x^3$ and $g(x)=\sqrt[3]{x}$. Then

$$(f\circ g)(x) = f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x$$

and $$(g\circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x.$$

__Example.__ Given a 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we can define a map $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$T_A(x,y) = (ax+by,\ cx+dy)$$

for any (x,y) in $\mathbb{R}^2$. This is matrix multiplication $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$

Maps from $\mathbb{R}^n$ to $\mathbb{R}^m$ given by matrices are called linear maps or linear transformations.

__Example.__ Suppose that $S=\{1,2,3\}$. Define a map $\pi : S \to S$ by

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

This is a bijective map. An alternative way of writing π is:

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

For any set S, a one-to-one and onto mapping $\pi : S \to S$ is called a permutation of S.

__Theorem 2.__ Let $f : A \to B$, $g : B \to C$ and $h : C \to D$. Then

1. The composition of mappings is associative, i.e. $(h\circ g)\circ f = h\circ(g\circ f)$.
2. If f and g are both one-to-one, then the mapping $g\circ f$ is one-to-one
3. If f and g are both onto, then the mapping $g\circ f$ is onto
4. If f and g are bijective, then so is $g\circ f$.

Part 4. follows directly from 2. and 3.

__Proof__ We prove 1. and 3. again.

1. We must show that $(h\circ g)\circ f = h\circ(g\circ f)$

For $a\in A$ we have (starting from the RHS) :
$$\begin{aligned}(h\circ(g\circ f))(a) &= (h(g\circ f)(a))\\ &= h(g(f(a)))\\ &= (h\circ g)(f(a))\\ &= ((h\circ g)\circ f)(a)\end{aligned}$$

3. Assume that f and g are both onto functions. Given $c \in C$, we must show that $\exists$ an $a \in A$ s.t. $(g \circ f)(a) = g(f(a)) = c$.

However since g is onto $\exists$ a $b \in B$ s.t. $g(b) = c$.
Similarly, $\exists$ an $a \in A$ s.t. $f(a) = b$. Accordingly

$$\begin{aligned}(g \circ f)(a) &= g(f(a)) \\ &= g(b) \\ &= c.\end{aligned}$$

$\square$

If S is any set we will use id_S or id to denote the identity mapping from S to itself. We define this map by $\boxed{id(s) = s}$ $\forall\, s \in S$

A map $g: B \to A$ is an inverse mapping of $f: A \to B$ if $g \circ f = id_A$ and $f \circ g = id_B$.

it "undoes" the function

A map is set to be invertible if it has an inverse. We use f^{-1} for the inverse of f.

Example. $f(x) = \ln(x)$ has inverse $f^{-1}(x) = e^x$ and vice versa (but we need to ensure that we carefully choose the domains).

Note that $f(f^{-1}(x)) = \ln(e^x) = x$

$f^{-1}(f(x)) = e^{\ln x} = x$

Example Suppose that $A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$. A defines a map from $\mathbb{R}^2$ to $\mathbb{R}^2$ by

$$T_A(x, y) = (3x + y,\ 5x + 2y).$$

We find the inverse map of T_A by inverting the matrix A $\boxed{T_A^{-1} = T_{A^{-1}}}$

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \Rightarrow T_A^{-1}(x, y) = T_{A^{-1}} = (2x - y,\ -5x + 3y)$$

Check that $T_A^{-1} \circ T_A(x, y) = T_A \circ T_A^{-1}(x, y) = (x, y)$

Theorem 3 A mapping is invertible if and only if it is both one-to-one and onto.

Proof. ($\Rightarrow$) Suppose that $f: A \to B$ is invertible with inverse $g: B \to A$. Then $g \circ f = id_A$ is the identity map. that is $\boxed{g(f(a)) = a}$

If $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$ then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. Thus f is one-to-one.

Now suppose that $b \in B$. To show that f is onto it's necessary to find an $a \in A$ s.t. $f(a) = b$ but $f(g(b)) = b$ with $g(b) \in A$. Let $a = g(b)$.

since f and g are inverses of each other

($\Leftarrow$)

Conversely, let f be bijective and let $b \in B$. Since f is onto, $\exists$ an $a \in A$ s.t. $f(a) = b$. Because f is one-to-one, a must be unique. Define g by letting $g(b) = a$.

We have now constructed the inverse of f

$g(b) = g(f(a)) = a$ ✓

□

Equivalence relations and partitions

We generalize equality with equivalence relations and equivalence classes.

An equivalence relation on a set X is a relation $R \subset X \times X$ such that

- $(x,x) \in R$ for all $x \in X$ — reflexive property
- $(x,y) \in R$ implies $(y,x) \in R$ — symmetric property
- (x,y) and $(y,z) \in R$ imply $(x,z) \in R$ — transitive property

Given an equivalence relation R on a set X we usually write $x \sim y$ instead of $(x,y) \in R$.

Example. Let p, q, r and s be integers with $q, s \neq 0$.

Define $\frac{p}{q} \sim \frac{r}{s}$ if $ps = qr$.

Clearly $\sim$ is reflexive and symmetric

$\frac{p}{q} \sim \frac{p}{q}$ if $pq = pq$ ✓ $\quad \frac{p}{q} \sim \frac{r}{s}$ if $ps = qr$ $\frac{r}{s} \sim \frac{p}{q}$ if $rq = ps$ ✓

To show that it is also transitive, suppose that $\frac{p}{q} \sim \frac{r}{s}$ and $\frac{r}{s} \sim \frac{t}{u}$ with $q, s, u \neq 0$

Then $\boxed{ps = qr}$ and $\boxed{ru = st}$. Thus $psu = qru = qst$

multiply $ps = qr$ with u → Subst. for $ru = st$

Since $s \neq 0$ $\quad s(pu) = qru = s(qt)$

Dividing by s we have $pu = qt$. Consequently, $\frac{p}{q} \sim \frac{t}{u}$.

Example Suppose that f and g are differentiable functions on $\mathbb{R}$. We can define an equivalence relation on such functions by letting $f(x) \sim g(x)$ if $f'(x) = g'(x)$.

$\sim$ is both reflexive and symmetric.

To show transitivity, suppose $f(x) \sim g(x)$ and $g(x) \sim h(x)$

$$\Rightarrow f'(x) = g'(x) \qquad g'(x) = h'(x)$$

Then $f(x) = g(x) + c_1$, $g(x) = h(x) + c_2$ where c_1, c_2 are constants.

$$f(x) = h(x) + c_1 + c_2$$

$$f(x) - h(x) = c_1 + c_2$$

$$f'(x) - h'(x) = 0$$

$$f'(x) = h'(x).$$

Thus $f(x) \sim h(x)$

$\square$

Given a nonempty set X, a partition of X is simply a collection of non-overlapping subsets whose union is the original set.

A partition $\mathcal{P}$ of a set X is a collection of nonempty sets $X_1, X_2, \ldots$ such that

$$\boxed{\bigcup_k X_k = X}$$

and $\boxed{X_i \cap X_j = \emptyset \text{ for } i \neq j}$

partition of S into 4 subsets

eg. the sets $\{0\}$, $\{1, 2, 3, \ldots\}$ and $\{\ldots, -3, -2, -1\}$ constitute a partition of the set of integers

Let $\sim$ be an equivalence relation on a set X and let $x \in X$.

Then $[x] = \{y \in X : y \sim x\}$ is called the equivalence class of x.

Theorem Given an equivalence relation $\sim$ on a set X, the equivalence classes of X form a partition of X.

Conversely, if $P = \{X_i\}$ is a partition of a set X, then there is an equivalence relation on X with equivalence classes X_i.

Proof Suppose that there exists an equivalence relation $\sim$ on the set X. For any $x \in X$, the reflexive property shows that $x \in [x]$ and so $[x]$ is nonempty. Clearly $X = \bigcup_{x \in X} [x]$

Now let $x, y \in X$. We need to show that either $[x] = [y]$ or $[x] \cap [y] = \emptyset$. Suppose that the intersection of $[x]$ and $[y]$ is not empty and that $z \in [x] \cap [y]$. Then $z \sim x$ and $z \sim y$. By symmetry $x \sim z$ and $y \sim z$

and by transitivity $x \sim y$

← since $[y] = \{x \in Y : x \sim y\}$

Hence $[x] \subset [y]$ since $[x] = \{y \in X : y \sim x\}$

(For $[y] \subset [x]$, $z \in [y] \cap [x]$

$z \in [y]$ and $z \in [x]$

$z \sim y$ $\quad$ $z \sim x$

(sym.) $y \sim z$ $\quad$ $x \sim z \Rightarrow$ (tran.) $y \sim x$)

Similarly we have $[y] \subset [x]$ and so $[x] = [y]$.

Thus any two equivalence classes are either disjoint $([x] \cap [y] = \emptyset)$ or exactly the same $([x] = [y])$

Conversely, suppose that $P = \{X_i\}$ is a partition of a set X. Let two elements be equivalent if they are in the same partition. The relation is reflexive. If x is in the same partition as y, then y is in the same partition as x so $x \sim y \Rightarrow y \sim x$. Finally, if x is in the same partition as y and y is in the same partition as z then x must be in the same partition as z and transitivity holds.

□

Example Let r and s be two integers and suppose that $n \in \mathbb{N}$. We say that r is congruent to s modulo n, if $r-s$ is divisible by n, i.e. $\boxed{r-s = nk \text{ for some } k \in \mathbb{Z}}$
$(s \bmod n)$

We write $\boxed{r \equiv s \pmod n}$

$41 \equiv 17 \pmod 8$ since $41-17 = 24$ is divisible by 8

We claim that congruence modulo n forms an equivalence relation of $\mathbb{Z}$.

Certainly any integer r is equivalent to itself since $r-r=0$ is divisible by n.

$r \equiv r \bmod n$

$r \sim r$

We now show that the relation is symmetric.

If $r \equiv s \pmod n$ then $r-s = -(s-r)$ is divisible by n

So $s-r$ is divisible by n and $s \equiv r \pmod n$.

Now suppose that $r \equiv s \pmod n$ and $s \equiv t \pmod n$

Then $\exists$ integers k and l s.t. $r-s = kn$ and $s-t = ln$

To show transitivity, we must show that $r-t$ is divisible by n.

$$\begin{aligned} r-t &= r-s+s-t \\ &= kn + ln \\ &= (k+l)n \end{aligned}$$

and so $r-t$ is divisible by n $\square$

- A nonempty subset S of $\mathbb{Z}$ is well-ordered if S contains a least element.

NOTE: The set $\mathbb{Z}$ is not well-ordered since it does not contain a smallest element. But the natural numbers are well-ordered.

Well-ordering principle: Every nonempty subset of the natural numbers is well-ordered

Section 2.2: The DIVISION ALGORITHM

Theorem 2.9 (Division algorithm) with $a>b$

Let a and b be integers, with $b>0$. Then $\exists$ unique integers q and r st

$$\boxed{a = bq + r}$$

where $0 \leq r < b$.

Proof [existence-and-uniqueness type of proof]

We must first show that the numbers q and r actually exist. Then we must show that they are unique: if q' and r' are two other such numbers, then $q=q'$ and $r=r'$

Existence of q and r. Let $S=\{a-bk : k\in\mathbb{Z} \text{ and } a-bk\geq 0\}$

If $0\in S$, then b divides a and we can let $q=\frac{a}{b}$ and $r=0$

remainder $a-bk$ is 0

If $0\notin S$ we can use the well-ordering principle (so there must be a smallest element)

We must show first that S is nonempty.

If $a>0$ then $a-b\cdot 0\in S \Rightarrow a\in S$

If $a<0$ then $a-b(2a)=a(1-2b)\in S$

if $a>0 \Rightarrow a-bk\geq 0$ & $k\in\mathbb{Z}$

take eg $k=0$

$\Rightarrow a\geq 0$

$\Rightarrow a\in S$

because it satisfies the properties of set S

choose eg $k=2a$ so that $1-2b<0$

In either case $S\neq\emptyset$.

By the well-ordering principle S must have a smallest member, say $r=a-bq$

Therefore $\boxed{a=bq+r,\ r\geq 0}$

we will use proof by contradiction

We must now show that $r<b$. We suppose that $r>b$. Then

$$a-b(q+1)=a-bq-b=r-b>0$$

work backwards

by assumption

In this case we would have $a-b(q+1)\in S$. But then $a-b(q+1)<a-bq$ which would contradict the fact that $r=a-bq$ is the smallest element of S. So by contradiction, $r\leq b$. Since $0\notin S$, $r\neq b$ and so $\boxed{r<b.}$

Uniqueness of q and r. Suppose $\exists$ integers $r, r', q,$ and q' s.t

$$a=bq+r,\quad 0\leq r<b \qquad (\dagger)$$

$$a=bq'+r',\quad 0\leq r'<b \qquad (\ddagger)$$

Then $bq+r=bq'+r'$ (‡)

Assume $r'\geq r$

From (‡) we have $bq - bq' = r' - r$

$$b(q-q') = r'-r$$

from (‡) we have $0 \le r < b$ and so $r'-r \le r'$

Thus b must divide $r'-r$ and $0 \le \overbrace{\underbrace{r'-r}_{} \le r'} < b$

from the assumption that $r' \geq r$ $\Rightarrow r'-r \geq 0$

since b must divide $r'-r$ but $r'-r$ is also $<b$

This is possible only if $r'-r = 0$

Hence $r' = r$ and $q = q'$. $\square$

↳ from (‡) then $bq + \cancel{r} = bq' + \cancel{r}$

$\Rightarrow q = q'$

Let a and b be integers. If $b = ak$ for some integer k we write $a \mid b$.

An integer d is called a common divisor of a and b if $d \mid a$ and $d \mid b$.

The greatest common divisor of a and b is a positive integer d s.t. d is a common divisor of a and b and if d' is any other divisor of a and b then $d' \mid d$.

We write $\gcd(24, 36) = 12$ and $\gcd(120, 102) = 6$

We say that two integers a and b are <u>relatively prime</u> if $\gcd(a,b) = 1$

<u>Theorem 2.10</u> Let a and b be nonzero integers. Then $\exists$ integers r and s s.t.

$$\gcd(a,b) = ar + bs.$$

Also the greatest common divisor of a and b is unique.

<u>Proof</u> Left as an exercise.

THE EUCLIDEAN ALGORITHM

<u>Example</u> Let's compute the greatest common divisor of 945 and 2415.

$$2415 = 945 \cdot 2 + 525$$
$$945 = 525 \cdot 1 + 420$$
$$525 = 420 \cdot 1 + 105$$
$$420 = 105 \cdot 4 + 0$$

Reversing these steps: 105 divides 420

$\Rightarrow$ 105 divides 525
105 // 945
105 // 2415

} 105 divides both 945 and 2415 so it's a common divisor

If d were another common divisor of 945 and 2415, then d would also have to divide 105. Thus $\gcd(945, 2415) = 105$.

Working backward through the sequence of equations, we can also obtain numbers r and s such that $\boxed{945r + 2415s = 105}$

$$
\begin{aligned}
105 &= 525 + (-1)\cdot 420 \\
&= 525 + (-1)(945 + (-1)\cdot 525) \\
&= 2\cdot 525 + (-1)\cdot 945 \\
&= 2\cdot[2415 + (-2)\cdot 945] + (-1)\cdot 945 \\
&= 2\cdot 2415 + (-5)\cdot 945
\end{aligned}
$$

Thus $r = -5$ and $s = 2$.

<u>Note</u> r and s are not unique, $r = 41$ and $s = -16$ would also work. □

To compute $\gcd(a,b) = d$ we use repeated divisions to obtain a decreasing sequence of positive integers $r_1 > r_2 > \dots > r_n = d$

$$
\Rightarrow \quad
\begin{aligned}
b &= aq_1 + r_1 \\
a &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\ \vdots \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= \underbrace{r_n}_{\text{divisor}} q_{n+1}
\end{aligned}
$$

$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

$\Rightarrow r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$

To find r and s s.t. $ar + bs = d$ we begin with the last eqn and subst. results obtained from the previous eqns

$$
\begin{aligned}
d &= r_n \\
&= r_{n-2} - r_{n-1}q_n \\
&= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\
&= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} \\
&\;\vdots \\
&= ra + sb
\end{aligned}
$$

The algorithm we used to find the greatest common divisor d of two integers a and b and to write d as a linear combination of a and b is known as the <u>Euclidean algorithm</u>.

Groups (Chapter 3)

We start with integer equivalence classes and symmetries

Applications: Cryptography, coding theory ...

Recall that two integers a and b are equivalent mod n if n divides $a-b$.

The integers mod n partition $\mathbb{Z}$ into n different equivalence classes, denoted as $\mathbb{Z}_n$

e.g. The integers mod 12 and the corresponding partition of the integers

$$
\begin{aligned}
[0] &= \{\ldots, -24, -12, 0, 12, 24, \ldots\} \\
[1] &= \{\ldots, -11, 1, 13, 25, \ldots\} \\
&\;\vdots \\
[11] &= \{\ldots, -13, -1, 11, 23, 35, \ldots\}
\end{aligned}
$$

<u>Example.</u> Integer arithmetic mod n. (arithmetic on $\mathbb{Z}_n$)

$7+4 \equiv 1 \mod 5$ — remainder when $7+4$ is divided by 5

$3+5 \equiv 0 \mod 8$

$3+4 \equiv 7 \mod 12$

addition

$7 \cdot 3 \equiv 1 \mod 5$ — remainder when $7 \cdot 3$ is divided by 5

$3 \cdot 5 \equiv 7 \mod 8$

$3 \cdot 4 \equiv 0 \mod 12$

multiplication

<u>Note</u> here we use eg 7 instead of [7] to indicate the equivalence class

Note that most of the usual laws of arithmetic hold for addition and multiplication in $\mathbb{Z}_n$, but not all. e.g. It is not necessarily true that there is a multiplicative inverse.

Example. Consider the multiplication table for $\mathbb{Z}_8$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Note 2, 4 and 6 do not have multiplicative inverses

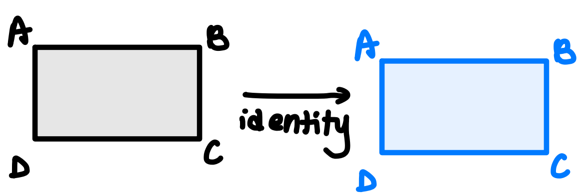
$\Rightarrow$ i.e. for $n = 2, 4, 6$ there is no integer k such that $kn \equiv 1 \pmod 8$

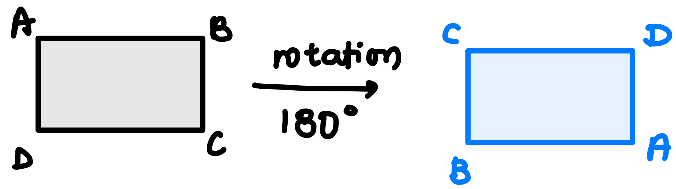
Symmetries

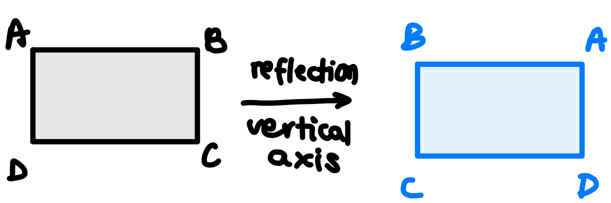
A **symmetry** of a geometric figure is a rearrangement of the figure keeping
(a) the arrangement of its sides and vertices
(b) its distances
(c) its angles

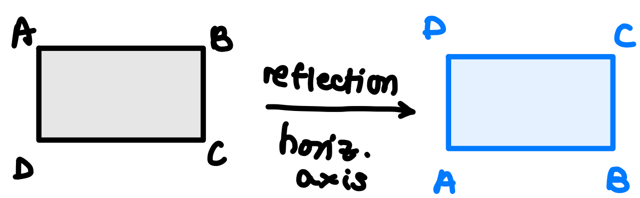
A map from the plane to itself preserving the symmetry of an object is called a *rigid motion.*

Example: Symmetries of a rectangle





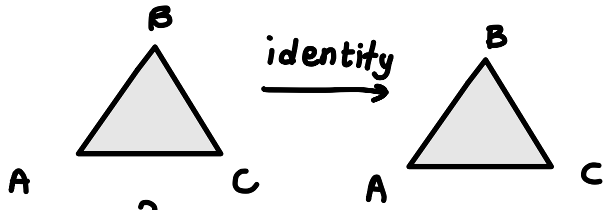




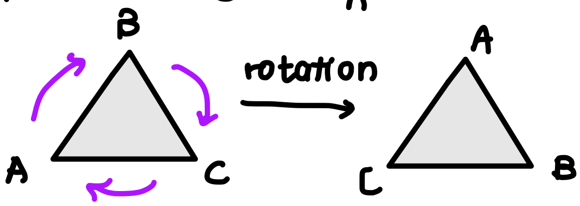
Note: a 90° rotation in either direction cannot be a symmetry unless the rectangle is a square.

Example. Symmetries of the equilateral triangle ΔABC.

recall permutations from earlier



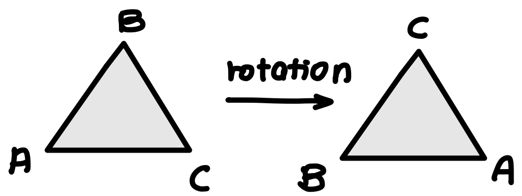
$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$



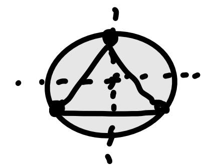
$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

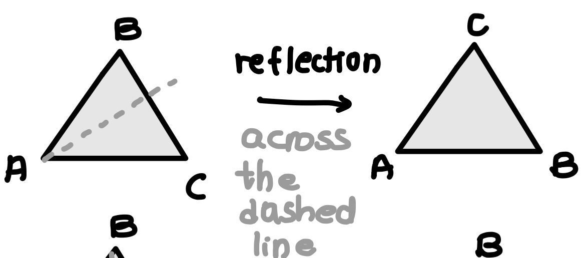
$120°$ in the clockwise direction

To denote the permutation of the vertices of an equilateral triangle that sends A to B, B to C, and $C \to A$ we write the array above



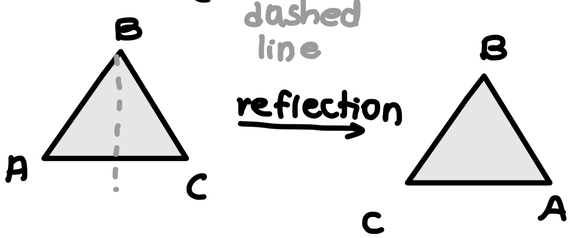
$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$



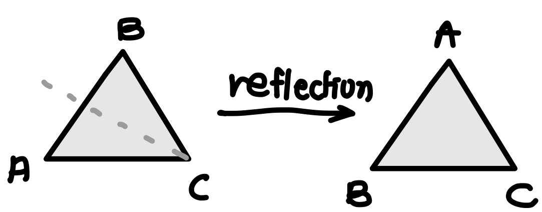


$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

1 identity
2 rotations
3 reflections



$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$



$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

A permutation of a set S is a one-to-one and onto map $\pi : S \to S$

The three vertices have $3! = 3 \cdot 2 \cdot 1 = 6$ permutations

3 different possibilities for the 1st vertex
2 remaining " for the 2nd vertex
1 " possibility for the 3rd vertex

$\Rightarrow$ the triangle has at most 6 symmetries.

Every permutation gives rise to a symmetry of the triangle

Q What happens if one motion of the triangle is followed by another?

Notation: $\mu_1\rho_1 \rightarrow$ first do permutation ρ_1
example then apply permutation μ_1

This is composition of functions so we go right to left

vertex

$$(\mu_1\rho_1)(A) = \mu_1(\rho_1(A)) = \mu_1(B) = C$$
$$(\mu_1\rho_1)(B) = \mu_1(\rho_1(B)) = \mu_1(C) = B$$
$$(\mu_1\rho_1)(C) = \mu_1(\rho_1(C)) = \mu_1(A) = A$$

see where $\mu_1\rho_1$ sends each of the vertices

$$\mu_1\rho_1 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = \mu_2$$

Now let's do the opposite and consider instead the symmetry $\rho_1\mu_1$

$$(\rho_1\mu_1)(A) = \rho_1(\mu_1(A)) = \rho_1(A) = B$$
$$(\rho_1\mu_1)(B) = \rho_1(\mu_1(B)) = \rho_1(C) = A$$
$$(\rho_1\mu_1)(C) = \rho_1(\mu_1(C)) = \rho_1(B) = C$$

$$\rho_1\mu_1 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = \mu_3$$

Thus, $\mu_1\rho_1 \neq \rho_1\mu_1$

If you continue this exercise for all 6 permutation combinations you can fill in a multiplication table for the symmetries of an equilateral triangle as follows

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Notice how orderly it looks! NOT A COINCIDENCE

1. It has been completely filled w/o introducing new motions
   This is because any sequence of motions turns out to be the same as one of these 6.

   Algebraically this says that if A and B are in this "group" then so is AB. This property is called closure

2. If A is any element of this group then $A \circ id = id \circ A = A$
   Thus combining any element on either side with id yields A back again.

   An element id with this property is called an identity, and every group must have one

3. For each element A in the group, there is one element B in the same group such that $AB = BA = id$

   B is said to be the inverse of A and vice versa

4. Every element in the table appears exactly once in each row and each column.

5. Observe that AB may or may not be the same as BA

   If it happens that $AB = BA$ for all choices of group elements A and B we say the group is commutative or Abelian.
   Otherwise we say the group is non-Abelian

The integers mod n ($\mathbb{Z}_n$) and the symmetries of a rectangle or a group are all examples of groups.

A binary operation or law of composition on a set G is a function $G \times G \to G$ that assigns to each pair $(a,b) \in G \times G$ a unique element $a \circ b$ or ab in G, called the composition of a and b

---

A group $(G, \circ)$ is a set G together with a law of composition $(a,b) \mapsto a \circ b$ that satisfies the following axioms.

- The law of composition is associative

$$(a \circ b) \circ c = a \circ (b \circ c) \quad \text{for all } a, b, c \in G$$

- There exists an element $e \in G$, the identity element, s.t.

$$e \circ a = a \circ e = a \quad \text{for all } a \in G$$

- For each $a \in G$, $\exists$ an inverse element in G denoted by a^{-1}, s.t

$$a \circ a^{-1} = a^{-1} \circ a = e$$

The concept of closure says that any pair of elements can be combined w/o going outside the set. ⚠ Be sure to verify closure when testing for a group

---

A group G w/ the property that $a \circ b = b \circ a$ $\forall a, b \in G$ is called abelian or commutative. Otherwise they are said to be nonabelian or noncommutative

Example. The integers $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$ form a group under the operation of addition.

Binary operation on two integers $m, n \in \mathbb{Z}$ is just their sum

Identity $= 0$

Inverse of $n \in \mathbb{Z}$ is $-n$

Note that the set of integers under addition satisfies $\boxed{m+n = n+m}$ and so it is an abelian group.

- Sometimes it's convenient to describe a group in terms of an addition or multiplication table which we call a Cayley table

<u>Proposition 3.4</u> Let $\mathbb{Z}_n$ be the set of equivalence classes of the integers mod n and $a, b, c \in \mathbb{Z}_n$.

(1) Addition and multiplication are commutative:

$$\boxed{\begin{array}{c} a+b \equiv b+a \pmod{n} \\ ab \equiv ba \pmod{n} \end{array}}$$

(2). They are both associative

$$\boxed{\begin{array}{c} (a+b)+c \equiv a+(b+c) \pmod{n} \\ (ab)c \equiv a(bc) \pmod{n} \end{array}}$$

(3). There are both additive and multiplicative identities

$$\boxed{\begin{array}{c} a+0 \equiv a \pmod{n} \\ a \cdot 1 \equiv a \pmod{n} \end{array}}$$

(4) Multiplication distributes over addition:

$$\boxed{a(b+c) \equiv ab+ac \pmod{n}}$$

(5) For every integer a there is an additive inverse $-a$

$$\boxed{a+(-a) \equiv 0 \pmod{n}}$$

a and n are relatively prime or coprime

(6). Let a be a nonzero integer. Then $\gcd(a,n)=1$ if and only if there exists a multiplicative inverse b for $a \pmod{n}$. I.e. a nonzero integer b such that

$$ab \equiv 1 \pmod{n}$$

<u>Proof</u> (6) ($\Rightarrow$)

Suppose that $\gcd(a,n)=1$ Then $\exists$ integers r and s s.t

$$ar + ns = 1$$ by theorem 2.10

$$\Rightarrow \quad ns = 1 - ar$$

Then $ar \equiv 1 \pmod{n}$ $\quad \to n$ divides $1-ar$ thus $ar \equiv 1 \mod n$

Letting b be the equivalence class of r, $ab \equiv 1 \pmod{n}$.

($\Leftarrow$) Suppose $\exists$ an integer b s.t $ab \equiv 1 \pmod{n}$

$\Rightarrow$ n divides $ab-1$

Thus there is an integer k s.t. $ab - 1 = nk$

$\Rightarrow$ $ab - nk = 1$

Let $\gcd(a,n) = d$. Since d divides $ab-nk$, d must also divide 1.
Therefore $d=1$

$\square$

<u>Example</u> Not every set with a binary operation is a group.

If the binary operation on $\mathbb{Z}_n$ is the modular multiplication, then $\mathbb{Z}_n$ is <u>not</u> a group.

Group identity : 1

since $1 \cdot k = k \cdot 1 = k$ for any $k \in \mathbb{Z}_n$

★ A multiplicative inverse for 0 does <u>not</u> exist since $0 \cdot k = k \cdot 0 = 0$ for every $k \in \mathbb{Z}_n$

Even the set $\mathbb{Z}_n \setminus \{0\}$ is <u>not</u> a group.

e.g. let $2 \in \mathbb{Z}_6$

·	0	1	2	3	4	5
0						
1						
2				. . .		
3						
4						
5						

Then 2 has no multiplicative inverse since

$0 \cdot 2 = 0$, $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 0$, $4 \cdot 2 = 2$, $5 \cdot 2 = 4$

By proposition 3.4, every nonzero k has an inverse in $\mathbb{Z}_n$ if k is relatively prime to n

$\gcd(k,n)=1$

Denote the set of all <u>such</u> nonzero elements in $\mathbb{Z}_n$ by $U(n)$

group of units of $\mathbb{Z}_n$

Cayley table for $U(8)$

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Example The subset $\{1, -1, i, -i\}$ of $\mathbb{C}$ is a group under complex multiplication

Inverse of 1 : 1   Identity is 1
Inverse of -1 : -1
" $-i$: i
" i : $-i$

Example The set S of positive irrational numbers together with 1, under multiplication satisfies the three properties given in the definition of a group but it is not a group

Take $\sqrt{3} \cdot \sqrt{3} = 3$ for example. So S is not closed under multiplication.

fails the closure criterion!

Example We denote the set of all 2×2 matrices by $M_2(\mathbb{R})$.

Let $GL_2(\mathbb{R})$ to be the subset of $M_2(\mathbb{R})$ consisting of invertible matrices

i.e. A matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ if $\exists$ a matrix A^{-1} s.t. $AA^{-1} = A^{-1}A = \underset{\substack{\uparrow \\ 2\times 2 \text{ identity matrix}}}{I}$

For A to have an inverse it's equivalent to requiring that $\det(A) \neq 0$
$\Leftrightarrow ad - bc \neq 0$

The set of invertible matrices forms a group called the general linear group

Identity : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Inverse of $A \in GL_2(\mathbb{R})$: $A^{-1} = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

The product of two invertible matrices is also invertible. $\det(AB) = \det(A)\det(B) \neq 0$

Matrix multiplication is associative.

Note In general $AB \neq BA$ so $GL_2(\mathbb{R})$ is a nonabelian group.

$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$

//

Definition A group is finite (or has finite order) if it contains a finite number of elements otherwise it's said to be infinite.

Definition The order of a finite group is the number of elements that it contains. If the # of elements it contains is n then we write $\boxed{|G|=n}$

e.g. $\mathbb{Z}_5$ is a finite group of order 5

The integers $\mathbb{Z}$ form an infinite group under addition and we write $|\mathbb{Z}|=\infty$.

Note

We can use exponential notation for groups

If G is a group and $g \in G$ then we define $g^0 = e$

For any $n \in \mathbb{N}$ we define $g^n = \underbrace{g \cdot g \cdots \cdot g}_{n \text{ times}}$ and $g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{n \text{ times}}$

Definition The order of an element g in a group G is the smallest positive integer n such that $\boxed{g^n = e}$. If no such integer exists, we say g has infinite order.

The order of an element g is denoted by $|g|$.

So to find the order of a group element g, you need only compute the sequence of products $g, g^2, g^3, \ldots$ until you reach the identity for the 1st time. The exponent of this product is the order of g

Example Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication modulo 15. This group has order 8.

To find the order of element 7, say, we compute the sequence

$7^1 = 7,\ 7^2 = 4,\ 7^3 = 13,\ 7^4 = 1$ so $|7| = 4$

To find the order of 11, we compute

$11^1 = 11,\ 11^2 = 1,$ so $|11| = 2$

Similar computations show that $|1| = 1$, $|2| = 4$, $|4| = 2$, $|8| = 4$, $|13| = 4$ and $|14| = 2$.

Do you see a trick that makes these calculations easier?

Rather than computing the sequence $13^1, 13^2, 13^3, \ldots$ we may observe that

$$13 = -2 \mod 15$$

Thus
$$13^2 = (-2)^2 = 4 \mod 15$$
$$13^3 = (-2)(4) = -8 \mod 15$$
$$13^4 = (-2)(-8) = -16 = 1 \mod 15$$

Properties of groups

Prop. 3.17 $\boxed{\text{The identity element in a group } G \text{ is unique}}$

I.e. In a group G there is only one element $e \in G$ s.t $eg = ge = g$ for all G

Proof Suppose e and e' are both identities

$$\Rightarrow \quad eg = ge = g$$
$$\text{and} \quad e'g = ge' = g$$

To show that e is unique we must show that $e = e'$.
If e is the identity then $ee' = e'$, and if e' is also the identity then $ee' = e$
Together this gives us $e = e'$.

$\square$

Prop 3.18 $\boxed{\text{If } g \text{ is any element in a group } G \text{ then the inverse of } g \text{, written as } g^{-1} \text{ is unique.}}$

Proof Similar to the previous proof, assume that g' and g'' are both inverses of an element $g \in G$, then

$$\left.\begin{aligned} &(\dagger)\; gg' = g'g = e \\ \text{and}\quad &(\ddagger)\; gg'' = g''g = e \end{aligned}\right\} \text{ from the def}^n \text{ of an inverse}$$

We wish to show that $g' = g''$. We know that

$$\begin{aligned} g' &= g'e \\ &= g'(gg'') \quad \text{from } (\ddagger) \\ &= (g'g)g'' \\ &= eg'' \\ &= g'' \end{aligned}$$

$\square$

Prop. 3.19 Let G be a group. If $a, b \in G$ then $\boxed{(ab)^{-1} = b^{-1}a^{-1}}$

Def^n of inverse is c s.t. $dc = e$, $cd = e$

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

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

Proof Let $a, b \in G$. Then $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$

Also $b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$

Since inverses are unique by prop. 3.18 we have that $(ab)^{-1} = b^{-1}a^{-1}$ $\square$

Prop. 3.20 Let G be a group. For any $a \in G$, $\boxed{(a^{-1})^{-1} = a}$

Proof Left as an exercise.

Prop. 3.22 Cancellation

In a group G, the right and left cancellation laws hold, that is

$$\begin{aligned} &ba = ca \Rightarrow b = c \\ \text{and}\quad &ab = ac \Rightarrow b = c \end{aligned}$$

Proof Suppose $ba = ca$

Let a' be the inverse of a. Then multiplying on the right by a' gives

$$(ba)a' = (ca)a'$$
$$b(aa') = c(aa') \quad \text{by associativity}$$
$$be = ce \quad \text{by defn of inverse}$$
$$b = c \quad \text{by defn of identity}$$

Similarly, one can prove that $ab = ac \Rightarrow b = c$ by multiplying by a' on the left.

Note A consequence of the cancellation property is that in a Cayley table for a group each group element occurs exactly once in each row and column. (search "Latin square")

//

Theorem 3.23 For all $g, h \in G$

1. $g^m g^n = g^{m+n} \ \forall m, n \in \mathbb{Z}$
2. $(g^m)^n = g^{mn} \ \forall m, n \in \mathbb{Z}$
3. $(gh)^n = (h^{-1}g^{-1})^{-n} \ \forall n \in \mathbb{Z}$. If G is abelian then $(gh)^n = g^n h^n$.

Section 3.3 SUBGROUPS

Defn If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

Notation: $H \leq G$ means H is a subgroup of G.

If we want to indicate that H is a subgroup of G but it's not equal to G itself, we write $H < G$ and we call it a proper subgroup

Note The subgroup $\{e\}$ is called the trivial subgroup of G

$\mathbb{Z}_n$ under addition modulo n is **not** a subgroup of $\mathbb{Z}$ under addition since addition mod n is not the operation of $\mathbb{Z}$.

Subgroup tests

Prop. 3.30 A subset H of G is a subgroup if and only if it satisfies the following 3 conditions:

1. The identity e of G is in H
2. If $h_1, h_2 \in H$ then $h_1 h_2 \in H$.
3. If $h \in H$ then $h^{-1} \in H$.

Proof ($\Rightarrow$) Suppose that H is a subgroup of G

We want to show that the 3 conditions hold.

① Since H is a group, it must have an identity, e_H. But we must show that $e_H = e$, with e = identity of G

Since they are both identities we have

$$e_H e_H = e_H \qquad (e_H \text{ is an identity})$$

$$e e_H = e_H e = e_H \qquad (e \text{ is an identity})$$

Thus, equating them gives

$$e_H e_H = e e_H$$

$$\Rightarrow \quad e = e_H \qquad \text{(by the right-hand cancellation)}$$

② The second condition holds since a subgroup H is a group. (closure property)

③ To prove the 3rd condition let $h \in H$. Since H is a group, there is an element $h' \in H$ such that $hh' = h'h = e$.

Since the inverse in G is unique, $h' = h^{-1}$.

($\Leftarrow$) If the 3 conditions hold, we must show that H is a group under the same operation as G. These conditions and the associativity of the binary operation are the axioms stated in the definition of a group $\square$

<u>Prop 3.31</u> Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$ and when $g, h \in H$ then $gh^{-1} \in H$.

<u>Proof</u> ($\Rightarrow$) Assume H is a subgroup of G.
We want to show that $gh^{-1} \in H$ when $g, h \in H$.
Since $h \in H$, $h^{-1} \in H$ from property ③ of prop. 3.30
By the closure property of the group operation we have $gh^{-1} \in H$.

($\Leftarrow$) Suppose H is a subset of G s.t. $H \neq \emptyset$ and $gh^{-1} \in H$ when $g, h \in H$.
We want to show that H is a subgroup (i.e. show ①–③ of prop. 3.30 hold)
We must show $e \in H$ Since H is nonempty, we may pick some $x \in H$.
Then letting $g = x$ and $h = x$ also (in the hypothesis) we have

$$gh^{-1} \in H \Rightarrow xx^{-1} \in H$$
$$\Rightarrow e \in H$$

We must show $x^{-1} \in H$ whenever $x \in H$. Choose $g = e$ and $h = x$ in the statement
Then $gh^{-1} = ex^{-1} = x^{-1} \in H$

We must show that H is closed, i.e. If $x, y \in H$ then $xy \in H$
We already showed that $h_2^{-1} \in H$ whenever $h_2 \in H$
So letting $g = h_1$ and $h = h_2^{-1}$ we have $gh^{-1} = h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$

Thus, H is a subgroup of G

$\square$

Example

Consider the set of nonzero real numbers $\mathbb{R}^*$ with the group operation of multiplication.

- Identity is 1
- Inverse of any element $a \in \mathbb{R}^*$ is $\frac{1}{a}$

We will show that $\mathbb{Q}^* = \{\frac{p}{q} : p$ and q are nonzero integers$\}$ is a subgroup of $\mathbb{R}^*$

- The identity of $\mathbb{R}^*$ is in $\mathbb{Q}^*$.
- Given two elements in $\mathbb{Q}^*$, e.g. $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}^*$, their product $\frac{pr}{qs} \in \mathbb{Q}^*$ also
- The inverse of any element $\frac{p}{q} \in \mathbb{Q}^*$ is again in $\mathbb{Q}^*$ since $\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}$.
- Since multiplication in $\mathbb{R}^*$ is associative, multiplication in $\mathbb{Q}^*$ is associative

Example Let $SL_2(\mathbb{R})$ be the subset of $GL_2(\mathbb{R})$ consisting of matrices of determinant 1. That is, a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ exactly when $ad-bc=1$.

To show that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$ we must show that it is a group under matrix multiplication.

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$ since $\det(I) = 1$

$$A^{-1} = \frac{1}{\underbrace{\cancel{ad-bc}}_{=1}} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbb{R}) \text{ since } \det(A^{-1}) = da - (-c)(-b) = ad - bc = 1$$

Finally, we must show that multiplication is closed. Ie, the product of two matrices of determinat 1 also has det 1.

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1 \quad ✓$$

The group $SL_2(\mathbb{R})$ is called the special linear group.

<u>Note</u> A subset H of a group G can be a group without being a subgroup of G. For H to be a subgroup of G it must have G's binary operation

<u>Example</u> The set of all 2x2 matrices $\mathbb{M}_2(\mathbb{R})$ is a group under addition

$GL_2(\mathbb{R}_2)$ is a subset of $\mathbb{M}_2(\mathbb{R})$ and is a group under matrix multiplication but it is <u>not</u> a subgroup of $\mathbb{M}_2(\mathbb{R})$.

If we add two invertible matrices, we do <u>not necessarily</u> get another invertible matrix

e.g. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin GL_2(\mathbb{R})$.

CHAPTER 4 : Cyclic groups

Section 4.1. Cyclic subgroups

Sometimes a subgroup will depend on a single element of the group.

i.e. knowing that particular element will allow us to compute any other element in the subgroup

<u>Example</u> Consider $3 \in \mathbb{Z}$ and look at all multiples of 3 (both +ve and -ve)

This set is $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

Let's check that $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Identity : $+0$

Inverse : $a \in 3\mathbb{Z} \Rightarrow -a$ is the inverse

Closure ✓

This subgroup is completely determined by the element 3 since we can obtain all of other elements of the group by taking multiples of 3.

Every element in the subgroup is "generated" by 3.

Theorem 4.3 Let G be a group and a be any element in G. Then the set

$$\boxed{\langle a\rangle = \{a^k . k\in\mathbb{Z}\}}$$

is a subgroup of G.

Proof. • The identity is in $\langle a\rangle$ since $a^0 = e$

• The set $\langle a\rangle$ is closed under multiplication since if $a^m, a^n \in \langle a\rangle$, for $m, n\in\mathbb{Z}$, then $a^m a^n = a^{m+n} \in \langle a\rangle$.

• If $g = a^n \in \langle a\rangle$ then the inverse $g^{-1} = (a^n)^{-1} = a^{-n} \in \langle a\rangle$

Any subgroup H of G containing a must contain all the powers of a by closure. Thus H contains $\langle a\rangle$. $\square$

Note If we are using addition, as in the case of the integers under addition, we write $\langle a\rangle = \{na : n\in\mathbb{Z}\}$.

The subgroup $\langle a\rangle$ is called the cyclic subgroup of G generated by a. In the case that $G = \langle a\rangle$, we say that G is cyclic and that a is a generator of G. Note that a cyclic group may have many generators.

Also, since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$, every cyclic group is abelian.

Example In $U(10)$ we have the elements $\{1, 3, 7, 9\}$ $\quad a\in\mathbb{Z}_n$ s.t. $\gcd(a, n) = 1$

This is also $\langle 3\rangle$. $\boxed{3 \text{ is a generator of } U(10)}$

$3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$, $3^5 = 3^4\cdot 3 = 1\cdot 3$, $3^6 = 3^5\cdot 3 = 3\cdot 3 = 9, \ldots$

Example $\mathbb{Z}$ is cyclic

Consider the group $\mathbb{Z}$, using the standard operation of addition of integers. Since the operation is denoted additively rather than multiplicatively, we must consider multiples rather than powers. Thus $\mathbb{Z}$ is cyclic if and only if $\exists$ an integer a s.t $\boxed{\mathbb{Z} = \{ na : n \in \mathbb{Z} \}}$ Either $a = 1$ or $a = -1$ will satisfy the condition. so $\mathbb{Z}$ is cyclic with generators 1 or -1.

Example. $\mathbb{Z}_n$ is cyclic

The additive group $\mathbb{Z}_n$ of integers modulo n is also cyclic generated by $[1]$, since each congruence class can be expressed as a finite sum of $[1]$'s. Precisely, $[k] = k[1]$.

It is interesting to determine all possible generators of $\mathbb{Z}_n$.
If $[a]$ is a generator of $\mathbb{Z}_n$, then in particular $[1]$ must be a multiple of $[a]$. On the other hand, if $[1]$ is a multiple of $[a]$, then certainly every other congruence class mod n is also a multiple of $[a]$. Thus, to determine all of the generators of $\mathbb{Z}_n$ we only need to determine the integers a s.t. some multiple of a is congruent to 1. These are precisely the integers that are relatively prime to n, $\gcd(a, n) = 1$.

The elements of $\mathbb{Z}_6$ are $\{0, 1, 2, 3, 4, 5\}$. $\mathbb{Z}_6$ is a group under addition.
Is 5 a generator of $\mathbb{Z}_6$? $\langle 5 \rangle = \{ k5 : k \in \mathbb{Z} \}$

$$5(1) = 5, \quad \underset{\text{mod } 6}{5(2) = 4}, \quad 5(3) = 3, \quad 5(4) = 2, \quad 5(5) = 1$$

Is 3 a generator of $\mathbb{Z}_6$? $3(1) = 3$, $3(2) = 0$, $3(3) = 3$, $3(4) = 0, \cdots$ $\langle 3 \rangle = \{0, 3\}$
The cyclic subgroup generated by 3 is $\langle 3 \rangle = \{0, 3\}$ No!

Example Sometimes $(\mathbb{Z}_n, \times) = U(8)$ is cyclic sometimes not.

First consider $(\mathbb{Z}_5, \times)$. We have $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$, $[2]^4 = [1]$

Thus, each element of $(\mathbb{Z}_5, \times)$ is generated from $[2]$ (i.e. each element of $U(5)$ is a power of $[2]$) showing that the group is cyclic. We write $U(5) = \langle [2] \rangle$.

You can also show that $[3]$ is a generator

But note that $[4]$ is not a generator, since $[4]^1 = [4]$, $[4]^2 = [1]$, $[4]^3 = [4]$, ...

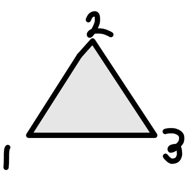
Thus $\langle [4] \rangle = \{[1], [4]\} \neq \mathbb{Z}_5^{\times}$.

Next, consider $\mathbb{Z}_8^{\times} = \{[1], [3], [5], [7]\} = U(8)$

The square of each element is the identity, so we have $\langle [3] \rangle = \{[1], [3]\}$

$\langle [5] \rangle = \{[1], [5]\}$ and $\langle [7] \rangle = \{[1], [7]\}$. So $U(8)$ is not cyclic

Example S_3 — the group of symmetries of an equilateral triangle — is not cyclic



Let's recall the symmetries, there are 6 of them.

$id = (1)$

$\rho_1 = (1,2,3)$

$\rho_2 = (1,3,2)$

$\mu_1 = (2,3)$

$\mu_2 = (1,3)$

$\mu_3 = (1,2)$.

The subgroups are

$\langle (1) \rangle = \{(1)\}$

$\langle (1,2,3) \rangle = \{(1), (1,2,3), (1,3,2)\} = \langle (1,3,2) \rangle$

$\langle (2,3) \rangle = \{(1), (2,3)\}$

$\langle (1,3) \rangle = \{(1), (1,3)\}$

$\langle (1,2) \rangle = \{(1), (1,2)\}$.

CYCLE NOTATION for permutations. We'll study this later, in detail.

Since no cyclic subgroup is equal to all of S_3, it is not cyclic.

That is, we have shown that there is no permutation σ in S_3 s.t. $S_3 = \langle \sigma \rangle$.

<u>Proposition</u> Let G be a group and let $a \in G$.
If K is any subgroup of G s.t. $a \in K$, then $\langle a \rangle \subseteq K$.

<u>Proof</u> If K is any subgroup that contains a, then it must contain all positive powers of a since it is closed under multiplication.
It also contains $a^0 = e$ and if $n<0$ then $a^n \in K$ since $a^n = (a^{-n})^{-1}$.
Thus $\langle a \rangle \subseteq K$. □

<u>Example</u> In the multiplicative group $(\mathbb{C}, \times)$, consider the powers of i.
We have $i^2 = -1$, $i^3 = -i$, $i^4 = 1$.
From this point on, the powers repeat, since $i^5 = ii^4 = i$, $i^6 = ii^5 = -1$, etc
For negative powers we have $i^{-1} = \frac{1}{i} \cdot \frac{i}{i} = -i$, $i^{-2} = -1$, and $i^{-3} = i$. Again, from this point on the powers repeat.
Thus, we have

$$\langle i \rangle = \{1, i, -1, -i\}$$

The situation changes when we consider $\langle 2i \rangle$ In this case the powers of $2i$ are all distinct, and the subgroup generated by $2i$ is <u>infinite</u>

$$\langle 2i \rangle = \left\{ \dots, \frac{1}{16}, \frac{1}{8}i, -\frac{1}{4}, -\frac{1}{2}i, 1, 2i, -4, -8i, 16, 32i, \dots \right\}$$

<u>Theorem 4.10</u> Every subgroup of a cyclic group is cyclic.

<u>Proof</u> We'll use the division algorithm & the Principle of well-ordering

Let G be a cyclic group generated by a. So $G = \langle a \rangle$.
Suppose also that H is a subgroup of G. If $H = \{e\}$, then H is cyclic trivially, $H = \langle e \rangle$
Suppose that H contains some element g, $g \neq e$. Then it can be written as $g = a^n$ for $n \in \mathbb{Z}$ $(n \neq 0)$. Since H is a subgroup, $g^{-1} = (a^n)^{-1} = a^{-n} \in H$, also.
Since H contains both a^n and a^{-n}, we can assume that H contains some power a^k with $k > 0$. Let m be the smallest natural number s.t. $a^m \in H$.

[We know by the Well-ordering principle that such an m exists.]

Well Ordering Principle: Every nonempty set of positive integers contains a smallest member.

We claim that $h = a^m$ is a generator for H.

Thus we must show that every $h' \in H$ can be written as a power of h.

Since $h' \in H$ and H is a subgroup of G, $\boxed{h' = a^k}$ for $k \in \mathbb{Z}$.

since $G = \langle a \rangle$

Using the division algorithm, we can find numbers q and r s.t.

$$k = mq + r \quad \text{where } 0 \le r < m$$

Thus

$$\begin{aligned} a^k &= a^{mq+r} \\ &= a^{mq} a^r \\ &= (a^m)^q a^r \\ &= h^q a^r \end{aligned}$$

Thus $a^k = h^q a^r \Rightarrow a^r = a^k h^{-q}$

Since a^k and h^{-q} are in H, a^r must also be in H. This contradicts the definition of a^m as the smallest positive power of a in H unless $r = 0$.

Thus, $k = mq \Rightarrow h' = a^k = a^{mq} = (a^m)^q = h^q \in \langle a^m \rangle$. from $0 \le r < m$

Thus $H = \langle a^m \rangle$ and so H is cyclic. $\square$

Prop 4.12 Let G be a cyclic group of order n and suppose that a is a generator of G. Then $a^k = e \Leftrightarrow n \mid k$.

[The order of an element in a cyclic group is the same as the order of the group]

Proof $(\Rightarrow)$ Suppose that $a^k = e$. By the division algorithm,

$$k = nq + r \quad \text{where } 0 \le r < n$$

Thus

$$e = a^k = a^{nq+r} = a^{nq} a^r = e a^r = a^r$$

since G is of order n, $a^n = e$

Recall. If a is a generator of the cyclic group G then we define the order of a to be the smallest positive integer n s.t. $a^n = e$.

Since the smallest positive integer m s.t. $a^m = e$ is n, $r=0$.

($\Leftarrow$) If n divides k, then $\boxed{k=ns}$ for some $s \in \mathbb{Z}$.

Thus $a^k = a^{ns} = (a^n)^s = e^s = e$ $\square$

Sidenote: The order of a generator of a cyclic group is the same as the order of the group

→ If $g \in G$ has order k, then set $\{e, g, \dots, g^{k-1}\}$ has distinct elements and $\{g^i \mid i \in \mathbb{Z}\} = \{e, g, \dots, g^{k-1}\}$. Here e is the identity of G → If G is generated by g then $G = \{g^i \mid i \in \mathbb{Z}\} = \{e, g, \dots, g^{k-1}\}$ and consequently $|G| = k$ i.e. the order of G is exactly the order of g

Multiplicative group of complex numbers

The complex numbers are $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$, where $i^2 = -1$.
If $z = a+ib$, $a = Re(z)$, $b = Im(z)$.

Prop 4.20 Let $z = r(\cos\theta + i\sin\theta)$, $w = s(\cos\phi + i\sin\phi)$ be two nonzero complex numbers. Then $zw = rs(\cos(\theta+\phi) + i\sin(\theta+\phi))$.

Theorem 4.22 (De Moivre)

Let $z = r(\cos\theta + i\sin\theta)$ be a nonzero complex number. Then

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

for $n = 1, 2, \dots$

The circle group and the roots of unity

The multiplicative group of the complex numbers denoted as $\mathbb{C}^*$ has some interesting subgroups of finite order.

Consider the circle group $\boxed{\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}}$

Prop. 4.24 The circle group is a subgroup of $\mathbb{C}^*$.

This is a direct result of prop. 4.20 above

Example Suppose that $H = \{1, -1, i, -i\}$. Then H is a subgroup of the circle group.

Identity : 1

Inverse $z\bar{z} = 1 \Rightarrow z^{-1} = \bar{z}$. So eg. inverse of i is $-i$.

Also, $1, -1, i, -i$ are exactly the complex numbers that satisfy $z^4 = 1$.

The complex numbers satisfying the equation $z^n = 1$ are called the n^{th} roots of unity

Theorem 4.25. If $z^n = 1$, then the nth roots of unity are

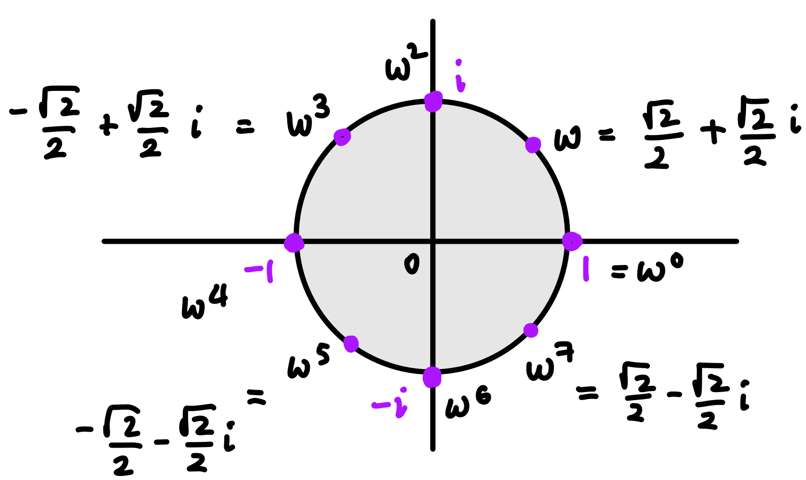
$$z = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$$

for $k = 0, 1, \ldots, n-1$.

Also, the nth roots of unity form a cyclic subgroup of $\mathbb{T}$ of order n.

A generator for the group of the nth roots of unity is called a primitive nth root of unity.

Example The 8^{th} roots of unity can be represented as 8 equally spaced points on the unit circle.



Chapter 5 : PERMUTATION GROUPS

Definition A permutation of a set A is a function from A to A that is both one-to-one and onto.

A permutation group of a set A is a set of permutations of A that forms a group under function composition.

Eg. We define a permutation α of the set $\{1,2,3,4\}$ by specifying $\alpha(1)=2$, $\alpha(2)=3$, $\alpha(3)=1$, $\alpha(4)=4$.

A convenient way to write α is in array form as: $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$.

Here $\alpha(j)$ is placed directly below j for each j.

e.g the permutation β of the set $\{1,2,3,4,5,6\}$ given by

$\beta(1)=5$, $\beta(2)=3$, $\beta(3)=1$, $\beta(4)=6$, $\beta(5)=2$, $\beta(6)=4$

can be expressed in array form as $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$

As we saw earlier in the course, composition of permutations expressed in array notation is carried out from right to left by going from top to bottom, then again from top to bottom.

e.g. let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$. Then

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$$

Example Symmetric Group S_3

Let S_3 denote the set of all one-to-one functions from $\{1,2,3\}$ to itself.

Then S_3 under function composition is a group with six elements:

identity

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \alpha^2=\alpha\circ\alpha=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},$$

$$\alpha\beta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad \alpha^2\beta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

If $f: S_3 \to S_3$ is a permutation, then f^{-1} exists since f is one-to-one and onto; hence every permutation has an inverse.

Note that $\beta\alpha=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\alpha^2\beta \neq \alpha\beta$, so S_3 is nonabelian.

$\square$

Note also that the relation $\beta\alpha=\alpha^2\beta$ can be used to compute other products in S_3 without resorting to the arrays. For instance,

$$\beta\alpha^2=(\beta\alpha)\alpha=(\alpha^2\beta)\alpha=\alpha^2(\beta\alpha)=\alpha^2(\alpha^2\beta)=\alpha^4\beta=\alpha\beta.$$

since $\alpha^3=e$

This example can be generalized to the symmetric group S_n.

Let $A=\{1,2,\dots,n\}$. The set of all permutations of A is called the symmetric group of degree n and is denoted by S_n. Elements of S_n have the form

$$\alpha=\begin{bmatrix}1&2&\cdots&n\\\alpha(1)&\alpha(2)&\cdots&\alpha(n)\end{bmatrix}$$

We can also compute the order of S_n. There are n choices for $\alpha(1)$

Once $\alpha(1)$ has been determined, we have $n-1$ possibilities for $\alpha(2)$

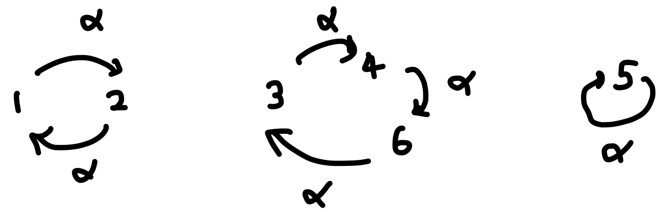
(note that since α is one-to-one, we must have $\alpha(1)\neq\alpha(2)$)

After choosing $\alpha(2)$, there are exactly $n-2$ possibilities for $\alpha(3)$

Continuing like this, we see that S_n has $n(n-1)\cdot\ \cdots\ \cdot 3\cdot 2\cdot 1 = n!$ elements.

Cycle notation As we've already briefly seen, there is another notation commonly used to specify permutations. It is called cycle notation and was introduced by Cauchy in 1815.

eg Consider the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$. Schematically this is



We leave out the arrows and instead simply write $\boxed{\alpha = (1\ 2)(3\ 4\ 6)(5).}$

An expression of the form $(a_1, a_2, \dots, a_m)$ is called a cycle of length m or an m-cycle.

A multiplication of cycles can be introduced by thinking of a cycle as a permutation that fixes any symbol not appearing in the cycle.
Thus $(4, 6)$ can be thought of as representing $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$.

e.g. Consider the following example from S_8 let $\boxed{\alpha = (1\ 3)(2\ 7)(4\ 5\ 6)(8)}$ and $\boxed{\beta = (1\ 2\ 3\ 7)(6\ 4\ 8)(5).}$

What is the cycle form of $\alpha\beta$?

Going from right to left:

(5) fixes 1
$(6\ 4\ 8)$ fixes 1
$(1\ 2\ 3\ 7)$ sends 1 to 2
} in β

as soon as you encounter within a cycle a diff. element go to the next cycle.

(8) fixes 2
$(4\ 5\ 6)$ fixes 2
$(2\ 7)$ sends 2 to 7
} in α

Thus we begin $\alpha\beta = (1\ 7\ \dots)\dots$

Now repeating the entire process starting with 7, we have

$$7 \xrightarrow{(5)} 7 \xrightarrow{(6\,4\,8)} 7 \xrightarrow{(1\,2\,3\,7)} 1 \xrightarrow[(8)]{} 1 \xrightarrow[(4\,5\,6)]{} 1 \xrightarrow{(2\,7)} 1 \xrightarrow{(1\,3)} 3$$

Thus $\alpha\beta = (1\ \ 7\ \ 3\ \ldots)\ldots$

At the end we obtain $\alpha\beta = (1\ 7\ 3\ 2)(4\ 8)(5\ 6)$

$4 \to 4 \to 8 \to 8 \to 8$

$8 \to 8 \to 6 \to 6 \to 6 \to 4$ ✓

★ when multiplying cycles "keep moving" from one cycle to the next from right to left ★

Remark: Some people prefer to not write cycles that have only one entry. In that case, it's understood that any missing element is mapped to itself.

Definition: Two cycles $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, b_2, \ldots, b_m)$ are disjoint if $a_i \neq b_j$ for all i and j

Example. The cycles $(1\ 3\ 5)$ and $(2\ 7)$ are disjoint; however the cycles $(1\ 3\ 5)$ and $(3\ 4\ 7)$ are not.

Remark: The product of two cycles that are not disjoint may reduce to something less complicated, however the product of disjoint cycles cannot be simplified.

e.g. $(1\ 3\ 5)(2\ 7) = (1\ 3\ 5)(2\ 7)$ stays as is

$(1\ 3\ 5)(3\ 4\ 7) = (1\ 3\ 4\ 7\ 5)$

Properties of permutations

Prop 5.8 [Disjoint cycles commute]

Let σ and τ be two disjoint cycles. Then $\boxed{\sigma\tau = \tau\sigma}$

Proof Let $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, b_2, \ldots, b_m)$.

For definiteness, let us say that α and β are permutations of the set

$$S = \{a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_m, c_1, c_2, \dots, c_l\}$$

where the c's are the members of S left fixed by both σ and τ (there may not be any c's).

To prove that $\sigma\tau = \tau\sigma$, we must show that $(\sigma\tau)(x) = (\tau\sigma)(x) \quad \forall x \in S$.

If x is one of the a elements, say a_i, then

$$(\sigma\tau)(a_i) = \sigma(\tau(a_i)) = \sigma(a_i) = a_{i+1}$$

Since τ fixes all a elements.

(Note. We interpret a_{i+1} as a_1 if $i = k$)

For the same reason $(\tau\sigma)(a_i) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = a_{i+1}$.

Therefore, the functions $\sigma\tau$ and $\tau\sigma$ agree on the a elements. A similar argument shows that $\sigma\tau$ and $\tau\sigma$ agree on the b elements as well.

Now, suppose that x is a c element, say c_i. Then, since both σ and τ fix c elements, we have

$$(\sigma\tau)(c_i) = \sigma(\tau(c_i)) = \sigma(c_i) = c_i$$

and $$(\tau\sigma)(c_i) = \tau(\sigma(c_i)) = \tau(c_i) = c_i$$

This completes the proof.

$\square$

<u>Theorem 5.9</u> Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

<u>Proof</u>. Let σ be a permutation on $A = \{1, 2, \dots, n\}$. To write σ in disjoint cycle form, we start by choosing any member of A, say a_1, and let

$$a_2 = \sigma(a_1), \quad a_3 = \sigma(a_2) = \sigma(\sigma(a_1)) = \sigma^2(a_1)$$

and so on, until we arrive at $a_1 = \sigma^m(a_1)$ for some m.

We know that such an m exists because the sequence $a_1, \sigma(a_1), \sigma^2(a_1), \dots$ must be finite; so there must be a repetition, say $\sigma^i(a_1) = \sigma^j(a_1)$ for some i and j with $i<j$.

e.g. $\sigma = (1\ 6\ 2\ 4)$, $\sigma(1) = 6$, $\sigma^2(1) = \sigma(6) = 2$, $\sigma^3(1) = \sigma(2) = 4$, $\sigma^4(1) = \sigma(4) = 1$
$\sigma^5(1) = \sigma(1) = 6, \dots$ Thus $\sigma(1) = \sigma^5(1)$ & $\sigma^{5-1}(1) = \sigma^4(1) = 1$ ✓

Then $a_1 = \sigma^m(a_1)$ where $m = j-i$. We express this relationship as

$$\sigma = (a_1\ a_2\ a_3 \dots a_m)\dots$$

this indicates the possibility that we may not have exhausted the set A in the process.

We now choose any element b_1 of set A not appearing in the first cycle and proceed to create a new cycle as before. Thus, we let

$$b_2 = \sigma(b_1), \quad b_3 = \sigma(b_2) = \sigma(\sigma(b_1)) = \sigma^2(b_1) \quad \text{etc}$$

until we reach $b_1 = \sigma^k(b_1)$ for some k. This new cycle will have no elements in common with the previously constructed cycle. For, if so, then $\sigma^i(a_1) = \sigma^j(b_1)$ for some i and j. But then $\sigma^{i-j}(a_1) = b_1$ and thus $b_1 = a_t$ for some t. This contradicts the way b_1 was chosen.

Continuing this process until we run out of elements of A, our permutation will appear as

$$\sigma = (a_1\ a_2 \dots a_m)(b_1\ b_2 \dots b_k)\cdots(c_1\ c_2 \cdots c_s)$$

Thus, every permutation can be written as a product of disjoint cycles. $\square$

<u>Example</u>. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$

$\sigma = (1\ 6\ 2\ 4)(3)(5) = (1\ 6\ 2\ 4)$
$\tau = (1\ 3)(2)(4\ 5\ 6) = (1\ 3)(4\ 5\ 6)$
$\sigma\tau = (1\ 3\ 6)(2\ 4\ 5)$
$\tau\sigma = (1\ 4\ 3)(2\ 5\ 6)$

Transpositions

Definition The simplest permutation is a cycle of length 2. Such cycles are called transpositions.

Prop. 5.12 Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

Proof First note that the identity can be expressed as $(1\ 2)(1\ 2)$ and so it is a product of 2-cycles. By thm 5.9, we know that every permutation can be written in the form

$$(a_1\ a_2 \cdots a_m)(b_1\ b_2\ \cdots b_k)\cdots(c_1\ c_2\ \cdots c_s)$$

A direct computation shows that this is the same as

$$(a_1\ a_m)(a_1\ a_{m-1})\cdots(a_1\ a_2)(b_1\ b_k)(b_1\ b_{k-1})\cdots(b_1 b_2)$$
$$\cdots(c_1 c_s)(c_1\ c_{s-1})\cdots(c_1 c_2)$$

$\square$

Example $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$

$(1\ 6\ 3\ 2)(4\ 5\ 7) = (1\ 2)(1\ 3)(1\ 6)(4\ 7)(4\ 5)$

on the right-most 2-cycle write the 2nd element & then proceed accordingly

start w/ first element of the cycle on the right

Lemma 5.14 If the identity is written as the product of r transpositions,

$$e = \tau_1\tau_2\cdots\tau_r$$

then r is an even number.

Proof. Left as an exercise. Use proof by induction

Finding inverses of permutations

Given $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ in S_n it is easy to compute $\boxed{\sigma^{-1}}$.

To find $\sigma^{-1}(j)$ we find j in the second row of σ, say $j = \sigma(i)$. The inverse of σ must referse this assignment and so under j we write i, giving $\sigma^{-1}(j) = i$. This can be accomplished by turning the two rows of σ upside down and then rearranging terms.

eg If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ then $\sigma^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

In cycle notation $\sigma = (1\ 4\ 2\ 3)$ and $\sigma^{-1} = (1\ 3\ 2\ 4) = (3\ 2\ 4\ 1)$

Thus to compute the inverse of a cycle, we just reverse the order of the cycle, since $(\sigma_1\ \sigma_2\ \ldots\ \sigma_m)(\sigma_m\ \sigma_{m-1}\ \ldots\ \sigma_1) = (1)$.

Theorem 5.15. If a permutation σ can be expressed as the product of an even number of transpositions, then any other product of transpositions equaling σ must also contain an even number of transpositions. Similarly for the odd case.

Proof Suppose that

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_m = \tau_1 \tau_2 \cdots \tau_n$$

where $\boxed{m \text{ is even}}$. We must show that n is also an even number.

The inverse of σ is $\sigma_m \cdots \sigma_1$. Since

$$e = \sigma \underbrace{\sigma_m \cdots \sigma_1}_{\sigma^{-1}} = \tau_1 \cdots \tau_n \sigma_m \cdots \sigma_1$$

n must be even by Lemma 5.14.

for $n+m$ = even when m = even

$\Rightarrow$ n has to be even.

Definition A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation.
A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation

Definition The group of even permutations of n symbols is denoted by A_n and is called the alternating group of degree n

Theorem 5.16 The set A_n is a subgroup of S_n

Proof Since the product of two even permutations must also be even, A_n is closed. The identity is an even permutation by lemma 5.14 and so the identity is in A_n.
If σ is an even permutation, then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$ where σ_i is a transposition and r is even. Since $\sigma^{-1} = \sigma_r \sigma_{r-1} \cdots \sigma_1$ [with the inverse of any transposition being itself] we have $\sigma^{-1} \in A_n$. □

The next result shows that exactly half of the elements of S_n $(n>1)$ are even permutations.

Prop 5.17 For $n \geq 2$, A_n has order $\frac{n!}{2}$.

This statement is the same as: The number of even permutations in S_n, $n \geq 2$ is equal to the number of odd permutations.

Proof Let A_n be the set of even permutations in S_n and
let B_n " odd "

If we show that there is a bijection between these sets, they must contain the same number of elements.

Fix a transposition σ in S_n. Since $n \geq 2$ such a σ exists.

Now define $\lambda_\sigma : A_n \to B_n$ by $\lambda_\sigma(\tau) = \sigma\tau$.

Suppose that $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Then by the def^n of λ_σ we have

$\boxed{\sigma\tau = \sigma\mu}$ and so $\tau = \underbrace{\sigma^{-1}\sigma}\tau = \sigma^{-1}\sigma\tau = \underbrace{\sigma^{-1}}_{e}\sigma\mu = \mu$

since $\sigma \in S_n$
its inverse σ^{-1} is also in S_n

Thus λ_σ is one-to-one.

Now we show that σ is surjective. Let $\beta \in B_n$. Then $\sigma^{-1}\beta$ is an even permutation since $\sigma \in B_n$

set of odd permut.

odd permutation

$\underbrace{(\ )(\ )(\ )}_{\text{odd}}\underbrace{(\ )(\ )(\ )}_{\text{odd}}$

$\Rightarrow$ even

Thus $\lambda_\sigma(\sigma^{-1}\beta) = \sigma\sigma^{-1}\beta$ ($\sigma^{-1}\beta$ acts as τ in $\lambda_\sigma(\tau) = \sigma\tau$ above)

$= \beta$

which proves that λ_σ is surjective.

□

<u>Example</u> The group A_4 is the subgroup of S_4 consisting of even permutations. There are 12 elements in A_4. $\left(|A_4| = \frac{4!}{2} = 12 \right)$

As an exercise try to write these elements down.

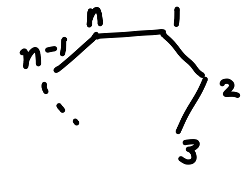
Dihedral groups

Dihedral groups are special types of permutation groups.

<u>Definition</u> The n^{th} dihedral group is the group of rigid motions of a regular n-gon. (i.e. n-sided polygon). We denote this group by D_n.

We number the vertices of a regular n-gon by $1, 2, \ldots, n$

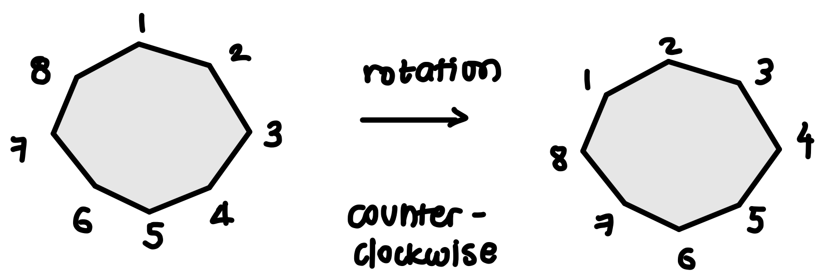
Note that there are exactly n choices to replace the first vertex. If we replace the 1^{st} vertex by k, then the 2^{nd} vertex must be replaced by either $k-1$ or $k+1$. Hence there are $2n$ possible rigid motions of the n-gon.

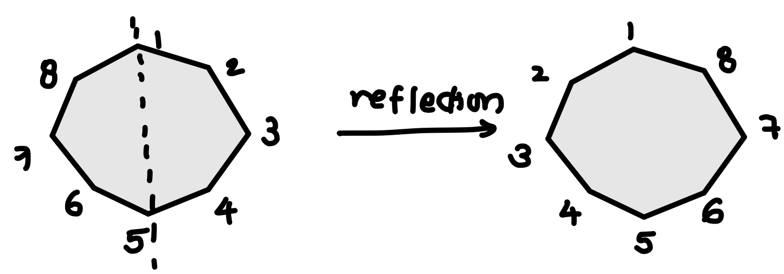


Remark. A rigid motion preserves the side lengths & angle measures of the polygon

Theorem 5.20 The dihedral group D_n, is a subgroup of S_n of order $2n$.

Example





Theorem 5.23 The group D_n, $n \geq 3$ consists of all products of the two elements r and s, satisfying the relations

$$\boxed{\begin{array}{l} r^n = 1 \\ s^2 = 1 \\ srs = r^{-1} \end{array}}$$

Proof The possible motions of a regular n-gon are either reflections or rotations. There are exactly n possible rotations:

$$e, \quad \frac{360^\circ}{n}, \quad 2\frac{(360^\circ)}{n}, \quad \ldots, \quad (n-1)\frac{(360^\circ)}{n}$$

We will denote the rotation $\frac{360^\circ}{n}$ by r. We note that the rotation r

generates <u>all</u> of the other rotations. In other words

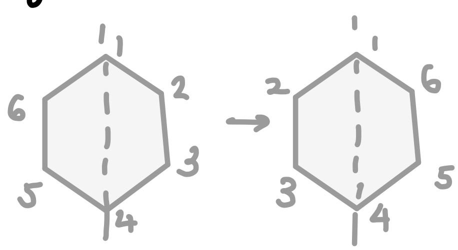
$$\boxed{r^k = k\left(\frac{360°}{n}\right)}$$

We label the n reflections $s_1, s_2, \ldots, s_n$, where s_k is the reflection that leaves vertex k fixed. There are 2 cases of reflections depending on whether

n is even <u>or</u> n is odd

If there are an n even number of vertices then two vertices are left fixed by a reflection

e.g.



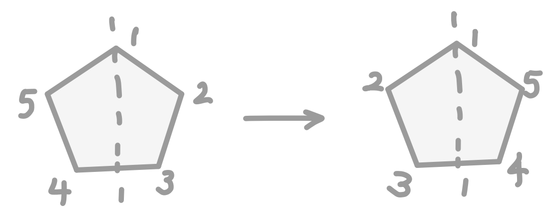
$n=6$

and $s_1 = s_{\left(\frac{n}{2}+1\right)}$, $s_2 = s_{\left(\frac{n}{2}+2\right)}$, $\ldots$ $s_{\left(\frac{n}{2}\right)} = s_n$

this leaves vertex 1 and $\frac{n}{2}+1 = 4$ fixed

this leaves vertex 3 and 6 fixed.

If there are an odd number of vertices then only a single vertex is left fixed by a reflection and $s_1, s_2, \ldots, s_n$ are distinct



there are also reflections through the edges that are combinations of reflections from the vertices w/ rotations

In either case, the order of each s_k is two

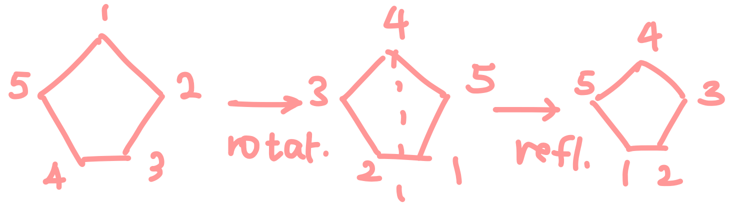
How many times we need to iterate this operation to go back to the identity? 2

Let $s = s_1$. Then $s^2 = 1$ and $r^n = 1$

Since any rigid motion t of the n-gon replaces the first vertex by vertex k, the 2nd vertex must be replaced by $k-1$ or $k+1$

If the 2nd vertex is replaced by $k-1$ then $t = sr^k$ rotation & then refl.

" $k+1$ then $t = r^k$ just rotation



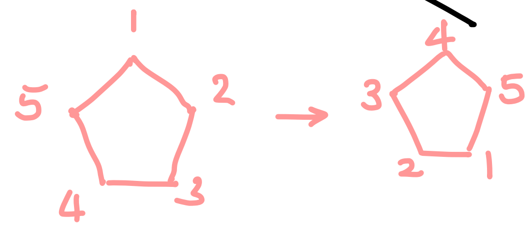
$(1\ 4)(2\ 3)(5)$

1 replaced by 4 k

2 replaced by 3 $k-1$

Other examples also exist.

eg



rotation: $(1\ 3\ 5\ 2\ 4)$

1 replaced by 4 k

2 replaced by 5 $k+1$

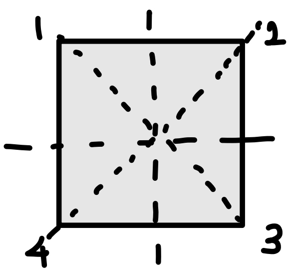
Thus r and s generate D_n.

I.e. D_n consists of all finite products of r and s

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

Think of how D_4 is different than S_4.

<u>Example</u> The group of rigid motions of a square D_4 consists of eight elements.



The group D_4

The rotations are
$r = (1\,2\,3\,4)$: $90°$
$r^2 = (1\ 3)(2\ 4)$: $180°$
$r^3 = (1\ 4\ 3\ 2)$: $270°$
$r^4 = (1)$

and the reflections are
$s_1 = (2\ 4)$
$s_2 = (1\ 3)$

reflections through vertices

But since $|D_4| = 2(4) = 8$, there are still two elements.

Those are $rs_1 = (1\ 2\ 3\ 4)(2\ 4) = (1\ 2)(3\ 4)$

and $r^3 s_1 = (1\ 4\ 3\ 2)(2\ 4) = (1\ 4)(2\ 3)$

all the reflections that pass from the edges rather than the vertices are combinations of s_1, s_2 and rotations

CHAPTER 6 Cosets and Lagrange's theorem

Definitions Let G be a group and H a subgroup of G. We define a left coset of H with representative $g \in G$ to be the set

$$\boxed{gH = \{gh : h \in H\}}$$

and similarly, right cosets as

$$\boxed{Hg = \{hg : h \in H\}.}$$

If left and right cosets coincide we will use "coset" w/o specifying left or right.

Example. Let H be the subgroup of $\mathbb{Z}_6$ under addition consisting of the elements $\underbrace{0 \text{ and } 3}_{\text{these are the } h\text{'s}}$. We recall that the elements of $(\mathbb{Z}_6, +)$ are $\{0,1,2,3,4,5\}$.
these are the g's

Thus the left cosets are

$0+H$, $= \{0,3\}$ since $H = \{0,3\}$

$1+H$, $= \{1,4\}$

$2+H$, $= \{2,5\}$

$3+H$, $= \{3,6\} = \{3,0\}$ since mod 6

$4+H$, $= \{4,1\}$

$5+H$ $= \{5,2\}$

$H = \{0,3\}$

$G = \{0,1,2,3,4,5\}$

Thus
$$0+H = 3+H = \{0,3\}$$
$$1+H = 4+H = \{1,4\}$$
$$2+H = 5+H = \{2,5\}$$

Example Let H be the subgroup of S_3 defined by the permutations $\boxed{H = \{(1),(1\,2\,3),(1\,3\,2)\}}$

The elements of S_3 are $\{(1),(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$

$|S_3| = 3! = 6$ ✓

Thus the left cosets of H are

$g \in S_3$.

$$(1)H = \{(1),(1\,2\,3),(1\,3\,2)\}$$
$$(1\,2)H = \{(1\,2),(1)(2\,3),(1\,3)\}$$

so we take each element $g \in S_3$ and perform gH.

(1 2 3) H .
(1 2 3)(1) = (1 2 3)
(1 2 3)(1 2 3) = (1 3 2)
(1 2 3)(1 3 2) = (1)(2)(3)
= (1)

Continuing like this we can show that

$$(1)H = (1\,2\,3)H = (1\,3\,2)H = \{(1), (1\,2\,3), (1\,3\,2)\}$$

and $$(1\,2)H = (1\,3)H = (2\,3)H = \{(1\,2), (1\,3), (2\,3)\}$$

We can also show that the right cosets of H are exactly the same as the left cosets

$$H(1\,3) = \{(1\,3), (1)(2\,3), (1\,2)\} \quad \text{etc.}$$

★ However, it's not always the case that a left coset is the same as a right coset.
Let K be a subgroup of S_3 defined by the permutations $\boxed{K = \{(1), (1\,2)\}}$. The left cosets of K are

$$(1)K = (1\,2)K = \{(1), (1\,2)\}$$
$$(1\,3)K = (1\,2\,3)K = \{(1\,3), (1\,2\,3)\}$$
$$(2\,3)K = (1\,3\,2)K = \{(2\,3), (1\,3\,2)\}$$

However, the right cosets are different.

$$K(1) = K(1\,2) = \{(1), (1\,2)\}$$
$$K(1\,3) = K(1\,3\,2) = \{(1\,3), (1\,3\,2)\}$$
$$K(2\,3) = K(1\,2\,3) = \{(2\,3), (1\,2\,3)\}$$

Properties of cosets Let H be a subgroup of G and let g_1 and g_2 belong to G. Then,

1. $g_1 \in g_1H$
2. $g_1H = H$ if and only if $g_1 \in H$.
3. $g_1H = g_2H$ if and only if $g_1 \in g_2H$
4. $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$
5. $g_1H = g_2H$ if and only if $g_1^{-1}g_2 \in H$

6. $|g_1H| = |g_2H|$

7. $g_1H = Hg_1$ if and only if $H = g_1Hg_1^{-1}$

8. g_1H is a subgroup of G if and only if $g_1 \in H$

Proof

1. $g_1 \in g_1H$

1. $g_1 = g_1 e \in g_1H$ $e \in H$.

2. $g_1H = H$ if and only if $g_1 \in H$.

2. $(\Rightarrow)$ We suppose that $g_1H = H$. Then $g_1 = g_1 e \in g_1H = H$
$(\Leftarrow)$ Next, we assume that $g_1 \in H$ and show that $g_1H \subseteq H$ and that $H \subseteq g_1H$, which would imply that $g_1H = H$

If $h \in H$ & $g_1 \in H$ (by ass.) then $g_1h \in H$ by closure & so $g_1H \subseteq H$

The first inclusion follows directly from the closure of H.
To show that $H \subseteq g_1H$, let $h \in H$. Then since $g_1 \in H$ and $h \in H$, we know that $g_1^{-1} \in H$, and by closure $g_1^{-1}h \in H$ by assumption

Thus $h = eh = g_1g_1^{-1}h = g_1(g_1^{-1}h) \in g_1H$

3. $g_1H = g_2H$ if and only if $g_1 \in g_2H$

3. $(\Rightarrow)$ If $g_1H = g_2H$, then $g_1 = g_1 e \in g_1H = g_2H$ by definition of coset
$(\Leftarrow)$ If $g_1 \in g_2H$ we have $g_1 = g_2h$ with $h \in H$, and thus
$$g_1H = (g_2h)H = g_2(hH) = g_2H$$

$hH = \{hh : h \in H\} = H$ check!

4. $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$

> **Theorem 6.4** Let H be a subgroup of a group G. Then the left cosets of H in G partition G. That is, the group G is the disjoint union of the left cosets of H in G

4. This follows directly from property 3, for if there is an element $c \in g_1H \cap g_2H$, then $cH = g_1H$ and $cH = g_2H$

5. $g_1H = g_2H$ if and only if $g_1^{-1}g_2 \in H$

5. Check that it's true using property 2.

6. $|g_1H| = |g_2H|$

6. To prove that $|g_1H| = |g_2H|$, it suffices to define a one-to-one mapping from g_1H onto g_2H.
Obviously, the correspondence $g_1h \to g_2h$ maps g_1H onto g_2H.
That it is one-to-one follows directly from the cancellation property.

7. $g_1H = Hg_1$ if and only if $H = g_1Hg_1^{-1}$

7. Note that $g_1H = Hg_1$ if and only if $(g_1H)g_1^{-1} = (Hg_1)g_1^{-1} = H(g_1g_1^{-1}) = H(e) = H$ if and only if $g_1Hg_1^{-1} = H$.

8. g_1H is a subgroup of G if and only if $g_1 \in H$

8. If g_1H is a subgroup, then it contains the identity e.
Thus $g_1H \cap eH \neq \emptyset$ and by property 4, we have $g_1H = eH = H$
Therefore, from property 2, we have $g_1 \in H$
Conversely, if $g_1 \in H$, then, again by property 2, $g_1H = H$.

$\triangledown$

<u>Definition</u> Let G be a group & H be a subgroup of G. The index of H in G is the number of left cosets of H in G. We denote the index by $[G:H]$.

<u>Example</u>. Recall from before that for $G = \mathbb{Z}_6^+ = \{0,1,2,3,4,5\}$ and $H = \{0,3\}$, we found that the cosets are
$$0+H = 3+H = \{0,3\}$$
$$1+H = 4+H = \{1,4\}$$
$$2+H = 5+H = \{2,5\}.$$

Thus $[G:H] = 3$ (# of left cosets)

Example. Also from before if $G = S_3$, $H = \{(1), (123), (132)\}$ and $K = \{(1), (12)\}$, then $[G:H] = 2$ and $[G:K] = 3$

Proposition 6.9 Let H be a subgroup of G with $g \in G$ and define a map $\phi : H \to gH$ by $\boxed{\phi(h) = gh}$. The map ϕ is bijective; thus the number of elements in H is the same as the number of elements in gH

Proof. We first show ϕ is one-to-one.

Suppose $\phi(h_1) = \phi(h_2)$ for $h_1, h_2 \in H$. We must show $h_1 = h_2$. But $\phi(h_1) = gh_1$ (by defn of $\phi(h)$) and $\phi(h_2) = gh_2$.

Thus $\phi(h_1) = \phi(h_2) \Rightarrow gh_1 = gh_2$

By the left cancellation property (i.e. $ab = ac \Rightarrow b = c$) we have $h_1 = h_2$.

$\phi . H \to gH$

We now also show that ϕ is onto. ($\forall\ y \in gH\ \exists\ x \in H$ s.t. $\phi(x) = y$)

By definition of gH, every element of gH is of the form gh for some $h \in H$, and $\phi(h) = gh$. ✓

□

Theorem 6.10 LAGRANGE

Let G be a finite group and let H be a subgroup of G.

Then $\frac{|G|}{|H|} = [G:H]$ is the number of distinct left cosets of H in G.

In particular, the number of elements in H must divide the number of elements in G. (i.e. the order of the subgroup H must divide the order of the group G)

Proof Since all the left cosets form a partition of G we only need to show that all the cosets have $|H|$ elements. By the definition of index,
this follows from prop. 6.9
there are $[G:H]$ left cosets in total, so we finish the proof.

$$|G| = \underbrace{[G:H]}_{\substack{\text{index} \\ = \#\text{ of left cosets } H \text{ in } G}} \cdot |H|.$$

Corollary 6.11. Suppose that G is a finite group and $g \in G$. Then the order of g must divide the number of elements in G

Corollary 6.12. If $|G| = p$ with p a prime number then G is cyclic and any $g \in G$ s.t. $g \neq e$ is a generator

Proof let $g \in G$ s.t $g \neq e$. Consider the subgroup $\langle g \rangle \leq G$. Its size divides $|G| = p$ by Lagrange's theorem, so it is 1 or p. But it's larger than 1 as it contains e and g. So $|\langle g \rangle| = p$. So $|\langle g \rangle| = |G|$. Thus the cyclic subgroup generated by g is equal to the group G itself. Hence G is generated by a single element g and is thus cyclic.

Recall $\langle g \rangle = \{ ng : n \in \mathbb{Z} \}$

Corollary 6.13 Let H and K be subgroups of a finite group G s.t. $K \subset H \subset G$. Then

$$\boxed{[G:K] = [G:H][H:K]}$$

Proof $[G:K] = \dfrac{|G|}{|K|} = \dfrac{|G|}{|H|} \cdot \dfrac{|H|}{|K|} = [G:H][H:K]$

$\square$

Note The converse of Lagrange's theorem is false.

The alternating group A_4 has order $|A_4| = \frac{4!}{2} = 12$.

However it can be shown that it does not have a subgroup of order 6.

Lagrange's theorem implies that subgroups of a group of order 12 can have order 1, 2, 3, 4, 6.

However, we are not guaranteed that subgroups of every possible order exist.

To prove that A_4 has no subgroup of order 6, we'll assume that it actually has such a subgroup and show that a contradiction must occur.

Recall that A_4 is the set of all even permutations of S_4.

The 12 elements are

(1), $(12)(34)$, $(13)(24)$, $(14)(23)$, (123), (132), (124)
(142), (134), (143), (234), (243)

every 3-cycle can be written as 2 2-cycles

e.g $(2\ 3)(2\ 4)$

if we take a 3-cycle & combine it w/ any other 3-cycle we'll get a 3-cycle

Since A_4 contains 8 3-cycles, we know that H must contain a 3-cycle.

We'll show that if H contains one 3-cycle then it must contain more than 6 elements

Prop 6.15. The group A_4 has no subgroup of order 6

Proof We assume A_4 has a subgroup H of order 6.

Then $[A_4 : H] = \frac{12}{6} = 2$, and so there are only two cosets of H in A_4.

One of the cosets is H itself. The right and left cosets must coincide.

Thus $gH = Hg$, which is equivalent to $gHg^{-1} = H$ for every $g \in A_4$.

Since there are 8 3-cycles in A_4, at least one 3-cycle must be in H

<u>Wlog</u> assume $(1\,2\,3) \in H$.

Then $(1\,2\,3)^{-1} = (3\,2\,1) \underset{\uparrow \text{also rewritten as}}{=} (1\,3\,2) \in H$ also

Since $ghg^{-1} \in H$ $\forall g \in A_4$ and all $h \in H$

If we use $h := (1\,2\,3) \in H$ and $g = (1\,2\,4)$ for example, then we get

$$ghg^{-1} = (1\,2\,4)(1\,2\,3)(1\,2\,4)^{-1}$$
$$= (1\,2\,4)(1\,2\,3)(4\,2\,1)$$
$$= (1)(2\,4\,3)$$
$$= (2\,4\,3)$$

Similarly, if we use $h = (1\,2\,3)$ still but pick $g = (2\,4\,3)$ we get

$$ghg^{-1} = (2\,4\,3)(1\,2\,3)(2\,4\,3)^{-1}$$
$$= (2\,4\,3)(1\,2\,3)(3\,4\,2)$$
$$= (1\,4\,2)$$

We conclude that H must have at least 7 elements. Namely,

$\underset{\uparrow\, e}{(1)}$, $\underset{\uparrow\, h}{(1\,2\,3)}$, $\underset{\uparrow\, h^{-1}}{(1\,3\,2)}$, $\underset{\uparrow\, ghg^{-1}}{(2\,4\,3)}$, $(2\,4\,3)^{-1} = (3\,2\,4) = (2\,3\,4)$,

$\underset{\uparrow\, ghg^{-1}}{(1\,4\,2)}$, $(1\,4\,2)^{-1} = (2\,4\,1) = (1\,2\,4)$

↯ Contradiction

Thus, A_4 has no subgroup of order 6

CHAPTER 9: Isomorphisms

It turns out that many groups that appear to be different are actually the same by simply renaming the group elements. Specifically if we demonstrate a one-to-one correspondence between the elements of the two groups and between the group operations then we say that the groups are isomorphic.

we use 2 different symbols here to show that the 2 groups can have different binary operations

Definition. Two groups $(G, \cdot)$ and $(H, \circ)$ are isomorphic if there exists a one-to-one and onto map $\phi : G \to H$ such that the group operation is preserved :

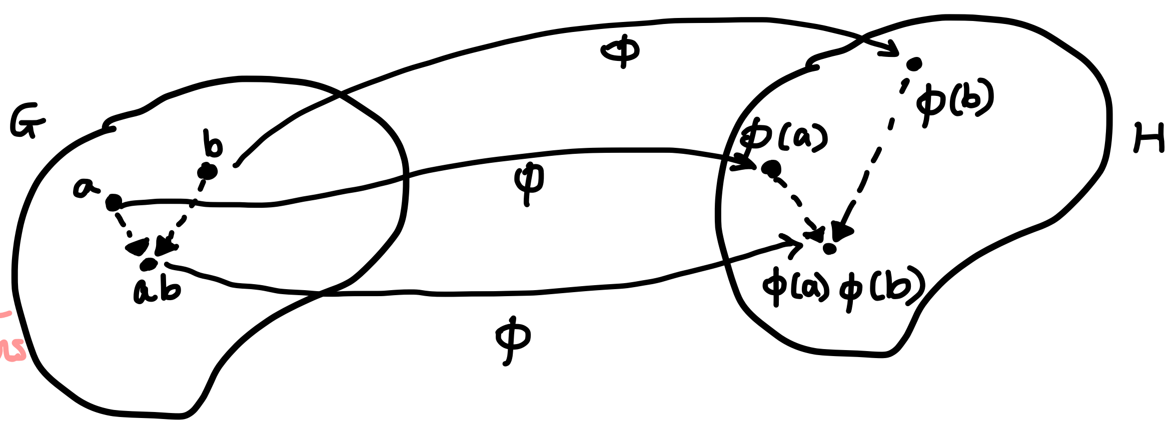
$$\boxed{\phi(a \cdot b) = \phi(a) \circ \phi(b)} \quad \forall\ a, b \in G.$$

The name comes from Greek. ἴσος = equal
μορφή = form

If G is isomorphic to H, we write $\boxed{G \cong H.}$

The map ϕ is called an isomorphism.

The dashed arrows represent the group operations



It is implicit in the definition of isomorphism that isomorphic groups have the same order.

It is also implicit that the operation on the left hand side of the equality sign is that of G & the operation on the RHS is that of H.

We next show the four cases involving $\cdot$ and $+$.

G operation	H operation	Operation Preservation
$\cdot$	$\cdot$	$\phi(a\cdot b)=\phi(a)\cdot\phi(b)$
$\cdot$	$+$	$\phi(a\cdot b)=\phi(a)+\phi(b)$
$+$	$\cdot$	$\phi(a+b)=\phi(a)\cdot\phi(b)$
$+$	$+$	$\phi(a+b)=\phi(a)+\phi(b)$

★ To prove that a group G is isomorphic to a group H, we must follow 4 separate steps. ★

STEP 1. "Mapping" Define a candidate for the isomorphism. I.e. define a function ϕ from G to H

STEP 2. "1–1" Prove that ϕ is one-to-one. I.e. Assume $\phi(a)=\phi(b)$ and prove that $a=b$.

STEP 3. "Onto" Prove ϕ is onto. I.e. For any $h\in H$, find an element $g\in G$ s.t. $\phi(g)=h$.

STEP 4. "Operation-preserving" Prove that ϕ is operation-preserving. I.e. show that $\phi(ab)=\phi(a)\phi(b)$ $\forall\ a,b\in G$.

In other words, this requires that one be able to obtain the same result by combining 2 elements & then mapping, or by mapping 2 elements and then combining them.

e.g. In calculus $\int_a^b (f+g)\,dx = \int_a^b f\,dx + \int_a^b g\,dx$

circle group $\mathbb{T}$ generated by i $=\{1,-1,i,-i\}$

Example. To show that $\mathbb{Z}_4 \cong \langle i\rangle$

we define a map $\phi:\mathbb{Z}_4\to\langle i\rangle$ by $\boxed{\phi(n)=i^n}$. We must show that ϕ is bijective and preserves the group operation.

$(\mathbb{Z}_4,+)=\{0,1,2,3\}$

The map ϕ is one-to-one and onto because

$$\phi(0)=i^0=1$$
$$\phi(1)=i^1=i$$
$$\phi(2)=i^2=-1$$
$$\phi(3)=i^3=-i$$

Since $\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n)$, the group operation is preserved.

group operation of G is $+$

group operation of $\langle i \rangle$ is $\times$

Example. We can define an isomorphism ϕ from the additive group of real numbers $(\mathbb{R}, +)$ to be the multiplicative group of positive real numbers $(\mathbb{R}^+, \times)$ with the exponential map. I.e.

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

Show that ϕ is bijective as an exercise.

Example. The integers are isomorphic to the subgroup of $\mathbb{Q}^*$ that consists of elements of the form 2^n.

We define a map $\phi : \mathbb{Z} \to \mathbb{Q}^*$ by $\boxed{\phi(n) = 2^n}$. Then

$$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n)$$

$\forall\ 2^n \in \mathbb{Q}^*\ \exists\ n \in \mathbb{Z}$ s.t. $\phi(n) = 2^n$ by definition of the map. Thus the map ϕ is onto the subset $\{2^n : n \in \mathbb{Z}\}$ of $\mathbb{Q}^*$.

Now we must show that ϕ is also one-to-one.

We assume that $m \neq n$. So we must show that $\phi(m) \neq \phi(n)$. Suppose that $m > n$ and assume that $\phi(m) = \phi(n)$ [then we want to arrive at a contradiction]

Then $\phi(m) = \phi(n)$ gives $2^m = 2^n \Rightarrow 2^{m-n} = 1$.

Since by assumption $m > n \Rightarrow m - n > 0$, $2^{m-n} = 1$ is impossible ↯

Thus, if $m \neq n$, then $\phi(m) \neq \phi(n)$ and ϕ is one-to-one. $\square$

Example: The groups $(\mathbb{Z}_8,+)$ and $(\mathbb{Z}_{12},+)$ cannot be isomorphic because they have different orders.

However $U(8) \cong U(12)$.

Recall that $U(8)$ is $(\mathbb{Z}_8,+)$ but with $a \in U(8)$ satisfying $\gcd(a,8)=1$.

Thus $U(8)=\{1,3,5,7\}$.

Similarly, $U(12)=\{1,5,7,11\}$.

We must find an isomorphism $\phi: U(8) \to U(12)$. One is given by

$$\begin{aligned} 1 &\mapsto 1 \\ 3 &\mapsto 5 \\ 5 &\mapsto 7 \\ 7 &\mapsto 11. \end{aligned}$$

Other possibilities also exist. Say ψ s.t.

$$\begin{aligned} 1 &\mapsto 1 \\ 3 &\mapsto 11 \\ 5 &\mapsto 5 \\ 7 &\mapsto 7 \end{aligned}$$

Example The symmetric group S_3 and $\mathbb{Z}_6$ have the same number of elements but $\mathbb{Z}_6$ is abelian whereas S_3 is nonabelian

Thus, one might suspect that the two groups are not isomorphic.

To show this is actually the case, we suppose that $\phi: \mathbb{Z}_6 \to S_3$ is an isomorphism.

Let $\boxed{a, b \in S_3}$ be two elements s.t. $\boxed{ab \neq ba}$

Since ϕ is an isomorphism, $\exists\, m, n \in \mathbb{Z}_6$ s.t.

$$\phi(m) = a \quad \text{and} \quad \phi(n) = b$$

since $\mathbb{Z}_6$ is abelian

Then $ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m) = ba$ ↯

by def^{n} of isomorphism

However, this contradicts the fact that a and b do not commute $\square$

Example There is no isomorphism from $(\mathbb{Q}, +)$ to $\mathbb{Q}^*$, the group of nonzero rational numbers under multiplication.

If ϕ were such a mapping there would be a rational number a, s.t.

$$\phi(a) = -1 \qquad \text{(since } \phi \text{ is onto)}$$

But then

operation of group G is +

$$-1 = \phi(a) = \phi\left(\tfrac{1}{2}a + \tfrac{1}{2}a\right) = \phi\left(\tfrac{1}{2}a\right)\phi\left(\tfrac{1}{2}a\right) = \left(\phi\left(\tfrac{1}{2}a\right)\right)^2$$

if ϕ were an isomorphism

However, no rational number squared is equal to -1.

Example Let $G = SL(2, \mathbb{R})$, the group of 2×2 matrices with determinant equal to 1. Let M be any 2×2 real matrix w/ det. 1.

Then we can define a mapping from G to G itself by

$$\boxed{\phi_M(A) = MAM^{-1}} \qquad \text{(since } M \text{ has det 1 its inverse } M^{-1} \text{ exists)}$$

$\forall$ matrices $A \in G$.

To verify that ϕ_M is an isomorphism we follow the 4 steps outlined above.

STEP 1. ϕ_M is a fcn from G to G. We must show that $\phi_M(A)$ is indeed an element of G whenever A is.

From the properties of determinants we have

$$\det(MAM^{-1}) = \det(M)\cdot\det(A)\cdot\underbrace{\det(M^{-1})}_{= \frac{1}{\det(M)}}$$
$$= 1\cdot 1\cdot \frac{1}{1}$$
$$= 1$$

Thus $MAM^{-1} \in G$.

STEP 2 ϕ_M is one-to-one.

Suppose that $\phi_M(A) = \phi_M(B)$. Then $MAM^{-1} = MBM^{-1}$!
By left and right cancellation we obtain $A = B$.

STEP 3. ϕ_M is onto.

Let $B \in G$. We must find a matrix $A \in G$ s.t. $\phi_M(A) = B$.
If such a matrix A is to exist, it must satisfy that $MAM^{-1} = B$.
But this tells us what A should be.
We can solve for A to obtain $A = M^{-1}BM$ and verify that

$$\phi_M(A) = MAM^{-1} = M(M^{-1}BM)M^{-1} = B.$$

STEP 4. ϕ_M is operation-preserving.

Let $A, B \in G$. Then

$$\begin{aligned}\phi_M(AB) &= M(AB)M^{-1} = MA\underbrace{M^{-1}M}_{\text{equal to identity}}BM^{-1} \\ &= (MAM^{-1})(MBM^{-1}) \\ &= \phi_M(A)\,\phi_M(B)\end{aligned}$$

The mapping ϕ_M is called <u>conjugation</u> by M.

<u>Theorem 9.6</u> Let $\phi: G \to H$ be an isomorphism of two groups. Then the following statements are true.

1) $\phi^{-1}: H \to G$ is an isomorphism.
2) $|G| = |H|$
3) If G is abelian, then H is abelian
4) If G is cyclic, then H is cyclic
5) If G is a subgroup of order n, then H has a subgroup of order n.

Proof. 1) Since ϕ is a bijection, ϕ^{-1} exists and it maps from H to G.

2) Since ϕ is bijective, $|G| = |H|$.

3) Suppose that $h_1, h_2 \in H$. Since ϕ is onto,

$$\exists\, g_1, g_2 \in G \text{ s.t. } \phi(g_1) = h_1 \text{ and } \phi(g_2) = h_2. \quad (*)$$

Thus

$$h_1 h_2 \underset{\text{by } (*)}{=} \phi(g_1)\phi(g_2) \underset{\substack{\text{by the fact}\\ \text{that } \phi \text{ is}\\ \text{an isomorphism}}}{=} \phi(g_1 g_2) \underset{\substack{\text{since } G \text{ is}\\ \text{abelian}\\ g_1 g_2 = g_2 g_1}}{=} \phi(g_2 g_1) \underset{\substack{\text{by the fact that}\\ \phi \text{ is an}\\ \text{isomorphism}}}{=} \phi(g_2)\phi(g_1) \overset{\text{by } (*)}{=} h_2 h_1$$

Theorem 9.7 All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$.

Proof Let G be a cyclic group with infinite order and suppose that a is a generator of G. Define a map $\phi: \mathbb{Z} \to G$ by $\boxed{\phi: n \to a^n}$.

Then

$$\underset{\substack{\text{operation of}\\ \mathbb{Z} \text{ is addition}}}{\phi(m+n)} \overset{\text{by def}^n \text{ of } \phi}{=} a^{m+n} = a^m a^n = \underset{\text{operation of } G}{\phi(m)\phi(n)}$$

To show that ϕ is injective, suppose that $m, n \in \mathbb{Z}$ where $m \neq n$. We assume $m > n$. We must show that $\phi(m) \neq \phi(n)$, i.e. $a^m \neq a^n$.

Let's suppose instead that $a^m = a^n$.

This gives $a^{m-n} = e$ where $m > n \Leftrightarrow m - n > 0$ which contradicts the fact that a has infinite order.

Thus $a^m \neq a^n$ and ϕ is therefore injective.

The map ϕ is onto since any element in G can be written as a^m for $n \in \mathbb{Z}$ and $\phi(n) = a^n$.

□

Theorem 9.8 If G is a cyclic group of order n, then G is isomorphic to $\mathbb{Z}_n$.

Proof Let G be a cyclic group of order n generated by a and define a map $\phi : \mathbb{Z}_n \to G$ by $\boxed{\phi(k) = a^k}$ where $0 \le k < n$.

The proof that ϕ is an isomorphism is similar to the proof of thm 9.7 but for showing ϕ is 1-1, $\phi(m) = \phi(k) \Rightarrow a^m = a^k \Rightarrow a^{m-k} = e$ implies $n \mid (m-k)$

order of G

This implies that $m = k$ because $m, k \in \mathbb{Z}_n$.

- In group theory, the main goal is to classify all groups.

Instead of classifying all groups, we want to classify all groups up to isomorphism

That is, we consider two groups to be the same if they are isomorphic.

Theorem 9.10 The isomorphism of groups determines an equivalence relation on the class of all groups.

CAYLEY'S THEOREM If G is a group, it is isomorphic to a group of permutations on some set. Hence, every group is a permutation group

This is what we call a representation theorem

The goal of representation theory is to find an isomorphism of some group G that we wish to study into a group that we know a lot about, eg a group of permutations or matrices.

Proof Let G be a group.

We must find a group of permutations $\bar{G}$ that is isomorphic to G.

For any $g \in G$, define a function $\lambda_g : G \to G$ by $\boxed{\lambda_g(a) = ga}$ $\forall a \in G$.

We claim that λ_g is a permutation of G.

We first show that the map λ_g is <u>one-to-one</u>. Suppose that $\lambda_g(a) = \lambda_g(b)$

Then $ga = gb$, which implies $a = b$ by the left cancellation property

To show that λ_g is <u>onto</u> we must show that for each $a \in G$ $\exists$ a b s.t. $\lambda_g(b) = a$. We use $gb = a$

$$\boxed{b = g^{-1}a}$$

Now we define the group $\bar{G}$. let $\boxed{\bar{G} = \{\lambda_g : g \in G\}}$.

We must show that $\bar{G}$ is a group under composition of functions and find an isomorphism between G and $\bar{G}$.

We have closure under composition of functions. For $a \in G$

$$\begin{aligned}(\lambda_g \circ \lambda_h)(a) &= \lambda_g(\lambda_h(a)) \\ &= \lambda_g(ha) && \text{by def}^{n} \text{ of } \lambda_g : G \to G \text{ above} \\ &= g(ha) && \lambda_g(a) = ga \quad \forall a \in G \\ &= (gh)a && \text{by associativity} \\ &= \lambda_{gh}(a) && \text{closure}\end{aligned}$$

We also have $\lambda_e(a) = ea = a$ identity

and

$$\begin{aligned}(\lambda_{g^{-1}} \circ \lambda_g)(a) &= \lambda_{g^{-1}}(\lambda_g(a)) \\ &= \lambda_{g^{-1}}(ga) \\ &= g^{-1}(ga) \\ &= (g^{-1}g)a \\ &= ea \\ &= a \\ &= \lambda_e(a) && \text{inverse}\end{aligned}$$

We define an isomorphism from G to $\overline{G}$ by $\boxed{\phi : g \to \lambda_g}$.

- ϕ is one-to-one because if $\phi(g)(a) = \phi(h)(a)$

then
$$\lambda_g(a) = \lambda_h(a)$$
$$ga = ha$$
$$g = h \quad \text{by the right cancellation property}$$

$\phi : G \to \overline{G}$

- ϕ is onto because $\phi(g) = \lambda_g$ for any $\lambda_g \in \overline{G}$.

- The group operation is preserved since for $g, h \in G$

$$\phi(gh) = \underset{\uparrow \text{ by def}^n \text{ of } \phi}{\lambda_{gh}} = gh = \lambda_g \lambda_h \overset{\text{by def}^n \text{ of } \phi}{=} \phi(g)\phi(h)$$

□

The isomorphism $g \mapsto \lambda_g$ is known as the left regular representation of G.

Example Consider $\mathbb{Z}_3$. The Cayley table for $(\mathbb{Z}_3, +)$ is

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

This suggests that it's the same as the permutation group

$$G = \{(0), (0\,1\,2), (0\,2\,1)\}$$

Cayley table

1st row: $\begin{matrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 \end{matrix}$ 2nd row: $\begin{matrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 0 \end{matrix}$ 3rd row: $\begin{matrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 2 & 0 & 1 \end{matrix}$

The isomorphism is

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = (0) \qquad 1 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (0\,1\,2), \quad 2 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (0\,2\,1)$$

Example Let's compute the left regular representation $\overline{U(12)}$ for $U(12) = \{1, 5, 7, 11\}$

$(\mathbb{Z}_{12}, +)$ with $\gcd(n, 12) = 1$

Writing the permutations of $U(12)$ in array form, we have

$$\lambda_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix}, \quad \lambda_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}, \quad \lambda_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}, \quad \lambda_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}$$

recall that λ_x is just multiplication by x

$\lambda_g(a) = ga \quad \forall a \in G$

$\lambda_5(1) = 5 \mod 12$

$\lambda_5(5) = 5(5) = 1 \mod 12$

$\lambda_5(7) = 5(7) = 11 \mod 12$

$\lambda_5(11) = 55 = 7 \mod 12$

where $\lambda_5(g) = 5g$ with $g \in G$

We next compare the Cayley table for $U(12)$ and its left regular representation $\overline{U(12)}$

remember it uses addition

$U(12)$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\overline{U(12)}$	λ_1	λ_5	λ_7	λ_{11}
λ_1	λ_1	λ_5	λ_7	λ_{11}
λ_5	λ_5	λ_1	λ_{11}	λ_7
λ_7	λ_7	λ_{11}	λ_1	λ_5
λ_{11}	λ_{11}	λ_7	λ_5	λ_1

The tables show that $U(12)$ and $\overline{U(12)}$ are only notationally different.

Section 9.2 DIRECT PRODUCTS

Given two groups G and H, it is possible to construct a new group from the Cartesian product of G and H, $\boxed{G \times H}$

Conversely, given a large group it is sometimes possible to decompose the group. I.e A group is sometimes isomorphic to the direct product of two smaller groups.

External direct products

If $(G, \cdot)$ and $(H, \circ)$ are groups, then we can make the Cartesian product of G and H into a new group. As a set, $G \times H$ is just the ordered pairs $\boxed{(g,h) \in G \times H}$ where $\boxed{g \in G \text{ and } h \in H}$

We define a binary operation on $G \times H$ by

$$\boxed{(g_1, h_1)(g_2, h_2) = (\underbrace{g_1 \cdot g_2}_{\text{operation in } G}, \underbrace{h_1 \circ h_2}_{\text{operation in } H})}$$

We will usually denote it simply as $(g_1 g_2, h_1 h_2)$ but it implied that we multiply elements in the 1st coord as we do in G & elements in the 2nd coord as we do in H.

Prop. 9.13 Let G and H be groups. The set $G \times H$ is a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ where $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Proof. The operation defined above is closed

Identity: If $e_G \in G$ and $e_H \in H$ are the identities of each group (e_G, e_H) is the identity of $G \times H$.

Inverse: The inverse of $(g,h) \in G$ is (g^{-1}, h^{-1}).

The operation is associative since G & H are associative. $\square$

Example Let $\mathbb{R}$ be the group of real numbers under addition.
The Cartesian product $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is also a group.
The group operation is addition in each coordinate, i.e.

$$(a,b) + (c,d) = (a+c, \ b+d) \quad \text{closure}$$

The identity is $(0,0)$

The inverse of (a,b) is $(-a,-b)$.

<u>Example</u> Consider $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$

and $(\mathbb{Z}_4,+) = \{0,1,2,3\}$.

$\mathbb{Z}_2 = \{\underset{a}{0},\underset{b}{1}\}$ and so $\mathbb{Z}_2\times\mathbb{Z}_2 = \{(a,a),(a,b),(b,a),(b,b)\}$

They both have order 4 but they are <u>not isomorphic</u>.

Every element $(a,b) \in \mathbb{Z}_2\times\mathbb{Z}_2$ has order 2 since $(a,b)+(a,b)=(0,0)$

- $(0,1)+(0,1)=(0,2)=(0,0) \mod 2$.

etc

- $(1,0)+(1,0)=(2,0)=(0,0) \mod 2$

NB The identity is $(0,0)$

But $\mathbb{Z}_4$ is cyclic and so one of its elements has order 4

$3+3=6=2 \mod 4$

$3+3+3=9=1 \mod 4$

$3+3+3+3=12=0 \mod 4$

$\not\cong$

<u>Example</u> $U(8)\times U(10) = \{(1,1),(1,3),(1,7),(1,9),$
$(3,1),(3,3),(3,5),(3,7),(3,9)$
$(5,1),(5,3),(5,5),(5,7),(5,9)$
$(7,1),(7,3),(7,5),(7,7),(7,9)\}$

$U(8)=\{1,3,5,7\}$

$U(10)=\{1,3,5,7,9\}$

Since the first components are combined by multiplication mod 8 whereas the 2nd comp. are combined by mult. mod 10

<u>Example</u> CLASSIFICATION OF GROUPS OF ORDER 4

A group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2\times\mathbb{Z}_2$ both are abelian and of order 4

cyclic

To verify this, let $G=\{e,a,b,ab\}$.

by closure

A key difference between the two groups is that the cyclic group $\mathbb{Z}_4$ has an element of order 4 but $\mathbb{Z}_2\times\mathbb{Z}_2$ only has elements of order 2

If G is not cyclic, then from Lagrange's theorem $|a|=|b|=|ab|=2$

Then the mapping $e\to(0,0)$, $a\to(1,0)$, $b\to(0,1)$, and $ab\to(1,1)$ is an isomorphism from G onto $\mathbb{Z}_2\times\mathbb{Z}_2$ $\square$

CHECK as an exercise

The group $G \times H$ is called the external direct product of G and H. We could also have more groups : $G_1, G_2, \ldots, G_n$ and then their external direct product would be defined in the same manner

$$\boxed{\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n}$$

$g^r = e$ and $h^s = e$

Theorem 9.17 Let $(g,h) \in G \times H$. If g and h have finite orders r and s, respectively then the order of $(g,h) \in G \times H$ is the least common multiple of r and s

Proof Suppose that m is the least common multiple of r and s and let $n = |(g,h)|$ ← the order of the element $(g,h) = n$

$(g,h)^m = (g,h)(g,h)\cdots(g,h) = (g^m, h^m)$. Recall the binary operation for $G \times H$ is $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ for $g_1, g_2 \in G$ & $h_1, h_2 \in H$

Then $(g,h)^m = (g^m, h^m) = (e_G, e_H)$ ← since $m = \operatorname{lcm}(r,s)$

hence n must divide m and $n \leq m$

$(g^n, h^n) = (g,h)^n = (e_G, e_H)$

by defn of the order of an element (smallest #)

However since r and s are the orders of elements g and h, respectively, we have

$$\left.\begin{array}{l} g^r = e_G \\ g^s = e_H \end{array}\right\} \Rightarrow \begin{array}{l} r \text{ must divide } n \\ \& \ s \text{ must divide } n \text{ as well} \end{array}$$

So n is a common multiple of r and s.

Since m is the least common multiple of r and s, $m \leq n$.

Thus m must equal n $\square$

Corollary 9.18 Let $(g_1, \ldots, g_n) \in \prod_{i=1}^{n} G_i$

If g_i has finite order r_i in G_i, then the order of $(g_1, \ldots, g_n) \in \prod G_i$ is the least common multiple of $r_1, \ldots, r_n$.

if $\gcd(n,a) \neq 1$ then $\gcd(n,a) = d$ and order(a) w/ $a \in \mathbb{Z}_n$ is $\frac{n}{\gcd(n,a)} = \frac{n}{d}$

Example 9.19 Let $(8,56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$

Since $\gcd(8,12) = 4$, the order of 8 is $\frac{12}{4} = 3$ in $\mathbb{Z}_{12}$

$\frac{n}{\gcd(a,n)}$ = order of element a in $\mathbb{Z}_n$

Similarly, $\gcd(56,60) = 4$. the order of 56 is $\frac{60}{4} = 15$ in $\mathbb{Z}_{60}$

Thus, the least common multiple is 15, which implies by theorem 9.17 that $(8,56)$ has order 15 in $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$.

Example. Consider $\mathbb{Z}_2 = \{0,1\}$ and $\mathbb{Z}_3 = \{0,1,2\}$. Then

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$$

order is 6.

In this case, $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

isomorphic

(unlike that of $\mathbb{Z}_2 \times \mathbb{Z}_2$ not being isomorphic to $\mathbb{Z}_4$)

Here we have to show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.

Let's consider the element $(1,1)$.

$$2(1,1) = (1,1) + (1,1) = (2,2) = (0,2)$$

mod 2 mod 3

$$3(1,1) = (1,1)+(1,1)+(1,1) = (0,2)+(1,1) = (1,3) = (1,0)$$

mod 2 mod 3

$$4(1,1) = (1,1)+(1,1)+(1,1)+(1,1) = (1,0)+(1,1) = (2,1) = (0,1)$$

$$5(1,1) = (0,1)+(1,1) = (1,2)$$

$$6(1,1) = (1,2)+(1,1) = (2,0) = (0,0)$$

order of $(1,1)$ is 6. ✓

least common multiple of 2 and 3

$\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic

$(1,1)$ is a generator!

The next theorem tells us exactly when the direct product of two cyclic groups is cyclic.

<u>Theorem 9.21</u> The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m,n)=1$.

<u>Proof</u> $(\Rightarrow)$ We want to show that if $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ then $\gcd(m,n)=1$

We prove the contrapositive i.e. if $\gcd(m,n)=d>1$ then $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic

Note that $\frac{mn}{d}$ is divisible by both m and n, hence for any element $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$

operation of $\mathbb{Z}_m \times \mathbb{Z}_n$ is addition

$$\underbrace{(a,b)+(a,b)+\cdots+(a,b)}_{\frac{mn}{d}\text{ times}} = (0,0)$$

identity

Thus no (a,b) can generate all of $\mathbb{Z}_m \times \mathbb{Z}_n$

$(\Leftarrow)$ This follows directly from theorem 9.17 since $\operatorname{lcm}(m,n)=mn$ if and only if $\gcd(m,n)=1$

CHAPTER 10: Normal subgroups & factor groups

We already saw that if H is a subgroup of a group G, then right cosets are not always the same as left cosets. I.e it's not always the case that $gH = Hg$ $\forall g \in G$.

The subgroups for which this property is true allow for the construction of a new class of groups called factor or quotient groups

Definition A subgroup H of a group G is normal in G if $\boxed{gH = Hg}$ $\forall g \in G$.
A normal subgroup of a group G is one in which the right and left cosets are the same. Sometimes we denote this by $H \triangleleft G$.

Example Let G be an abelian group. Every subgroup H of G is a normal subgroup. Since $gh = hg$ for all $g \in G$ and $h \in H$, it will always be that $gH = Hg$.

Example Let H be the subgroup of S_3 that is $\{(1), (12)\}$. not normal in S_3

$$S_3 = \{(1), (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\}$$

Since $(1\,2\,3)H = (1\,2\,3)\{(1), (1\,2)\} = \{(1\,2\,3), (1\,3)\}$ $\neq$ and $H(1\,2\,3) = \{(1), (1\,2)\}(1\,2\,3) = \{(1\,2\,3), (2\,3)\}$

H cannot be a normal subgroup of S_3.

However, the subgroup N, consisting of the permutations $(1), (1\,2\,3)$, and $(1\,3\,2)$, is normal since the cosets of N are

$$N = \{(1), (123), (132)\}$$ normal in S_3

$$(1\,2)N = \{(1\,2), (1\,3), (2\,3)\} = N(1\,2)$$

$$(2\,3)N = \{(2\,3), (1\,3), (1\,2)\} = N(2\,3)$$

etc...

The next example shows a way to use a normal subgroup to create new subgroups from existing ones

<u>Example</u> Let H be a <u>normal</u> subgroup of a group G and K be <u>any</u> subgroup of G. Then $HK = \{hk \mid h \in H \text{ and } k \in K\}$ is a subgroup of G.

To verify this, note that $e = ee$ is in HK.

Then for any $a = h_1 k_1$ and $b = h_2 k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$ there is an element $h' \in H$ s.t.

$$ab^{-1} = h_1 k_1 (h_2 k_2)^{-1}$$
$$= h_1 k_1 k_2^{-1} h_2^{-1}$$
$$= h_1 (k_1 k_2^{-1}) h_2^{-1}$$
$$= \underbrace{(h_1 h')}_{\in H} \underbrace{(k_1 k_2^{-1})}_{\in K}$$

which makes $ab^{-1} \in HK = \{hk \mid h \in H \text{ \& } k \in K\}$

Note that $h_2^{-1} \in H$ and so $k_1 k_2^{-1} h_2^{-1} \in k_1 k_2^{-1} H$

since H is normal in G $\exists$ h' s.t $k_1 k_2^{-1} h_2^{-1} = h' k_1 k_2^{-1}$, $h' \in H$ $(*)$ why?

Let $g = k_1 k_2^{-1}$ & $h = h_2^{-1}$ since $H \triangleleft G$

$gH = Hg$. $\exists$ $h' \in H$ s.t $gHg^{-1} \in H$. $ghg^{-1} = k_1 k_2^{-1} h_2^{-1} (k_1 k_2^{-1})^{-1} = k_1 k_2^{-1} h_2^{-1} k_2 k_1^{-1} = h'$

Thus $k_1 k_2^{-1} h_2^{-1} = h' k_1 k_2^{-1}$

So $ab^{-1} \in HK$.

<u>Theorem 10.3</u> <u>Normal subgroup test</u>

A subgroup H of G is normal in G if and only if $gHg^{-1} \subseteq H$ $\forall g \in G$

<u>Proof</u> $(\Rightarrow)$ If H is normal in G, then for any $g \in G$ and $h \in H$ $\exists$ $h' \in H$ s.t. $gh = h'g$.

(since by def^n of normal subgroup $gH = Hg$ & $gH = \{gh : h \in H\}$, $Hg = \{hg : h \in H\}$

Thus $ghg^{-1} = h' \Rightarrow gHg^{-1} \subseteq H$

$(\Leftarrow)$ If $gHg^{-1} \subseteq H$ $\forall g \in G$ then letting $g = a$, we have $aHa^{-1} \subseteq H$ or $aH \subseteq Ha$.

On the other hand, letting $g = a^{-1}$, we have $gHg^{-1} = a^{-1} H (a^{-1})^{-1}$
$$= a^{-1} H a \subseteq H$$

$\Rightarrow Ha \subseteq aH$.

This implies that $aH = Ha$ and so H is normal in G.

$\square$

<u>Definition</u> If N is a normal subgroup of a group G, then the cosets of N in G form a group $\boxed{G/N = \{gN : g \in G\}}$ under the operation $\boxed{(aN)(bN) = abN}$

This group is called the factor or quotient group of G and N.

read as "G mod N"

<u>Theorem 10.4</u> Let N be a normal subgroup of a group G. The cosets of N in G form a group G/N of order $[G:N]$.

index = # of left cosets

<u>Proof</u> The group operation on G/N is $(aN)(bN) = abN$.

We must show that the group multiplication is independent of the choice of coset representative. ← this shows that the operation is well defined, i.e. the correspondence above from $G/N \times G/N$ into G/N is actually a function.

Let $aN = bN$ and $cN = dN$.

We must show that $(aN)(cN) = acN = bdN = (bN)(dN)$

since $aN = bN$ since $cN = dN$ left coset def: $cN = \{cn : n \in N\}$

Then $a = bn_1$ and $c = dn_2$ for some $n_1, n_2 \in N$

Thus
$$\begin{aligned} acN &= (bn_1)(dn_2)N \\ &= bn_1(dN) \\ &= bn_1(Nd) \\ &= bNd \\ &= bdN \end{aligned}$$

$aN = \{an : n \in N\}$
$bN = \{bn : n \in N\}$

← since N is a normal subgroup $dN = Nd$

$n_1 N = N$ since n_1 "gets absorbed" in N

← here we used associativity a lot

<u>Note</u>
We also used one of the properties of cosets; that $gH = H$ iff $g \in H$.

The identity is $eN = N$

The inverse of gN is $g^{-1}N$.

$(gN)(g^{-1}N) = (gg^{-1})N = eN = N$ ← identity ✓

The order of G/N is the number of cosets of N in G which is the definition of index $[G:N]$.

□

Example Consider the normal subgroup of S_3, $\boxed{N = \{(1), (1\,2\,3), (1\,3\,2)\}}$

$S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$

The cosets of N in S_3 are N and $(12)N$.

The factor group S_3/N has the following multiplication table

	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

Note that if you compute $(1\,3)N$ you will get that it's equal to $(1\,2)N$. So the distinct cosets of N in S_3 are N & $(1\,2)N$.

index $[G:N] = \frac{6}{3} = 2$ cosets

where $(12)N = (1\,2)\{(1), (1\,2\,3), (1\,3\,2)\}$

$= \{(1\,2), (2\,3), (1\,3)\} = (1\,3)N$

and indeed $\underline{(1\,2)N\,(1\,2)N}$ is $(1\,2)\{(1\,2), (2\,3), (1\,3)\}$
$= \{(1), (1\,2\,3), (1\,3\,2)\}$ etc

but also you get this from $(1\,2)N(1\,2)N = (1\,2)(1\,2)N = (1)N = N$ ✓

This group is isomorphic to $\mathbb{Z}_2 = \{0,1\}$ $(S_3/N \simeq \mathbb{Z}_2)$

Consider $\phi : S_3/N \to \mathbb{Z}_2$ defined by $\phi(N) = 0$ and $\phi((12)N) = 1$.
ϕ is bijective.

How about operation-preserving?

$$\phi(NN) = \phi(N) = 0 = 0+0 = \phi(N) + \phi(N)$$

operation in S_3/N from multipl. table   operation in $\mathbb{Z}_2$

Also, $\phi((12)N\,N) = \phi((12)N) = 1 = 1+0 = \phi((12)N) + \phi(N)$

and $\phi((12)N(12)N) = \phi(N) = 0 = 1+1 = \phi((12)N) + \phi((12)N)$

$\mathbb{Z}$ mod 2

Note also that S_3/N is abelian and cyclic, $S_3/N = \langle (12)N \rangle$.

Notice that S_3/N is a smaller group than S_3.

We note that $\boxed{N = A_3}$ ← alternating group, i.e. the group of even permutations

and $(12)N = (1\,2)\{(1), (1\,2\,3), (1\,3\,2)\}$

$= \{(1\,2), (2\,3), (1\,3)\}$ is the set of odd permutations.

product of odd number of 2-cycles

So the information captured in G/N is parity → odd vs even

→ multiplying two even or two odd permutations results in an even permutation

→ multiplying an odd permutation by an even permutation yields an odd permutation.

$(12)N$

Example Consider the normal subgroup $3\mathbb{Z}$ of $\mathbb{Z}$. $(3\mathbb{Z} \triangleleft \mathbb{Z})$

$3\mathbb{Z} = \{0, \pm 3, \pm 6, \ldots\} = \langle 3 \rangle$ w/ addition

We note $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3 = \{0, 1, 2\}$. We have $\underbrace{|\mathbb{Z}/3\mathbb{Z}|}_{\text{order of group}} = \underbrace{[\mathbb{Z} : 3\mathbb{Z}]}_{\text{(distinct cosets)}} = 3$

The cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are

$gN = \{gn : n \in N\}$ where $G = \mathbb{Z}$ and $N = 3\mathbb{Z}$

$g_1N = 0 + 3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}$

$g_2N = 1 + 3\mathbb{Z} = \{\ldots, -2, 1, 4, 7, \ldots\}$

$g_3N = 2 + 3\mathbb{Z} = \{\ldots, -1, 2, 5, 8, \ldots\}$

$g_4N = 3 + 3\mathbb{Z} = \{\ldots, 0, 3, 6, \ldots\} = 0 + 3\mathbb{Z}$ and it keeps repeating

The group $\mathbb{Z}/3\mathbb{Z}$ is given by

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

e.g $(2+3\mathbb{Z})+(2+3\mathbb{Z})$
$= 4+3\mathbb{Z} = 1+(3+3\mathbb{Z})$
$= 1+3\mathbb{Z}$

Note, $\mathbb{Z}/3\mathbb{Z}$ is cyclic. Consider for example $\mathbb{Z}/3\mathbb{Z} = \langle 1+3\mathbb{Z} \rangle$.

Generally, the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is normal. Elements of $\mathbb{Z}/n\mathbb{Z}$ are cosets:

$$n\mathbb{Z}, \quad 1+n\mathbb{Z}, \quad 2+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$$

and $\boxed{\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n}$

multiplicative group $\mathbb{Z}_{32}$

Example: let $G = U(32) = \{1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31\}$ and $H = \{1,17\}$. Then $H \trianglelefteq G$ since G is abelian. (on pg 78 we show that when G is abelian all subgroups are normal).

$|G/H| = [G:H] = \dfrac{|G|}{|H|} = \dfrac{16}{2} = 8$. So we have 8 distinct cosets of H in G.

Elements of the group $U(32)/H$ are:

$1H = H = \{1,17\}$

$3H = \{3,19\}$ ← to compute this $3H = 3\{1,17\} = \{3,51\} = \{3,19\}$ (mod 32)

$5H = \{5,21\}$

$7H = \{7,23\}$

$9H = \{9, 25\}$

$11H = \{11, 27\}$

$13H = \{13, 29\}$

$15H = \{15, 31\}$

by closure all combinations of elements should give other elements in the group

Note : The operation is $\boxed{aH\,bH = abH}$ So, for example

$$11H\,13H = (11)(13)H = 143H = \{143, 2431\} = \{4(32)+15, 75(32)+31\}$$
$$= \{15, 31\} = 15H$$

Note

Sometimes we use the terminology "G mod H" for G/H This arises from the analogy w/ modular arithmetic. When we work in $\mathbb{Z}$ mod 5, we say $8 = 3 \bmod 5$ because $8 = 3+5 = 3 \bmod 5$ because the 5 "gets absorbed" into the modulus. That is, $8 \bmod 5 = (3+5) \bmod 5 = 3 + (5 \bmod 5) = 3 \bmod 5$

Similarly, if we look at gH and if $g = g'h$ then $gH = g'hH = g'H$ because the h "gets absorbed" by the H.

CHAPTER 11 HOMOMORPHISMS

This is a generalization of an isomorphism.
If we relax the requirement that an isomorphism of groups be bijective, we have a homomorphism.

Section 11.1: Group homomorphisms

Definition: A **homomorphism** between groups $(G, \cdot)$ and $(H, \circ)$ is a map $\phi : G \to H$ such that $\boxed{\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)}$ for $g_1, g_2 \in G$.

The range of ϕ in H is called the **homomorphic image** of ϕ

Note: This suggests that two groups are strongly related if they are isomorphic but a weaker relationship can exist between two groups.

Example. Let G be a group and $g \in G$. Define a map $\phi: \mathbb{Z} \to G$ by $\phi(n) = g^n$. Then ϕ is a group homomorphism since

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

This homomorphism maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g.

Example. Let $G = GL_2(\mathbb{R})$. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in G, then the determinant is nonzero $\det(A) = ad - bc \neq 0$. For any $A, B \in G$, $\det(AB) = \det(A)\det(B)$.

Using the determinant, we define a homomorphism $\phi: GL_2(\mathbb{R}) \to \mathbb{R}^*$ by $A \mapsto \det(A)$.

Example We define a homomorphism ϕ from $(\mathbb{R}, +)$ to $\mathbb{T}$ (the circle group consisting of all complex numbers z s.t. $|z| = 1$), as

$$\phi: \theta \longmapsto \cos\theta + i\sin\theta$$

using the addition formulae of cos & sin

$$\begin{aligned} \phi(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) \\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= \phi(\alpha)\,\phi(\beta) \end{aligned}$$

binary operation of $(\mathbb{R}, +)$

binary operation of $\mathbb{T}$

could also use $e^{i\theta}$.

Example The map $\phi(x) = x^2$ from $\mathbb{R}^*$, the nonzero real numbers under multiplication to itself is a homomorphism since

$$\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\,\phi(b) \quad \forall\, a, b \in \mathbb{R}^*$$

Example The map $\phi(x) = x^2$ from $(\mathbb{R}, +)$ to itself is not a homomorphism since $\phi(a+b) = (a+b)^2 = a^2 + 2ab + b^2 \neq \phi(a) + \phi(b)$
$= a^2 + b^2$.

When defining a homomorphism from a group in which there are several ways to represent the elements, we must ensure that the correspondence is a function. (i.e. a well-defined mapping)

e.g. since $3(x+y) = 3x + 3y$ in $\mathbb{Z}_6$, one might believe that the correspondence $x + \langle 3 \rangle \to 3x$ from $\mathbb{Z}/\langle 3 \rangle$ to $\mathbb{Z}_6$ is a homomorphism.
But it is not a function, since $0 + \langle 3 \rangle = 3 + \langle 3 \rangle$ in $\mathbb{Z}/\langle 3 \rangle$ but $3 \cdot 0 \neq 3 \cdot 3$ in $\mathbb{Z}_6$.

The following proposition lists some basic properties of group homomorphisms

Prop. 11.4 Let $\phi : G_1 \to G_2$ be a homomorphism of groups. Then

① If e is the identity of G_1, then $\phi(e)$ is the identity of G_2

② For any element $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$

③ If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2

④ If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{g : G_1 \cdot \phi(g) \in H_2\}$ is a subgroup of G_1.
Also, if $H_2 \lhd G_2$, then $\phi^{-1}(H_2) \lhd G_1$
(normal)

Proof ① Suppose e and e' are the identities of G_1 and G_2, respectively.

Then $e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$

since ϕ is a homomorphism

$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$
B.P. of G_1 B.O. of G_2
$\phi(ee) = \phi(e)$

By right cancellation $e' = \phi(e)$.

② For any $g \in G_1$,

since ϕ is a hom.

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e'$$

from property ①

Thus $\phi(g^{-1}) = \frac{1}{\phi(g)} e' = (\phi(g))^{-1} e' = (\phi(g))^{-1}$

since e' is the identity of G_2

③ $\phi(H_1)$ is a nonempty set since the identity of G_2 is in $\phi(H_1)$. from prop. ①

Suppose that H_1 is a subgroup of G_1 and let $x, y \in \phi(H_1)$.

$\exists\ a, b \in H_1$ s.t. $\phi(a) = x$ and $\phi(b) = y$.

Since
$$\begin{aligned} x y^{-1} &= \phi(a)(\phi(b))^{-1} \\ &= \phi(a)\phi(b^{-1}) && \text{by property ②} \\ &= \phi(ab^{-1}) && \text{since } \phi \text{ is a homomorphism.} \\ &\in \phi(H_1) && \text{since } a, b \in H_1 \text{ and } H_1 \text{ is a subgroup, } ab^{-1} \in H_1. \end{aligned}$$

Thus $\phi(H_1)$ is a subgroup of G_2 by prop. 3.31.

i.e Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \phi$ and whenever $g, h \in H$ then gh^{-1} is in H.

④ Let H_2 be a subgroup of G_2 and define H_1 to be $\phi^{-1}(H_2)$

That is, $H_1 = \{g \in G_1 : \phi(g) \in H_2\}$

- The identity e is in H_1 since $\phi(e) = e' \in H_2$
- If $a, b \in H_1$ then $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} \in H_2$ since H_2 is a subgroup of G_2.

$\rightarrow \phi(ab^{-1}) \in H_2 \Rightarrow ab^{-1} \in \underbrace{\phi^{-1}(H_2)}$

Thus $ab^{-1} \in H_1$ and H_1 is a subgroup of G_1

since by def^n of H_1 $ab^{-1} \in H_1 : \phi(ab^{-1}) \in H_2$

this implies $\phi^{-1}(H_2)$ is a subgroup but this is the def^n of H_1 so H_1 is a subgroup

- If H_2 is normal in G_2, then we must show that $g^{-1}hg \in H_1$ for $h \in H_1$ and $g \in G_1$.

Recall

Theorem 10.3 Normal subgroup test

A subgroup H of G is normal in G if and only if $gHg^{-1} \subseteq H \quad \forall g \in G$

But $\phi(g^{-1}hg) = \phi(g^{-1})\phi(h)\phi(g)$

$= (\phi(g))^{-1}\phi(h)\phi(g) \quad \in H_2$

since H_2 is a normal subgroup of G_2. Thus $g^{-1}hg \in H_1$. by def^n of $H_1 = \{g \in G_1 : \phi(g) \in H_2\}$ □

Let $\phi: G \to H$ be a group homomorphism and suppose that e is the identity of H.

From Prop. 11.4 (4) we know that if H_2 is a subgroup of G_2 then $\phi^{-1}(H_2)$ is a subgroup of G_1 (where $\phi: G_1 \to G_2$). Thus, in this case, $\phi^{-1}(\{e\})$ is a subgroup of G. This subgroup of G is called the kernel of ϕ, denoted by $\boxed{\ker\phi}$. Equivalently: $\boxed{\ker\phi = \{g \in G : \phi(g) = e\}}$

Theorem 11.5 Let $\phi: G \to H$ be a group homomorphism. Then $\ker\phi$ is a normal subgroup of G.

Note This says that with every homomorphism of groups we can naturally associate a normal subgroup.

Example Let $\phi: GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined by $\boxed{\phi(A) = \det(A)}$ be a homomorphism.

Identity of $\mathbb{R}^*$ is 1.

Thus $\ker\phi$ is all 2x2 matrices having determinant 1.

i.e. $\ker\phi = \phi^{-1}(\{e\}) = \{g \in G_1 : \phi(g) = \{e\})$

This implies that $\ker\phi = SL_2(\mathbb{R})$

Example The kernel of the group homomorphism $\phi: \mathbb{R} \to \mathbb{C}^*$ defined by $\phi(\theta) = \cos\theta + i\sin\theta$ is $\{2\pi n \cdot n \in \mathbb{Z}\}$.

This is because:

$\phi(2\pi n) = \cos(2\pi n) + i\sin(2\pi n) = 1$ and 1 is the identity of $\mathbb{C}^*$

We note that since $\boxed{\ker\phi = \{2\pi n : n \in \mathbb{Z}\}}$ we have that $\ker\phi$ is isomorphic to $\mathbb{Z}$.

$$\boxed{\ker\phi \cong \mathbb{Z}}$$

Example How do we find all possible homomorphisms $\phi: \mathbb{Z}_7 \to \mathbb{Z}_{12}$?

Since $\ker\phi$ must be a subgroup of $\mathbb{Z}_7$, there are only two possible kernels: $\{0\}$ and all of $\mathbb{Z}_7$

The image of a subgroup of $\mathbb{Z}_7$ must be a subgroup of $\mathbb{Z}_{12}$.
This implies that there is no injective homomorphism.
Otherwise $\mathbb{Z}_{12}$ would have a subgroup of order 7 which is not possible.

Therefore, the only possible homomorphism $\phi: \mathbb{Z}_7 \to \mathbb{Z}_{12}$ is the one that maps all elements to 0.

Example. Let G be a group. Suppose $g \in G$ and $\phi: \mathbb{Z} \to G$, given by $\phi(n) = g^n$ is a homomorphism

- If the order of g is infinite, then the kernel of this homomorphism is $\{0\}$ since ϕ maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g.
- If g has finite order, say n, then $\ker\phi = n\mathbb{Z}$.

CHAPTER 16 RINGS

So far we studied sets with a single binary operation satisfying certain axioms. Often, we are interested in working with sets that have two binary operations. E.g. think of the integers with the operations of addition and multiplication. These are related by the distributive property.

If we consider a set with two such related binary operations satisfying certain axioms, we have an algebraic structure called a ring.

Section 16.1: Rings

Definition: A nonempty set R is a ring if it has two closed binary operations, addition and multiplication, satisfying the following conditions:

a ring is an abelian group under addition

1. $a+b=b+a$ for $a,b \in R$
2. $(a+b)+c = a+(b+c)$ for $a,b,c \in R$
3. There is an element 0 in R such that $a+0=a$ for all $a \in R$
4. For every element $a \in R$, there exists an element $-a$ in R such that $a+(-a)=0$
5. $(ab)c = a(bc)$ for $a,b,c \in R$
6. For $a,b,c \in R$

$$a(b+c) = ab+ac$$
$$(a+b)c = ac+bc$$

distributive axiom

In 3. We have not assumed that $0 \cdot a = a \cdot 0 = 0$ $\forall a \in R$. What 3. says is that 0 is an identity with respect to addition.

We do not assume that multiplication is commutative and we have not assumed that there is an identity for multiplication, much less that elements have inverses with respect to multiplication.

In 4. $-a$ is the additive inverse of a. Subtraction in a ring is defined by the rule $a-b = a+(-b)$ $\forall a,b \in R$.

the multiplicative identity is not the additive identity

Def^n: If there is an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for each element $a \in R$ we say that R is a ring with unity or identity.

Def^n: A ring R for which $ab = ba$ $\forall a,b \in R$ is called a commutative ring

Note that the addition in a ring is always commutative but the multiplication may not be commutative

Def^n: A ring R is said to be an integral domain if the following conditions hold:

1. R is commutative
2. R contains an identity $1 \neq 0$
3. If $a,b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$

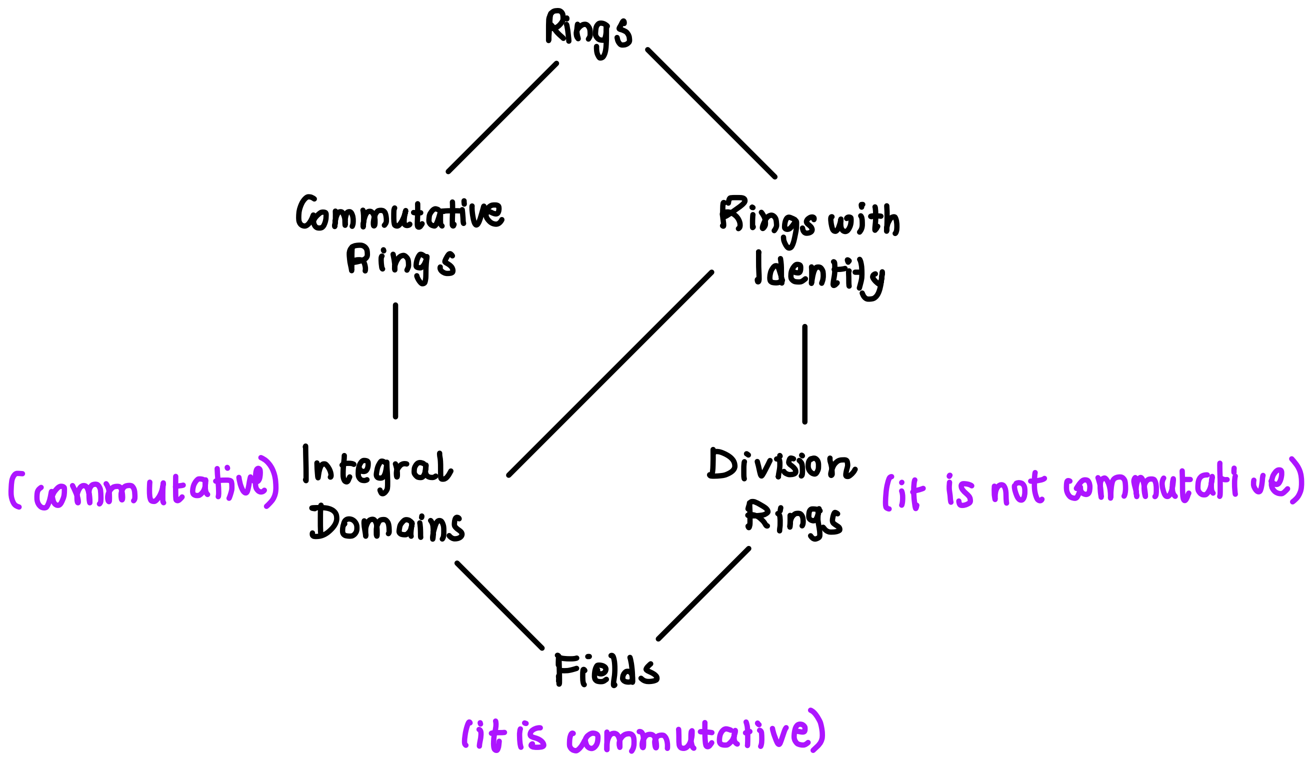
Def^n: A division ring is a ring R with an identity, in which every nonzero element in R is a unit. That is, for each $a \in R$ with $a \neq 0$, $\exists$ a unique element a^{-1} such that $a^{-1}a = aa^{-1} = 1$

Def^n: A ring R is said to be a field if it satisfies the following properties

1. R is commutative
2. R contains an identity $1 \neq 0$
3. For each $x \in R$ such that $x \neq 0$ $\exists$ $y \in R$ such that $xy = 1$.

I.e. a field is a commutative division ring.

TYPES OF RINGS



Example The integers form a ring, since they satisfy axioms 1-6.

$\mathbb{Z}$ is also an integral domain. I.e. it is a commutative ring with identity. Recall that this means there is an element $1 \in \mathbb{Z}$ such that $1 \neq 0$ and $1a = a1 = a$, for each $a \in \mathbb{Z}$. (more succinctly for every $a, b \in \mathbb{Z}$ such that $ab = 0$ either $a = 0$ or $b = 0$).

$\mathbb{Z}$ is not a field. There is no integer that is a multiplicative inverse of 2 since $1/2 \notin \mathbb{Z}$. The only integers with multiplicative inverses are 1 and -1

Example. Under the ordinary operations of addition and multiplication all of the familiar number systems are rings:

- the rationals $\mathbb{Q}$
- the real numbers $\mathbb{R}$
- the complex numbers $\mathbb{C}$

Each of these rings is a field.

<u>Example</u> We can define the product of two elements $a, b \in \mathbb{Z}_n$ by $ab \pmod{n}$

e.g. in $\mathbb{Z}_{12}$. $5 \cdot 7 \equiv 11 \mod 12$

- This product makes the abelian group $\mathbb{Z}_n$ into a ring. (check that it satisfies the 6 axioms of a ring).

- $\mathbb{Z}_n$ is a commutative ring
- $\mathbb{Z}_n$ might fail to be an integral domain

  e.g. Consider $3 \cdot 4 \equiv 0 \pmod{12}$ in $\mathbb{Z}_{12}$. A product of two nonzero elements in the ring can be equal to zero.

  Recall for an integral domain for every $a, b \in R$ such that $ab = 0$ either $a = 0$ or $b = 0$.

<u>Definition</u>. A nonzero element a in a ring R is called a **zero divisor** if there is a nonzero element $b \in R$ s.t. $ab = 0$.

e.g. In $3 \cdot 4 \equiv 0 \pmod{12}$ in $\mathbb{Z}_{12}$, 3 and 4 are zero divisors in $\mathbb{Z}_{12}$.

<u>Example</u>. In calculus the continuous real-valued functions on an interval $[a, b]$ form a commutative ring.

Explanation: We add or multiply two functions by adding or multiplying the values of the functions If $f(x) = x^2$ and $g(x) = \cos x$, then

$$(f+g)(x) = f(x) + g(x) = x^2 + \cos x$$
$$(fg)(x) = f(x)g(x) = x^2 \cos x.$$

Example. The 2x2 matrices with entries in $\mathbb{R}$ form a ring under the usual operations of matrix addition and multiplication

However, the ring is noncommutative, since usually $AB \neq BA$.

Note that we can have $AB = 0$ when neither A nor B is zero

e.g. $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (thus the 2x2 matrices are not an integral domain)

Example Example of a noncommutative division ring

Let $\underline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\underline{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\underline{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\underline{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ where $i^2 = -1$

We can check that these elements satisfy the following relations:

$$\underline{i}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\underline{1} = \underline{j}^2 = \underline{k}^2$$

$$\underline{ij} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \underline{k}$$

$$\underline{jk} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \underline{i}$$

$$\underline{ki} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \underline{j}$$

$$\underline{ji} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -\underline{k}$$

$$\underline{kj} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -\underline{i}$$

$$\underline{ik} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -\underline{j}$$

Let $\mathbb{H}$ consist of elements that have the form $\boxed{a + b\underline{i} + c\underline{j} + d\underline{k}}$ where $a, b, c, d \in \mathbb{R}$.

Equivalently, $\mathbb{H}$ can be considered as the set of all 2x2 matrices of the form

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \quad \text{where} \quad \begin{aligned} \alpha &= a + di \in \mathbb{C} \\ \beta &= b + ci \in \mathbb{C} \end{aligned}$$

$$= \begin{pmatrix} a+di & b+ci \\ -b+ci & a-di \end{pmatrix} = \begin{pmatrix} a+di & b+ci \\ -(b-ci) & a-di \end{pmatrix}$$

We can define addition and multiplication on $\mathbb{H}$ either by the usual matrix operations or in terms of the generators $1, \underline{i}, \underline{j}, \underline{k}$.

Addition $(a_1 + b_1\underline{i} + c_1\underline{j} + d_1\underline{k}) + (a_2 + b_2\underline{i} + c_2\underline{j} + d_2\underline{k})$

$$= (a_1 + a_2) + (b_1 + b_2)\underline{i} + (c_1 + c_2)\underline{j} + (d_1 + d_2)\underline{k}$$

Multiplication $(a_1 + b_1\underline{i} + c_1\underline{j} + d_1\underline{k})(a_2 + b_2\underline{i} + c_2\underline{j} + d_2\underline{k})$

$$\begin{aligned} &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) \\ &\quad + (a_1 b_2 + a_2 b_1 + c_1 d_2 - d_1 c_2)\underline{i} \\ &\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)\underline{j} \\ &\quad + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)\underline{k} \end{aligned}$$

When doing this calculation recall the relations between the generators $\underline{i}, \underline{j}$ and $\underline{k}$

$$:= \alpha + \beta\underline{i} + \gamma\underline{j} + \delta\underline{k}$$

The ring $\mathbb{H}$ is called the $\boxed{\text{ring of quaternions}}$

Q: Show that the quaternions are a division ring.

i.e. show that for each $a \in R$ with $a \neq 0$, $\exists$ a unique element a^{-1} such that

$$a^{-1}a = aa^{-1} = 1$$

(find an inverse for each nonzero element)

A : Notice that $(a+b\underline{i}+c\underline{j}+d\underline{k})(a-b\underline{i}-c\underline{j}-d\underline{k})$

$$\begin{aligned}
&= a^2+b^2+c^2+d^2 \\
&\quad + \left(\cancel{a(-b)} + \cancel{ab} + \cancel{c(-d)} - \cancel{d(-c)}\right)\underline{i} \\
&\quad + \left(\cancel{a(-c)} - \cancel{b(-d)} + \cancel{ca} + \cancel{d(-b)}\right)\underline{j} \\
&\quad + \left(\cancel{a(-d)} + \cancel{b(-c)} - \cancel{c(-b)} + \cancel{da}\right)\underline{k} \\
&= a^2+b^2+c^2+d^2
\end{aligned}$$

This element can be zero if and only if a, b, c, d are all zero.

So if $a+b\underline{i}+c\underline{j}+d\underline{k} \neq 0$

$$\underbrace{(a+b\underline{i}+c\underline{j}+d\underline{k})}_{\text{if this is } a\in R}\underbrace{\left(\frac{a-b\underline{i}-c\underline{j}-d\underline{k}}{a^2+b^2+c^2+d^2}\right)}_{\text{this is } a^{-1}\in R \text{ satisfying } aa^{-1}=a^{-1}a=1.} = 1.$$

Proposition 16.8: Let R be a ring with $a, b \in R$. Then

① $a0 = 0a = 0$

② $a(-b) = (-a)b = -ab$

③ $(-a)(-b) = ab$

Proof ① Note that $0 + a0 = a(0+0) = a0 + a0$

distributive property $a(b+c) = ab+ac$

R is a group under addition with additive identity 0

Thus $a0 = 0$. (by the right cancel.)

Similarly $0a = (0+0)a = 0a + 0a \Rightarrow 0a = 0$

distributive property $(b+c)a = ba+ca$

② We have $ab + a(-b) = a(b-b) = a0 = 0$ (from ①)

$$\Rightarrow a(-b) = -ab$$

Similarly $ab + (-a)b = (a-a)b = 0b = 0$

$$\Rightarrow (-a)b = -ab.$$

Thus $a(-b) = (-a)b = -ab$

$a(-b) + ab$
$= a(-b+b)$
$= a0$
$= 0$

Adding $-ab$ to both sides gives $a(-b) = -ab$

③ This follows from ② since $(-a)(-b) = -(a(-b)) = -(-ab) = ab.$ □

<u>Note</u> Some have the mistaken tendency to treat a ring as if it were a group under multiplication. But it is <u>not</u>. The two most $\boxed{\text{common errors}}$ are the assumptions that:

- → ring elements have multiplicative inverses – they need not
- → a ring has a multiplicative identity – it need not.

For example, if $a, b, c \in R$, $a \neq 0$ and $ab = ac$, we <u>cannot</u> conclude that $b = c$.
(the right might not have a multiplicative cancellation)

Similarly, if $a^2 = a$, we cannot conclude that $a = 0$ or $a = 1$ (as is the case w/ $\mathbb{R}$)
(the ring might not have a multiplicative identity)

Similar to subgroups of groups, we have subrings for rings.

<u>Example</u> If R is any ring, then the set $M_n(\mathbb{R})$ of $n \times n$ matrices with coefficients in $\mathbb{R}$ with the usual addition and multiplication of matrices forms a ring. Here the <u>additive identity is the zero matrix</u> and the multiplicative identity is the identity matrix (hence the names).

$M_n(\mathbb{R})$ is a non-commutative ring.

Definition A subring S of a ring R is a subset S of R such that R is also a ring under the inherited operations from R.

Just as was the case for subgroups, there is a simple test for subrings

SUBRING TEST

A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication; that is, if $a-b$ and ab are in S whenever a and b are in S.

Proof Since addition in R is commutative and S is closed under subtraction we know by the subgroup test that S is an abelian group under addition.

Why?

Recall that the subgroup test stated: let G be a group and H a nonempty subset of G. If $ab^{-1} \in H$ whenever $a, b \in H$, then H is a subgroup of G.

In additive notation, if $a-b \in H$ whenever $a, b \in H$, then H is a subgroup of G.

Also, since multiplication in R is associative as well as distributive over addition the same is true for multiplication in S.

Axioms
5. $(ab)c = a(bc)$ for $a, b, c \in R$
6. For $a, b, c \in R$

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

$$a(b-c) = ab - ac \in H \quad \text{whenever} \quad ab, ac \in H$$

Thus, the only condition remaining to be checked is that multiplication is a binary operation on S but this is exactly what closure is.

Example The ring $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Notice that even though the original ring might not have a multiplicative identity, we do not require that its subring has an identity.

Recall $2 \in \mathbb{Z}$, does not have a multiplicative inverse $\left(\frac{1}{2} \notin \mathbb{Z}\right)$
The multiplicative identity would be $1 \in \mathbb{Z}$ $\quad a \cdot 1 = a$

Example Let $R = \mathbb{M}_2(\mathbb{R})$ be the ring of 2×2 matrices with entries in $\mathbb{R}$.
If T is the set of upper triangular matrices in R, i.e.

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

then T is a subring of R. If $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$ are in T then

$$A - B = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix} \in T \text{ also.}$$

Similarly, $AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \in T$ also.

Thus T is a subring of R.

Example Given two rings R, S, the product ring $R \times S$ is defined as a set by $R \times S = \{(r,s) : r \in R,\ s \in S\}$ with operations of addition and multiplication performed component wise.

The additive identity is given by $(0_R, 0_S)$ and the multiplicative identity is given by $(1_R, 1_S)$. If R is a ring and $A, B \subset R$ are two subrings, then using the subring test one can check that $A \cap B$ is another subring of R.

Integral domains and fields

Remembering some of the definitions we have already seen...

- If R is a ring and r is a nonzero element in R, then r is said to be a zero divisor if there is some nonzero element $s \in R$ such that $rs = 0$.

- A commutative ring with identity is an integral domain if it has no zero divisors. i.e. if for every $r, s \in R$ such that $rs = 0$, either $r = 0$ or $s = 0$.

- If an element a in a ring R with identity has a multiplicative inverse, we say a is a unit. i.e. for each $a \in R$ with $a \neq 0$ $\exists$ a unique a^{-1} s.t $a^{-1}a = aa^{-1} = 1$.

- If every nonzero element in a ring R is a unit, then R is called a division ring

- A commutative division ring is a field.

Example If $i^2 = -1$, then $\boxed{\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}}$ forms a ring known as the Gaussian integers

The Gaussian integers are a subring of the complex numbers since they are closed under addition and multiplication.

Say $m + ni \in \mathbb{Z}[i]$ for $m, n \in \mathbb{Z}$ and $q + si \in \mathbb{Z}[i]$ for $q, s \in \mathbb{Z}$. Then

$$(m+ni) + (q+si) = (m+q) + (n+s)i \in \mathbb{Z}[i]$$

Similarly $(m+ni)(q+si) = mq + msi + nqi - ns$

$$= (mq-ns) + (ms+nq)i \in \mathbb{Z}[i]$$

Let $\alpha = a+bi$ be a unit in $\mathbb{Z}[i]$. Then $\bar{\alpha} = a-bi$ is also a unit since

if $\alpha\beta = 1$ then $\bar{\alpha}\bar{\beta} = 1$.

multiplicative identity

by def^n of a unit: for each $a \in R$ with $a \neq 0$ $\exists$ a unique a^{-1} s.t. $a^{-1}a = aa^{-1} = 1$.

in this case for each $\alpha \in \mathbb{Z}[i]$ $\exists$ β s.t. $\alpha\beta = 1$.

Then $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta} = 1$

If $\beta = c+di$ then $1 = (\alpha\beta)(\bar{\alpha}\bar{\beta})$

$$= (a+bi)(c+di)\,(a-bi)(c-di)$$

$$= (a^2+b^2)(c^2+d^2)$$

since $\mathbb{Z}[i] = \{m+ni : m,n \in \mathbb{Z}\}$

When can this happen? Say $a+bi = 1$ and $c+di = 1$

$$\Rightarrow (a^2+b^2)(c^2+d^2) = 1$$

If $a+bi = -1$ and $c+di = -1$ $\Rightarrow (a^2+b^2)(c^2+d^2) = 1$

If $a+bi = i$ and $c+di = i$ $\Rightarrow (a^2+b^2)(c^2+d^2) = 1$

If $a+bi = -i$ and $c+di = -i$ $\Rightarrow (a^2+b^2)(c^2+d^2) = 1$

Thus, units of this ring are ± 1 or $\pm i$.

Q Are the Gaussian integers a field?

A No, they are not a field.

Proposition 16.15 Cancellation law

Let D be a commutative ring with identity. Then D is an integral domain if and only if $\forall$ nonzero elements $a \in D$ with $ab = ac$ we have $b = c$

Proof $(\Rightarrow)$ Let D be an integral domain.

Then D has no zero divisors. (by definition)

Let $ab = ac$ with $a \neq 0$.

Then $ab - ac = 0 \Rightarrow a(b-c) = 0$ from the distributive property.

Since D is an integral domain then for every $r, s \in D$ s.t $rs = 0$, either $r = 0$ or $s = 0$.

In this case since $a \neq 0$, $b - c = 0$.

Therefore $b = c$.

$(\Leftarrow)$ Let us now suppose that cancellation is possible in D.

i.e. suppose that $ab = ac \Rightarrow b = c$.
(as in the assumption in the proposition)

Let $ab = 0$. If $a \neq 0$ then $ab = a0$ or $b = 0$.

Thus a cannot be a zero divisor. (recall $r \neq 0$, $r \in R$ is said to be a zero divisor if $\exists$ $s \neq 0$, $s \in R$ s.t. $rs = 0$).

Example Field with 9 elements

Let $\mathbb{Z}_3[i] = \{m+ni : m,n\in\mathbb{Z}_3\}$

$$= \{0,1,2,\ i,1+i,2+i,\ 2i,1+2i,2+2i\}, \quad \text{where } i^2=-1$$

This is the ring of Gaussian integers modulo 3.

Elements are added and multiplied as in the complex numbers, except that the coefficients are reduced modulo 3.

Note that $-1=2$

This means that the additive inverse of 1 (i.e. -1) is 2. $1+2=0 \mod 3$

additive identity

Example Let $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b\in\mathbb{Q}\}$. Check that it's a ring!

Q: Is it a field?

A: This means that every nonzero element must be a unit ($\exists$ a mult. inverse)

The multiplicative inverse of any nonzero element of the form $a+b\sqrt{2}$ is $\frac{1}{a+b\sqrt{2}}$. We rationalize this to get

$$\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} - \frac{b\sqrt{2}}{a^2-2b^2}$$

$$= \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$$

$$= c+d\sqrt{2}$$

Thus the inverse of $a+b\sqrt{2}$ is $c+d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

Note that $a+b\sqrt{2}\neq 0$ guarantees that $a-b\sqrt{2}\neq 0$.

Wedderburn's theorem

Theorem 16.16: Every finite integral domain is a field.

Proof Let D be a finite integral domain.

Let D^* be the set of nonzero elements of D.

We must show that every element in D^* has an inverse. (this is precisely a field)

For each $a \in D^*$ we can define a map $\lambda_a : D^* \to D^*$ by $\boxed{\lambda_a(d) = ad}$

If $a \neq 0$ and $d \neq 0$ then $ad \neq 0$ Why? Because for an integral domain for every $a, b \in R$ s.t $ab = 0$ either $a = 0$ or $b = 0$.
If neither $a = 0$ nor $b = 0$ then $ab \neq 0$.

The map λ_a is one-to-one since for $d_1, d_2 \in D^*$

$$\lambda_a(d_1) = \lambda_a(d_2)$$
$$\Rightarrow \quad ad_1 = ad_2$$

which by left-cancellation gives $d_1 = d_2$.

Recall that by proposition 16.15 the multiplicative cancellation law holds when D is an integral domain.

Since D^* is a finite set (look at the statement of theorem 16.16), the map λ_a must also be onto. Hence for some $d \in D^*$, $\lambda_a(d) = ad = 1$.

↑ we know $1 \in D^*$ because D is an integral domain which means it's a ring with an identity

Thus a has a right inverse.

Since D is commutative, a also has a left inverse, which is d.

Therefore, D is a field.

$\square$

For any nonnegative integer n and any element r in a ring R we write $r+\dots+r$ n times as nr.

[order of the underlying group]

Definition The characteristic of a ring R is the least positive integer n such that $\boxed{nr=0 \quad \forall\, r\in R}$ order under addition

If no such integer exists, then the characteristic of R is defined to be 0.

We denote the characteristic of R by $\boxed{\text{char } R}$.

Example. For every prime p, $\mathbb{Z}_p$ is a field of characteristic p.

By proposition 3.4 every nonzero element in $\mathbb{Z}_p$ has an inverse, hence $\mathbb{Z}_p$ is a field.

[Remark: In property (c) of prop. 3.4 we had the following:

Let $\mathbb{Z}_n$ be the set of integers mod n. Let a be a nonzero integer. Then $\gcd(a,n)=1$ if and only if $\exists$ a multiplicative inverse b for a (mod n). i.e. a nonzero integer b s.t. $ab\equiv 1 \pmod n$]

If a is any nonzero element in the field, then $pa=0$, since the order of any non-zero element in the abelian group $\mathbb{Z}_p$ is p

By the definition of the characteristic of a ring R, we know that $\mathbb{Z}_p$ is a field of characteristic p.

Lemma 16.18 Let R be a ring with identity.
If 1 has order n, then the characteristic of R is n.

Proof If 1 has order n, then n is the least positive integer such that $\boxed{n1=0}$ thus, for all $r \in R$,

$nr = n(1r)$ using the definition of identity $1r = r1 = r$

$= (n1)r$ by associativity (axiom 5 of rings)

$= 0r$ since 1 has order $n \Rightarrow n1 = 0$

$= 0$

If no positive n exists such that $n1=0$ then the characteristic of R is zero.

Theorem 16.19 The characteristic of an integral domain is either prime or zero

Proof Let D be an integral domain.

Suppose that the characteristic of D is n with $n \neq 0$.

- If n is not prime then $n = ab$ where $\boxed{1<a<n}$ and $\boxed{1<b<n}$

By lemma 16.18, we need only consider the case $n1=0$.

Since $0 = n1$
$= (ab)1$
$= (a1)(b1)$ we can do this by def^n of an identity $a1 = a$ and $b1 = b$.

and an integral domain has no zero divisors, we have either $a1 = 0$ or $b1 = 0$.

↳ these imply that the characteristic of D is either a or b and both are less than n.

Thus, the characteristic of D must be less than n, which is a contradiction.

Thus, n must be prime.

$\square$

Section 16.3 RING HOMOMORPHISMS AND IDEALS

If you recall from back when we were doing groups, a homomorphism is a map that preserves the operation of the group.

Similarly, a homomorphism between rings preserves the operations of addition and multiplication in the ring.

Definition: If R and S are rings, then a **ring homomorphism** is a map $\phi : R \to S$ satisfying

$$\boxed{\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \end{aligned}}$$

$\forall a, b \in R$.

Definition: If $\phi : R \to S$ is a one-to-one and onto homomorphism, then ϕ is called a **ring isomorphism**.

Definition: For any ring homomorphism $\phi : R \to S$, we define the **kernel** of a ring homomorphism to be the set

$$\boxed{\ker \phi = \{ r \in R : \phi(r) = 0 \}}$$

<u>Example</u> For any integer n we can define a ring homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}_n$ by $\boxed{\phi(a) = a \pmod{n}}$. Let's check that this is actually a ring homomorphism

$$\begin{aligned}\phi(a+b) &= a+b \pmod{n} \\ &= a \pmod{n} + b \pmod{n} \\ &= \phi(a) + \phi(b)\end{aligned}$$

and
$$\begin{aligned}\phi(ab) &= ab \pmod{n} \\ &= a \pmod{n} \cdot b \pmod{n} \\ &= \phi(a)\phi(b)\end{aligned}$$

<u>Q</u> : What's the kernel of this ring homomorphism?

<u>A</u> : $\ker\phi = n\mathbb{Z}$ ← integers that are multiples of n, i.e. $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$

<u>Example</u> Let $C[a,b]$ be the ring of real-valued, continuous functions on an interval $[a,b]$.

[This is a (commutative ring). $(f+g)(x) = f(x) + g(x)$
and $(fg)(x) = f(x)g(x)$]

For a fixed $\alpha \in [a,b]$, we can define a ring homomorphism $\phi_\alpha : C[a,b] \to \mathbb{R}$ by $\boxed{\phi_\alpha(f) = f(\alpha)}$

Let's check this is indeed a ring homomorphism:

$$\begin{aligned}\phi_\alpha(f+g) &= (f+g)(\alpha) \\ &= f(\alpha) + g(\alpha) \\ &= \phi_\alpha(f) + \phi_\alpha(g)\end{aligned}$$

$$\phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g)$$

In fact, this type of ring homomorphism $\phi_\alpha(f) = f(\alpha)$ is known as evaluation homomorphism.

<u>Proposition 16.22</u> Let $\phi: R \to S$ be a ring homomorphism

1. If R is a commutative ring, then $\phi(R)$ is also a commutative ring
2. $\phi(0) = 0$
3. Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto then $\phi(1_R) = 1_S$
4. If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.

Recall that several sections ago when we were learning group theory we saw that <u>normal subgroups</u> are interesting to study.

The corresponding objects in ring theory are special subrings known as ideals.

<u>Definition</u>: An ideal in a ring R is a subring I of R such that if $a \in I$ and $r \in R$, then both $\boxed{ar \in I \text{ and } ra \in I}$

That is, a subring I of a ring R is an ideal of R if I "absorbs" elements from R. i.e. if $rI = \{ra \mid a \in I\} \subseteq I$ and $Ir = \{ar \mid a \in I\} \subseteq I$ $\forall r \in R$

<u>Example</u> Every ring R has at least two ideals: $\{0\}$ and R.

We will these ideals the trivial ideal

Let R be a ring with identity and suppose that I is an ideal in R such that $1 \in I$. Since for any $r \in R$, $r1 = r \in I$ by the definition of an ideal, $I = R$.

$r1 \in I$ and $1r \in I$

but by def^n of identity

$r1 = 1r = r \Rightarrow r \in I$

Example If a is an element in a commutative ring R with identity, then the set $\boxed{\langle a \rangle = \{ar : r \in R\} \text{ is an ideal in } R.}$

$\langle a \rangle \neq \emptyset$ since $a = a1$ ← multiplicative identity is in $\langle a \rangle$

(since R is a commutative ring with identity)

The sum of two elements in $\langle a \rangle$ is again in $\langle a \rangle$ since

$$ar + ar' = a(r + r')$$

by the distributive property

Inverse of ar is $-ar = a(-r) \in \langle a \rangle$.

If we multiply an element $ar \in \langle a \rangle$ by an arbitrary element $s \in R$ we have

$$\begin{aligned} s(ar) &= (sa)r && \text{associativity} \\ &= (as)r && \text{commutative (since } R \text{ is a comm. ring)} \\ &= a(sr) && \text{associativity} \end{aligned}$$

Therefore, $\langle a \rangle$ satisfies the definition of an ideal. $\square$

Defn If $a \in I$ and $r \in R$ then both $ar \in I$ and $ra \in I$

→ in our case $ar \in I$ and $s \in R \Rightarrow (ar)s \in I$

and $s(ar) \in I$

would mean that I is an ideal.

Definition : If R is a commutative ring with identity, then an ideal of the form $\langle a \rangle = \{ar : r \in R\}$ is called a principal ideal.

Theorem 16.25 Every ideal in the ring of integers $\mathbb{Z}$ is a principal ideal.

Proof The zero ideal $\{0\}$ is a principal ideal since $\langle 0 \rangle = \{0\}$.

If I is any nonzero ideal in $\mathbb{Z}$, then I must contain some positive integer m.

By the Well-ordering principle $\exists$ a least positive integer $n \in I$.

Now let a be any element in I.

Using the division algorithm, we know $\exists$ $q, r \in \mathbb{Z}$ s.t.

$$a = nq + r \quad \text{with } 0 \leq r < n$$

$\Rightarrow$ $r = a - nq \in I$

But r must be zero since n is the least positive element in I.

$$\Rightarrow \quad a = nq + \underbrace{\cancel{r}}_{0}$$

$$\Rightarrow \quad a = nq$$

and $I = \langle n \rangle$.

$\square$

Example The set $n\mathbb{Z}$ is ideal in the ring of integers.

why? Because if $na \in n\mathbb{Z}$ and $b \in \mathbb{Z}$, then $nab \in n\mathbb{Z}$ as required.

ideal ring

By theorem 16.25 (that every ideal in the ring of integers $\mathbb{Z}$ is a principal ideal), these are the only ideals of $\mathbb{Z}$

[recall that a principal ideal is an ideal of the form $\langle a \rangle = \{ar : r \in R\}$]

Proposition 16.27 The kernel of any ring homomorphism $\phi : R \to S$ is an ideal in R.

Proof From group theory, we know that $\ker\phi$ is an additive subgroup of R. (Check this for practice)

Suppose that $a \in \ker\phi$ and $r \in R$.

For $\ker\phi$ to be an ideal in R we must show that $ar \in \ker\phi$ and $ra \in \ker\phi$.

We have $\phi(ar) = \phi(a)\phi(r)$ by def^n of homom.

$= 0\,\phi(r)$ $a \in \ker\phi \Rightarrow \phi(a) = 0$

$= 0$

and, similarly, $\phi(ra) = \phi(r)\phi(a)$

$= \phi(r)0$

$= 0$

125

Thus $\phi(ar)=0 \Rightarrow ar \in \ker\phi$ and $\phi(ra)=0 \Rightarrow ra \in \ker\phi$.

$\square$

<u>Remark</u> In the definition of an ideal we have required that $rI \subset I$ and $Ir \subset I$ for all $r \in R$. Such ideals are sometimes referred to as two-sided ideals.

But there are also <u>one-sided ideals</u> that only require that either $\underbrace{rI \subset I}_{\text{left ideals}}$ or $\underbrace{Ir \subset I}_{\text{right ideals}}$ for $r \in R$ hold but <u>not</u> both.

- In a commutative ring any ideal must be two-sided.

For the scope of this class you only need to know about two-sided ideals.

<u>Theorem 16.29</u> Let I be an ideal of R. The factor group R/I is a ring with multiplication defined by

$$\boxed{(r+I)(s+I) = rs+I}$$

<u>Proof</u> We know that R/I is an abelian group under addition.

Let $r+I \in R/I$ & $s+I \in R/I$ } We must show that $(r+I)(s+I)=rs+I$ is independent of the choice of coset

This is equivalent to showing that if $r' \in r+I$ and $s' \in s+I$, then $r's' \in rs+I$.

Since $r' \in r+I$ $\exists$ an element $a \in I$ such that $r' = r+a$.

Similarly, since $s' \in s+I$ $\exists$ $b \in I$ s.t. $s' = s+b$.

$$\Rightarrow \quad r's' = (r+a)(s+b)$$
$$= rs + \underbrace{rb + as + ab}_{\text{the ideal } I \text{ "absorbs" these elements}}$$

Since I is an ideal we have that $rb + as + ab \in I$

Therefore $r's' \in rs + I$

Since $a \in I$ and $b \in I$
for $r \in R$, $rb \in I$ } def^n of ideal
$s \in R$, $as \in I$
(and $ab \in I$ by closure)

To show that R/I is a ring with multiplication we must also prove the last two axioms of a ring. Namely that associativity and the distributive property hold. Please check this!

<u>Definition</u>: The ring R/I with multiplication defined as

$$\boxed{(r+I)(s+I) = rs + I}$$

is called the factor or quotient ring

Just as with group homomorphisms and normal subgroups, we have a relationship between ring homomorphisms and ideals.

<u>Theorem 16.30</u> Let I be an ideal of R. The map $\phi: R \to R/I$ defined by $\phi(r) = r+I$ is a ring homomorphism of R onto R/I with kernel I.

<u>Proof</u>. $\phi: R \to R/I$ is a surjective abelian group homomorphism

$$\phi(r+s) = (r+s)+I \underset{\uparrow}{=} (r+I)+(s+I) = \phi(r)+\phi(s)$$

definition of addition binary operation

We must now show that ϕ is a ring homomorphism, so it works correctly under ring multiplication.

Let $r, s \in R$, then

$$\phi(r)\phi(s) = (r+I)(s+I)$$

for the factor group R/I the ring multipl. is $(r+I)(s+I) = rs+I$.

$$= rs + I$$
$$= \phi(rs)$$

□

<u>Example</u> $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$.

Recall from pg 83 of these notes that elements of $\mathbb{Z}/n\mathbb{Z}$ are the cosets:

$$n\mathbb{Z},\ 1+n\mathbb{Z},\ 2+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}$$

To see how to add and multiply consider the elements $2+4\mathbb{Z}$ and $3+4\mathbb{Z}$

$$(2+4\mathbb{Z}) + (3+4\mathbb{Z}) = 5+4\mathbb{Z} = 1+4+4\mathbb{Z} = 1+4\mathbb{Z}$$
$$(2+4\mathbb{Z})(3+4\mathbb{Z}) = 6+4\mathbb{Z} = 2+4+4\mathbb{Z} = 2+4\mathbb{Z}$$

Thus, the two operations are essentially modulo 4 arithmetic.

<u>Example</u> $2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$

$2k+6\mathbb{Z}$ mod 6

Let's look at the addition and multiplication operations again.

e.g. $(4+6\mathbb{Z})+(4+6\mathbb{Z}) = 8+6\mathbb{Z} = 2+6+6\mathbb{Z} = 2+6\mathbb{Z}$

$$(4+6\mathbb{Z})(4+6\mathbb{Z}) = 16+6\mathbb{Z} = 4+12+6\mathbb{Z} = 4+6\mathbb{Z}$$

So here the operations are essentially modulo 6 arithmetic

Example Noncommutative ideal and factor ring

Let $R = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \middle| \; a_i \in \mathbb{Z} \right\}$ and let I be the subset of R consisting of matrices with even entries. It can be shown that I is indeed an ideal of R.

$$I = \left\{ \begin{pmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{pmatrix} \middle| \; k_i \in \mathbb{Z} \right\}$$

Then for $A \in R$ and $B \in I$, $AB = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\begin{pmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{pmatrix}$

$$= \begin{pmatrix} 2a_1k_1 + 2a_2k_3 & 2a_1k_2 + 2a_2k_4 \\ 2a_3k_1 + 2a_4k_3 & 2a_3k_2 + 2a_4k_4 \end{pmatrix}$$

$$= \begin{pmatrix} 2(a_1k_1 + a_2k_3) & 2(a_1k_2 + a_2k_4) \\ 2(a_3k_1 + a_4k_3) & 2(a_3k_2 + a_4k_4) \end{pmatrix} \in I$$

since every entry is an even one

$$BA = \begin{pmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in I$$

can be shown in a similar manner to above

Now consider the factor ring R/I.

* The interesting question about this ring is: What is its size?

We claim R/I has <u>16 elements.</u>

In fact $R/I = \left\{ \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} + I \; : \; r_i \in \{0,1\} \right\}$

An example illustrates the typical situation.

Which of the 16 elements is $\begin{pmatrix} 7 & 8 \\ 5 & -3 \end{pmatrix} + I$?

Observe that $\begin{pmatrix} 7 & 8 \\ 5 & -3 \end{pmatrix} + I = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 6 & 8 \\ 4 & -4 \end{pmatrix} + I = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + I$

all even entries so it can be absorbed in the ideal I

in general an ideal absorbs its own elements.

Examples Consider the factor ring of Gaussian integers $R = \mathbb{Z}[i]/\langle 2-i\rangle$

What does this ring look like?

The elements of R all have the form $a+bi+\langle 2-i\rangle$ where $a,b\in\mathbb{Z}$

What do the distinct cosets look like?

The fact that $2-i+\langle 2-i\rangle = 0+\langle 2-i\rangle$ means that when dealing with coset representatives we may treat $2-i$ as equivalent to 0 $\Rightarrow$ $2=i$.
mod $(2-i)$

For example, the coset $3+4i+\langle 2-i\rangle = 3+8+\langle 2-i\rangle = 11+\langle 2-i\rangle$

replaced i with 2 $\Rightarrow$ so $4i$ became 8

Similarly, all the elements of R can be written in the form $\boxed{a+\langle 2-i\rangle,\ a\in\mathbb{Z}.}$

We can further reduce the set of distinct coset representatives by observing that when dealing with coset representatives $\boxed{2=i}$ implies by squaring both sides that

$$\boxed{\begin{array}{l} 4=-1 \\ \text{or} \quad 5=0 \end{array}}$$

Therefore, the coset $3+4i+\langle 2-i\rangle = 11+\langle 2-i\rangle = 1+5+5+\langle 2-i\rangle = 1+\langle 2-i\rangle$

0 0
under the coset representatives

This way we show that every element of R is equal to one of the following cosets:

$0+\langle 2-i\rangle$
$1+\langle 2-i\rangle$
$2+\langle 2-i\rangle$
$3+\langle 2-i\rangle$
$4+\langle 2-i\rangle$
since $5=0$ then $5+\langle 2-i\rangle = 0+\langle 2-i\rangle$

Is any further reduction possible? OK.. enough

To demonstrate that there is not, we will show that $1+\langle 2-i\rangle$ has additive order 5

Since $5(1+\langle 2-i\rangle) = 5+\langle 2-i\rangle = 0+\langle 2-i\rangle$

$1+\langle 2-i\rangle$ has order 1 or order 5. Why can $1+\langle 2-i\rangle$ have order 1? Because depending on the chosen representative it can either be equivalent to the identity or not

If the order is actually 1 then $1+\langle 2-i\rangle = 0+\langle 2-i\rangle$ so $1\in\langle 2-i\rangle$

Thus $1=(2-i)(a+bi) = 2a+2bi-ai+b = 2a+b+(-a+2b)i$ for $a,b\in\mathbb{Z}$

But this implies that $\begin{bmatrix} 2a+b=1 \\ -a+2b=0\end{bmatrix} \Rightarrow$ $a=2b$ and $2(2b)+b=1$

$b=\frac{1}{5}\notin\mathbb{Z}$

Contradiction.

So the ring R is essentially the same as the field $\mathbb{Z}_5$.

Example let $\mathbb{R}[x]$ denote the ring of polynomials with real coefficients and let $\langle x^2+1\rangle$ denote the principal ideal generated by x^2+1.

$$\langle x^2+1\rangle = \{ f(x)(x^2+1) : f(x)\in\mathbb{R}[x]\}$$

Then $$R[x]/\langle x^2+1\rangle = \{g(x)+\langle x^2+1\rangle : g(x)\in\mathbb{R}[x]\}$$
$$= \{ax+b+\langle x^2+1\rangle : a,b\in\mathbb{R}\}$$

To see that this last equality is true note that if $g(x)$ is any member of $\mathbb{R}[x]$, then we may write $g(x)$ in the form

$$g(x) = \underbrace{q(x)}_{\text{quotient}}(x^2+1) + \underbrace{r(x)}_{\text{remainder}}$$

upon dividing $g(x)$ by x^2+1

In particular, $r(x)=0$ or the degree of $r(x)$ is less than 2 so that $r(x)=ax+b$ for some $a,b\in\mathbb{R}$.

$q(x)(x^2+1)$ gets "absorbed" by the ideal $\langle x^2+1\rangle$

Thus $$g(x)+\langle x^2+1\rangle = q(x)(x^2+1)+r(x)+\langle x^2+1\rangle$$
$$= r(x)+\langle x^2+1\rangle$$

How is the multiplication done?

Since $x^2+1+\langle x^2+1\rangle = 0+\langle x^2+1\rangle$ one should think of x^2+1 as 0

$\Rightarrow$ $\boxed{x^2=-1}$

any two elements of $\mathbb{R}[x]/\langle x^2+1\rangle$

So for example: $(x+3+\langle x^2+1\rangle)\cdot(2x+5+\langle x^2+1\rangle)$

$$= 2x^2+5x+6x+15+\langle x^2+1\rangle$$
$$= 2x^2+11x+15+\langle x^2+1\rangle$$
$$= 2(-1)+11x+15+\langle x^2+1\rangle$$

using $x^2=-1$

$$= 11x+13+\langle x^2+1\rangle$$

CHAPTER 17. POLYNOMIALS

I'm sure you are already familiar with polynomials. If you are given two polynomials

e.g. $p(x) = x^3-3x+2$

$q(x) = 3x^2-6x+5$

then it's clear what $p(x)+q(x)$ and $p(x)q(x)$ mean. We just add and multiply polynomials as functions:

$$(p+q)(x) = p(x)+q(x)$$
$$= x^3+3x^2-9x+7$$

and $(pq)(x) = p(x)q(x)$

$$= (x^3-3x+2)(3x^2-6x+5)$$
$$= 3x^5-6x^4-4x^3+24x^2-27x+10$$

It's not surprising perhaps that polynomials form a ring (especially since we've already seen that)

This brings us to the next section of the textbook.

Section 17.1 Polynomial rings

In this section we'll assume that R is a commutative ring with identity

Definitions:

- Any expression of the form $f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ where $a_i \in \mathbb{R}$ and $a_n \neq 0$ is a polynomial over $\mathbb{R}$ with indeterminate x
- The elements $a_0, a_1, \dots, a_n$ are called the coefficients of f.
- a_n = leading coeff.
- A polynomial is called monic if the leading coeff. is 1
- If n is the largest nonnegative number for which $a_n \neq 0$ we say that the degree of f is n, $\deg(f) = n$.

* The set of all polynomials with coefficients in a ring R are denoted by $\mathbb{R}[x]$

- Two polynomials are equal exactly when their corresponding coeff. are equal. I.e. if we let

$$p(x) = a_0 + a_1 x + \dots + a_n x^n$$
$$q(x) = b_0 + b_1 x + \dots + b_m x^m$$

then $p(x) = q(x)$ if and only if $a_i = b_i \ \forall i \geq 0$.

- To show that the set of all polynomials forms a ring, we must first define addition and multiplication.

Then the sum of $p(x)$ and $q(x)$ is $\boxed{p(x) + q(x) = c_0 + c_1 x + \dots + c_k x^k}$ where $\boxed{c_i = a_i + b_i}$ for each i.

Product of two polynomials is $\boxed{p(x)\, q(x) = c_0 + c_1 x + \dots + c_{m+n} x^{m+n}}$ where

$$\boxed{c_i = \sum_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \dots + a_{i-1} b_1 + a_i b_0}, \text{ for each } i.$$

Notice that in each case some of the coefficients may be zero

$$p(x)\, q(x) = \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i$$

Example Let $p(x) = 3 + 3x^3$ and $q(x) = 4 + 4x^2 + 4x^4$ be polynomials in $\mathbb{Z}_{12}[x]$.

The sum is $p(x) + q(x) = 7 + 4x^2 + 3x^3 + 4x^4$

$$p(x)q(x) = (3 + 3x^3)(4 + 4x^2 + 4x^4)$$
$$= 12 + 12x^2 + 12x^4 + 12x^3 + 12x^5 + 12x^7 \pmod{12}$$
$$= 0 \quad \leftarrow \text{zero polynomial}$$

This example tells us that we cannot expect $R[x]$ to be an integral domain if R is not an integral domain.

Example. Consider $f(x) = 2x^3 + x^2 + 2x + 2$ and $g(x) = 2x^2 + 2x + 1$ in $\mathbb{Z}_3[x]$

Then using the definitions of addition and multiplication we get

$$f(x) + g(x) = (2+0)x^3 + (1+2)x^2 + (2+2)x + (2+1)$$
$$= 2x^3 + 3x^2 + 4x + 3 \quad \text{mod } 3$$
$$= 2x^3 + x$$

remember that addition and multipl. of the coeff. is done mod3

and
$$f(x)g(x) = \sum_{i=0}^{3+2}\left(\sum_{k=0}^{i} a_k b_{i-k}\right)x^i = \sum_{i=0}^{5}\left(\sum_{k=0}^{i} a_k b_{i-k}\right)x^i$$
$$= \sum_{i=0}^{5}\left(a_0 b_i + a_1 b_{i-1} + \dots + a_i b_0\right)x^i$$
$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2$$
$$+ (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0)x^3$$
$$+ (a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0)x^4$$
$$+ (a_0 b_5 + a_1 b_4 + a_2 b_3 + a_3 b_2 + a_4 b_1 + a_5 b_0)x^5$$

Now if we look at the polynomials $\begin{bmatrix} f(x) = 2x^3 + x^2 + 2x + 2 \\ g(x) = 2x^2 + 2x + 1 \end{bmatrix}$ we see that

$a_0 = 2$ $\quad$ $b_0 = 1$
$a_1 = 2$ $\quad$ $b_1 = 2$
$a_2 = 1$ $\quad$ $b_2 = 2$
$a_3 = 2$ $\quad$ $b_3 = 0$
$a_4 = 0$ $\quad$ $b_4 = 0$
$a_5 = 0$ $\quad$ $b_5 = 0$

Thus $f(x)g(x) = 2(1) + (\overbrace{2\cdot 2 + 2\cdot 1}^{6})x + (\overbrace{2\cdot 2 + 2\cdot 2 + 1\cdot 1}^{9})x^2$

$+ (\overbrace{2\cdot 0 + 2\cdot 2 + 1\cdot 2 + 2\cdot 1}^{8})x^3$

$+ (\overbrace{2\cdot 0 + 2\cdot 0 + 1\cdot 2 + 2\cdot 2 + 0\cdot 1}^{6})x^4$

$+ (\underbrace{2\cdot 0 + 2\cdot 0 + 1\cdot 0 + 2\cdot 2 + 0\cdot 2 + 0\cdot 1}_{4})x^5$ $\qquad$ mod 3

$= 2 + 2x^3 + x^5$

Theorem Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.

Proof. We first show that $R[x]$ is an abelian group under polynomial addition.

Additive identity: zero polynomial $f(x) = 0$

Given a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i$, the inverse of $p(x)$ is $-p(x) = \sum_{i=0}^{n} (-a_i)x^i = -\sum_{i=0}^{n} a_i x^i$

From the definition of polynomial addition we have commutativity and associativity.

To show that multiplication is associative let

$$p(x) = \sum_{i=0}^{m} a_i x^i, \quad q(x) = \sum_{i=0}^{n} b_i x^i, \quad r(x) = \sum_{i=0}^{n} c_i x^i$$

Then $[p(x)q(x)]\,r(x) = \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{n} c_i x^i\right)$

$= \left[\sum_{i=0}^{m+n} \underbrace{\left(\sum_{j=0}^{i} a_j b_{i-j}\right)} x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right)$

from the earlier def^n we saw for a product of polys.

$= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right) c_{i-j}\right] x^i$

a new multiplication between $\left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)x^i\right]$ which you should treat as a new poly. with another polyn. $\sum_{i=0}^{p} c_i x^i$.

$= \sum_{i=0}^{m+n+p}\left(\sum_{j+k+l=i} a_j b_k c_l\right) x^i$

$\left(\sum_{i=0}^{m+n} d_i x^i\right)\left(\sum_{i=0}^{p} c_i x^i\right)$

$= \sum_{i=0}^{m+n+p}\left(\sum_{j=0}^{i} d_j c_{i-j}\right) x^i$

$= \sum_{i=0}^{m+n+p}\left(\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{i-k}\right)\right) x^i$

$$= \sum_{i=0}^{m+n+p} \left[\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k} \right) \right] x^i$$ go backward & open it up to two sums

$$= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\sum_{i=0}^{n+p} \left(\sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right]$$

$$= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\left(\sum_{i=0}^{n} b_i x^i \right) \left(\sum_{i=0}^{p} c_i x^i \right) \right]$$ using the product representation

$$= p(x) [q(x) r(x)]$$

You can also show the commutative and distributive properties of polynomial multipl. in a similar way.

Proposition 17.4 Let $p(x)$ and $q(x)$ be polynomials in $R[x]$ where R is an integral domain. Then $\boxed{\deg p(x) + \deg q(x) = \deg(p(x)q(x))}$. $R[x]$ is also an integral domain.

Proof Suppose that we have two nonzero polynomials

$$p(x) = a_m x^m + \dots + a_1 x + a_0 \quad \leftarrow \text{degree } m$$
$$q(x) = b_n x^n + \dots + b_1 x + b_0 \quad \leftarrow \text{degree } n$$

with $a_m \neq 0$ and $b_n \neq 0$

The leading term of $p(x)q(x)$ is $\boxed{a_m b_n x^{m+n}}$, by definition. The leading coeff. $a_m b_n$ cannot be zero since R is an integral domain.

Therefore, the degree of $p(x)q(x)$ is $m+n$ and $p(x)q(x) \neq 0$

Since $p(x) \neq 0$ and $q(x) \neq 0$ imply that $p(x)q(x) \neq 0$ we have that the ring of polynomials $R[x]$ is also an integral domain.

□

Theorem 17.5 Let R be a commutative ring with identity and $\alpha \in R$. Then we have a ring homomorphism $\phi_\alpha : R[x] \to R$ defined by

$$\boxed{\phi_\alpha(p(x)) = p(\alpha)} = a_n \alpha^n + \dots + a_1 \alpha + a_0$$

evaluated x at α

where $p(x) = a_n x^n + \ldots + a_1 x + a_0$.

<u>Proof</u> Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x^i$

We show that ϕ_α preserves addition:

$$\begin{aligned}\phi_\alpha(p(x) + q(x)) &= p(\alpha) + q(\alpha) \\ &= \sum_{i=0}^{n} a_i \alpha^i + \sum_{i=0}^{m} b_i \alpha^i \\ &= \phi_\alpha(p(x)) + \phi_\alpha(q(x))\end{aligned}$$

We also show that ϕ_α preserves multiplication:

$$\begin{aligned}\phi_\alpha(p(x))\phi_\alpha(q(x)) &= p(\alpha) q(\alpha) \\ &= \left(\sum_{i=0}^{n} a_i \alpha^i\right)\left(\sum_{i=0}^{m} b_i \alpha^i\right) \\ &= \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) \alpha^i \\ &= \phi_\alpha(p(x) q(x))\end{aligned}$$

since $p(x)q(x) = \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) x^i$. So $\phi_\alpha(p(x)q(x))$ is just $p(\alpha)q(\alpha)$.

The map $\phi_\alpha : R[x] \to R$ is called the <u>evaluation homomorphism</u> at α.

Section 17.2 The division algorithm

Recall back when we covered chapter 2 we learned about the division algorithm for integers.

★ If a and b are integers with $b > 0$, then $\exists$ unique integers q & r s.t. $a = bq + r$ where $0 \le r < b$. ★

A similar theorem exists for polynomials.

Theorem 17.6 (Division algorithm for polynomials)

Let $f(x)$ and $g(x)$ be polynomials in $F[x]$ where $F[x]$ is a field and $g(x)$ is a nonzero polynomial. Then $\exists$ unique polynomials $q(x), r(x) \in F[x]$ s.t.

$$\boxed{f(x) = g(x)q(x) + r(x)}$$

where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

Proof [EXISTENCE of $q(x)$ and $r(x)$]

- If $f(x)$ is the zero polynomial then

$$0 = g(x)\,0 + 0$$

hence both $q(x)$ and $r(x)$ must also be the zero polynomial.

- Now suppose that $f(x)$ is not the zero poly. and that $\boxed{\deg f(x) = n}$ and $\boxed{\deg g(x) = m}$

If $m > n$ then we can let $q(x) = 0$ and $r(x) = f(x)$.

Hence, we assume that $m \leq n$ and continue with proof by induction

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$
$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$

the polynomial $\tilde{f}(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ has degree less than n or is the zero polynomial.

By induction, $\exists$ polynomials $\tilde{q}(x)$ and $r(x)$ s.t.

$$\tilde{f}(x) = \tilde{q}(x)g(x) + r(x)$$

Where $r(x) = 0$ or the degree of $r(x)$ is $< \deg g(x) = m$.

Now let $q(x) = \tilde{q}(x) + \frac{a_n}{b_m} x^{n-m}$

Then $f(x) = q(x)g(x) + r(x)$ with $r(x)$ the zero poly or $\deg r(x) < \deg g(x)$

[UNIQUENESS of $q(x)$ and $r(x)$]

Suppose that $\exists$ two other polynomials $q_1(x)$ and $r_1(x)$ such that

$$f(x) = q_1(x)g(x) + r_1(x)$$

with $\deg r_1(x) < \deg g(x)$ or $r_1(x) = 0$ so that

$$f(x) = q(x)g(x) + r(x)$$
$$= q_1(x)g(x) + r_1(x)$$

Thus $q(x)g(x) + r(x) = q_1(x)g(x) + r_1(x)$

$$\Rightarrow g(x)[q(x) - q_1(x)] = r_1(x) - r(x)$$

If $q(x) - q_1(x)$ is not the zero polynomial, then

$$\deg\left(g(x)[q(x) - q_1(x)]\right) = \deg\left(r_1(x) - r(x)\right) \geq \deg g(x)$$

just taking the degree of both

this inequality holds because as the previous sentence says if $q(x) - q_1(x)$ is not the zero-poly. then $g(x)[q(x) - q_1(x)]$ has degree larger than $g(x)$

But the degrees of both $r(x)$ and $r_1(x)$ are strictly less than the degree of $g(x)$.

Thus $\lightning$ $r(x) = r_1(x)$ and $q(x) = q_1(x)$.

<u>Example</u> (LONG DIVISION FORMALIZATION.)

Suppose we divide $x^3 - x^2 + 2x - 3$ by $x - 2$.

$$\begin{array}{r|l}
 & x^2 + x + 4 \\
x - 2 & x^3 - x^2 + 2x - 3 \\
 & -\underline{(x^3 - 2x^2)} \\
 & \quad x^2 + 2x \\
 & \quad -\underline{(x^2 - 2x)} \\
 & \qquad 4x - 3 \\
 & \qquad -\underline{(4x - 8)} \\
 & \qquad\quad 5
\end{array}$$

This implies that $x^3 - x^2 + 2x - 3 = \underbrace{(x-2)}_{\text{divisor}}\underbrace{(x^2+x+4)}_{\text{quotient}} + \underbrace{5}_{\text{remainder}}$

Definition. Let $p(x)$ be a polynomial in $F[x]$ and $\alpha \in F$. We say that α is a zero or root of $p(x)$ if $p(x)$ is in the kernel of the evaluation homomorphism ϕ_α.
I.e. α is a zero of $p(x)$ if $\phi_\alpha(p(x)) = \boxed{p(\alpha) = 0}$

Corollary 17.8 Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F(x)$ if and only if $x - \alpha$ is a factor of $p(x)$ in $F[x]$. i.e. $p(\alpha) = 0$

Proof ($\Rightarrow$) Suppose that $\alpha \in F$ and $p(\alpha) = 0$
By the division algorithm, $\exists$ polynomials $q(x)$ and $r(x)$ s.t.

$$p(x) = (x-\alpha)q(x) + r(x)$$

and the degree of $r(x)$ must be less than the degree of $x-\alpha$. Since $\deg r(x) < 1$, $r(x) = a$ for $a \in F$. Thus

$$p(x) = (x-\alpha)q(x) + a.$$

However
$$\begin{aligned} 0 &= p(\alpha) \quad \text{(by assumption)} \\ &= (\alpha-\alpha)q(\alpha) + a \\ &= a \end{aligned}$$

So $p(x) = (x-\alpha)q(x) + \underbrace{\cancel{a}}_{0} = (x-\alpha)q(x)$ and $x-\alpha$ is a factor of $p(x)$

($\Leftarrow$) Suppose that $x-\alpha$ is a factor of $p(x)$. Say, $p(x) = (x-\alpha)q(x)$. Then

$$p(\alpha) = 0 \cdot q(\alpha) = 0$$

$\square$

Corollary 17.9 Let F be a field. A nonzero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F.

Proof We use induction on the degree of $p(x)$.

If $\boxed{\deg p(x) = 0}$, then $p(x)$ is a constant polynomial and has no zeros.

Let $\boxed{\deg p(x) = 1}$ Then $p(x) = ax + b$ for some $a, b \in F$.

the coeff. are in F

the entire polynomial is in $F[x]$

If α_1 and α_2 are zeros of $p(x)$, then $a\alpha_1 + b = 0$, $a\alpha_2 + b = 0$ $\Rightarrow \alpha_1 = \alpha_2$

Now assume that $\boxed{\deg p(x) > 1}$

If $p(x)$ does not have a zero in F, then we are done.

If α is a zero of $p(x)$, then $p(x) = (x-\alpha)q(x)$ for some $q(x) \in F[x]$ by Corollary 17.8 The degree of $q(x)$ is $n-1$ by prop. 17.4 (Prop 17.4: $p(x), q(x) \in R[x]$ then $\deg p(x) + \deg q(x) = \deg(p(x)q(x))$)

Here, $\underbrace{\deg p(x)}_{=n} = \deg((x-\alpha)q(x)) = \underbrace{\deg (x-\alpha)}_{=1} + \deg q(x)$

by the statement of the corollary

$\Rightarrow \deg q(x) = \deg p(x) - \deg(x-\alpha) = n-1.$

Let β be some other zero of $p(x)$ that is distinct from α Then

$p(\beta) = (\beta - \alpha)q(\beta) = 0.$

since β is a zero of $p(x)$

Since $\alpha \neq \beta$ and F is a field, $q(\beta) = 0$.

By our induction hypothesis, $q(x)$ can have at most $n-1$ zeros in F that are distinct from α. Thus, $p(x)$ has at most n distinct zeros in F. $\square$

Section 17.3 · Irreducible polynomials

When you learned about polynomials, you spend a lot of time factoring them and computing their zeros. We will consider similar problems but in a more abstract setting.

To discuss factorization of polynomials, we first introduce the polynomial analogue of a prime number: irreducible polynomials.

Definition A nonconstant polynomial $f(x) \in F[x]$ is **irreducible** over a field F if $f(x)$ cannot be expressed as a product of two polynomials $g(x)$ and $h(x)$ in $F[x]$ where $\deg g(x) < \deg f(x)$ and $\deg h(x) < \deg f(x)$. (given in Judson's book)

Alternative definition: Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called reducible over D.

Easiest definition If F is a field, a non-constant polynomial is irreducible over F if its coefficients belong to F and it cannot be factored into the product of two non-constant polynomials with coefficients in F.

Example The polynomial $x^2-2 \in \mathbb{Q}[x]$ is irreducible as it cannot be factored any further over the rational numbers.

Note: $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$
irrational

Example x^2+1 is irreducible over the real numbers. $\rightarrow (x-i)(x+i)$
complex

Example $f(x) = 2x^2+4$ is irreducible over $\mathbb{Q}$ & it's irreducible over $\mathbb{Z}$,

since $2(x^2+2)$

constant poly.

Example The polynomial x^2+1 is irreducible over $\mathbb{Z}_3$ but reducible over $\mathbb{Z}_5$. Why?

$$\text{e.g. } (x+3)(x+2) = x^2+5x+6 \mod 5$$
$$= x^2+1$$

Exercise to be completed during class-time.

The following 6 polynomials demonstrate some elementary properties of reducible & irreducible polynomials. Decide whether they're irreducible over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ & $\mathbb{C}$.

1. $p_1(x) = x^2+4x+4 = (x+2)^2$
2. $p_2(x) = x^2-4 = (x-2)(x+2)$
3. $p_3(x) = 9x^2-3 = 3(3x^2-1) = 3(\sqrt{3}x-1)(\sqrt{3}x+1)$
4. $p_4(x) = x^2-\frac{4}{9} = \left(x-\frac{2}{3}\right)\left(x+\frac{2}{3}\right)$
5. $p_5(x) = x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$
6. $p_6(x) = x^2+1 = (x-i)(x+i)$

Irreducible over

- $\mathbb{Z}$: 4, 5, 6 over $\mathbb{Z}$ 3 is not invertible
- $\mathbb{Q}$: 3, 5, 6 over $\mathbb{Q}$ 3 is a unit.
- $\mathbb{R}$: 6
- $\mathbb{C}$: none. They are all reducible over $\mathbb{C}$.

Example The polynomial $p(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3[x]$.

Suppose that this polynomial was reducible over $\mathbb{Z}_3[x]$ By the division algorithm there would have to be a factor $x-a$, where a is some element in $\mathbb{Z}_3[x]$.

by corollary 17.8

Hence, it would have to be true that $p(a) = 0$, for $a \in \mathbb{Z}_3[x]$. The elements of $\mathbb{Z}_3$ are $\{0, 1, 2\}$. Thus

$$p(0) = 0^3 + 0^2 + 2 = 2$$
$$p(1) = 4 \mod 3 = 1$$
$$p(2) = 14 \mod 3 = 2$$

Thus, $p(x)$ has no zeros in $\mathbb{Z}_3$ and must be irreducible.

Lemma 17.13 Let $p(x) \in \mathbb{Q}[x]$. Then $p(x) = \frac{r}{s}(a_0 + a_1 + \cdots + a_n x^n)$, where $r, s, a_0, \ldots, a_n$ are integers, the a_i's are relatively prime, and r and s are relatively prime.

Proof Suppose that $p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n$, where $b_i, c_i \in \mathbb{Z}$

since $p(x) \in \mathbb{Q}[x]$

We can rewrite $p(x)$ as

$$p(x) = \frac{1}{c_0 \cdot c_1 \cdots c_n}\left(d_0 + d_1 x + \cdots + d_n x^n\right)$$

where $d_i \in \mathbb{Z}$. Let $d = \gcd(d_0, d_1, \ldots, d_n)$. the greatest common divisor of $d_0, \ldots, d_n$

Then

$$p(x) = \frac{d}{c_0 \cdot c_1 \cdots c_n}\left(a_0 + a_1 x + \cdots + a_n x^n\right) \quad \text{where } \boxed{d_i = d a_i}$$

and the a_i's are relatively prime.

Reducing $\frac{d}{c_0 \cdot c_1 \cdots c_n}$ to its lowest terms, we can write

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n)$$

where $\gcd(r,s) = 1$.

$\square$

Reducibility test for degrees 2 and 3

Let F be a field. If $f(x) \in F[x]$ and $\deg f(x) = 2$ or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

<u>Proof</u> ($\Rightarrow$) Suppose that $f(x)$ is reducible. That is $f(x) = g(x)h(x)$, where both $g(x), h(x) \in F[x]$ and have degrees less than that of $f(x)$.

Since by prop. 17.4 $\deg f(x) = \deg(g(x)h(x)) = \deg g(x) + \deg h(x)$ and $\deg f(x)$ is either 2 or 3, we have at least one of $g(x)$ and $h(x)$ has degree 1. Say $g(x) = ax+b$.

Then $g(\alpha) = a\alpha + b = 0 \Rightarrow \alpha = -a^{-1}b$ is a zero of $g(x)$ and thus it's a zero of $f(x)$ also

($\Leftarrow$) Suppose that $f(x)$ has a zero in F. Say $\alpha \in F$.

Then $f(\alpha) = 0$. By corollary 17.8, we know that $x - \alpha$ is a factor of $f(x)$ and thus $f(x)$ is reducible over F.

$\square$

This reducibility test is particularly easy to use when the field is $\mathbb{Z}_p$. because in this case we can check for reducibility by simply testing to see if $f(a)=0$ for $a=0,1,\dots,p-1$.

Example Since 2 is a zero of x^2+1 over $\mathbb{Z}_5$, x^2+1 is reducible over $\mathbb{Z}_5$.
Instead, since neither 0, 1, nor 2 is a zero of x^2+1 over $\mathbb{Z}_3$ we have that x^2+1 is irreducible over $\mathbb{Z}_3$.

$0^2+1=1 \bmod 3$
$1^2+1=2 \bmod 3$
$2^2+1=5 \bmod 3=2$

Note that polynomials of degree larger than 3 may be reducible over a field even though they don't have zeros in the field.
Example. In $\mathbb{Q}[x]$ the polynomial x^4+2x^2+1 is equal to $(x^2+1)^2$ but has no zeros in $\mathbb{Q}$.

Theorem 17.14 GAUSS'S LEMMA

Let $p(x)\in\mathbb{Z}[x]$ be a monic (leading coeff $=1$) polynomial s.t. $p(x)$ factors into a product of two polynomials $\alpha(x)$ and $\beta(x)\in\mathbb{Q}[x]$, where $\deg\alpha(x)<\deg p(x)$ and $\deg\beta(x)<\deg p(x)$.
Then $\boxed{p(x)=a(x)\,b(x)}$, where $a(x)$ and $b(x)$ are monic polynomials in $\mathbb{Z}[x]$ with $\deg\alpha(x)=\deg a(x)$ and $\deg\beta(x)=\deg b(x)$.

Proof By lemma 17.13 (Let $p(x)\in\mathbb{Q}[x]$. Then $p(x)=\frac{r}{s}(a_0+a_1x+\dots+a_nx^n)$ where $r,s,a_0,\dots,a_n\in\mathbb{Z}$, the a_i's are relatively prime and $\gcd(r,s)=1$)
we can assume that since $\alpha(x)\in\mathbb{Q}[x]$:

$$\alpha(x)=\frac{c_1}{d_1}(a_0+a_1x+\dots+a_mx^m)$$
$$=\frac{c_1}{d_1}\alpha_1(x)$$

and similarly, since $\beta(x) \in \mathbb{Q}[x]$, we also have

$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \dots + b_n x^n)$$
$$= \frac{c_2}{d_2}\beta_1(x)$$

where the a_i's are relatively prime and the β_i's are relatively prime.

Thus $p(x) = \alpha(x)\beta(x) = \frac{c_1}{d_1}\alpha_1(x) \cdot \frac{c_2}{d_2}\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x)$, where $\frac{c}{d} = \frac{c_1 c_2}{d_1 d_2}$, expressed in lowest terms.

Therefore, if we rearrange this we obtain

$$\boxed{dp(x) = c\alpha_1(x)\beta_1(x).}$$

for the theorem to be proven we must show that $d=1$

<u>Case 1</u> $d=1$

Then $c\alpha_m b_n = 1$ since $p(x)$ is a monic polynomial.

$$\alpha_1(x) = a_0 + a_1 x + \dots a_m x^m \quad \text{and} \quad \beta_1(x) = b_0 + b_1 x + \dots + b_n x^n$$

Recall that: A polynomial is called monic if the leading coeff. is 1

Thus, since $p(x)$ is a monic polynomial we have that

$$c a_m b_n = 1 \quad \text{given that} \quad dp(x) = c\alpha_1(x)\beta_1(x)$$
$$d = 1 \Rightarrow p(x) = c\alpha_1(x)\beta_1(x)$$

Hence from $c a_m b_n = 1$ we can infer that either $c=1$ or $c=-1$

- If $c=1$, then either $a_m = b_n = 1$ or $a_m = b_n = -1$ (both a_m and b_n must have the same sign).

- In the first case $p(x) = \alpha_1(x)\beta_1(x)$ where $\alpha_1(x)$ and $\beta_1(x)$ are monic polynomials with $\deg \alpha(x) = \deg \alpha_1(x)$ and $\deg \beta(x) = \deg \beta_1(x)$.

- In the second case $a(x) = -\alpha_1(x)$ and $b(x) = -\beta_1(x)$ are the correct monic polynomials since $p(x) = (-\alpha_1(x))(-\beta_1(x)) = a(x)b(x)$.

- If $c=-1$ then the procedure is similar

Case 2 $d \neq 1$

Since $\gcd(c,d)=1$ from the theorem statement, $\exists$ a prime p s.t. $p \mid d$ and $p \nmid c$. (given what it means for c and d to be coprime)

Also, since the coefficients of $\alpha_1(x)$ are relatively prime, $\exists$ a coefficient a_i s.t. $p \nmid a_i$.

Similarly, $\exists$ a coefficient b_j of $\beta_1(x)$ s.t. $p \nmid b_j$.

Let $\tilde{\alpha}_1(x)$ and $\tilde{\beta}_1(x)$ be the polynomials in $\mathbb{Z}_p[x]$ obtained by reducing the coefficients of $\alpha_1(x)$ and $\beta_1(x)$ modulo p.

Since $p \mid d$, $\tilde{\alpha}_1(x)\tilde{\beta}_1(x)=0$ in $\mathbb{Z}_p[x]$. we have $dp(x) = c\,\alpha_1(x)\beta_1(x)$

But this is impossible since neither $\tilde{\alpha}_1(x)$ nor $\tilde{\beta}_1(x)$ is the zero polynomial and $\mathbb{Z}_p[x]$ is an integral domain.

Thus, $d=1$ & the theorem has been proven. $\square$

<u>Corollary 17.15</u> Let $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ (monic polynomial) be a polynomial w/ coefficients in $\mathbb{Z}$ and $a_0 \neq 0$. If $p(x)$ has a zero in $\mathbb{Q}$, then $p(x)$ also has a zero α in $\mathbb{Z}$. Also, α divides a_0 (i.e. the zero in $\mathbb{Z}$ divides the constant term in $p(x)$)

<u>Proof</u> Let $p(x)$ have a zero $a \in \mathbb{Q}$. (this is $a \in \mathbb{Q}$ and it's different than $\alpha \in \mathbb{Z}$)

Then $p(x)$ must have a linear factor $x-a$ by corollary 17.8.

By Gauss's lemma (theorem 17.14), $p(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$.

Hence for some $\alpha \in \mathbb{Z}$, we have

since we know the form of $p(x)$ is $x^n + a_{n-1}x^{n-1} + \dots + a_0$

$$p(x) = (x-\alpha)\left(x^{n-1} + \dots - \frac{a_0}{\alpha}\right)$$

Thus $\frac{a_0}{\alpha} \in \mathbb{Z}$ and so $\alpha \mid a_0$.

How come we have $\underset{\alpha \in \mathbb{Z}}{x-\alpha}$ instead of $\underset{a \in \mathbb{Q}}{x-a}$?

$\rightarrow$ since $\deg \alpha(x) = \deg a(x)$ & $a(x)$ is monic

Example Let $p(x) = x^4 - 2x^3 + x + 1$

We want to show that $p(x)$ is an irreducible polynomial over $\mathbb{Q}[x]$.

Assume that $p(x)$ is reducible. Then either $p(x)$ has a linear factor, say

$$p(x) = (x-\alpha)\, q(x)$$

where $q(x)$ is a polynomial of degree 3, or $p(x)$ has two quadratic factors.

If $p(x)$ has a linear factor in $\mathbb{Q}[x]$ then it has a zero in $\mathbb{Z}$.

By Corollary 17.15, any zero must divide 1 (any zero in $\mathbb{Z}$ must divide the constant term in corollary 17.15) and therefore must be ± 1. ($a_0 = 1$ in $p(x)$)

However $p(1) = 1^4 - 2(1)^3 + 1 + 1 = 1$ and $p(-1) = (-1)^4 - 2(-1)^3 + (-1) + 1 = 3$

Consequently, we eliminate the possibility that $p(x)$ has any linear factors since $p(1) \neq 0$ and $p(-1) \neq 0$ either

Therefore, if $p(x)$ is reducible it must factor into two quadratic polynomials, say

$$p(x) = (x^2 + ax + b)(x^2 + cx + d)$$
$$= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$$

where each factor is in $\mathbb{Z}[x]$ by Gauss's lemma.

Hence, since $p(x) = x^4 - 2x^3 + x + 1$, we have

$$a + c = -2$$
$$ac + b + d = 0$$
$$ad + bc = 1$$
$$bd = 1$$

by matching like terms.

Since $bd=1$ either $b=d=1$ or $b=d=-1$.

In either case $\boxed{b=d}$ and so

$$ad+bc=1 \Rightarrow ad+cd=1$$
$$d(a+c)=1$$

Since $a+c=-2 \Rightarrow d(-2)=1 \Rightarrow d=-\frac{1}{2}$

But this is impossible since $d \in \mathbb{Z}$.

Thus, $p(x)$ must be irreducible over $\mathbb{Q}$.

Definition The content of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ where the a's $\in \mathbb{Z}$ is the greatest common divisors of the integers $a_0, \dots, a_{n-1}, a_n$.

A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.

Remark In this language, Gauss's lemma states that the product of two primitive polynomials is primitive.

Remember that the question of reducibility depends on which ring of coefficients one permits. Thus x^2-2 is irreducible over $\mathbb{Z}$ but reducible over $\mathbb{Q}[\sqrt{2}]$

in this thm you have to choose the p so that it satisfies these criteria

Theorem 17.A Eisenstein's criterion

Let p be a prime and suppose $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$

If $p \mid a_i$ for $i=0,\dots,n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

leading term const. term

Proof By Gauss's lemma, we need only show that $f(x)$ does not factor into polynomials of smaller degree in $\mathbb{Z}[x]$. Let

$$f(x) = (b_r x^r + \dots + b_0)(c_s x^s + \dots + c_0)$$

be a factorization in $\mathbb{Z}[x]$ with $b_r, c_s \neq 0$ and $r, s < n$.

Since $p^2 \nmid a_0 = b_0 c_0$, either b_0 or c_0 is not divisible by p.

Suppose that $p \nmid b_0$ and $p \mid c_0$.

Since $p \nmid a_n$ and $a_n = b_r c_s$ (leading coeffs) neither b_r nor c_s is divisible by p

Let m be the smallest value of k s.t. $p \nmid c_k$. Then here $c_m \not\equiv 0 \mod p$ by choice of m

$$a_m = b_0 c_m + b_1 c_{m-1} + \dots + b_m c_0$$ (standard polyn. multipl. $a_m = \sum_{i=0}^{m} b_i c_{m-i}$)

is not divisible by p, since each term on the RHS of the eqn is divisible by p apart from $b_0 c_m$.

Thus $m = n$ since a_i is divisible by p for $m < n$.

Hence $f(x)$ cannot be factored into polynomials of smallest degree and therefore must be irreducible.

$\square$

Example The polynomial $f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion if $p = 3$. $a_5x^5 + a_4x^4 + a_2x^2 + a_1x + a_0$

Note p must be a prime, where $p \mid a_i$ for $i = 0, \dots, 4$ but $p \nmid a_5$ and $p^2 \nmid a_0$

if $p = 3$ then $3 \mid a_1, a_2, a_4$ but $3 \nmid 16$ and $9 \nmid 21$

Eisenstein's criterion is more useful in constructing irreducible polynomials of a certain degree over $\mathbb{Q}$ than in determining the irreducibility of an arbitrary polynomial in $\mathbb{Q}[x]$: given an arbitrary polynomial, it is not very likely that we can apply Eisenstein's criterion.

The real value of theorem 17.17 (EISENSTEIN'S CRITERION) is that we now have an easy method of generating irreducible polynomials of any degree

eg $f(x) = x^n + px^{n-1} + px^{n-2} + \dots + px + p$ satisfies Eisenstein's criterion for any prime p and is guaranteed to be irreducible over $\mathbb{Q}$

Now let us return for a bit back to chapter 16

Section 16.4: Maximal and prime ideals

These ideals give us special types of factor rings. We would like to characterize those ideals I of a commutative ring R s.t. R/I is an integral domain or a field.

Defn Let R be a ring. An ideal $M \subset R$ is called a **maximal ideal** if ① $M \neq R$, ② there is no ideal I of R s.t. $M \subset I \subset R$. That is, the only ideals containing M are M itself and the whole ring R.

A maximal ideal is an ideal that is as big as possible without being the whole ring

Example The ideal $\langle x^2+1 \rangle$ is maximal in $\mathbb{R}[x]$.

Assume that A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2+1 \rangle$.

We will show that $A = \mathbb{R}[x]$ by showing that A contains some nonzero real number c (This is the constant polynomial $h(x) = c \ \forall x$)

Then $1 = \left(\frac{1}{c}\right)c \in A$ (since $\mathbb{R}[x]$ is a commutative ring w/ identity)

(why? Practice for exam... Show that: if A is an ideal of a ring R and $1 \in A$ then $A = R$) $\to$ for any $r \in R$ since $1 \in A$ and A is closed under multipl. by elements of R, we have $r = r \cdot 1 \in A$. So every element of R is in A $\Rightarrow A = R$

Thus $A = \mathbb{R}[x]$ (by what is written in red)

To this end, let $f(x) \in A$ but $f(x) \notin \langle x^2+1 \rangle$

Then by the division algorithm: $f(x) = q(x)(x^2+1) + r(x)$ where $r(x) \neq 0$ (since $f(x) \notin \langle x^2+1 \rangle$)

if $f(x)$ does not belong to $\langle x^2+1 \rangle$ then x^2+1 doesn't divide $f(x)$ exactly

and $\deg r(x) < 2$.

(remember $r(x)$ satisfies

$\deg r(x) < \deg(x^2+1) = 2 \Rightarrow r(x) = ax+b \in \mathbb{R}[x]$

It follows that $r(x) = ax+b$, where a, b are not both zero, and

$$ax+b = r(x) = \underbrace{f(x)}_{} - \underbrace{q(x)(x^2+1)}_{} \in A$$

by def^n of ideal $\in A$ — element of the ring

Thus $a^2x^2 - b^2 = \underbrace{(ax+b)}_{\in A}\underbrace{(ax-b)}_{\in \mathbb{R}[x]} \in A$ and $a^2\underbrace{(x^2+1)}_{\text{elm of the ideal}} \in A$

So $0 \neq a^2+b^2 = \underbrace{(a^2x^2+a^2) - (a^2x^2-b^2)}_{\text{by closure}} \in A$ ⌟

Defn A prime ideal A of a commutative ring R is a proper ideal of R s.t. $a, b \in R$ and $\boxed{ab \in A \text{ imply } a \in A \text{ or } b \in A}$

Example The set $P = \{0, 2, 4, 6, 8, 10\}$ is an ideal in $\mathbb{Z}_{12}$.
$= \langle 2 \rangle = \{2k \bmod 12 \mid k \in \mathbb{Z}\}$

This ideal is prime.

If $a \in I$ and $r \in R$ then $ar \in I$ and $ra \in I$

$\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$

Check $\forall a, b \in \mathbb{Z}_{12}$ whether $ab \in P \Rightarrow a \in P$ or $b \in P$

eg $a=3, b=4 \Rightarrow ab = 3 \cdot 4 = 12 = 0 \in P$

$a \in P$ and $r \in \mathbb{Z}_{12}$ then $ar \in P$ and $ra \in P$? Yes!

But $3 \notin P$, $4 \in P$.

Can we find $a, b \notin P$ s.t. $ab \in P$? Elements not in P: $\mathbb{Z}_{12}/P = \{1, 3, 5, 7, 9, 11\}$

Try $a=3$, $b=5$

$3.5 = 15 \equiv 3 \notin P$

Nonexample The ideal $\langle x^2+1 \rangle$ is not prime in $\mathbb{Z}_2[x]$ since it contains

$$(x+1)^2 = x^2+2x+1 \equiv x^2+1$$

$ab \in \mathbb{Z}_2[x]$ $\quad a = (x+1) = b$

but does not contain $x+1$.

but neither $a \in \mathbb{Z}_2[x]$ nor $b \in \mathbb{Z}_2[x]$

Theorem R/A is an integral domain if and only if A is prime

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime

Proof ($\Rightarrow$) Suppose that R/A is an integral domain and $ab \in A$

Then $(a+A)(b+A) = ab + A = A$

ab gets absorbed in A

This is the zero element of the ring R/A. So either $a+A=A$ or $b+A=A$. That is, either $a \in A$ or $b \in A$. Therefore, A is prime.

($\Leftarrow$) We first observe that R/A is a commutative ring with identity for any proper ideal A. Therefore, our task is to show that when A is prime, R/A has no zero-divisors (remember for ($\Leftarrow$) we must show that if A is prime, then R/A is an integral domain, i.e. R/A has no zero-divisors)

Suppose that A is prime and $(a+A)(b+A) = 0+A = A$

Then $ab \in A$ and thus $a \in A$ or $b \in A$ (by def^n of prime ideal)

Thus, one of $\underset{=0+A}{a+A}$ or $\underset{=0+A}{b+A}$ is the zero coset in R/A, and R/A is an integral domain.

$\square$

Theorem R/A is a field if and only if A is maximal

Let R be a commutative ring with identity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

Proof ($\Rightarrow$) Suppose that R/A is a field and B is an ideal of R that properly contains A ($A \subset B$). Let $b \in B$ but $b \notin A$

Then $b+A$ is a nonzero element of R/A (since $b \notin A$, b does not get absorbed in A)

Therefore, $\exists$ an element $c+A$ s.t.

$$(b+A)(c+A) = 1+A \quad \text{(the multiplicative identity of } R/A)$$

Since $b \in B$, we have $bc \in B$. Because $1+A = (b+A)(c+A) = bc+A$
(since B is an ideal)
we have $1-bc \in A \subset B$.

So $1 = (1-bc)+bc \in B$

(Before we saw this (which was left as an exercise). If A is an ideal of a ring R and 1 belongs to A, then $A=R$)

Using the statement above ..

$B=R$. This proves that A is a maximal ideal.

($\Leftarrow$) Suppose that A is maximal and let $b \in R$ but $b \notin A$.

It suffices to show $b+A$ has a multiplicative inverse. (all other properties for a field follow trivially).

Consider $B = \{br+a \mid r \in R, a \in A\}$.

This is an ideal that properly contains A Let's show that B is an ideal in R

The set B is nonempty since $b0+0=0 \in B$
since R and A contain 0

If br_1+a_1 and br_2+a_2 are two elements in B, then

$$(br_1+a_1)-(br_2+a_2) = (r_1-r_2)b+(a_1-a_2) \in B$$

Also, for any $r \in R$ it is true that $rB \subset B$, hence B is closed under multipl. and satisfies the necessary conditions to be an ideal.

Since A is maximal, we must have $\boxed{B=R}$

Thus, $1 \in B$, say $1 = bc+a'$ where $a' \in A$
(by defn of set B above)

Then $1+A = bc+a'+A$
$= bc+A$ (a' gets absorbed in A since $a' \in A$)
$= (b+A)(c+A)$

□

THE END