# MA-138

Haria

October 2025

## 1 Lecture 1 - Sets

### 1.1 What are Sets

**Definition 1.** *A set is a collection of elements*

Commonly these are denoted by a listing of elements within braces. For example $\{1, 2, 3\}$ is the set containing 1, 2, and 3. Sometimes ellipses may be used inside the set

**Example 1.** $\{0, 1, 2, 3, \dots\}$ *denotes the set of the natural numbers* $\mathbb{N}$

When ellipses are seen a natural continuation of elements is assumed in this case the rest of the natural numbers. Note here $\mathbb{N}$ contains 0.

**Definition 2.** *If $x$ is and element of a set $X$ we nay write $x \in X$*

**Example 2.** $1 \in \mathbb{N}$

We can also demonstrate the converse

**Example 3.** $-1 \notin \mathbb{N}$

### 1.2 Set Relations

#### 1.2.1 Equality

The first thing we want to be able to tell about pairs of sets is whether two are the same.

**Definition 3.** *Sets $X$ and $Y$ are equal if for every $x \in X$ we have $x \in Y$ and for every $y \in Y$ we have $y \in X$*

From this definition falls out two interesting things

- Sets do not care about the order of their elements
- Sets do not care how many times their elements occur

This makes them fundamentally different from lists.

**Example 4.** $\{1, 2, 3\} = \{2, 2, 3, 1, 1, 3, 3\}$

### 1.2.2 Empty Set

Before the next relation it is useful to introduce a special set known as the empty set.

**Definition 4.** *There exists a set $\emptyset$ such that there does not exist an $x \in \emptyset$ called the empty set*

An interesting result is given two empty sets $\emptyset_1$ and $\emptyset_2$ these two are always equal. This is because any element in the first is necessarily in the second and vice versa as their are no elements in either. This tells us that there is only one empty set.

### 1.2.3 Numeric Sets

Another useful set to know is as follows before the next relation

**Definition 5.** *The set denoted $[n] = \{0, 1, 2, \ldots n-1\}$*

This is the set of all the natural numbers less than $n$ and is non-standard notation.

### 1.2.4 Subsets

**Definition 6.** *We can say a set $X$ is a subset of a set $Y$ if for every $x \in X$ we also know that $x \in Y$ this is denoted $X \subseteq Y$*

**Example 5.** $\{0, 1\} \subseteq \{0, 1, 2\}$

**Example 6.** $[n] \subseteq [n+1]$

From here we can derive the fact that if $X \subseteq Y$ and $Y \subseteq X$ we can say $X = Y$. Each direction of the subset satisfies half the condition for equality so having both directions of the subset we can claim equality. this is similar to how when $x \leq y$ and $y \leq x$ we know that $x = y$.

For every set $X$ we can also say two things

1. $\emptyset \subseteq X$
2. $X \subseteq X$

Which is also similar to what we can say for $\leq$

## 1.3 Set Function

## 1.4 Power Set

Every set can have many power sets so it is useful to be able to easily reference this collection of subsets

**Definition 7.** *For a set $X$ let $\mathcal{P}(X)$ denote its power set such that $x \in \mathcal{P}(X)$ if and only if $x \subseteq X$*

**Example 7.** $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

**Example 8.** $\mathcal{P}(\emptyset) = \{\emptyset\}$

It is important to remember that $\{\emptyset\}$ is a distinct set from $\emptyset$ as the first contains $\emptyset$ as an element $\emptyset \in \{\emptyset\}$ We also have a useful result that

$$|\mathbb{P}([[n]])| = 2^n$$

As for each element in $[[n]]$ for each subset of $[[n]]$ it can either be in or out of the subset.

# 2 Lecture 2 + 3 - Functions

## 2.1 Specification

**Definition 8.** ***Specification*** *: Let $X$ be a set and $S(x)$ be a property for $x \in X$. We can form a set*

$$\{x \in X | S(X)\}$$

*This gives the subset of $X$ satisfying $S(x)$ for all $x$ in the subset*

An example of this is $\{k \in \mathbb{N} | k < n\}$ being the set of natural numbers less than $n$. This is the same as the set $[[n]]$ as defined earlier.

It is important to make sure you keep track of what set you are specifying against. For example the sets $\{k \in \mathbb{N} | x^2 - 1 = 0\}$ and $\{k \in \mathbb{Z} | x^2 - 1 = 0\}$ are different sets as the latter also contains $-1$. Its also important to remember you are taking a subset of a set in this invocation. Not doing so is unrestricted comprehension and leads to Russel's paradox.

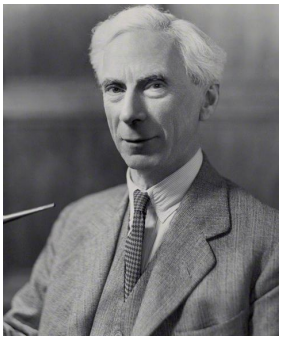

Figure 1: Russel angered by your use of unrestricted comprehension

## 2.2 Functions

### 2.2.1 Basics

Here we can start with a slightly informal definition of a function.

**Definition 9.** *Let $X$ and $Y$ be sets. A function $f$ from $X$ to $Y$ (denoted $f : X \to Y$) contains three pieces of information*

1. *A domain $X$*
2. *A codomain $Y$*
3. *A rule mapping every in $x \in X$ to one $f(x) \in Y$*

Two examples of functions are given as $f_1 : \mathbb{N} \to \mathbb{N}$ with $f_1(x) = x^2$ and another example is $f_2 : \mathbb{N} \to \mathbb{Z}$ with $f_2(x) = x^2$. These both are are different functions as they have different codomains. Two functions are only equal if all three pieces of information agree.
It is important to note that the rule portion of a function need not be given by a formula and can instead just tell you where each element goes. For example $g : \{0, 1\} \to \{2, 3\}$ can have its rule expressed as $g(0) = 2$ and $g(1) = 2$. We can also get the useful property

$$|[[n]] \to [[m]]| = m^n$$

If a function $f$ is $X \to X$ we say it is a function on $X$. A special function is the identity function on $X$ $id_X : X \to X$ given by rule $id_X(x) = x$

### 2.2.2 Types of functions

**Definition 10.** *A function $f : X \to Y$ is called injective if $f(x) = f(x') \Rightarrow x = x'$ for all $x, x' \in X$*

**Definition 11.** *A function $f : X \to Y$ is called surjective if for any $y \in Y$ there is an $x \in X$ such that $y = f(x)$*

And if a function satisfies both of these we can call it bijective.
For finite sets we can say a lot of things about injections and surjections between them. For a pair of sets $X, Y$ if $|X| = |Y|$ then any injective function is surjective. this is due to the fact to be injective each element in the domain needs a separate element in the codomain. So their are as many elements in the image as the domain which is the same as the size of the codomain so every element in the codomain is hit. And for the reverse argument each element in the codomain binds a unique element in the domain which is every element in the domain. It cant bind 2 elements to one element in the codomain otherwise the image would not be the codomain and as such would not be surjective.
We also get the fact we have no injections $f : [[n]] \to [[m]]$ if $m < n$ and no surjections $f : [[n]] \to [[m]]$ if $n < m$

### 2.2.3 Cardinality

**Definition 12.** *Given any sets $X$ and $Y$, $X$ and $Y$ have the same cardinality iff there exists a bijection $f : X \to Y$. This is denoted $|X| = |Y|$*

**Definition 13.** *For a finite set $X$ if there is a bijection $f : [[n]] \to X$ then we may say that $|X| = n$*

This makes sense for finite sets but has some interesting implications for infinite sets. Consider and $f : \mathbb{Z} \to \mathbb{N}$ defined as follows

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{if } x < 0 \end{cases}$$

This function is a bijection between the two sets mapping even naturals to positives and odds to negatives. As such we have $|\mathbb{N}| = |\mathbb{Z}|$ despite $\mathbb{N} \subseteq \mathbb{Z}$. We can construct a similar argument between $\mathbb{N}$ and $\mathbb{Q}$ by use of **The Cantor Pairing Function** which constructs the bijection between pairs of natural numbers and naturals which gets you 99% of the way to a bijection and infact shows that $|\mathbb{N}| \geq |\mathbb{Q}|$ as there are multiple pairs of naturals that can give a single rational number.
This is however not possible between $\mathbb{R}$ and $\mathbb{N}$. It can be shown there is no such bijection. this is done using Cantor's diagonalization argument to prove that there is no surjection.

*Proof.* Assume that theres is a surjection $f : \mathbb{N} \to \mathbb{R}$ This would allow us to list elements of $\mathbb{R}$ on the output. Here we will represent elements of $\mathbb{R}$ in binary expansions

$$\begin{aligned} f(1) &= 0.010110101111\ldots \\ f(2) &= 0.101100110001\ldots \\ f(\cdots) &= \cdots \end{aligned}$$

Now we con construct a new number $x$. We make x by making the $n$th digit of $x$ the opposite of the $n$th digit of $f(n)$. Now the question is : is $x$ on our list. If $x$ is in the image of $f$ then there is some $k$ such that $f(k) = x$ but this means that $x$ will differ from $f(k)$ in the $k$th digit so $x$ cannot be $f(k)$ so $x$ cannot be in the image so $f$ cannot be a surjection □

We can also very similarly consider cantor theorem

**Proposition 1.** *There is no surjection $X \to \mathcal{P}(X)$*

*Proof.* By contradiction assume there is a function $f : X \to \mathcal{P}(X)$ such that $f$ is a surjection. The means for an $A \in \mathcal{P}(X)$ we know there is an $a \in X$ so that $f(a) = A$ We can define a set $C \subseteq X$ as follows

$$C = \{x \in X | x \notin f(x)\} \in \mathcal{P}(X)$$

As $f$ is a surjection there exists a $d$ such that $f(d) = C$. We can consider two cases.

1. Consider $d \in C$. this gives that $d \in f(d)$ so by defninition $d \notin f(d)$ leading to a contraditcion
2. Consider $d \notin C$ this gives that $d \notin f(d)$ so by definition $d \in C$ leading to a contradiciotn

Both paths lead to a contradition so we can assume our premise was wrong meaning that there is no such surjection. □

This is somewhat related to how russels pradox works.

# 3 Lecture 4 + 5 + 6- More sets

## 3.1 Products

**Definition 14.** *Given $x \in X, y \in Y$ We can construct an ordered pair $(x, y)$. We may say for two pairs $(x, y) = (x', y')$ if and only if $x = x', y = y'$*

**Definition 15.** *The cartesian product $X \times Y$ is the set of all pairs $(x, y)$ such that $X \in X, y \in Y$*

$$X \times Y = \{(x, y) | x \in X, y \in Y\}$$

We can from here get a few algebraic properties of the cartesian product.

**Proposition 2.** $X \times \emptyset = \emptyset$

*Proof.* Suppose by contradiction $X \times \emptyset \neq \emptyset$. this means there is a pair $(a, b) \in X \times \emptyset$ this means there is a $b \in \emptyset$ which is false yeilding a contradiction. □

We also know that $|[[m]] \times [[n]]| = mn$ and that $X \times Y$ does not generally equal $Y \times X$.

**Definition 16.** $X^2 = X \times X$

## 3.2 Relations

**Definition 17.** *A relation $R$ from $X \to Y$ consists of three parts*

1. *A set $X$ as the domain*
2. *A set $Y$ as the codomain*
3. *A set $R \subseteq X \times Y$*

You may write $xRy$ to say that $x$ is related to $y$ is $(x, y) \in R$

**Definition 18.** *A relation $R$ from $X \to Y$ may be called graphical if the every $x \in X$ there is only one pair $(x, y) \in R$*

### 3.2.1 Functions

**Definition 19.** *A function $f : X \to Y$ is a graphical relation $F$ from $X \to Y$ such that*

$$f(x) = y \Leftrightarrow (x, y) \in F$$

**Example 9.**
1. *$\{(0,1),(1,2),(2,3)\} \subseteq [[3]] \times [[5]]$ is a graphical relation and associates to $f(x) = x + 1$*
2. *$\{(0,0),(0,1)\} \subseteq [[1]] \times [[2]]$ is not graphical as there is more than one pair for zero*

**Definition 20.** *A function $f$ with graphical relation $F$ can be called injective if for every $y \in Y$ there is at nmost one $(x, y) \in F$*

## 3.3 Unions

**Definition 21.** *Given two sets $X, Y$ we can define their union as the set*

$$\{z | z \in X \text{ or } z \in Y\}$$

*And given a set of sets $\mathbb{X}$*

$$\bigcup_{X \in \mathbb{X}} X = \{x | x \in X \text{ for some } X \in \mathbb{X}\}$$

For example let $\mathbb{X} = \{[[n]] | n \in \mathbb{N}\}$ then $\bigcup_{X \in \mathbb{X}} X = \mathbb{N}$

## 3.4 Intersections

**Definition 22.** *The intersection of two sets $X, Y$ is*

$$X \cap Y = \{z | z \in X \text{ and } z \in Y\}$$

*Let $\mathbb{X}$ be a set of sets*

$$\bigcap_{x \in \mathbb{X}} X = \{z | z \in X \text{ for all } X \in \mathbb{X}\}$$

For example let $\mathbb{X} = \{[[n]] | n \in \mathbb{N}\}$ then $\bigcap_{X \in \mathbb{X}} X = \emptyset$

## 3.5 Set difference

**Definition 23.** *The set difference of $X, Y$ is*

$$X - Y = \{x \in X | x \notin Y\}$$

For example $\mathbb{Z} - \mathbb{N} = \mathbb{Z}_{>0}$

## 3.6 Alegebra of Sets

### 3.6.1 Difference

The following identities hold for the set difference

- $X - \emptyset = X$
- $\emptyset - X = \emptyset$
- $X - X = \emptyset$

### 3.6.2 Union

The union is associative and commutative. The following identities also hold

- $X \subseteq X \cup Y$
- $X \cup \emptyset = X$

### 3.6.3 Intersection

The intersection is also associative and commutative. The following idnetities also hold

- $X \cap Y \subseteq X$
- $X \cap \emptyset = \emptyset$

### 3.6.4 Misc

Both the intersection and the union can distrobute over each other. The following identity also holds.

$$X - (Y \cup Z) = (X - Y) \cap (X - Z)$$

The identity also holds if you reverse the unions and intersections

# 4 Lecture 6 - Composition

**Definition 24.** *Suppose $f : X \to Y$ and $g : Y \to Z$ are both functions then we can compose these to get the new function $(g \circ f) : X \to Z$ where $(g \circ f)(x) = g(f(x))$*

The associated graphical realtionship is as follows

$$\{(x, g(f(x)))|x \in X\} \subseteq X \times Z$$

**Theorem.** $(f \circ g) \circ h = f \circ (g \circ h)$

**Definition 25.** *Given an $f : X \to Y$ we can say a function $g : Y \to X$ is a*

- *left inverse of $f$ if $(g \circ f) = id_X$*
- *right inverse of $f$ if $(f \circ g) = id_Y$*

**Theorem.** *Given $f : X \to Y$ we can say*

- *If $f$ has a left inverse it is injective*
- *If $f$ has a right inverse it is surjective*

# 5 Lecture 7 - Relations

## 5.1 Functions on Functions

**Definition 26.** *Given a function $f : X \to Y$ we say show the image of $A \subseteq X$ as*

$$f(A) = \{f(x) \in Y | x \in A\} \subseteq Y$$

**Definition 27.** *Given a function $f : X \to Y$ we may say the preimage of a set $B \subseteq Y$ as follows*

$$f^{-1}(B) = \{x \in X | f(x) \in B\} \subseteq X$$

## 5.2 Relations - Equivalence Properties

**Definition 28.** *Suppose we have a set $X$ and a relation $R \subseteq X^2$ we may make the following comments on the relation*

- *If for all $x \in X$ we know that $xRx$ we may call this relation reflexive*
- *If for all $x, y \in X$ we have $xRy \implies yRx$ we may call this relation symmetric*
- *If for all $x, y, z \in X$ we have $xRy \wedge yRz \implies xRz$*

**Definition 29.** *If a relation $R \subseteq X^2$ is all of reflexive symmetric and transitive we may call this an equivalence relation.*

The idea of an equivalence relation is to capture the idea of what makes two things equal. If there are properties that you dont care about for an object you can create an equality relation. Though not an equvalence relation (due to there being no set of sets) we can somewhat see this idea in the definition of equality for sets where we ingore ordering and repetion for the determination of equality.

### 5.3 Partial Orders

**Definition 30.** *Suppose $X$ is a set and a realtion $R \subseteq X^2$. We may call this relation antisymetric if for all $x, y \in X$, $xRy$ and $yRx$ implies that $x = y$*

An example of such a relation is $\geq$

**Definition 31.** *Suppose we have a set $X$ and a relation $R \subseteq X^2$ that is reflexive transitive and antisymetric. We may call this realtion a partial order and we may call the pair $(X, R)$ a poset.*

**Example 10.** *A special poset is the boolean poset on $X$ which is the pair $(\mathcal{P}(X), \subseteq)$*

### 5.4 Total Orders

**Definition 32.** *Suppose we have a set $X$ and a relation $R \subseteq X^2$ if we have that for all $x, y \in X$ that either $xRy$ or $yRx$ we may call this relation total.*

**Definition 33.** *If a relation $R$ is total and is a partial order we may call it a total order.*

## 6 Lecture 8

### 6.1 Partitions

**Definition 34.** *Suppose $X$ is a set. A set $P \subseteq \mathcal{P}(X)$ is a partition if*

- *Every element of $P$ is non-empty*
- $\bigcup_{p \in P} p = X$
- *Elements of $P$ are mutually disjoint*

We can note two sepcial partitions one that partitions the set ontp singletons and one that contiains only one partition that is the entire set itself.

### 6.2 Equivalence Classes

**Definition 35.** *Suppose we have a set $X$ with an equivalence relation $E \subseteq X^2$. Given an $x \in X$ we may show its equivalence class as follows*

$$[x]_E = \{y \in X | xEy\}$$

Similar to the two partitions given eralier we have the identity relation whos equivalence classes are singletons and the universal relation whose sole equivalence class is the whole set $X$.

We may denote the set of all equvalence classes as follows

$$X/E = \{[x]_E | x \in X\}$$

We can also define a function $q_E : X \to X/E$ defined as $q_E(x) = [x]_E$

**Proposition 3.** *Given a set $X$ and an eqivalence relation $E$ we may say $X/E$ is a partition of $X$*

*Proof.* To prove this we must go through each of the properties of partitions

- As we know that $x \in [x]_E$ we can see no class is enmpty
- By the point above we know that all $x$ is in at least one class so the union is the original set
- We will attempt to prove by contradiction that all classes are dissjoint. Suppose by contradiciotn for some some $x, y$ that there is a $z \in [x]_E \cap [y]_E$ where $[x]_E \neq [y]_E$. We can deduce that $xRz$ and $yRz$. By the properties of an equivalence relation we can deduce $xRy$. This means for all $y' \in [y]_E$ we can say $y' \in [x]_E$ and also show the same for $x$ so they are the same set leading to a contradiction.

□

### 6.3 Well definedness

Functions out of equicvalence classes have to be careful tnhat they operate thae same no matter what representation of a class it operates on. So if we have some $x \neq y, [x]_E = [y]_E$ we do want to have $f([x]_E) = f([y]_E)$. As susch we can introduce a property called well definedness.

**Definition 36.** *Consider two sets $X, Y$ an equivalence relation on $X$,$E$ and a funciton $f : X \to Y$. We may call $f$ well defined if for all $x, x' \in X$ if $xEx'$ then $f(x) = f(x')$*

This definition can be used to the induce a function $f_E : X/E \to Y$.

## 7 Lecture 9

Omiited because tedius to write

## 8 Lecture 10 - Modular Arithmetic

**Definition 37.** *LEt $E_n$ be the equivalence relation on $\mathbb{Z}$ fegiven by*

$$xE_ny \iff y = x + kn$$

$$[a]_n = \{x \in \mathbb{Z} | aE_nx\}$$

*Is the congruence class of a module $n$*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{[a]_n | a \in \mathbb{Z}\}$$

Given a congruence class $[b]_n$ we say $b$ is a representative instance for $[b]_n$

**Theorem.** *There is a bijection $q_n : [[n]] \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ that takes a natural number to an equivalence class. To do the inverse case we must choose a representative for the class.*

$$q_n(k) = [k]_n$$

**Definition 38.** *Recall $[b]_n = [b + kn]_n, k \in \mathbb{Z}$.*
*If $[x]_n = [y]_n$ we write*

$$x \equiv y \mod n$$

*and say $x$ is congruent to $y$ modulo $n$*

**Definition 39.** *We define the following operations*

- *Addition :* $[a]_n + [b]_n := [a + b]_n$
- *Multiplication :* $[a]_n \times [b]_n := [a \times n]_n$
- *Negation :* $-[a]_n := [-a]_n$

*We also define two special elements*

- $[0]_n$ *is the zero element so* $[0]_n + a = a$ *and* $[0]_n \times b = [0]_n$
- $[1]_n$ *is the unit(identity??) element so* $[1]_n \times b = b$

With these definitions we want to have that if $a \equiv c \mod n$ and $b \equiv d \mod n$ then $[a + b]_n = [c + d]_n$. This is the same as saying we want addition to be a function $+ : \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$. So we are essentially looking for a well definedness.

*Proof.* The fact $[a]_n = [c]_n$ means that $c = a + kn$. Like wise for $b, d$ we can say $d = b + jn$.

$$\begin{aligned}
[c + d]_n &= [a + kn + b + jn] \\
&= [a + b + (k + j)n] \\
&= [a + b]_n
\end{aligned}$$

□

We may carry out similar proofs for multiplication and negation

*Proof.* The fact $[a]_n = [c]_n$ means that $c = a + kn$. Like wise for $b, d$ we can say $d = b + jn$.

$$\begin{aligned}
[c \times d]_n &= [(a + kn)(b + jn)]_n \\
&= [a \times b + akn + bkn + jkn^2]_n \\
&= [a \times n + (ak + bk + jkn)n]_n \\
&= [a \times b]_n
\end{aligned}$$

□

*Proof.* The fact $[a]_n = [c]_n$ means that $c = a + kn$.

$$-[a]_n = [-1]_n \times [a]_n$$

By the fact multiplication is well defined negation is well defined $\square$

By the fact that all of these definitions are in terms of simple aritmetic theorems regarding these arithmetic operations still hold under modular arithmatic so we get to keep commutivity associativy distributivity which is very fun :3.

**Example 11.** *Say you where told to find the last didgit of* $3^{1000}$*. This is athe same as finding an* $x \in [[10]]$ *such that* $x \equiv 3^{1000} \mod 10$

$$3^{1000} = 9^{500} \equiv (-1)^{500} = 1 \mod 10$$

# 9 Lecture 11 - Boolean Operators

**Definition 40.** *A Boolean is an element of the set* $\{T, F\}$

Consider the statement "2 is a prime number". This statement has an boolean value in this case that value is $T$. Another statement is "2 is an odd number" this aslo has a boolean value which in this case is $T$. Both of these statements are propositions.

**Definition 41.** *A proposition is a statement that evaluates to a boolean*

**Definition 42.** *A boolean operator* $\sigma$ *of arity* $n$ *(an* $n$*-ary function) is a function* $\sigma : \{T, F\}^n \to \{T, F\}$

**Definition 43.** *Negation :* $\neg : \{T, F\} \to \{T, F\}$*. This has arity 1*

| $p$ | $\neg p$ |
|---|---|
| $T$ | $F$ |
| $F$ | $T$ |

**Definition 44.** *Or :* $\vee : \{T, F\}^2 \to \{T, F\}$ *is a 2-ary operator defined as follows*

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $F$ |

**Definition 45.** *And :* $\wedge : \{T, F\}^2 \to \{T, F\}$ *is a 2-ary operator defined as follows*

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $F$ |

**Definition 46.** *Implies :* $\Rightarrow$*:* $\{T,F\}^2 \to \{T,F\}$ *is a 2-ary operator defined as follows*

| $p$ | $q$ | $p \Rightarrow q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $T$ |
| $F$ | $F$ | $T$ |

**Definition 47.** *Is equivalent to (iff) :* $\Leftrightarrow$ $\{T,F\}^2 \to \{T,F\}$ *is a 2-ary operator defined as follows*

| $p$ | $q$ | $p \Leftrightarrow q$ |
|---|---|---|
| $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ |
| $F$ | $T$ | $F$ |
| $F$ | $F$ | $T$ |

**Definition 48.** *We say two n-ary boolean operators are equal if they are equal as funtions.*

**Example 12.** *The expression* $\neg((\neg P) \vee (\neg Q)) = P \wedge Q$

**Theorem.** *Any boolean operator is a composition of those operators given above (not even all five is needed as some can be expressed as other. all operators can be made with (nand)/(or with negation))*

# 10 Lecture 12

The operations given last time (and, or) satosfy identities similarly to intersections and unions.

For the or we have

- $P \vee T = T$
- $P \wedge F = P$

It is also commutative and associative. We also know that $P \vee P = P$

For and we know

- $P \wedge T = P$
- $P \wedge F = F$

They are also commutative and associative and $P \wedge P = P$

These also distrobute over each other

- $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee Q)$
- $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge Q)$

They also realte bye demorgans law **PUT DM LAW**

**Definition 49.** *A boolean operator $f : \{T, F\}^n \to \{T, F\}$ is a tautology if $f(x) = T$ for all $x \in \{T, F\}^n$*

**Definition 50.** *A boolean operator $f : \{T, F\}^n \to \{T, F\}$ if $f(x) = F$ is an antimony for all $x \in \{T, F\}^n$*

**Example 13.** *The statement $P \vee \neg P$ is a tautology*

**Definition 51.** *The lookup table for a boolean operations $f : \{T, F\}^n \to \{T, F\}$ is a two columned table. The first column is $x \in \{T, F\}^n$ and the second is $f(x)$*

For large and complex tables this can be hard to do (well not hard but very fucking long)

**Example 14.**

$$(P \wedge (Q \vee R)) \Rightarrow R$$

| $P$ | $Q$ | $R$ | $f$ |
|---|---|---|---|
| $F$ | $F$ | $F$ | $T$ |
| $F$ | $F$ | $T$ | $T$ |
| $F$ | $T$ | $F$ | $T$ |
| $F$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $T$ |
| $T$ | $F$ | $T$ | $T$ |
| $T$ | $T$ | $F$ | $F$ |
| $T$ | $T$ | $T$ | $T$ |

**Theorem.** *If $f, g$ are of the same aritty then $f = g$ if and only if $f \Leftrightarrow g$*

The following are useful tautologies

- DNE : $\neg\neg P \Leftrightarrow P$
- Contraposition : $(Q \Rightarrow P) \Leftrightarrow (\neg P \Rightarrow \neg Q)$
- Bidirectionality : $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \vee (Q \Rightarrow P))$
- LEM : $(P \vee \neg P)$
- Modus Ponens : $(P \wedge (P \Rightarrow R)) \Rightarrow R$
- Chaining : $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$
- Contradiction : $((\neg P) \Rightarrow F) \Rightarrow P$

# 11 Lecture 14

**Theorem.** *Suppose $X \neq \emptyset$*

$$\forall x \forall y P(x, y) \Leftrightarrow \forall y \forall x P(x, y)$$

*We can also firther show the one way chain of implications*

$$\begin{aligned}\forall x\forall y P(x,y) &\Rightarrow \exists x\forall y P(x,y)\\ &\Rightarrow \forall y\exists x P(x,y)\\ &\Rightarrow \exists x\exists y P(x,y)\end{aligned}$$

*And further*

$$\exists x\exists y P(x,y) \Leftrightarrow \exists y\exists x P(x,y)$$

**Theorem.** *Suppose* $X = \emptyset$

$$\forall x P(x) \Leftrightarrow T$$
$$\exists x P(x) \Leftrightarrow F$$

**Definition 52.** *Let $A$ be a set of axioms. Let $D$ be a set of deduction rules. A proof of $S$ from $A$ is a sequence of statements $(S_k)_{k=0}^n$ such that $S_k$ is either an axiom or $S_k$ can be deduced from $(S_i)_{i<k}$ using elements of $D$.*

**Example 15.**

$$A = \{(\exists X, |X| = 0), (\exists X, |X| = n \Rightarrow \exists Y, |Y| = 2^n)\}$$
$$D = \{(P \wedge (P \Rightarrow Q)) \Rightarrow Q\}$$

**Theorem.**

$$\exists x, |x| = 2$$

*Proof.*

$$\begin{aligned}&S_0 : (\exists X, |X| = 0)\\ &S_1 : (\exists X, |X| = 0 \Rightarrow \exists Y, |Y| = 1)\\ &S_2 : \exists Y, |Y| = 1 \text{ by } D\\ &S_3 : (\exists Y, |Y| = 1 \Rightarrow \exists Z, |Z| = 2)\\ &S_4 : \exists Z, |Z| = 2 \text{ by } D\end{aligned}$$

□

PRoving tings like this is unweildy so we generally use the following definition

**Definition 53.** *Proof (Informal) : A convincing argument of a statement.*

**Theorem.** *There are arbitrariliy large rpimes*

$$\forall n \in \mathbb{N}\exists p \in \mathbb{N}, (p > n) \wedge (prime(p))$$

The normal proof for this is done and it is done by contradiction. Proofs done be contradiction is done by $(\neg P \Rightarrow F) \Rightarrow P$ Which under the assumption of LEM is a tautology. One part of the proof entails the fact a;; primes $p \leq n$ where from there you construct a set of such primes. This relies on the axiom of specification and when doing formal proof you would need to quote this and do it poperly but for general convinicing arguments you wont need to state it.

**Theorem.** *Show there exists infinitley many primes $p$ such that $p \equiv 3 \mod 4$*

# 12 Lecture 16 - Contradiction + induction

## 12.1 Contradiction

A prrof by contradiction of a statement $P$ invloves the assumption of $\neg P$ and making an attempt to show that it is contradictory and so by LEM $P$ must be true. Formally a contradiction is a statement of the form $(C \wedge \neg C)$

**Theorem.** *If* $0 < x < 1$ *then* $\frac{1}{x(1-x)} \geq 4$

*Proof.* Suppose for contradiction that we have $0 < x < 1$ and $\frac{1}{x(1-x)} < 4$

We may also note $0 < 1 - x < 1$. So we may then say $x(1-x) > 0$ So from the assumption we deduce that

$$\begin{aligned} 1 &< 4x(1-x) \\ 1 &< 4x - 4x^2 \\ 4x^2 - 4x + 1 &< 0 \\ (2x+1)^2 &< 0 \end{aligned}$$

But we know that for all $y \in \mathbb{R}$ that $y^2 \geq 0$ so we know that $(2x+1)^2 \geq 0$ yeilding a contradiction. □

## 12.2 Induction

**Theorem.** *Let* $P(n)$ *be a sequence of statements for all* $n \in \mathbb{N}$. *Suppose it is known that* $P(0)$ *holds and that* $P(k) \Rightarrow P(k+1)$ *holds then we may say* $\forall n \in \mathbb{N}, P(n)$

If instead we want to start the proof from another base case i.e. $P(n)$ for all $n \in \mathbb{N}, n \geq l$. Induction can still be used. Formally this would be proving a proposition $C(n) := P(n+l)$

## 12.3 Strong Induction

**Definition 54.** *If there is a sequence of statements* $P(n)$ *for all* $n \in \mathbb{N}$. *If* $P(l)$ *holds and if* $P(k)$ *holds for all* $l < k < m$ *implies that* $P(m)$ *holds we may say that it holds for all* $n \in \mathbb{N}, n \geq l$

**Theorem.** *All* $n \geq 2$ *can be written as a product of primes.*

*Proof.* This proof will be done by strong induction

- Base Case $n = 2$ : 2 is the product 2 so the base case holds
- Indcutive Step Assume it holds for all $k, 2 < k < m$ : We aim to show the statement holds for $m$. We may consider here two cases
  - Consider $m$ is prime. This product then is just $m$ so $P(m)$ holds‘

– Consider $m$ is not prime. As $m$ is not one it is therefroe composite. This means we can write $m = rs$ where $1 < r, s < m$. As such by the inductive hypothesis $r, s$ both have prime facotrisations. So we may note

$$r = p_1 \times \cdots \times p_a$$

$$s = q_1 \times \cdots \times q_b$$

Where all $p_i, q_j$ are primes. As such we may write

$$m = p_1 \times \cdots \times p_a \times q_1 \times \cdots \times q_b$$

□

# 13 Lecture 18

## 13.1 Well ordering

Well ordering is a property that we can generally apply to many sets. This is an extension to other types of ordering where we necessitate that there is also a least element. In general we cant decide if there is a relation that well orders a set so we generally assume this is true (AOC). For the natural numbers we propose it as follows

**Theorem.** *Every non empty subset $S$ of $\mathbb{N}$ There is a $t \in S$ such that for all $s' \in S, t \leq s'$*

This proof my be done by indction

*Proof.* The thoerem may be more simply states as For every subset $S$ of $\mathbb{N}$. If $S$ is non empty then there is a least element. We will aim to prove the contrapositve; If $S$ has no least element then it is empty. As such we would know that $S \cap [[n]] = \emptyset$ for all n. As such we may do this by inducting on $n$.

- Base case n = 0: AS for all sets $X \cap \emptyset = \emptyset$ The base case trivially holds
- Inductive case, Assume for some $k \geq 0, S \cap [[k]] = \emptyset$. We will then assume by contradiction that $S \cap [[k+1]] \neq \emptyset$. From here we can conclude that $n+1 \in S$ which would make it the least element contradicting the statement so it is empty.

□

## 13.2 Recursion

Sometimes functions are definied in terms of themselfves. One way this is done is linear recursion. Linear recursion is given below.

**Definition 55.** *Given a function $F : \mathbb{N} \times X \to X$ and theat there is a $x_0 \in X$ We can uniquely define a function $f : \mathbb{N} \to X$ satisfying the following*

- $f(0) = x_0$
- $f(k+1) = F(k, f(k))$

This definition can be firther generalised by allwing the recursive case access to more than the previous term.

We can also use reccurence to define a repeated composition of some function.

**Definition 56.** *Let $f : X \to X$ we may defined its repeated application as follows*

- $f^{(0)} = id_X$
- $f^{(n+1)} = f \circ f^{(n)}$

**Definition 57.** *We may say $x \in X$ is a fixed point of $f : X \to X$ if $f(x) = x$*

**Definition 58.** *We may define and denote the orbit of $x \in X$ under $f : X \to X$ as follows*

$$\mathcal{O}_f(x) = \{f^{(n)}(x) | x \in \mathbb{N}\}$$

If $x$ is a fixed point of $f$ then we may say that $\mathcal{O}_f(x) = \{x\}$. If $f$ is a permutation then the orbits partition the set

## 13.3 Pigeon hole principle

The pigeon hole priciple rougly states that if you have some finite collection of elements and some amounts of categories you can put them in if

- You have more items than categories
- You have each element is in a category

We may say that some category has at least 2 elements.

We will now make some attempt to build up to a proof of this.

We will first prove the following

**Theorem.** *If $f : [[n]] \to [[n+1]]$ is a function it is not a surjeciton.*

*Proof.* We will do this by induction on $n$.

- Base case: Suppose by contradiction that is is surjective. This means that thhere is a $a \in \emptyset$ such that $f(a) = 0$ which is a contradiciton

- Inductive case: Assume by contradiciton $f : [[n+1]] \to [[n+2]]$ is a surjection it is not a funciton. Construct a function $g : [[n]] \to [[n+1]]$ as follows
$$g(k) = \begin{cases} f(k) & f(k) < n+1 \\ f(n) & f(k) = n+1, f(n) < n+1 \\ 0 & f(k) = f(n) = n+1 \end{cases}$$
Now we aim to show that this is surjective. Consider some $l \in [[n+1]]$ We can also say $l \in [[n+2]]$ This means there is a $k \in [[n+1]], f(k) = l$. This means either $k = n$ or $k < n$
  - Suppose $k < n$. We may say then that $g(k) = l$
  - Suppose instead that $k = n$. As such $k$ is not in the domain of $g$. By the surjectivity of $f$ there is some $k', f(k') = n+1$. In the current case we have $f(n) = f(k) = l$ and we also know that $l < n+1 = f(k')$ as such $k' \neq n$ so $g(k') = l$.

  So we have $g$ is s surjection which contradicts the hypothesis.

□

# 14 Lecture 20

**Definition 59.**
$$D(n) = \{k \in \mathbb{N} | k \textit{ divides } n\}$$

**Definition 60.**
$$\gcd(m,n) = \begin{cases} 0 & m = n = 0 \\ max(D(m) \cap D(n)) \end{cases}$$

Some generally useful facts are
$$\begin{cases} \gcd(n,0) = 0 \\ \gcd(n,1) = n \\ \gcd(m,n) = \gcd(n,m) \end{cases}$$

This definition of gcd is really clunky to use and very long slow and error prone

**Theorem.** *Given $m, n \in \mathbb{N}, m, n \neq 0$. Let*

- $m = p_1^{a_1} \cdot p_2^{a_2} \cdots$
- $n = p_1^{b_1} \cdot p_2^{b_2} \cdots$

*Be the prime facotrisations. We may then say*
$$\gcd(m,n) = p_1^{c_1} \cdot p_2^{c_2} \cdots$$
*Were* $c_i = \min(a_i, b_i)$

This is also clunky. We may not the following

**Lemma 1.** *if $m \geq n$ then* $\gcd(m, n) = \gcd(m - n, n)$

**Theorem.** *Suppose $m, n \in \mathbb{N}, n \geq 0$ There is a unique $q, r \in \mathbb{N}$ such that $m = qn + r$ and $r < n$*

From here we can say if $m = qn + r$ then $\gcd(m, n) = \gcd(r, n)$ by succesive subtracti9on of $r$.

From here we can induce the fast euclid algorithm for gcd.

- Set $n = 0, A_0 = m, B_0 = n$
- while $B_n$ is non-zero find $q_n, r_n$ as given above
- Set $A_{n+1} = B_n, B_{n+1} = r_n$
- If $B_n$ was zero then $A_n$

# 15 Lecture 21

**Proposition 4.** *Given $a, b \in \mathbb{N}$ and $c, d \in \mathbb{Z}$*
*$ac + bd$ is divisible by* $\gcd(a, b)$

**Lemma 2.** *Berzouts Lemma: Given $a, b \in \mathbb{N}$ there exist $c, d \in \mathbb{Z}$ such that* $ac + bd = \gcd(a, b)$

In order to find thise two integer we utilise the fast euclidean algortihm. We write out $r_n = A_n - q_n B_n$ for each iteration of the algorith. Working from the last equality subsitiute in the one from the previous iteration repeatedly. This will eventually give you an equation in terms of the orginal two parameters to the gcd.

## 15.1 Group

**Definition 61.** *A group is a set $G$ equipped with a function $\cdot : G \times G \to G$ satisfying*

- *There exists an element $e_G \in G$ called the identity such that for all $g \in G$*

$$e_G \cdot g = g = g \cdot e_G$$

- *For all $g \in G$ there is a $h \in G$ such that*

$$g \cdot h = e_G = h \cdot g$$

  *This is unique and is called the inverse usually denoted $g^{-1}$*

- *For all $a, b, c \in G$ we have*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

A group is atype of algebra. Algebras are sets equiped with functions on this group. They are often used as a way to abstract away particualrs of many objects in order to make proofs that can hold in a more general case. For this definition of groups the property of closure is given by the domain and codomains of the group operation.

**Example 16.** *An example of a group is* $(\mathbb{Z}, +)$*. We can show this by checking the poperties*

- *The identity element for this* 0
- *The inverse of* $n \in \mathbb{N}$ *is* $-n \in \mathbb{N}$
- *It is known that integer addition is associative*

# 16 Lecture 22 - Dihedral Groups

**Definition 62.** *Suppose* $\theta \in \mathbb{R}$ *We may define 2 functions* $R_\theta, M_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ *defines as following*

$$R_\theta(x, y) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$$

$$M_\theta(x, y) = (x\cos\theta + y\sin\theta, x\sin\theta - y\cos\theta)$$

Both of these function respectivley encode rotations and reflections of obejects on the plane. As such we can note $R_0 = Id_{\mathbb{R}^2 = R_{2\pi}}$ In general we may say

$$R_\phi \circ R_\theta = R_{\phi+\theta}$$

Whic is clear from the fact that it is a rotation and can be shown properly by making use of trig identities. Similarly for $M$ we can say

$$M_\theta \circ M_\theta = Id_{\mathbb{R}^2}$$

As this is a double relfection in the same line it simly returns to the original position. This can also be properly proven by making use of the trig identites.

**Lemma 3.** *Here are some general identities*

$$R_0 = R_{2\pi} = Id_{\mathbb{R}^2} \tag{1}$$
$$R_\lambda \circ R_\theta = R_{\lambda+\theta} \tag{2}$$
$$M_\lambda \circ M_\theta = R_{\lambda-\theta} \tag{3}$$
$$R_\lambda \circ M_\theta = M_{\lambda+\theta} \tag{4}$$
$$M_\lambda \circ M_\theta = M_{\lambda-\theta} \tag{5}$$
$$M_\theta \circ M_\theta = R_0 \tag{6}$$

We can notice that if we collect all functions $R, M$ into a set $D$ we can notice $(D, \circ)$ is a Group.

**Definition 63.** *Let* $\Theta(n) = \{\frac{2\pi k}{n} | k \in \mathbb{Z}\}$

**Definition 64.** *Let* $D_{2n} = \{R_\theta, M_\theta | \theta \in \Theta(n)\}$

**Definition 65.** *We can define the Dihedral Group of order n to be* $(D_{2n}, \circ)$

We can note that the dihedral group of order $2n$ ecnodes the symmetries of a regular $n$-gon. For example the dihedral group $D_8$ encodes the reflectional and rotational symmetry of a square.

**Definition 66.** *Let* $(G, \circ)$ *be a group. Consider a* $g \in G$ *we can definie to fucntions* $L_g, R_g : G \to G$ *as follows*

$$R_g(h) = h \circ g$$
$$L_g(h) = g \circ h$$

These are the right and left multiplications of $g$

**Lemma 4.** *Both of these are Bijections*

# 17 Lecture 23

## 17.1 Group Tables

**Definition 67.** *Given a group G the group table has rows and columns indexed by elements oh G and position* $(g, h) = gh$

**Example 17.** *The group table for* $(\mathbb{Z}/4\mathbb{Z}, +)$

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

## 17.2 Sub Groups

**Definition 68.** *Suppose* $(G, \circ)$ *is a group then for* $H \subseteq G$ *is a subgroup if*

- $e_G \in H$
- *If* $g \in H$ *then* $g^{-1} \in H$
- *If* $g, h \in H$ *then* $gh \in H$

The definition is enssentially asking if $(H, \circ)$ aslo forms a group. IF $H$ is a subgroup of $G$ we may say $H \leq G$ By manking use of the second and third requirement of forming a subgroup we can use certain elements of the orginial group $G$ as "generators" for the subgroups. Consider for the group $\mathbb{Z}/6\mathbb{Z}$ Using the element 2 we can generate the subgroup $\{, 0, 2, 4\}$ and if you use the element 1 we generate the entire group.

**Definition 69.** *We say G is commutatuve or abelian if* $gh = hg$ *for all* $g, h \in G$

# 18 Symmetric groups

**Definition 70.** *The symmetric group $Sym(X)$ is the set of all bijections $\sigma : X \to X$ with composition as the gorup action.*

Permutations may be written with a one or two line notation. In two line notation two lines of elements are written. One of the lines is the group elements before permutation the second after. In some cases the initial order will be obvious (such as for numeric sets) so only the second line is given giving a one line notation.

## 18.1 Cycles

**Definition 71.** *Given a permutation $\sigma \in Sym(n)$ We can call the orbit decomposition*

$$\mathcal{O}_\sigma = \{\mathcal{O}_\sigma(k) \ k \in [[n]]\}$$

This is a partition of the symmetric $[[n]]$ which is simple to prove.

**Definition 72.** *We call $\sigma$ a $k$-cycle if there is exactly one $R \in \mathcal{O}_\sigma$ with cardinality $k$ and everything else has cardinality 1.*
*We call $R$ the support of $\sigma$*

The only one cycle in $Sym(X)$ is $Id_X$. Two cycles are sometimes called transpositions.

Given the smallest element of a support $a \in R$ we may write

$$\begin{pmatrix} a & \sigma(a) & \sigma^2(a) & \dots & \sigma^{k-1}(a) \end{pmatrix}$$

as the cycle notation for $\sigma$ The composition of disjoint cycles with dosjpint supports is commutative as they affect different elements.

## 18.2 Inversion and parity

**Definition 73.** *We can let $\mathcal{D}_n$ denote all the unordered pairs of cardinality 2 $\{a, b\}$ where $a, b \in [[n]], a \neq b$*

This allwos us given a $\sigma \in Sym(n)$ to induce a function $\sigma : \mathcal{D}_n \to \mathcal{D}_n$ where

$$\sigma(\{a, b\}) = \{\sigma(a), \sigma(b)\}$$

As we know that the image of distinct elements are distinct as $\sigma$ is bijective so we mainiain cardinality 2.

**Definition 74.** *Consider a permutation $\sigma \in Sym(n)$ and a pair $A \in \mathcal{D}_n$ if we have that $\sigma$ flips the order of the elements of $A$ $(a < b \Rightarrow \sigma(a) > \sigma(b))$ we may call $A$ an inversion of $\sigma$*

We can let $INV_\sigma : \mathcal{D}_n \to \{0, 1\}$ be an indicator function of inversions.

**Proposition 5.** *Suppose $\rho, \sigma \in Sym(n)$ and let $A \in \mathcal{D}_n$*

$$INV_{\rho\circ\sigma}(A) \equiv INV_\rho(A) + INV_\sigma \mod 2$$

This is trivial to prove.

$$INV(\sigma) = \sum_{A\in D_n} INV_\sigma(A)$$

With this we make the following definition

**Definition 75.**

$$pari : Sym(n) \to \mathbb{Z}/2\mathbb{Z}$$
$$pari(\sigma) = [INV(\sigma)]_2$$

*This function denotes the parity of $\sigma$ or the parity of the count of inversions.*

We can note that pari forms a Homomorphisms

**Proposition 6.**

$$pari(\rho \circ \sigma) = pari(\rho) + pari(\sigma)$$

*Proof.*

$$\begin{aligned}
\text{pari}(\rho \circ \sigma) &\equiv INV(\rho \circ \sigma) \\
&\equiv \sum_{A\in D_n} INV_{\rho\circ\sigma}(A) \\
&\equiv \sum_{A\in D_n} INV_\rho(A) + \sum_{A\in D_n} INV_\sigma(A) \\
&\equiv INV(\rho) + INV(\sigma) \\
&\equiv \text{pari}(\rho) + \text{pari}(\sigma)
\end{aligned}$$

□

We may not that this suggest firther that the set of even permutaitons forms a closed subgoup (Alternating group)

# 19 Lecture 26 - Group Homomorphisms

**Definition 76.** *Suppose you have two groups $(G, \circ_G), (H, \circ_H)$ we say a function $\varphi : G \to H$ if it satisfies*

$$\varphi(x \circ_G y) = \varphi(x) \circ_H \varphi(y)$$

*for all $x, y \in G$*

Some useful identities are that $\varphi(e_G) = e_H$ and from here it follows that $\varphi(g^{-1}) = \varphi(g)^{-1}$ and this generalizes to all powers

**Example 18.** *Define a function* $\varphi : \mathbb{Z} \to (0, \infty)$ *as* $\varphi(k) = e^k$

$$\begin{aligned}\varphi(x+y) &= e^{x+y} \\ &= e^x \times e^y \\ &= \varphi(x) \times \varphi(y)\end{aligned}$$

**Proposition 7.** *Given a pair of homomorphisms* $\varphi : G \to H, \psi : H \to K$ *we may construct a homomorphism* $(\psi \circ \varphi) : G \to K$

**Definition 77.** *We can say that* $\varphi$ *is an isomoprhism if it is a homomorphism and it is bijective.*

I will here prove that the inverse is a homomorphism. We should not each $h \in H$ associates a $g \in G$

*Proof.*

$$\begin{aligned}\varphi^{-1}(\varphi(x) \circ \varphi(y)) &= \varphi^{-1}(\varphi(x \circ y)) \\ &= x \circ y \\ &= \varphi^{-1}(\varphi(x)) \circ \varphi^{-1}(\varphi(y))\end{aligned}$$

□

We can use isomorphisms to form to create an eqivalence relation where we call two elements of the equivalence class isomporphic.

# 20 Lecture 28 - Parity, Images and kernels

## 20.1 Parity

It would be nice to have an easier way to compute the parity then counting crosses (especially for cycle notations)

**Proposition 8.** *All transpositions* $\sigma$ *satisfy* $pari(\sigma) \equiv 0$

*Proof.* We know $\sigma = (a \quad b)$. Wlog let $a < b$ so we can see then that $\sigma(a) = b > a = \sigma(a)$. So $\{a, b\}$ is a inversion. For an element $c, a < c < b$ we have that $c$ is a inversion with both $a, b$. as such we have that

$$Inv(\sigma) = 1 + 2(a + b - 1) \equiv 1 \mod 2$$

□

**Proposition 9.** *Every permutation can be written as a compositions of non disjoint transpositions*

*Proof.* Let an $n > 1$ cycle be written as $(a_1 \quad \dots \quad a_n)$. Then we may show it as trasnpositions as follows

$$(a_1 \quad a_2) \dots (a_{n-1} \quad a_n)$$

□

This means that by decomposing a permutation into transpositions we can compute its parity. From here we deduce

**Proposition 10.** *If $\sigma$ is a $l$ cycle then we have*

$$pari(\sigma) = \begin{cases} [0]_2 & l \text{ is odd} \\ [1]_2 & l \text{ is even} \end{cases}$$

## 20.2 Images and kernels

**Definition 78.** *Let $\varphi : G \to H$ be a homomorphism we may define the following*

- $Image(\varpi) = \{\varpi(g) | g \in G\}$
- *The kenenel of $\varpi$ is* $Kern(\varpi) = \{g \in G | \varpi(g) = e_H\}$

**Theorem.** *The image of $\varpi$ is a subgroup of $H$*

*Proof.* We must check all of the properties of subgroups

- Identiy : $e_H = \varpi(e_G)$
- Closure Inverse : $h^{-1} = \varpi(g)^{-1} = \varpi(g^{-1})$
- Closure Product : $h_1 \circ h_2 = \varpi(g_1) \circ \varpi(g_2) = \varpi(g_1 \circ g_2)$

□

**Theorem.** *The kenrel of $\varphi$ is a subgroup of $G$*

*Proof.*
- Identity is clear
- Closure under inverses : Let $g \in G$ be in the kernel

  $$e_H = \varphi(g) \circ \varphi(g)^{-1} = e_H \circ \varphi(g^{-1})$$

  Therefore we may conclue $\varphi(g^{-1}) = e_H$ so the inverse of $g$ is in the kernel
- Closure under operation : Let $g, h \in G$ be in the kernel.

  $$e_H = \varphi(g) \circ \varphi(h) = \varphi(g \circ h)$$

  So the $g \circ h$ is in the kernel

□

# 21 Lecture 29 - Cosets

**Definition 79.** *Let $G$ be a group and let $H \leq G$. We can define a realtion $R$ on $G$.*

$$gRh \iff g^{-1}h \in H$$

**Lemma 5.** *The above is an equivalence*

*Proof.*
- Reflexivity : $gg^{-1} = e_G \in H$ so $gRg$
- Syymetric : if $gRh$ we have $g^{-1}h \in H$. By closure under inverses we have $h^{-1}g \in H$ so $hRg$
- if $gRh$ and $hRk$ then $g^{-1}h, h^{-1}k \in H$. By closure under product we have $g^{-1}k \in H$ so $gRk$

□

**Definition 80.** *A coset of $H$ is an equivalence class of $R$ as defined above. The coset $[g]_R$ is denoted $gH$*

Since $[g]_R = \{x \in G | g^{-1}x \in H\}$ this definition is essentally telling us that by multiplying every element in $gH$ by $g^-1$ we get elements of $H$.

$$\begin{aligned}
[g]_R &= \{x \in G | g^{-1}x \in H\} \\
&= \{x \in G | \exists h \in H, h = g^{-1}x\} \\
&= \{x \in G | \exists h \in H, hg = x\} \\
&= \{hg | h \in H\}
\end{aligned}$$

It is improtant to note all of this defines **LEFT** cosets. We write $G/H$ to denote $G/R$.

**Proposition 11.** *The cosets form a partition of the group*

This comes from it being a set quotient.

It is important to also note $g \in gH$ as $gRg$ sure to the thact $e_G \in H$ We can remember that $L_g$ is a bijection so all cosets are the same size.