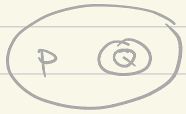
- Logistics (Name, Maithreya, 10 minute break 10.10 – 10.20)
- History of algebra (in the sense of solving for unknowns)
  - Rethorical algebra
    - Egypt. Rhind papyrus (1550 BC) $x + \frac{x}{4} = 15$ The thing together with the fourth part of the thing is fifteen. Then substitute $x = 5$.
    - India. Brahmagupta and co (600-700 AD) 0, negative numbers
      gives formula for quadratic equation
    - Al-Khwarizmi (820 AD) solves quadratic equation by rethorical algebraic manipulations
      introduces Europeans to algebra
  - Symbolic algebra
    - Viète (1590), Descartes (1600s): current symbolic system

      Made cumbersome manipulations
      - more intuitive
      - easier to check
      - more aesthetic
  - Diagrammatic algebra Math on a line ~> math on a plane

    allows to make unintuitive definitions intuitive e.g. (bi)adjoint functors $F, G : \mathcal{C} \to \mathcal{C}$
    become the simple equalities

    - Peirce (1882) Diagrammatic logic

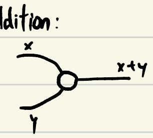
      $P \to Q$
    - Hotz (1965) String diagrams
      - Fun!
      - Powerful enough to describe linear algebra
      - Many equations at once
      - Underlying category theory
        - it perfectly encapsulates the structure of a PROP, a symmetric monoidal category generated by 1 object
        - diagrams encode equational bureaucracy
- String diagrams

1. The natural numbers

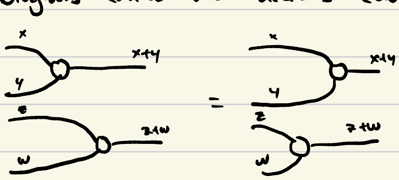
Rules:

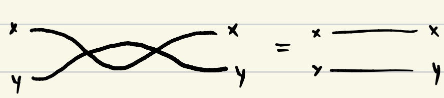
- Diagrams are special graphs which have inputs on the left and outputs on the right

  Addition:

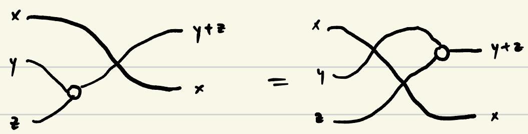
  

  $(x, y \in \mathbb{Z}_{\geq 0})$
- Diagrams can be slid accross each other "the output is unchanged"

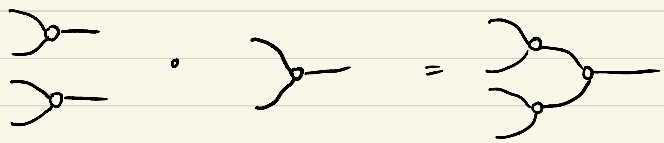
  

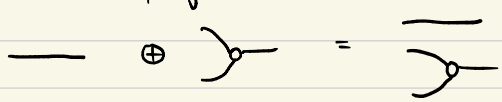
  "wires don't tangle" (that would be braided)



- Inputs and outputs cannot be permuted, they are fixed, we therefore drop the labels, as they are redundant
- Diagrams can be composed, as long as inputs/outputs match:

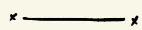


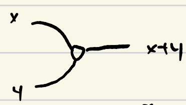
- Direct sum of diagrams

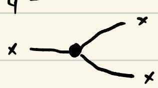


- Operations:

  Direct sum and composition

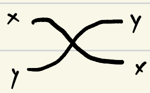
  Identity: 

  Addition: 

  Copying: 

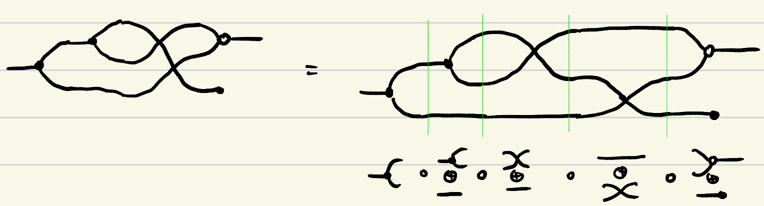
  Zero: 

  Discard: 

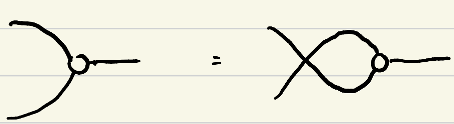
  Twist: 

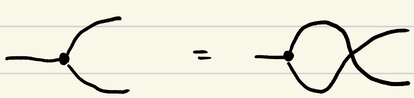
  (for now)

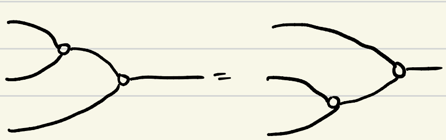
- One last rule: diagrams are built from these blocks

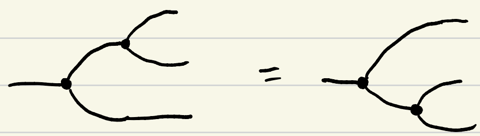


Axioms

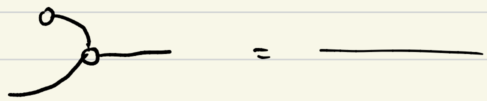
 (Comm) compare with $\forall x, y \in \mathbb{Z}_{\geq 0}, \ x+y = y+x$

 (Cocomm) note that symbolic algebra doesn't express copying

 (Assoc) compare with $\forall x, y, z \in \mathbb{Z}_{\geq 0}, \ (x+y)+z = x+(y+z)$

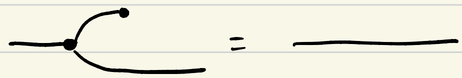


(Coassoc)



(Unit)

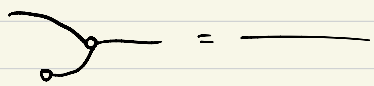
Ask: next axiom.



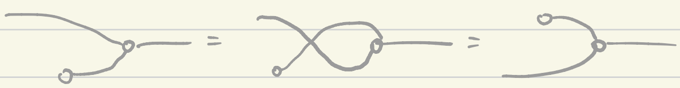
(Counit)

Things we can do

Theorem



(Let them prove it)



(Ask for analogous theorem)

do we need to prove it?

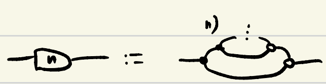
Counting Devise a diagram that takes a number x and multiplies it by n

x —— ? —— nx

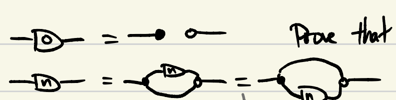
If stuck: general theme in math is solving easier problems

What about n=0?

Let us abbreviate it:



Define it recursively:

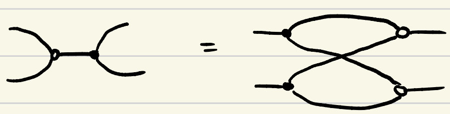


explain

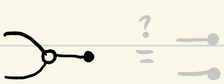
Prove that it works inductively.

What is its reflected version?

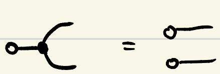
Some more axioms



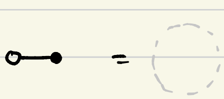
(B1) Convince. What is the reflected version?



(B2)



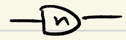
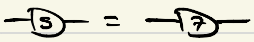
(B3)



(B4)

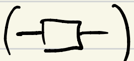
Rmk: fancy word for these: cocommutative bialgebra

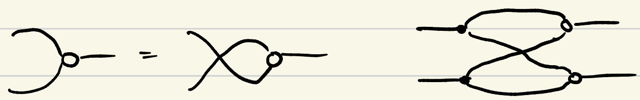
Exercises

We have seen that we may represent the numbers as . Is it possible to prove
 ?

Ask.

How do we prove things are different in mathematics? Invariants (e.g. Euler char, dimension)

We define $\chi($$)$ = number of paths from left to right. To see that this is an invariant, it suffices to check it on the axioms, e.g.:

 . . .

2. Linear algebra and diagrams

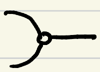
I promised that diagrams encode linear algebra.

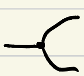
The main point is that there is a translation

$$\left\{ \begin{array}{c} \text{string diagrams} \\ n \longrightarrow m \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{matrices} \\ n \text{ columns } \; m \text{ rows} \end{array} \right\}$$

this is an example of an equivalence of categories, but even further: isomorphism of categories.

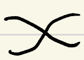
The translation goes as follows:

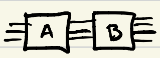
 $\longrightarrow \begin{pmatrix} 1 & 1 \end{pmatrix}$

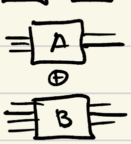
 $\longrightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

 $\longrightarrow ()$ (1 column, 0 rows)

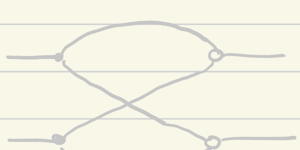
 $\longrightarrow ()$ (0 columns, 1 row)

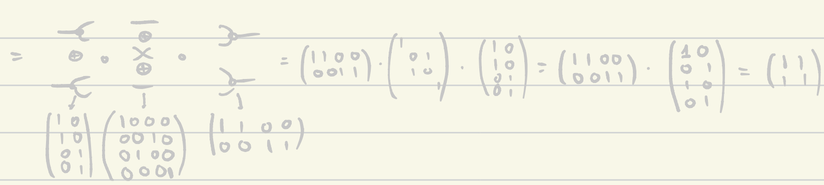
 $\longrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

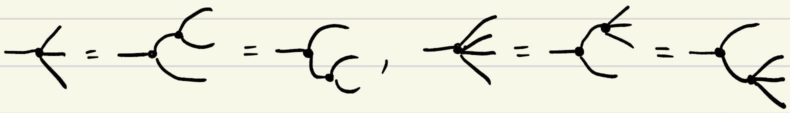
 $\longrightarrow BA$

 $\longleftrightarrow \left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right]$

Reflection $\longleftrightarrow$ Transpose

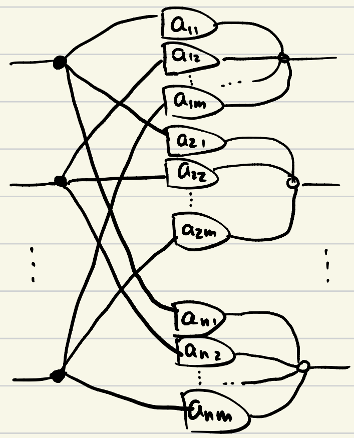
Example: 



Define the shortcuts  etc.

similarly . Then we can translate back

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{nm} \end{pmatrix} \longrightarrow$$



Claim: any diagram can be transformed into one as above

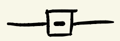
Claim: one can also go from diagram to matrix by counting

Could give formal proofs, but it is more important that they familiarize themselves with the kind of arguments, and it is more fun to discover things by yourself.

Exercises

3. Beyond $\mathbb{N}$

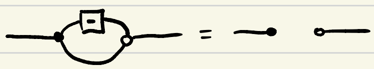
We introduce a new (morphism) basic diagram to our (category) system:



"the antipode"

This multiplies a number by -1 :

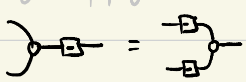
and the defining feature is that



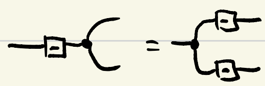
(A1)

How does it interact with the rest of diagrams?

Adding / copying:

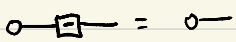


(A2)

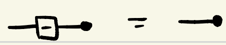


(coA2)

Zero / discarding:



(A3)



(coA3)

Rmk: fancy word for these: bicommutative Hopf algebra

Exercises

4. In construction: The power of a flip: rationals, linear maps for free.

Change of plans: braid groups

Week 2

We have seen that diagrammatics can represent algebraic manipulations.
But algebra is not only about solving equations, it is also "the study of algebraic structures". We will look at the most foundational algebraic structure: the group.
These are "the essence" of many phenomena in mathematics and elsewhere.

Def: a set, as a bag of elements. Examples: $\{1,2,\dots\}$, "$\mathbb{Z}$", "$\mathbb{Q}$", $\{a,b,\dots,z\}$, ..

Def: a group, an abelian group

abstract! e = identity

Examples:

(1) $(\mathbb{Z},+)$

(1') $(\mathbb{Z}_{\geq 1},+)$ no identity

(1'') $(\mathbb{Z}_{\geq 0},+)$ no inverses

(1''') $(\mathbb{Z},-)$ not associative

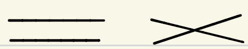
(1^{IV}) $(\mathbb{Z},\div)$ not always defined

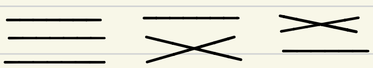
(1^{V}) $(\mathbb{Z},\cdot)$ no inverses

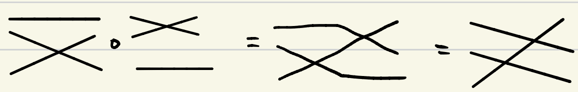
(1^{VI}) $(\mathbb{Q},\cdot)$ not defined at zero

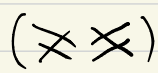
(2) A clock

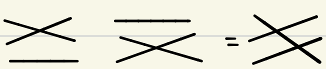
(3) C_n

(4) 

(5)  "and all their combinations, including repeats and inverses"

Operation is composition: 

Composition of diagrams is associative, has identity, inverses  so it is a group

Not abelian: 

How many elements?

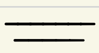
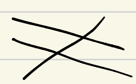
a) 5

b) 6

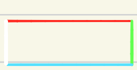
c) 7

d) ∞

(discuss, vote again)

(6) All combinations of  and . How many elements? "order" "Isomorphic to C_3"

"S_n"

(6)  V_4

(7)  "Isomorphic to S_3"

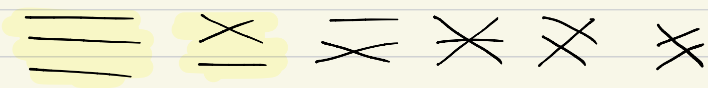
Exercises 1st Block: vote if these are groups, discuss disagreements.
2nd Block: S_3, C_n, S_4, D_4

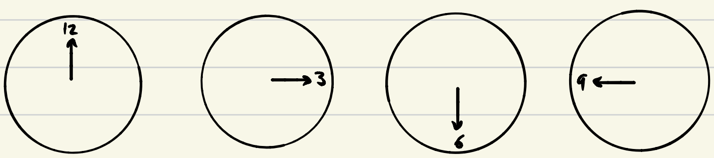
When done:

- Lagrange's theorem:
  - A subgroup $H \subseteq G$ is a subset such that (i) $\forall x,y \in H$ $xy \in H$
    (ii) $\forall x \in H$, $x^{-1} \in H$

H is itself a group!

Examples (don't erase)





$\subset$ C_{12}

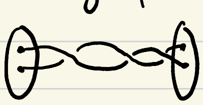
Notice: $|H| \mid |G|$

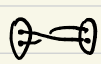
The kind of theorems you prove in algebra: Lagrange's theorem

Relate to original question about S_3.

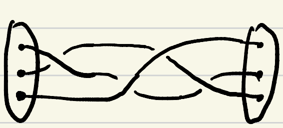
Proof?

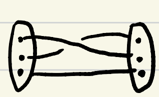
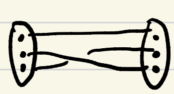
Braid group on 2 strands:



"wires tangle!" "generated by " "isomorphic to $\mathbb{Z}$"

On 3 strands:



"generated by , "