CHAPTER 1

Groups, and other algebraic structures (section 8.1)

1.1. Introduction

A mathematical structure is a formal model which capture common properties or behavior of different sets.

It consists of an abstract set, together with operations and relations which obey certain rules.

For example the set of tasks to build a house, and the set of all courses available at CSM have something in common: the notion of prerequisite. This notion can be formalized using a structure of partially ordered set.

We will introduce here certain algebraic structures, which are useful to model arithmetic, as well as to the study of symmetries.

1.2. Permutations

DÉFINITION. Let A be a set. A *permutation* of A is a bijection from A to A.

Let S_A be the set of all permutations of A.

Let S_n be the set of all permutations of $\{1, \dots n\}$.

A permutation σ of S_n can be written in *array form* as follow:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 3 & 6 \end{pmatrix},$$

meaning that $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 4$, and so on.

EXERCICE 1. Write all permutations in S_1, S_2, and S_3.

What is the size of S_n?

1.2.1. Operation on S_n.

S_n as a set is not very interesting.

Can we define operations on S_n?

PROPOSITION. *The composition $\bullet$is an operation of S_n.*

Indeed, the composition of two permutations is still a permutation.

We also call this operation product of permutations.

EXERCICE 2. Compute the following:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 6 & 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

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

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

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

The permutation above produces a *cycle*: $1 \to 2 \to 3 \to 4 \to 5 \to 1$

DÉFINITION. By (a, b, c, d), we denote the permutation σ such that $\sigma(a) = b$, $\sigma(b) = c$, $\sigma(c) = d$, $\sigma(d) = a$, and $\sigma(x) = x$ for any other element x.

Such a permutation is called a *cycle*.

A cycle (i, j) of length two is called a *transposition*.

A transposition $(i, i+1)$ is called *elementary transposition*.

EXERCICE 3. Write $(3, 4, 2, 1)$ and $(2, 1, 3, 4)$ in array notation.

Write the following permutations in array notation:

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

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

$$(1, 2, 3) \bullet (4, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$(4, 5) \bullet (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$(1, 2, 3) \bullet (3, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$(3, 4) \bullet (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

PROPOSITION. *The product of two disjoint cycles is commutative.*

This is not the case for non-disjoint cycles.

EXERCICE 4. Are the following permutations cycles?

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 3 & 6 \end{pmatrix}$$

PROBLEM 1.2.1. So there are permutations that are not cycles.

Would it be possible to write them using only cycles?

THÉORÈME. *Any permutation can be written as a product of disjoint cycles.*

This product is unique, up to the order.

EXERCICE 5. Compute the following permutations

$$(2,3,1,5,4)^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 10 & 2 & 1 & 6 & 4 & 8 & 3 & 7 & 9 \end{pmatrix}^{131} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

Writting a permutation in cycle notation is a good way to compute powers of this permutation.

1.2.2. Generators of S_n. If you have a list, you can use a permutation to change its order.

Well, S_n is pretty big, so this makes quite a lot of possible operations.

However, some operations can be obtained by combining other operations.

Could we try to reduce the size of S_n?

DÉFINITION. A subset G of S_n *generates* S_n if any permutation can be written as a product of elements of G.

PROBLEM 1.2.2. Find a set of generators of S_n as small as possible.

PROBLEM 1.2.3. Does the set of all cycles generate S_n?

PROBLEM 1.2.4. How many cycles are there ?

Can you do better?

PROBLEM 1.2.5. Does the set of all transpositions generate S_n?

How many transpositions are there?

Can you do better?

PROBLEM 1.2.6. Does the set of all elementary transposition generate S_n?

How many elementary transpositions are there ?

By the way, how many elementary transpositions at most do you need to express a permutation?

Can you do better than $n-1$ generators?

1.3. Groups

1.3.1. Definitions and examples. The notation $[A, \bullet]$ denote a set A together with an operation $\bullet$."

PROBLEM 1.3.1. Is there anything in common between $[S_n, \bullet]$ and $[\mathbb{Z}+]$.

DÉFINITION. Let A be a set with an operation $\bullet$

- The operation $\bullet$ is *associative* if:
$$(\forall x)(\forall y)(\forall z)\ x \bullet (y \bullet z) = (x \bullet y) \bullet z$$
- The operation $\bullet$ is *commutative* if:
$$(\forall x)(\forall y)\ x \bullet y = y \bullet x$$

- $i \in A$ is an *identity element* if:
$$(\forall x)\ x \bullet i = i \bullet x = x$$
- Assume $[A, \bullet]$ has an identity element i. Then $y \in A$ is an inverse for $x \in A$ if
$$y \bullet x = x \bullet y = i$$

What are the properties of $[\mathbb{Z}, +]$?

- $+$ associative;
- $+$is commutative;
- 0 is an identity element;
- If x is an integer, then$-x$ is an inverse for x.

What are the properties of $[\mathbb{R}^*, \cdot]$?

Those structures have many common properties.

DÉFINITION. $[G, \bullet]$ is a *group* if G is a non empty set, and $\bullet$is a binary operation on G such that:

(1) $\bullet$ is associative
(2) an identity element exists (in G).
(3) each element of G has an inverse (in G) with respect to $\bullet$.

If the operation $\bullet$is commutative, G is called a *commutative group*.

EXERCICE 6. Which of the following are groups ?

(1) $[\mathbb{Z}, +]$
(2) $[\mathbb{N}, +]$
(3) $[\mathbb{Z}, -]$
(4) $[\{true, false\}, \wedge\}$
(5) $[\mathbb{R}, +]$
(6) $[\mathbb{R}, \cdot]$
(7) $[S_n, \bullet]$
(8) $[n\mathbb{Z}, +]$

What's the point ?

- Many structures, coming in particular from arithmetics, are groups.
- If you prove a property for groups in general, you have proved this property for all of those structures.
- Group theory is a vast field, and there are hundreds of theorems about groups waiting for you to apply them on your favorite structure.
- Basic tool to study the Rubicks Cube.

1.3.2. Just some examples of results and questions about groups.

THÉORÈME. *The identity of a group is unique.*

The inverse of an element is unique.

The equations $a \bullet x = b$ and $x \bullet a = b$ have a unique solution.

The inverse of a product can be computed by $(x \bullet y)^{-1} = y^{-1} \bullet x^{-1}$.

DÉFINITION. Let $[G, \bullet]$ be a group, and $A \subseteq G$.

Then $[A, \bullet]$ is a *subgroup* of $[G, \bullet]$ if $[A, \bullet]$ itself is a group.

THÉORÈME. *The size of a subgroup divides the size of the group.*

PROBLEM 1.3.2. Common problems about a group:

- Find a minimal set of generators
- Express an element of the group as product of generators
- Efficient computations
- Find all subgroups
- Are two groups structurally the same (are they isomorphic?)

For playing with groups, there is a very nice program:
`http://www-history.mcs.st-and.ac.uk/~gap/`

1.3.3. Groups and Symmetries. One common use of groups if for the study of problems with symmetries.

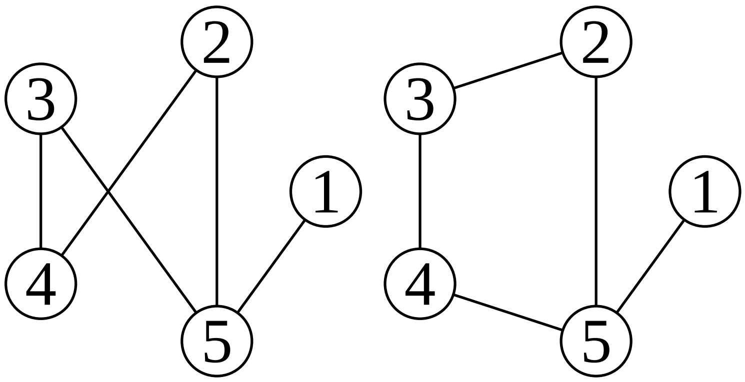
EXEMPLE. Computing the temperature in a house with a heater in the middle.

- Case 1: the house has a random shape;
- Case 2: the house is round;
- Case 3: the house is square.

Most of the time, a problem with symmetry has a symmetric solution.
Using this can save a LOT of time.
Problem: finding the orbits
The set of all symmetries is a group, so group theory can help you.

1.3.4. Groups and isomorphy of graph.

DÉFINITION. The two following structures are labelled graphs:

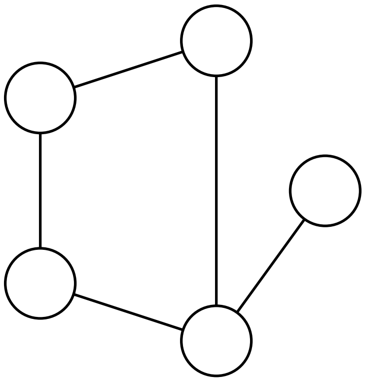


If you exchange the nodes 3 and 4 of the first graph, you get the second.
The group S_n *acts* on graphs on n nodes.
Structurally, except for the numbering, there is no difference between them:
They are *isomorphic*.

PROBLEM 1.3.3. Testing if two graphs are isomorphic.

This is an important but very difficult problem.

DÉFINITION. The following structure is an *unlabelled graph*:



It can be defined as an equivalence class of labelled graphs.

PROBLEM 1.3.4. How many labelled graphs on n nodes ?
How many unlabelled graphs on n nodes ?

Group theory provides a tool (Pólya enumeration) for this.

1.4. Conclusion

- Groups are an abstract model for many common structures
- Results about groups apply to all of those structures
- Groups are a powerful tool to study problems with symmetries
- Groups often occurs when dealing with unlabeled structures