Lecture 6

Reference: Judson, Chapter 3.2

Groups

Last time we have introduced *laws of composition* $(S,*)$ and defined what it means for $*$ to be associative/commutative and to admit an identity.

Compare the following proposition to problem #5 from the first homework.

Proposition 1

Let $(S,*)$ be a set with an associative composition law and identity. Let $x,y \in S$ be two invertible elements, then $x*y$ is also invertible with $(x*y)^{-1} = y^{-1} * x^{-1}$

Proof. Indeed, we have

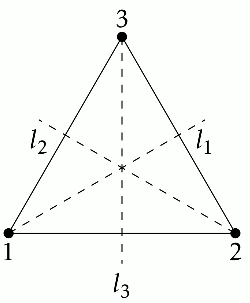
$$(x*y)*(y^{-1}*x^{-1}) = x*(y*y^{-1})*x^{-1} = x*e*x^{-1} = x*x^{-1} = e$$

where in the first equality we used associativity, in the second the fact that y^{-1} is the inverse of y, in the third the property of the identity e, and in the last the fact that x^{-1} is the inverse of x.
Similarly we check that $(y^{-1}*x^{-1})*(x*y) = e$ which proves that $(y^{-1}*x^{-1}) = (x*y)^{-1}$. □

Definition of a group

Groups is one of the most fundamental notions in mathematics. Whenever you have an object (of any nature) admitting *symmetries*, there is a group lurking behind.

Example 1: Key motivating example



Let Δ be an equilateral triangle. Then there 6 rigid motions mapping Δ onto itself, i.e., bijections $f: \Delta \to \Delta$ preserving the distances between points:

- 3 rotations – by 0°, 120° and 240° (denote them μ_0, μ_1, μ_2)
- 3 reflections along 3 altitudes l_1, l_2, l_3 (denote the reflection by $\sigma_1, \sigma_2, \sigma_3$).

We claim that the composition operation on the set $\{\mu_0, \mu_1, \mu_2, \sigma_1, \sigma_2, \sigma_3\}$ defines a law of composition (exercise).

Problem 1: Prove that the above law of composition is associative, has an identity and every element admits an inverse. Show that it is **not** commutative.

Definition 1

Let $(G,*)$ be a set with a law of composition. We will say that $(G,*)$ is a group if the following properties hold:

(G1) $*$ is associative

(G2) there is an identity $e \in G$

(G3) every element $x \in G$ is invertible.

Definition 2

A group $(G,*)$ is *commutative* or *abelian* if $*$ is commutative.

Proposition 2: Cancellation law

If $(G,*)$ is a group and $x,y,z \in G$ are elements such that

$$x*y = x*z,$$

then $y = z$, i.e., we can cancel out x from the both sides.

Proof. Let us multiply both sides of the above identity by x^{-1} *from the left*. Then we will have

$$x^{-1}*x*y = x^{-1}*x*z.$$

Due to associativity we do not have to specify the brackets and can perform multiplication in any order we like (without swapping the elements). Then on both sides we have $x^{-1}*x = e$, so

$$e*y = e*z$$

Now, due to the definition of e, we have $y = z$. □

Remark 1

For $n \in \mathbb{Z}$ we will write

$$x^n := \underbrace{x*x*\cdots*x}_{n \text{ times}}$$

if $n > 0$ and

$$x^n := (\underbrace{x*x*\cdots*x}_{-n \text{ times}})^{-1}$$

if $n < 0$. As usual, $x^0 = e$.
Check that for $n,m \in \mathbb{Z}$ we have $(x^n)^m = (x^m)^n = x^{nm}$.

To feel better the notion of a group we will need to stock on examples.

Example 2

$(\mathbb{Z},+)$, integers under addition form a group with the neutral element being 0.
$(\mathbb{Z},\times)$ is **not** a group, since 2 does not have a multiplicative inverse in $(\mathbb{Z},\times)$.
$(\mathbb{R},\times)$ is **not** a group, since 0 does not have a multiplicative inverse.
$(\mathbb{R}\backslash\{0\},\times)$ is a group with neutral element being 1.
$(\mathbb{Z}_n,+)$ is a group with neutral element $[0]$.
$(\mathbb{Z}_n,\times)$ is **not** a group since $[0]$ does not have a multiplicative inverse, however, similarly to the example of $(\mathbb{R}\backslash\{0\},\times)$, we find that the set of units $(\mathbb{Z}_n^\times,\times)$ is a group.

All of the above groups are commutative.