MAT1100 - Grublegruppe
Extra Problems 8

Jørgen O. Lye

Introductory group theory

This note is meant as a brief introduction to some aspects of elementary group theory. We start with the definition. A group G is a set together with a binary operation $*: G \times G \to G$ satisfying the following.

- There is an element $e \in G$ such that $e * g = g * e = g$ for all $g \in G$.
- If $g \in G$, there is an element $g^{-1} \in G$ such that $g * g^{-1} = e$.
- If $f, g, h \in G$ then $f * (g * h) = (f * g) * h$.

These requirements state that there should exist an **identity element**, all elements should have **inverses**, and **associativity** should hold.

Examples

Show (or convince yourself) that the following satisfy the group axioms.

$\mathbb{R}$

The set $G = \mathbb{R}$ with operation $* = +$, $e = 0$, $g^{-1} = -g$. Why not choose $* = \cdot$ on this set?

$\mathbb{R}^+$

The set $G = \mathbb{R}^+ = \{x \in \mathbb{R} \big| x > 0\}$ with $* = \cdot$, $g^{-1} = \frac{1}{g}$. Why not choose $* = +$?

$\mathbb{C}$

The set $G = \mathbb{C}$ with $* = +$.

$\mathbb{C}^*$

The set $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $* = \cdot$.

$\mathbf{Z}$

$G = \mathbf{Z}$ and $* = +$.

Exercise

Show (by only using the group axioms) that the inverse element is unique. Similarly, show that the identity element is unique.

Commutativity

Notice that I never required $g * h = h * g$. Groups for which this holds are called **abelian** (after Abel). Convince yourself that all the above examples are Abelian groups. If you know about matrices, then the following example is a non-abelian group:

Matrix groups

Let $G = GL(2, \mathbb{R})$ or $GL(2, \mathbb{C})$ where

$$GL(2, \mathbf{F}) = \{2 \times 2 \text{ invertible matrices with entries in } \mathbf{F}\}$$

Show that this is a group with normal matrix multiplication. Show that

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

and that all the matrices involved have inverses. This shows that $GL(2, \mathbf{F})$ is non-abelian.

Maps between groups

The maps, or functions, we study in Calculus are usually assumed to be continuous. Often differentiable as well. For groups, these notions don't necessarily make sense[1]. We need another requirement on our functions to make them respect group structure, and that requirement is as follows:

[1] Differentiability can make sense for a group, and it's often very interesting when it does.

Let H and G be groups.

$$\phi : G \to H$$

is called a (group) **homomorphism** if

$$\phi(a *_G b) = \phi(a) *_H \phi(b)$$

for all $a, b \in G$.

Note that this says that I can compute the product between a and b in G *or* I can map them to H and use the product there. The answer should be the same.

Examples

Argue that

$$\exp : \mathbb{R} \to \mathbb{R}^+$$

is a group homomorphism. Same with

$$\ln : \mathbb{R}^+ \to \mathbb{R}$$

Argue that $\phi : \mathbf{Z} \to \mathbf{Z}$ given by $\phi(x) = ax$ is a homomorphism for any $a \in \mathbf{Z}$.

Exercise

Argue that for $\phi : G \to H$ to be a homomorphism, we must have $\phi(e_G) = e_H$.

Inverses

Assume a homomorphism $\phi : G \to H$ is bijective, meaning it is one-to-one and onto (injective and surjective). As a map of sets, the inverse function exists. If ϕ^{-1} is also a homomorphism, we call ϕ an **isomorphism** and say that G and H are isomorphic groups. Isomorphic groups are denoted by $G \cong H$, or even $G = H$.

Example

Argue that $\mathbb{R} \cong \mathbb{R}^+$ as groups where the operation on $\mathbb{R}$ is $+$ and the operation of $\mathbb{R}^+$ is $\cdot$.

Exercise

Show that if $\phi : G \to H$ is an isomorphism, then $\phi(g^{-1}) = \phi(g)^{-1}$.

The complex case:

Argue that the map

$$\exp : \mathbb{C} \to \mathbb{C}^*$$

is a group homomorphism. Is this an isomorphism of groups?

Modular arithmetics

Let $p \in \mathbf{Z}$ and define the set $p\mathbf{Z} = \{p \cdot n \big| n \in \mathbf{Z}\}$. Argue that $p\mathbf{Z}$ is a group for any p with addition as operation. As an example, $2\mathbf{Z}$ are all the even integers. Do the odd integers form a group?

Quotients

We will look more at quotients next time. For now, define the set

$$\mathbf{Z}/(p\mathbf{Z}) = \{0, 1, 2, \cdots p - 1\}$$

and define addition modulo p on it. As an example, $\mathbf{Z}/(3\mathbf{Z}) = \{0, 1, 2\}$ and $1 + 1 = 2$, $2 + 1 = 0$, $2 + 2 = 1$ etc. Argue that this is a group for any p.

Unit roots

The groups $\mathbf{Z}/(p\mathbf{Z})$ are written additively, but they are in fact isomorphic to a group written multiplicatively. Let

$$C_n = \{\text{n'th roots of unity}\} = \{\zeta \in \mathbb{C} \Big| \zeta^n = 1\}$$

Here the group operation is multiplicative

$$\zeta * \omega = e^{\frac{2\pi ik}{n}} e^{\frac{2\pi il}{n}} = e^{\frac{2\pi i(k+l)}{n}}$$

Argue that $C_p \cong \mathbf{Z}/(p\mathbf{Z})$.