Notes for CS203

Contents

Chapter 1

Groups

> You also get dramatic advances when you spot that you can leave out part of the problem. Algebra, for instance (and hence the whole of computer programming), derives from the realisation that you can leave out all the messy, intractable numbers.
>
> Douglas Adams (The Salmon of Doubt: Hitchhiking the Galaxy One Last Time, 2002)

The term Group was first used by Galois in his quest of solutions of roots of polynomial equations of degrees higher than four. The development of group theory has three main roots, the theory of algebraic equations, geometry and number theory. Today, group theory and abstract algebra in general sees many uses in the field computer science, from cryptography and coding theory, down to finding computationally faster methods to multiply integers.

1.1 Introduction

Definition 1. *Let G be a set. Let $\circ : G \times G \to G$ be a map that satisfies the following properties:*

- *Closure: For all $a, b \in G$, we have $a \circ b \in G$.*

- *Associativity: For all $a, b, c \in G$, we have $(a \circ b) \circ c = a \circ (b \circ c)$*
- *Identity: There exists an element in G, say e that satisfies $a \circ e = e \circ a = a$, for all $a \in G$.*
- *Inverse: For every element $a \in G$, there exists an unique element b that satisfies $a \circ b = b \circ a = e$, where e is the identity, as described above.*

Such a set G, if the operation satisfies the above properties, is called a group under $\circ$.

Put in words, a group is a set, along with a binary operation that is closed under the operation, the operation is associative in the elements of the set, there exists an identity for the operation in the set, and all elements of the set have an inverse.

Further, if the elements satisfy the property that for all $a, b \in G, a \circ b = b \circ a$, then the group is called an **abelian** group, or a commutative group. If not, then the group is called **non-abelian**, or non commutative.

A number of examples and counterexamples are presented below to reinforce the concept of the group, and to set up notation for the rest of this text.

Examples

- *Example 1:* $\mathbb{Z}$, the set of all integers, is a group under the addition operation. It is easy to see that all the group properties are satisfied by addition, with 0 being the identity, and the inverse of any number a being $-a$. It is also easy to see that this group is abelian. Further, the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all similarly sets under addition (the set of rationals, reals, and complex numbers respectively).
  Note however, that $\mathbb{N}$, the set of natural numbers is NOT a group, since no element except the identity 0 has an inverse.
- *Example 2:* Similarly, the set of all $n \times m$ matrices with entries from $\mathbb{Z}$, under the operation of matrix addition is an abelian group.
- *Example 3:* The set of all non-zero rational numbers, $\mathbb{Q}^*$ is an abelian group under the operation of multiplication, with identity 1. Note however, that the set $\mathbb{Z}^*$ is not a group, since integers do not have integer multiplicative inverses. Also, we require that our set contains all rationals EXCEPT 0, since 0 cannot have a multiplicative inverse.

- *Example 4:* The set of all invertible $n \times n$ matrices with entries in $\mathbb{Q}$ is a group under the operation of matrix multiplication. The $n \times n$ identity matrix I acts as the identity element. Further, since the product of invertible matrices is invertible, the operation is closed. This group is non-abelian.

Chapter 2

Rings

Lorem Ipsum

Chapter 3

Fields

Lorem Ipsum