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.

- *Example 5:* Let $S_n = \{f | f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}\}$, such that every f is a permutation. S_n is a group under the operation of permutation.

- *Example 6:* Define $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. This set is an abelian group under the operation $+ \pmod{n}$.

- *Example 7:* Define $\mathbb{Z}_n^* = \{0, 1, \ldots, n-1\}$. This set is an abelian group under the operation $* \pmod{n}$, when n is prime.
  Note that this is not the case when n is composite. For example, in $\mathbb{Z}_6^*$, $2 * 3 \equiv 0 \pmod{6}$, which is not in the set, that is, closure is violated.

- *Example 8:* For composite numbers, we redefine $\mathbb{Z}_n^* = \{m | 1 \leq m \leq n, gcd(m, n) = 1\}$. Under this definition, $\mathbb{Z}_n^*$ is an abelian group under modular multiplication for all n.

- *Example 9:* The set of complex n^{th} roots of unity for any n is an abelian group under multiplication.

- *Example 10:* Consider the curve $y^2 = x^3 - x$. Let the set E be the $\{$ All points on the curve$\} \cup \{\infty\}$. For any $p, q \in E$, define $p+q$ as first joining p and q by a line, getting the unique point of intersection of the line with the curve itself, and then taking its mirror with respect to the x axis. E is then a group under the above operation.

Now that a large number of examples have been presented, the reader should have a basic intuitive idea of a group. In the next sections, we study the structure of groups, and mapping between groups.

1.2 Subgroups and Group Morphisms

Definition 2. *Let G be a group. A set $H \subseteq G$ is a **subgroup** of G if H is a group under the same operation.*

More verbosely, H is a subgroup of G if it is a subset of G, and the following three properties hold.

- $e \in H$, where e is the identity element of G.
- If $a, b \in H$, then $a \circ b \in H$, where $\circ$ is the operation under which G is a group.
- If $a \in H$, and $a \circ b = e$ in G, then $b \in H$. In other words, if an element is in a subgroup, so is its inverse.

Some examples of subgroups are:

- *Example 1:* The set $\mathbb{Z}$ under addition is a subgroup of $\mathbb{Q}$, which itself is a subgroup of $\mathbb{R}$, which further is a subgroup of $\mathbb{C}$.
- *Example 2:* For any group G, G is a subgroup of itself. G is called the improper subgroup of G.
- *Example 3:* For any group G, the set consisting of only the identity element is a subgroup. This is called the trivial subgroup of G. All other subgroups are called non-trivial.
- *Example 4:* Let G be the group of all nxn invertible matrices under multiplication. Consider the subset of all matrices that have determinant 1. This forms a subgroup of G. Similarly, the subset of all matrices that have determinant ± 1 also form a subgroup of G. Both of these subgroups are proper and non-trivial.

Definition 3. *Let G and H be groups under the operations $+$ and $\oplus$ respectively. Let $\psi : G \to H$. Mapping ψ is a **homomorphism** if for all $a, b \in G$, we have $\psi(a+b) = \psi(a) \oplus \psi(b)$. Further, if ψ is also one-one and onto, then ψ is called an **isomorphism**. In this case, we generally write $G \cong H$.*

For example, consider the group $\mathbb{Z}$ of integers under addition, and the group $\mathbb{Q}^*$ of non zero rationals under multiplication. Let the map $\psi : \mathbb{Z} \to \mathbb{Q}^*, \psi(n) = 2^n$. ψ is a homomorphism, as for all $a, b \in \mathbb{Z}$, $2^{a+b} = 2^a \times 2^b$.

Chapter 2

Rings

Lorem Ipsum

Chapter 3

Fields

Lorem Ipsum