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 [1] 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] Galois was a brilliant mathematician, but he unfortunately was killed in a duel when he was just 20, which might have had been motivaed by a conflict arising from a romantic entanglement, or his political involvements.

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 $\circ$. Note that the third condition forces the identity to be unique. The proof for this is trivial, and has been left as an exercise. [2] *If this were not the case, the fourth condition would not have made sense.*

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.

[2] Hint: Attempt a proof by contradiction

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

- *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 $\mathbb{Z}_n^* = \{1, \ldots, n-1\}$. 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 set $\{$ 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 $n \times n$ 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 $a, b \in \mathbb{Z}$, $2^{a+b} = 2^a \times 2^b$.

Let ψ be a homomorphism from G to H.

Lemma 1. *Let $\widehat{H} = \{b|\psi(a) = b, a \in G\}$. $\widehat{H}$ is a subgroup of H.*

Proof. If $b, c \in H$, then we have $x, y \in G$ such that $\psi(x) = b, \psi(y) = c$. Then $\psi(x + y) = b \oplus c$ by property of homomorphisms. $\widehat{H}$ is thus closed. Associativity is inherited from H. Homomorphisms necessarily map identities to identities. This can trivially be checked by noting that $\psi(e_g + e_g) = \psi(e_g) = \psi(e_g) \oplus \psi(e_g)$ where e_g is the identity of G. This gives us existence of identity in $\widehat{H}$. Finally, if $\psi(x) = a$, then the image of the inverse of x is the inverse of a. This can be derived again by using the fact that identities are mapped to identities. □

If ψ is a one-one map, then clearly ψ gives an isomorphism between G and $\widehat{H}$. If not, then consider the set $\widehat{G} = \{a|a \in G, \psi(a) = e_h\}$, where e_h is the identity of H.

Lemma 2. *$\widehat{G}$ is a subgroup of G.*

Proof. Closure holds since if for $a, b \in \widehat{G}$ we have $\psi(a) = \psi(b) = e_h$, then $\psi(a + b) = \psi(a) + \psi(b) = e_h + e_h = e_h$. Associativity is inherited from G. Identity exists because homomorphisms map identities to identities. Finally for any $a \in \widehat{G}$, we have that the image of the inverse of a is the inverse of the image of a, or the inverse of e_h, which is e_h itself. □

This subgroup is called the **kernel** of ψ.

1.3 Effect of ψ on G - Quotienting

For each b in $\widehat{H}$, let by $[b] = \{a|a \in G, \psi(a) = b\}$. In this notation, the kernel of ψ is clearly represented by $[e_h]$.

Lemma 3. *For each $b \in \widehat{H}$, we have $[b] = a + \widehat{G}$ for some $a \in G$. Here, $a+\widehat{G}$ refers to the set of all elements that we get by adding a to each element of $\widehat{G}$, or more formally $a + \widehat{G} = \{b|b = a + g, g \in \widehat{G}\}$.*

Proof. Let $\psi(a_1) = \psi(a_2) = b$. This gives us that $\psi(a_1 - a_2) = 0 \Rightarrow a_1 - a_2 \in \widehat{G}$, where $-a_2$ refers to the inverse of a_2 in G. This gives us $a_1 \in a_2 + \widehat{G}$. But a_1 was picked arbitrarily. We can repeat the above argument with any element from $[b]$ in place of a_1, and we always get, for all elements a, $a \in a_2 + \widehat{G}$. This completes the proof. □

Further, also note that for every element a that belongs to $a_2 + \widehat{G}$, we have $\psi(a) = \psi(a_2) + \psi(g)$ for some $g \in \widehat{G}$. Every element of $a_2 + \widehat{G}$ maps to b under ψ. Thus, the elements of G are partitioned, and each can be recognized by an element of $\widehat{H}$ (for every element $b \in \widehat{H}$, the corresponding partition is $[b]$) or by a single element of each partition (implicitely adding G will give the whole class). The above gives us an equivalence relationship, with $a_1 R a_2 \Leftrightarrow \psi(a_1) = \psi(a_2)$.

Define operator $\boxplus$ be defined as $[b_1] \boxplus [b_2] = [b_1 \oplus b_2]$.

Define $G\Big/\widehat{G} = \{[b_i] | b_i \in \widehat{H}\}$.

Lemma 4. *$G\Big/\widehat{G}$ is a group under $\boxplus$.*

Proof. Closure is clear from the definition of $\boxplus$. For associativity, we have

$$\begin{aligned}([a] \boxplus [b]) \boxplus [c] &= [a \oplus b] \boxplus [c] \\ &= [(a \oplus b) \oplus c] \\ &= [a \oplus (b \oplus c)] \\ &= [a] \boxplus [b \oplus c] \\ &= [a] \boxplus ([b] \boxplus [c])\end{aligned}$$

$[e_h]$ clearly acts as the identity. Further, for any $[a]$, the inverse of $[a]$ is simply $[b]$ such that b is the inverse of a in H. This follows since $[a] \boxplus [b] = [a \oplus b] = [e_h]$. □

It is quite obvious that $G/\widehat{G}$ and H are isomorphic, with the map being one that sends $[b] \to b$.

The above formulation is known as the the **First Isomorphism Theorem**.

We now Quotient G with other subgroups and study the resulting structure.

Let G be an abelian group, and $\widehat{G}$ be a subgroup of G.

For any $a \in G$, define $[a] = \{b | b \in G, b - a \in \widehat{G}\}$. For any $a_1, a_2 \in G, either [a_1] = [a_2]$ or $[a_1] \cap [a_2] = \phi$. Define $G\Big/\widehat{G} = \{[a] | a \in G\}$. Define $[a_1] \boxplus [a_2] = [a_1 + a_2]$. $G\Big/\widehat{G}$ is a group under $\boxplus$. It is called the quotient group of $\widehat{G}$.

The element $a \in G$ is called the representative element of $[a]$ in the quotient group. The representative element is clearly not unique.

Examples

- *Example 1:* Consider the group $\mathbb{Z}$, and its subgroup $n\mathbb{Z}$. $\mathbb{Z}\big/n\mathbb{Z} = \{[m]\}$, ie all numbers that are congruent to m modulo n. The most natural representative set is $0, 1, \ldots, n-1$.

- *Example 2:* Consider the group $\mathbb{Q}^*$ under multiplication and its subgroup $G = \{2^n | n \in \mathbb{Z}\}$. $\mathbb{Q}^*\big/G = \{[\alpha]\}$, where the representative set can be $\{\frac{n}{m}, n, m \in \mathbb{Z}, m \neq 0, m, n\ odd\}$.

- *Example 3:* Consider the group of all $n \times n$ matrices under addition, and its subgroup, the set of all $n \times n$ upper triangular matrices. The quotient group of this subgroup can be represented by the set of all lower triangular matrices, with zero in their diagonals.

- *Example 4:* Consider the group $\mathbb{Z}_6$, and its subgroup $G = \{0, 3\}$. $\mathbb{Z}_6\big/G = [m]$, where the representative set can be $0, 1, 2$. Note that this quotient group is isomorphic to $\mathbb{Z}_3$.

- *Example 5:* Let the group be all two dimensional vectors over $\mathbb{R}$, with addition as the group operation. Let the subgroup be any line through the origin. The quotient group is the set $\{[\alpha, \beta]\}$ where a possible representative element can be the intersection of the new line with the x axis.

From this point onwards, we drop the unwieldy notation of using different symbols for representing group actions of various groups. All groups will generally be represented by G or H, with operation $+$. The context should make clear what group the operation is being performed on. Further, the identity element will be represented by 0, and the inverse of an element a by $-a$.

1.4 Finite Groups

The **order** of a group is its cardinality, i.e the number of elements in its set. We represent the order of a group G by $|G|$, or $\mathrm{ord}(G)$.

Theorem 1. *Let H be a subgroup of an abelian group G, with ord(G) $= l$. Then, ord(H)$|l$, and in particular, $l =$ ord(H) $\times$ ord($G\big/H$).*

Proof. H divides G into equivalence classes as discussed above, all of size $|H|$. This implies both that $\mathrm{ord}(H) \mid \mathrm{ord}(G)$ and that $\mathrm{ord}(G) = \mathrm{ord}(H) \times \mathrm{ord}(G/H)$ □

Similar to how the order for the group was defined, we can also define the order of an element $a \in G$ as follows:

For any $a \in G$, let $H_a = \{k \times a | k \in \mathbb{Z}\}$ where $k \times a$ denotes the addition of a to itself k times. Then, $\mathrm{ord}(a) = \mathrm{ord}(H_a)$. H_a is then a subgroup, and it is easy to see that it is isomorphic to $\mathbb{Z}_{ord(a)}$

H_a is more commonly denoted as $\langle a \rangle$. a is called a **generator** if $\langle a \rangle = G$.

Definition 4. *Let G be a commutative group, and $a_1, a_2, \ldots, a_k \in G$. This set is called a generator set if for all $b \in G$, we have $b = \Sigma_{i=1}^{k} k_i \times a_i$. Such a group is called finitely generated, and the set $a_1, \ldots a_k$ is called the generator set.*

We now give, without proof, a very powerful theorem about finite groups.

Theorem 2. *Structure Theorem for Finite Abelian Groups: Let G be a finite abelian group of order l. Then, $G \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ where p_i are primes, and e_i are integers such that $\Pi p_i^{e_i} = l$.*

Chapter 2

Rings

Lorem Ipsum

Chapter 3

Fields

Lorem Ipsum