Math 297 Discussion 10 Notes

Annie Xu

March 27, 2019

Group

A **group** is a set G with a binary operation $\cdot : G \times G \to G$ s.t.
i) $\cdot$ is associative $x(yz) = (xy)z \ \forall x, y, z \in G$
ii) $\exists$ identity element $1 \in G$, $1 \cdot x = x \cdot 1 = x \ \forall x \in G$
iii) Every element x has an inverse, i.e. an element y s.t. $xy = yx = 1$
Note: Commutativity not required. Commutative groups are also called **abelian groups**.
Note: Condition ii) ensures that a group is always nonempty.
Note: G is a **finite group** if in addition G is a finite set.

Examples

1) Zero group: $G = \{1\}$ $\#G = 1$. $\#$ is called the **order** of G
2) $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \quad \cdot = +$
3) $G = \mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+, \quad \cdot = \times$
4) Non-example: $\mathbb{Z}$ with multiplication: only ± 1 have inverses
5) A vector space V along with vector addition is an abelian group. Thus any vector space such as $\mathbb{R}^n$ is, in particular, an additive group.
6) For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation $+$ of addition of residue classes. We might be able to prove later that $+$ is well-defined and associative. For now take it for granted.
7) For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes $\bar{a}$ which have multiplicative inverses mod n is an abelian group under multiplication of residue classes. Again, take for granted that this operation is well-defined and associative.
8) S_n – **symmetric group** on n letters
$S_n = \{f | f \text{ is a bijection from } \{1, \dots, n\} \text{ to itself}\}$
$\cdot$ = composition of functions
$\#S_n = n!$
Cycle notation: $i_1, \dots, i_k$ are distinct $\#'s$ in $\{1, 2, \dots, n\}$
$(i_1, \dots, i_k) \in S_n$ is a map s.t. $i_1 \to i_2, \dots, i_k \to i_1$ everything else fixed.
$(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$
9) F_2 **free groups** in a, b
elements are formall words in letters a, b, a^{-1}, b^{-1}
multiplication: concatenation of words
$(a\ b\ a^{-1})(a\ a\ b\ b) = a\ b\ a\ b\ b$

10) If $(A, \star), (B, \diamond)$ are groups, their **direct product** is defined to be $A \times B = \{(a,b) | a \in A, b \in B\}$. Operation is defined componentwise: $(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$

Basic Properties

You can prove some general facts about group, using the same techniques from 297:
the identity is unique.
the inverse of each element is unique.
$(a^{-1})^{-1} = a \ \forall a \in G$
$(a \cdot b)^{-1} = (b^{-1})(a^{-1})$
generalized associative law holds.
cancellation rule: if $au = av$, then $u = v$; and if $ub = vb$, $u = v$.

Order

For G a group and $x \in G$, define the **order** of x to be the smallest positive integer n s.t. $x^n = 1$, and denote the integer by $|x|$. Also say x is of order n. If no positive power of x is the identity, the order of x is defined to be infinity.

Examples

1) $x \in G$ has order 1 if and only if x is the identity.
2) In the additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, every nonzero (nonidentity) element has infinite order.
3) In the multiplicative group $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$ the element -1 has order 2 and all other nonidentity elements have infinite order.
4) In the additive group $\mathbb{Z}/9\mathbb{Z}$, $\bar{6}$ has order 3 (Why?); the order of $\bar{5}$ is 9.
5) In the multiplicative group $(\mathbb{Z}/7\mathbb{Z})^\times$, $\bar{2}$ has order 3 (Why?); $\bar{3}$ has order 6.
6) S_n: using cycle notation, (1 2 3) has order 3.