Chapter 1 Introduction to Groups

Contents

1 Basic Axioms and Examples

Definition. ***(Binary Operation)***

1. ***(binary operation)*** *$\star$ on a set G is a function $\star : G \to G$. write $a \star b$ instead of $\star(a,b)$*
2. ***(associative $\star$)*** *A binary operation on G is associative if for all $a,b,c \in G$ $a \star (b \star c) = (a \star b) \star c$*
3. ***(commutative $\star$)*** *A binary operation on G is commutative if for all $a,b \in G$, $a \star b = b \star a$*
4. ***(closed under $\star$)*** *$\star$ is a binary operation on G and $H \subset H$, if $\star|_H$ is a binary operation on H, i.e. for all $a,b \in H$, $a \star b \in H$, then H is closed under $\star$. Associativity/Commutativity of $\star$ is inherited on H*

- *(examples)*
  1. *$+$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a commutative binary operation*
  2. *$\times$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a commutative binary operation*
  3. *$-$ is not commutative on $\mathbb{Z}$ ($a - b \neq b - a$ usually)*
  4. *$-$ is not commutative on $\mathbb{Z}^+$ ($1, 2 \in \mathbb{Z}^+$, but $1 - 2 = -1 \notin \mathbb{Z}^+$)*

Definition. ***(Group)***

1. ***(group)*** *A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying*
   (a) *(associative) $\forall\, a,b,c \in G$, $(a \star b) \star c = a \star (b \star c)$*
   (b) *(identity) $\exists\, e \in G \;\; \forall\, a \in G \;\; a \star e = e \star a = a$ (e is an identity of G, alternatively denoted by 1)*
   (c) *(inverse) $\forall\, a \in G \;\; \exists\, a^{-1} \in G$, $a \star a^{-1} = a^{-1} \star a = e$ (a^{-1} is an inverse of a)*
2. ***(abelian group)*** *A group if abelian/commutative if $a \star b = b \star a$ for all $a, b \in G$*
3. ***(finite group)*** *G is a finite group if G is a finite set*
4. ***(direct product)*** *If $(A, \star)$ and $(B, \circ)$ are groups, a new group $A \times B$ called direct product are defined as*

$$A \times B = \{(a,b) \mid a \in A \;\; b \in B\}$$

with binary operation defined component-wise

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \circ b_2)$$

- *(examples)*
  - *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $+$ ($e = 0$, $a^{-1} = -a$, associativity by axioms of $+$)*
  - *$\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ are gorups under $\times$ ($e = 1$, $a^{-1} = 1/a$, associativity by $\times$))*
  - *$(\mathbb{Z} - \{0\}, \times)$ is not a group ($2^{-1} = 1/2 \notin \mathbb{Z} - \{0\}$)*
  - *$(V, +)$ is an abelian group, where V is a vector space (commutativity by axioms of a vector space)*
  - *$(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group ($e = \overline{1}$, $a^{-1} = \overline{-a}$)*
  - *$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ is abelian group ($e = \overline{1}$, a^{-1} exists by definition of $(\mathbb{Z}/n\mathbb{Z})^\times$)*
- ***(theorem)*** *direct product of two groups is a group*
- ***(proposition)***
  1. *(identity unique) identity of G is unique*
  2. *(inverse unique) inverse a^{-1} of any a in G is unique*
  3. *$(a^{-1})^{-1} = a$ for all a in G*
  4. *$(a \star b)^{-1} = b^{-1} \star a^{-1}$*
  5. *(generalized associativity law) value of $a_1 \star a_2 \star \cdots \star a_n$ independent of how its bracketed*
- *(notation)*

- $(\times)$ *denote* $x^n = xx\cdots x$ *by* x^n *and* $x^{-n} = x^{-1}x^{-1}\cdots x^{-1}$ *and* $x^0 = 1$ *the identity*
- $(+)$ *denote* $na = a + a + \cdots + a$ *and* $-na = -a - a - \cdots - a$ *and* $0a = 0$ *the identity*

- ***(proposition)*** *Let* $a, b, u, v \in G$
  1. *(left cancellation law holds) if* $au = av$, *then* $u = v$
  2. *(right cancellation law holds) if* $ub = vb$, *then* $u = v$

Definition. ***(order for an element*** $x \in G$***)*** *is the smallest positive integer* $n \in \mathbb{Z}^+$ *such that* $x^n = 1$, *denoted by* $|x|$. *If no positive power of* x *is the identity, the order of* x *is defined to be infinity*

- *(examples)*
  - *if* $|x| = 1$, *then* $x = 1$ *the identity*
  - *In* $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, +)$, *every nonzero elements has infinite order*
  - *In* $(\mathbb{R} - \{0\}, \mathbb{Q} - \{0\}, \times)$, $|-1| = 2$ *and all other nonidentity elements have infinite order*
  - *In* $\mathbb{Z}/9\mathbb{Z}$, $|\overline{5}| = 9$ *since* 9 *is the smallest integer multiple of* 5 *that is congruent to* $0 \pmod 9$
  - *In* $(\mathbb{Z}/7\mathbb{Z})^\times$, $|\overline{3}| = 6$ *since* 3^6 *is smallest positive power of* 3 *that is congruent to* $1 \pmod 7$

Definition. ***(multiplication/group table)*** *Let* $G = \{g_1, g_2, \cdots, g_n\}$ *be a finite group where* $g_1 = 1$. *The multiplication or group table of* G *is a* $n \times n$ *matrix* A *where* $A_{ij} = g_i g_j$.

- *(fact) For finite groups, the group table contains all information about the group*

2 Dihedral Groups

Definition. ***(Dihedral Groups)***

1. ***(symmetry of*** n***-gon)*** *is any rigid motion of the* n*-gon. We can describe symmetry by choosing a labelling of vertices* $\{1, 2, \cdots, n\}$ *and let the corresponding permutation* σ *over the set as symmetry* s
2. ***(order of*** D_{2n}***)*** *is* $2n$. *(lower bound: vertex 1 can be sent to any vertex* i, *and vertex 2 can be sent to either* $i-1$ *or* $i+1$. *Knowing position of* $1, 2$ *determines position of all other vertices; upper bound: by reasoning that any element of* D_{2n} *can be written as* $r^i s^j$ *where* $0 \le i \le n-1$ *and* $0 \le j \le 1$*)*
3. ***(dihedral group*** D_{2n}***)*** *Fix a regular* n*-gon at origin and label vertices through from 1 to n in a clockwise manner. Let* r *be rotation clockwise about the origin through* $2\pi/n$ *radian and let* s *be reflection about line of symmetry through vertex 1 and the origin.*
$$D_{2n} = \left\{r, s \mid r^n = s^2 = 1\ ,\ \ sr^k = r^{-k}s\right\} = \left\{1, r, r^2, \cdots, r^{n-1}, s, rs, r^2s, \cdots, r^{n-1}s\right\}$$
   (a) $|r| = n$ *and* $|s| = 2$
   (b) $s \neq r^i$ *for any* i *and* $sr^i \neq sr^j$ *for all* $i \neq j$
   (c) $r^k s = sr^{-k}$ *for all* $0 \le i \le n$
4. ***(interpreting presentation for*** D_{2n}***)*** $r^n = 1$ *means any power of* r *can be reduced so that the power lie between 0 and* $n-1$. *Similarly, any power of* s *can be reduced so that the power is either 0 or 1.* $sr^k = r^{-k}s$ *means every element in the group can be written as* $r^i s^j$ *for some* i, j

Definition. ***(generators and relations)***

1. ***(generators of*** G***)*** *is the set* $S \subset G$ *where every element of* G *can be written as a (finite) product of elements of* S *and their inverses. Denote* $G = \langle S \rangle$ *and say* G *is generated by* S *and* S *generates* G
2. ***(relations in*** G***)*** *any equation in a general group* G *that the generator satisfies*
3. ***(presentation of*** G***)*** *If* $G = \langle S \rangle$ *and* $R_1, R_2, \cdots, R_m$ *are relations in* G *such that any relation among* S *can be deduced from these, the generators and relations are called presentations*
$$G = \langle S \mid R_1, R_2, \cdots, R_m \rangle$$

- *(example)* $\mathbb{Z} = \langle 1 \rangle$
- *(example)* $D_{2n} = \langle r, s \rangle$

3 Symmetric Groups

Definition. ***(Symmetric Group)***

1. ***(symmetric group S_Ω on set Ω)*** *Let Ω be nonempty set, $S_\Omega = \{\sigma : \Omega \to \Omega \mid \sigma \text{ is a bijection}\}$, the set of all permutations of Ω. $(S_\omega, \circ)$ is the symmetric group on Ω.*

2. ***(symmetric group of degree n)*** *If $\Omega = \{1, 2, \cdots, n\}$, S_n is the symmetric group of degree n*

3. *($|S_n| = n!$) (by counting number of possible permutations using the constraint that σ is injective)*

4. ***(cycle)*** *a string of integers representing elements of S_n, which cyclically permutes them. $(a_1\ a_2\ \cdots\ a_m)$ is the permutation sending a_i to a_{i+1}. $1 \leq i \leq m-1$ and sends a_m to a_1*

5. ***(length of cycle)*** *is the number of integers which appear in it*

6. ***(t-cycle)*** *is a cycle with length t*

7. ***(disjoint cycle)*** *A cycle is disjoint if they have no numbers in common*

8. ***(k cycles)*** *Any $\sigma \in S_n$, we can represent σ with k cycles of the form*

$$(a_1\ a_2\ \cdots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \cdots\ a_{m_2})\cdots(a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \cdots\ a_{m_k})$$

9. ***(cycle-decomposition of σ)*** *is the product of k-cycles that representing σ*

- *(convention) 1-cycle not written during cycle-decomposition. This convention ensures that cycle decomposition of $\tau \in S_n$ is exactly the same as cycle decomposition of permutation in S_m where $m > n$, which acts as τ on $\{1, 2, \cdots, n\}$ and fixes elements in $\{n+1, n+2, \cdots, m\}$*

- *(computing inverse) Let $\sigma \in S_n$, cycle decomposition of σ^{-1} can be obtained by writing numbers in each cycle of the cycle decomposition of σ in reverse order*

- *(computing product) by following elements in successive permutations*

- ***(proposition)*** *S_n is non-abelian for $n \geq 3$ (counterexample: $(12)\circ(13) = (1\ 3\ 2)$ but $(13)\circ(12) = (1\ 2\ 3)$)*

-