AM 106: Applied Algebra **Salil Vadhan**

Lecture Notes 5

September 18, 2018

1 Groups

- Reading: Gallian Ch. 2
- **Def:** A *group* is a set G with a binary operation on G (i.e. $\circ : G \times G \to G$) satisfying the following:

  0. (Closure) If $a, b \in G$, then $a \circ b \in G$.
  1. (Associativity) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
  2. (Identity) There is an element $e \in G$ (called the *identity*) s.t. $e \circ a = a \circ e = a$ for all $a \in G$.
  3. (Inverses) For all $a \in G$, there is an element $b \in G$ (called the *inverse* of a) such that $a \circ b = b \circ a = e$.

- **Note:** We don't require that $a \circ b = b \circ a$. A group that satisfies this for all $a, b \in G$ is called *Abelian* or *commutative*.

2 Examples

- See table on next page. We give some more details on some of the examples here.
- Group of Units modulo n (Gallian Example 2.11)
  - $\{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ under multiplication modulo n.
  - Gallian notation: $U(n)$.
  - Our notation (more standard): $\mathbb{Z}_n^*$.
  - Inverse of a:
    - Why does it exist?
    - How to compute it?
- $n \times n$ matrices, with real entries:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & & a_{nn} \end{pmatrix}.$$

Notation	Set	Operation	Closure?	Associative?	Identity?	Inverses?	Group?	Commutative?
	$\mathbb{Z}$	$+$						
	$\mathbb{R}$	$+$						
	$\mathbb{N}$	$+$						
	odd integers	$+$						
	even integers	$+$						
	$\mathbb{Z}$	max						
	$\mathbb{Z}$	$-$						
	$\mathbb{Z}$	$\times$						
	$\mathbb{Q}$	$\times$						
$\mathbb{Q}^*$	$\mathbb{Q} \setminus \{0\}$	$\times$						
	$\mathbb{Q}^+$	$\times$						
	$\mathbb{R}^n$	$+$ componentwise						
	$\mathbb{R}^n \setminus \{(0, \ldots, 0)\}$	$\times$ componentwise						
$\mathbb{Z}_n$	$\{0, \ldots, n-1\}$ or $\{[0]_n, \ldots, [n-1]_n\}$	$+$ mod n $[a]_n + [b]_n = [a+b]_n$						
	$\{1, \ldots, n\}$	$\times$ mod n						
$\mathbb{Z}_n^*$, $U(n)$	$\{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$	$\times$ mod n						
$M_n(\mathbb{R})$	$n \times n$ real matrices	$+$ entrywise						
	$n \times n$ real matrices	matrix mult.						
$GL_n(\mathbb{R})$	$n \times n$ invertible real matrices	matrix mult.						
S_n	permutations $[n] \mapsto [n]$	composition						
$Sym(S)$	permutations $S \mapsto S$	composition						
D_n	symmetries of regular n-gon	composition						

  - Defines a linear transformation from $\mathbb{R}^n \to \mathbb{R}^n$ by $Av = w$, where $w_i = \sum_j a_{ij}v_j = \langle r_i, v\rangle$ and r_i is i'th row of A.
  - $A + B$ has (i,j)'th entry $a_{ij} + b_{ij}$.
  - AB has (i,j)'th entry $\sum_k a_{ik}b_{kj} = \langle r_i, c_j\rangle$ if r_i is i'th row of A and c_j is j'th column of B.

3 Basic Properties of Groups

- **Thm 2.1 (Identity is Unique):** In every group G, there is only one identity element.
  Proof:

- **Thm 2.3 (Inverses are Unique):** For every group G and every element $a \in G$, there is only one inverse of a in G (typically denoted a^{-1}).
  Proof: similar to uniqueness of the identity.
- Multiplicative Notation for Groups
  - Group operation: $a \cdot b$ or just ab
  - Identity: 1 or e
  - Inverse of a: a^{-1}
  - a multiplied n times: a^n
- Additive Notation for Groups
  - Group operation: $a + b$
  - Identity: 0
  - Inverse of a: $-a$
  - a added n times: na
  - Only used for abelian groups!
- **Thm 2.2 (Left-cancellation and Right-cancellation):** In a group:
  1. $ab = ac \Rightarrow b = c$.
  2. $ba = ca \Rightarrow b = c$.
- **Thm 2.4 (Shoes-Socks Property):** In a group, $(ab)^{-1} = b^{-1}a^{-1}$.
  Proof: omitted