

Lecture 8

A little bit of “fun” math...
Read: Chapter 7 (and 8)

1

Finite Algebraic Structures

- Groups
 - Abelian
 - Cyclic
 - Generator
 - Group order
- Rings
- Fields
- Subgroups
- Euclidian Algorithm
- CRT (Chinese Remainder Theorem)

2

GROUPS

DEFINITION: A nonempty set G and *operator* \otimes , (G, \otimes) is a *group* if:

- **CLOSURE:** for all x, y in G :
 $(x \otimes y)$ is also in G
- **ASSOCIATIVITY:** for all x, y, z in G :
 $(x \otimes y) \otimes z = x \otimes (y \otimes z)$
- **IDENTITY:** there exists *identity element* I in G , such that, for all x in G :
 $I \otimes x = x$ and $x \otimes I = x$
- **INVERSE:** for all x in G , there exist *inverse element* x^{-1} in G , such that:
 $x^{-1} \otimes x = I = x \otimes x^{-1}$

DEFINITION: A group (G, \otimes) is **ABELIAN** if:

- **COMMUTATIVITY:** for all x, y in G :
 $x \otimes y = y \otimes x$

3

Groups (contd)

DEFINITION: An element g in G is a *group generator* of group (G, \otimes) if: for all x in G , **there exists** $i \geq 0$, such that:

$$x = g^i = g \otimes g \otimes g \otimes \dots \otimes g \text{ (i times)}$$

This means every element of the group can be generated by g using \otimes .

In other words, $G = \langle g \rangle$

DEFINITION: A group (G, \otimes) is *cyclic* if a group generator exists!

DEFINITION: Group *order* of a group (G, \otimes) is *the size of set G* , i.e., $|G|$ or $\#\{G\}$ or $\text{ord}(G)$

DEFINITION: Group (G, \otimes) is **finite** if $\text{ord}(G)$ is finite.

4

Rings and Fields

DEFINITION: A structure $(R, +, *)$ is a **ring** if $(R, +)$ is an Abelian group (usually with identity element denoted by 0) and the following properties hold:

***CLOSURE:** for all x, y in R , $(x * y)$ in R

***ASSOCIATIVITY:** for all x, y, z in R , $(x * y) * z = x * (y * z)$

***IDENTITY:** there exists $1 \neq 0$ in R , s.t., for all x in R , $1 * x = x$

***DISTRIBUTION:** for all x, y, z in R , $(x + y) * z = x * z + y * z$

In other words $(R, +)$ is an Abelian group with identity element 0 and $(R, *)$ is a **monoid** with identity element $1 \neq 0$.

The ring is *commutative ring* if

***COMMUTATIVITY:** for all x, y in R , $x * y = y * x$

5

Rings and Fields

DEFINITION: A structure $(F, +, *)$ is a **field** if $(F, +, *)$ is a commutative ring and:

***INVERSE:** all *non-zero* x in R , have multiplicative inverse.

i.e. there exists an **inverse element** x^{-1} in R , such that: $x * x^{-1} = 1$.

6

Example: Integers under addition

$$G = \mathbf{Z} = \text{integers} = \{ \dots -3, -2, -1, 0, 1, 2 \dots \}$$

the group operator is "+", ordinary addition

- ❑ the integers are closed under addition
- ❑ the identity is 0
- ❑ the inverse of x is $-x$
- ❑ the integers are associative
- ❑ the integers are commutative (so the group is Abelian)

7

Non-zero rationals under multiplication

$$G = \mathbf{Q} - \{0\} = \{a/b\} \text{ where } a, b \text{ in } \mathbf{Z}^*$$

the group operator is "*", ordinary multiplication

- If $a/b, c/d$ in $\mathbf{Q} - \{0\}$, then: $a/b * c/d = (ac/bd)$ in $\mathbf{Q} - \{0\}$
- the identity is 1
- the inverse of a/b is b/a
- the rationals are associative
- the rationals are commutative (so the group is Abelian)

8

Non-zero reals under multiplication

$$G = \mathbb{R} - \{0\}$$

the group operator is "*", ordinary multiplication

- If a, b in $\mathbb{R} - \{0\}$, then $a*b$ in $\mathbb{R} - \{0\}$
- the identity is 1
- the inverse of a is $1/a$
- the reals are associative
- the reals are commutative (so the group is Abelian)

9

Integers mod N under addition

$$G = \mathbb{Z}_N^+ = \text{integers mod } N = \{0 \dots N-1\}$$

the group operator is "+", modular addition

- the integers modulo N are closed under addition
- the identity is 0
- the inverse of x is $-x (=N-x)$
- addition is associative
- addition is commutative (so the group is **Abelian**)

10

Integers mod p (prime) under multiplication

$$G = \mathbb{Z}_p^* = \text{non-zero integers mod } p = \{1 \dots p-1\}$$

the group operator is "*", modular multiplication

- integers mod p are closed under *:
because if $\text{GCD}(x, p) = 1$ and $\text{GCD}(y, p) = 1$
then $\text{GCD}(xy, p) = 1$
(Note that x is in \mathbb{Z}_p^* iff $\text{GCD}(x, p) = 1$)
- the identity is 1
- the inverse of x is u s.t. $ux \pmod p = 1$
 - u can be found either by extended Euclidian algorithm
 $ux + vp = 1 = \text{GCD}(x, p)$
 - Or using Fermat's little theorem $x^{p-1} = 1 \pmod p$, $u = x^{-1} = x^{p-2}$
- * is associative
- * is commutative (so the group is Abelian)

11

Positive Integers under Exponentiation?

$$G = \{0, 1, 2, 3, \dots\}$$

the group operator is "^", exponentiation

- closed under exponentiation
- the (one-sided?) identity is 1, $x^1 = x$
- the (right-side only) inverse of x is always 0, $x^0 = 1$
- the integers are NOT commutative,
 $x^y \neq y^x$ (non-Abelian)
- the integers are NOT associative,
 $(x^y)^z \neq x^{(y^z)}$

12

Z_N^* : positive integers mod N relatively prime to N

$G = Z_N^*$ = non-zero integers mod N = {1, ..., x, ..., n-1} such that $\gcd(x, N) = 1$

Group operator is "*", modular multiplication

Group order $\text{ord}(Z_N^*)$ = number of integers relatively prime to N denoted by $\phi(N)$

- integers mod N are closed under multiplication:
if $\text{GCD}(x, N) = 1$ and $\text{GCD}(y, N) = 1$, $\text{GCD}(x*y, N) = 1$
- identity is 1
- inverse of x is from Euclid's algorithm:
 $ux + vN = 1 \pmod{N} = \text{GCD}(x, N)$
so, $x^{-1} = u (= x^{\phi(N)-1})$
- multiplication is associative
- multiplication is commutative (so the group is Abelian)

13

Non-Abelian Groups: 2x2 non-singular real matrices under matrix mult-n

$$GL(2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, ad-bc \neq 0 \right\}$$

- if A and B are non-singular, so is AB
- the identity is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} / (ad-bc)$$

- matrix multiplication is associative
- matrix multiplication is **not** commutative

14

Non-Abelian Groups (contd)

$$\begin{bmatrix} 2 & 5 \\ 10 & 30 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & -0.5 \\ -1 & 0.2 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 5 \\ 10 & 30 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 20 \\ 60 & 110 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 10 & 30 \end{bmatrix} = \begin{bmatrix} 56 & 165 \\ 22 & 65 \end{bmatrix}$$

15

Subgroups

DEFINITION: $(H, @)$ is a **subgroup** of $(G, @)$ if:

- H is a subset of G
- $(H, @)$ is a group

16

Subgroup example

Let $(G, *)$, $G = Z_7^* = \{1, 2, 3, 4, 5, 6\}$

Let $H = \{1, 2, 4\} \pmod{7}$

Note:

1. H is closed under multiplication mod 7
2. 1 is still the identity
3. 1 is 1's inverse, 2 and 4 are inverses of each other
4. associativity holds
5. commutativity holds (H is Abelian)

17

Subgroup example

Let $(G, *)$, $G = \mathbb{R} - \{0\}$ = non-zero reals

Let $(H, *)$, $H = \mathbb{Q} - \{0\}$ = non-zero rationals

H is a subset of G and both G and H are groups in their own right

18

Order of an element

Let x be an element of a (multiplicative) finite integer group G . The *order* of x is the smallest positive number k such that $x^k = 1$

Notation: $\text{ord}(x)$

19

Order of an element

Example: Z_7^* : multiplicative group mod 7

Note that: $Z_7^* = Z_7$

$\text{ord}(1) = 1$ because $1^1 = 1$

$\text{ord}(2) = 3$ because $2^3 = 8 = 1$

$\text{ord}(3) = 6$ because $3^6 = 9^3 = 2^3 = 1$

$\text{ord}(4) = 3$ because $4^3 = 64 = 1$

$\text{ord}(5) = 6$ because $5^6 = 25^3 = 4^3 = 1$

$\text{ord}(6) = 2$ because $6^2 = 36 = 1$

20

Theorem (Lagrange)

$\Phi(n)$ - order of G_n^*
largest order of any element!

order of g : smallest
integer m such that
 $g^m \equiv 1 \pmod n$

Theorem (Lagrange): Let G be a multiplicative group of order n . For any g in G , $\text{ord}(g)$ divides $\text{ord}(G)$.

COROLLARY 1:

$$b^{\Phi(n)} \equiv 1 \pmod n \quad \forall b \in Z_n^*$$

because: $\Phi(n) = \text{ord}(Z_n^*)$

$$\text{ord}(b) = \text{ord}(Z_n^*) / k = \Phi(n) / k$$

$$\text{thus: } b^{\Phi(n)} = b^{\Phi(n)/k} = 1^{1/k} = 1$$

21

COROLLARY 2:

if p is prime then

$$\forall b \in Z_p^*$$

$$1) \quad b^p \equiv b \pmod p$$

and

$$2) \quad \exists a \in Z_p \ni \text{ord}(a) = p - 1$$

a - primitive element

Example: in Z_{13}^*
primitive elements are:
 $\{2, 6, 7, 11\}$

22

Euclidian Algorithm

Purpose: compute GCD (x,y)

Recall that:

b^{-1} - multiplicative inverse of b ,

$$b * b^{-1} \equiv 1 \pmod n$$

$$\forall b \in \mathbb{Z}_n \exists b^{-1} \Leftrightarrow \gcd(b, n) = 1$$



$$\text{Euclidian}(n, b) = 1 \Rightarrow \exists b^{-1}$$

23

Euclidian Algorithm (contd)

init: $r_0 = x \quad r_1 = y$

$$q_1 = \lfloor r_0 / r_1 \rfloor \quad r_2 = r_0 \bmod r_1$$

... = ...

$$q_i = \lfloor r_{i-1} / r_i \rfloor \quad r_{i+1} = r_{i-1} \bmod r_i$$

... = ...

$$q_{m-1} = \lfloor r_{m-1} / r_i \rfloor \quad r_m = r_{m-2} \bmod r_{m-1}$$

($r_m == 0$)

OUTPUT r_{m-1}

Example: 24,15

1. 1 9
2. 1 6
3. 1 3
4. 2 0

Example: 23, 14

1. 1 9
2. 1 5
3. 1 4
4. 1 1
5. 4 0

24

Extended Euclidian Algorithm

Purpose: compute GCD(x,y) and inverse of y (if it exists)

$$\text{init: } r_0 = x \quad r_1 = y \quad t_0 = 0 \quad t_1 = 1$$

$$q_1 = \lfloor r_0 / r_1 \rfloor \quad r_2 = r_0 \bmod r_1 \quad t_2 = t_0 - t_1 q_1 \bmod r_0$$

... = ...

$$q_i = \lfloor r_{i-1} / r_i \rfloor \quad r_{i+1} = r_{i-1} \bmod r_i \quad t_i = t_{i-2} - q_{i-1} t_{i-1} \bmod r_0$$

... = ...

$$q_{m-1} = \lfloor r_{m-1} / r_m \rfloor \quad r_m = r_{m-2} \bmod r_{m-1} \quad t_m = t_{m-2} - q_{m-1} t_{m-1} \bmod r_0$$

if ($r_m = 1$) OUTPUT t_m else OUTPUT "no inverse"

25

Extended Euclidian Algorithm (contd)

Theorem: $r_i = t_i r_1 \quad (i > 1) \longrightarrow t_m r_1 = 1$

$$q_i = \lfloor r_{i-1} / r_i \rfloor \quad r_{i+1} = r_{i-1} \bmod r_i \quad t_i = t_{i-2} - q_{i-1} t_{i-1} \bmod r_0$$

Example: x=87 y=11

<u>I</u>	<u>R</u>	<u>T</u>	<u>Q</u>
0	87	0	--
1	11	1	7
2	10	80	1
3	1	8	--

26

Extended Euclidian Algorithm (contd)

Example: $x=93$ $y=87$

$$q_i = \lfloor r_{i-1} / r_i \rfloor \quad r_{i+1} = r_{i-1} \bmod r_i \quad t_i = t_{i-2} - q_{i-1} t_{i-1} \bmod r_0$$

I	R	T	Q
0	93	0	--
1	87	1	1
2	6	92	14
3	3	15	2
4	0	62	--

No Inverse Exists

27

Chinese Remainder Theorem (CRT)

The following system of n modular equations (congruences)

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ &\dots \\ x &\equiv a_n \bmod m_n \end{aligned} \quad (\text{all } m_i\text{-s relatively prime}).$$

Has a unique solution:

$$x = \sum_{i=1}^n a_i \left(\frac{M}{m_i} \right) y_i \bmod M$$

where :

$$M = m_1 * \dots * m_n$$

$$y_i = \left(\frac{M}{m_i} \right)^{-1} \bmod m_i$$

28

CRT Example

$$\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}$$

$$x = [5(M/m_1)y_1 + 3(M/m_2)y_2] \pmod{M}$$

$$M = 77$$

$$M/m_1 = 11$$

$$M/m_2 = 7$$

$$y_1 = 11^{-1} \pmod{7} = 4^{-1} \pmod{7} = 2$$

$$y_2 = 7^{-1} \pmod{11} = 8$$

$$x = (5 \cdot 11 \cdot 2 + 3 \cdot 7 \cdot 8) \pmod{77} = 47$$

29