Lecture 7

Algebraic Structures (Groups, Rings, Fields) and Some Basic Number Theory

Read: Chapter 7 and 8 in KPS

[lecture slides are adapted from previous slides by Prof. Gene Tsudik]

Finite Algebraic Structures

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

GROUPs

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

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

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

- COMMUTATIVITY: for all x, y in G:
- x @ y = y @ x

Groups (contd)

DEFINITION: An element g **in** G is a ***group generator*** of group (G,@) if:

for all x **in** G, **there exists $i \geq 0$,** such that:

$$x = g^i = g \; @ \; g \; @ \; g \; @ \; \ldots \; @ \; g \quad (i \text{ times})$$

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

In other words, G=<g>

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

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

DEFINITION: Group (G,@) is **finite** if ord(G) is finite.

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 ≠ 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≠0. A *Monoid* is a set with a single associative binary operation and an identity element.

The Ring is *commutative Ring* if

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

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:
$x * x^{-1} = 1$.

Example: Integers Under Addition

G = **Z** = integers = { … -3, -2, -1, 0 , 1 , 2 …}

the group operator is “+”, ordinary addition

- integers are closed under addition
- identity element with respect to addition is 0 (x+0=x)
- inverse of x is -x (because x + (-x) = 0)
- addition of integers is associative
- addition of integers is commutative (the group is **Abelian**)

Non-Zero Rationals under Multiplication

G = **Q** - {0} = {a/b} where a, b in **Z***

the group operator is "*", ordinary multiplication

- if a/b, c/d in Q-{0}, then: a/b * c/d = (ac/bd) in Q-{0}
- the identity element is 1
- the inverse of a/b is b/a
- multiplication of rationals is associative
- multiplication of rationals is commutative (the group is **Abelian**)

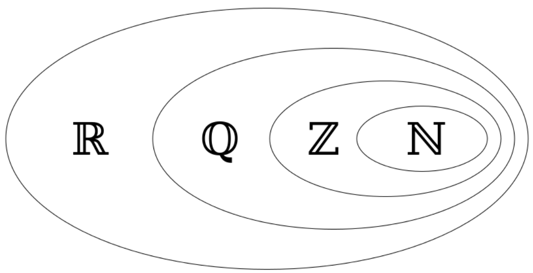
Non-Zero Reals under Multiplication

G = **R** - {0}

the group operator is "*", ordinary multiplication

- if a, b in R - {0}, then a*b in R-{0}
- the identity is 1
- the inverse of a is 1/a
- multiplication of reals is associative
- multiplication of reals is commutative
  (the group is **Abelian**)

Remember:



Positive Integers under Exponentiation?

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

the group operator is "^", exponentiation

- closed under exponentiation
- the identity is 1, x^1=x
- the inverse of x is always 0, x^0=1
- exponentiation of integers is NOT commutative,

x^y ≠ y^x (non-Abelian)

- exponentiation of integers is NOT associative,

(x^y)^z ≠ x^(y^z)

Integers mod N Under Addition

G = $\mathbf{Z}^{+}_{\mathbf{N}}$ = positive integers mod N = {0 ... N-1}

the group operator is "+", modular addition

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

Integers mod(p) (where p is Prime) under Multiplication

$G = Z^*_p$ non-zero integers mod p = {1 … p-1}

the group operator is "*", modular multiplication

- integers mod p are closed under the * operator:
- because if GCD(x, p) =1 and GCD(y, p) = 1 (GCD = Greatest Common Divisor)
- then GCD(xy, p) = 1
- Note that x is in Z^*_P iff GCD(x, p)=1
- the identity is 1
- the inverse of x is u such that ux (mod p)=1
  - u can be found either by Extended Euclidean Algorithm
  - ux + vp = GCD(x, p) = 1
  - or by 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**)

Z^*_N : Non-zero Integers mod(N) Relatively Prime to N

G = $\mathbf{Z^*_N}$

non-zero integers mod N = {1 …, x, … n-1} such that GCD(x, N)=1

- Group operator is "*", modular multiplication
- Group order ord(Z^*_N) = number of integers **relatively prime (or co-prime)** to N denoted by **phi(N), or Φ (N)**

- integers mod N are closed under multiplication:

  if GCD(x, N) =1 and GCD(y,N) = 1, GCD(x*y,N) = 1
- identity is 1
- inverse of x is from Euclidean algorithm:

ux + vN = 1 (mod N) = GCD(x,N)

so, $x^{-1} = u$ (= $x^{\text{phi(N)-1}}$)

- multiplication is associative
- multiplication is commutative (so the group is **Abelian**)

Subgroups

<u>DEFINITION</u>: (H,@) is a **subgroup** of (G,@) if:

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

Subgroup Example

Let (G,*), G = Z^*_7 = {1, 2, 3, 4, 5, 6}
Let H = {1, 2, 4} (mod 7)

Note that:
- H is closed under multiplication mod 7
- 1 is still the identity
- 1 is 1's inverse, 2 and 4 are inverses of each other
- Associativity holds
- Commutativity holds (H is **Abelian**)

Subgroup Example

Let (G,*), G = R-{0} = non-zero reals
Let (H,*), Q-{0} = non-zero rationals

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

Order of a Group 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 $\mathbf{x}^k = 1$

Notation: ord(x)

Order of an Element

Example: Z^*_7: multiplicative group mod 7

Note that: $Z^*_7 = Z_7$

ord(1) = 1 because $1^1 = 1$
ord(2) = 3 because $2^3 = 8 = 1$
ord(3) = 6 because $3^6 = 9^3 = 2^3 = 1$
ord(4) = 3 because $4^3 = 64 = 1$
ord(5) = 6 because $5^6 = 25^3 = 4^3 = 1$
ord(6) = 2 because $6^2 = 36 = 1$

Theorem (Lagrange)

$\Phi(n)$ - order of G_n^*

largest order of any element!

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

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

COROLLARY 1:

$$b^{\Phi(n)} \equiv 1 \bmod n \; \forall \, b \in Z_n^*$$

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

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

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

COROLLARY 2:

if p is prime then

$\forall\, b \in Z_p^{\,*}$

1) $b^p \equiv b \bmod p$

and

2) $\exists\, a \in Z_p \ni ord(a) = p - 1$

a – primitive element

Example: in Z^*_{13} primitive elements are: {2, 6, 7, 11}

Euclidean Algorithm

Purpose: compute GCD(x,y)
GCD = Greatest Common Divisor

Recall that:

$$b^{-1} - \textit{multiplicative inverse}\text{ of } b,$$

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

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

$$\Downarrow$$

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

Euclidean Algorithm (contd)

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

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

$$\ldots = \ldots$$

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

$$\ldots = \ldots$$

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

$$(r_m == 0)?$$

$$OUTPUT \quad r_{m-1}$$

Example: x=24, y=15

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

Example: x=23, y=14

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

Extended Euclidean Algorithm

<u>Purpose:</u> compute GCD(x,y) and inverse of y (if it exists)

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

$$q_1 = \lfloor r_0 / r_1 \rfloor \qquad r_2 = r_0 \; mod \; r_1 \qquad t_1 = 1$$

$$\ldots = \ldots$$

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

$$\ldots = \ldots$$

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

$$if \, (r_m = 1) \;\; OUTPUT \;\; t_m \;\; else \; if \, (rm = 0) \;\; OUTPUT \; "no \; inverse"$$

Extended Euclidean Algorithm (contd)

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

Example: x=87 y=11

I	R	T	Q
0	87	0	--
1	11	1	7
2	10	80	1
3	1	8	--

Extended Euclidean Algorithm (contd)

Example: x=93 y=87

$q_i = \lfloor r_{i-1} / r_i \rfloor \qquad r_{i+1} = r_{i-1} \, mod \; r_i \qquad t_i = t_{i-2} - q_{i-1} t_{i-1} \; mod \; r_0$

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

Chinese Remainder Theorem (CRT)

The following system of ***n*** modular equations (congruences)

$$x \equiv a_1 \ mod \ m_1$$
$$\ldots$$
$$x \equiv a_n \ mod \ m_n$$

(all $\boldsymbol{m_i}$-s relatively prime).

Has a unique solution:

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

$$\text{where}:$$

$$M = m_1 * \ldots * m_n$$

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

CRT Example

$$\begin{pmatrix} x \equiv 5 \ \ mod\,7 \\ x \equiv 3 \ \ mod\,11 \end{pmatrix}$$

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

$$M = 77$$

$$M/m_1 = 11$$

$$M/m_2 = 7$$

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

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

$$x = (5*11*2 + 3*7*8)mod\ 77 = 47$$