Lecture 6

Groups, Rings, Fields and Some Basic Number Theory

Read: Chapter 7 and 8 in KPS
Finite Algebraic Structures

• Groups
  • Abelian
  • Cyclic
  • Generator
  • Group Order
• Rings
• Fields
• Subgroups
• Euclidian Algorithm
• CRT (Chinese Remainder Theorem)
GROUPS

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

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

DEFINITION: A group $(G, \oplus)$ is ABELIAN if:

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

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

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

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

**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 $\operatorname{ord}(G)$

**DEFINITION:** Group $(G, @)$ is finite if $\operatorname{ord}(G)$ 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 \(1 \neq 0 \in R\), 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 \(1 \neq 0\). 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: \( x \times x^{-1} = 1 \).
Example: Integers Under Addition

G = \mathbb{Z} = \text{integers} = \{ \ldots -3, -2, -1, 0, 1, 2 \ldots \}

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

\[ G = \mathbb{Q} - \{0\} = \{a/b\} \text{ where } a, b \in \mathbb{Z}^* \]

the group operator is “\(*\)”, ordinary multiplication

- if \(a/b, c/d\) in \(\mathbb{Q}-\{0\}\), then: \(a/b \times c/d = (ac/bd)\) in \(\mathbb{Q}-\{0\}\)
- 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 \textbf{Abelian})
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 \(1/a\)
- multiplication of reals is associative
- multiplication of reals is commutative
  (the group is Abelian)
Integers mod N Under Addition

\[ G = \mathbb{Z}_N^+ = \text{integers mod N} = \{0 \ldots N-1\} \]

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

\[ G = \mathbb{Z}_p^* \] non-zero integers mod p = \{1 \ldots p-1\}

the group operator is “*”, modular multiplication

- integers mod p are closed under “*” (where GCD = Greatest Common Divisor):
  
  because if GCD(x, p) = 1 and GCD(y, p) = 1
  
  then GCD(xy, p) = 1
  
  (Note that x is in \( \mathbb{Z}_p^* \) iff GCD(x, p)=1)

- the identity is 1

- the inverse of x is u s.t. ux (mod 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)
Positive Integers under Exponentiation?

\[ G = \{0, 1, 2, 3\ldots\} \]

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, \( x^0 = 1 \)
- exponentiation of integers is NOT commutative, \( x^y \neq y^x \) (non-Abelian)
- exponentiation of integers is NOT associative, \( (x^y)^z \neq x^{y^z} \)
$\mathbb{Z}_N^*$: Positive Integers mod(N) Relatively Prime to N

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

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

- Group operator is “*”, modular multiplication
- Group order ord($\mathbb{Z}_N^*$) = number of integers \textbf{relatively prime} to N denoted by $\text{phi}(N)$
- 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 Euclid’s algorithm:
  
  $ux + vN = 1 \pmod{N} = \text{GCD}(x,N)$

  so, $x^{-1} = u = x^{\text{phi}(N)-1}$
- multiplication is associative
- multiplication is commutative (so the group is \textbf{Abelian})
Non-Abelian Group Example: 2x2 Non-Singular Real Matrices under Matrix Multiplication

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

- if A and B are non-singular, so is AB
- the identity is \( I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \)
- Inverse:
  \[ \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} / (\text{ad-bc}) \]

- matrix multiplication is associative
- matrix multiplication is \textbf{not} commutative

Recall: a square matrix is non-singular if its determinant is non-zero. A non-singular matrix has an inverse.
Non-Abelian Groups (contd)

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

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

\[
\begin{bmatrix}
3 & 5 \\
1 & 2
\end{bmatrix} \begin{bmatrix}
2 & 5 \\
10 & 30
\end{bmatrix} =
\begin{bmatrix}
56 & 165 \\
22 & 65
\end{bmatrix}
\]
**Definition:** $(H, @)$ is a **subgroup** of $(G, @)$ if:

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

Let \((G, \cdot), G = \mathbb{Z}_{\cdot}^* = \{1, 2, 3, 4, 5, 6\}\)
Let \(H = \{1, 2, 4\} \text{ (mod 7)}\)

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 \((G, \ast)\), \(G = \mathbb{R}\setminus\{0\} = \text{non-zero reals}\)
Let \((H, \ast)\), \(Q\setminus\{0\} = \text{non-zero rationals}\)

\(H\) 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 $x^k = 1$

Notation: $\text{ord}(x)$
Order of an Element

Example: $\mathbb{Z}^*_7$: multiplicative group mod 7

Note that: $\mathbb{Z}^*_7=\mathbb{Z}_7$

$$\text{ord}(1) = 1 \text{ because } 1^1 = 1$$
$$\text{ord}(2) = 3 \text{ because } 2^3 = 8 = 1$$
$$\text{ord}(3) = 6 \text{ because } 3^6 = 9^3 = 2^3 = 1$$
$$\text{ord}(4) = 3 \text{ because } 4^3 = 64 = 1$$
$$\text{ord}(5) = 6 \text{ because } 5^6 = 25^3 = 4^3 = 1$$
$$\text{ord}(6) = 2 \text{ because } 6^2 = 36 = 1$$
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:**

$$b^{\Phi(n)} \equiv 1 \mod n \quad \forall b \in \mathbb{Z}_n^*$$

because: $\Phi(n) = \text{ord}(\mathbb{Z}_n^*)$

$$\text{ord}(b) = \frac{\text{ord}(\mathbb{Z}_n^*)}{k} = \frac{\Phi(n)}{k}$$

thus: $b^{\Phi(n)} = b^{\Phi(n)/k} = 1^{1/k} = 1$
COROLLARY 2:
if \( p \) is prime then
\[ \forall b \in \mathbb{Z}_p^* \]
1) \( b^p \equiv b \mod p \)
and
2) \( \exists a \in \mathbb{Z}_p^* \exists \text{ord}(a) = p - 1 \)
a \(-\) primitive element

Example: in \( \mathbb{Z}_{13}^* \)
primitive elements are:
\{2, 6, 7, 11\}
Euclidian Algorithm

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

Recall that:

\[ b^{-1} - \text{multiplicative inverse of } b, \]
\[ b \cdot b^{-1} \equiv 1 \mod n \]
\[ \forall b \in \mathbb{Z}_n \; \exists b^{-1} \iff \gcd(b, n) = 1 \]

\[ \text{Euclidian } (n, b) = 1 \Rightarrow \exists b^{-1} \]
Euclidian Algorithm (contd)

**init**: \( r_0 = x \) \( r_1 = y \)

\[ q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor \quad r_2 = r_0 \mod r_1 \]

... = ...

\[ q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \quad r_{i+1} = r_{i-1} \mod r_i \]

... = ...

\[ q_{m-1} = \left\lfloor \frac{r_{m-2}}{r_{m-1}} \right\rfloor \quad r_m = r_{m-2} \mod r_{m-1} \]

\((r_m == 0)\)?

**OUTPUT** \( r_{m-1} \)

---

**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 Euclidian Algorithm

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

\[
\begin{align*}
\text{init:} & \quad r_0 = x \quad r_1 = y \quad t_0 = 0 \quad t_1 = 1 \\
q_1 &= \left\lfloor \frac{r_0}{r_1} \right\rfloor \quad r_2 = r_0 \mod r_1 \quad t_1 = 1 \\
\ldots &= \ldots \\
q_i &= \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \quad r_{i+1} = r_{i-1} \mod r_i \quad t_i = t_{i-2} - q_{i-1} t_{i-1} \mod r_0 \\
\ldots &= \ldots \\
q_{m-1} &= \left\lfloor \frac{r_{m-2}}{r_{m-1}} \right\rfloor \quad r_m = r_{m-2} \mod r_{m-1} \quad t_m = t_{m-2} - q_{m-1} t_{m-1} \mod r_0 \\
\text{if } (r_m = 1) \quad \text{OUTPUT } t_m \quad \text{else if } (r_m = 0) \quad \text{OUTPUT "no inverse"}
\end{align*}
\]
Extended Euclidian Algorithm (contd)

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

\[
q_i = \left[ \frac{r_{i-1}}{r_i} \right] \quad r_{i+1} = r_{i-1} \mod r_i \quad t_i = t_{i-2} - q_{i-1} t_{i-1} \mod r_0
\]

Example: \( x=87 \) \( y=11 \)

<table>
<thead>
<tr>
<th>I</th>
<th>R</th>
<th>T</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>87</td>
<td>0</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>80</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>8</td>
<td>---</td>
</tr>
</tbody>
</table>
Extended Euclidian Algorithm (contd)

Example: \( x=93 \ y=87 \)

\[
q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \quad r_{i+1} = r_{i-1} \mod r_i \quad t_i = t_{i-2} - q_{i-1} t_{i-1} \mod r_0
\]

<table>
<thead>
<tr>
<th>I</th>
<th>R</th>
<th>T</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>93</td>
<td>0</td>
<td>--</td>
</tr>
<tr>
<td>1</td>
<td>87</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>92</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>62</td>
<td>--</td>
</tr>
</tbody>
</table>
Chinese Remainder Theorem (CRT)

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

$$\begin{align*}
x &\equiv a_1 \mod m_1 \\
&\vdots \\
x &\equiv a_n \mod m_n
\end{align*}$$

(All $m_i$-s relatively prime).

Has a unique solution:

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

Where:

$$M = m_1 \ast \ldots \ast m_n$$

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

\[
\begin{align*}
    x &\equiv 5 \ mod \ 7 \\
    x &\equiv 3 \ mod \ 11
\end{align*}
\]

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

\[
M = 77
\]

\[
M / m_1 = 11
\]

\[
M / m_2 = 7
\]

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

\[
y_2 = 7^{-1} \mod 11 = 8
\]

\[
x = (5 \times 11 \times 2 + 3 \times 7 \times 8) \mod 77 = 47
\]