ECE 297:11 Lecture 17

Mathematical background
Groups, rings, and fields

Evariste Galois (1811-1832)

Studied the problem of finding algebraic solutions for the general equation of the degree ≥ 5, e.g.,

\[ f(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \]

Answered definitely the question which specific equations of a given degree have algebraic solutions

On the way, he developed \textbf{group theory},

one of the most important branches of modern mathematics.
**Evariste Galois (1811-1832)**

1829  
Galois submits his results for the first time to the French Academy of Sciences  
*Reviewer 1*  
Augustin-Louis Cauchy forgot or lost the communication

1930  
Galois submits the revised version of his manuscript, hoping to enter the competition for the Grand Prize in mathematics  
*Reviewer 2*  
Joseph Fourier – died shortly after receiving the manuscript

1931  
Third submission to the French Academy of Sciences  
*Reviewer 3*  
Simeon-Denis Poisson – does not understand the manuscript and rejects it.

---

**Evariste Galois (1811-1832)**

May 1832  
Galois provoked into a duel  

The night before the duel he writes a letter to his friend containing the summary of his discoveries. The letter ends with a plea:  
“Eventually there will be, I hope, some people who will find it profitable to decipher this mess.”

May 30, 1832  
Galois is grievously wounded in the duel and dies in the hospital the following day.

1843  
Galois manuscript rediscovered by Joseph Liouville

1846  
Galois manuscript published for the first time in a mathematical journal
Group

Example 1

(\(\mathbb{Z}\) - set of integers, + addition) is an abelian group

i) + is associative \(\text{e.g., } (5+7)+13 = 5+(7+13)\)

ii) Identity element = 0 \(\text{a+0 = 0+a = a}\)

iii) Inverse of a = -a \(\text{e.g., } 7 + (-7) = 0\)

iv) + is commutative \(\text{e.g., } 5 + 8 = 8 + 5\)

Group

Example 2

(\(\mathbb{Z}\) - set of integers, \(\cdot\) multiplication) is NOT a group

i) \(\cdot\) is associative \(\text{e.g., } (5 \cdot 7) \cdot 13 = 5 \cdot (7 \cdot 13)\)

ii) Identity element = 1 \(\text{a \cdot 1 = 1 \cdot a = a}\)

iii) No inverse of \(a\) for any \(a \neq 1\) or -1

\(\text{e.g., there is no integer } x, \text{ such that } 5 \cdot x = 1\)

iv) \(\cdot\) is commutative \(\text{e.g., } 5 \cdot 8 = 8 \cdot 5\)


**Group**

**Example 3**

$(\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, \; + \mod n : \text{addition modulo } n)$

is an abelian finite group of order $n$

i) $+ \mod n$ is associative

\[ \text{e.g., } ((5+7) \mod 16) + 13 \mod 16 = (5+(7 + 13 \mod 16)) \mod 16 \]

ii) Identity element = 0

\[ (0+a) \mod n = (a+0) \mod n = a \]

iii) Inverse of $a = 0$ for $a=0$

\[ \text{e.g., } 7 + (16-7) = \]

\[ n-a \quad \text{otherwise} \]

\[ 7 + 9 \mod 16 = 0 \]

iv) $+ \mod n$ is commutative

\[ \text{e.g., } 5 + 8 \mod 16 = 8 + 5 \mod 16 \]

**Group**

**Example 4**

$(\mathbb{Z}_n-\{0\} = \{1, 2, \ldots, n-1\}, \cdot \mod n : \text{multiplication modulo } n)$

is NOT a group if $n$ is composite

i) $\cdot \mod n$ is associative

\[ \text{e.g., } ((5\cdot7) \mod 16) \cdot 4 \mod 16 = (5 \cdot ((7 \cdot 4) \mod 16)) \mod 16 \]

ii) Identity element = 1

\[ (a \cdot 1) \mod n = (1 \cdot a) \mod n = a \]

iii) There is no inverse of $a$ for any $a$ that is not relatively prime with $n$

\[ \text{e.g., there is no } x \in \mathbb{Z}_n-\{0\} \]

\[ \text{such that} \]

\[ (2 \cdot x) \mod 16 = 1 \]

iv) $\cdot \mod n$ is commutative

\[ \text{e.g., } (5 \cdot 8) \mod 16 = (8 \cdot 5) \mod 16 \]
Example 5a

\((Z^n_* = \{a: a \in \{1, 2, ..., n-1\} \text{ and } a \text{ is relatively prime with } n\}, \cdot \mod n : \text{multiplication modulo } n)\)

is an abelian finite group of order \(\varphi(n)\)

For \(n = 15\), \(Z^n_* = \{1, 2, 4, 7, 8, 11, 13, 14\}\) \(\varphi(15) = 8\)

i) \(\cdot \mod n\) is associative

\(e.g., (((4 \cdot 7) \mod 15) \cdot 2) \mod 16 = (4 \cdot ((7 \cdot 2) \mod 15)) \mod 16\)

ii) Identity element = 1 \(a \cdot 1) \mod n = (1 \cdot a) \mod n = a\)

iii) There is an inverse for every element of the group

\(e.g., (2 \cdot 8) \mod 15 = 1\)
\((4 \cdot 4) \mod 15 = 1\)
\((7 \cdot 13) \mod 15 = 1\)
\((11 \cdot 11) \mod 15 = 1\)

iv) \(\cdot \mod n\) is commutative \(e.g., (5 \cdot 8) \mod 15 = (8 \cdot 5) \mod 15\)

Example 5b

\((Z^n_* = \{1, 2, ..., p-1\} \text{ where } p \text{ is prime}, \cdot \mod p : \text{multiplication modulo } p)\)

is an abelian finite group of order \(p-1\)

For \(p = 11\), \(Z^n_* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\) \(\varphi(11) = 11-1=10\)

i) \(\cdot \mod n\) is associative

\(e.g., (((4 \cdot 7) \mod 11) \cdot 2) \mod 11 = (4 \cdot ((7 \cdot 2) \mod 11)) \mod 11\)

ii) Identity element = 1 \(a \cdot 1) \mod p = (1 \cdot a) \mod p = a\)

iii) There is an inverse for every element of the group

\(e.g., (2 \cdot 6) \mod 11 = 1\)
\((3 \cdot 4) \mod 11 = 1\)
\((5 \cdot 9) \mod 11 = 1\)
\((7 \cdot 8) \mod 11 = 1\)

iv) \(\cdot \mod n\) is commutative \(e.g., (5 \cdot 8) \mod 11 = (8 \cdot 5) \mod 11\)
Cyclic Group

Example 6

\( Z_p^* = \{1, 2, \ldots, p-1\} \text{ where } p \text{ is prime}, \)
\( \mod p : \text{multiplication modulo } p \)

is a cyclic group with \( \phi(p-1) \) generators

For \( p = 11 \), \( Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \)

There are \( \phi(10) = 4 \) generators

In particular:

\[
\begin{align*}
2^1 \mod 11 & = 2 & 2^6 \mod 11 & = 9 \\
2^2 \mod 11 & = 4 & 2^7 \mod 11 & = 7 \\
2^3 \mod 11 & = 8 & 2^8 \mod 11 & = 3 \\
2^4 \mod 11 & = 5 & 2^9 \mod 11 & = 6 \\
2^5 \mod 11 & = 10 & 2^{10} \mod 11 & = 1
\end{align*}
\]

2 is a generator (primitive element) of \( Z_{11}^* \)

---

Cyclic Group

Example 6 - continued

\[
\begin{align*}
3^1 \mod 11 & = 3 \\
3^2 \mod 11 & = 9 \\
3^3 \mod 11 & = 5 \\
3^4 \mod 11 & = 4 \\
3^5 \mod 11 & = 1
\end{align*}
\]

3 is NOT a generator of \( Z_{11}^* \)

\(<3> = \{3, 9, 5, 4, 1\} \) is a cyclic subgroup of \( Z_{11}^* \) generated by 3

3 is an element of \( Z_{11}^* \) of order 5

\(|<3>| : \text{size of the subgroup generated by } 3 = \text{order of } 3 = 5\)

Size of the subgroup = 5 | 10 = size of of the group
Test for a generator of a cyclic group

Size of the cyclic group $Z_{11}^* = 10 = 2 \cdot 5$

Test for $a=2$

$2^{10/2} \mod 11 = 2^5 \mod 11 = 10 \neq 1$
$2^{10/5} \mod 11 = 2^2 \mod 11 = 4 \neq 1$

Result: 2 is a generator of $Z_{11}^*$

Test for $a=3$

$3^{10/2} \mod 11 = 3^5 \mod 11 = 243 \mod 11 = 1$
$3^{10/5} \mod 11 = 3^2 \mod 11 = 9 \neq 1$

Result: 3 is NOT a generator of $Z_{11}^*$

Ring

Example 7

($Z$ - set of integers, $+$ addition, $\cdot$ multiplication)

is a commutative ring

i)  $(Z, +)$ is an abelian group with identity element 0

ii)  $\cdot$ is associative  
    e.g.,  $(5 \cdot 7) \cdot 13 = 5 \cdot (7 \cdot 13)$

iii)  $\cdot$ has an identity element $= 1$  
      $a \cdot 1 = 1 \cdot a = a$

iv)  $\cdot$ is distributive over $+$
    e.g.,  $5 \cdot (7 + 13) = 5 \cdot 7 + 5 \cdot 13$, and
    $(5 + 7) \cdot 13 = 5 \cdot 13 + 7 \cdot 13$

v)  $\cdot$ is commutative  
    e.g.,  $5 \cdot 8 = 8 \cdot 5$
### Ring

**Example 8**

\[ ( \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, + \mod n: \text{addition modulo } n, \cdot \mod n: \text{multiplication modulo } n) \]

is a commutative ring

i) \( (\mathbb{Z}_n, +) \) is an abelian group with identity element 0

ii) \( \cdot \) is associative

\[ \text{e.g., } ((5 \cdot 7 \mod 16) \cdot 4) \mod 16 = (5 \cdot (7 \cdot 4 \mod 16)) \mod 16 \]

iii) \( \cdot \) has an identity element = 1 \( a \cdot 1 \mod n = 1 \cdot a \mod n = a \)

iv) \( \cdot \) is distributive over +

\[ \text{e.g., } (5 \cdot ((7 + 4) \mod 16)) \mod 16 = (5 \cdot 7 \mod 16) + (5 \cdot 4 \mod 16) \]

v) \( \cdot \) is commutative

\[ \text{e.g., } (5 \cdot 8) \mod 16 = (8 \cdot 5) \mod 16 \]

### Field

**Example 9**

\( (\mathbb{Z} - \text{set of integers, } + \text{ addition, } \cdot \text{ multiplication}) \)

is NOT a field

No inverse of \( a \text{ for any } a \neq 1 \text{ or -1} \)

\[ \text{e.g., there is no integer } x, \text{ such that } 5 \cdot x = 1 \]

**Example 10**

\( ( \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, + \mod n: \text{addition modulo } n, \cdot \mod n: \text{multiplication modulo } n) \)

is NOT a field if \( n \) is composite

No inverse of \( a \text{ if } a \text{ is not relatively prime with } n \)

\[ \text{e.g., there is no } x \in \mathbb{Z}_n, \text{ such that } 2 \cdot x = 1 \mod 16 \]
Field

Example 11

(\(Z_p = \{0, 1, 2, \ldots, p-1\}\), \(+\mod p\): addition modulo \(p\),
\(\cdot\mod p\): multiplication modulo \(p\))

is a field if and only if \(p\) is prime

i) \((Z_p, + \mod p, \cdot \mod p)\) is a commutative ring

ii) There is multiplicative inverse for all numbers from \(Z_p - \{0\}\)

\[\begin{align*}
(2 \cdot 6) \mod 11 = 1 \rightarrow 2^{-1} \mod 11 = 6 \\
(3 \cdot 4) \mod 11 = 1 \rightarrow 3^{-1} \mod 11 = 4 \\
(5 \cdot 9) \mod 11 = 1 \rightarrow 5^{-1} \mod 11 = 9 \\
(7 \cdot 8) \mod 11 = 1 \rightarrow 7^{-1} \mod 11 = 8
\end{align*}\]

Field

Example 12

(\(Z_p = \{0, 1, 2, \ldots, p-1\}\), \(+\mod p\): addition modulo \(p\),
\(\cdot\mod p\): multiplication modulo \(p\))

is a field of characteristic \(p\)

\[\underbrace{(1 + 1 + 1 + \ldots + 1)}_{p \text{ times}} \mod p = 0\]
Sets of polynomials

$Z[x]$ - polynomials with coefficients in $Z$,

e.g., $f(x) = -4 x^3 + 254 x^2 + 45 x + 7$

$Z_n[x]$ - polynomials with coefficients in $Z_n$

e.g., for $n=15$

$f(x) = 3 x^3 + 14 x^2 + 4 x + 7$

$Z_2[x]$ - polynomials with coefficients in $Z_2$

e.g., $f(x) = 1 x^3 + 0 x^2 + 1 x + 1 = x^3 + x + 1$

Polynomial rings

$(Z[x], \text{polynomial addition, polynomial multiplication})$

$(Z_n[x], \text{polynomial addition, polynomial multiplication})$

$(Z_2[x], \text{polynomial addition, polynomial multiplication})$

For $Z_2[x]$

i) $(Z_2[x], +)$ is an abelian group with identity element 0

ii) $\cdot$ is associative

e.g., $((x^2+x+1) \cdot (x+1)) \cdot (x^2+1) = (x^2+x+1) \cdot ((x+1) \cdot (x^2+1))$

iii) $\cdot$ has an identity element = 1

$f(x) \cdot 1 \mod n = 1 \cdot f(x) \mod n = f(x)$

iv) $\cdot$ is distributive over $+$

e.g., $(x^2+x+1) \cdot ((x+1)+(x^2+1)) = (x^2+x+1) \cdot (x+1)+(x^2+x+1) \cdot (x+1)$
Finite sets of polynomials

\[ Z_2[x]/f(x) \] - polynomials with coefficients in \( Z_2 \)
of degree less than \( n=\deg f(x) \)
e.g., for \( f(x) = x^3 + x + 1 \)
\[
\begin{align*}
g_0(x) &= x^2 + x + 1 & g_3(x) &= x + 1 \\
g_4(x) &= x^2 + x & g_2(x) &= x \\
g_5(x) &= x^2 + 1 & g_1(x) &= 1 \\
g_6(x) &= x^2 & g_0(x) &= 0
\end{align*}
\]

\[ Z_p[x]/f(x) \] - polynomials with coefficients in \( Z_p \)
of degree less than \( n=\deg f(x) \)
e.g., for \( f(x) = x^3 + x + 1 \), and \( p=3 \)
\[
\begin{align*}
g_0(x) &= 0 & \text{Total: } 3^n \text{ polynomials} \\
\text{...} \\
g_{M-1}(x) &= 2x^2 + 2x + 2
\end{align*}
\]

Polynomial rings

\((Z_2[x]/f(x), \text{polynomial addition mod } f(x),\)
\(\text{polynomial multiplication mod } f(x))\)

\((Z_p[x]/f(x), \text{polynomial addition mod } f(x),\)
\(\text{polynomial multiplication mod } f(x))\)

**Polynomial addition:**
\[
(x^3 + x + 1) + (x^2 + 1) \mod (x^4 + 1) = x^3 + x^2 + x
\]

**Polynomial multiplication:**
\[
(x^3 + x + 1) (x^2 + 1) \mod (x^4 + 1) = \\
= (x^5 + x^3 + x^2) + (x^4 + x + 1) \mod (x^4 + 1) = \\
= x^5 + x^2 + x + 1 \mod (x^4 + 1) = \\
= x \cdot (x^4 + 1) + x^2 + 1 \mod (x^4 + 1) = x^2 + 1
\]
Finite fields

$f(x)$ is an irreducible polynomial of degree $m$

$F_q = \text{GF}(2^m) = (\mathbb{Z}_2[x]/f(x)$, polynomial addition mod $f(x)$,
polynomial multiplication mod $f(x))$

where $q = 2^m$

$F_q = \text{GF}(p^m) = (\mathbb{Z}_p[x]/f(x)$, polynomial addition mod $f(x)$,
polynomial multiplication mod $f(x))$

where $q = p^m$

All non-zero elements have multiplicative inverses

e.g., for $f(x) = x^3 + x + 1$, and $p=2$

$(x+1) \cdot (x^2 + x) \mod x^3 + x + 1 = 1 \rightarrow (x+1)^{-1} \mod f(x) = x^2+x$

---

Number of primitive polynomials
over $\mathbb{Z}_2$ of degree $m$

<table>
<thead>
<tr>
<th>$m$</th>
<th>$\varphi(2^m-1)/m$</th>
<th>$f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>$x^2+x+1$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$x^3+x+1, x^3+x^2+1$</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$x^4+x+1, x^4+x^3+1$</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>$x^5+x^2+1, \text{etc.}$</td>
</tr>
</tbody>
</table>
Test for a primitive polynomial

Test for $f(x) = x^4 + x + 1$, $f(x)$ irreducible

Size of the cyclic group $F_q^* = q - 1 = 2^m - 1 = 15 = 3\cdot 5$

$x^{15/5} \mod x^4 + x + 1 = x^3 \neq 1$

$x^{15/3} \mod x^4 + x + 1 = x^2 + x \neq 1$

Result: $x$ is a generator of $F_q = \mathbb{Z}_2[x]/f(x)$

Test for $f(x) = x^4 + x^2 + 1$, $f(x)$ is reducible

$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + x + 1)$

Result: $(\mathbb{Z}_2[x]/f(x), \cdot \mod f(x))$ is not a group