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 \geq 5, e.g.,

 $f(x) = a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$

Answered definitely the question which specific equations of

a given degree have algebraic solutions

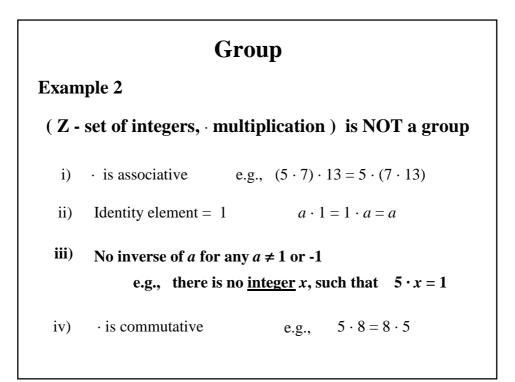
On the way, he developed group theory,

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 <i>Reviewer 1</i>
1930	Augustin-Luis Cauchy <i>forgot or lost</i> the communication Galois submits the revised version of his manuscript,
	hoping to enter the competition for the Grand Prize in mathematics <i>Reviewer 2</i>
1931	Joseph Fourier – <i>died</i> shortly after receiving the manuscript Third submission to the French Academy of Sciences
1751	Reviewer 3
	Simeon-Denis Poisson – <i>does not understand</i> 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: <i>"Eventually there will be, I hope, some people who will find it profitable to decipher this mess."</i>
May 30, 18	32 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** (Z - set of integers, + addition) is an abelian group i) + is associative e.g., (5+7)+13 = 5+(7+13)ii) Identity element = 0a+0 = 0+a = aiii) Inverse of a = -a7 + (-7) = 0e.g., + is commutative 5 + 8 = 8 + 5iv) e.g.,



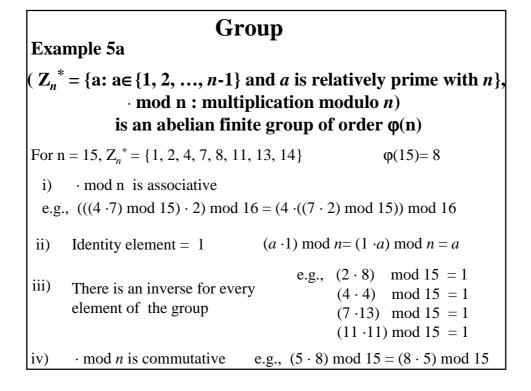
Group

Example 3

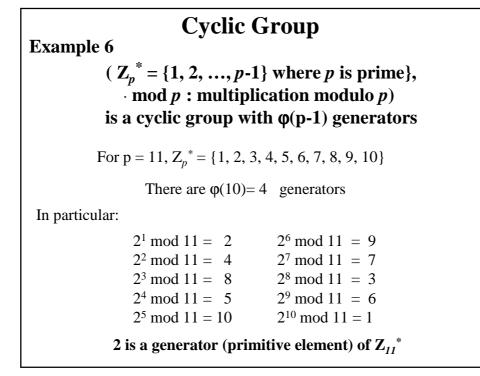
$(Z_n = \{0, 1, 2, ..., n-1\}, + \text{mod } n : \text{addition modulo } n)$ is an abelian finite group of order n

```
i) + mod n is associative
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 e.g., 7 + (16-7) = 7 + 9 \mod 16 = 0
iv) + mod n is commutative e.g., 5 + 8 \mod 16 = 8 + 5 \mod 16
```

Group **Example 4** $(Z_n - \{0\} = \{1, 2, ..., n-1\}, \dots \text{ mod } n : \text{ multiplication modulo } n)$ is NOT a group if *n* is composite \cdot mod n is associative i) e.g., $(((5\cdot7) \mod 16) \cdot 4) \mod 16 = (5 \cdot ((7 \cdot 4) \mod 16)) \mod 16$ $(a \cdot 1) \mod n = (1 \cdot a) \mod n = a$ ii) Identity element = 1iii) e.g., there is no $x \in Z_n$ -{0} There is no inverse of *a* for any *a* that is not relatively prime with *n* such that $(2 \cdot x) \mod 16 = 1$ iv) $\cdot \mod n$ is commutative e.g., $(5 \cdot 8) \mod 16 = (8 \cdot 5) \mod 16$



GroupExample 5b $(Z_p^* = \{1, 2,, p-1\} \text{ where } p \text{ is prime}\},$ $\cdot \mod p$: multiplication modulo p)is an abelian finite group of order p-1
For $p = 11$, $Z_p^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $\phi(11) = 11 - 1 = 10$ i) $\cdot \mod n$ is associative e.g., (((4 ·7) mod 11) · 2) mod 11 = (4 ·((7 · 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 groupe.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 GroupExample 6 - continued $3^1 \mod 11 = 3$ $3^2 \mod 11 = 9$ $3^3 \mod 11 = 5$ $3^4 \mod 11 = 4$ $3^5 \mod 11 = 1$ 3 is NOT a generator of of Z_{II}^* <3> = {3, 9, 5, 4, 1} is a cyclic subgroup of Z_{II}^* generated by 33 is an element of Z_{II}^* of order 5|<3>| : size of the subgroup generated by 3 = order of 3 = 5Size 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

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

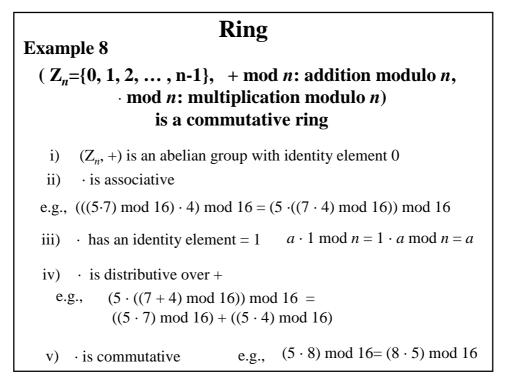
Result: 2 is a generator of Z_{11}^{*}

Test for a=3

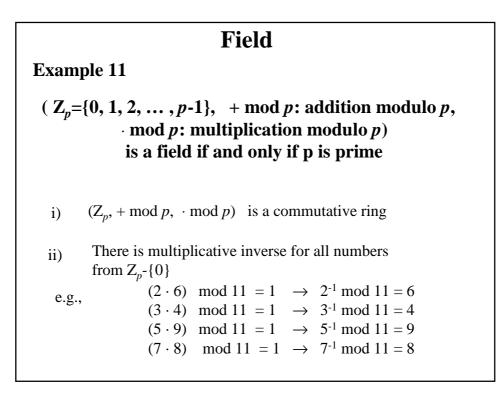
 $3^{10/2} \mod 11 = 3^5 \mod 11 = 243 \mod 11 = 1$ $3^{10/5} \mod 11 = 3^2 \mod 11 = 9 \neq 1$

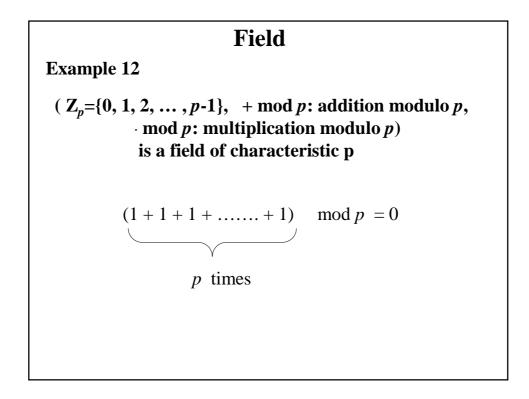
Result: 3 is NOT a generator of Z_{II}^{*}

Ring **Example 7** (Z - set of integers, + addition, · multiplication) is a commutative ring i) (Z, +) is an abelian group with identity element 0 \cdot is associative ii) 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 $5 \cdot 8 = 8 \cdot 5$ e.g.,



Field
Example 9
(Z - set of integers, + addition, · multiplication) is NOT a field
No inverse of <i>a</i> for any $a \neq 1$ or -1
e.g., there is no <u>integer</u> x, such that $5 \cdot x = 1$
Example 10
 (Z_n={0, 1, 2,, n-1}, + mod n: addition modulo n, · mod n: multiplication modulo n) is NOT a field if n is composite
No inverse of <i>a</i> if a is not relatively prime with <i>n</i> e.g., there is no $x \in \mathbb{Z}_n$, such that $2 \cdot x = 1 \mod 16$





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], polynomial addition, polynomial multiplication) $(Z_n[x], polynomial addition, polynomial multiplication)$ $(Z_2[x], polynomial addition, polynomial multiplication)$

For $Z_2[x]$

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

ii) \cdot is associative

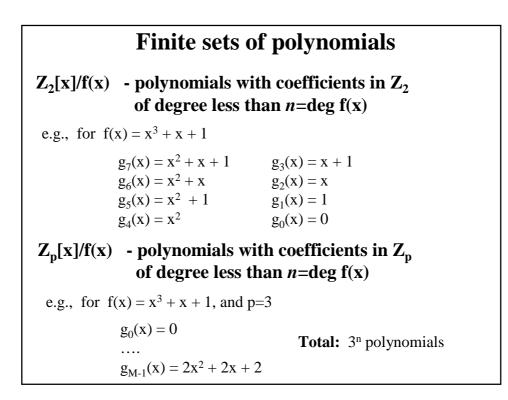
e.g., $((x^2+x+1) \cdot (x+1)) \cdot (x^2+1) = (x^2+x+1) \cdot ((x+1) \cdot (x^2+1))$

iii) \cdot has an identity element = 1

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

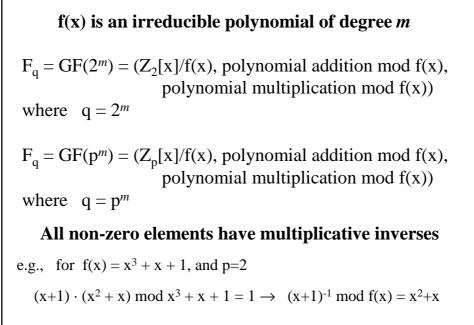
iv) \cdot is distributive over +

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



 $\begin{array}{l} \textbf{Polynomial rings} \\ (Z_2[x]/f(x), polynomial addition mod f(x), polynomial multiplication mod f(x)) \\ (Z_p[x]/f(x), polynomial addition mod f(x), polynomial multiplication mod f(x)) \\ \textbf{Polynomial addition:} \\ (x^3 + x + 1) + (x^2 + 1) mod (x^4 + 1) = x^3 + x^2 + x \\ \textbf{Polynomial multiplication:} \\ (x^3 + x + 1) (x^2 + 1) mod (x^4 + 1) = \\ = (x^5 + x^3 + x^2) + (x^3 + x + 1) mod (x^4 + 1) = \\ = x^5 + x^2 + x + 1 mod (x^4 + 1) = \\ = x \cdot (x^4 + 1) + x^2 + 1 mod (x^4 + 1) = x^2 + 1 \\ \end{array}$

Finite fields



Number of primitive polynomials over Z_2 of degree <i>m</i>				
m	φ(2 ^m -1)/m	f(x)		
2	1	x ² +x+1		
3	2	x ³ +x+1, x ³ +x ² +1		
4	2	x ⁴ +x+1, x ⁴ +x ³ +1		
5	6	$x^{5}+x^{2}+1$, etc.		

Test for a primitive polynomial

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

Size of the cyclic group $F_q^* = q-1 = 2^m-1 = 15=3.5$

 $x^{15/5} \mod x^4 + x + 1 = x^3 \neq 1$ $x^{15/3} \mod x^4 + x + 1 = x^2 + x \neq 1$

Result: x is a generator of $F_q=Z_2[x]/f(x)$

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