# 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

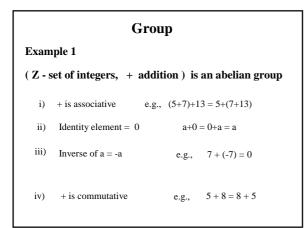
On the way, he developed **group theory**,

one of the most important branches of modern mathematics.

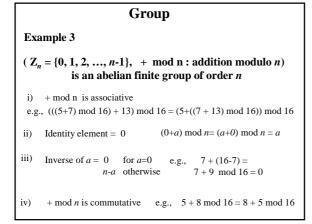
## Evariste Galois (1811-1832)

1829	Galois submits his results for the first time to	
	the French Academy of Sciences	
	Reviewer 1	
	Augustin-Luis 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 – <i>died</i> 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: <i>"Eventually there will be, I hope, some people who</i> <i>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	

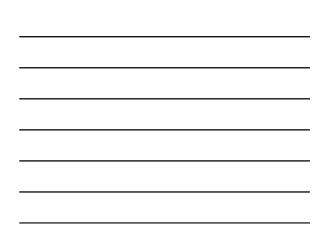


Group			
Example 2			
( ${\bf Z}$ - set of integers, $\cdot$ multiplication ) is NOT a group			
i)	• is associative e.g., $(5 \cdot 7) \cdot 13 = 5 \cdot (7 \cdot 13)$		
ii)	Identity element = 1 $a \cdot 1 = 1 \cdot a = a$		
iii)	iii) No inverse of <i>a</i> for any $a \neq 1$ or -1 e.g., there is no <u>integer</u> <i>x</i> , such that $5 \cdot x = 1$		
iv)	$\cdot$ is commutative e.g., $5 \cdot 8 = 8 \cdot 5$		



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

Exa	Gro mple 5a	oup
$(\mathbf{Z}_n^*)$	· mod n : multip	and <i>a</i> is relatively prime with <i>n</i> } plication modulo <i>n</i> ) to group of order $\phi(n)$
i)	$n = 15, Z_n^* = \{1, 2, 4, 7, 8, 11, \dots \text{ mod } n \text{ is associative} \\ (((4 \cdot 7) \mod 15) \cdot 2) \mod 10 $	13, 14} $\varphi(15)=8$ 6 = (4 ·((7 · 2) mod 15)) mod 16
ii)	Identity element = 1	$(a \cdot 1) \mod n = (1 \cdot a) \mod n = a$ e.g., $(2 \cdot 8) \mod 15 = 1$
iii)	There is an inverse for every element of the group	$\begin{array}{c} (4 \cdot 4) \mod 15 = 1 \\ (7 \cdot 13) \mod 15 = 1 \\ (11 \cdot 11) \mod 15 = 1 \end{array}$
iv)	$\cdot \mod n$ is commutative	e.g., $(5 \cdot 8) \mod 15 = (8 \cdot 5) \mod 15$



GroupExample 5b( $Z_p^* = \{1, 2,, p-1\}$ where p is prime},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) · 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 group $(3 \cdot 4) \mod 11 = 1$ $(7 \cdot 8) \mod 11 = 1$		
iv) $\cdot \mod n$ is commutative e.g., $(5 \cdot 8) \mod 11 = (8 \cdot 5) \mod 11$		



Cyclic GroupExample 6 $(Z_p^* = \{1, 2,, p-1\} \text{ where } p \text{ is prime}\},$ $\cdot \mod p$ : multiplication modulo $p$ )is a cyclic group with $\varphi(p-1)$ generators		
For $p = 11$ , $Z_p^* = \{1, 2, 3,$	4, 5, 6, 7, 8, 9, 10}	
There are $\varphi(10) = 4$	4 generators	
In particular:		
$2^1 \mod 11 = 2$	$2^6 \mod 11 = 9$	
$2^2 \mod 11 = 4$	$2^7 \mod 11 = 7$	
$2^3 \mod 11 = 8$	$2^8 \mod 11 = 3$	
$2^4 \mod 11 = 5$	$2^9 \mod 11 = 6$	
$2^5 \mod 11 = 10$	$2^{10} \mod 11 = 1$	
2 is a generator (prim	itive element) of $\mathbf{Z}_{II}^{*}$	



Cyclic Group		
Example 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 $\mathbf{Z}_{II}^*$		
$\langle 3 \rangle = \{3, 9, 5, 4, 1\}$ is a cyclic subgroup of $Z_{II}^*$ generated by 3 3 is an element of $Z_{II}^*$ of order 5		
<3>  : size of the subgroup generated by 3 = 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  $Z_{II}^{*} = 10 = 2 \cdot 5$ 

Test for a=2

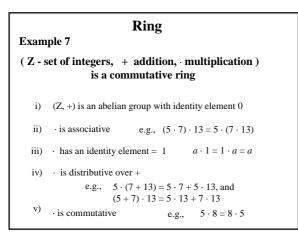
 $2^{10/2} \mod 11 = 2^5 \mod 11 = 10 \neq 1$  $2^{10/5} \mod 11 = 2^2 \mod 11 = 4 \neq 1$ 

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

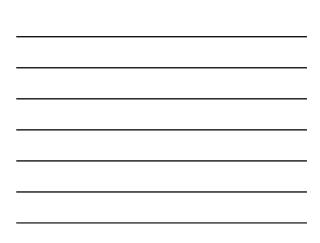
#### Test for a=3

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

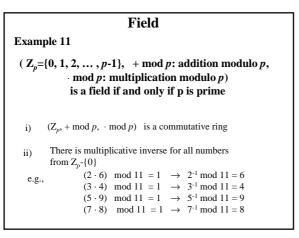
Result: 3 is NOT a generator of  $Z_{II}^{*}$ 

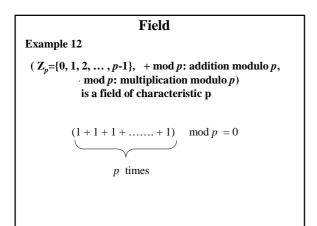


Ring Example 8		
$(Z_n = \{0, 1, 2,, n-1\}, + mod n: addition modulo n,mod n: multiplication modulo n)is a commutative ring$		
i) $(Z_n, +)$ is an abelian group with identity element 0 ii) $\cdot$ is associative		
e.g., $(((5.7) \mod 16) \cdot 4) \mod 16 = (5 \cdot ((7 \cdot 4) \mod 16)) \mod 16$		
iii) $\cdot$ has an identity element = 1 $a \cdot 1 \mod n = 1 \cdot a \mod n = a$		
iv) · is distributive over + e.g., (5 · ((7 + 4) mod 16)) mod 16 = ((5 · 7) mod 16) + ((5 · 4) mod 16)		
v) $\cdot$ is commutative e.g., $(5 \cdot 8) \mod 16 = (8 \cdot 5) \mod 16$		



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	
$(Z_n = \{0, 1, 2,, n-1\}, + \text{mod } n: \text{ addition modulo } n,$ mod $n$ : multiplication modulo $n$ )	
is NOT a field if <i>n</i> 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

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

 $\mathbf{Z}_2[\mathbf{x}]~$  - polynomials with coefficients in  $\mathbf{Z}_2$ 

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<sub>2</sub>[x]

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

ii)  $\cdot$  is associative

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

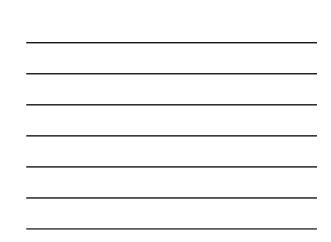
iii)  $\cdot$  has an identity element = 1

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

iv) · 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  $f(x) = x^3 + x + 1$  $g_7(x) = x^2 + x + 1$  $g_3(x) = x + 1$  $g_6(x) = x^2 + x$  $g_2(x) = x$  $g_5(x) = x^2 + 1$  $g_1(x)=1$  $g_4(x)=x^2$  $g_0(x) = 0$  $Z_{\rm p}[x]/f(x)~$  - polynomials with coefficients in  $Z_{\rm p}$ of degree less than *n*=deg f(x) e.g., for  $f(x) = x^3 + x + 1$ , and p=3 $g_0(x) = 0$ Total: 3<sup>n</sup> polynomials  $g_{M-1}(x) = 2x^2 + 2x + 2$ 



#### **Polynomial rings**

```
(Z_2[x]/f(x)), polynomial addition mod f(x),
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:**

 $\begin{array}{l} (x^3+x+1) \ (x^2+1) \ mod \ (x^4+1) = \\ = (x^5+x^{3'}\!+x^2) + (x^{3'}\!+x+1) \ mod \ (x^4+1) = \\ = x^5+x^2+x+1 \ mod \ (x^4+1) = \\ = x \cdot (x^4+1) + x^2\!+1 \ mod \ (x^4+1) = x^2\!+1 \end{array}$ 

# Finite fields

f(x) is an irreducible polynomial of degree m

 $\begin{aligned} F_q &= GF(2^m) = (Z_2[x]/f(x), \text{ polynomial addition mod } f(x), \\ & \text{polynomial multiplication mod } f(x)) \\ \text{where} \quad q = 2^m \end{aligned}$ 

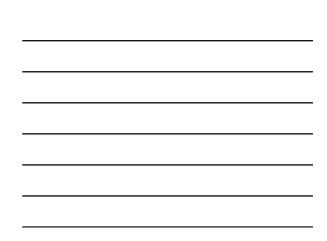
$$\label{eq:fq} \begin{split} F_q &= GF(p^m) = (Z_p[x]/f(x), \, polynomial \, addition \, mod \, f(x), \\ & polynomial \, multiplication \, mod \, f(x)) \\ where \quad q = p^m \end{split}$$

All non-zero elements have multiplicative inverses

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

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

Number of primitive polynomials over $\mathbb{Z}_2$ of degree <i>m</i>			
	m	φ(2 <sup>m</sup> -1)/m	f(x)
	2	1	x <sup>2</sup> +x+1
	3	2	x <sup>3</sup> +x+1, x <sup>3</sup> +x <sup>2</sup> +1
	4	2	x <sup>4</sup> +x+1, x <sup>4</sup> +x <sup>3</sup> +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  $F_q^* = q-1 = 2^{m}-1 = 15=3.5$ 

 $\begin{array}{ll} x^{15/5} \mbox{ mod } x^4{+}x{+}1 = & x^3 \neq 1 \\ x^{15/3} \mbox{ mod } x^4{+}x{+}1 = & x^2{+}x \neq 1 \end{array}$ 

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