Chapter 5

Finite Fields

Discovery

- Evariste Galois (1811-1832)
- Niels Abel (1802-1829)
- Applications
  - Solve unsolved problems of ancient Greek, 2000+ years old
    - Squaring a circle
    - Trisecting an angle
  - Show that degree-5 equations have no formula solutions. 250+ years old
  - Physics
  - Cryptography
  - …

Abelian Group

(G, •) is a **group**, where G is a set of elements and the binary operator • has the following properties:

- (A1) Closure
  - If a and b belong to G, then $a \bullet b$ is also in G
- (A2) Associative
  - $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G
- (A3) Identity element
  - There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G
- (A4) Inverse element
  - For each a in G, there is an element a^{-1} in G such that $a \bullet a^{-1} = a^{-1} \bullet a = e$
- (A5) Commutative: $a \bullet b = b \bullet a$ for all a, b in G

Examples

- (Z, +)
- (R, +)
- (R-{0}, ×)
- (Q-{0}, x)
- $(Z_n, +_n)$, where $Z_n = \{0, 1, 2, \ldots, n-1\}$
- (Z_n^*, x_n), where $Z_n^* = \{a\colon 1 \le a \le n-1, \gcd(a, n) = 1\}$
- $(Z_p, +_p)$, for any prime p
- (Z_p^*, x_p), for any prime p

Cyclic Group

- Notation
  - $a^3 = a \bullet a \bullet a$
  - $a^0 = e$: identity element
  - $a^{-n} = (a^{-1})^n$, where a^{-1} is the inverse of a
- (G, •) is **cyclic** if there is $g \in G$, such that any $a \in G$ can be expressed as $a = g^k$ for some k.
- g is called a **generator** of G
  - g spans all elements of G, that is, $G = \{g^k : k \geq 0\}$
- $\{Z_7^*, \times_7\}$ is a cyclic group with generators 3 and 5. Check $3^0=1$, $3^1=3$, $3^2=2$, $3^3=6$, $3^4=5$, $3^5=4$.

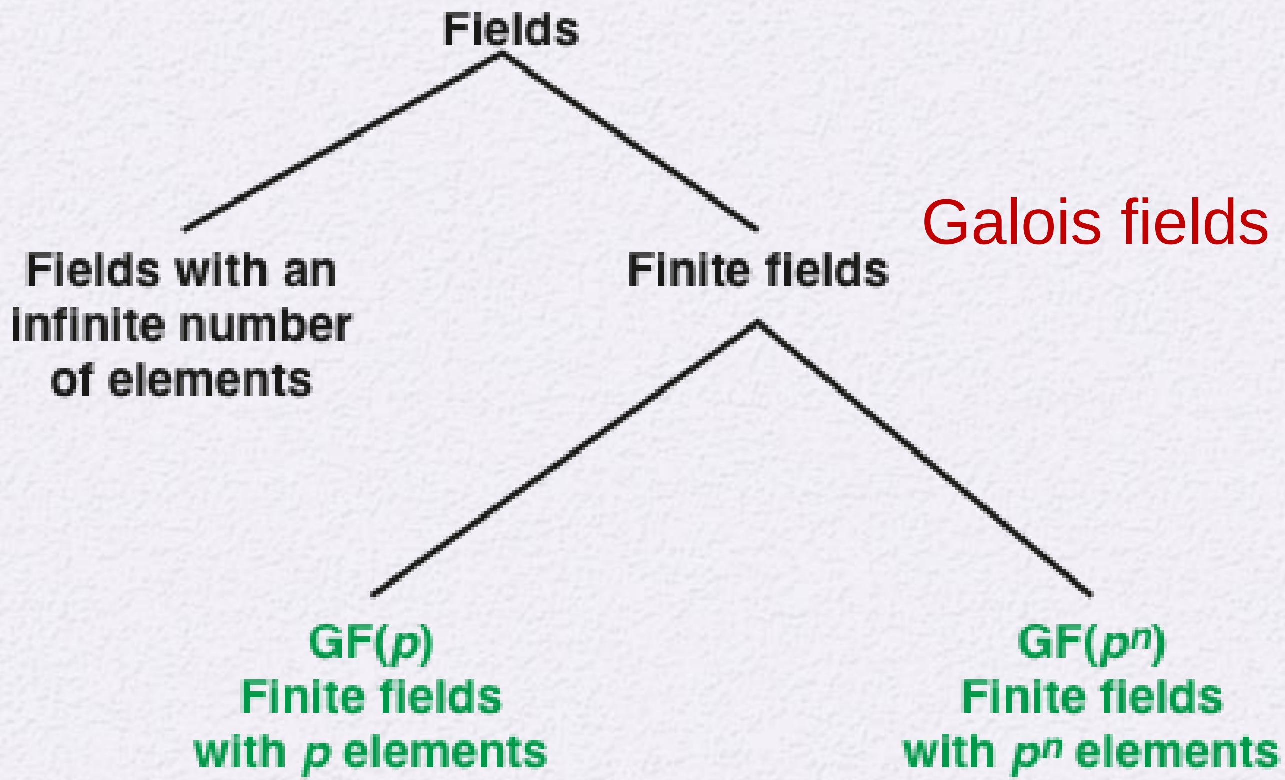
Field

- $\{F, +, \times\}$ is a **field**, where F is a set of elements and
  - $\{F, +\}$ and $\{F-\{0\}, \times\}$ are both groups
  - Distributive laws
    - $a(b+c) = ab + ac$ for all a, b, c in F
    - $(a+b)c = ac + bc$ for all a, b, c in F
- 0: the identity for +
- 1: the identity for $\times$
- -a: the inverse of a under +
- a^{-1}: the inverse of a under $\times$
- $a-b = a+(-b)$
- $a/b = a \times b^{-1}$

Field: examples

- {R, +, x} is an infinite field, where R is the set of reals
- {Q, +, x} is an infinite field, where Q is the set of rationals
- $\{Z_p, +_p, \times_p\}$ is a finite field of p elements, where p is prime

Types of fields



Finite Fields GF(p^m)

- For every prime p and m≥,1 there is a unique finite field, up to isomorphism
- GF(p^m): **the** finite field with p^m elements

Finite Field: GF(p)

- $GF(p) = \{Z_p, +_p, x_p\}$
- GF(2): Boolean algebra
- $GF(7) = \{Z_7, +_7, x_7\}$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Polynomial arithmetic

$$
\begin{array}{rl}
 & x^3 + x^2 \qquad + 2 \\
+ & (x^2 - x + 1) \\
\hline
 & x^3 + 2x^2 - x + 3
\end{array}
$$

(a) Addition

$$
\begin{array}{rl}
 & x^3 + x^2 \qquad + 2 \\
- & (x^2 - x + 1) \\
\hline
 & x^3 \qquad + x + 1
\end{array}
$$

(b) Subtraction

$$
\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
\times\ (x^2 - x + 1) \\
\hline
x^3 + x^2 \qquad + 2 \\
-x^4 - x^3 \qquad - 2x \qquad \\
x^5 + x^4 \qquad + 2x^2 \qquad\qquad \\
\hline
x^5 \qquad\qquad + 3x^2 - 2x + 2
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r|l}
 & x + 2 \\
\hline
x^2 - x + 1 & x^3 + x^2 \qquad + 2 \\
 & x^3 - x^2 + x \\
\cline{2-2}
 & \qquad 2x^2 - x + 2 \\
 & \qquad 2x^2 - 2x + 2 \\
\cline{2-2}
 & \qquad\qquad x
\end{array}
$$

(d) Division

Polynomials over GF(p)

- $f(x) = a_t x^t + a_{t-1} x^{t-1} + \cdots + a_0$ over GF(p), each $a_i \in$ GF(p)
- Operations over GF(5)
  - $(3x^2+2x+4) + (2x^2+x+3) = 5x^2+3x+7 = 3x+2$
  - $(3x^2+2x+4) \times (2x^2+x+3) = 6x^4+7x^3+19x^2+10x+12 = x^4+2x^3+4x^2+2$
  - $4x^5+2x^3+x+3 \bmod 3x^2+x+1 = 4x+1$

Irreducible poly over GF(p)

- $g(x)$ over GF(p) is **irreducible (or prime)** if $g(x)$ cannot be expressed as a product of two polynomials over GF(p) of degree ≥1.
    - x^3+x+1 is irreducible over GF(2)
    - $x^2+1 = (x+2)(x+3)$ over GF(5)

Finite field: $GF(p^m)/g(x)$, $m \geq 2$

- $GF(p^m)$ = the set of polys over GF(p) with degree < m
- g(x) is degree-m and irreducible over GF(p)
- Operations of $GF(p^m)/g(x)$
  - -a(x): additive inverse of a(x) mod g(x)
  - $a(x)^{-1}$: multiplicative inverse of a(x) mod g(x)
    - existent since gcd(a(x), g(x))=1
  - a(x)+b(x) mod g(x)
  - a(x)b(x) mod g(x)

Finite field: $GF(p^m)/g(x)$, $m \geq 2$

- $GF(p^m)/g(x)$ and $GF(p^m)/h(x)$ are isomorphic for any degree-m irreducible polys $g(x)$ and $h(x)$

Example: $GF(2^3)/x^3+x+1$

- $g(x)=x^3+x+1$ is irreducible over GF(2)
- $GF(2^3)= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
- Operations
  - $-(x^2+1) \bmod g(x) = x^2+1$
  - $(x+1)^{-1} \bmod g(x) = x^2+x$
  - $(x+1)(x^2) \bmod g(x) = x^2+x+1$
  - …

Example: $GF(2^3)/x^3+x+1$

- Trick: computing a(x) mod g(x)
  - $a(x) = q(x)\, g(x) + r(x)$
  - Let $g(x)=x^3+x+1=0 \rightarrow x^3 = -x-1 = x+1$
  - Substitute $x+1$ for x^3 in a(x) repetitively and get r(x)

GF(2^3)/($x^3 + x + 1$)

		000	001	010	011	100	101	110	111
	+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

		000	001	010	011	100	101	110	111
	×	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

$GF(2^m)/g(x)$: computation

- Since coefficients are 0 or 1, a polynomial can be represented as a binary string
- Addition/substraction: XOR of these strings
- Multiplication
  - long-hand multiplication
  - the “shift-XOR” algorithm
- Modulo reduction:
  - repeatedly substituting highest power with with irreducible polynomial (also shift and XOR)

GF(2^m)/g(x): computation

- Multiplication: "shift-XOR" algorithm
  - Example: GF(2^3)/x^3+x+1

```
      1  0  1  (multiplicand)
   x  1  1  1  (multiplier)
----------------------
1  0  1
   1  0  1
----------------------
1  1  1  1
1  0  1  1
----------------------
   1  0  0
      1  0 1
----------------------
   1  1  0  1
   1  0  1  1
----------------------
      1  1   0
```

$GF(2^m)/g(x)$: example

- $GF(2^8)/x^8+x^4+x^3+x+1$ (1 0001 1011)
- axb = 3Fx86 = 0011 1111 x 1000 0110
  - Let $b_7b_6b_5b_4b_3b_2b_1b_0$ = 1000 0110 and a= 0011 1111

i	b_i	f (shift-XOR)	f' (mod g(x))
Initial			0000 0000
7	1	0011 1111	0011 1111
6	0	0111 1110	0111 1110
5	0	1111 1100	1111 1100
4	0	1 1111 1000	1110 0011
3	0	1 1100 0110	1101 1101
2	1	1 1000 0101	1001 1110
1	1	1 0000 0011	0001 1000
0	0	0011 0000	0011 0000

Finite field: $GF(p^{nm})/g(x),f(y)$

- Let $f(y)$ be an irreducible m-degree polynomial with coefficients over a field $GF(p^n)/g(x)$
- $GF(p^{nm})/g(x),f(y)$
  - The element set consists of all polynomials (of y) with coefficients over $GF(p^n)/g(x)$ and degree $< m$
  - On variable y, the operations are mod $f(y)$
  - Coefficient operations are operated on $GF(p^n)/g(x)$

$GF(p^{nm})/g(x),f(y)$: Example

- $GF(2^{3\times4})/x^3+x+1,\ y^4+(x^2+1)y^2+(x+1)$
  - $a(y) = (x+1)y^3 + (x^2+1)\ y^2 + (x+1)$ is a polynomial over the field $GF(2^3)/x^3+x+1$
- $f(y) = y^4 + (x^2+1)\ y^2 + (x+1)$ is irreducible over $GF(2^3)/x^3+x+1$
- $[(x+1)y^3 + (x)\ y^2 + 1]\times[y+(x^2+1)] \bmod f(y)$

$= (x+1)y^4 + [(x+1)(x^2+1) + x]y^3 + [(x)(x^2+1)]y^2 + y + (x^2+1)$

$= (x+1)\ \mathbf{[(x^2+1)y^2+(x+1)]} + [(x+1)(x^2+1) + x]y^3 +$

$[(x)(x^2+1)]y^2 + y + (x^2+1)$

$= (x^2+x)y^3 + (x^2)y^2 + (1)y$

Finite field: $GF(p^{nm})/g(x),f(y)$

- For any a(y) and b(y) over $GF(p^n)/g(x)$ of degree < m,
  - a(y)+b(y) and a(y)xb(y) are defined on "mod f(y)", where coefficients are operated over $G(p^n)/g(x)$
  - -a(y) mod f(y) is defined by negating coefficients
  - $a^{-1}(y)$ mod f(y) is also defined except a(y)=0 since gcd(a(y), f(y))=1
- Thus, $GF(p^{nm})/g(x),f(y)$ is indeed a field.

Generator for GF(q)/f(x)

- A **generator** **g** for GF($q=p^m$) is an element whose powers span all non-zero elements of GF(q)
  - GF(q) $=\{ 0, g^0, g^1, \ldots, g^{q-2} \}$
- Example, 3 and 5 are generators for GF(7).
- For a polynomial field GF(q)/f(x)
  - Let g be a root of f(x)=0, that is, f(g)=0
    - Use g as a symbol, no need to find out
  - g is a generator for GF(q)/f(x)

Generator for GF(2^3)/$x^3 + x + 1$

- g is a root of x^3+x+1. Thus, $g^3+g+1=0$, or $g^3=g+1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
g^0 (= g^7)	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Operations using generator

		000	001	010	100	011	110	111	101
	+	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
001	1	1	0	$g+1$	g^2+1	g	g^2+g+1	g^2+g	g^2
010	g	g	$g+1$	0	g^2+g	1	g^2	g^2+1	g^2+g+1
100	g^2	g^2	g^2+1	g^2+g	0	g^2+g+1	g	$g+1$	1
011	g^3	$g+1$	g	1	g^2+g+1	0	g^2+1	g^2	g^2+g
110	g^4	g^2+g	g^2+g+1	g^2	g	g^2+1	0	1	$g+1$
111	g^5	g^2+g+1	g^2+g	g^2+1	$g+1$	g^2	1	0	g
101	g^6	g^2+1	g^2	g^2+g+1	1	g^2+g	$g+1$	g	0

		000	001	010	100	011	110	111	101
	×	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
010	g	0	g	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1
100	g^2	0	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g
011	g^3	0	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g	g^2
110	g^4	0	g^2+g	g^2+g+1	g^2+1	1	g	g^2	$g+1$
111	g^5	0	g^2+g+1	g^2+1	1	g	g^2	$g+1$	g^2+g
101	g^6	0	g^2+1	1	g	g^2	$g+1$	g^2+g	g^2+g+1

Summary

- Groups
  - Abelian group
  - Cyclic group
- Finite fields of the form GF(*p*)
  - Finite fields of order *p*
  - Finding the multiplicative inverse in GF(*p*)
- Polynomial arithmetic
  - Ordinary polynomial arithmetic
  - Polynomial arithmetic with coefficients in Z_p
- Finite fields of the form GF(2^n)
  - Motivation
  - Modular polynomial arithmetic
  - Finding the multiplicative inverse
  - Computational considerations
  - Using a generator