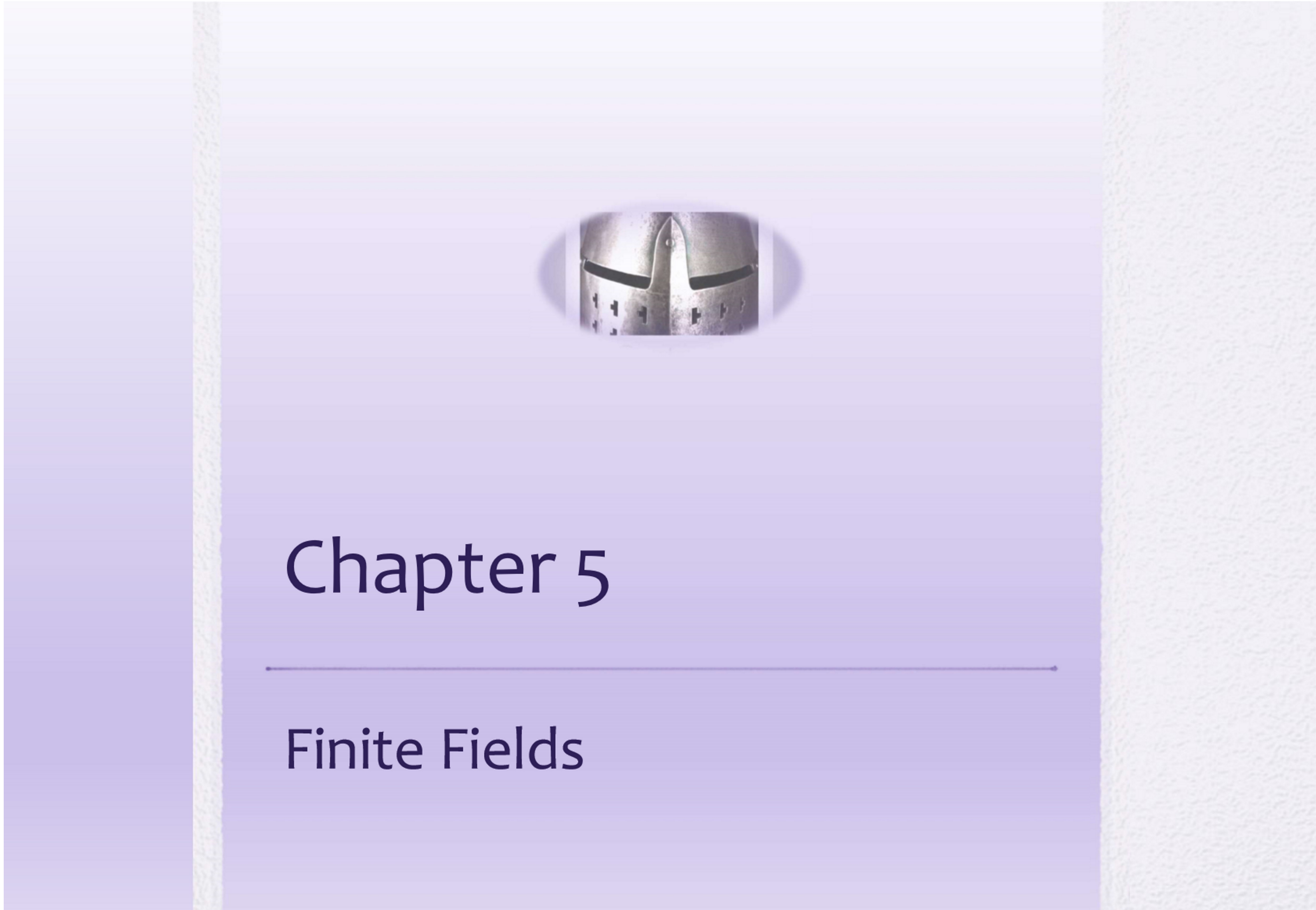
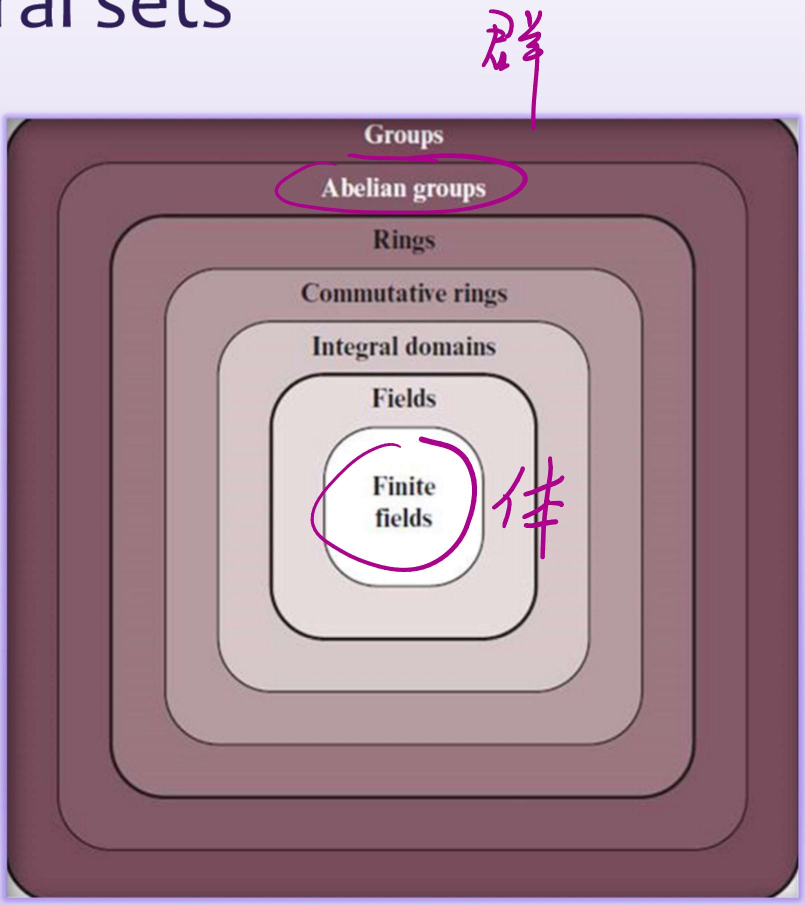
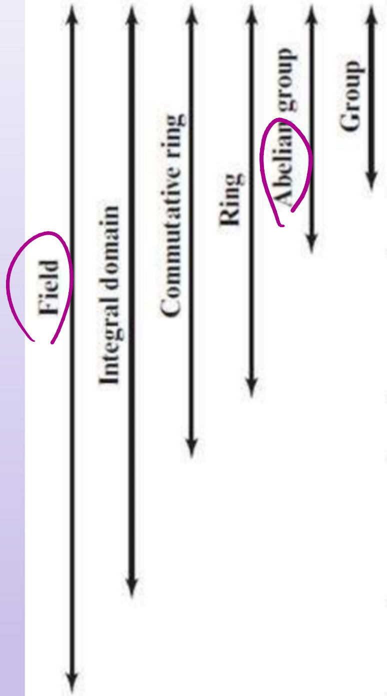
列印成品

2024年3月4日　　上午 08:04



Structural sets





(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Abelian Group

- (G, ∘) is a group, where G is a set of elements and the binary operator ∘ has the following properties:
  - Closure
    - $a \circ b$, for $a, b \ in\ G$
  - Associativity
    - $a \circ (b \circ c) = (a \circ b) \circ c$, for $a, b, c\ in\ G$
  - Identity
    - There is an element e in G such that $a \circ e = e \circ a = a$, for a in G
  - Inverse
    - For each a in G, there is an element $a^{-1}\ in\ G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$
  - ***Commutative***: $a \circ b = b \circ a$, for $a, b\ in\ G$

Examples

- Additive groups
  - $(R, +)$
  - $(\mathrm{Z}, +)$
  - $(Z_n, +),\ Z_n = \{0, 1, 2, \dots, n-1\}$, "+" is mod n
- Multiplicative groups
  - $(R - \{0\},\ \times)$, $(Z, *)$ $\times$
    $2 \to ?\ (\frac{1}{2})$
  - $(Q - \{0\},\ \times)$
  - $(Z_n^*,\ \times),\ Z_n^* = \{a: 1 \le a < n, \gcd(a, n) = 1\}$, "×" is mod n
- $N_n = \{\pi: \pi$ is a permuation over $\{1, 2, \dots, n\}\}$
  $(123)(321)(213) \cdots$
  - Not abelian
- The operator is omitted if no misunderstanding occurs

Cyclic group

- G is $\boldsymbol{cyclic}$ if there is a generator $g \in G$ such that for any $a \in G$, $a = g^k$ for some k
  - g spans all elements of G, that is, $G = \{g^k | k \geq 0\}$
- Notation
  - $g^k = g \circ g \circ \cdots \circ g$ (k times)
  - $a^0 = e$: identity
  - $a^{-k} = (a^{-1})^k$
- Z_7^* is a cyclic group with generators 3 and 5
  - $3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$
  - $5^0 = 1, 5^1 = 5, 5^2 = 4, 5^3 = 6, 5^4 = 2, 5^5 = 3$

$Z_n^* \rightarrow$ cyclic

iff $n = 2, 4, p^\alpha, 2p^\alpha$

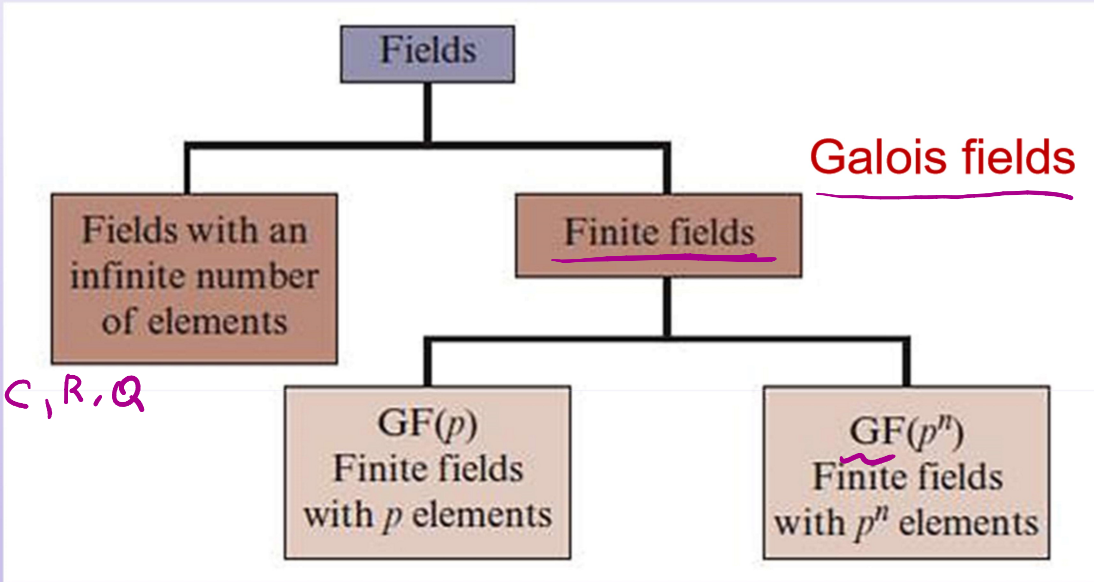
Field: $\{F, +, \times\}$

- $\{F, +\}$ is an additive abelian group
- $\{F - \{0\}, \times\}$ is a multiplicative abelian group
- Distributive laws
  - $a \times (b + c) = a \times b + a \times c,$ for a, b, c $in\ F$
  - $(a + b) \times c = a \times c + b \times c,$ for a, b, c $in\ F$
- 0: the identity for $+$
- 1: the identity for $\times$
- $-a$: the additive inverse of a
- a^{-1}: the multiplicative inverse of a
- $a - b = a + (-b)$
- $a/b = a \times b^{-1}$
- We can do 4 operators $(+,\ -,\ \times,\ /)$ over a field

Field: examples

- $\{R, +, \times\}$, where R is the set of reals
- $\{Q, +, \times\}$, where Q is the set of rationals
- $\{Z_p, +, \times\}$, where p is prime and operators are mod p
  - $-a = p - a$ $Z_p = \{0, 1, 2, 3, \cdots, p-1\}$
  - $a^{-1}, 1 \leq a < \mathrm{p}$
    - Use extended Euclidean algorithm to compute integral (x, y) for $xa + yp = 1$
    - $a^{-1} = x \bmod p$
  - Additive identity: 0
  - Multiplicative identity: 1

Field: types


Fields
Fields with an infinite number of elements
Finite fields
Galois fields
C, R, Q
GF(p) Finite fields with p elements
GF(p^n) Finite fields with p^n elements

Finite Field: GF(p^n)

- Evariste Galois (1811-1832) first studied finite fields
- Finite fields play crucial role in AES and many cryptosystems
- Every finite field F must have p^n elements for some prime p and $n \geq 1$
- For every prime p and $n \geq 1$, there is a finite field of p^n elements
- F of p^n elements may have different forms. Nevertheless, they are all isomorphic
  - Thus, $GF(p^n)$ is the finite field of p^n elements

Finite Field: $GF(p), n = 1$

Finite Field: $GF(p), n = 1$

- $GF(p) = \{Z_p, +, \times\}$, where + and × under "mod p"
  - The finite filed of p elements $Z_p = \{0, 1, 2, \cdots, p-1\}$, => p elements
- Example $\{0,1\}$
  - $GF(2) = \{Z_2, \text{xor}, \text{and}\}$: Boolean algebra
  - $GF(7) = Z_7$

+	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

Ordinary polynomials: arithmetic

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

Polynomials over $GF(p)$

- A polynomial of degree n-1 over GF(p) is of form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

where each $a_i \in GF(p), 0 \leq i < n$

over GF(3)

$$
\begin{array}{r}
2x^3+x^2+x+1 \\
2x+1 \;)\; x^4+x^3+0+0+1 \\
x^4+2x^3 \\
0+2x^3+0+0+1 \\
2x^3+x^2 \\
2x^2+0+1 \\
2x^2+x \\
2x+1 \\
2x+1 \\
0
\end{array}
$$

- Polynomials over GF(2)
  - $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, \ldots$
- Addition over GF(2)
  - $(x^2+1)+(x^2+x) = 2x^2+x+1 = x+1$
- Multiplication over GF(2)
  - $(x^2+1)\times(x^2+1) = x^4+x^2+x^2+1 = x^4+1$

Polynomials over $GF(p)$ mod $m(x)$

- $f(x)$ mod $m(x) = r(x)$, where $\deg(r(x)) < \deg(m(x))$
  - $f(x) = q(x)m(x) + r(x)$
- Example over GF(2)
  - $f(x) = x^4 + x^2 + 1$
  - $m(x) = x^3 + x + 1$
  - $f(x) = x \cdot m(x) + (x + 1)$
- Simple way of computing $f(x)$ mod $m(x)$
  - Substitute $m(x) = 0$ to $f(x)$ and get $r(x)$
  - $m(x) = 0 \rightarrow x^3 = x + 1$
  - $f(x)$ mod $m(x) = x(x + 1) + x^2 + 1 = x + 1$

Irreducible polynomial over GF(p)

- $m(x)$ is $\boldsymbol{irreducible}$ if $m(x)$ cannot be factored into a product of two polynomials over $GF(p)$ of degree ≥ 1
- Example
  - $x^3 + x + 1$ is irreducible over $GF(2)$
  - $x^3 + x^2 + x + 1 = (x+1)^3$ is reducible over $GF(2)$
- Let $m(x)$ be degree-n irreducible polynomial over $GF(p)$ (prime in $\mathbb{Z}$)
  - $f(x)$ over $GF(p)$ with $\deg(f(x)) \leq n-1$
  - $\gcd(f(x), m(x)) = 1$ for $f(x) \neq 0$
  - $f^{-1}(x) \bmod m(x)$ exists for $f(x) \neq 0$
  - Use extended Euclidean algorithm to find $(a(x), b(x))$ for $a(x)f(x) + b(x)m(x) = 1 = \gcd(f(x), m(x))$
  - $f^{-1}(x) \bmod m(x) = a(x) \bmod m(x)$

$\mathbb{Z}_p$

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

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

- $GF(p^n)$ is the set of polynomials over $GF(p)$ of degree at most $n-1$
- $m(x)$ is an irreducible degree-n monic polynomial over $GF(p)$
- Coefficient operations are over $GF(p)$
- Multiplicative operations are "mod $m(x)$"
- Additive identity: 0
- Additive inverse: -f(x)
- Multiplicative identity: 1
- Multiplicative inverse: $f(x)^{-1}$ mod $m(x)$
- Closure, inverse, associative, commutative, and distributive rules are satisfied

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

- $S = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
- $m(x) = x^3 + x + 1$: irreducible over $GF(2)$

- $S = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
- $m(x) = x^3 + x + 1$: irreducible over $GF(2)$
- Example
  - $(x^2+1) + (x+1) = x^2 + x$
  - $(x^2+1) \times (x+1) \bmod m(x) = x^2$
  - $-(x^2+x) = x^2 + x$
  - $(x^2+x)^{-1} \bmod m(x) = x + 1$
  - $(x^2)^{-1} \bmod m(x) = x^2 + x + 1$

$x^3+x^2+x^2+x = x^3+x$

x^3+x^2+1

- $GF(2^3)/\ x^3+x+1$ and $GF(2^3)/\ \cancel{x^3+1}$ are isomorphic since x^3+x^2+1 is also irreducible over $GF(2)$

x^2 x 1

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

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
	$\times$	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	$x+1$

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

- $S = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$
- $m(x) = x^2 + 1$: irreducible over $GF(3)$
- Example
  - $(x+1) + (x+2) = 2x$
  - $(x+1) \times (x+2) \mod m(x) = 1$
  - $-(x+2) = 2x+1$
  - $(x+1)^{-1} \mod m(x) = x+2$
  - $(2x)^{-1} \mod m(x) = x$

+	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

×	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

$GF(2^n)/m(x)$: computaton

- Represent polynomial $f(x) = \sum_{i=0}^{n-1} b_i x^i$ as binary string $b_{n-1}b_{n-2}\cdots b_1 b_0$
- Addition: bitwise XOR (no need to carry)

		000	001	010	011	100	101	110	111
	+	0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

- Multiplication: Shift-XOR
  - long-hand multiplication, but from high bit to low bit
  - Example: 1001×1101 multiplier
    - Let $1101 = \mathrm{b}_3\mathrm{b}_2\mathrm{b}_1\mathrm{b}_0$
    - Initiation: $f = 0000\ 0000$
    - $b_3 = 1 \rightarrow f = \text{shift-left}(f) \oplus 1001 = 0000\ 1001$
    - $b_2 = 1 \rightarrow f = \text{shift-left}(f) \oplus 1001 = 0001\ 1011$
    - $b_1 = 0 \rightarrow f = \text{shif -left}(f) = 0011\ 0110$
    - $b_0 = 1 \rightarrow f = \text{shift-left}(f) \oplus 1001 = 0110\ 0101$

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

- Modular multiplication
  - Shift-XOR-Mod: like Shift-XOR, do modulo whenever necessary
  - $m(x) = x^8 + x^4 + x^3 + x + 1$ (binary: 1 0001 1011)
  - $a \times b = 3F \times 86 = 0011\ 1111 \times 1000\ 0110$

i	b_i	f: shift-XOR	f: mod g(x) --> bitwise XOR
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

Computation: table lookup

- $GF(2^8)$ / $x^8 + x^4 + x^3 + x + 1$
- Build a table for $a(x)b(x)$ mod $x^8 + x^4 + x^3 + x + 1$
- Table size: $2^8 \times 2^8 \times 2^8$ bits = 2^{16} bytes = 64K bytes

$(p^{n_1 n_2})$

Field: $GF(p^{n_1 \times n_2})/m_1(x), m_2(y)$

Field: $GF(p^{n_1 \times n_2})/m_1(x), m_2(y)$

- Consider degree-(n_2-1) polynomials of y over $GF(p^{n_1})/m_1(x)$
- Example
  - p $= 2, n_1 = 3,\ n_2 = 4$
  - $GF(p^{n_1})/m_1(x) = GF(2^3)/x^3 + x + 1$
  - A polynomial of the field is like : $(\mathrm{x}+1)y^3 + (\mathrm{x}^2)y^2 + 1$
- Let $m_2(y)$ be an irreducible degree-n_2 polynomial with coefficients over $GF(p^{n_1})/m_1(x)$
- $GF(p^{n_1 \times n_2})/m_1(x), m_2(y)$
  - The element set consists of all degree-(n_2-1) polynomials (of y) with coefficients over $G(p^{n_1})/m_1(x)$
  - Coefficients are operated over$G(p^{n_1})/m_1(x)$

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

$x\,(x)y+1$

Example: $GF(2^{3\times 4})/m_1(x), m_2(y)$

- $GF(2^{3\times 4})/x^3 + x + 1, y^4 + (x^2+1)y^2 + (x+1)$
- $m_2(y) = y^4 + (x^2+1)y^2 + (x+1)$ is irreducible over field

- $GF(2^{3\times4})/x^3+x+1, y^4+(x^2+1)y^2+(x+1)$
- $m_2(y) = y^4+(x^2+1)y^2+(x+1)$ is irreducible over field $GF(2^3)/x^3+x+1$

$=0 \Rightarrow y^4 = (x^2+1)y^2+(x+1)$

- Multiplication

$$[(x+1)y^3+xy^2+1)] \times [y+(x^2+1)] \bmod m_2(y)$$
$$= (x+1)y^4+[(x+1)(x^2+1)+x]y^3+[x(x^2+1)]y^2$$
$$+y+(x^2+1) \bmod m_2(y)$$
$$= (x+1)[(x^2+1)y^2+(x+1)]+(x^2+x)y^3+y^2$$
$$+y+(x^2+1) \bmod m_2(y)$$
$$= (x^2+x)y^3+(x^2+1)y^2+y+ \quad y^0$$

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

$= x^3+x^2+x+1+1$

$x+1$