# Fundamentals of Information & Network Security ECE 471/571


Lecture #13: Polynomial Arithmetic and Galois Field


Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

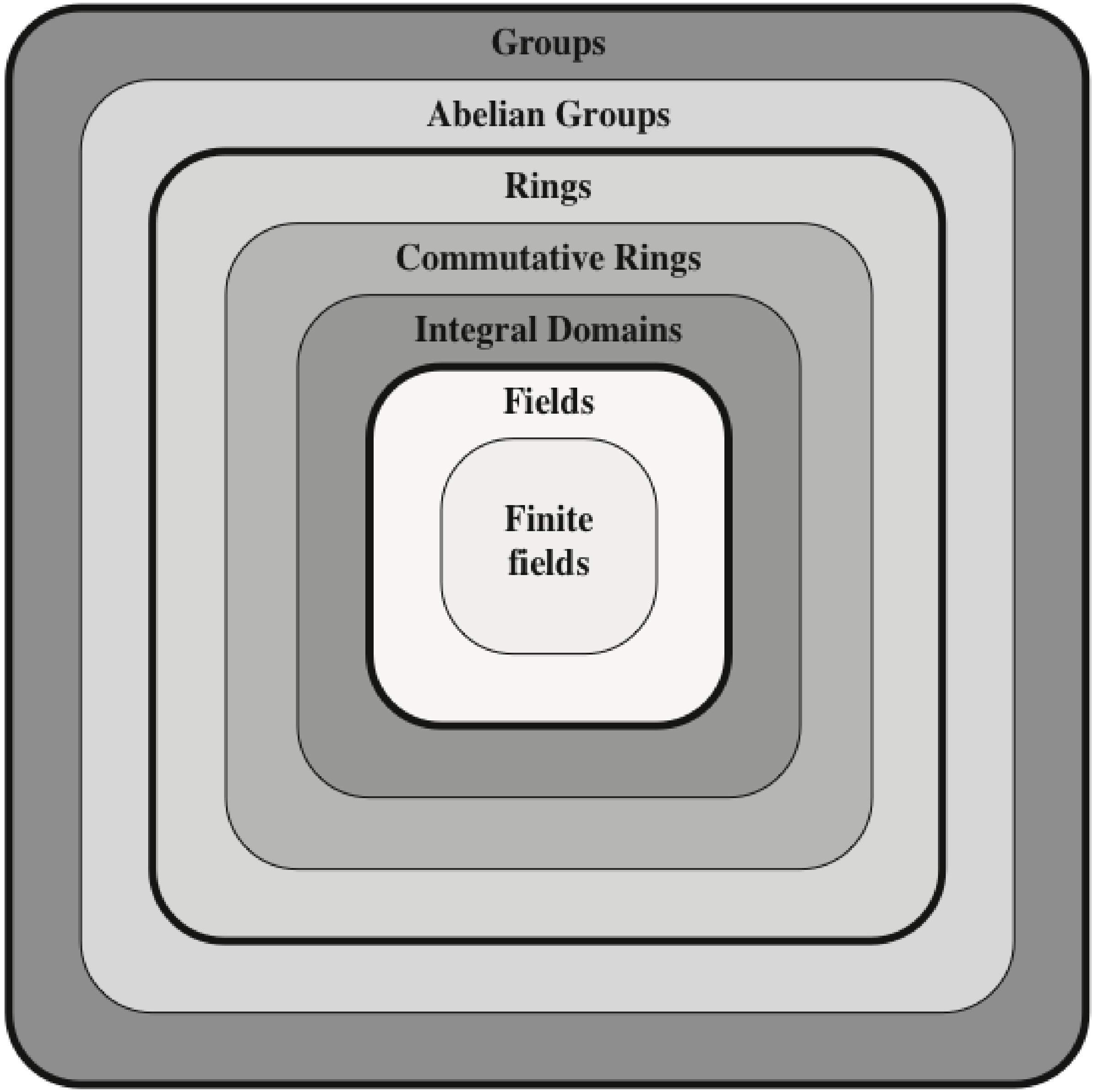
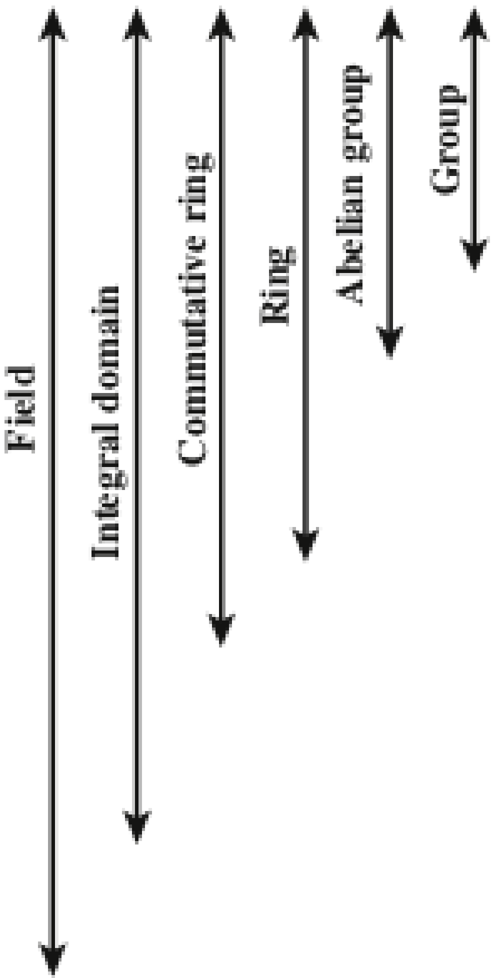



**Figure 5.1 Groups, Rings, and Fields**




| | |
|---|---|
| (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 $S$<br>$(a + b)c = ac + bc$ 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 $aa^{-1} = a^{-1}a = 1$ |

**Figure 5.2 Properties of Groups, Rings, and Fields**

# Fields

- A **field** *F* , sometimes denoted by {F, +,* }, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all *a, b, c* in *F* the following axioms are obeyed:

  **(A1–M6)**

  *F* is an integral domain; that is, *F* satisfies axioms A1 through A5 and M1 through M6

  **(M7) Multiplicative inverse:**

  For each $a$ in $F$, except 0, there is an element $a^{-1}$ in $F$ such that $aa^{-1} = (a^{-1})a = 1$

- In essence, a field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with the following rule: $a / b = a (b^{-1})$

Familiar examples of fields are the rational numbers, the real numbers, and the complex numbers. Note that the set of all integers is not a field, because not every element of the set has a multiplicative inverse.

# Types of Fields

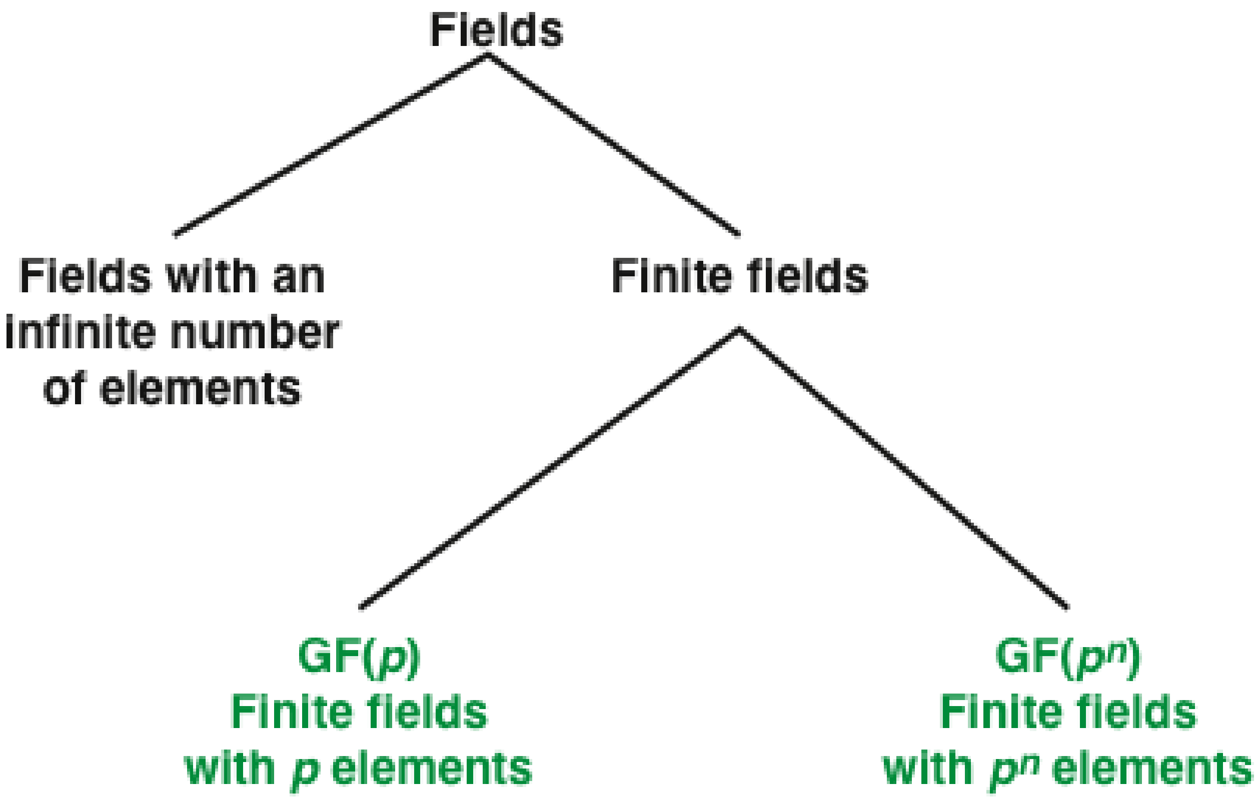



**Figure 5.3 Types of Fields**

# Addition modulo 8

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

# Multiplication modulo 8

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

# Additive and multiplicative inverses modulo 8

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 7 | 1 |
| 2 | 6 | — |
| 3 | 5 | 3 |
| 4 | 4 | — |
| 5 | 3 | 5 |
| 6 | 2 | — |
| 7 | 1 | 7 |

# Addition modulo 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 |

# Multiplication modulo 7

| × | 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 |

# Additive and multiplicative inverses modulo 7

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 6 | 1 |
| 2 | 5 | 4 |
| 3 | 4 | 5 |
| 4 | 3 | 2 |
| 5 | 2 | 3 |
| 6 | 1 | 6 |

# GF(p) is defined with the following properties

- 1. GF($p$) consists of $p$ elements
- 2. The binary operations + and * are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse
- We have shown that the elements of GF($p$) are the integers $\{0, 1, \ldots, p - 1\}$ and that the arithmetic operations are addition and multiplication mod $p$

# Treatment of Polynomials

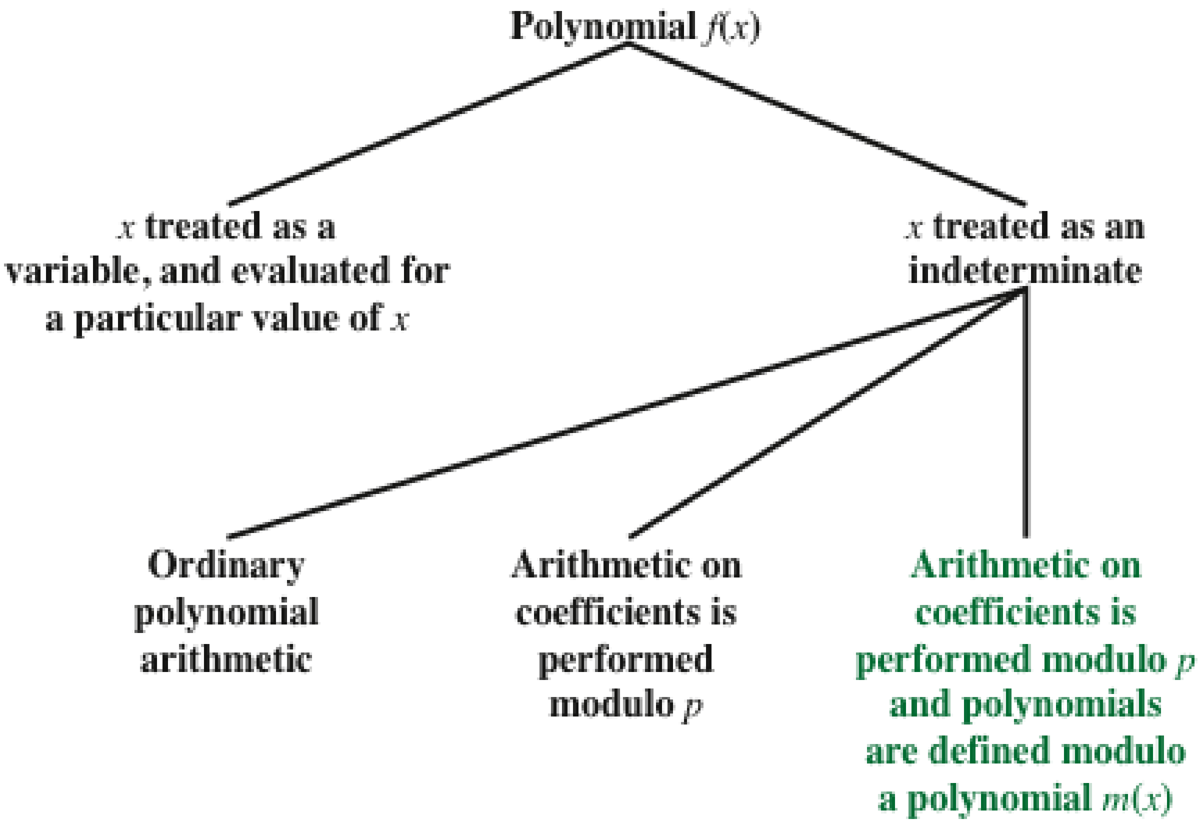



**Figure 5.4 Treatment of Polynomials**

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

**Figure 5.5 Examples of Polynomial Arithmetic**

# Polynomial Division

- Consider polynomials over the field F. The set of such polynomials is a ring (i.e., polynomial ring). Polynomial division is not necessarily exact

- We can write any polynomial in the form:

$$f(x) = q(x)\, g(x) + r(x)$$

  - *r(x)* can be interpreted as being a remainder
  - *So* $r(x) = f(x) \bmod g(x)$
- If there is no remainder we can say *g(x)* **divides** *f(x)*
  - Written as $g(x) \mid f(x)$
  - We can say that *g(x)* is a **factor** of *f(x)*
  - *Or* g(*x)* is a **divisor** of *f(x)*
- A polynomial *f(x)* over a field *F* is called **irreducible** if and only if *f(x)* cannot be expressed as a product of two polynomials, both over *F,* and both of degree lower than that of *f(x)*
  - An irreducible polynomial is also called a **prime polynomial**

# Example of Polynomial Arithmetic Over GF(2)

(Figure 5.6 can be found on page 137 in the textbook)

$$\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
+\,(x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4
\end{array}$$

(a) Addition

$$\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
-\,(x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4
\end{array}$$

(b) Subtraction

$$\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\times\,(x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4 + x^3 + x + 1 \\
x^8 + x^6 + x^5 + x^4 + x^2 + x \\
x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 \\
\hline
x^{10} + x^4 + x^2 + 1
\end{array}$$

(c) Multiplication

$$\begin{array}{r l}
 & x^4 + 1 \\
\cline{2-2}
x^3 + x + 1 \,\big) & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\
\cline{2-2}
\end{array}$$

(d) Division

Figure 5.6 Examples of Polynomial Arithmetic over GF(2)

# Polynomial Arithmetic Modulo ($x^3 + x + 1$)

| | + | 000<br>$0$ | 001<br>$1$ | 010<br>$x$ | 011<br>$x+1$ | 100<br>$x^2$ | 101<br>$x^2+1$ | 110<br>$x^2+x$ | 111<br>$x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|---|
| 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 | $x^2+x+1$ | $x^2+x+1$ | $x^2+x$ | $x^2+1$ | $x^2$ | $x+1$ | $x$ | $1$ | $0$ |

(a) Addition

| | × | 000<br>$0$ | 001<br>$1$ | 010<br>$x$ | 011<br>$x+1$ | 100<br>$x^2$ | 101<br>$x^2+1$ | 110<br>$x^2+x$ | 111<br>$x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|---|
| 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 | $x^2+x+1$ | $0$ | $x^2+x+1$ | $x^2+1$ | $x$ | $1$ | $x^2+x$ | $x^2$ | $x+1$ |

(b) Multiplication

# Arithmetic in GF($2^3$)

| | | 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 |

(a) Addition

# Arithmetic in GF($2^3$)

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

(b) Multiplication

# Arithmetic in GF($2^3$)

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 1 | 1 |
| 2 | 2 | 5 |
| 3 | 3 | 6 |
| 4 | 4 | 7 |
| 5 | 5 | 2 |
| 6 | 6 | 3 |
| 7 | 7 | 4 |

(c) Additive and multiplicative inverses

# Computational Considerations

- Since coefficients are 0 or 1, they can represent any such polynomial as a bit string
- Addition becomes XOR of these bit strings
- Multiplication is shift and XOR
  - cf long-hand multiplication
- Modulo reduction is done by repeatedly substituting highest power with remainder of irreducible polynomial (also shift and XOR)