□ Finite Fields

Let $p(x)$ be a polynomial of degree n over F. Define

$$\begin{aligned} F[x]/(p(x)) &= \{f(x) \bmod p(x) \mid f(x) \in F[x]\} \\ &= \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in F \right\}. \end{aligned}$$

- Addition:

$$\sum_{i=0}^{n-1} a_i x^i + \sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^{n-1} (a_i + b_i) x^i.$$

- Multiplication:

$$\left(\sum_{i=0}^{n-1} a_i x^i \right) \left(\sum_{i=0}^{n-1} b_i x^i \right) = \sum_{i=0}^{n-1} c_i x^i \mod p(x).$$

Theorem 23 *The polynomials over F with addition and multiplication* $\bmod p(x)$ *form a ring, i.e., $F[x]/(p(x))$ is a ring.*

Proof: Exercise. (check the axioms of ring.) □

Note: The ring $F[x]/(p(x))$ is called the *ring of polynomials modulo $p(x)$ over F*.

Example: Let $p(x) = x^3 + 1$ and $F = \mathbb{F}_2$. Then

$$F_2[x]/(x^3+1) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

$$\begin{aligned} x^2 \cdot (x^2+1) &= x^4 + x^2 \mod (x^3+1) \\ &= x(x^3+1) + x + x^2 \mod (x^3+1) \\ &= x^2 + x \mod (x^3+1) \end{aligned}$$

$$\begin{aligned} (x^2+x+1)(x+1) &= x^3 + x^2 + x + x^2 + x + 1 \mod (x^3+1) \\ &= x^3 + 1 \mod (x^3+1) \\ &= 0 \mod (x^3+1) \end{aligned}$$

Theorem 24 *The ring $F[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible (prime).*

Proof: ($\Leftarrow$) If $p(x)$ is irreducible, we must show that every element has an inverse under multiplication modulo $p(x)$. Let $a(x) \in F[x]/(p(x))$. Then we can assume WLOG that deg$a(x) <$ deg$p(x)$.

$\Rightarrow$ $(a(x), p(x)) = \alpha \in F$ since $p(x)$ is irreducible.

$\Rightarrow$ $1 = a(x)s(x) + p(x)t(x)$ for some $s(x), t(x) \in F[x]$.

$\Rightarrow$ $1 = a(x)s(x) \mod p(x)$.

$\Rightarrow$ $s(x)$ is the inverse of $a(x)$ under multiplication modulo $p(x)$.

($\Rightarrow$) If $p(x)$ is not irreducible, then

$$p(x) = a(x)b(x)$$

where deg$a(x) <$ deg$p(x)$ and deg$b(x) <$ deg$p(x)$. From the assumption, $a(x)$ has an inverse $a^{-1}(x)$ under multiplication modulo $p(x)$. Therefore,

$$\begin{aligned} b(x) &= b(x) \mod p(x) \\ &= a^{-1}(x)a(x)b(x) \mod p(x) \\ &= a^{-1}(x)p(x) \mod p(x) \\ &= 0 \mod p(x) \end{aligned}$$

which is a contradiction. □

Example: Irreducible and reducible polynomials over $\mathbb{F}_2$.

degree	irreducible	reducible
1	x $x+1$	
2	x^2+x+1	$x^2 = x \cdot x$ $x^2+1 = (x+1)(x+1)$ $x^2+x = x(x+1)$
3	x^3+x+1 x^3+x^2+1	x^3 $x^3+1 = (x+1)(x^2+x+1)$ $x^3+x = (x+1)^2 x$ $x^3+x^2 = x^2(x+1)$ $x^3+x^2+x = x(x^2+x+1)$ $x^3+x^2+x+1 = (x+1)^3$

Remark: Let $p(x) \in F[x]$, where deg $p(x) = m$.

1) $F(x)/(p(x))$ is an m-dimensional vector space over F, whose basis is given by

$$\{1, x, x^2, \cdots, x^{m-1}\}.$$

2) When $F = \mathbb{F}_q$,

$$\begin{aligned} |F(x)/(p(x))| &\triangleq \#\text{ of elements in } F(x)/(p(x)) \\ &= q^m. \end{aligned}$$

Corollary 25 *If there is an irreducible polynomial of degree m over $\mathbb{F}_q$, then there exists a finite field of order q^m.*

Example: Extension Field $\mathbb{F}_q = \mathrm{GF}(q)$

$$\begin{aligned} \mathrm{GF}(4) = \mathrm{GF}(2^2) &= \mathrm{GF}(2)[x]/(x^2+x+1), \\ \mathrm{GF}(8) = \mathrm{GF}(2^3) &= \mathrm{GF}(2)[x]/(x^3+x+1) \\ &\text{or } \mathrm{GF}(2)[x]/(x^3+x^2+1). \end{aligned}$$

Remark: Factorization of $x^{q^m} - x$ over $\mathbb{F}_q$

1) $x^{q^m} - x =$ product of all monic polynomials, irreducible over $\mathbb{F}_q$, whose degree divides m.

   Example: $q = 2$ case

$$\begin{aligned} x^{2^2} - x &= x(x-1)(x^2+x+1) \\ x^{2^3} - x &= x(x-1)(x^3+x+1)(x^3+x^2+1) \\ x^{2^4} - x &= x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1) \\ &\quad \cdot (x^4+x^3+x^2+x+1) \\ &\vdots \end{aligned}$$

2) $\mathbb{F}_{q^m} =$ the set of all roots of the polynomial $x^{q^m} - x$.

Theorem 26 *Let $I_q(k)$ be the number of all monic polynomials of degree k which are irreducible over $\mathbb{F}_q$. Then*

$$I_q(k) = \frac{1}{k}\sum_{d|k} \mu(d) q^{\frac{k}{d}}$$

where

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^r & \text{if } d \text{ is the product of } r \text{ distinct primes, i.e., } d = p_1 p_2 \cdots p_r, \\ 0 & \text{if } d \text{ contains any repeated prime.} \end{cases}$$

Remark:

1) $\mu(n)$ is called the *Möbius function* of n.
2) **Möbius inversion formula**: Let $f(n)$ and $g(n)$ be any two integer functions. If
$$f(n) = \sum_{d|n} g(d),$$
then
$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

Proof of Theorem 26:

$x^{q^m} - x =$ product of all monic polynomials, irreducible over $\mathbb{F}_q$, whose degree divides m.

$$\Rightarrow \qquad q^m = \sum_{d|m} d I_q(d).$$

By Möbius inversion formula,

$$m I_q(m) = \sum_{d|m} \mu(d) q^{\frac{m}{d}}.$$

□

Corollary 27 *For any q $(q > 1)$ and m,*

$$I_q(m) \geq 1.$$

Proof: Note that $\mu(d) \geq -1$ for any $d > 1$. Therefore,

$$\begin{aligned} I_q(m) &= \frac{1}{m}\sum_{d|m} \mu(d)\, q^{\frac{m}{d}} \\ &\geq \frac{1}{m}\left[q^m - \sum_{\substack{d|m\\ d>1}} q^{\frac{m}{d}}\right] \\ &> (q^m - q^{m-1} - \cdots - 1)/m \\ &\geq 0 \quad \text{(for any } q > 1.) \end{aligned}$$

□

Example: Number of irreducible polynomials over $\mathbb{F}_2$

$I_2(1) = 2^1;$ $\quad x, x+1$

$I_2(2) = \frac{1}{2}(2^2 - 1) = 1;$ $\quad x^2 + x + 1$

$I_2(3) = \frac{1}{3}(2^3 - 2) = 2;$ $\quad x^3 + x + 1, x^3 + x^2 + 1$

$I_2(4) = \frac{1}{4}(2^4 - 2^2 + 0) = 3;$ $\quad x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$

$I_2(5) = \frac{1}{5}(2^5 - 2) = 6$

$I_2(6) = \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9$

$\vdots$

$I_2(60) = 19,215,358,392,200,893.$ □

Theorem 28 *For any prime power q^m, there is one and only one finite field of order q^m up to isomorphism.*

Example: Consider the case $q = 2,\ m = 2$.

$$\mathsf{GF}(2^2) = \mathsf{GF}(4) \ \cong\ \mathsf{GF}(2)[x]/(p(x)) \triangleq \{0, 1, x, x+1\}$$

where $p(x) = x^2 + x + 1$.

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

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Example: $\mathsf{GF}(2^3) = \mathbb{F}_2[x]/(x^3 + x + 1)\ \Big(\cong \mathbb{F}_2[x]/(x^3 + x^2 + 1)\Big)$

$$\mathsf{GF}(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

$$\begin{aligned}(x^2+1)(x^2+x) &= x^4 + x^3 + x^2 + x \mod x^3 + x + 1 \\ &= x^2 + x + x^3 + x^2 + x \mod x^3 + x + 1 \\ &= x^3 \mod x^3 + x + 1\end{aligned}$$

Example: $\mathrm{GF}(16) = \mathbb{F}_{2^4}$ defined by $p(x) = x^4 + x + 1$.

log	multiplicative representation	additive representation	binary expression $x^3\ x^2\ x\ 1$
$-\infty$	0	0	0 0 0 0
0	$x^0 = 1$	1	0 0 0 1
1	x^1	x	0 0 1 0
2	x^2	x^2	0 1 0 0
3	x^3	x^3	1 0 0 0
4	x^4	$x + 1$	0 0 1 1
5	x^5	$x^2 + x$	0 1 1 0
6	x^6	$x^3 + x^2$	1 1 0 0
7	x^7	$x^4 + x^3 = x^3 + x + 1$	1 0 1 1
8	x^8	$x^4 + x^2 + x = x^2 + 1$	0 1 0 1
9	x^9	$x^3 + x$	1 0 1 0
10	x^{10}	$x^4 + x^2 = x^2 + x + 1$	0 1 1 1
11	x^{11}	$x^3 + x^2 + x$	1 1 1 0
12	x^{12}	$x^4 + x^3 + x^2 = x^3 + x^2 + x + 1$	1 1 1 1
13	x^{13}	$x^4 + x^3 + x^2 + x = x^3 + x^2 + 1$	1 1 0 1
14	x^{14}	$x^4 + x^3 + x = x^3 + 1$	1 0 0 1
	$x^{15} = 1$	$x^4 + x = 1$	

$$x^{15} + 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$
$$x^{15} = 1 \mod x^4 + x + 1.$$

Definition 29 A *primitive* element of $\mathbb{F}_q$ is an element α such that every nonzero field element can be expressed as a power of α (i.e., $\alpha^{q-1} = 1$, but $\alpha^s \neq 1$ for any positive integer $< q - 1$ or equivalently $o(\alpha) = q - 1$)

Example: (cont.) In $\mathbb{F}_{16}$, $x = \alpha$ is a primitive element.

Remark:

1) $\mathbb{F}_q =$ the set of all roots of $x^q - x$.

2) Let $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. Then

$$x^{q-1} - 1 = \prod_{\beta \in \mathbb{F}_q^*} (x - \beta).$$

Proof: $\mathbb{F}_q^*$ is a group of order $q-1$ under multiplication. Let $\beta \in \mathbb{F}_q^*$ and denote its order by $o(\beta)$. Then $o(\beta) \,|\, q-1$, so $q - 1 = o(\beta) \cdot l$. This implies that

$$\beta^{q-1} = \beta^{o(\beta)l} = \left(\beta^{o(\beta)}\right)^l = 1.$$

Therefore, β is a root of $x^{q-1} - 1$. □

Theorem 30 *In $\mathbb{F}_q$, there is a primitive element α of order $q-1$. In other words, $\mathbb{F}_q^*$ is a cyclic group.*

Proof: If $q-1$ is prime, then we are done, because every element except 0 and 1 has order $q-1$ and so primitive.

If $q-1$ is not prime, let $q - 1 = p_1^{\nu_1} p_2^{\nu_2} \cdots p_m^{\nu_m}$. For each i, $i = 1, 2, \ldots, m$, there are at most $\frac{q-1}{p_i}$ roots of the equation $x^{\frac{q-1}{p_i}} - 1 = 0$, since $\mathbb{F}_q$ is a field. Therefore, for each i, there exists $a_i \in \mathbb{F}_q$ such that

$$a_i^{\frac{q-1}{p_i}} \neq 1.$$

Let $b_i = a_i^{(q-1)/p_i^{\nu_i}}$ and $b = b_1 b_2 \cdots b_m$. By Claim 1 and Claim 2 in the following, $\alpha := b$ is an element of order $q-1$ in $\mathbb{F}_q$. Therefore, α is a primitive element in $\mathbb{F}_q$. □

Claim 1: $o(b_i) = p_i^{\nu_i}$ for each i.

(proof) Note that $b_i^{p_i^{\nu_i}} = a_i^{q-1} = 1$ for each i, since $\mathbb{F}_q^*$ is a group of order $q-1$ under multiplication. This means that $o(b_i) \,|\, p_i^{\nu_i}$, so $o(b_i) = p_i^{n_i}$ for some $n_i \leq \nu_i$. If $n_i < \nu_i$, then

$$b_i^{p_i^{\nu_i - 1}} = 1.$$