信息安全数学基础

1 原根与指标

1.1 原根

定义 1.1 (指数)**.** 设 $m \in \mathbb{Z}, m > 1, a \perp m$, 称使得

$$a^e \equiv 1 \pmod{m}$$

的最小正整数 e 为 a 模 m 的**指数** (阶), 记为 $\mathrm{ord}_m(a)$

定义 1.2 (原根)**.** 若 $\mathrm{ord}_m(a) = \varphi(m)$, 则 a 称为 m 的**原根**.

定理 1.1. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 整数 d 满足 $a^d \equiv 1 \pmod{m} \iff \mathrm{ord}_m(a) \mid d$.

根据这个定理, 指数一定是 $\varphi(m)$ 的因子, 只需要在这些数里面找就行了.

定理 1.2. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 如果 $n \mid m$, 则 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

定理 1.3. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 如果 $a \equiv b \pmod{m}$, 则 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

定理 1.4. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 如果 $ab \equiv 1 \pmod{m}$, 则 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

定理 1.5. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 则

$$a^0(=1), a^1, \cdots, a^{\mathrm{ord}_m(a)-1}$$

模 m 互不同余.

如果恰好 $\mathrm{ord}_m(a) = \varphi(m)$, 则 $a^0, a^1, \cdots, a^{\mathrm{ord}_m(a)-1}$ 构成一个简化剩余系.

定理 1.6. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. $a^k \equiv a^l \pmod{m} \iff k \equiv l \pmod{\mathrm{ord}_m(a)}$.

定理 1.7. 设 $m \in \mathbb{Z}(m > 1), a \perp m$, k 是非负整数. 则,

$$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), k)}$$

定理 1.8. 设 $m \in \mathbb{Z}(m > 1), k \in \mathbb{Z}^+$. a 是 m 的原根 $\iff \gcd(k, \varphi(m)) = 1$.

定理 1.9. 设 $m \in \mathbb{Z}(m > 1)$. 如果 m 有原根, 则原根个数是 $\varphi(\varphi(m))$.

定理 1.10. 设 $m \in \mathbb{Z}(m > 1), a \perp m, b \perp m$. 则,

$$\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \iff a \perp b.$$

定理 1.11. 设 $m \in \mathbb{Z}(m > 1), a \perp m, b \perp m$. 则 $\exists c$ 使得

$$\mathrm{ord}_m(c) = \mathrm{lcm}(\mathrm{ord}_m(a), \mathrm{ord}_m(b)).$$

更一般地, $\exists g$ 使得 $\mathrm{ord}_m(g) = \mathrm{lcm}(\mathrm{ord}_m(a_1), \cdots, \mathrm{ord}_m(a_k)), \quad 2 \le k \le \varphi(m)$.

定理 1.12. 设 $m,n\in\mathbb{Z}(m>1),a,m,n$ 两两互素. 则

$$\mathrm{ord}_{mn}(a)=\mathrm{lcm}(\mathrm{ord}_m(a),\mathrm{ord}_n(a)).$$

定理 1.13. 设 $m,n\in\mathbb{Z}(m>1,n>1,m\perp n),a_1\perp mn,a_2\perp mn$ 两两互素. 则 $\exists a$:

$$\mathrm{ord}_{mn}(a)=\mathrm{lcm}(\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_2)).$$

其中 a 是同余方程组 $x\equiv a_1\pmod m, x\equiv a_2\pmod n$ 的解.

定理 1.14. p 是素数 $\Longrightarrow$ p 有原根.

定理 1.15 (原根判定)**.** 设 p 是奇素数, $q_i(1\le i\le s)$ 都是 $p-1$ 的不同的素因数. 则 g 是模 p 原根 iff

$$g^{\frac{p-1}{q_i}}\neq 1\pmod p,\quad 1\le i\le s.$$

定理 1.16. 设 a,m,n 两两互素,

定理 1.17. 模 m 存在原根当且仅当 $m=1$ 或 2 或 4 或 p^α 或 $2p^\alpha$. 其中 α 是奇素数.

定理 1.18. g 是模 $p^{\alpha+1}$ 的原根 $\Longrightarrow$ g 是模 p^α 的原根. p 是奇素数.

定理 1.19. 如果 g 是 p^α 的原根, 则 $\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^\alpha)$ 或 $\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^{\alpha+1})$

定理 1.20. 设 g 是模奇素数 p 的原根, 且 g 满足 $g^{p-1}=1+rp$ 且 $p\nmid r$, 则 g 是模 p^α 的原根.

定理 1.21. 如果 g' 是模奇素数 p 的原根, 则 $g=g'+kp$ 都是 p 的原根.

通过原根找原根:

- p 为奇素数, 则模 p 的素数必然存在, 如 g.
- 可以构造一个模 p 的原根 $\tilde{g}$

1.2 指标

定义 1.3 (指标)**.** 对于整数 r 满足 $0<r\le\varphi(m)$, 如果

$$g^r\equiv a\pmod m$$

则称 r 为**以 g 为底的 a 模 m 的指标**. 记为 $\mathrm{ind}_g a$. 也可以称为**离散对数**, 记为 $\log_g a$.

定理 1.22 (指数-对数互换)**.** 设 m 是大于 1 的整数, g 是模 m 的原根. 如果 $g^s\equiv a\pmod m$, 则

$$s\equiv\mathrm{ind}_g a\pmod{\varphi(m)}$$

定理 1.23.

$$\mathrm{ind}_g(a_1\cdots a_n)=\mathrm{ind}_g a_1+\cdots+\mathrm{ind}_g a_n$$

定理 1.24. 设 g 是模 m 的原根. 在模 m 的简化剩余系中, 指数为 e 的整数个数为 $\varphi(e)$.

特别地: $(\mathbb{Z}/m\mathbb{Z})^*$ 的原根个数为 $\varphi(\varphi(m))$

定理 1.25 (n 次同余方程)**.**

2 素性检验

2.1 Fermat 伪素数

定义 2.1 (Fermat 伪素数)**.** 设 n 是一个奇合数, $b \in \mathbb{Z}^+, \gcd(b,n) = 1$ 且:

$$b^{n-1} \equiv 1 \pmod{n}$$

则称 n 是基于 b 的 Fermat 伪素数伪素数

定理 2.1 (Fermat 伪素数伪素数的性质)**.** 奇合数 n 是基于 b 的 Fermat 伪素数伪素数 iff

$$\mathrm{ord}_n(b) \mid (n-1)$$

定理 2.2 (Fermat 伪素数与模逆)**.** 奇合数 n 是基于 b 的 Fermat 伪素数伪素数 $\implies$ n 是基于 b^{-1} 的 Fermat 伪素数伪素数.

定理 2.3 (Fermat 伪素数与简化剩余系)**.** 假设奇合数 n 以及整数 $b, b \perp n$ 满足:

$$b^{n-1} \not\equiv 1 \pmod{n}$$

则在 $(\mathbb{Z}/n\mathbb{Z})^*$ 中至少有一半的元素满足

$$b_i^{n-1} \not\equiv 1 \pmod{n}$$

Fermat 素性检验 给定整数 $n \geq 3$ 以及安全参数 t.

- 随机选择 b 满足 $2 \leq b \leq n-2$ 以及 $b \perp n$.
- 计算 $r = b^{n-1} \pmod{n}$.
- 若 $r \neq 1$, 则 r 是合数.
- 上述步骤循环 t 次.

注: 每计算一次, r 是素数的概率就会降低 $\frac{1}{2}$. 计算一定次数之后就可以近似认为 r 是素数. 但是也存在一数 $b, b \perp n$ 满足 $b^{n-1} \equiv 1 \pmod{n}$ 但 n 仍然是合数. 这样的数字称为 Carmichael 数. 一旦出现这种数字, Fermat 素性检验将会失效.

2.2 Euler 伪素数

定义 2.2 (Euler 伪素数)**.** 设奇合数 n 满足 $\forall b \in Z$:

$$b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \pmod{n}$$

则称 n 为基于 b 的 Euler 伪素数.

定义 2.3 (Euler 伪素数的性质)**.** 如果 n 是基于 b 的 Euler 伪素数, 则 n 一定是基于 b 的 Fermat 伪素数.

Solovay-Stassen 素性检验 给定整数 $n \geq 3$ 以及安全参数 t.

- 随机选择 b 满足 $2 \leq b \leq n-2$ 以及 $b \perp n$.
- 计算 $r = b^{\frac{n-1}{2}} \pmod{n}$.
- 若 $r \neq \left(\frac{b}{n}\right)$, 则 r 是合数.
- 上述步骤循环 t 次.

注:*Euler 伪素数是 Fermat 伪素数的子集, 也就是说通过 Solovay-Stassen 素性检验得到的素数可信度更高.*

2.3 强伪素数

定义 2.4 (强伪素数)**.** 设奇合数 n, 且 $n-1 = 2^s \cdot t$. 如果以下任何一个同余方程成立

$$b^t \equiv 1 \pmod{n}$$
$$b^{2^i \cdot t} \equiv -1 \pmod{n}, \quad 0 \leq i < s$$

则称 n 为基于 b 的强伪素数.

定理 2.4 (强伪素数为什么是神)**.** n 是基于 b 的强伪素数 $\implies$ n 是基于 b 的 Euler 伪素数.

且 $\forall n$ 是 Carmichael 数 $\forall b(b \perp n) : n$ 不是基于 b 的强伪素数

Miller-Rabin 素性检验 给定整数 $n \geq 3$.

- 随机选择 b 满足 $2 \leq b \leq n-2$ 以及 $b \perp n$.
- 计算 $r_0 := b^t \pmod{n}$. 如果 $r_0 \neq \pm 1$, 则通过检验, 否则令 $i := 1$ 继续.
- 计算 $r_i := r_{i-1}^2$. 如果 $r_i \neq -1$, 则通过检验, 否则 $i := i+1$ 再来一次.
- 如果 $i = s$ 时算法仍未结束, 则判断不通过.

3 连分数

定义 3.1 (有限连分数)**.** 记形如

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots}}, \quad \text{最深处为} x_n$$

的数为 n 阶有限连分数. 简单记为

$$[x_0; x_1, x_2, \cdots, x_n]$$

如果 x_i 都为正整数, 则称为简单连分数.

$[x_0; x_1, x_2, \cdots, x_k] = \frac{P_k}{Q_k} = \theta_k$ 称为第 k 渐进连分数.

定义 3.2 (无限连分数)**.** 假设在上一个定义中的数列 $\{x\}$ 是无穷序列, 则称其为无限连分数, 记为:

$$[x_0; x_1, x_2, \cdots, x_l, \cdots]$$

如果 $\lim_{k\to\infty} \theta_k = \theta$ 则称这个连分数是收敛的, 否则称为发散的.

例 3.1. $\sqrt{2}$ *可以写为无穷连分数:*

$$\begin{aligned}
\sqrt{2} &= 1 + \frac{1}{2+\sqrt{2}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2+\sqrt{2}}} \\
&\cdots \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}} \\
&= [1; 2, 2, 2, \cdots]
\end{aligned}$$

实数的简单连分数构造法 给定实数 x.

- 令 $x_0 := \lfloor x \rfloor, r := x - x_0$
- 如果 $r = 0$, 则返回 $x = [x_0]$. 否则令 $x_1 := \lfloor \frac{1}{r} \rfloor, r := x_0 - x_1$.
- 如果 $r = 0$, 则返回 $x = [x_0; x_1]$. 否则令 $x_1 := \lfloor \frac{1}{r} \rfloor, r := x_1 - x_2$.
- ...
- 直到精度满足要求, 返回 $x = [x_0; x_1, \cdots, x_i]$.

定理 3.1. 有理数的简单连分数一定可以在有限步中计算出.

有理分数的简单连分数构造法 给定实数 x. 令 $x = \frac{p}{q}$ 是有理数. 对其使用 Euclid 除法即可得到有限简单连分数:

$$\frac{p}{q} = [\lfloor \frac{p}{q} \rfloor; \lfloor \frac{q}{r_0} \rfloor, \cdots, \lfloor \frac{r_{k-1}}{r_k} \rfloor]$$

定理 3.2 (有限简单连分数的唯一性)**.** 给定两个有限简单连分数 $[a_0; a_1, \cdots, a_m], [b_0; b_1, \cdots, b_n]$, 其中 $a_m \geq 2, b_n \geq 2$ 是整数. 如果 $[a_0; a_1, \cdots, a_m] = [b_0; b_1, \cdots, b_n]$ 则 $m = n$ 且 $\forall i \leq m : a_i = b_i$

定理 3.3 (连分数嵌套)**.**

$$[x_0; x_1 + \cdots + x_n + x_{n+1} + \cdots + x_{n+r}] = [x_0; x_1 + \cdots + x_n + [x_{n+1}; x_{n+2}, \cdots + x_{n+r}]]$$

定理 3.4 (加点料)**.**

$$[x_0; x_1 + \cdots + x_{2k}] < [x_0; x_1 + \cdots + x_{2k} + \eta]$$

$$[x_0; x_1 + \cdots + x_{2k-1}] > [x_0; x_1 + \cdots + x_{2k-1} + \eta]$$

$$\theta_{2k} < \theta_{2k+r} \quad (r \geq 1)$$

$$\theta_{2k-1} > \theta_{2k-1+r} \quad (r \geq 1)$$

奇数阶加料变小, 偶数阶加料变大.

定理 3.5 (计算渐进分数)**.** 连分数 θ 的渐进分数 $\frac{P_n}{Q_n}$ 满足:

$$P_n = x_n P_{n-1} + P_{n-2}, \quad Q_n = x_n Q_{n-1} + Q_{n-2}$$

注: 黄金分割可以用连分数表示.

$$\phi = \frac{\sqrt{5}+1}{2} = [1; \overline{1}]$$

定理 3.6.

$$\theta_0 < \theta_2 < \cdots < \theta_{2n} < \cdots < \theta_{2n+1} < \theta_{2n-1} < \cdots \theta_1$$

定理 3.7 (什么连分数会循环)**.** 有且只有正系数二次方程的实无理数根的连分数会循环.

定理 3.8 (实数的最佳逼近)**.** 对于实数 θ, 称有理数 $\frac{p}{q}$ 的最佳逼近, 当

$$\frac{p}{q} = \arg\min_r |\theta - r|$$

4 环

定理 4.1. 设 R 是有单位元的交换环, M 是 R 中极大理想的充要条件是: R/M 是域.

群 $(\mathbb{Z}_n, +_n)$ 的幂零元是什么?

$n = \prod p_i^{\alpha_i}$, 那么幂零元素就是

$$x = \prod p_i^w \quad \text{if} \quad w \neq 0$$

5 多项式环

定义 5.1 (多项式环)**.** 整数环、有理数域、实数域上的全体多项式构成的**多项式环**:

$$\mathbb{Z}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{Z}, n \geq 0\}$$

$$\mathbb{Q}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{Q}, n \geq 0\}$$

$$\mathbb{R}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{R}, n \geq 0\}$$

定义 5.2. 设 R 是一个整环. 系数取自 R 的全体多项式构成的集合:

$$R[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in R, n \geq 0\}$$

则称 $R[x]$ 是**多项式整环**.

定义 5.3. 设 $f(x), g(x)$ 是多项式整环 $R[x]$ 中的任意两个多项式, 其中 $g(x) \neq 0$. 如果存在多项式 $q(x)$ 使得等式

$$f(x) = q(x) \cdot g(x)$$

成立, 就称 $g(x)$ **整除** $f(x)$, 记为 $g(x) \mid f(x)$.

定义 5.4 (不可约多项式)**.** 设 $f(x)$ 是整环 R 上的非常数多项式. 如果除了平凡因式 $f(x)$ 以外, $f(x)$ 没有其他非常数多项式, 那么, $f(x)$ 就称为 **不可约多项式**; 否则称为可约多项式.

例子: $4x^2 + 4$ 是一个不可约多项式.

定理 5.1. 设 $f(x)$ 是域 K 上的次数为 n 的可约多项式, $p(x)$ 是 $f(x)$ 的次数最小的非常数因式. 则 $p(x)$ 一定是不可约多项式, 且

$$\deg p < \frac{1}{2} \deg f$$

定理 5.2. 设 $f(x)$ 是域 K 上的多项式, 如果 $\forall p(x)$ 满足 $\deg p < \frac{1}{2} \deg f$ 且 $p(x)$ 不可约, 都有: $p(x) \nmid f(x)$, 则 $f(x)$ 一定是不可约多项式.

例 5.1. $f(x) = x^8 + x^4 + x^3 + x + 1$ 是 $\mathbb{F}_2[x]$ 中的不可约多项式.

定义 5.5 (多项式的 Euclid 除法)**.** 给定整环上的多项式 $f(x), g(x) (\deg f \geq \deg g)$, 那么可以找到两个多项式 $q(x), r(x)$ 使得

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

且 $\deg r < \deg g$.

定义 5.6 (最大公因式, 最小公倍式)**.** 设 $f(x), g(x), d(x)$ 是整环 R 上的多项式. 称 $d(x)$ 是 $f(x), g(x)$ 的 **最大公因式**, 如果

$$d(x) \mid f(x), \quad d(x) \mid g(x)$$

并且 $\forall h(x) : h(x) \mid f(x), h(x) \mid g(x)$ 都有 $h(x) \mid d(x)$.

称 $m(x)$ 是 $f(x), g(x)$ 的 **最小公倍式**, 如果

$$f(x) \mid m(x), \quad g(x) \mid m(x)$$

并且 $\forall h(x) : f(x) \mid h(x), g(x) \mid h(x)$ 都有 $m(x) \mid h(x)$.

$d(x), m(x)$ 都可以记为 $\gcd(f(x), g(x)), \operatorname{lcm}(f(x), g(x))$.

定义 5.7 (多项式互素)**.** 设 $f(x), g(x), d(x)$ 是整环 R 上的多项式. 若 $\gcd(f(x), g(x)) = 1$, 则称 $f(x)$ 与 $g(x)$ 互素. 记为 $f(x) \perp g(x)$

定理 5.3 (多项式广义 Euclid 除法)**.** 设 $f(x), g(x), d(x)$ 是域 K 上的多项式. $\exists s_k(x), t_k(x)$ 使得

$$s_k(x)f(x) + t_k(x)g(x) = \gcd(f(x), g(x))$$

对于 $i = 0, 1, 2, \cdots, k$. $s_i(x), t_i(x)$ 归纳定义为:

$$\begin{cases} r_{-2}(x) = f(x), \quad r_{-1}(x) = g(x), \quad r_i = r_{i-2} \bmod r_{i-1} \\ q_i = \lfloor \frac{r_{i-2}}{r_{i-1}} \rfloor \\ s_{-2}(x) = 1, \quad s_{-1}(x) = 0, \quad s_i(x) = -q_i(x)s_{i-1} + s_{i-2} \\ t_{-2}(x) = 0, \quad s_{-1}(x) = 1, \quad t_i(x) = -q_i(x)t_{i-1} + t_{i-2} \end{cases}$$

还可以在域 K 上的多项式环 $K[x]$ 上完美复刻第二章关于同余的知识点.

定义 5.8 (多项式环的商环)**.** 设 $p(x)$ 是域 K 上的多项式环 $K[x]$ 中的一个多项式

定理 5.4. 设 $p(x)$ 是域 K 上的多项式环 $K[x]$ 的一个不可约多项式, 则 $K[x]$ 关于理想 $(p(x))$ 的商环 $K[x]/(p(x))$ 关于多项式模 $p(x)$ 加法以及模 $p(x)$ 乘法构成一个域.

定理 5.5 (有限域构造)**.** 设素数 p. $p(x)$ 是多项式环 $\mathbb{F}_p[x]$ 中的一个代数次数为 n 的不可约多项式, 则 $\mathbb{F}_p[x]$ 关于理想 $(p(x))$ 的商环 $\mathbb{F}_p[x]/(p(x))$ 满足:

$$\mathbb{F}_p[x]/(p(x)) = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 | a_i \in \mathbb{F}_p\}$$

一般记 $\mathbb{F}_p[x]/(p(x)) = \mathbb{F}_{p^n}$.

定义 5.9 (本原多项式)**.** 设素数 p. 设 $f(x)$ 是有限域 $\mathbb{F}_p$ 上的多项式环 $\mathbb{F}_p[x]$ 中的一个 n 次多项式. 使得

$$x^e \equiv 1 \pmod{f(x)}$$

成立的最小正整数 e 叫做 $f(x)$ 在有限域 $\mathbb{F}_p$ 上的指数. 记为 $\mathrm{ord}_p(f(x))$.

特别地, 如果 $\mathrm{ord}_p(f(x)) = p^n - 1$, 则称 $f(x)$ 为 $\mathbb{F}_p$ 上的本原多项式

例 5.2. 对于计算机最喜欢的 $\mathbb{F}_2 = (\{0,1\}, +_2, (\cdot)_2)$, 有一个本原多项式 $x^8 + x^4 + x^3 + x^2 + x$, 令

$$\mathbb{F}_{2^8} = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x^2 + x)$$

$\mathbb{F}$ 的本原元就是 $\mathbb{F}^*$ 的生成元.

定理 5.6 (**本原多项式的性质**)**.** 设素数 p, 设 $f(x), g(x) \in \mathbb{F}_p[x]$. 则有以下性质:

- 若整数 x^d 使得 $x^d \equiv 1 \pmod{f(x)}$, 则 $\mathrm{ord}_p(f(x)) \mid d$.
- 若 $g(x) \mid f(x)$, 则 $\mathrm{ord}_p(g(x)) \mid \mathrm{ord}_p(f(x))$.
- 如果 $\gcd(f(x), g(x)) = 1$, 则 $\mathrm{ord}_p(f(x) \cdot g(x)) = \mathrm{lcm}(\mathrm{ord}_p(f(x)), \mathrm{ord}_p(g(x)))$.
- 如果 $f(x)$ 是不可约多项式, 则 $\mathrm{ord}_p(f(x)) \mid p^n - 1$.
- $f(x)$ 是本原多项式 $\implies$ $f(x)$ 是不可约多项式.

定理 5.7 (**本原多项式判定**)**.** 设素数 p. 设 $f(x) \in \mathbb{F}_p[x], \deg f = n$. 如果 $x^{p^n-1} \equiv 1 \pmod{f(x)}$, 且对于 $p^n - 1$ 的所有不同素因数 q_i, 都有

$$x^{\frac{p^n-1}{q_i}} \neq 1 \pmod{f(x)}$$

则 $f(x)$ 是本原多项式.

6 域

定义 6.1 (线性空间)**.** 设非空集合 V, 数域 K. 在 K 与 V 之间定义数乘, 即 $\forall k \in K, \forall \alpha \in V$ 按照数乘法则唯一对应 V 中的一个元素 $k\alpha$. 如果 V 关于加法构成交换群, 且数乘满足线性空间的数乘公理

则称其为线性空间.

定义 6.2 (扩域)**.** 设 F 是一个域, 如果 K 是 F 的子域, 则称 F 是 K 的**扩域**.

定理 6.1 (扩域与线性空间)**.** 如果 F 是 K 的扩域, 则 F 是域 K 上的线性空间.

定义 6.3 (有限扩张)**.** 设 F 是 K 的扩域. 用 $[F:K]$ 表示 F 在 K 上的线性空间的维数. $[F:K]=n$ 表示存在线性无关的一组基底 $\beta_1,\cdots,\beta_n\in F$, $\forall\alpha\in V:\exists b_1,\cdots,b_n\in K$ s.t.

$$\alpha=b_1\beta_1+\cdots+b_n\beta_n$$

注: 如果 $[F:K]$ 是有限的, 则称 F 为 K 的有限扩域, 否则称无限扩域.

定理 6.2 (扩张次数)**.** 设 E 是 F 的扩域, F 是 K 的扩域, 则 $[E:K]=[E:F]\cdot[F:K]$.

注: 当且仅当 E 是 F 的有限扩域, F 是 K 的有限扩域时 E 是 K 的有限扩域.