抽象代数学

我们学习有限域的理论，它广泛应用于编码等理论。

定理1 设p是一个素数，$n\in\mathbb{N}$，$n\neq 0$. 则在同构意义下，有唯一一个阶数为p^n的有限域.

证明：令$\mathbb{F}=\mathbb{Z}_p$，$f(x)=x^{p^n}-x\in\mathbb{Z}_p[x]=\mathbb{F}[x]$，考虑$f(x)$在$\mathbb{F}$上分裂域$\mathbb{E}$. 因为$f(x)$在$\mathbb{E}[x]$中分裂，即$f(x)$在$\mathbb{E}$中恰有$p^n$个零点（包括重数），$f'(x)=-1$
即$(f(x),f'(x))=1$，因此$f(x)$在$\mathbb{E}$中零点均是单根，即p^n个零点互异. 这些零点包含$\mathbb{Z}_p$且关于$\mathbb{E}$中加、减、乘、除封闭，从而是$\mathbb{E}$的子域，但$\mathbb{E}$是包含零点的最小域，

$\Rightarrow$ 零点集合$=\mathbb{E}$；$|\mathbb{E}|=p^n$ （存在性证明）

设K是一个阶为p^n的域，则存在子域（即由"1"生成的最小子域）同构于$\mathbb{Z}_p$. $K^*=K\setminus\{0\}$是一个p^n-1阶循环群，且$\forall a\in K$，$a^{p^n}=a$，即K的全部元素是$f(x)=x^{p^n}-x$的根.

$\Rightarrow K$是$f(x)$在$\mathbb{Z}_p$上分裂域. 由分裂域唯一性，$K\simeq\mathbb{E}$.

（以上：唯一性证明）

由唯一性，可以记$GF(p^n)$表明p^n阶有限域. 意思是：p^n阶

由 扫描全能王 扫描创建

Galois域 (the Galois field of order p^n)

有限域的结构：

定理 作为一个加法群，$GF(p^n) \simeq \overbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}^{n个}$

考虑 $GF(p^n)^* = GF(p^n)\setminus\{0\}$，作为一个乘法群，它同构于 $\mathbb{Z}_{p^n-1}$

证明：$GF(p^n)$是一个有限Abel群，$\forall x \in GF(p^n)$，$px=0$

应用有限Abel群结构，$GF(p^n) \simeq \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

$GF(p^n)^*$是p^n-1阶循环群已在过去讲过，略.

注：$GF(p^n) \simeq \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$，右边不能看作$p^n$阶的域. 因为$(a_1, \cdots, a_n)$可能没有逆(例如某个$a_i=0$)

$\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$看作$\mathbb{Z}_p$上$n$维向量空间. $\{e_i=(0,\cdots,0,\underset{i\text{-th}}{1},0,\cdots,0) \mid i=1,\cdots,n\}$是一组标准基. 按这种看法，得

性质(1) $[GF(p^n):GF(p)]=n$ 这里$GF(p)=\mathbb{Z}_p$

(2) 设a是$GF(p^n)^*$的一个生成元，则a是$\mathbb{Z}_p=GF(p)$上的代数元，极小多项式是n次多项式.

证明：(2) $GF(p^n)$是$x^{p^n}-x$在$GF(p)$上分裂域. a是$GF(p^n)^*$的生成元，则$GF(p^n)=GF(p)(a) \Rightarrow [GF(p)(a):GF(p)]=n$.

由 扫描全能王 扫描创建

例 $p=2, n=4$ $GF(16)$ 设 a 是 $GF(16)^*$ 的生成元

$GF(p)(a)=\{c_0+c_1a+c_2a^2+c_3a^3 \mid c_0,c_1,c_2,c_3\in\mathbb{Z}_2\}$

因为 $[GF(p^n):GF(p)]=n$

因为 x^4+x+1 在 $\mathbb{Z}_2[x]$ 中不可约. 令 $g(x)=x^4+x+1$

则 $\dfrac{\mathbb{Z}_2[x]}{(g(x))}$ 是 $\mathbb{Z}_2$ 上 4 次扩域. 可以令 $a=x+(g(x))$

这样容易刻划 $GF(p)(a)$ 中乘法和加法, 例如:

$(a^3+a^2+a+1)(a^3+a)=a^6+a^4+a^5+a^3+a^4+a^2+a^3+a$

$=a^6+(a^4+a)+(a^5+a^2)+2a^3+a^4=a^6+(-1)+(-a)+2a^3+(-a-1)$

$=a^3-a^2-2a-2=a^3-a^2=a^3+a^2$

可以检验 $x^4+x+1=(x-a)(x-a^2)(x-a^4)(x-a^8)$ 在 $GF(16)[x]$ 中

有限域的子域

定理 对于 n 的任意因子 m, $GF(p^n)$ 有唯一一个阶为 p^m 的子域. 反之, $GF(p^n)$ 的任一子域均是这种形式.

证明: 设 $m|n$. 由 $p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\cdots+p^m+1)$

$\Rightarrow p^m-1 \mid p^n-1$ 令 $p^n-1=(p^m-1)t$, 设 $K=\{x\in GF(p^n) \mid x^{p^m}=x\}$

容易检查 K 是 $GF(p^n)$ 的子域. 因为 $x^{p^m}-x=0$ 至多在有 p^m 个零点 (在 $GF(p^n)$ 中) $\Rightarrow |K|\le p^m$, 另一方面, $GF(p^n)^*$ 是循环群, a 是一个生成元, 则 a^t 的阶为 p^m-1 $\Rightarrow a^t\in K$

由 扫描全能王 扫描创建

$\Rightarrow |K| = p^m$ (存在性), 因为 $x^{p^m} - x = 0$ 在 $GF(p^n)$ 中全部零点属于 K. 且设 L 是 $GF(p^n)$ 中阶为 p^m 的一个子域, $\forall x \in L$ $x^{p^m} = x$ (L^* 是 $p^m - 1$ 阶循环群) $\Rightarrow L = K$ (唯一性)

反之, 设 $\mathbb{F}$ 是 $GF(p^n)$ 的一个子域, 则 $\mathbb{F} \simeq GF(p^m)$, $\exists m$.

$$[GF(p^n):GF(p)] = [GF(p^n):GF(p^m)] \cdot [GF(p^m):GF(p)]$$

$\Rightarrow m \mid n$.

例 $GF(16)$ 有3个子域, 阶数 2, 4, 16

令 $GF(16) = \{0, 1 = x^0, x^1, x^2, \cdots, x^{14}\}$

$L_1 = \{0, 1\} \simeq \mathbb{Z}_2$

$L_2 = \{0, 1, x^5, x^{10}\}$ ~~$=\{0, 1, x$~~

$L_3 = GF(16)$

例 $GF(2^{24})$ 的子域