信息安全数学基础

第六章 有限域

聂旭云
信息与软件工程学院
电子科技大学

信息安全数学基础

有限域的定义

聂旭云
信息与软件工程学院
电子科技大学

什么是域

- F是一个非空集合，定义了加法、乘法两个二元运算，对这两个运算封闭
- 加法满足：对于任意a,b,c∈F
  - a+b=b+a；交换律
  - (a+b)+c=a+(b+c)；结合律
  - 存在0 ∈F，使得a+0=a；有零元
  - 存在-a ∈F，使得a+(-a)=0；有负元

加法交换群

- 乘法满足：对于任意a,b,c∈F
  - a·b=b·a；交换律
  - (a·b) ·c=a·(b·c)；结合律
  - 存在e ∈F，使得a·e=a；有单位元
  - 存在a^{-1} ∈F，使得$a \cdot a^{-1}$ =e；有逆元

非零元构成乘法交换群

- 乘法对加法满足分配率
  - a·(b+c)=a·b+a·c

域的例子：

有理数域Q

实数域R

复数域C

有限域的定义

- 定义6.1.1 一个有限域F是指只含有限个元素的域，F的阶是指F中元素的个数。有限域又称为Galois域。若域F的阶为n，则可将F记为F_n或GF(n)。

有限域的例子

- $Z_n=\{0,1,2,\ldots,n-1\}_{modn}$，加法和乘法都是模n的运算，运算封闭
- 加法满足结合律和交换律，有零元0，有负元
- 乘法满足结合律和交换律，有单位元1，不一定有逆元
- Z_n中的什么数才有乘法逆元呢？
- 引理：整数a在模n乘法下有逆元，当且仅当a与n互素。
- 所有与n互素的元素在模n乘法下构成乘法交换群
- 1,…,n-1都与n互素，则n为素数
- 对于任一素数p，Z_p为域，其元素个数为p个

有限域的例子

- $GF(2) = F_2$： {0, 1},
- 加法：0+0=1+1=0, 1+0=0+1=1;
- 乘法：0*0=0*1=1*0=0, 1*1=1

- $GF(7) = F_7$:
- {0, 1, 2, 3, 4, 5, 6}
- mod 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

加法表

*	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

乘法表

有限域的例子（续）

- $F[x]/(f(x))=\{r(x)=r_{n-1}x^{n-1}+r_{n-2}x^{n-2}+\cdots+r_1x+r_0|r_i\in F, 0\le i\le n-1\}$，加法和乘法都是模$f(x)$的运算，运算封闭
- 加法满足结合律和交换律，有零元0，有负元
- 乘法满足结合律和交换律，有单位元1，不一定有逆元
- $F[x]/(f(x))$中的多项式什么时候才有乘法逆元呢？

有限域的例子（续）

- 引理：r(x)在模f(x)乘法下有逆元，当且仅当r(x)与f(x)互素。
- 所有与f(x)互素的元素在模f(x)乘法下构成乘法交换群
- 次数比f(x)的次数低的多项式都与f(x)互素，则f(x)为不可约多项式
- 对于任一首项系数为1的不可约多项式，F[x]/(f(x))为域
- 若$F=Z_p$，则F[x]/(f(x))中元素个数为p^n个
- p^n域的构造方法是首先选取Z_p中的一个n次不可约多项式，然后构造集合

$$F[x]/(f(x))=\{r(x)=r_{n-1}x^{n-1}+r_{n-2}x^{n-2}+\ldots+r_1x+r_0 \mid r_i\in F,\ 0\le i\le n-1\}$$

集合中的加法和乘法运算为模多项式f(x)的运算

有限域的例子

- $GF(2^2)$：取$GF(2)$上2次不可约多项式$f(x)=x^2+x+1$
- $GF\left(2^2\right)=\{0,1,x,x+1\}$，定义运算为模$f(x)$下的加法和乘法

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

加法表

*	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

乘法表

有限域的例子（续）

- $GF(2^3)$：取$GF(2)$上3次不可约多项式$f(x) = x^3 + x + 1$
- $GF(2^3) = \{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}$，定义运算为模$f(x)$的加法和乘法。乘法表如下：

*	1	x	1+x	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
1	1	x	1+x	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
x	x	x^2	$x+x^2$	1+x	1	$1+x+x^2$	$1+x^2$
1+x	1+x	$x+x^2$	$1+x^2$	$1+x+x^2$	x^2	1	x
x^2	x^2	1+x	$1+x+x^2$	$x+x^2$	x	$1+x^2$	1
$1+x^2$	$1+x^2$	1	x^2	x	$1+x+x^2$	1+x	$x+x^2$
$x+x^2$	$x+x^2$	$1+x+x^2$	1	$1+x^2$	1+x	x	x^2
$1+x+x^2$	$1+x+x^2$	$1+x^2$	x	1	$x+x^2$	x^2	1+x

有限域的例子（续）

- $GF(3^2)$：取$GF(3)$上2次不可约多项式$f(x) = x^2 + 1$
- $GF(3^2) = \{0, 1, 2, x, 1 + x, 2 + x, 2x, 1 + 2x, 2 + 2x\}$，定义运算为模$f(x)$下的加法和乘法。加法表略，以下是乘法表：

*	1	2	x	1+x	2+x	2x	1+2x	2+2x
1	1	2	x	1+x	2+x	2x	1+2x	2+2x
2	2	1	2x	2+2x	1+2x	x	2+x	1+x
x	x	2x	2	2+x	2+2x	1	1+x	1+2x
1+x	1+x	2+2x	2+x	2x	1	1+2x	2	x
2+x	2+x	1+2x	2+2x	1	x	1+x	2x	2
2x	2x	x	1	1+2x	1+x	2	2+2x	2+x
1+2x	1+2x	2+x	1+x	2	2x	2+2x	x	1
2+2x	2+2x	1+x	1+2x	x	2	2+x	1	2x

素域与扩域

定义6.1.2 设F是域，K是F的子集。如果K在F的运算下也构成一个域，则称K为F的子域，称F为K的扩域。特别地，如果K≠F，则称K为F的真子域。一个域如果不包含真子域，则称该域为素域。

例6.1.1 有理数域和阶为素数p的有限域Z_p都是素域。

例6.1.2 $GF(2)$是$GF(2^2)=\{0,1,x,x+1\}$的子域。

例6.1.3 $GF(3)$是$GF(3^2)=\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$的子域。

向量空间（线性空间）

- 定义6.1.3 设F是一个域，V是一个加群，且集合F×V={ (a,v) | a∈F, v ∈ V}到V有一个映射，这一映射表示为 (a,v) → av ∈ V。假定映射满足下列条件，对每a,b ∈ F，u,v ∈ V有
  - （1）a(u+v)=au+av
  - （2）(a+b)v=av+bv
  - （3）a(bv)=(ab)v
  - （4）1v=v
- 则V称为域F上的向量空间。

若存在$v_1, v_2, \cdots, v_n \in V$使得对于任意$v \in V$都有$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$，其中$a_i \in F$，$1 \le i \le n$且$a_1v_1 + a_2v_2 + \cdots + a_nv_n = b_1v_1 + b_2v_2 + \cdots + b_nv_n$当且仅当$a_i = b_i$，$1 \le i \le n$，则称$V$为有限维向量空间，$v_1, v_2, \cdots, v_n \in V$称为$V$的一组基，$n$是$V$的维数。

域与扩域

- 定理 6.1.1 若E是F的扩域，则E是F上的向量空间。

- 定义 6.1.4 如果E作为F上的向量空间是有限维的，则称E为域F的有限扩域，E作为F上的向量空间的维数称为扩张次数，记为[E:F]

- 定义6.1.5 设F是一个域，E是F的扩域，S⊆E，将E中既包含F又包含S的最小子域记为F(S)，称之为由S生成的F的扩域。如果S仅含一个元α, 则称F(α)为F的单扩域。

感 谢 聆 听!

xynie@uestc.edu.cn