2022-2023学年秋季学期

课程名称：信息安全数学基础

英文名称：*Mathematical Foundations for Information Security*

授课团队：胡磊、许军、王丽萍

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 11 次课] 有限域

授课教师：许军

授课时间：2022年11月23日

概　要

- 有限域的结构
- 有限域的乘法群
- 有限域上元素的表示与运算

有限域

- 定义：一个有限域F是指只含有限个元素的域。有限域又称为Galois域。若域F的大小为q，则可将F记为F_q或GF(q)。

例：(1)整数模素数p剩余类环Z_p是有限域

(2) Z_p上多项式环$Z_p[x]$模Z_p上n次不可约多项式f(x)生成的理想(f(x))的商环是p^n个元素的有限域

断言：这些是全部的有限域！其中p可以是任意素数，n可以是任意正整数。

有限域结构的三个定理

- 定理： 设F是一个有限域，其特征为某个素数p，则F中的元素个数为p^n，n是一个正整数。

- 定理（存在性）： 对于任何素数p和任意正整数n，总存在一个有限域恰好含有p^n个元素。

- 定理（惟一性）：任意两个$q=p^n$元域都同构，即p^n元域在同构意义下是惟一的。

有限域的大小

- 定理： 设F是一个特征为素数p的有限域，则F中的元素个数为p^n，n是一个正整数。

证明：由于 F 的特征为 p，所以 F 包含 p 个元素的子集{1,2,...,p-1,p=0}，可验证这个子集是域 $GF(p)$。由于 F 是一个有限域，因此 F 是 $GF(p)$ 上的有限维向量空间，设其维数为 n，且 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 F 在 $GF(p)$ 上的一组基，则

$$F=\{a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n \mid a_i\in GF(p), i=1,2,\cdots,n\}$$

所以 F 中的元素个数为 p^n。

向量空间（线性空间）

- 定义： 设F是一个域，V是一个加群，且集合$F\times V=\{(a,v) \mid a\in F, v\in V\}$到V有一个映射，这一映射表示为$(a,v)\to av\in V$。假定映射满足下列条件，对每$a,b\in F$，$u,v\in V$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

- **用计数办法可证，一定存在Z_p上n次不可约多项式f(x)，因此，得到 p^n个元素的有限域 $Z_p[x]/(f(x))$ 。**
- 这是构造和表示非素数阶有限域的常见方法（多项式基方法），但是还有其他方法
- 例：构造 GF(4)、GF(8)、GF(9)
- 定理（惟一性）：任意两个$q=p^n$元域都同构，即p^n元域在同构意义下是惟一的。
- 理解同构和这个唯一性的例子： **$Z_2[y]/(y^4+y+1)$**的4元子域

$$\{0,\ 1,\ y^2+y,\ y^2+y+1\}$$

这里的y^2+y 和 y^2+y+1分别相对于 $Z_2[x]/(x^2+x+1)$ 中的 x 和x+1，或 x+1 和 x

有限域的乘法群

定理： 设 F_q 是 q 元域，则其乘法群 F_q^* 是一个循环群。

证：与证明整数模p剩余类环的乘法群为循环群方法相同（只用到乘法群的阶的性质和域上多项式方程的根的个数不超过多项式次数的性质）。

本原元

- 定义：F_q^* 中的生成元成为F_q 的本原元。

根据定理，F_q 中的本原元有 $\varphi(q-1)$ 个。

例 6.2.1 x^2+x+1 是 F_2 上的不可约多项式，设 α 是 x^2+x+1 的根，则

$$F_2(\alpha)=\{0,1,\alpha,\alpha+1\}$$

又 $\alpha^2=\alpha+1$，$\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha=1$，所以 α 是 $F_2(\alpha)$ 的本原元。

有限域的子域

定理： 设 $q = p^n$，其中 p 是素数，n 是正整数，则有限域 F_q 的任意一个子域含有 p^m 个元素，其中 $m \mid n$；反之，对于任意正整数 m，若 $m \mid n$，则 F_q 含有惟一一个子域包含 p^m 个元素。

例： $F_{2^{30}}$ 域的子域完全由 30 的因子决定。30 的因子有 1，2，3，5，6，10，15，30。因此 $F_{2^{30}}$ 的子域有

$$F_2, F_{2^2}, F_{2^3}, F_{2^5}, F_{2^6}, F_{2^{10}}, F_{2^{15}}, F_{2^{30}}。$$

有限域上元素的表示

多项式表示法（常见方法）

- 例：给出有限域F_9的元素表示，并给出F_9的乘法表。

解： F_9 可以看成是 F_3 通过添加一个二次不可约多项式的根 α 得到的 2 次扩张。

$f(x)=x^2+1$ 是 F_3 上一个不可约多项式，设 α 是 $f(x)$ 的一个根，即 $f(\alpha)=\alpha^2+1=0$，则 $1,\alpha$ 是 F_9 在 F_3 上的一组基，从而，F_9 中的元素可以表示成 F_3 上 α 的次数小于 2 的多项式，即

$$F_9=\{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}$$

多项式表示法（续）

乘法表如下：

*	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	0	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	0	α	2α	2	$2+\alpha$	$2+2\alpha$	1	$1+\alpha$	$1+2\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	2α	1	$1+2\alpha$	2	α
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	1	α	$1+\alpha$	2α	2
2α	0	2α	α	1	$1+2\alpha$	$1+\alpha$	2	$2+2\alpha$	$2+\alpha$
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	2	2α	$2+2\alpha$	α	1
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	α	2	$2+\alpha$	1	2α

本原元表示法（离散对数表示法）

仅适用于很小的有限域

设ξ是F_q中的本原元，则$F_q=\{0,\xi,\xi^2,\cdots,\xi^{q-1}\}$。在本原元表示下，乘法很容易实现，但加法需要结合$F_q$的多项式表示或查表来计算。

例：设$F_9=F_3(\xi)$，其中ξ是F_9中的本原元，且ξ是多项式x^2+x+2的根，则有$F_9=\{0,\xi,\xi^2,\cdots,\xi^8\}$。注意到，若$\alpha^2+1=0$，则$\xi=1+\alpha$是多项式$x^2+x+2$的根，可建立对应关系：$\xi=1+\alpha$，$\xi^2=2\alpha$，$\xi^3=1+2\alpha$，$\xi^4=2$，$\xi^5=2+2\alpha$，$\xi^6=\alpha$，$\xi^7=2+\alpha$，$\xi^8=1$。

这样就可以很方面的计算F_9中的加法。

有限域中的运算

- 素域F_p中的加法和乘法可由第二章介绍的模整数的加法和乘法来实现。求逆运算也可由算法2.5.1来实现。
- 根据F_{p^n}中元素的多项式表示，F_{p^n}中元素的乘法和求逆运算都可以通过模F_p上的不可约多项式来实现。

设$f(x)$是F_p上的n次不可约多项式，取α为$f(x)$的根，设$g(\alpha), h(\alpha) \in F_{p^n}$，则$g(\alpha), h(\alpha)$乘积可以这样得出，先将$g(\alpha)h(\alpha)$按照一般的多项式乘法求积，再以$f(\alpha)$去除得出余式，余式即为所求。

元素求逆

- 扩展欧几里德算法
- 利用循环群的有限性和重复平方—乘法：$a^{q-1}=1$，$a^{-1}=a^{q-2}$

有限域运算举例

例 6.5.1 考察阶为16的有限域 F_{2^4} 。容易验证多项式 $f(x)=x^4+x+1$ 在 F_2 上不可约。设 α 是 $f(x)$ 的一个根。因此有限域 F_{2^4} 可以表示为 α 的所有 F_2 次数小于 4 的多项式集合，即

$$F_{2^4}=\{a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0 \,|\, a_i\in\{0,1\}\}$$

为方便起见，多项式 $a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$ 可以用长度为 4 的向量 $(a_3a_2a_1a_0)$ 表示，且

$$F_{2^4}=\{(a_3a_2a_1a_0) \,|\, a_i\in\{0,1\}\}$$

有限域运算举例（续）

- 域 F_{2^4} 中算术的一些例子：
- （1）域中元素相加，即为对应分量的简单相加，例如(1011)+(1001)=(0010)；
- （2）要将域中元素(1101)与(1001)相乘，将它们做多项式乘法，再模去$f(\alpha)$得到的乘积，取其余式：

$$(\alpha^3+\alpha^2+1)(\alpha^3+1)=\alpha^6+\alpha^5+\alpha^2+1$$

$$\equiv \alpha^3+\alpha^2+\alpha+1 (\mathrm{mod}\ f(\alpha))$$

- 因此(1101) ×(1001）=(1111)；
- （3）F_{2^4} 的乘法单位元是（0001）；
- （4）（1011）的逆元是（0101），因为：

$$(\alpha^3+\alpha+1)(\alpha^2+1)=\alpha^5+\alpha^2+\alpha+1$$

$$\equiv 1 (\mathrm{mod}\ f(x))$$

- 即(1011) × (0101)=(0001)。

GF(256)中运算

域 F_2 上的 8 次不可约多项式 $f(x)=x^8+x^6+x^5+x+1$，α 是 $f(x)$ 的一个根。因此有限域 F_{2^8} 可以表示为 α 的所有 F_2 次数小于 8 的多项式集合，即

$$F_{2^8}=\{a_7\alpha^7+a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0 \,|\, a_i\in\{0,1\}\}$$

定义一个由 $a_7a_6a_5a_4a_3a_2a_1a_0$ 组成的字节 a 可表示为系数为{0，1}的二进制多项式：

$$a_7\alpha^7+a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$$

GF(256)中运算

- 还可以将每个字节表示为一个16进制数，即每4比特表示一个16进制数，代表较高位的4比特的符号仍在左边。例如，01101011可表示为6B。
- 也可以用0-255这256个十进制整数来表示域 中的元素。
- 加法定义为二进制多项式的加法，且其系数模2
- 乘法定义为多项式的乘积模一个次数为8的不可约多项式 。
- 元素“02”是域 中的一个本原元。

乘法的两种方法

- 直接模多项式m(x)
  - 需要64个GF(2)上乘法以及模多项式运算
- 建立乘法表
  - 需要256×256字节（64K）的存储空间
- 建立指数对数表
  - 512个字节的存储，每次乘法仅需要查表3次和1次加法

指数对数表的建立

- 域GF(256)中的元素用0-255这256个十进制整数来表示

（1）将元素‘02’表示成为α，依次计算$\alpha^i \bmod(f(\alpha))$，$i=0,1,\cdots,254$，将所得结果转变为十进制数，设为$\beta_i$，$i=0,1,\cdots,254$；如下表所示：

（2）建表。第一行为$0,1,\cdots,254,255$，第二行元素依次为β_i，$i=0,1,\cdots,254$。

由于$\alpha^0 \equiv \alpha^{255} \bmod(f(\alpha))$，约定第 2 行，第 255 列元素为 0。

0	1	2	3	···	253	254	255
1	2	4	8	···	233	177	0

指数对数表的建立（续）

（3）按所建表的第二行元素的大小进行重排列，如下表所示：

255	0	1	197	…	72	230	104
0	1	2	3	…	253	254	255

（4）将（3）中表的第一行放在（2）中表的第三行，即

序号	0	1	2	3	…	253	254	255
$(02)^i$	1	2	4	8	…	233	177	0
$\log_{(02)} i$	255	0	1	197	…	72	230	104

指数对数表的使用

例 6.5.2 取 F_2 上的 8 次不可约多项式 $f(x)=x^8+x^6+x^5+x+1$

α 是 $f(x)$ 的一个根。试求 F_{2^8} 中元素 $\alpha+1$ 和

$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$ 的乘积，并计算 $\alpha+1$ 的逆元。

解：$\alpha+1$ 对应于“03”，$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$ 对应于“253”。通过查指数对数表可得 $03=(02)^{197}$，$253=(02)^{72}$，因此，

$$(03)\cdot(253)=(02)^{197+72(\mathrm{mod}\,255)}=(02)^{14}=100。$$

“100”对应于 $\alpha^6+\alpha^5+\alpha^2$，即

$$(\alpha+1)(\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1)\equiv(\alpha^6+\alpha^5+\alpha^2)(\mathrm{mod}\,f(\alpha))$$

由 $03=(02)^{197}$，而 $255-197=58$，所以 $(03)^{-1}=(02)^{58}=222$。

“222”对应于

$$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha\ ,$$

即 $(\alpha+1)^{-1}\equiv(\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha)\bmod(f(\alpha))$。

AES S-盒

S－盒有一个简单的数学描述。在有限域$GF(2^8)$上的字节$x_7x_6x_5x_4x_3x_2x_1x_0$的乘法逆可以表示为$y_7y_6y_5y_4y_3y_2y_1y_0$。假定字节00000000的逆为00000000，则通过S－盒的$x_7x_6x_5x_4x_3x_2x_1x_0$的值可以通过如下公式计算

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{bmatrix}。$$

例子3 有限域$GF(2^8)$上的字节 11001011的乘法逆为 00000100。

我们计算

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}。$$

这产生了字节 00011111 = 31。我们也可以查前面的 S－盒 表，行为1100 + 1 = 13，列为1011 + 1 = 12。我们得到的值也是 31。

表 1　AES 加密算法 S – 盒表(十六进制)

S	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	63	7c	77	7b	f2	6b
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	ca	82	c9	7d	fa	59
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	b2	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

x