现代密码学

Modern Cryptography

张方国

中山大学计算机学院

Office: Room 305, IM School Building

E-mail: isszhfg@mail.sysu.edu.cn

HomePage: https://cse.sysu.edu.cn/content/2460

第五讲 密码的数学基础(复习二)

- 群论基础
  定义，交换群，循环群， 子群，商群
- 环论
- 有限域

代数运算定律

- 假如◦是一个**A**×**A**到**A**的代数运算，我们就说，集合**A**对于代数运算◦来说是封闭的，也说◦是**A**的代数运算或二元运算。
- 一个集合**A**的代数运算◦适合结合律，假如对于**A**的任何三个元**a,b,c**来说，都有**(a ◦b) ◦c=a ◦(b ◦c)**
- 一个**A**×**A**到**D**的代数运算◦适合交换律，假如对于**A**的任何两个元**a,b**来说，都有**a ◦b= b◦a**
- 代数运算⊙ ⊕适合分配律，假如对于**B**的任何元素**b**，**A**的任何元素**a1,a2**来说，都有

  b ⊙(a1⊕a2）=（b ⊙ a1 ） ⊕ （b ⊙ a2 ）

  或者， **(a1⊕a2）⊙b =（ a1 ⊙ b） ⊕ （ a2 ⊙b ）**

群（Group）

群G，有时记做{**G, ◦**}，是定义了一个二元运算的非空集合，这个二元运算可表示为◦，**G**中的每一个序对(a,b)通过运算生成G中的元素(a◦b)，并满足以下公理：

- ①**封闭性：**如果a 和 b都属于G，则 (a◦b)也属于G 。
- ②**结合律成立：****a ◦(b◦c)=(a◦b)◦c**，对于**G**的任意三个元素都**a,b,c**成立
- ③**单位元：****G**里至少存在一个元素**e**，对于**G**的任何元**a**，都有**e◦a=a◦e=a**成立。
- ④**逆元：**对于**G**的每一个元素**a**，在**G**里至少存在一个元素**a’**，**使得a’◦a=a◦a’=e**成立。

例子9

1) 整数集在加法$+$下构成群，单位元$e=0$;

2) 有理数，实数，复数集在乘法$\times$下构成群；

3) 所有2×2矩阵在加法$+$下构成群，所有行列式不等于0的矩阵在乘法$\times$下构成群；

4) 集合$\{T, F\}$在逻辑异或XOR下构成群，单位元$e=F$，$T^{-1}=T$。

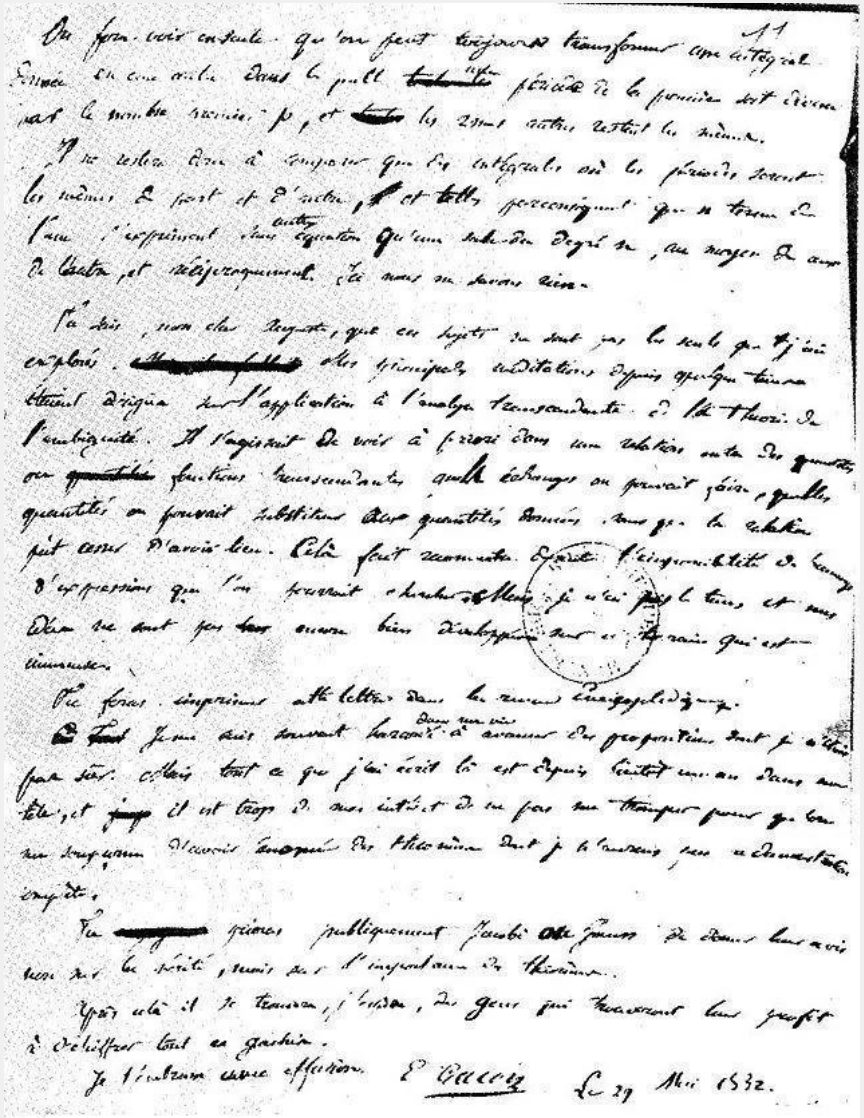
群论–近代代数学的基本概念之一

Hermann Weyl: "Galois' ideas, which for several decades remained a book with seven seals but later exerted a more and more profound influence upon the whole development of mathematics are contained in a farewell letter written to a friend on the eve of his death,which he met in a silly duel at the age of twenty-one. This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind."

伽罗瓦(1811-1832)

1829年 18岁 群论

伽罗瓦的手稿（1846年出版）



有关群的概念

- 一个群叫做有限群，假如这个群的元素个数是一个有限整数。否则，这个群叫做无限群。一个有限群的元素的个数叫做这个群的阶，用#G表示。
- 一个群叫做交换群（阿贝尔群），假如**a**。**b=b**。**a**，对于**G**里的任何两个元**a,b**都成立。
- 若一个群的每一个元素都是**G**的某一个固定元素**a**的乘方，我们把**G**叫做循环群，我们也说**G**是由元素**a**所生成的，并且用符号**G=**（**a**）来表示。**a**叫做**G**的一个生成元。

子群与Lagrange 定理

设G是一个群，若H是G的一个非空子集且同时H在和G一样的单位元与代数运算下是一个群，则H称为G的一个子群。

陪集： $a \circ H=\{a \circ h,\ h \in H\}$称$H$的一个陪集，这里 H 是 G的子群.

Lagrange 定理：#H |#G

商群： $G/H=\{a \circ H, a \in G\}$ $(a \circ H)*(b \circ H)=(a \circ b) \circ H$

恒等元 $e \circ H$

推论： 如果 H 是 有限群 G 的子群，则有

 # （G/H ）=#G / # H

群元素的阶

定义：$a \in G$, 满足 $a^i=e$ 的最小的正整数 i 称作 a 的阶, 记作 $ord(a)$.

Lagrange 推论：$ord(a) \mid \#G$

RSA： $a^{\varphi(N)}=1 \bmod N$,

这里， 群 Z_N^* 的阶是 $\varphi(N)$

循环群

定义：任意的 $b \in G$, 都存在$a \in G$ 和一个整数i，都有 $b=a^i$，我们把a 叫群的生成元。记$G=\langle a \rangle$.

Euler 函数 $\varphi(N)$：不超过N且和N互素的元素的个数。

定理：

1、循环群$G=\langle a \rangle$的任何子群都是循环群。

2、任意的d $|\#\langle a \rangle$ ， 都唯一存在一个阶为d的子群。

3、如果$\#\langle a \rangle=m$， 那么$\#\langle a^k \rangle=ord（a^k）=m/（k，m）$

4、任意$d |\#\langle a \rangle$ ， $\langle a \rangle$中存在$\varphi(d)$个阶为d 的元素。

5、如果$\#\langle a \rangle=m$，那么$\langle a \rangle$中有$\varphi(m)$个生成元。

6、素数阶的循环群的任何非恒等元都是生成元。

环

- 一个集合**R**叫做一个环，假如
- ① **R**对于一个叫做加法的代数运算作成一个交换群
- ② **R**对于一个叫做乘法的代数运算来说是封闭的
- ③ 这个乘法适合结合律**a(bc)=(ab)c**，对于属于**R**的任意的元素**a,b,c**都成立
- ④ 分配律成立，**a(b+c)=ab+ac**，**(b+c)a=ba+ca**
- 环**R**被称为含有单位元的环，是指**R**内含有乘法单位元“**1**”，使得$\forall a \in R$,有$a \cdot 1=1 \cdot a=a$。
- 我们同城考虑的环一般是有单位元的。无乘法单位元的的环一般记为Rng

环的定义也可以描述为：一个集合**R**叫做一个环，假如R对于加法构成一个交换群，对于乘法运算构成幺半群，乘法对加法满足左右分配律。

在抽象代数产生的19世纪，数学家们开始研究满足所有合成律（即加法交换律、结合律，乘法交换律、结合律，以及乘法对加法的分配律等等）或者满足其中的一部分的集合。倘若一个集合具有加法、乘法和相应的运算性质，就称为环。环论是抽象代数中较晚成熟的，20世纪以来环论得到了快速和广泛的发展。韦德伯恩研究了线性结合代数，这种代数实际上就是环，而环和理想的系统理论由诺特给出。

全体整数构成的集合对于普通加法和乘法来说作成一个环。

全体有理数构成的集合对于普通加法和乘法来说作成一个环。

n阶实方阵全体在矩阵的加和和乘法下构成一个环

交换环

- 一个环叫做一个交换环，假如**ab=ba**，对于属于**R**的任意两个元素**a,b**都成立。
- 剩余类环**Zn**。**Zn**为整数模**n**剩余类的集合**Zn={[0],[1],…,[n-1]},**它对剩余类的加法和乘法构成一个含有单位元“**[1]**”的交换环。
- 各式各样的数域都对通常的数的加法和乘法形成一个含有“**1**”的交换环
- 设**F**表示上面几个例子给出的任意一个数环。定义**F[x]={anx^{n}+an-1x^{n-1}+…+a1x+a0| ai∈F,n**为正整数**}**，它是**F**上的一元多项式环。
- 取大于**1**的正整数**n**，则**n**的一切整数倍形成的集合**nZ**对数的加法和乘法形成了一个不含单位元“**1**”的交换环。

整环

- 整环：含有乘法单位元“1”而无零因子的交换环称为整环。
- 若在一个环里，**a≠0，b ≠0但ab=0,**我们就说**a**是这个环的一个左零因子， **b**是这个环的一个右零因子。
- 任何一个整环都至少含有**2**个元素。恰含有**2**个元素的整环是存在的，例如**F2={0,1}**它对模**2**的加法乘法运算形成一个整环，事实上，它为二元域

定义 设 R与$\overline{R}$是两个环. 如果有一个R到 $\overline{R}$的映射φ满足

$$\varphi(a+b)=\varphi(a)+\varphi(b),$$

$$\varphi(ab)=\varphi(a)\varphi(b)\ \ (\forall a,b\in R)\ ,$$

则称φ是环 R到 $\overline{R}$ 的一个同态映射.

如果φ是满射(单射、双射), 则称 φ为环同态满射(环同态单射, 环同构). 特别 φ是环同态满射时, 则称R与$\overline{R}$同态, 记为$R\sim\overline{R}$.

域

- 除环：一个环被称为除环（或斜域），是指该环的非零元全体对“.”形成一个群。
- 域：一个可交换的除环称为域。
- **Fp**为整数模**p**的剩余类环，**p**为素数，可以验证它为域。因为**Fp**中的元素有限，称它为有限域；又因为**p**为素数，又称之为素域.
- 有理数域，实数域
- 域首先必是整环；反之则不然

有限域

- 一个元素个数有限的域称为有限域，或者伽罗华域（**Galois field**） 。
- 有限域中元素的个数为一个素数，或者一个素数的幂，记为**GF（p）**或**GF（p^n),**其中**p**为素数。
- 有限域中运算满足交换律、结合律、和分配律。
- 加法的单位元是**0,**乘法的单位元是**1**，每个非零元素都有一个唯一的乘法逆元。
- 密码学中用到很多有限域中的运算，因为可以保持数在有限的范围内，且不会有取整的误差。
- **– GF(p)**
- **– GF(2^n)**

有限域的结构

域F_p：用Z_P表示， p是一个素数。所有的素数P阶的域都同构于Z_P。

特征：任意的$a \in A$，满足 na=o的最小的自然数n 叫做A的特征。

定理：任何一个有限域都有一个素特征。

有限域的结构

任何一个有限域都可以表示成 GF(p)　或者 GF(p^n)，p是一个素数。 GF(p^n)叫做 GF(p)的 n 次扩域，它可以表示成定义在 GF(p)上一个 n 维的向量空间。

子域： GF(p^n)的子域只有GF(p^m)，m | n 。

Modular Polynomial Arithmetic

- can write any polynomial in the form:
  - $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if have no remainder say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- polynomial arithmetic modulo an irreducible polynomial with coefficients in the field Zp forms a field

Polynomial GCD

- can find greatest common divisor for polys
  - *c(x)* = GCD(*a(x)*, *b(x)*) if *c(x)* is the poly of greatest degree which divides both *a(x)*, *b(x)*
  - can adapt Euclid's Algorithm to find it:
  - EUCLID[*a*(*x*), *b*(*x*)]

1. A(*x*) = *a*(*x*); B(*x*) = *b*(*x*)
2. **2. if** B(*x*) = o **return** A(*x*) = gcd[*a*(*x*), *b*(*x*)]
3. R(*x*) = A(*x*) mod B(*x*)
4. A(*x*) ¨ B(*x*)
5. B(*x*) ¨ R(*x*)
6. **goto** 2

Polynomials over Z_p

- $Z_p[x]$ = polynomials on x with coefficients in Z_p.
  - Example of $Z_5[x]$: $f(x) = 3x^4 + 1x^3 + 4x^2 + 3$
  - $\deg(f(x)) = 4$ (the **degree** of the polynomial)
- Operations: (examples over $Z_5[x]$)
- Addition: $(x^3 + 4x^2 + 3) + (3x^2 + 1) = (x^3 + 2x^2 + 4)$
- Multiplication: $(x^3 + 3) * (3x^2 + 1) = 3x^5 + x^3 + 4x^2 + 3$
- $I_+ = 0$, $I_* = 1$
- + and * are associative and commutative
- Multiplication distributes and 0 cancels
- Do these polynomials form a field?

Galois Fields

- The polynomials $Z_p[x] \bmod p(x)$ Where $p(x) \in Z_p[x]$, $p(x)$ is irreducible, and $\deg(p(x)) = n$ (i.e., $n+1$ coefficients) **form a finite field.** Such a field has p^n elements.
- Proof:
- These fields are called **Galois Fields** or **GF(p^n).**
- The special case $n = 1$ reduces to the fields Z_p
- The multiplicative group of GF(p^n)/{o} is cyclic (this will be important later).

$GF(2^n)$

- **Hugely practical!**
- The coefficients are **bits** {0,1}.
- For example, the elements of $GF(2^8)$ can be represented as **a byte**, one bit for each term, and $GF(2^{64})$ as **a 64-bit word**.
  - *e.g.*, $x^6 + x^4 + x + 1 = 01010011$
- How do we do addition?

Addition over Z_2 corresponds to xor.

- Just take the xor of the bit-strings (bytes or words in practice). This is dirt cheap

Multiplication over GF(2^n)

- If n is small enough can use a table of all combinations.
- The size will be 2^n x 2^n (e.g. 64K for GF(2^8)).
- Otherwise, use standard shift and add (xor)

- **Note**: dividing through by the irreducible polynomial on an overflow by 1 term is simply a test and an xor.
- e.g. 0111 / 1001 = 0111
- 1011 / 1001 = 1011 xor 1001 = 0010

Finding inverses over GF(2^n)

- Again, if n is small just store in a table.
  - Table size is just 2^n.
- For larger n, use Euclid's algorithm.
- 费马小定理

有限域上不可约多项式

- 2次3次不可约多项式的判定
- 4次不可约多项式的判定
- 高次不可约多项式的判定，多项式分解

PETERSON'S TABLE OF IRREDUCIBLE POLYNOMIALS OVER GF(2)

- http://www.csee.umbc.edu/~lomonaco/f97/442/Peterson_Table.html

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

有限域的结构

定理：有限域的乘法群都是循环群。

本原根：有限域的乘法群的生成元。

随堂测试

- 设m=4,密钥流按照如下线性递归关系产生 $z_{i+4}=(z_i+z_{i+3}) \bmod 2$ $i>0$.
  若初始向量为(1,0,1,0)，请写出由它产生的一个周期的密钥流。
- 计算gcd(57,93)，并找出整数s和t，使得 $57s+93t=\gcd(57,93)$。
- 有限域$GF(2^5)$可以由$Z_2[x]/(x^5+x^2+1)$构造得到。在域中利用扩展欧几里得算法计算 $(x^3+x^2)^{-1}$