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 9 次课]　群

授课教师：许军

授课时间：2021年11月10日

概 要

- 二元运算、运算律
- 群的定义和简单性质
- 子群、陪集、拉格朗日定理
- 正规子群、商群
- 循环群

二元运算

- 定义： 设**A**为集合， 一个映射 $f: A \times A \to A$ 称为集合**A**上的二元代数运算。
- 一个集合**A**上的二元运算必须满足以下条件：
  - 可运算性，即**A**中的任何两个元素都可以进行这种运算；

$$f(x, y) = z$$

  - 单值性，即**A**中的任何两个元素的运算结果是惟一的；
  - 封闭性，即**A**中的任何两个元素运算的结果都属于**A**。
- 注：一个代数运算一般可用“。”、“·”、“+”、“×”符号来表示。

下面将集合**A**上的代数运算写成 $z = x \circ y$

- 例3.1.1（1）整数集合Z上的加法、减法运算是代数运算，满足代数运算的3个性质。
- （2）自然数集合N上的减法运算不是代数运算，因为它不满足封闭性。

定义：设“。”是A上的代数运算，如果对于A中的任意三个元素 *a*，*b*，*c*都有

$$(a \circ b) \circ c = a \circ (b \circ c)$$

则称“。”在集合A上满足结合律。

• 椭圆曲线的点加运算满足结合律（一个繁杂的证明）

因为实数域$\mathbf{R}$ 的特征不为2，3，所以实数域$\mathbf{R}$ 上椭圆曲线E 的Weierstrass 方程可设为

$$E:\ y^2 = x^3 + a_4 x + a_6,$$

其判别式$\Delta = -16(4a_4^3 + 27a_6^2) \neq 0$. E 在$\mathbf{R}$ 上的运算规则为:

设$P_1 = (x_1, y_1)$，$P_2 = (x_2, y_2)$是曲线E 上两个点, O 为无穷远点. 则

(1) $O + P_1 = P_1 + O$;

(2) $-P_1 = (x_1, -y_1)$;

(3) 如果$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \quad \begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + a_4}{2y_1} & \text{如果 } x_1 = x_2. \end{cases} \tag{10}$$

定义：设“ 。”是A上的代数运算，如果对于A中的任意两个元素a，b，都有

$$a \circ b = b \circ a$$

则称“ 。”在集合A上满足交换律。

例： 整数集合Z上的加法运算、乘法运算满足结合律和交换律。同样，整数模m剩余类环上的加法、乘法运算也满足结合律和交换律。

椭圆曲线的点加显然满足交换律。

不满足交换律的例子：域上一般方矩阵的乘法

但是，域上对角方矩阵的乘法又满足交换律

两个运算的联接：分配律

- 定义：设“。”和“+”是A上的两个代数运算，如果对于A中的任意三个元素*a*，*b*，*c*都有

$$a \circ (b + c) = a \circ b + a \circ c$$

$$(b + c) \circ a = b \circ a + c \circ a$$

则称“。”对“+”在集合A上分别满足左分配律、右分配律。我们习惯把“。”叫做乘法，“+”叫做加法。 在交换律下，左分配律＝右分配律

例： 整数集合Z上的乘法对加法满足分配律，而加法对乘法不满足分配律。

- 见惯了有结合律的代数运算，运算可能有交换律、也可能没有交换律
- 见过有交换律、没有结合律的代数运算吗？半域（semifield）的乘法！

群的定义

定义： 设 G 是具有一个代数运算 $\circ$ 的非空集合，并且满足：

I. **结合律：** $\forall a,b,c \in G$, 有
$$(a \circ b) \circ c = a \circ (b \circ c)$$

II. G 中有单位元 e：$\forall a \in G$, $e \circ a = a \circ e = a$

III. 对 G 中每一个元素 a，有逆元 $a^{-1} \in G$，使得 $a^{-1} \circ a = a \circ a^{-1} = e$

则称 G 关于代数运算 $\circ$ 构成一个群.

具有交换律的群称为交换群或**Abelian**群

可以证明：

- 群里单位元唯一
- 每个元素的逆元唯一
- 左、右消去律都成立：

  ab=ac 可推出 b=c

  ba=ca 可推出 b=c

  （省去乘法符号）
- $(ab)^{-1}=b^{-1}a^{-1}$

- 例3.2.1 （1）全体整数Z对于通常的加法成一个群，这个群称为整数加群，在整数加群中，单位元是0，a的逆元是-a；同样全体有理数集合Q，全体实数集合R，全体复数集合C对加法也构成群。

（2）全体非零实数 R^* 对于通常的乘法构成一个群，全体正实数 R^+ 对于通常的乘法也构成一个群。

（3）模正整数n的剩余类环系 Z_n，对于模n的加法构成一个群，这个群称为整数模n加群，其单位元为0，a 的逆元是 $n-a$。但是，Z_n 对于乘法不是一个群，要考虑它的既约剩余系才是乘法群。

Z_n 加群是“无用”的

- Z_n 上加法群是循环群，由1生成：a 等于a个1 相加。
- 设 g 与 n 互素，$gx = a \pmod n$ 对于任意 Z_n a有解，设解为b，则a 等于b个g 相加，也由 g 生成
- Z_n 上加法群的离散对数是很容易计算的
- 所以，剩余类环上，我们考虑乘法群上的离散对数

子群、陪集

- 定义3.3.1 如果群G的非空子集合H对于G中的运算也构成一个群，那么H称为G的子群，记为 H ≤ G。

- 在群G中，仅有单位元素构成的子集合{e}和G本身显然都是G的子群。这两个子群称为G的平凡子群，其余的子群称为非平凡子群。

子群的例子

- **整数m的所有倍数的集合 mZ** 是整数集 Z 的子群
- n 的所有倍数的剩余类的集合是 Z_m 的子群
  - ✓ 当n 整除 m 且 n 大于1时，是真子群
  - ✓ 当 n 与 m 互素时，为 Z_m 本身

陪集

- 定义：设H是群G的一个子群。对于G中的任意元素a，称集合

$$\{ah|h \in H\}$$

为H的一个左陪集，简记为 aH。因为H中有单位元素，所以 $a \in aH$ 。 aH 是包含a 的左陪集

- 同样可以定义右陪集为

$$Ha=\{ha|h \in H\}$$

- 对于有限群和任意元素$a \in G$， aH与H中有相同的元素个数。因为对于任意 $h_1, h_2 \in H$， 由 $ah_1 = ah_2$ 可推导出 $h_1 = h_2$
- **aH=bH** 等价于 **$b^{-1}a \in H$**
- 对交换群，**aH=Ha**, 左陪集和右陪集是一回事

群是子群陪集的无交并

- **定理： 设H是群G的一个子群。**

（1）H的任意两个左陪集或者相等或者不交

（2）群G可以表示成H的若干个不相交的左陪集之并。

（3）对右陪集亦有类似结论

证明思路：假设H的两个陪集有公共元素从而推导出这两个陪集相等。

证明

证明：***aH***和***bH***是两个左陪集。假如它们有公共元素，即存在 $h_1, h_2 \in H$，使得

$$ah_1 = bh_2$$

于是有 $a = bh_2h_1^{-1}$ ，其中 $h_2h_1^{-1} \in H$。由

$$ah = bh_2h_1^{-1}h \in bH$$

可知 $aH \subseteq bH$。同理可证，$bH \subseteq aH$，即有***aH=bH***
这就证明了第一个结论。

证明（续）

- 因为 $a \in aH$，所以

$$G = \bigcup_{a \in G} aH$$

- 把其中重复出现的左陪集去掉，即可得

$$G = \bigcup_{\alpha} a_{\alpha} H$$

例：设 H 是 m 的倍数的集合 mZ，则

Z = (0+ mZ)∪ (1+ mZ) ∪…∪ (m-1+ mZ)

指数

定义：群G关于子群H的左陪集的个数称为子群 H 在G中的指数，记为[G:H]。

拉格朗日定理：设群G是一个有限群，H是群G的一个子群，则H的阶|H|是群G的阶|G| 的因子，而且

$$\left|G\right| = \left|H\right|[G : H]$$

证明：设|G|=n ，|H|=m ，[G:H]=t。G可以表示成H的不相交的左陪集之并，即

$$G = a_1H \cup a_2H \cup \ldots \cup a_tH$$

又因为 $\left|a_iH\right| = \left|H\right| = m$，所以有 **n=mt**，即$\left|G\right| = \left|H\right|[G : H]$

元素的阶

- 群G中的任意一个元素 ***a*** 的全体方幂构成的集合 $\langle a\rangle = \{a^i \mid i \in Z\}$，对于群G中的乘法构成子群，这个子群**称为由*a*生成的子群**

定义: 对于群G当中的任一元素***a***，若存在正整数***k***，使得

$$a^k = e$$

那么，称满足上式的最小正整数***k***为元素***a***的阶，记为 $o(a)$ 。

等价地，***a***生成的子群的阶也为 ***o***(***a***)。

- **推论: 设G是一个有限群，则G中每一个元素的阶一定是|G|的因子。设 |G| = n，对于G中的每一个元素*a*，有** $a^n = e$

推论（欧拉定理）： 设m是正整数，$\varphi(m)$ **为m的欧拉函数，** $r \in Z_m$ **，若** $\gcd(r, m) = 1$ **，则**

$$r^{\varphi(m)} \equiv 1 (\bmod m)$$

证明：因为 $\left|Z_m^*\right| = \varphi(m)$ **，** $r \in Z_m^*$ **，根据推论，有**

$$r^{\varphi(m)} \equiv 1 (\bmod m)$$

商群

- 定义：设H是G的子群，记 $G/H = \{aH \mid a \in G\}$，在集合 G/H 上定义运算：

$$(aH)\cdot(bH) := (ab)H$$

- 这个定义有没有问题（是不是well defined）？
- 即若 $a'H = aH, b'H = bH$, 有没有 $a'b'H = abH$? 即希望有 $(ab)^{-1}(a'b') \in H$, 亦即 $b^{-1}(a^{-1}a')b(b^{-1}b') \in H$
- 已经有 $(b^{-1}b') \in H$ ，所以等价于要求 $b^{-1}(a^{-1}a')b \in H$
- 这就是说，对于 $(a^{-1}a') \in H$ 和任意的 b， 都要求有要求 $b^{-1}(a^{-1}a')b \in H$
- 这就是正规子群的定义

正规子群的定义

定义：设H是G的子群。若对任意的 $a \in G$，任意的 $h \in H$，均有 $a^{-1}ha \in H$，则 H称为G的正规子群。

（等价于保证上述定义的商集合运算不依赖陪集代表元的选择）

定理：若 H 是 G的正规子群，则 *G/H*在这个乘法下构成群，称为 G 对 H 的商群。

交换群的子群都是正规子群。

商群（例）

- **例3.4.2 对于正整数m，mZ是整数加法群Z的正规子群，其所有加法陪集为**

$$r + mZ = \{mk + r \mid k \in Z\}, 0 \le r < m$$

- **分别用[0]，[1]，…，[m-1]表示这m个陪集：**

$$Z / mZ = \{[0],[1],\cdots,[m-1]\}$$

- **定义加法:**

$$[a]+[b]=[a+b(\operatorname{mod} m)]$$

- **显然，在这个运算下， Z/(mZ)构成一个加群。由于[*a*] 又表示*a*这个整数所在的剩余类，因此， Z/(mZ) 又称为加法剩余类群。**

循环群

定义： 设G是一个群，若存在一个元素*a*，使得 $G=\langle a\rangle$ ，则称G为循环群，元素*a*称为G的生成元。

例：（1）整数加法群 Z 是循环群，其生成元为 1 或 -1。

（2）模整数m剩余类加群 Z_m 是循环群，其生成元为[1]。

乘法呢？模 m 既约剩余类乘法群是循环群的条件?

循环群的生成元

- 设 $G=\langle a\rangle$ 是n阶循环群，则群G中的元素都是 a^k的形式，其中 $0\le k\le n$ 。

定理： 设$G=\langle a\rangle$是n阶循环群，a^k是G的生成元的充要条件是 gcd(k,n)=1 。

引理 3.5.1 设a 是群 G 中的一个有限阶元素，$o(a)=n$ ，则对于任意正整数 m， $a^m=e$ 当且仅当$n\mid m$ 。

引理 3.5.2 设a 是群 G 中的一个有限阶元素，$o(a)=n$ ，则对于任意正整数k ， a^k 的阶为$\frac{n}{\gcd(k,n)}$。

循环群的子群

- n 阶循环群 $G=\{g, g^2, \ldots, g^{n-1}, g^n=1\}$的子群的阶 m 必整除 n （拉格朗日定理）
- 设 $n = md$
- m阶子群唯一存在，必为 $H_m=\{(g^d), (g^d)^2, \ldots, (g^d)^{m-1}, (g^d)^m=1\}$ 。因为其元素 g^i 的指数 i 必须是d 的倍数
- 阶为素数方幂之积（非素数）的循环群上离散对数的易解性分析