Lecture-2

近世代数

内容

- **Euclidean算法**
- 同余和剩余类
- 同态与同构
- 群
- 环
- 域
- 子群，正规子群，与商群
- 子格与划分

Euclidean 算法

- 最大公约数
  - 同时除尽 $a, b, \ldots, l$（不全为0）的最大正整数，记为 $(a, b, \ldots, l)$ 或 GCD $(a, b, \ldots, l)$
- 最小公倍数
  - 同时被 $a, b, \ldots, l$（不全为0）除尽的最小正整数，记为 $[a, b, \ldots, l]$ 或LCM $(a, b, \ldots, l)$
- **Euclidean除法**
  - 设b是正整数，则任意正整数 $a > b$皆可唯一地表示成

    $a = qb + r$，$0 <= r < b$ ➔ $(a, b) = (b, r)$ （证明见pp.18-19）
- **Euclidean算法**（证明见 p. 20）
  - ***对任意给定的正整数a, b,必存在整数A, B使 (a, b) = Aa+Bb***
- 性质：$ab=(a, b)[a, b]$（参见p. 22）

Euclidean 算法

- 例子：求 **[595, 493]**
  - 595 = 493 + 102　　493 = 102×4 + 85
  - 102 = 85 + 17　　85 = 17×5
  - (595, 493) = 17；　[595, 493] = (595×493)/17 = 17255

- 例子: **(595, 493)的Euclidean算法表示**
  - (595, 493) = 17
    = 102 - 85
    = 102 - (493 - 4×102)
    = 5×102 - 493
    = 5×(595 - 493) - 493
    = 5×595 + (-6)×493

同余和剩余类

- 同余
  - 若整数 a 和 b 被同一正整数 m 除时，有相同的余数，则称a、b关于模 m 同余，记为 $a \equiv b \pmod{m}$
  - 若$a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, 则
  - $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$, $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ （见p. 24）
- 剩余类
  - 给定正整数m，将全体整数按余数相同进行分类，可获得m个剩余类：

$$\overline{0}, \overline{1}, \ldots, \overline{m-1} \qquad \overline{a} + \overline{b} = \overline{a+b}, \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

- 例子
  - 25 ≡ 4 (mod 7); 12 ≡ 5 (mod 7); 25×12 = 300 ≡ 6 (mod 7)

    ≡ 4×5(mod 7)
  - m = 3 → $\overline{0} = \cdots, -3, 0, 3, \cdots$; $\overline{1} = \cdots, -2, 1, 4, \cdots$; $\overline{2} = \cdots, -1, 2, 5, \cdots$

映射

- **单值映射**
  - 设 A 和 B 是两个集合，如果存在某个对应法则f，使得对任一 $a \in A$，都能唯一确定一个元素 $b \in B$ 与之对应，则称 f 是 A 到 B 的一个单值映射。称 b 是 a 在 f 下的像，a 为原像。
- **满射**
  - 设 f 是集合 A 到集合 B 的单值映射，如果对任一 $b \in B$，必然存在有 $a \in A$，使得 $b = f(a)$，则称 f 是 A 到 B 的满射。
- **单射，双射**
  - 如果对集合A中不同的元素，在 f 之下在集合 B 中有不同的像，即当且仅当$a_1 = a_2$ 时，$f(a_1) = f(a_2)$，则称 f 是 A 到 B 的单射。如果 f 既是满射又是单射，就称为双射或一一映射。
- **变换**
  - 设 f 是集合 A 到 A 的映射，则称 f 是 A 中的变换。A 到 A 的满射称为满变换，单射称为单变换，一一映射称为一一变换或置换。如果变换保持 A 中的任一元素不变，则称为恒等变换或恒等置换。

同态与同构

- 代数系统
  - 满足一定规律或定律的系统称为代数系统。且有：
  1. 有一群元素构成一个集合；
  2. 在元素集合中有一个等价关系；
  3. 在集合中定义了一个或数个运算，通过运算建立起元素之间的关系；
  4. 有一组假定。

- 同态与同构：
  - 设f是代数系统 $(A, \cdot)$ 到 $(B, *)$ 的映射，如果它满足条件

$$f(a_1 \cdot a_2) = f(a_1) * f(a_2) \qquad a_1, a_2 \in A, \qquad f(a_1), f(a_2) \in B$$

则称 f 是 A 到 B 的同态映射，集合 A 与 B 同态。如果同态映射 f 又是双射，则称为同构映射，集合 A 与 B 同构。若 f 是 A 到 A 自身的同构映射，则称为自同构。

同态与同构

- 例子：
  - $(R,+)$ 和 $(R^+,\times)$，这里＋，×分别为数的加法和乘法。规定映射 $f: R \to R^+$ 为 $f(x) = 10^x$，则 f 是 $R \to R^+$ 的同构映射。
  - *Proof*：对于任何 $y \in R^+$，存在 $x = \lg y$ 使 $f(x) = y$，所以 f 是$R \to R^+$的满射；对任意的 x，$y \in R$，如果$10^x = 10^y$，得 $x = y$，所以 f 为 $R \to R^+$的单射。因此 f 是 $R \to R^+$的双射。又由于$f(x+y) = 10^{x+y} = 10^x \times 10^y = f(x) \times f(y)$，所以 f 是 R 到 R^+的同构映射。
  - 整数集合与剩余类集合之间仅是同态映射（See Slide-7）

同态与同构

- 设 (Z, +) 和 (A, ×), 这里A = {1, -1}, 规定映射*f*：Z→A为对任何*x*∈Z,

$$f(x)=\begin{cases}1, & \text{if } x \text{ is even (include negative even number)}\\ -1, & \text{if } x \text{ is odd (include negative odd number)}\end{cases}$$

证明： *f* 是 Z → A 的同态映射

➢ *Proof*： 对于任何*x*, *y* ∈Z

(1) 如果*x*, *y*都是偶数，则*f* (*x*) = 1, *f* (*y*) = 1，于是

$$f(x+y) = 1 = 1\times 1 = f(x)\times f(y)$$

(2) 如果 x, y都是奇数，则 *f* (*x*) = -1, *f* (*y*) = -1 ，于是

$$f(x+y) = 1 = (-1)\times(-1) = f(x)\times f(y)$$

(3) 如果 *x* 是奇数， *y* 是偶数，则 *f* (*x*) = -1, *f* (*y*) = 1，于是

$$f(x+y) = -1 = (-1)\times 1 = f(x)\times f(y)$$

同理可证： *x* 是偶数， *y* 是奇数时， $f(x+y) = f(x)\times f(y)$。

因此， *f* 是Z→A的同态映射。QED

同态与同构

- 设有理数集 **Q**，代数运算为数的加法，**Q*** 为非零有理数集，代数运算为数的乘法，证明: **(Q, +)** 与 **(Q*, ×)** 不存在同构映射。
  - Proof (反证法）：假定 Q → Q* 存在同构映射 f，并令$f(0) = x \in Q^*$。再令 $f(x) = x' \neq 0$，于是

$$f(0 + x) = f(0) \times f(x) = x \times x' \rightarrow f(x) = x \times x'$$

$$\rightarrow x' = x \times x' \rightarrow x = 1 \rightarrow f(0) = 1$$

但另一方面，设$f(a) = -1 \rightarrow f(a + a) = (-1) \times (-1) = 1$，但 $f(0) = 1$，所以 $a + a = 0 \rightarrow a = 0$，于是又有 $f(0) = -1$，这与 f 是Q → Q*的双射矛盾。因此，Q 与 Q*不存在同构映射。QED

群的定义

- 设 G 是一个非空集合，并在G内定义了一种代数运算 “ 。”，若满足：
  - 1) 封闭性：对任意 $a,b\in G$ ，恒有 $a\circ b\in G$
  - 2) 结合律：对任意 $a,b,c\in G$ ，恒有 $(a\circ b)\circ c=a\circ(b\circ c)$
  - 3) G 中存在一恒等元 e，对任意 $a\in G$ ，使 $a\circ e=e\circ a=a$
  - 4) 对任意 $a\in G$ ，存在a的逆元 $a^{-1}\in G$ ，使

$$a\circ a^{-1}=a^{-1}\circ a=e$$

- 则称 G 构成一个群。
  - 若加法，恒等元用 **0** 表示，
  - 若为乘法，恒等元 称为 单位元

群实例

- 例子
  - 全体整数：对加法构成群；对乘法不构成群
  - 全体偶数：对加法构成群；对乘法不构成群
  - 全体实数：对加法构成群；对乘法构成群（除**0**元素）
  - 全体复数：对加法构成群；对乘法构成群（除**0**元素）
  - 全体有理数：对加法构成群；对乘法构成群（除**0**元素）
  - 模***m***的全体剩余类 $\overline{0},\overline{1},\ldots,\overline{m-1}$ ：对模 ***m*** 加法构成群；对模 ***m*** 乘法，除**0**外，根据 ***m*** 值不同有不同的结论。如***m* = 4**时，剩余类 $\overline{2}$ 中的元素的逆元不存在。如对模 ***m* = 3** 乘法，除 **0** 外，剩余类全体构成群。

群实例

- **设G = {1, -1, i, -i}, ×为数的乘法，则 (G, ×) 是一个交换群。**
  - 因为，G中任意两个元的乘积还是G的一个元。于是，G在×下是封闭的。数的乘法总是满足结合律和交换律。G的单位元为1，且$(-1)^{-1} = -1$, $i^{-1} = -i$, $(-i)^{-1} = i$。

- **(S = {1, 2, 3, 4, 6, 12}, GCD) 是群吗？**
  - 任给$a, b, c \in S$, $GCD(a, b) \in S$, 所以 S 对 GCD 是封闭的。

    $$GCD[GCD(a, b), c] = GCD[a, GCD(b, c)]$$

    满足结合律。因为$GCD(12, a)=a$，所以 S 的单位元为12。因为

    $$GCD(1, a) = 1 \neq 12,$$

    所以 1 没有逆元。因此，(S, GCD) 不是群

群性质

- 群的恒等元、每个元素的逆元都是唯一的。
  - **Proof**：反证法, **p. 27**

- 若$a, b \in G$,则$(a \cdot b)^{-1}=b^{-1} \cdot a^{-1}$。
  - **Proof**：直接代换, **p. 27**

- 给定 **G** 中任意两个元素a和b，方程 $a \cdot x = b$ 和 $y \cdot a = b$ 在 **G** 中有唯一解：$x = a^{-1} \cdot b$，$y = b \cdot a^{-1}$

- 群 **G** 中消去律成立。即由 $a \cdot x = a \cdot y$ → $x = y$

群的相关概念

- 群的阶(Order of a Group)
  - 有限群(Finite Group)、无限群(Infinite Group)
- 加群、乘群
- 阿贝尔群(Abelian Group)、可换群、交换群：满足交换律
  - 所有*n*阶满秩矩阵的全体对矩阵乘法构成的群为非阿贝尔群
- 半群(Semigroup) (满足前两个条件)
  - 如正整数在加法运算下构成一个半群（无恒等元）
- 弱群(Monoid) (满足前三个条件)
  - 整数在乘法运算下构成一个Monoid（无逆元）
- 对称群(Symmetric Group)
  - 由*n*个元素构成的集合A到自身的所有*n*!个置换构成的集合在置换运算下构成对称群。

置换群

置换群(Permutation Group)

- 例子：A={1, 2, 3}

$$\varphi_1(1)=1 \quad \varphi_1(2)=2 \quad \varphi_1(3)=3$$
$$\varphi_2(1)=2 \quad \varphi_2(2)=3 \quad \varphi_2(3)=1$$
$$\varphi_3(1)=3 \quad \varphi_3(2)=1 \quad \varphi_3(3)=2$$

$$\varphi_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \quad \varphi_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \quad \varphi_3=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

$$\varphi_1=(1 \quad 2 \quad 3) \quad \varphi_2=(2 \quad 3 \quad 1) \quad \varphi_3=(3 \quad 1 \quad 2)$$

$$\varphi_2\circ\varphi_3=(2 \quad 3 \quad 1)\circ(3 \quad 1 \quad 2)=(1 \quad 2 \quad 3)=\varphi_1$$

φ_2,φ_3 互为逆元　　φ_1 为单位元

$\{\varphi_1,\ \varphi_2,\ \varphi_3\}$ 在置换运算下构成置换群

- 置换群不一定是对称群；对称群一定是置换群

环的定义

- 非空集合R中，若定义了两种代数运算加和乘，且满足：
  - 1) 集合R在加法运算下构成阿贝尔群
  - 2) 乘法有封闭性
  - 3) 乘法结合律成立，且加和乘之间有分配律
- 环＝阿贝尔加群＋乘法半群
- 例子
  - 全体整数；全体偶数；实系数多项式全体均构成环
  - 模整数 *m* 的全体剩余类构成剩余类环
- 相关概念
  - 有单位元环（乘法有单位元）
  - 交换环（乘法满足交换率）

环的相关概念

- 有零因子环
  - 对于环中的两个非零元素 a 和 b，若它们在环上定义的乘法运算下为零，即$ab = 0$，则 a、b 为零因子，对应的环为有零因子环。
  - 乘法消去率不成立
  - 例：Z_6：$2\times3 = 6 = 0 \pmod 6$; $2\times3 = 0\times3 \pmod 6$ but $2 \neq 0$
- 整环（交换律，单位元，无零因子环）
  - 例： Z
- 除环
  - 有单位元、每个非零元素有逆元，非可换的环
  - 例如所有 n 阶实数满秩矩阵全体和全零矩阵构成除环

环

- **$R=\{a+b5^{1/2} | a, b \in Z\}$关于数的加法和乘法是否构成环？**
  - 任给$p, q \in R$, $p=a_1+b_1 5^{1/2}$, $q=a_2+b_2 5^{1/2}$, $a_1, b_1 , a_2, b_2 \in Z$.

$$p+q = (a_1+b_1 5^{1/2})+(a_2+b_2 5^{1/2})$$

$$= (a_1+a_2) +(b_1+b_2) 5^{1/2} \in R$$

$$pq = (a_1+b_1 5^{1/2}) (a_2+b_2 5^{1/2})$$

$$= (a_1 a_2+5 b_1 b_2) +(a_1 b_2 + a_2 b_1) 5^{1/2} \in R$$

显然，(R, +)是加群， (R, ×)是半群且乘法对加法满足分配律，所以(R, +, ×)是环。

域

- 定义：非空集合 **F**，若 **F** 中定义了加和乘两种运算，且满足：
  - 1) F 关于加法构成阿贝尔群，加法恒等元记为 0
  - 2) F 中所有非零元素对乘法构成阿贝尔群，乘法恒等元记为 1
  - 3) 加法和乘法之间满足分配律
- 域是一个可换的、有单位元、非零元素有逆元的环，且域中一定无零因子。
- 有理数域；实数域；复数域。
- 元素个数无限的域称为无限域；元素个数有限的域称为有限域，用 **GF(*q*)** 或 F_q 表示 ***q*** 阶有限域。有限域也称为伽逻华域。

伽罗瓦

伽罗瓦使用群论的想法去讨论方程式的可解性，整套想法现称为伽罗瓦理论，是当代代数与数论的基本支柱之一。它直接推论的结果十分丰富：

- 它系统化地阐释了为何五次以上之方程式没有公式解，而四次以下有公式解。
- 他漂亮地证明高斯的论断：若用尺规作图能作出正 p 边形，p 为质数的充要条件为 $p=2^{2^n}+1$ （所以正十七边形可做图）。
- 他解决了古代三大作图问题中的两个：“不能任意三等分角”，“倍立方不可能”。

出生日期：1811年10月25日

逝世日期：1832年05月31日

阿贝尔

阿贝尔在数学方面的成就是多方面的：

- 证明了五次及五次以上的方程不能用公式求解 (鲁菲尼-阿贝尔定理)
- 研究了更广的一类代数方程，后人发现这是具有交换的伽罗瓦群的方程。为了纪念他，后人称交换群为阿贝尔群。
- 研究过无穷级数，得到了一些判别准则以及关于幂级数求和的定理。
- 阿贝尔和雅可比是公认的椭圆函数论的奠基者。

出生日期：1802年08月05日

逝世日期：1829年04月06日

域

- 设 ***p*** 为素数，则整数全体关于模 ***p*** 的剩余类 $\overline{0},\overline{1},\ldots,\overline{p-1}$ 在模 ***p*** 的运算下(模 ***p*** 加和乘)构成 ***p*** 阶域 **GF(*p*)**

  - *Proof*：(只需证非0元素有逆元）。其中 1 为单位元，因为 *p* 为素数，因此任意小于 *p* 的数 *a* 和 *p* 互素。所以由Euclidean算法可知：

$$(a, p) = 1 = Aa + Bp$$

在等式两边对*p*取模，则有

$$1 \equiv Aa \pmod{p}$$

所以剩余类中任一元素均有逆。Q.E.D.

域

- 设集$Q(2^{1/2}) = \{a+b2^{1/2} | a, b \in Q\}$，证明 $(Q(2^{1/2}), +, \times)$ 是域。

  - *Proof*：不难证明，$(Q(2^{1/2}), +, \times)$ 是交换环，单位元为1。并且，如果非零元$a + b2^{1/2} \in Q(2^{1/2})$，则 a，b 至少有一个不是零。 $a+b2^{1/2}$ 的逆元为

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{\left(a+b\sqrt{2}\right)\left(a-b\sqrt{2}\right)}$$

$$= \frac{a}{a^2-2b^2} - \frac{b\sqrt{2}}{a^2-2b^2} \in Q\left(\sqrt{2}\right)$$

因此， $(Q(2^{1/2}), +, \times)$是域。QED

子群

- 定义：
  - 若群 **G** 的非空子集 **H** 对于 **G** 中定义的代数运算也构成群，称 **H**为 **G** 的子群
  - 例如，偶数全体构成的群是全体整数构成的加群的一个子群
- 平凡子群（假子群）
  - 群本身和一个由恒等元所构成的群
- 真子群
  - 所有其他子群
- 群 **G** 的非空子集 **H** 为 **G** 的子群的充要条件　（证明见**p. 33**）
  - **1**）若 $a \in H$, $b \in H$, 则 $ab \in H$
  - **2**）若 $a \in H$, 则 a 的逆元 $a^{-1} \in H$

  或归纳为
  - 对任意的 $a, b \in H$, 恒有 $a^{-1}b \in H$

陪集

- 若 **H** 是 **G** 的子群，则可利用 **H** 把 **G** 划分等价类
  - 用$g_1, g_2, \ldots$表示群 **G** 中的元素，用$h_1, h_2, \ldots$表示子群 **H** 中的元素

$h_1 = e$	h_2	h_3	子群H
$g_1 h_1 = g_1$	$g_1 h_2$	$g_1 h_3$	左陪集
$g_2 h_1 = g_2$	$g_2 h_2$	$g_2 h_3$	左陪集
$g_3 h_1 = g_3$	$g_3 h_2$	$g_3 h_3$	左陪集

↑

陪集首

陪集

- 定义
  - H 是群 G 的一个子群，*g* 是 G 中的任意一个元素，将 *g* 左(右)乘 H 中的每一个元素，得到一个集合，记为 *g*H (H*g*)，该集合为子群 H 的一个左(右)陪集，*g* 为该陪集的陪集首。在Abel群中，*hg* = *gh*，左陪集等于右陪集
- 例：
  - 对整数全体，以*m*为倍数的整数全体是一个子群，可按此子群对全体整数划分陪集（见 pp. 33 - 34）
- 性质
  - 有限群 G 可以按子群 H 划分成有限个互不相交的陪集，且各陪集都具有相同的元素个数，即等于子群 H 的阶。（由定理 2. 4. 3 可得, p. 34）
  - 若按H划分得到 *j* 个陪集，则集合G中的所有元素都包括在其中，无一遗漏。即*N* = *jn*，N，*n* 分别为 G 和 H 的阶。（拉格朗日定理, p. 34 ）
  - 例如 m = 9 的剩余类全体对模 9 加法运算构成一个群，而 $\overline{0}, \overline{3}, \overline{6}$ 是它的一个子群，以此子群划分陪集

    H: $\overline{0}, \overline{3}, \overline{6}$;　　1+H: $\overline{1}, \overline{4}, \overline{7}$;　　2+H: $\overline{2}, \overline{5}, \overline{8}$

陪集

- 找出$C_{12}=\{e, g, \ldots, g^{11}\}$关于 $H=\{e, g^4, g^8\}$ 的所有右陪集。

  - $He=H$，取 $g\in C_{12}$，但 $g!\in H$，$Hg=\{g, g^5, g^9\}$。由于$H\cup Hg\neq C_{12}$，所以再取不属于$H\cup Hg$的 C_{12} 元素，如 g^2，则$Hg^2=\{g^2, g^6, g^{10}\}$，由于$H\cup Hg\cup Hg^2\neq C_{12}$，再取不属于 $H\cup Hg\cup Hg^2$ 的元素 g^3，则$Hg^3=\{g^3, g^7, g^{11}\}$。

$$H\cup Hg\cup Hg^2\cup Hg^3=C_{12}$$

于是C_{12}关于H的所有右陪集为 H，Hg，Hg^2，Hg^3。

正规子群

- 定义
  - 设 H 是 G 的一个子群，若对每一个 $a \in G$，恒有 $aH=Ha$，则称 H 是 G 的一个 正规子群 或 不变子群
  - Abel 群的每一个子群都是正规子群
- **H 是 G 的一个正规子群的充要条件**
  - 对每一个 $a \in G$，恒有 $a^{-1}ha \in H$, $h \in H$ (证明见 p. 35)
- **若 H 是 G 的正规子群，则 H 的全体陪集必构成群。**
  - **M 是以 *m* 的一切倍数所构成的一个正规子群。例如 *m* = 3,则全体整数按 3 的一切倍数构成的正规子群，进行如下划分**

$$\overline{0} = M = \cdots,-3,0,3,\cdots;\quad \overline{1} = M+1 = \cdots,-2,1,4,\cdots;\quad \overline{2} = M+2 = \cdots,-1,2,5,\cdots$$

  - **M 的 3 个陪集：$\overline{0}$, $\overline{1}$, $\overline{2}$ 关于剩余类加法构成群（见p. 36）**
- 商群
  - 定义：设 H 是 G 的正规子群，于是把 H 的全体陪集所构成的群成为 G 关于 H 的商群，记为 G/H。
  - 模 *m* 的剩余类群与商群 Z/M 同构。

正规子群

- 设 **H** 是群 **G** 的子群，且具有性质：**H** 的任意两个左陪集的乘积仍然是一个左陪集。证明：**H** 是 **G** 的一个正规子群。

➢ *Proof*：先证：两个左陪集$a\mathbf{H}$，$b\mathbf{H}$的乘积$(a\mathbf{H})(b\mathbf{H})$为$(ab)\mathbf{H}$。由题设$(a\mathbf{H})(b\mathbf{H})$是一个左陪集，记为$c\mathbf{H}$，即$(a\mathbf{H})(b\mathbf{H}) = c\mathbf{H}$，但$ab = (ae)(be) \in (a\mathbf{H})(b\mathbf{H})$，故$ab \in c\mathbf{H}$，于是$c\mathbf{H} = (ab)\mathbf{H}$。

下面证明：H是G的正规子群。任给$h \in \mathbf{H}$，$a \in \mathbf{G}$，

$a^{-1}ha\,h \in (a^{-1}\mathbf{H})(a\mathbf{H}) = (a^{-1}a)\mathbf{H} = \mathbf{H}$，于是$a^{-1}ha \in \mathbf{H}$。因此，**H**是**G**的正规子群。

QED