第一讲　课程简介与基础知识

周　晓　聪

中山大学计算机学院

2024年1月

isszxc@mail.sysu.edu.cn

邀请码 8103157

手机APP首页右上角输入

该邀请码2024年08月24日前有效

2022级代数结构韦宝典老师班级

保存图片

教学目标、教学内容、学习方法与考核

集合、关系与函数基本知识回顾

代数一般概念回顾

教学目标

知识性目标

- 在离散数学课程的基础上
  - 熟悉群、子群、正规子群及群同态的基本定理，了解群的应用
  - 熟悉环、子环、理想与商环的基本概念与性质，尤其是熟悉整环的性质
  - 了解域的扩张理论和有限域的构造与基本性质

能力性目标

- 提高理解能力、学习能力
  - 学会把握重点，学会归纳总结
- 培养计算思维
  - 探索如何利用计算机程序求解一些代数系统问题
- 锻炼逻辑思维能力
  - 学习构建数学证明的思路，让思维更有条理、更严谨、更周密

教学内容

群的基本理论

- 群与子群的基本概念
- 循环群、置换群与对称群
- 群的同构与群的同态基本定理
- 子群陪集、正规子群与商群
- 群的直积

深化群的认识，了解群更多例子与应用，锻炼抽象思维能力和逻辑证明能力

教学内容

环的基本理论

- 熟悉环的一般基础知识
  - 环的定义与基本性质
  - 理想、商环、素理想与极大理想、环的特征与素域
  - 环的同态
- 了解整环、域和除环的基础知识
  - 整环、域和除环的基本定义与基本性质
  - 多项式整环、整环的商域、唯一分解整环、主理想整环与欧几里得整环

教学内容

域扩张的基础知识

- 了解域的扩张的一些基础知识
  - 向量空间
  - 扩域
  - 代数扩张
  - 多项式的分裂域
  - 有限域

了解代数发展的历史，进一步培养抽象思维能力与科学探索精神

学习方法与课程考核

- 主要是学习幻灯片内容，并适当阅读补充材料
  - 韩士安编写的教材主要是面向数学专业学生
- 注意例题的讲解，认真完成习题
  - 尽量举例子，大家一起演绎基本定义与结果
  - 有时间可预习，并在复习后完成课后作业
  - 加入QQ群，有问题及时与老师一起讨论

课程考核

- 平时作业、课堂练习与平时出勤占40%
- 期末开卷考试占60%，笔试题目难度不超过讲义习题的难度

教学目标、教学内容、学习方法与考核

集合、关系与函数基本知识回顾

代数一般概念回顾

不严格定义的概念

- **集合**：作为整体研究的一堆东西，用大写字母$A, B, C, \cdots$表示
- **元素**：集合这一堆东西中的每一个，用小写字母$a, b, c, \cdots$表示
- **属于**：元素与集合间的关系，元素a属于集合A，记为$a \in A$；a不属于A，记为$a \notin A$。
  - 元素与集合间的属于关系也称为成员关系，元素是集合的成员
- **全集**：研究范围内的所有东西，记为U

用逻辑语言严格定义的概念

- **子集关系**：$A \subseteq B$当且仅当$\forall x(x \in A \to x \in B)$
- **集合相等**：$A = B$当且仅当$\forall x(x \in A \leftrightarrow x \in B)$
  - $A = B$当且仅当$A \subseteq B \land B \subseteq A$
- **空集$\emptyset$**：$\forall x(x \notin \emptyset)$

朴素集合论的外延原则

两个集合只要有完全相同的元素则是相等的集合，不考虑集合名字本身的内涵

- 概念(名字)的外延是它所指称的对象，内涵是它有区别于其他概念的属性全体
- 对于集合(名字)，外延是它包含的所有元素，内涵则视具体的应用而定

定义集合的方法有：元素枚举法、性质概括法和归纳定义法

元素枚举法

将集合的所有元素一一罗列出来

- 适合元素比较少，或可按明显规律罗列元素时定义集合
- 元素罗列规律明显时可使用省略号

归纳定义法

给出基本元素和从已有元素构造其他元素的规则

- 从某种意义上说，集合的归纳定义给出了构造集合元素的算法

性质概括法

用谓词概括一个集合的所有元素满足的共同性质

- 基本形式：$A = \{x \mid P(x)\}$，含义是$\forall x\big(x \in A \leftrightarrow P(x)\big)$
  - 允许P是任意性质时有可能产生悖论：罗素悖论
  - 公理集合论运用子集分离原则避免悖论：$A = \{x \in B \mid P(x)\}$，$B$是已知的大集合
- 扩展形式：$A = \{f(y) \mid P(y)\}$，含义是：
$$\forall x\Big(x \in A \leftrightarrow \exists y\big(x = f(y) \land P(y)\big)\Big)$$
  - 这里f是一个函数，或说$f(x)$是含有自由变量x的表达式

关系的定义

二元关系(binary relation)

集合A到B的二元关系R定义为笛卡尔积$A\times B$的子集，即$R\subseteq A\times B$

- 当$A=B$时，称$R\subseteq A\times A$为集合A上的二元关系
- 对于元素$a\in A, b\in B$，
  - 若$\langle a,b\rangle\in R$，则称a和b有关系R，有时简记为$a\,R\,b$
  - 若$\langle a,b\rangle\notin R$，则称$a$和$b$没有关系$R$，有时简记为$a\,\not R\,b$

一些特殊的关系（下面A,B是任意集合）

- 笛卡尔积$A\times B$的子集$\emptyset$称为空关系
- 笛卡尔积$A\times B$的子集$A\times B$称为全关系
- 笛卡尔积$A\times A$的子集$\Delta_A=\{\langle a,a\rangle\mid a\in A\}$称为$A$上的恒等关系，或对角关系

设$A=\{a,b,c,d\}$，则：
$\Delta_A=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle,\langle d,d\rangle\}$

等价关系、等价类与商集

非空集合A上的等价关系是集合A上同时满足自反性、对称性和传递性的关系

等价类(equivalence class)

设R是非空集合A上的等价关系

- $\forall a \in A$, a所在的R**等价类**，记为$[a]_R$, 定义为：
  $$[a]_R = \{b \in A \mid \langle a, b\rangle \in R\}$$
  - 即对任意$x \in A$，$x \in [a]_R$当且仅当$\langle a, x\rangle \in R$
  - A的每个元素所在的**等价类都是一个集合**

商集(quotient set)

设R是非空集合A上的等价关系

- R的所有等价类构成的集合称为A关于等价关系R的**商集**，记为A/R，即
  $$A/R = \{[a]_R \mid a \in A\}$$
  - 注意A/R是集合的集合，即**集合族**
  - 注意要剔除重复的等价类

集合的划分(partition)

设A是非空集合，$\mathcal{F}$是集合族，其中每个集合都是A的子集。说集合族$\mathcal{F}$是A的划分，如果：

- 非空：对任意的$S \in \mathcal{F}$有$S \neq \emptyset$
- 两两不交：对任意两个集合$S_1, S_2 \in \mathcal{F}$，$S_1 \cap S_2 = \emptyset$
- 覆盖集合A：$\bigcup \mathcal{F} = A$

非空集合A的划分$\mathcal{F}$中的每个集合称为这个划分的一个划分块(block)

非空集合A上的等价关系与它的划分有一一对应关系

A关于一个等价关系的商集是A的划分，而A的一个划分导出的“在同一划分块”关系是等价关系

- 进一步，A关于“在同一划分块”这个等价关系的商集就是这个划分，而A关于等价关系的商集作为A的划分所导出的“在同一划分块”关系就是这个等价关系本身

同余关系

设m是正整数（通常$m \geq 2$），在整数集$\mathbb{Z}$上定义关系R：$\forall a, b \in \mathbb{Z}$，$a\,R\,b$当且仅当$m \mid a-b$，则$R$是等价关系，$a\,R\,b$通常记为$a \equiv b \pmod{m}$，读做$a$与$b$模$m$同余，$R$称为**模$m$同余关系**，简称**同余关系**

- 对任意整数$a \in \mathbb{Z}$, a在R下的等价类$[a]_R$称为整数集$\mathbb{Z}$的一个（与a同余的）**模m剩余类**，并记为$\bar{a}$，商集$\mathbb{Z}/R$记为$\mathbb{Z}_m$

$$\bar{a} = \{\, x \in \mathbb{Z} \mid x \equiv a \pmod{m} \,\} = \{\, x \in \mathbb{Z} \mid m \mid x - a \,\} = \{\, a + mz \mid z \in \mathbb{Z} \,\}$$

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{(m-1)}\}, \text{有时直接记 } \mathbb{Z}_m = \{0, 1, \cdots, m-1\}$$

- 不难证明，对任意整数a, b, c, d，若$a \equiv b \pmod{m}$且$c \equiv d \pmod{m}$，则有$(a+c) \equiv (b+d) \pmod{m}$和$ac \equiv bd \pmod{m}$

等价关系练习

在有理数$\mathbb{Q}$上定义关系R：$\forall a, b \in \mathbb{Q}$, $a\,R\,b$当且仅当$a-b$是整数，证明R是等价关系，并给出所有的等价类，以及商集$\mathbb{Q}/R$。

等价关系练习

在有理数$\mathbb{Q}$上定义关系R：$\forall a, b \in \mathbb{Q}, a\ R\ b$当且仅当$a-b$是整数，证明$R$是等价关系，并给出所有的等价类，以及商集$\mathbb{Q}/R$。

1. R是自反的，因为对任意$a \in \mathbb{Q}$，$a-a=0$是整数，因此$a\ R\ a$。对任意$a, b \in \mathbb{Q}$，若$a\ R\ b$，则$a-b$是整数，从而$b-a$也是整数，因此$b\ R\ a$，所以R是对称的。对任意$a, b, c \in \mathbb{Q}$，若$a-b$是整数，$b-c$是整数，则$a-c=a-b+b-c$也是整数，因此$a\ R\ c$，所以R是传递的，综上R是等价关系。
2. 对每个有理数a，记$\lfloor a \rfloor$是不大于a的最大整数，则$a-(a-\lfloor a \rfloor)=\lfloor a \rfloor$是整数，因此$a \in [a-\lfloor a \rfloor]_R$，由于$0 \le a-\lfloor a \rfloor < 1$，因此大于等于0小于1的有理数可作为每个等价类的代表，即$\mathbb{Q}/R=\{[r]_R \mid 0 \le r < 1\}$，而对任意$0 \le r < 1, [r]_R = \{r+z \mid z \in \mathbb{Z}\}$

函数的基本概念

集合A到B的**函数**f，记为$f: A \to B$，是笛卡尔积$A \times B$的子集，且满足：对任意$a \in A$，都**有且只有唯一**的$b \in B$使得$\langle a, b \rangle \in f$

- 对于函数$f: A \to B$，称A是f的**定义域**，或简称**域**，而B称为f的**陪域**
- 对于$S \subseteq A$，S在f下的**像集**，记为$f(S)$，定义为：

$$f(S) = \{f(x) \in B \mid x \in S\} = \{y \in B \mid \exists x \in S, y = f(x)\} \subseteq B$$

  - 特别地，称$f(A)$为函数f的**值域**(range)，有时也记为$\mathrm{ran}(f)$
- 对于$T \subseteq B$，T在f下的**逆像集**，也称为**原像集**，记为$f^{-1}(T)$，定义为：

$$f^{-1}(T) = \{x \in A \mid f(x) \in T\} \subseteq A$$

$f^{-1}(T)$是一个整体记号，对任意函数f都适用，不意味着函数f必然有逆函数f^{-1}

单函数、满函数和双函数

f是单函数，若对任意$x, y \in A$，$f(x) = f(y)$蕴涵$x = y$, 也即$\forall x, y \in A$，$x \neq y$蕴涵$f(x) \neq f(y)$

- 陪域B的每个元素至多有定义域的一个元素与之对应，单函数也称为一对一(one-to-one)函数

说f是满函数，如果对任意$y \in B$，都存在$x \in A$使得$f(x) = y$，也即$\mathrm{ran}(f) = B$

- 陪域B的每个元素至少有定义域的一个元素与之对应，满函数也称为映上(onto)函数

说f是双函数，如果f既是单函数又是满函数

- 陪域B的每个元素都有且有唯一的定义域元素与之对应，双函数也称为一一对应(one-to-one correspondence)

设A是非空集，定义函数$f: A \times A \to ?$，对任意$a, b \in A$，$f(a, b) = \{\{a\}, \{a, b\}\}$，证明$f$是单函数

根据这个函数的定义，函数 f 的陪域应该是什么?

函数性质的证明

设A是非空集，定义函数$f: A \times A \to \wp(\wp(A))$，对任意$a, b \in A$，$f(a,b) = \{\{a\},\{a,b\}\}$，证明$f$是单函数

有序对$\langle a, b\rangle$的集合论定义就是$\{\{a\},\{a,b\}\}$

对任意$a,b,c,d \in A$，若$f(a,b) = f(c,d)$，则$\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$。这时：

1. 若$a = b$，则$\{\{a\},\{a,b\}\} = \{\{a\}\}$，因此$\{\{a\}\} = \{\{c\},\{c,d\}\}$，因此必有$\{c\} = \{c,d\}$，从而也有$d = c$，从而$\{\{a\}\} = \{\{c\}\}$，从而$\{a\} = \{c\}$，从而$a = c$，从而$a = b = c = d$，从而$\langle a,b\rangle = \langle a,a\rangle = \langle c,c\rangle = \langle c,d\rangle$

2. 若$a \neq b$，则$\{a\} \neq \{a,b\}$，从而也必有$\{c\} \neq \{c,d\}$，从而也必有$c \neq d$。从而必有$\{a\} = \{c\}$且$\{a,b\} = \{c,d\}$，因此$a = c$且$\{a,b\} = \{c,d\} = \{a,d\}$，由于$a = c \neq d$，因此必有$b = d$，总之有$a = c$且$b = d$，即$\langle a,b\rangle = \langle c,d\rangle$

函数与等价关系

设$f: A \to B$是函数，定义A上的关系R，$\forall a, b \in A$，$a\ R\ b$当且仅当$f(a) = f(b)$。证明R是等价关系，并给出它的等价类和商集

函数与等价关系

设$f: A \to B$是函数，定义A上的关系R，$\forall a, b \in A$，$a\ R\ b$当且仅当$f(a) = f(b)$。证明R是等价关系，并给出它的等价类和商集

1. 显然R是等价关系，因为对任意$a, b, c \in A$，$f(a) = f(a), f(a) = f(b)$蕴涵$f(b) = f(a), f(a) = f(b)$且$f(b) = f(c)$蕴涵$f(a) = f(c)$。

2. 对任意$a \in A$，$[a]_R = \{ x \mid f(x) = f(a) \}$，$A/R = \{ [a]_R \mid a \in A \}$。实际上，对任意$a \in A$，若$f(a) = y \in B$，则$[a]_R = f^{-1}(y)$。因此若$f$是满函数，则$A/R = \{ f^{-1}(b) \mid b \in B \}$，即$A/R$中的等价类与$B$的元素一一对应！

3. 对集合A上的任意等价关系R，自然映射$\rho: A \to A/R$，$\rho(a) = [a]_R$是满函数，因此A上的等价关系与以A为定义域的满函数对应！

4. 设$|A| = n$，则A上有m个等价类的等价关系个数等于A到$Z_m = \{0, 1, \cdots, m-1\}$的满函数个数除以$m!$(在$\mathbb{Z}_m$的元素作为原像的所有可能排列中选一个即可！）。

等价关系计数

设$|A|=n$，则A上不同的等价关系有多少个?

1. A上的等价关系与以A为定义域的满函数对应！
2. 设$|A|=n$，则A上有m个等价类的等价关系个数等于A到$Z_m=\{0,1,\cdots,m-1\}$的满函数个数除以$m!$(在$\mathbb{Z}_m$的元素作为原像的所有可能排列中选一个即可！）。
3. 当$|A|=n$，$|B|=m$，$n\geq m$，A到B的满函数个数是：

$$m^n - C(m,1)(m-1)^n + \cdots + (-1)^k C(m,k)(m-k)^n + \cdots + (-1)^{m-1} C(m,m-1)\cdot 1^n$$

4. 因此n元素集合A上有m个等价类的等价关系有：

$$B(n,m)=\frac{\sum_{k=0}^{m-1}(-1)^k C(m,k)(m-k)^n}{m!}$$

5. 从而n元素集合A上的不同等价关系个数有：$B(n)=\sum_{m=1}^{n}\frac{\sum_{k=0}^{m-1}(-1)^k C(m,k)(m-k)^n}{m!}$

等价关系计数

设$|A| = n$，则A上不同的等价关系有多少个?

用$B(n)$表示n元素集合上不同等价关系的个数，教材给出了如下递推关系式：

$$B(n+1) = \sum_{k=0}^{n} C(n,k)B(k)$$

这个递推关系式的理解是：对于有$n+1$元素集合（不妨假定为$\{0,1,\cdots,n\}$）的划分，按照最后一个元素n所在的划分块进行分类：

- 若n不与$\{0,\cdots,n-1\}$的任意元素在一个划分块，即n单独在一个划分块，这种划分的个数就等于$\{0,\cdots,n-1\}$的划分个数，即等于$B(n)$
- 若n与$\{0,\cdots,n-1\}$的某$j = n-k (k = 0,\cdots,n)$个元素在一个划分块，则这j个元素有$C(n,j) = C(n,n-k) = C(n,k)$ 种选择，而每种选择的划分个数等于剩下的 k 个元素构成集合的划分个数，即等于$B(k)$，因此有$C(n,k)B(k)$个划分

等价关系计数

设$|A| = n$，则A上不同的等价关系有多少个?

1. A上的不同等价关系个数$(n \geq 1, B(0) = 1, C(0,0) = 1)$

$$B(n) = \sum_{m=0}^{n-1} C(n-1, m)B(m) = \sum_{m=1}^{n} \frac{\sum_{k=0}^{m-1}(-1)^k C(m,k)(m-k)^n}{m!} = \sum_{m=1}^{n} B(n,m)$$

2. 注意其中$B(n,m)$满足递推式: $B(n,m) = B(n-1, m-1) + mB(n-1, m)$（含义？）
3. 当$|A| = 3$，则A上等价关系个数$1 + (2^3 - C(2,1))/2! + (3^3 - C(3,1)2^3 + C(3,2))/3! = 1 + 3 + 1 = 5$
4. 当$|A| = 4$，则A上等价关系个数$1 + (2^4 - C(2,1))/2! + (3^4 - C(3,1)2^4 + C(3,2))/3! + (4^4 - C(4,1)3^4 + C(4,2)2^4 - C(4,3))/4! = 15$

教学目标、教学内容、学习方法与考核

集合、关系与函数基本知识回顾

代数一般概念回顾

集合上的运算

集合上的运算(operation)

- 集合S上的（或直接说S的）二元(binary)运算，是形如$f: S \times S \to S$的函数f
  - 集合S是运算的陪域，S的笛卡尔积是定义域
  - 运算是具有特殊形式的定义域和陪域的函数，形如$g: \mathbb{N} \to \mathbb{R}$的函数不是运算
- 集合S的（或直接说S的）n-元(n-ary)运算，是形如$f: S^n \to S$的函数f
  - 必要时，将集合S的元素作为S的零元运算，也称为常量运算

这里定义的是严格意义上的运算，是具有特殊形式的定义域和陪域的函数

- 生活和数学中有时也将其他形式的函数称为运算，例如向量的数量积运算，两个向量的数量积是一个数，而不再是一个向量
- 生活和数学中提到运算，有时不太关注它是哪个集合上的运算

运算的封闭性

人们通常关注运算法则，但代数系统中更强调集合S的运算的下面两点性质

- S中任何两个元素都可进行该运算，且运算结果惟一
- S的任意两个元素的运算结果都属于S，这称为S对于该运算封闭

运算的封闭性

若函数$f: S \times S \to S$是集合S的运算，则称集合S对运算f封闭

- 设$T \subseteq S$是S的子集，如果对任意的$t_1, t_2 \in T$都有$f(t_1, t_2) \in T$，则称子集T对S的运算f封闭，这时f也是T的运算

运算的性质和特殊元素

运算的性质

- 一个运算可能满足交换律、结合律、幂等律、消去律
- 两个运算之间可能满足分配律、吸收律

运算$\circ$满足消去律指，对任意a, b, c，~~当a不是零元时有~~ $a \circ b = a \circ c$蕴涵$b = c$，以及$b \circ a = c \circ b$蕴涵$b = c$

运算的特殊元素

- 一个运算可能有单位元或零元
  - 运算如果有单位元或零元，则有唯一的单位元或零元
- 一个元素对于有单位元的运算可能有逆元
  - 当运算满足结合律时，一个元素有逆元，则有唯一的逆元

- 集合并满足交换律、结合律、幂等律
- 集合交对集合并有分配律
- 集合交和集合并有吸收律
- 实数集或整数集上的加法运算满足消去律

- 整数集上的乘法有单位元1和零元0
- 给定全集U，$\wp(U)$上的集合并运算的单位元是空集，零元是全集U
- 整数加法有单位元0，这时整数a的逆元是$-a$

代数的定义

代数(algebra)

代数是一个集合及这个集合上的一些运算，这个集合称为代数的**基集**

- 整数集$\mathbb{Z}$及它的加法$+$、乘法$*$运算构成代数$(\mathbb{Z}, +, *)$
- 集合$\mathbb{Z}_5$及模5加$\oplus_5$和模5乘$\otimes_5$构成代数$(\mathbb{Z}_5, \oplus_5, \otimes_5)$

- 全集U，$(\wp(U), \cup, \cap, \emptyset, U)$是一个有两个二元运算，两个零元运算的代数

- 集合$\mathbf{2} = \{0, 1\}$和逻辑运算构成代数$(\mathbf{2}, \neg, \wedge, \vee, \rightarrow, \leftrightarrow)$
- 命题逻辑公式构成集合$\mathcal{F}$和这些逻辑运算也构成代数

子代数(Sub-algebra)

Remark： (1)如果代数基集的一个子集对所有运算都**封闭**，则称该子集及相应运算为该代数的一个子代数。(2)无法直接推广到群与子群的关系(c.f.Th1.3.2)。

代数的子代数是基集的一个子集，且对代数的所有运算都**封闭**

- 子集对运算封闭意味着这个子集的任意元素做运算，结果还属于该子集

对代数$(\mathbb{Z},+,*)$，偶数集$\mathbb{Z}_E=\{2k \mid k\in\mathbb{Z}\}$对运算$+,*$封闭，因此构成代数$(\mathbb{Z},+,*)$的子代数，记为$(\mathbb{Z}_E,+,*)$

- 这时封闭的直观含义就是，偶数加偶数仍是偶数，偶数乘偶数仍是偶数
- 奇数集合$\mathbb{Z}_O=\{2k+1 \mid k\in\mathbb{Z}\}$对运算$+,*$不封闭，奇数加奇数得到的不再是奇数
- 集合$\mathbb{Z}_E$的所有整数可由2和-2用加法和乘法运算得到，因此子代数$(\mathbb{Z}_E,+,*)$是由2和-2**生成的子代数**

Remark： (3)对群(Z,+)而言，$(Z_E,+)$是由2或-2**生成的子代数**。

子代数(Sub-algebra)

代数的子代数是基集的一个子集，且对代数的所有运算都**封闭**

- 子集对运算封闭意味着这个子集的任意元素做运算，结果还属于该子集

对代数$(\mathbb{Z}_5,\otimes_5)$，集合$U=\{1,2,3,4\}$对运算$\otimes_5$封闭，因此$(U,\otimes_5)$是它的子代数

- 且$(U,\otimes_5)$是由**2生成的子代数**：$2\otimes_5 2=4, 2\otimes_5 2\otimes_5 2=3, 2\otimes_5 2\otimes_5 2\otimes_5 2=1$

对代数$(\mathbb{Z}_5,\oplus_5)$，除集合$\{0\}$外，$\mathbb{Z}_5$的任意真子集对运算$\oplus_5$都不封闭，因此它没有除$(\{0\},\oplus_5)$外的**真子代数**

- 除0外，$\mathbb{Z}_5$的任意元素都可通过运算$\oplus_5$得到$\mathbb{Z}_5$的所有元素，因此说$1,2,3,4$都是代数$(\mathbb{Z}_5,\oplus_5)$的**生成元**

同余关系(Congruence Relation)

代数上的同余关系是基集上的一个等价关系，且与代数的所有运算都**可替换**

- 或说代数的所有运算都**保持**这个等价关系
    - 直观含义是，参与运算的对应元素有这个关系，则运算的结果也有这个关系

对代数$(\mathbb{Z},*)$，关系$\equiv_5 = \{\langle a,b\rangle \mid a$和$b$整除5余数相同$\}$，即$\equiv_5$是模5同余关系，则$\equiv_5$是$(\mathbb{Z},*)$上的同余关系

$$\left.\begin{matrix} a \equiv_5 b \\ c \equiv_5 d \end{matrix}\right\} (a*c) \equiv_5 (b*d) \quad \longrightarrow \quad \left.\begin{matrix} 3 \equiv_5 8 \\ 2 \equiv_5 12 \end{matrix}\right\} (3*2=6) \equiv_5 (8*12=96)$$

$\equiv_5$与$*$的可置换性 　　　 $\equiv_5$与$*$的可置换性

不难验证，关系$\equiv_5$也是代数$(\mathbb{Z},+)$上的同余关系，这种例子是一般同余关系的发源

商代数(Quotient Algebra)

对代数上的同余关系，基集关于这个同余关系的商集(即等价类的集合)

- 可定义与原代数对应的运算(同余关系的可置换性保证运算定义的可行性)而构成商代数
  - 直观地说，等价类做商代数运算的结果 = 等价类代表做原来代数运算的结果所在的等价类

对代数$(\mathbb{Z},*)$，模5同余关系$\equiv_5$是$(\mathbb{Z},*)$上的同余关系，商集是$\mathbb{Z}_{\equiv_5}=\{[0]_5,[1]_5,\cdots,[4]_5\}$，可在$\mathbb{Z}_{\equiv_5}$上定义运算$\otimes_{\equiv_5}$，构成商代数$(\mathbb{Z}_{\equiv_5},\otimes_{\equiv_5})$

- $[0]_5=\{\,5k\mid k\in\mathbb{Z}\,\}=\{0,5,10,\cdots\}$, $[1]_5=\{\,5k+1\mid k\in\mathbb{Z}\,\}=\{1,6,11\cdots\}$等等

等价类做商代数运算 $[a]_5\otimes_{\equiv_5}[b]_5=[a*b]_5$ 代表做原代数运算 $\rightarrow$ $[2]_5\otimes_{\equiv_5}[3]_5=[2*3]_5=[6]_5=[1]_5$

代数同态(Homomorphism)

Remark：(1)详细严格的定义参考教材P81Def.2.3.1

两个同类型的代数之间的同态是它们基集之间的函数，且对代数的所有运算可交换

- 可交换的直观含义是，先运算再映射 = 先映射再运算
  - 先做源代数的运算再映射（求函数值）的结果=先求函数值再做目标代数对应运算的结果

对于代数$(\mathbb{Z},*)$和$(\mathbb{Z}_5=\{0,1,2,3,4\},\otimes_5)$，函数$f:\mathbb{Z}\to\mathbb{Z}_5$，$\forall x, f(x) = x \bmod 5$，是同态

$$\begin{tikzcd}
a,\ b \arrow[r, "\text{源代数运算}"] \arrow[d, "\text{映射}"'] & a*b \arrow[d, "\text{映射}"] \\
f(a),\ f(b) \arrow[r, "\text{目标代数运算}"'] & f(a*b) = f(a)\otimes_5 f(b)
\end{tikzcd}
\quad\Rightarrow\quad
\begin{tikzcd}
8,\ 12 \arrow[r, "\text{源代数运算}"] \arrow[d, "\text{映射}"'] & 8*12=96 \arrow[d, "\text{映射}"] \\
f(8)=3,\ f(12)=2 \arrow[r, "\text{目标代数运算}"'] & \begin{array}{c} f(8*12)=f(96)=1 \\ f(a)\otimes_5 f(b)=3\otimes_5 2=1 \end{array}
\end{tikzcd}$$

子代数、商代数都是与原来代数同类型的代数，它们实质上也可用同态刻画

- 子代数与单同态(即既是单函数又是同态)一一对应，商代数与满同态(即既是满函数又是同态)一一对应

代数同构(isomorphism)

两个代数之间存在同态，且这个同态是双函数，则称这两个代数同构

- **同构的两个代数具有完全相同的代数性质**

对代数$(\mathbb{Z},*)$，关系$\equiv_5$是$(\mathbb{Z},*)$上的同余关系，商集$\mathbb{Z}_{\equiv_5} = \{[0]_5,[1]_5,\cdots,[4]_5\}$构成商代数$\left(\mathbb{Z}_{\equiv_5},\otimes_{\equiv_5}\right)$

- $[0]_5 = \{\,\mathbf{5}\boldsymbol{k} \mid \boldsymbol{k} \in \mathbb{Z}\,\} = \{\mathbf{0},\mathbf{5},\mathbf{10},\cdots\}$, $[1]_5 = \{\,\mathbf{5}\boldsymbol{k}+\mathbf{1} \mid \boldsymbol{k} \in \mathbb{Z}\,\} = \{\mathbf{1},\mathbf{6},\mathbf{11}\cdots\}$等等

等价类做商代数运算 $[\boldsymbol{a}]_5 \otimes_{\equiv_5} [\boldsymbol{b}]_5 = [\boldsymbol{a} * \boldsymbol{b}]_5$ 代表做原代数运算 $\rightarrow$ $[\mathbf{2}]_5 \otimes_{\equiv_5} [\mathbf{3}]_5 = [\mathbf{2} * \mathbf{3}]_5 = [\mathbf{6}]_5 = [\mathbf{1}]_5$

商代数$\left(\mathbb{Z}_{\equiv_5},\otimes_{\equiv_5}\right)$与$(\mathbb{Z}_5 = \{\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}\},\otimes_5)$同构，$\boldsymbol{\phi} : \left(\mathbb{Z}_{\equiv_5},\otimes_{\equiv_5}\right) \rightarrow (\mathbb{Z}_5,\otimes_5)$，$\boldsymbol{\phi}([\boldsymbol{a}]_5) = \boldsymbol{a} \bmod \mathbf{5}$

- $[\mathbf{0}]_5$对应0, $[\mathbf{1}]_5$对应1等等，$\otimes_{\equiv_5}$本质上就是模5乘运算$\otimes_5$

代数同态基本定理

两个代数之间存在同态，且这个同态是双函数，则称这两个代数**同构**

- 同构的两个代数具有完全相同的代数性质

一般来说，对于**同态**$f:(A,*)\rightarrow(B,\circ)$

- f导出$(A,*)$上一个**同余关系**R_f，$\langle a_1,a_2\rangle\in R_f$当且仅当$f(a_1)=f(a_2)$
- $f(B)$对$(B,\circ)$的运算封闭，构成**子代数**$(f(B),\circ)$
  - 代数$(A,*)$关于同余关系R_f的商代数$(A/R_f,\otimes)$与子代数$(f(B),\circ)$同构，这称为**代数同态基本定理**

总结

集合、关系和函数的基本概念

- 集合的基本概念：子集、相等、集合的性质概括法定义、集合集合并交差补和幂集运算
- 关系的基本概念：关系的定义、关系逆与关系复合运算、关系性质、等价关系与划分
- 函数的基本概念：像集、逆像集、单函数、满函数、双函数、集合等势、有穷集、无穷集、可数集、不可数集

学习这一部分的目标

- 回忆集合、关系和函数的一些基本概念
- 了解证明的构建思路：从结论开始分析，自顶向下构造

作业

第一讲不布置笔试作业，请及时预习下一讲！

谢谢大家！

有什么问题和建议请及时反馈给老师！