15.4 同余关系与商代数

- 同余关系
  - 同余关系与同余类
  - 同余关系的实例
- 商代数
  - 商代数定义
  - 商代数性质
- 同态映射、同余关系与商代数之间的联系

同余关系与同余类

定义 设$V=<A,o_1,o_2,\ldots,o_r>$是代数系统，其中o_i为k_i元运算，关系~为A上的等价关系，任取A上$2k_i$个元素$a_1,a_2,\ldots,a_{ki},b_1,b_2,\ldots,b_{ki}$，如果对于所有的$j=1,2,\ldots,k_i$，$a_j\sim b_j$就有

$$o_i(a_1,a_2,\ldots,a_{ki})\sim o_i(b_1,b_2,\ldots,b_{ki})$$

则称等价关系~对于运算o_i具有**置换性质**.

如果等价关系~对于V中的所有运算都具有置换性质，则称~是V上的**同余关系**，称A中相关的等价类为**同余类**.

实例

例1 $V=<Z_4,\oplus>$, 有15个等价关系，采用对应的划分表示.
划分{{0},{1,2,3}} 对应的不是同余关系，因为1~3，但是 $1\oplus3 \sim 3\oplus3$不成立.

同理可以验证以下11个划分对应的也不是同余关系

{{1},{0,2,3}}　{{2},{1,3,0}}　{{3},{1,2,0}}
{{0,1},{2,3}}　{{0,3},{1,2}}
{{0},{1},{2,3}}　{{0},{2},{1,3}}　{{0},{3},{1,2}}
{{1},{2},{0,3}}　{{1},{3},{0,2}}　{{2},{3},{0,1}}

只有以下3个划分对应于同余关系：

{{0},{1},{2},{3}}　{{0,1,2,3}}　{{0,2},{1,3}}

恒等关系与全域关系都是同余关系，任何代数系统都存在同余关系.

商代数定义

定义 设代数系统$V=<A,o_1,o_2,\ldots,o_r>$，其中 o_i 为 k_i 元运算，$i=1, 2, \ldots, r$. 关系 R 为V上的同余关系，V关于R的商代数记作

$$V/R=<A/R,\overline{o_1},\overline{o_2},\ldots,\overline{o_r}>$$

其中A/R 是关于同余关系的商集. 对于$i=1,2,\ldots,r$, 运算$\overline{o_i}$定义为

$$\overline{o_i}([a_1],[a_2],\ldots,[a_{k_i}])=[o_i(a_1,a_2,\ldots,a_{k_i})]$$

实例：模n的同余类

$V = \langle Z,+\rangle$，同余关系：$x\sim y \Leftrightarrow x = y \bmod 3$

$Z/\sim = \{ [0], [1], [2] \}$

$V/\sim = \langle Z/\sim,\oplus\rangle$，$\forall[x],[y]\in Z/\sim$，$[x]\oplus[y] = [x+y]$

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

商代数的良定义性

运算的良定义

运算结果与参与运算元素的表示无关

对于任意运算 o_i, 设为 k_i 元运算，$a_j \sim b_j$, $j = 1, 2, \ldots, k_i$,
则

$$\overline{o_i}([a_1],[a_2],\ldots,[a_{k_i}])$$
$$=[o_i(a_1,a_2,\ldots,a_{k_i})]$$
$$=[o_i(b_1,b_2,\ldots,b_{k_i})]$$
$$=\overline{o_i}([b_1],[b_2],\ldots,[b_{k_i}])$$

商代数的性质

设代数系统 V, R是V上的同余关系，V 关于 R 的商代数 V/R，那么

(1) V/R 保持 V 的下述性质：

交换、结合、幂等、分配、吸收律

(2) V/R 保持V 的单位元、零元、逆元，即

$[e]$是商代数的单位元

$[\theta]$是商代数的零元

$[a^{-1}]=[a]^{-1}$

注 消去律不一定保持. 例如$\langle Z,\cdot\rangle$有消去律，定义等价关系如下： $xRy \Leftrightarrow x \equiv y \pmod 4$.

商代数为 $V/R = \langle\{[0],[1],[2],[3]\},\otimes\rangle$.

没有消去律. $[2]\otimes[2] = [0]\otimes[2]$, 但是$[0] \neq [2]$.

同态、同余关系与商代数的联系

- 同态映射导出同余关系
- 商代数是原代数的同态像

  通过自然映射
- 同态基本定理

  代数系统的同态像同构于它的商代数

同态映射导出同余关系

定理1 设 $V_1=<A,o_1,o_2,\ldots,o_r>$ 与 $V_2=<B,o_1',o_2',\ldots,o_r'>$ 是同类型的代数系统，对于 $i=1, 2, \ldots, r$，o_i 为 k_i 元运算，函数 $f:A\to B$ 为代数系统 V_1到 V_2的同态映射，则由 f 导出的 A 上的等价关系为 V_1 上的同余关系.

证 $\forall x, y\in A,\ x\sim y \Leftrightarrow f(x)=f(y)$

任取V_1上的运算 $o_i,(k_i\geq 1)$，对任意的 $a_j\sim b_j, j=1, 2, \ldots, k_i$,

$$f(o_i(a_1,a_2,\ldots,a_{k_i}))=o_i'(f(a_1),f(a_2),\ldots,f(a_{k_i}))$$

$$=o_i'(f(b_1),f(b_2),\ldots,f(b_{k_i}))\quad f(a_j)=f(b_j), j=1,2,\ldots,k_i$$

$$=f(o_i(b_1,b_2,\ldots,b_{k_i}))$$

$$o_i(a_1,a_2,\ldots,a_{k_i})\sim\ o_i(b_1,b_2,\ldots,b_{k_i})$$

~关于o_i运算具有置换性质，根据o_i的任意性，定理得证.

实例

例2 $V=<Z_4,\oplus>$, $f_i: Z_4 \to Z_4$, $f_i(x) = (i\,x) \bmod 4$，$i = 0,1,2,3$

函数	导出的同余关系
$f_0(x)=0$, $x=0,1,2,3$	全域关系
$f_1(x)=x$, $x=0,1,2,3$	恒等关系 I_{Z4}
$f_2(0)=f_2(2)=0$, $f_2(1)=f_2(3)=2$	$\{<0,2>,<2,0>,<1,3>,<3,1>\}\cup I_{Z4}$
$f_3(0)=0$, $f_3(1)=3$, $f_3(2)=2$, $f_3(3)=1$	恒等关系 I_{Z4}

注意：在这个例子中，每个同态都可以导出一个同余关系；不同的同态，若同态像一样，导出相同的同余关系.

商代数是原代数同态像

定理2 设代数系统$V=<A,o_1,o_2,\ldots,o_r>$，其中o_i为 k_i元运算，$i=1,2,\ldots,r$, R是V上的同余关系， 则自然映射

$$g:A\to A/R,\ \ g(a)=[a],\ \forall a\in A,$$

是从V到 V/R 的同态映射.

证 设 $V/R=<A/R,\overline{o_1},\overline{o_2},\ldots,\overline{o_r}>$

考虑 o_i, 设为 k_i元运算. $k_i>0$. 任取 $a_1, a_2, \ldots, a_{ki}\in A$

$$g(o_i(a_1,a_2,\ldots,a_{k_i}))=[o_i(a_1,a_2,\ldots,a_{k_i})]$$

$$=\overline{o_i}([a_1],[a_2],\ldots,[a_{k_i}])=\overline{o_i}(g(a_1),g(a_2),\ldots,g(a_{k_i}))$$

由于o_i的任意性，定理得证.

同态基本定理

定理 3 设$V_1=<A,o_1,o_2,...,o_r>$与$V_2=<B,o_1',o_2',...,o_r'>$是同类型的代数系统，对于 i=1,2,…,r，o_i 与 o_i'都是 k_i 元运算，f:A→B 是 V_1 到 V_2 的同态，关系 R 是 f 导出的 V_1 上的同余关系，则 V_1 关于同余关系 R 的商代数同构于 V_1 在 f 下的同态像，即

$$V_1/R\cong<f(A),o_1',o_2',\ldots,o_r'>$$

证明思路：

(1) 定义h：$V_1/R\to f(A)$, $h([a])=f(a)$

(2) 验证h是良定义的　　$[a]=[b]\Leftrightarrow aRb\Leftrightarrow f(a)=f(b)$

(3) 验证h是双射的

(4) 验证h是同态映射

同态的验证

考虑任意运算 $\overline{o_i}$，设为 k_i 元，$k_i>0$, $i=1,2,\ldots,r$

$$h(\overline{o_i}([a_1],[a_2],\ldots,[a_{k_i}]))$$

$$= h([o_i(a_1,a_2,\ldots,a_{k_i})]) \qquad \text{商代数定义}$$

$$= f(o_i(a_1,a_2,\ldots,a_{k_i})) \qquad h\text{函数定义}$$

$$= o_i'(f(a_1), f(a_2),\ldots, f(a_{k_i})) \qquad \text{同态定义}$$

$$= o_i'(h([a_1]),h([a_2]),\ldots,h([a_{k_i}])) \qquad h\text{函数定义}$$

如果是 0 元运算$[a]\in V_1/R$,则

$$h([a]) = f(a) = a'$$

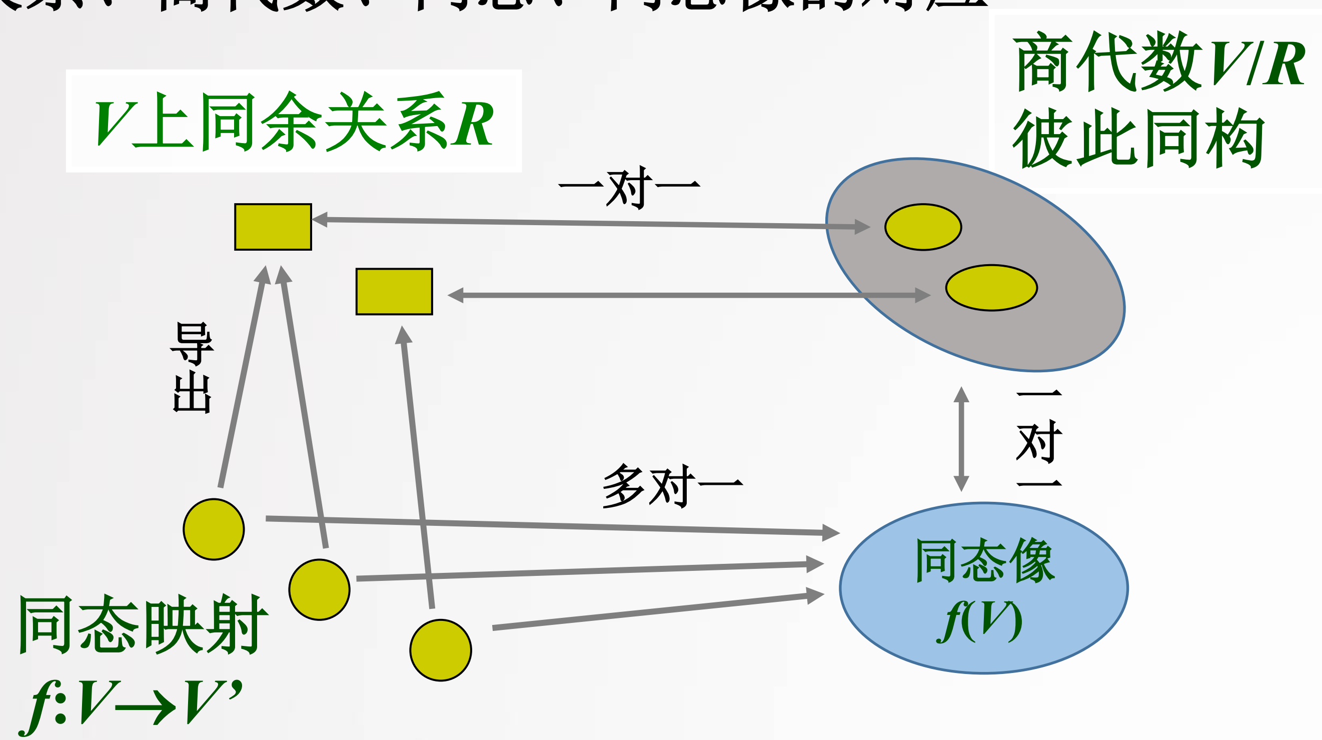
且a'是 $f(A)$ 中对应的 0 元运算

同态、同余关系与商代数的联系

定理2 任何商代数都是同态像

定理3 任何同态像在同构意义下是商代数

同余关系、商代数、同态、同态像的对应



实例说明

$G_1 = \{ e, a, b, c \}$, Klein四元群, $G_2 = \{ e, x \}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$f_1{:}G_1 \to G_2$

$f_1 = \{<e,e>,<a,e>,<b,x>,<c,x>\}$

$f_2{:}G_1 \to G_2$

$f_2 = \{<e,e>,<b,e>,<a,x>,<c,x>\}$

$f_1(G_1) = f_2(G_1) = G_2$

f_1导出的同余关系R_1：$e \sim a,\ b \sim c$，$G_1/R_1 = \{[e],[b]\}$

f_2导出的同余关系R_2：$e \sim b,\ a \sim c$，$G_1/R_2 = \{[e],[a]\}$

$$G_1/R_1 \cong G_1/R_2 \cong G_2$$

例题

例3 $V = < Z_6, \oplus >$，求V上的同余关系

方法一：确定所有的等价关系，然后判断置换性质

方法二：先找自同态，由同态像确定同余关系

自同态为：$f_i : Z_6 \to Z_6$，$f_i(x) = (i\,x) \bmod 6$，$i = 0,1,2,3,4,5$

f_0 的同态像为$\{ 0 \}$，f_0导出的同余关系为全域关系

f_1和f_5的同态像为 Z_6，f_1导出的同余关系为恒等关系

f_2和f_4的同态像为 $\{ 0, 2, 4 \}$

f_2导出的同余关系为:

$\{<0,3>,<1,4>,<2,5>,<3,0>,<4,1>,<5,2>\} \cup I_{Z_6}$

f_3的同态像为$\{ 0, 3 \}$, f_3导出的同余关系为:

$\{<0,2>,<2,0>,<4,0>,<0,4>,<2,4>,<4,2>, <1,3>,$

$<3,1>,<1,5>,<5,1>,<3,5>,<5,3>\} \cup I_{Z_6}$

例题（续）

例 4 设$V_1=<A,*,\Delta,k>$，$V_2=<B,\circ,\Delta',k'>$为代数系统，

$$\forall<a,b>,<c,d>\in A\times B,\ <a,b>R<c,d>\Leftrightarrow a=c$$

(1) 证明 R 为 $V_1\times V_2$ 上的同余关系

(2) 证明 $(V_1\times V_2)/R\cong V_1$

证明思路：

(1) 证明 R 的自反、对称、传递性

(2) 证明 R 具有置换性质，即令$V_1\times V_2=<A\times B,\bullet,\Diamond,K>$，

$$<a,b>R<c,d>\text{且}<a',b'>R<c',d'>$$
$$\Rightarrow<a,b>\bullet<a',b'>R<c,d>\bullet<c',d'>$$
$$<a,b>R<c,d>\Rightarrow\Diamond<a,b>R\Diamond<c,d>$$

(3)定义$f:V_1\times V_2\to V_1$，$f(<a,b>)=a$，证明f为满同态

(4)证明 R 是f导出的同余关系，即

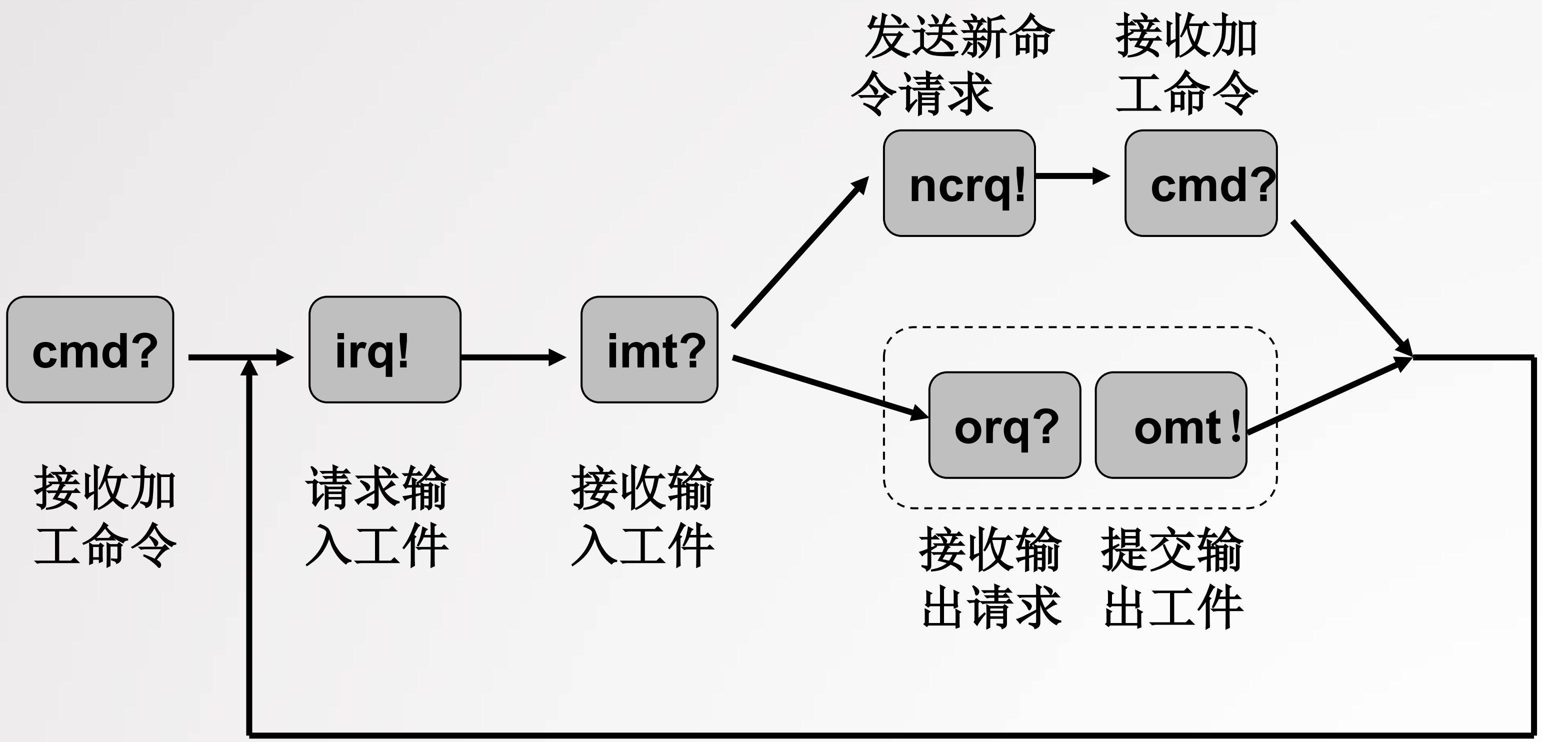
$$f(<a,b>)=f(<c,d>)\Leftrightarrow a=c\Leftrightarrow<a,b>R<c,d>$$

進程代数: Process Algebra

实例

- 基础单元——Bunit
- 进程
  - 接受加工命令——cmd
  - 请求输入工件——irq
  - 接受输入工件——imt
  - 发送新命令的请求——ncrq
  - 接受输出请求——orq
  - 提交输出工件——omt
  - 空进程——δ

基础单元的工作流程



？表示进程有输入，！表示进程有输出.
不与外部进行交互的称为内部行为，用 τ 表示.

基础单元的代数规范

Bunit= cmd? • ((irq! • imt? • (ncrq! • cmd? || orq? | omt!))*δ)

- 进程集合 A, 其中B={cmd, irq, imt, ncrq, orq, omt}$\subseteq A$
- 算子 |：$A\times A\rightarrow A$，同步，　||：$A\times A\rightarrow A$，并发

  •：$A\times A\rightarrow A$，顺序，　+：$A\times A\rightarrow A$，选择

  *：重复　　*δ：非终止重复

  优先级：| > • > ||，* 优先于||

- 算律 $x+y=y+x$, $(x+y)+z=x+(y+z)$,

  $(x+y)\bullet z=x\bullet z+y\bullet z$,

  $x+\delta=x$, $\delta\bullet x=x$,

  $(x\,\|\,y)\,\|\,z=x\,\|\,(y\,\|\,z)$, …

小结

- 代数系统的基本概念
  - 构成：载体，运算集(包括 0元运算), 公理(算律,特异元素)
  - 分类
- 子代数、积代数、商代数
  - 子代数：构成，判定(封闭)，性质(同种代数) ——分解
  - 积代数：构成(直积), 性质(同类型,消去律例外)——组合
  - 商代数：构成(同余), 性质(同类型,消去律例外)——抽象
- 同态
  - 同态映射的概念
  - 性质(同类型, 消去律例外)
  - 同态映射与商代数之间的关系