学问之道,其得之不难者,失之必易;惟艰难以得之者,斯能兢业以守之.

————(清)魏源《默觚上·学篇七》

《近世代数》参考书目

1. 张禾瑞. 近世代数基础. 高等教育出版社,1978 年修订本.
2. 吴品三. 近世代数. 人民教育出版社,1979 年.
3. 刘绍学.近世代数基础. 高等教育出版社,1999年.
4. 丁石孙,聂灵绍.代数学引论.北京大学出版社出版,2002年.
5. 熊全淹. 近世代数. 武汉大学出版社, 1984年修订版.
6. 冯克勤,李尚志,查建国,章璞. 近世代数引论,中国科学技术大学出版社,2002年.
7. 姚摹生. 抽象代数学. 复旦大学出版社,1998年.
8. B. L. 范德瓦尔登, 丁石孙,曾肯成,郝鈁新译,万哲先校. 代数学(I).科学出版社,1963年.
9. B. L. 范德瓦尔登, 曹锡华,曾肯成,郝鈁新译,万哲先校. 代数学(II).科学出版社,1976年.
10. N. 贾柯勃逊, 黄缘芳译. 抽象代数学(卷1). 科学出版社,1987年.
11. T. W. Hungerford, 冯克勤译,聂灵绍校.代数学. 湖南教育出版社,1985年.
12. N. Jacobson. Basic Algebra I. New York: Freeman and Company,1974.
13. N. Jacobson. Basic Algebra II. San Francisco: Freeman and Company, 1980.
14. J. Rotman. Abstract Algebra(A First Course in Abstract Algebra.Prentice-Hall). 机械工业出版社, 2004年.
15. M. Artin. Algebra. Englewood Cliffs: Prentice-Hall, 1999.

课程说明

集合论初步与高等代数(线性代数)是学习本课程的准备知识. 本课程学习以后可以继续研读:群论、环论、模论、李群、李代数、计算机科学、信息科学与编码理论等,同时,本课程在近代物理与近代化学等学科中也有着广泛的应用.

本课程是理论性较强的学科,由于教学时数所限, 本课程的理论推证较少,因此必须通过做练习题来加深对概念的理解和掌握, 熟悉各种公式的运用,从而达到消化、掌握所学知识的目的.独立完成作业是学好本课程的重要手段.

第一章 基本概念

§1 集合

要求掌握集合、元素的概念,空集合,集合与集合之间的包含、交、并、积,集合与元素之间的关系以及子集的概念.

定义 1.1 设$A_1,\dots,A_n$是n个集合,称

$$A_1\times\cdots\times A_n=\{(a_1,\dots,a_n)\mid a_i\in A_i\}$$

为集合$A_1,\dots,A_n$的积(或笛卡儿积).

例 1.1 $B\subset A$,但B不是A的真子集,这个情况什么时候才能出现?

例 1.2 假定$A\subset B$.$A\cap B=?$ $A\cup B=?$

§2 映射

定义 1.2 设X,Y是两个集合.从X到Y的映射是子集$f\subset X\times Y$,记为

$$f:\ X\to Y,$$

满足$\forall x\in X,\exists y\in Y$使得$(x,y)\in f$.

若$f:X\to Y,(x,y)\in f$通常记为$y=f(x)$,并称y为x在f下的象,x为y在f下的一个逆象.

定义 1.3 两个映射$f:X\to Y$和$g:X'\to Y'$相等当且仅当$X=X',Y=Y'$,且子集$f\subset X\times Y$与子集$g\subset X'\times Y'$是相等的(即$\forall x\in X,f(x)=g(x)$).

一个映射$f:X\to Y$由三部分构成: 源(domain)X,靶(target)Y和图(graph)f.我们说两个映射相等,当且仅当它们有相同的源, 相同的靶和相同的图.

例 1.3 设$A_1=A_2=\cdots=A_n=D=\mathbb{R}$, $f(a_1,a_2,\ldots,a_n)=0$, 其中$a_i\in A_i$,是$A_1\times A_2\times\cdots\times A_n$到$D$的映射.

例 1.4 设$A=D=\mathbb{Z}$,

$$f(n)=\begin{cases} n, & \text{when } n\neq 1,\\ b, & n=1,\text{where } b^2=1.\end{cases}$$

不是A到D的映射.

§3 代数运算

定义 3.1 集合G上的代数运算就是映射$\circ:\ G\times\times G\to G$.一般地,设$A_1,A_2,\ldots,A_n,D$为集合, 称$A_1\times A_2\times\cdots\times A_n$到$D$的映射为$A_1\times A_2\times\cdots\times A_n$到$D$的$n$元代数运算.2元代数运算简称为代数运算.

代数运算是一种特殊的映射,常记为$\circ(a,b)=a\circ b$.

例 3.1 设$A=\mathbb{Z},B=\mathbb{Z}-\{0\},D=\mathbb{Q}$,则

$$\circ:\quad A\times B\to D;\ (a,b)\mapsto\frac{a}{b}=a\circ b$$

是一个$\times B\to$到D的代数运算.这个代数运算就是通常的除法.

例 3.2 ${}_FV$中有几个代数运算?(不计逆运算)

当A,B都是有限集合时,一个$A\times B$到D的代数运算常用如下的表来表示

$\circ$	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
a_2	d_{21}	d_{22}	$\cdots$	d_{2m}
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

例 3.3 设$A=\{0,1,2,3,4,5,6\}$, A上的一个代数运算可表示为

$\circ$	0	1	$\cdots$	6
0	0	1	$\cdots$	6
1	1	2	$\cdots$	0
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
6	6	0	$\cdots$	5

试给出A^*上的一个“乘法”代数运算.

定义 3.2 如果$\circ$是A上的代数运算,则称集合A对于代数运算$\circ$是闭的.

§4 结合律

定义 4.1 设$\circ$是集合A上的代数运算,如果对$\forall a,b,c\in A$,

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

则称$\circ$满足结合律.

例 4.1 设$A=\mathbb{R},B=\mathbb{R}-\{0\},C=\mathbb{R}^+$(正实数集合),则$A$上加法满足结合律,而$A$上的减法不满足结合律; B上乘法满足结合律,而B上的除法不满足结合律,C上的幂指代数运算(即$a\circ b=a^b$)也不满足结合律.

通俗地说,如果A上的代数运算满足结合律,在运算时,就可以不考虑运算的“次序”,就可以在运算中任意加括号.一般而言, 对A上的代数运算$\circ$来说(只能进行两个元素间的运算,必须加括号才能得到两个以上元素的运算结果),以$\pi(a_1\circ a_2\circ\cdots\circ a_n)$表示$A$中的$n$个元素$a_1,a_2,\cdots,a_n$以某种方式加括号所得到的运算结果, 则这$n$个元素的运算结果$\pi(a_1\circ a_2\circ\cdots\circ a_n)$可能由于运算的次序不同(即加括号的方式不同),而得出不同的结果,这是我们所不愿意看到的(因为$a_1\circ a_2\circ\cdots\circ a_n$不是一个确定的元素,因而也就没有意义了).

定义 4.2 若对于A的$n(n\geq 2)$个元素$a_1,a_2,\ldots,a_n$,对$a_1\circ a_2\circ\cdots\circ a_n$任意加括号后,所得的运算结果都相等, 就把这唯一的结果记为$a_1\circ a_2\circ\cdots\circ a_n$.

定理 4.1 如果A的代数运算$\circ$满足结合律,则对于A的任意$n(n\geq 2)$个元素$a_1,a_2,\cdots,a_n$,符号$a_1\circ a_2\circ\cdots\circ a_n$都有意义.

证 用归纳法.注意到

$$\begin{aligned}
&\pi(a_1\circ a_2\circ\cdots\circ a_n)\\
=\ &\pi_1(a_1\circ\cdots\circ a_i)\circ\pi_2(a_{i+1}\circ\cdots\circ a_n)\\
=\ &(a_1\circ\pi_{11}(a_2\circ\cdots\circ a_i))\circ\pi_2(a_{i+1}\circ\cdots\circ a_n)\\
=\ &a_1\circ(\pi_{11}(a_2\circ\cdots\circ a_i)\circ\pi_2(a_{i+1}\circ\cdots\circ a_n))\\
=\ &a_1\circ(a_2\circ(\cdots\circ a_n)\cdots)
\end{aligned}$$

即得. □

§5 交换律

定义 5.1 如果$\circ$是$A\times A$到D的代数运算,且对$\forall a,b\in A, a\circ b=b\circ a$,就称$\circ$满足交换律.

小学中的凑整能简化运算,就是因为加法和乘法运算满足结合律和交换律. $\mathbb{R}^+$上的幂指运算以及矩阵乘法等运算都是不满足交换律的代数运算.

定理 5.1 如果集合A上的代数运算$\circ$同时满足结合律和交换律,那么在$a_1\circ a_2\circ\cdots\circ a_n$里,元的次序可以任意调换.

证 用归纳法.假设$i_1i_2\cdots i_n$是$1,2,\ldots,n$的任意一个排列,注意到

$$\begin{aligned}
& a_{i_1}\circ a_{i_2}\circ\cdots\circ a_{i_n}\\
= \ & [(a_{i_1}\circ\cdots\circ a_{i_{k-1}}\circ a_1)]\circ(a_{i_{k+1}}\circ\cdots\circ a_{i_n})\\
= \ & [(a_1\circ(a_{i_1}\circ\cdots\circ a_{i_{k-1}}))]\circ(a_{i_{k+1}}\circ\cdots\circ a_{i_n})\\
= \ & a_1\circ(a_2\circ\cdots\circ a_{n-1})\\
= \ & a_1\circ a_2\circ\cdots\circ a_n
\end{aligned}$$

即得. □

§6 分配律

定义 6.1 设$\odot$是一个$B\times A$到A的代数运算,$\oplus$是一个A上的代数运算, 如果对$\forall b\in B,\forall a_1,a_2\in A$,有

$$b\odot(a_1\oplus a_2)=(b\odot a_1)\oplus(b\odot a_2)$$

则称代数运算$\odot,\oplus$满足第一分配律.

例 6.1 设${}_FV$是线性空间,$\odot$是数与向量的乘法,$\oplus$是向量的加法,则第一分配律就变成

$$k(\alpha+\beta)=(k\alpha)+(k\beta).$$

定理 6.1 设$\oplus$满足结合律,且$\odot,\oplus$满足第一分配律,则对$\forall b\in B,\forall a_1,a_2,\ldots,a_n\in A$,有

$$b\odot(a_1\oplus\cdots\oplus a_n)=(b\odot a_1)\oplus\cdots\oplus(b\odot a_n).$$

证 用归纳法.注意到

$$\begin{aligned}
& b\odot(a_1\oplus\cdots\oplus a_n)\\
= \ & b\odot[(a_1\oplus\cdots\oplus a_{n-1})\oplus a_n]\\
= \ & [b\odot(a_1\oplus\cdots\oplus a_{n-1})]\oplus(b\odot a_n)\\
= \ & [(b\odot a_1)\oplus\cdots\oplus(b\odot a_{n-1})]\oplus(b\odot a_n)\\
= \ & (b\odot a_1)\oplus\cdots\oplus(b\odot a_n)
\end{aligned}$$

即得. □

类似地,可以定义第二分配律

$$(a_1 \oplus a_2) \odot b = (a_1 \odot b) \oplus (a_2 \odot b).$$

且同理可证

定理 6.2 若$\oplus$满足结合律,且$\odot, \oplus$满足第二分配律,则对$\forall b \in B, \forall a_1, a_2, \ldots, a_n \in A$,有

$$(a_1 \oplus \cdots \oplus a_n) \odot b = (a_1 \odot b) \oplus \cdots \oplus (a_n \odot b).$$

§7 一一映射、变换

定义 7.1 设$f : A \to B$.

(1) 若对$\forall b \in B, \exists a \in A, \ni (= \text{such that}) f(a) = b$ *(即*B*中的每个元素都有逆象),则称*f*为*A*到*B*的满射;*

(2) 若$a \neq b \Rightarrow f(a) \neq f(b)$*(即*$A$*中不同元素的象不同), 则称*$f$*为*$A$*到*$B$*的单射;*

(3) 若f*既是单射又是满射,则称*f*为*A*到*B*的一一映射.*

显然,对任意集合A,恒等映射$I_A : A \to A; a \mapsto a$是一一映射.

定理 7.1 设A, B是两个非空集合,且$f : A \to B$.

(1) f*为单射当且仅当存在映射*$g : B \to A, \ni gf = I_A$;

(2) f*为满射当且仅当存在映射*$h : B \to A, \ni fh = I_B$;

(3) f*为一一映射当且仅当存在一一映射*$f^{-1} : B \to A, \ni ff^{-1} = I_B, f^{-1}f = I_A$*,并称*$f^{-1}$*为*$f$*的逆映射.*

证 (1) ($\Rightarrow$).任取定$a_0 \in A$,定义

$$g : B \to A; b \mapsto \begin{cases} a, & \text{若} b = f(a), \\ a_0, & \text{其它} \end{cases}$$

容易验证,g为映射且$\forall a \in A, gf(a) = g(f(a)) = a = I_A(a)$,所以$gf = I_A$.

($\Leftarrow$).$\forall a_1, a_2 \in A, a_1 \neq a_2$,有$g(f(a_1)) = gf(a_1) = I_A(a_1) = a_1 \neq a_2 = I_A(a_2) = gf(a_2) = g(f(a_2))$,所以$f(a_1) \neq f(a_2)$,即$f$为单射.

(2) ($\Rightarrow$).由于f为满射知,$\forall b \in B, f^{-1}(b) \neq \emptyset$(即$b$的逆象集非空),根据选择公理,可在$B$的每个元素的原象集合$f^{-1}(b)$中选取一个元素$a$, 定义$h : B \to A; b \mapsto a$,则$h$为映射且$\forall b \in B, fh(b) = f(h(b)) = b = I_B(b)$,所以$fh = I_B$.

($\Leftarrow$).$\forall b \in B, \exists h(b) \in A, \ni f(h(b)) = I_B(b) = b$,所以$f$为满射.

(3) ($\Rightarrow$).由f是一一映射可知有$g,h:B\to A$使$gf=I_A, fh=I_B$.下证$g=h$:
事实上,对$\forall b\in B$,

$$g(b)=gI_B(b)=g(fh)(b)=(gf)h(b)=I_Ah(b)=h(b),$$

所以,$g=h\overset{\text{def}}{=}f^{-1}$, f^{-1}满足要求.
($\Leftarrow$).由(1)与(2)即得. □

定义 7.2 一个A到A的映射叫做A的一个变换.
一个A到A的满射、单射或A与A间的一一映射分别叫做A的一个满射变换、单射变换或一一变换.

例 7.1 $A=\mathbb{R}$,则$A\to A; x\mapsto e^x$是A的单射变换.

例 7.2 $A=\mathbb{Z}$,则

$$A\to A; x\mapsto \begin{cases} x, & x\text{为奇数},\\ x/2 & x\text{为偶数}\end{cases}$$

是A的满射变换; 而$A\to A; x\mapsto x+1$是A的一一变换.

映射可以表征两个集合之间元素的多寡,要研究具有代数运算的两个集合之间的关系, 还需要学习下面的同态的概念.

§8 同态

定义 8.1 设$\circ,*$分别是集合A,B的代数运算,$f:A\to B$.若对$\forall a,b\in A$,有

$$f(a\circ b)=f(a)*f(b),$$

则称f是A到B的同态映射.此外,若f还是满射,则称f为满同态;若f为单射,则称f为单同态;若f为一一映射, 则称f为同构,并记为$A\cong B$.

例 8.1 设$A=\mathbb{Z}, B=\{1\}, C=\{-1\}$, A中的代数运算为通常的加法或乘法, B中的代数运算为通常的乘法,则$n\mapsto 1$为A到B的同态满射, $n\mapsto -1$不是A到C的同态映射.

例 8.2 设$A=\mathbb{Z}, B=\{1,-1\}$, A中的代数运算为通常的加法,B中的代数运算为通常的乘法,则

$$A\to B;\quad n\mapsto \begin{cases} 1, & n\text{ 为偶数},\\ -1 & n\text{为奇数}\end{cases}$$

是A到B的同态满射.

定义 8.2 若存在$(A,\circ)$到$(\bar{A},\bar{\circ})$的满射的同态映射,则称这个映射是一个同态满射,并称对于代数运算$\circ$与$\bar{\circ}$来说, A与$\bar{A}$同态.

定理 8.1 假设对于代数运算$\circ$和$*$来说,A与B存在满同态f.

(1) 若$\circ$适合结合律,则$*$也适合结合律;

(2) 若$\circ$适合交换律,则$*$也适合交换律.

证 (1) 可以假设$f(a),f(b),f(c)$是B的任意三个元素,于是

$$\begin{aligned}&(f(a)*f(b))*f(c)\\ =\ & f(a\circ b)*f(c)\\ =\ & f((a\circ b)\circ c)\\ =\ & f(a\circ(b\circ c))\\ =\ & f(a)*f(b\circ c)\\ =\ & f(a)*(f(b)*f(c)).\end{aligned}$$

(2) 可以假设$f(a),f(b)$是B的任意两个元素,则

$$f(a)*f(b)=f(a\circ b)=f(b\circ a)=f(b)*f(a).$$

□

定理 8.2 假定$\odot,\oplus$都是集合A的代数运算,$\bar{\odot},\bar{\oplus}$都是集合B的代数运算,并且存在一个A到B的满射f,使得A与B对于代数运算$\odot,\bar{\odot}$来说同态,对于代数运算$\oplus,\bar{\oplus}$来说也是同态.

(1) 若$\odot,\oplus$满足第一分配律,则$\bar{\odot},\bar{\oplus}$也满足第一分配律;

(2) 若$\odot,\oplus$满足第二分配律,则$\bar{\odot},\bar{\oplus}$也满足第二分配律.

证 只证(2).事实上,由

$$\begin{aligned}&(f(a)\bar{\oplus}f(b))\bar{\odot}f(c)\\ =\ & f(a\oplus b)\bar{\odot}f(c)\\ =\ & f((a\oplus b)\odot c)\\ =\ & f((a\odot c)\oplus(b\odot c))\\ =\ & f(a\odot c)\bar{\oplus}f(b\odot c)\\ =\ & (f(a)\bar{\odot}f(c))\bar{\oplus}(f(b)\bar{\odot}f(c))\end{aligned}$$

得证. □

作业

P6. 1; P9. 1,2; P12. 2;
P14. 2; P19. 3; P23. 1

§9 同构、自同构

我们已经知道,同构是一一映射的同态.

例 9.1 设$A=\mathbb{Z}^+=\{1,2,3,\ldots\},\bar{A}=\mathbb{Z}^-=\{-1,-2,-3,\ldots\}$,而运算$\circ,\bar{\circ}$都是整数中通常的加法"+", 现作$\varphi:(A,\circ)\to(\bar{A},\bar{\circ})$,其中$\varphi(n)=-n$,则$\varphi$是同构映射.

事实上

(1) φ显然是映射;

(2) φ是单射:当$m,n\in A,m\neq n$时,$\varphi(m)\neq\varphi(n)$, 所以φ是单射;

(3) φ是满射:$\forall n\in\bar{A}$有$-n\in A$,使$\varphi(-n)=n$, 所以φ是满射;

(4) φ是同态映射:$\forall m,n\in A$

$$\varphi(m\circ n)=\varphi(m+n)=-(m+n)=(-m)+(-n)=\varphi(m)\bar{\circ}\varphi(n),$$

由*(1),(2),(3)*知,φ是同构映射,即$A\cong\bar{A}$.

例 9.2 设$A=\{1,2,3\},\bar{A}=\{4,5,6\}$,其运算$\circ,\bar{\circ}$如下

$\circ$	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

$\bar{\circ}$	4	5	6
4	6	6	6
5	6	6	6
6	6	6	6

作$\varphi:A\to\bar{A}$,其中$\varphi(1)=4,\varphi(2)=5,\varphi(3)=6$.则$\varphi$是$A$到$\bar{A}$的同构映射.

一般地,假设对于代数运算$\circ$与$\bar{\circ}$来说,A与$\bar{A}$同构,则仅考虑代数运算$\circ$与$\bar{\circ}$来说,A与$\bar{A}$没有什么区别(仅符号上的差别而已).简单地说,在代数中,同构的对象我们认为是相同的.特别地,

定义 9.1 对于$\circ$与$\circ$来说,A与A间的同构映射称为一个对于$\circ$ 来说的自同构.

例 9.3 求$(\mathbb{Z},+)$的自同构映射.

解. 设φ是$\mathbb{Z}$的同构映射,且设$\varphi(1)=a$,则$\forall n\in\mathbb{Z},\varphi(n)=n\varphi(1)=na$.

由于φ为双射,所以$\exists m\in\mathbb{Z},\ni 1=\varphi(m)=m\varphi(1)=ma$,于是$a=1$或$a=-1$.

另一方面,容易验证:$\varphi:\mathbb{Z}\to\mathbb{Z};n\mapsto n$ 或$\varphi:\mathbb{Z}\to\mathbb{Z};n\mapsto -n$是$\mathbb{Z}$的同构映射. □

§10 等价关系与集合的分类

定义 10.1 设A为集合,称$R(\subset A\times A)$为A上的一个二元关系.如果$(a,b)\in R$,则称a与b具有关系R,也记为aRb.如果R上的二元关系满足

(1) 自反性:$\forall a\in A, aRa$;

(2) 对称性:$\forall a,b\in A, aRb\Rightarrow bRa$;

(3) 传递性:$\forall a,b,c\in A, aRb$且$bRc\Rightarrow aRc$

则称R为A上的等价关系,此时把aRb简记为$a\sim_R b$或$a\sim b$.

例 10.1 $\mathbb{Z}$上的"等于"关系是等价关系,而$\leq,<$等均不是$\mathbb{Z}$上的等价关系.

例 10.2 $\mathbb{Z}$上的关于模n的同余关系是等价关系.

证. 设$n\in\mathbb{Z}^+,\forall x,y\in\mathbb{Z}$定义$\sim$如下:

$$x\sim y\Leftrightarrow x\equiv y\pmod n(\text{即}n\mid x-y).$$

欲证$\sim$为等价关系,只需证:对$\forall x,y,z\in\mathbb{Z}$有

(1) $x\sim x$,即$x\equiv x\pmod n$;

(2) $x\sim y\Rightarrow y\sim x$即$x\equiv y\pmod n\Rightarrow y\equiv x\pmod n$.

(3) $x\sim y, y\sim z\Rightarrow x\sim z$即$x\equiv y\pmod n$且$y\equiv z\pmod n\Rightarrow x\equiv z\pmod n$. □

例 10.3 设$R^*=\{\{a_n\}\mid\{a_n\}$为有理数基本列$\}$,定义R^*上如下:$\{a_n\}\sim\{b_n\}$定义为$\forall\varepsilon>0,\exists N>0$,当$n>N$时,$|a_n-b_n|<\varepsilon$.其中$\varepsilon,N$均为有理数. 容易验证$\sim$为$R^*$上的等价关系.

定义 10.2 设R是A上的等价关系,对$\forall a\in A, a$关于R的等价类$[a]_R$(或$[a],\bar{a}$)定义为$\{b\in A\mid aRb\}$.

例 10.4 若R为$\mathbb{Z}$上关于模n的同余关系,则$[a]=\{b\in\mathbb{Z}\mid a\equiv b\pmod n\}=\{a+kn\mid k\in\mathbb{Z}\}$.且只有$n$个等价类:$[0],[1],\ldots,[n-1]$.

例 10.5 例*10.3*有无数多个等价类,每个等价类$[a_n]$ 被称为实数.

等价类具有一些重要性质:

定理 10.1 设$\sim$为A上的等价关系,则

(1) $\forall a\in A, a\in[a]$;

(2) $\forall a,b\in A, a\sim b\Leftrightarrow[a]=[b]$;

(3) $\forall a,b\in A, a\nsim b\Leftrightarrow[a]\cap[b]=\emptyset$;

(4) $\forall a,b\in A,[a]=[b]$与$[a]\cap[b]=\emptyset$恰具其一;

(5) $\cup\{[a]\mid a\in A\}=A$.

证 (1) 因为$a \in A, a \sim a$,所以$a \in [a]$.

(2) 设$a, b \in A$且$a \sim b, c \in [a]$,则$c \sim a$,于是$c \sim b$, 所以$c \in [b]$即$[a] \subset [b]$;再由$b \sim a$同样可得$[b] \subset [a]$. 所以$[a] = [b]$.

(3) 设$a \nsim b$,且$[a] \cap [b] \neq \emptyset$则有$c \in [a] \cap [b]$, 于是$c \sim a, c \sim b$,从而$a \sim b$, 矛盾,所以$[a] \cap [b] = \emptyset$.反之,由(2),若$a \sim b$,则$[a] = [b]$,此与$[a] \cap [b] = \emptyset$相矛盾.

(4) 由(2),(3)即得.

(5) 由$a \in [a]$即得. □

定义 10.3 设$A \neq \emptyset$,若A的一些子集$A_i, i \in I$满足

(1) $A_i \neq \emptyset$;

(2) $\forall i, j \in I, A_i \neq A_j \Rightarrow A_i \cap A_j = \emptyset$;

(3) $\cup_{i \in I} A_i = A$.

则称$A_i, i \in I$为集合A的一个分类*(*或划分*)*.

等价关系与集合的分类有如下关系:

定理 10.2 *(1)* 集合A的一个分类决定A上的一个等价关系*;*

(2) 集合A上的一个等价关系决定A的一个分类.

证 (1) 设$A_i, i \in I$为集合A的一个分类,定义$\sim$为

$$a \sim b \Leftrightarrow \exists i \in I, \ni a, b \in A_i.$$

则$\sim$是A上的一个等价关系.

(2) 设$\sim$为A上的等价关系,则A关于等价关系确定的所有的等价类$[a], a \in A$ 就是A的一个分类. □

定义 10.4 假设集合A有一个分类.一个类中的任意一个元叫做这个类的一个代表,刚好由每一类的一个代表作成的集合叫做几个全体代表团.

例 10.6 例*10.2*有n个等价类:$[0], [1], [2], \ldots, [n-1]$.这个类叫做模$n$的剩余类.通常用$0, 1, \ldots, n-1$作为这$n$个类的全体代表团.

作 业

P.26 1,2,3 P.30 1,2,3

练习与思考题

1. 给定集合A及其运算如下

$*$	1	2	3	4
1	2	3	1	2
2	3	4	2	1
3	1	2	3	4
4	1	2	4	4

   (1) 该运算是否交换?

   (2) 该运算是否存在单位元?

   (3) 如果存在单位元,哪些元素在A中有逆元素?

2. 设$|A| = m, |B| = n$,求

   (1) A到B的映射的个数;

   (2) A到B的单射的个数;

   (3) A到B的满射的个数.

3. 设φ是集合A到B的任意一个映射,S与S'分别为A与B的非空子集.证明:

   (1) $\varphi^{-1}(\varphi(S)) \supseteq S$,且当$\varphi$为单射时等号成立;

   (2) $\varphi(\varphi^{-1}(S)) \subseteq S$,且当$\varphi$为满射时等号成立.

4. 设$f : A \to B, g : B \to C$.证明:

   (1) 若f, g均为单射,则gf为单射;

   (2) 若gf为单射,则f为单射;

   (3) 若f, g为满射,则gf为满射;

   (4) 若gf为满射,则g为满射.

5. 设$f : A \to B$.证明

   (1) f为单射$\Leftrightarrow$对任意集合X到A的任意映射g_1, g_2,若$fg_1 = fg_2$,则$g_1 = g_2$;

   (2) f为满射$\Leftrightarrow$对任意集合B到Y的任意映射h_1, h_2,若$h_1 f = h_2 f$,则$h_1 = h_2$.

6. 设$f : A \to B$为满射,则f为双射$\Leftrightarrow$ f有唯一的左逆.

7. 设A与B是数域F上两个n阶相似方阵,$F[A]$为系数属于F的关于A的一切多项式作成的集合.证明:$\forall f(x) \in F[x], \varphi : F[A] \to F[B]; f(A) \mapsto f(B)$为双射.

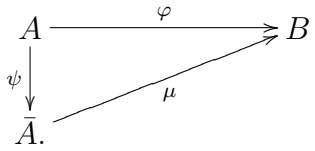
8. 定义$\mathbb{N} \times \mathbb{N}$上的关系如下:$(a,b) \sim (c,d) \Leftrightarrow a+d=b+c$,证明:$\sim$是等价关系,能求出其全体代表团吗?

9. 证明:等价关系的三个条件可以改为

   (1) $a \sim a$;

   (2) 如果$a \sim b, b \sim c$,则$b \sim c$.

10. 设$\varphi : A \to B$是满射,定义A上的二元关系如下:$a \sim b \Leftrightarrow \varphi(x) = \varphi(y)$,证明这是一个等价关系.等价类的集合记为$\bar{A}$,$\bar{A}$中的元素记为$\bar{a}$.定义$\psi : A \to \bar{A}$使$\psi(a) = \bar{a}$,证明$\psi$也是满射,并且$\mu : \bar{a} \to \varphi(a)$是$\bar{A}$到$B$的双射.同时映射等式$\mu\psi = \varphi$成立,此等式可用下面的交换图表示



11. 定义$\mathbb{Z}$中的运算$*$如下:$a * b = a + b - 1$.证明:$(\mathbb{Z}, *)$与$(\mathbb{Z}, +)$同构.

12. 设$N = \{0, 1, 2, , \ldots\}, N^* = \{1, 2, \ldots\}$.$(N, +)$ 与$(N^*, +)$ 不同构,$(N, \cdot)$与$(N^*, \cdot)$也不同构.

13. $(\mathbb{Z}, +)$与$(\mathbb{Z}, \cdot)$不同构.

14. $(\mathbb{Q}, +)$与$(\mathbb{Q}, \cdot)$不同构.

判天地之美，析万物之理
—庄子

吾思故吾在
—[法]笛卡尔

第二章 群论

§1 群的概念

定义 1.1 (第一定义) 设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) 封闭性: $\forall a,b\in G, ab\in G$;

(2) 结合律: $\forall a,b,c\in G, a(bc)=(ab)c$;

(3) $\forall a,b\in G$,方程

$$ax=b,\quad ya=b$$

都在G中有解,

则称G关于该代数运算成为群.

定义 1.2 (第二定义) 设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) 封闭性: $\forall a,b\in G, ab\in G$;

(2) 结合律: $\forall a,b,c\in G, a(bc)=(ab)c$;

(3) 单位元: $\exists e\in G, \ni \forall a\in G, ea=ae=a$;

(4) 逆元: $\forall a\in G, \exists a^{-1}\in G, \ni aa^{-1}=a^{-1}a=e$,

则称G关于该代数运算成为群.

定义 1.3 (第三定义) 设G为非空集合,若存在二元运算(称为乘法)满足下列条件:

(1) 封闭性: $\forall a,b\in G, ab\in G$;

(2) 结合律: $\forall a,b,c\in G, a(bc)=(ab)c$;

(3) 左单位元: $\exists e\in G, \ni \forall a\in G, ea=a$;

(4) 左逆元: $\forall a\in G, \exists a^{-1}\in G, \ni a^{-1}a=e$,

则称G关于该代数运算成为群.

这里给出了群的三个定义,实际上,这三个定义是等价的.

第一定义⇒第二定义: 由$ax=a, ya=a$分别得解e_r, e_l.对$\forall b\in G, \exists c,d\in G\ni ac=b, da=b$,于是$e_lb=(e_la)c=ac=b, be_r=d(ae_r)=da=b$,所以$e_l=e_le_r=e_r\overset{\text{def}}{=}e$,且$\forall b\in G, eb=be=e$.再由$ax=e, ya=e$分别得解$a_r, a_l$,于是$a_l=a_le=a_l(aa_r)=(a_la)a_r=ea_r=a_r\overset{\text{def}}{=}a^{-1}$.

第二定义⇒第三定义是自动的.

第三定义⇒第二定义: 由条件,$\forall a\in G, \exists a^{-1}\in G\ni a^{-1}a=e$,可知$\exists a'\in G\ni a'a^{-1}=e$,于是$aa^{-1}=e(aa^{-1})=(a'a^{-1})(aa^{-1})=a'((a^{-1}a)a^{-1})=a'a^{-1}=e$(即左逆元也为右逆元),所以$a=ea=(aa^{-1})a=a(a^{-1}a)=ae$(即左单位元也为右单位元).故对$\forall a,b\in G$,方程$ax=b, ya=b$分别有解$a^{-1}b, ba^{-1}$.

定义 1.4 设G为群.

(1) G中使$\forall a\in G$,均有$ea=ae=a$的元素e叫做G的单位元;

(2) G中使$\forall a\in G$, 均有$ea=a$的元素e叫做G的左单位元;

(3) G中使$\forall a\in G$, 均有$ae=a$的元素e叫做G的右单位元;

(4) 对$a\in G$,使$a'a=aa'=e$的元素a'叫做G的逆元,记为a^{-1};

(5) 对$a\in G$,使$a'a=e$的元素a'叫做G的左逆元;

(6) 对$a\in G$,使$aa'=e$的元素a'叫做G的右逆元.

推论 1.1 群G的单位元是惟一的.

推论 1.2 设G为群,$a\in G$.a的逆元是惟一的.

定义 1.5 元素个数有限的群叫做有限群, 有限群G的元素个数称为这个群的阶,简记为$|G|$. 不是有限群的群叫做无限群.

定义 1.6 设G为群,如果对$\forall a,b\in G$均有$ab=ba$,则称G为交换群(或*Abel*群).

注 1.1 *(1)* 如果非空集合G上的二元运算满足群定义中的第一、二两个条件, 则称G为半群.

(2) 将第三定义中的左改成右,可得群的又一等价定义.

(3) 将第三定义中的一个左改为右,不能得出群的定义.见

$$\begin{array}{c|cc} \circ & e & a \\ \hline e & e & a \\ a & e & a \end{array} \quad \text{或} \quad \begin{array}{c|cc} \circ & e & a \\ \hline e & e & e \\ a & a & a \end{array}.$$

(4) 由于群中的运算满足结合律,因此$a_1a_2\cdots a_n$是有意义的, 通常记$\overbrace{aa\cdots a}^{n}$($n$为正整数)为$a^n$.

(5) 群中元素a的逆元通常记为a^{-1}.且对任意整数m,n有

$$a^m\cdot a^n=a^{m+n},(a^m)^n=a^{mn}.$$

(6) 当群是加法群时,称逆元为负元,记a 的负元为$-a$;称单位元为零元,记为0.此时, 对任意整数m,n有

$$\begin{gathered} ma=\overbrace{a+a+\cdots+a}^{m}, \\ 0a\overset{\text{def}}{=}0, \\ ma+na=(m+n)a, na+nb=n(a+b), \\ m(na)=(mn)a, \\ (-n)a=\overbrace{-a-a-\cdots-a}^{n}=-(\overbrace{a+a+\cdots+a}^{n})=-(na). \end{gathered}$$

例 1.1 设$G=\{g\}$,乘法是$gg=g$.G关于这个乘法作成一个群.

例 1.2 设$G=\mathbb{Z}$,G关于通常的加法作成群,但G关于通常的乘法作成半群,不作成群.

例 1.3 设$G=\{0,1,2,3,4,5,6\}$,G中的运算为

$$i\circ j=\begin{cases} i+j, & \text{若} i+j\leq 6 \\ i+j-6, & \text{若} i+j>6 \end{cases}$$

则$(G,\circ)$作成一个群.这个群也记为$(\mathbb{Z}_7,+)$.

例 1.4 (上例的一般情形) 设$\mathbb{Z}_n$是模n的剩余类(即$\mathbb{Z}_n=\{[0],[1],\ldots,[n-1]\}$),定义$\mathbb{Z}_n$中的加法"$+$":$[i]+[j]=[i+j]$,则$(\mathbb{Z}_n,+)$ 成为一个群.

例 1.5 设$\mathbb{Z}_7 = \{[1],[2],[3],[4],[5],[6]\}$, $\mathbb{Z}_7^*$ 中的运算为

$$[i]\cdot[j] = [ij],$$

则$(\mathbb{Z}_7^*,\cdot)$作成一个群.

例 1.6 设$G=\mathbb{Z}$, G中的运算定义为$a\circ b = a+b-2$, $(G,\circ)$作成群.

例 1.7 设F为数域,$M_n(F)$为数域F上的所有n阶矩阵的集合,则$M_n(F)$关于矩阵加法作成群,$M_n(F)$关于矩阵乘法不构成群.

例 1.8 设$GL_n(F)$为数域F上所有n阶可逆矩阵的集合,则$GL_n(F)$关于矩阵的乘法作成群.这个群叫做一般线性群.当$n>1$时, 这个群不是交换群.

例 1.9 设$SL_n(F)$为数域F上所有行列式等于1的n阶矩阵的集合,则$GL_n(F)$关于矩阵的乘法作成群.这个群叫做特殊线性群. 当$n>1$时,这个群也不是交换群.

练习

判断下列哪些代数体系是群,为什么?

1 $(\mathbb{Z},+)$; $(\mathbb{Z},\cdot)$;

2 $(\mathbb{Q},+)$; $(\mathbb{Q},\cdot)$; $(\mathbb{Q}^*,\cdot)$;

3 $(\mathbb{R},+)$; $(\mathbb{R},\cdot)$; $(\mathbb{R}^{\cdot},\cdot)$;

4 $(\mathbb{C},+)$; $(\mathbb{C},\cdot)$; $(\mathbb{C}^{\cdot},\cdot)$;

5 $(\mathbb{N},+)$; $(\mathbb{N},\cdot)$; $(\mathbb{N}^+,+)$; $(\mathbb{N}^+,\cdot)$;

6 $(M_n(F),+)$; $(M_n(F),\cdot)$; $(M_n(F)^*,\cdot)$;

7 $(\mathbb{R},\circ)$,其中运算为$x\circ y = x+y+c, c$为常数;

8 $(\mathbb{R}^*,\circ)$,其中运算为$x\circ y = xy/2$;

9 $(\mathbb{R}-\{-1\},\circ)$,其中运算为$x\circ y = x+y+xy$;

10 $(\{x\mid x\in\mathbb{R}, -1<x<1\},\circ)$其中运算为$x\circ y = \dfrac{x+y}{xy+1}$.

§2 单位元、逆元、削去律

定义 1.7 设G为群,$a \in G$.使$a^m = e$的最小正整数m称为a的阶,记为$|a| = m$.如果这样的m不存在, 则称a的阶是无限的,记为$|a| = +\infty$.

例 1.10 群$(\mathbb{Z}_7^*, \cdot)$中,$|[1]| = 1, |[2]| = |[4]| = 3, |[3]| = |[5]| = 6, |[6]| = 2$.

例 1.11 群$(\mathbb{Z}, +)$中,$|0| = 1, |n| = +\infty (n \neq 0)$.

注 1.2 加法群G中,设$a \in G$, 能够使$ma = 0$的最小正整数m叫做a的阶,若这样的m不存在,则称a的阶是无限的,a的阶仍记为$|a|$.

例 1.12 设$G = \{\varepsilon_0, \varepsilon_1, \varepsilon_2\}$是$x^3 = 1$的三个复根的集合,$G$的运算是复数乘法,则$(G, \cdot)$作成一个群,且$|\varepsilon_0| = 1, |\varepsilon_1| = |\varepsilon_2| = 3$.

注 1.3 思考题 设$G = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$是$n$次单位根的集合,即$\varepsilon_k = \cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n}, k = 0, 1, \ldots, n-1$,则$G$关于复数乘法也构成群.元素$|\varepsilon_k| =$?

定理 1.1 每个群都适合消去律:

(1) 左消去律 $ax = ax' \Rightarrow x = x'$;

(2) 右消去律 $ya = y'a \Rightarrow y = y'$.

§3 有限群的另一定义

定理 3.1 (定理与定义) 设G是一个有限集,若$(G, \circ)$满足*(1)* 封闭性,*(2)* 结合律,*(3)* 消去律,那么$(G, \circ)$一定是一个群.

证 设$G = \{a_1, a_2, \ldots, a_n\}$,注意到对$\forall a_i \in G$有

$$\{a_i a_1, a_i a_2, \ldots, a_i a_n\} = G$$

即得. □

一、问题与练习

1 若$|G| = +\infty$,即使$(G, \circ)$能满足封闭性、结合律和消去律, $|G|$也不可能成为群.对吗?

2 设G是个有限半群,则G为群$\Leftrightarrow$ G中消去律成立.

3 设G是群.

(1) $\forall a \in G$,若存在$n \in \mathbb{Z}^+$, 使$a^n = e$,则$|a| \leq n$;

(2) $\forall a \in G, |a| = |a^{-1}|$;

(3) $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$;

(4) $\forall a_1, a_2, \ldots, a_n \in G, (a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$;

(5) 在G中判断正误: (i) $x^2 = e \Rightarrow a = e$; (ii) $x^2 = a^2 \Rightarrow x = a$; (iii) $(ab)^2 = a^2b^2$; (iv) $x^2 = x \Rightarrow x = e$; (v) $a^k = e \Rightarrow |a| = k$;

(6) 在G中解关于x的方程: (i) $axb = c$; (ii) $x^2b = xa^{-1}c$;
(iii) $(xax)^3 = bx$且$x^2a = (xa)^{-1}$; (iv) $ax^2 = b$且$x^3 = e$; (v) $x^2 = a^2$ 且$x^5 = e$;

4 如果G是有限群,则G的每个元素都是有限阶的.(其逆成立吗?为什么?)

二、几个结论

设G为群.关于G的元素的阶有如下结论:

1 设$a \in G$,若$\exists m \in \mathbb{Z}^+, \ni a^m = e$,则$|a| = n < +\infty$且$n \mid m$.

2 设$a \in G$且$|a| = n$.则$\forall m \in \mathbb{Z}, a^m = e \Leftrightarrow n \mid m$.

3 设$a, b \in G$且$|a| = m, |b| = n, ab = ba$,记$g = [m, n]$,则

(1) $|ab| \mid g$;

(2) 若$(m, n) = 1$则$|ab| = g = mn$;

(3) 若$|a^k| = \dfrac{m}{(k, m)}$;

(4) 存在$d \in G \ni |d| = g$;

4 若G为可换群,且G中存在阶最大的元素$a, |a| = m$,则$\forall b \in G, |b| \mid m$.

§4 群的同态

一、群同构

设$(G, \circ)$与$(\bar{G}, \bar{\circ})$是两个群.如果存在双射$\varphi : G \to \bar{G} \ni \forall a, b \in G, \varphi(a \circ b) = \varphi(a) \bar{\circ} \varphi(b)$, 则称$\varphi$是同构映射, 并称$G$与$\bar{G}$同构,记为$G \cong \bar{G}$.对于同构的群,我们认为是代数相同的,因为它们除了符号与名称上的区别之外, 二者没有实质的差异.

性质 4.1 *设$\varphi : G \to \bar{G}$是群的同构映射,则$\varphi^{-1} : \bar{G} \to G$ 也是群的同构映射.*

性质 4.2 设$\varphi_1 : G_1 \to G_2, \varphi_2 : G_2 \to G_3$均为群的同构映射, 则$\varphi_2\varphi_1 : G_1 \to G_3$也是群的同构映射.

二、群同态

设$(G, \circ)$与$(\bar{G}, \bar{\circ})$是两个群.如果存在映射$\varphi : G \to \bar{G} \ni \forall a, b \in G, \varphi(a \circ b) = \varphi(a)\bar{\circ}\varphi(b)$, 则称$\varphi$是群同态映射; 如果$\varphi$是满射,则称$\varphi$是群满同态映射, 并称$G$与$\bar{G}$同态, 记为$G \sim \bar{G}$.

定理 4.1 设φ是$(G, \circ)$到$(\bar{G}, \bar{\circ})$的同态满射.若$(G, \circ)$是群, 则$(\bar{G}, \bar{\circ})$也是群.

注 4.1 本定理的逆是不成立的:令$G = \{$一切奇数$\}$,其运算为通常的乘法,$\bar{G} = \{e\}$ 是一个元素的群,$\varphi : G \to \bar{G}; n \mapsto e$是满同态,但$G$不是群.

例 4.1 设$A = \{a, b, c\}$, A的乘法为

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明:A作成一个群.

分析:本题通过运算表也许能解决单位元和逆元问题,但结合律的检验相当麻烦. 证明思路是:设法找一个群G,使A是G的同态象.

证. $(\mathbb{Z}, +)$是一个群,定义映射为

$$\varphi : \mathbb{Z} \to A; \quad n \mapsto \begin{cases} a, \text{若} n \equiv 0 \pmod 3; \\ b, \text{若} n \equiv 1 \pmod 3; \\ c, \text{若} n \equiv 2 \pmod 3. \end{cases}$$

则φ为满射,且φ为同态:

(1) 当$m \equiv 0 \pmod 3, n \equiv 0 \pmod 3$时,$\varphi(m+n) = a = aa = \varphi(m)\varphi(n)$;

(2) 当$m \equiv 0 \pmod 3, n \equiv 1 \pmod 3$时,$\varphi(m+n) = b = ab = \varphi(m)\varphi(n)$;

(3) 当$m \equiv 0 \pmod 3, n \equiv 2 \pmod 3$时,$\varphi(m+n) = c = ac = \varphi(m)\varphi(n)$;

(4) 当$m \equiv 1 \pmod 3, n \equiv 1 \pmod 3$时,$\varphi(m+n) = c = bb = \varphi(m)\varphi(n)$;

(5) 当$m \equiv 1 \pmod 3, n \equiv 2 \pmod 3$时,$\varphi(m+n) = a = bc = \varphi(m)\varphi(n)$;

(6) 当$m \equiv 2 \pmod 3, n \equiv 2 \pmod 3$时,$\varphi(m+n) = b = cc = \varphi(m)\varphi(n)$.

所以,$\mathbb{Z}$与A同态,由定理,A是群. □

定理 4.2 设$\varphi: G \to \bar{G}$是群同态满射.则

(1) 若e是G的单位元,则$\varphi(e) = \bar{e}$是$\bar{G}$的单位元;

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

注 4.2 设$\varphi: G \to \bar{G}$是两个代数系统的同态映射*(*未必是满射*)*,上面两个定理就未必成立了.但我们可以考虑φ的象集合$\bar{\bar{G}} = \{\varphi(x) \mid \forall x \in G\}$,则$\varphi: G \to \bar{\bar{G}}$是同态满射,上面的定理又可以用了.

定义 4.1 设G是群.若φ是G到G自身的同态,则称φ为G的一个自同态;若φ是G到G自身的同构,则称φ为G的一个自同构.

例 4.2 设$G = F[x]$为多项式加法群,映射$\varphi: G \to G; (f(x)) \mapsto f'(x)$ 是G的自同态.

例 4.3 设G为群,G的自同态集合通常记为$End\ G$,则$End\ G$关于映射的复合作成一个幺半群.

例 4.4 设G为群,a为G的任一元素,则$\varphi_a: G \to G; x \mapsto axa^{-1}$是$G$的自同构,这个同构称为$G$的内自同构.

例 4.5 设G为群,G的所有自同构所组成的集合记为$Aut\ G$,则$Aut\ G$关于映射的复合作成一个群;G的所有内自同构所组成的集合记为$Inn\ G$,$Inn\ G$关于映射的复合也作成一个群.显然有

$$Inn\ G \subset Aut\ G \subset End\ G.$$

例 4.6 设G为群,$\varphi: G \to G; x \mapsto x^{-1}$,则$\varphi$是自同构$\Leftrightarrow$ G是*Abel*群.

作业p. 35 1,2 p. 38 2,4 p. 44 习题

§5 变换群

研究一种代数体系就是要解决这种代数体系的下面三个问题:

1 存在问题;

2 数量问题

3 结构问题.

如果这些问题都得到完满的解答就算达到了目的. 关于数量问题,指的是彼此不同构的代数体系的数量, 因为同构的代数体系抽象地看可以认为是相同的代数体系.

凯莱定理告诉我们,如果将所有变换群都研究清楚了, 也就等于把所有群都研究清楚了.

一、集合A的变换和表示形式

先回顾一个定义:

定义 5.1 设$A \neq \emptyset$,若τ是A到A自己的映射,则称τ是A的一个变换.

注 5.1 注意 在表示形式方面,当$\tau : A \to B$是映射时,用"$\tau(a)$"表示a的象;当$\tau : A \to A$是变换时,使用"a^τ"表示a的象.

如果τ_1, τ_2都是A的变换,$\tau_1\tau_2$还是A的变换,但是$\tau_1\tau_2(a) = \tau_1(\tau_2(a)), a^{\tau_1\tau_2} = (a^{\tau_1})^{\tau_2}$.

例 5.1 设$A = \{1, 2\}$.

$$\tau_1 : 1 \longrightarrow 1, 2 \longrightarrow 1 \quad (i.e.\ 1^{\tau_1} = 1, 2^{\tau_1} = 1)$$

$$\tau_2 : 1 \longrightarrow 2, 2 \longrightarrow 2 \quad (i.e.\ 1^{\tau_2} = 2, 2^{\tau_2} = 2)$$

$$\tau_3 : 1 \longrightarrow 1, 2 \longrightarrow 2 \quad (i.e.\ 1^{\tau_3} = 1, 2^{\tau_3} = 2)$$

$$\tau_4 : 1 \longrightarrow 2, 2 \longrightarrow 1 \quad (i.e.\ 1^{\tau_4} = 2, 2^{\tau_4} = 1)$$

是A的所有变换.其中τ_3, τ_4是一一变换.

注 5.2 几个简单事实 在上面的例子中,容易验证:$\tau_1\tau_2 = \tau_2$; $\tau_2\tau_4 = \tau_1$; $\tau_3\tau_i = \tau_i = \tau_i\tau_3$.由$(a^\tau)^{\lambda\mu} = \{(a^\tau)^\lambda\}^\mu = (a^{\tau\lambda})^\mu$可知$\tau(\lambda\mu) = (\tau\lambda)\mu$.

性质 5.1 设$A \neq \emptyset, \varepsilon$是$A$的恒等映射,则对$A$的任一变换$\tau, \varepsilon\tau = \tau\varepsilon = \tau$.

二、变换群的概念和基本性质

设$A \neq \emptyset, S$为A的所有变换组成的集合,我们来考虑S的哪些元素能构成群的问题.对于上面的例子来说,由于$2^{\tau_i\tau_1} = 1$,所以τ_1不存在逆元素,因而S不构成群.

S的某些子集G关于上面的乘法肯定能成为群,注意到群的元素都有逆元, 容易得到G作成群的一个必要条件:

定理 5.1 假设G是集合A的若干个变换所成的集合,并且G包含恒等映射ε. 若G对于变换乘法作成一个群,则G只包含A的一一变换.

定义 5.2 集合A的若干个双射作成的群叫做A的一个变换群.

变换群的存在性如何呢?下面我们给出相对于A来说“最大”的变换群.

定理 5.2 非空集合A的所有一一变换作成一个变换群.

例 5.2 设$A=\mathbb{R}^2, G=\{\tau_\theta \mid \tau_\theta$是绕原点逆时针转$\theta$角的旋转$\}$.则$G$作成一个变换群.但$G$显然不包含$A$的全部一一变换.

注 5.3 变换群也未必是交换群,例如仍设$A=\mathbb{R}^2, G$为A的全部一一变换组成的变换群,τ_1是A的一个平移变换,使$(0,0)_1^\tau=(1,0), \tau_2$是绕原点逆时针转$\pi/2$的旋转变换,则$\tau_1,\tau_2$都是$A$的一一变换,但$(0,0)^{\tau_1\tau_2}=(0,1)\neq(1,0)=(0,0)^{\tau_2\tau_1}$,即$\tau_1\tau_2\neq\tau_2\tau_1$.

定理 5.3 (凯莱(Cayley)定理) 任何一个群都和一个变换群同构.

证 1 (证) 设$G=\{a,b,c,\ldots\}$是一个群.$\forall x\in G$,规定G的一个变换$\tau_x: G\longrightarrow G; g\longmapsto gx=g^{\tau_x}$.则$\tau_x$是$G$的一一变换.

记由G的所有元所得到的G的一一变换所构成的集合为$\bar{G}$,即$\bar{G}=\{\tau_a,\tau_b,\tau_c,\ldots\}$.则

$$\phi: G\longrightarrow \bar{G}; x\longmapsto \tau_x$$

是一一映射.且对$\forall g\in G$,

$$g^{\tau_{xy}}=g(xy)=(gx)y=(gx)^{\tau_y}=(g^{\tau_x})^{\tau_y}=g^{(\tau_x\tau_y)}$$

即$\tau_{xy}=\tau_x\tau_y$,所以是$G\overset{\phi}{\cong}\bar{G}$,而$G$是群,所以$\bar{G}$也是群.

群论基本知识小结

一、群的定义.

第一定义

第二定义

第三定义

有限群的定义

二、群的性质.

设G是一个群,则G

(1) G满足结合律;

(2) G满足消去律;

(3) G中有单位元e,且e是唯一的;

(4) $\forall a \in G, a$在G中必有逆元a^{-1},且a^{-1}是唯一的.

群G可能发生的状况:

(1) G中的元素是有限的,此时称G是有限群.

(2) G中的元素个数是无限的,此时称G是无限群.

(3) 如果$\forall a, b \in G$,都有$ab = ba$,则称G是交换群.

三、群的阶和群元素的阶,以及这二个阶的联系

(1) 群G的阶=群G中所含元素的个数.

(2) 设$a \in G$.则a的阶=使"$a^k = e$"成立的最小自然数.记为$|a|$. 如果满足"$a^k = e$"的自然数不存在,则称a的阶是无限的.

(3) $|G| < \infty \Rightarrow |a| < \infty, \forall a \in G$, 即:有限群的元素都是有限阶的.

问题:无限群的元素的阶是怎样的?

事实上,每个群都有有限阶的元素.譬如单位元.

无限群G中除e外,也许还有其他有限阶元素,如$(\mathbb{R}^*, \cdot)$除了单位元1外,-1也是有限阶元.

无限群G中除e外,其他元也可能都是无限阶的.如$(\mathbb{Z}, +)$除了单位元0外,其他元素是无限阶的.

无限群G中可能每个元素都是有限阶的,如$G = \{x | \exists n \in \mathbb{Z} \ni x^n = 1\}$关于复数乘法所构成的群.

(4) $|a| = 2 \Leftrightarrow a = a^{-1}$.

(5) 若$\forall a \in G$,都有$a^2 = e$,则G必是交换群.

四. 群元素阶的性质

(1) 设$|G| = n < \infty, A = \{a \in G \mid |a| = e\}, B = \{b \in G \mid |b| \geq 3\}$,则$|B|$是偶数,且$n$的奇偶与$|A|$的奇偶相反. ,

(2)与元素a的阶n的有关问题:

- n是自然数,且是使等式"$a^n = e$"成立的最小者.
- 如果有自然数(整数)m使$a^m = e$,则$n|m$反之也成立.
- 元素$e = a^0, a = a^1, a^2, \ldots, a^{n-1}$是$n$个两两不等的元.

- 如果$a^r = a^k$,则$n \mid r-k$.
- $a = e \Leftrightarrow n = 1$.
- $|a| = |a^{-1}|$.
- $a^{n-r} = a^{-r}$.
- $|ab| = |ba|$.
- $|abc| = |cab| = |bca|$(可推广到k个元素相乘的情形).
- $\forall m \in \mathbb{Z}, \exists r(0 \leq m \leq n) \ni a^m = a^r$.
- 如果n是奇数,则$|a^2| = n$(可推广为若$(m,n) = 1$,则$|a^m| = n$)

(3) 元素a的阶是∞的几个结论

- $\forall m(\neq 0) \in \mathbb{Z}, a^m \neq e$.
- $a^m = a^n \Rightarrow m = n$.
- $\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots$是无限个两两不同的元素.

五、几个重要的群

- 整数加群$(\mathbb{Z}, +)$.
- 数字乘群$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$等.
- 模n剩余类加群$(\mathbb{Z}_n, +)$.

练习:设G是一个幺半群(有单位元的半群),则G中所有有逆元的元作成的集合必是群.

六、群同态

问题: 若$A \sim \bar{A}$,当$\bar{A}$是群时,能保证A也是群吗?

问题: 对两个群$A, \bar{A}$,若$A \sim \bar{A}$, A中哪些性质不能“传递”给$\bar{A}$?

七、变换群.

(Cayley定理) 任何一个群都能与某个变换群同构.

作业p. 50 2,4,5

wujunanhuiwuhu@gmail.com

§6 置换群

置换群是现今所研究的一切抽象群的来源,是抽象代数创始人E.Galais(1811-1832)在证明次数大于四的一元代数方程不可能用根号求解时引进的. 置换群是一种特殊的变换群.或者说,置换群就是有限集上的变换群. 由于是定义在有限集上,故每个置换的表现形式,固有特点都是可揣测的.

由Cayley定理可以知道:如把所有置换群研究清楚了,就等于把所有有限群都研究清楚了,但实际上,研究置换群并不比研究抽象群容易.所以,一般研究抽象群用的还是直接的方法,并且也不能一下子把所有群都找出来.因为问题太复杂了,人们的方法是将群分成若干类(即附加一定条件),比如有限群、无限群;变换群、非变换群等等.对每个群类进行研究以设法回答上述三个问题.可惜,人们能弄清的群当今只有少数几类(后面的循环群就是完全解决了的一类群)大多数还在等待人们去解决.

定义 6.1 一个有限集合A到自身的一个一一变换(双射)叫做A的一个置换.

有限集合A的若干个置换作成的群叫做置换群.

含有n个元素的有限群的全体置换作成的群,叫做n次对称群.这个群通常记为S_n.

由于n个元的置换有$n!$个, 所以有

定理 6.1

$$|S_n| = n!.$$

设$A = \{a_1, a_2, a_3\}$,π是A的一个置换:$a_1^\pi = a_2, a_2^\pi = a_3, a_3^\pi = a_1$.由于我们只关心置换中元素之间的关系,而不在乎元素的具体形式. 故可视$A = \{1, 2, 3\}$,而π为:$1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$.即

$$\pi: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix} \quad \text{或} \quad \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

显然,用$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$来描述$A$的一个置换是方便的.当然,上面的置换还可以写为$\begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}, \ldots$.但习惯上都将第一行按自然序列排写, 这就可以让我们统一在一种表示置换的方法内进行工作了.

3次对称群有6个元素,$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$,分别计算$i^{\pi\tau}, i^{\tau\pi}$得到

$$\pi\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\tau\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

所以,$\pi\tau \neq \tau\pi$.因此,S_3不是交换群.以后我们将知道,这是元素个数最少的非交换群.

注 6.1 置换乘积中,是从左到右求变换值,这是与过去的习惯方法不同的.

前面已经引入了置换的记法,下面再介绍一种记法.设有8元置换$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 6 & 2 & 5 & 1 & 7 & 8 \end{pmatrix}$,$\pi$使$1 \to 4 \to 2 \to 3 \to 6 \to 1$,而其它元素保持不变.若将不发生改变的文字都删掉,那么上述置换可写成循环置换的形式:$\pi = (14236)$.一般地,

定义 6.2 S_n的一个把A中i_1变到i_2, i_2变到$i_3, , \ldots, i_k$变到i_1,而使A中其余元素不变的置换,叫做一个k-循环置换.这样的置换用符号

$$(i_1 i_2 \cdots i_k), (i_2 i_3 \cdots i_k i_1), \cdots, (i_k i_1 \cdots i_{k-1})$$

来表示.

如果S_n的两个循环置换π, τ没有共同的文字,则称这两个循环置换是不相连的

注 6.2 *(1)* 循环置换是置换的另一种表达形式,它以发生变化的文字的变化次序为序, 表达成轮换的形式.虽然表达形式简捷,但所含置换的原有文字的数目可能反映不出来. 这要求事先予以说明.例如.*"8*元置换$\pi = (14236)$.*"*

(2) 每个循环的表达方法一般不唯一,如$(i_1 i_2 \cdots i_k) = (i_2 i_3 \cdots i_k i_1) = \cdots = (i_k i_1 \cdots i_{k-1})$.

(3) S_8的单位*(*恒等置换*)*$\pi_0 = (1) = (2) = \cdots = (8)$,习惯写成$\pi_0 = (1)$.

定理 6.2 (循环置换分解定理) 每一个n元置换π都可以写成若干个不相连的循环置换的乘积.

证 对π变动的元素个数进行归纳.如果π使任何元素都不变动,则$\pi = (1)$,结论成立.

假设对于最多变动$r-1 (r \leq n)$个元的π定理是对的,则对变动r 个元的π,任取一个被π变动的元i_1,从i_1出发找i_1的象i_2, i_2 的象$i_3, \cdots$,直到找到一个i_k为止,i_k的象不再是一个新的元,而是我们已经得到的一个元:$i_k^\pi = i_j, j \leq k$.因为$i_j (2 \leq j \leq k)$是i_{j-1}的象, 所以$i_k^\pi = i_1$,即

$$i_1 \to i_2 \to \cdots \to i_k \to i_1.$$

因为π只使r个元变动,$k \leq r$.如果$k = r$,则π本身就是一个k-循环置换,结论成立.假设$k < r$,则

$$\begin{aligned} \pi &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n \end{pmatrix} \\ &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \end{pmatrix} \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n \\ i_1 & i_2 & \cdots & i_k & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n \end{pmatrix} \\ &= (i_1 i_2 \cdots i_k)\pi_1 \end{aligned}$$

但π_1只使$r-k<r$个元变动,由归纳假设,可以写成不相连的循环置换的乘积: $\pi_1=\eta_1\eta_2\cdots\eta_m$.

还需要说明:π_1中的所有循环置换$\eta_1,\ldots,\eta_m$中不可能再出现$i_1,\ldots,i_k$.否则,若$\eta_t=(\cdots i_p i_q\cdots), p\le k$,由于$\eta_1,\ldots,\eta_m$不相连,所以$i_p$只在$\eta_t$中出现,于是$i_p^{\pi_1}=i_q$,这与$\pi_1$使$i_p$不动相矛盾.所以

$$\pi=(i_1i_2\cdots i_k)\eta_1\cdots\eta_m$$

是不相连的循环置换的乘积. □

把置换写成不相连的循环置换的乘积是表示置换的又一方法.

由Caylay定理立得

定理 6.3 每一个有限群都与一个置换群同构.

定义 6.3 每个2-循环置换叫做一个对换.

性质 6.1 k-循环置换$(i_1i_2\cdots i_k)$的阶是k.

性质 6.2 循环置换$\pi=(i_1i_2\cdots i_k)$的逆置换是$\pi^{-1}=(i_ki_{k-1}\cdots i_1)$.

性质 6.3 两个不相连的循环置换可以交换.

性质 6.4

$$\begin{aligned}(i_1i_2\cdots i_k) &= (i_1i_2)(i_1i_3)\cdots(i_1i_k)\\ &= (i_1i_k)(i_2i_k)\cdots(i_{k-1}i_k).\end{aligned}$$

于是有

性质 6.5 每个n元置换都能表示成若干个对换的乘积.

性质 6.6 设$j\notin\{i_1,i_2,\ldots,i_k\}$,则$(i_1i_2\cdots i_k)=(ji_1i_2\cdots i_k)(ji_1)$.

性质 6.7 任意一个置换表成对换之积时,表示式中对换个数的奇偶性不变.

定义 6.4 一个置换π叫做偶(奇)置换 $\Leftrightarrow$ π可以表成偶(奇)数个对换之积.

性质 6.8 一个k-循环置换π是偶(奇)置换$\Leftrightarrow$ k为奇(偶)数.

定义 6.5 n次对称群S_n中全部偶置换组成的集合A_n构成一个群,叫做n次交错群. 并且有$|A_n|=\frac{1}{2}|S_n|=\frac{n!}{2}$.

作业P. 55 1,3,4

§7 循环群

例 7.1 整数加群$(\mathbb{Z},+)$中每个元素都是1的倍数.

例 7.2 模n的剩余类加群$(\mathbb{Z}_n,+)$中每个元素都是$1([1])$的倍数.

注 7.1 以上两个例子都说明群中有一个特殊的元素,使得其余元素都是这个元素的倍数(因为是加群,所以用倍数,如果是乘法群,则是方幂.以下用乘法群为例).一般地,

定义 7.1 设G是一个(乘法)群,如果G中有一个元素a,使G中每个元素都是a的乘方, 即$G=\{a^m|m\in Z\}$,则称G为循环群; 也称G是由a所生成的,记为$G=(a)$.a叫做G的一个生成元.

设G是一个群,a是G的生成元.则有

引理 7.1

$$|G|=|a|.$$

事实上,

(1) 若$|a|=\infty$,则$G=(\cdots,a^{-2},a^{-1},e,a,a^2,\cdots)$.

(2) 若$|a|=n<\infty$,则$G=(e,a,a^2,\cdots,a^{n-1})$.

所以有

引理 7.2 设$G=(a)$,则:(1) G是无限循环群$\Leftrightarrow|a|=\infty$; (2) G是n阶循环群$\Leftrightarrow|a|=n$.

考察

$$\begin{array}{rcccccccc} G & = & (\cdots, & a^{-2}, & a^{-1}, & e, & a^1, & a^2, & \cdots) \\ & & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{Z} & = & (\cdots, & -2, & -1, & 0, & 1, & 2, & \cdots) \end{array}$$

与

$$\begin{array}{rcccccc} G & = & (e, & a, & a^2, & \cdots, & a^{n-1}) \\ & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ \mathbb{Z}_n & = & (0, & 1, & 2, & \cdots, & n-1) \end{array}$$

我们有

定理 7.1 (循环群的结构定理) 设G是由a生成的循环群,

(1) 如果$|a|=\infty$,则$G\cong\mathbb{Z}$.

(2) 如果$|a|=n<\infty$,则$G\cong\mathbb{Z}_n$.

上面的定理说明,在同构的意义下,循环群只有两个:$\mathbb{Z}, \mathbb{Z}_n$.我们可以把循环群研究得更透彻一些.

很显然,$\mathbb{Z}$有且仅有两个生成元,而$\mathbb{Z}_n$的生成元就要复杂一些.我们再回到$G = (a), |G| = |a| = n$上来,若$b \in G \ni G = (b)$,则只需$|b| = n$ 就可以了,所以

$$b = a^k \text{是} G \text{的生成元} \Leftrightarrow (k, n) = 1.$$

例如,$n = 6$时,$G = (e, a, a^1, a^2, a^3, a^4, a^5), a, a^5$都是$G$的生成元, 而$e, a^2, a^3, a^4$不是$G$的生成元.

定义 7.2 设n为正整数,称$\varphi(n)$(=不超过n且与n互素的正整数的个数)为欧拉函数.

推论 7.1 $\mathbb{Z}_n$有$\varphi(n)$个生成元.

§8 子群

定义 8.1 设G是一个群,$H(\neq \emptyset) \subseteq G$,如果$H$对于$G$的运算来说也作成群,则称$H$是$G$的一个子群.记为$H \leq G$.

例 8.1 设G为群,则$G \leq G, (e) \leq G$.这两个群称为G的平凡子群.

例 8.2 设$G = S_3$,则$H = ((1), (12))$是G的一个非平凡子群.

例 8.3 $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

定理 8.1 (子群的判定定理1) 设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \begin{cases} (1)\ a, b \in H \Rightarrow ab \in H; \\ (2)\ a \in H \Rightarrow a^{-1} \in H. \end{cases}$$

推论 8.1 设$H \leq G$,则H的单位元就是G的单位元,H中元a在H中的逆元就是a在G中的逆元.

判定定理1中的两个条件可以简化为一个条件:

定理 8.2 (子群的判定定理2) 设G为群,$H(\neq \emptyset) \subseteq G$.则

$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab^{-1} \in H\text{”}.$$

定理 8.3 (有限子群的判定定理) 设G为群,$H(\neq \emptyset) \subseteq G$,且$H$是有限集.则

$$H \leq G \Leftrightarrow \text{“}a, b \in H \Rightarrow ab \in H.$$

例 8.4 任一群不可能是两个真子群的并.

例 8.5 设$K_4 = ((1),(12)(34),(13)(24),(14)(23))$,则$K_4 \leq S_4$.且$H_1 = ((1),(12)(34)), H_2 = ((1),(13)(24)), H_3 = ((1),(14)(23))$都是$K_4$的真子群, 直接验证知$K_4 = H_1 \cup H_2 \cup H_3$.

例 8.6 设$G = S_3, H_1 = ((1),(12)), H_2 = ((1),(13)), H_3 = ((1),(23)), H_4 = ((1),(123),(132))$, 则$H_i$都是$G$的真子群,且$S_3 = H_1 \cup H_2 \cup H_3 \cup H_4$.

对于群G的非空子集S,未必有$S \leq G$.但

$$K = \{a_1^{r_1}a_2^{r_2}\cdots a_m^{r_m} \mid a_i \in S, r_i = \pm 1, m \in \mathbb{N}, 1 \leq i \leq m\} \leq G.$$

并且K是G的含S的最小的子群,称K为由S生成的子群,记为$K = (S)$,称S为K的生成集.当$S = \{a_1,\ldots,a_n\}$为有限集合时,称$K = (a_1,\ldots,a_n)$为有限生成的, 当$S = \{a\}$只有一个元素时,称$K = (a)$为循环群(这正是我们前面所讨论的). 如果$S \leq G$,则$S = (S)$.

设$H \leq G, K \leq G$,记$HK = \{hk|h \in H, k \in K\}$, HK未必为G的子群.例如$H = ((1),(12)) \leq S_3, K = ((1),(13)) \leq S_3$,则$HK = \{(1),(12),(13),(123)\}$, 但$(13)(12) \notin HK$,即$HK \not\leq G$.何时有$HK \leq G$呢?

定理 8.4 设$H \leq G, K \leq G$,则$HK \leq G \Leftrightarrow HK = KH$.

§9 子群的陪集

例 9.1 $(\mathbb{Z}_4,+)$实际上给出了$\mathbb{Z}$的一个分类:*[0],[1],[2],[3]*. 在这个分类中, 只有*[0]*构成$(\mathbb{Z},+)$的一个子群,而其余分类均不构成$(\mathbb{Z},+)$的子群.并且$\mathbb{Z}_4$中的每个类$[i]$都是类*[0]*中的每个元素普遍加上i 得到的,或者说,类$[i]$中任意两个元素的差是*[0]*中的元素.

例 9.2 给定S_3的一个分类$\Omega = \{H,K,M\}$,其中$H = \{(1),(12)\}, K = \{(13),(123)\}, M = \{(23),(132)\}$.只有$H \leq G$,而$K, M$均不构成$G$的子群,但$K$中的元素恰是由$H$中的元素右乘$(13)$所得到的类,$MK$中的元素恰是由$H$中的元素右乘$(23)$所得到的类,或者说,$\forall a,b \in K(M) \Rightarrow ab^{-1} \in H$.

一般地,设$H \leq G$,规定G中的一个关系$\sim$如下:$a,b \in G, a \sim b \Leftrightarrow ab^{-1} \in H$.则$\sim$是$G$的一个等价关系.

定义 9.1 由上面的等价关系确定的类叫做H的右陪集,包含元素a的右陪集记为Ha.

类似地,设$H \leq G, a,b \in G$.由等价关系$a \sim b \Leftrightarrow a^{-1}b \in G$确定的类叫做左陪集,包含元素$a$的左陪集记为$aH$.

注 9.1 设H,K为两个集合,通常记$HK = \{ab|a \in K, b \in K\}$.特别地, $H\{b\}(\{a\}K)$记为$Hb(aK)$.

若群G的两个非空子集$H = K$,则$\forall a \in G, Ha = Ka$.

$Ha = Hb$是集合相等,未必有$ha = hb, h \in H$.

定理 9.1 设$H \leq K, a, b \in G$.则下列叙述等价:

(1) $a \in Hb$;

(2) $Ha = Hb$;

(3) $ab^{-1} \in H$;

(4) $b \in Ha$;

(5) $ba^{-1} \in H$.

定理 9.2 一个群H的右陪集的个数和左陪集的个数相等.

定义 9.2 一个群G的一个子群H的右(左)陪集的个数叫做H在G里的指数,记为$[G : H]$.

引理 9.1 一个子群H与H的每一个右陪集Ha之间都存在一一映射.

定理 9.3 (Lagrange定理) 设$H \leq G$,则$|G| = [G : H]|H|$.

推论 9.1 设G为有限群,$a \in G$.则$|a| \mid |G|$.

作业p. 61 2,3,5 p. 64 1,2,4,5 p. 70 1,2,5

§10 不变子群、商群

设$H \leq G$,由H决定的所有的右陪集构成的集合$S_l = \{aH | a \in G\}$. 我们来看S_l构成群的条件.

S_l中的运算应该与G中的运算有某种联系并且S_l中的运算应该封闭, 即对$\forall a, b \in G, \exists c \in G \ni (aH)(bH) = cH \in S_l$,于是$ab = (ae)(be) \in cH$,从而$aHbH = abH$. 特别地(取$a = e$), $HbH = bH$.于是有$b = h_1 b h_2$,故$Hb \subseteq HbH = bH$;再由b 的任意性,有$Hb^{-1} \subseteq b^{-1}H$,所以,$bH \subseteq Hb$.

事实上,我们证明了

性质 10.1 设$H \leq G$,则对$\forall aH, bH \in S_l = \{aH | a \in G\}, aHbH \in S_l \Leftrightarrow \forall a \in G, aH = Ha$.

在证明S_l关于如上定义的运算作成一个群之前,我们先来看"$aH = Ha$"的几个性质.

满足条件"$aH = Ha, \forall a \in G$"的子群H具有极其重要的意义.

定义 10.1 设$H \leq G$,如果对$\forall a \in G$都有$aH = Ha$,则称H为G的不变子群(或正规子群), 记为$H \lhd G$.如果$H \lhd G$,则G的左(右)陪集统一称为G的陪集.

例 10.1 $G \lhd G, \quad \{e\} \lhd G.$

例 10.2 如果G为交换群,则G的每一个子群都是G的不变子群.

例 10.3 设G为群,称$C(G) = \{a \in G | \forall x \in G, ax = xa\}$为$G$的中心,我们有$C(G) \leq G$且$C(G) \lhd G$.

例 10.4 设$H = \{(1), (123), (132)\} \leq S_3$,则$H \lhd S_3$.

本题可以直接验证,也可以利用Lagrange定理来证明.

证 由于$|S_3| = 6, |H| = 3$,所以H只有两个左(右陪集),并且其中有一个为H. 故有$(12)H = (13)H = (23)H = H(12) = H(13) = h(23), (123)H = (132)H = (1)H = H(1) = H(123) = H(132)$. □

一般地,我们有

例 10.5 如果$H \leq G$且$[G : H] = 2$,则$H \lhd G$.

证 $\forall x \in G$,若$x \in H$,则$Hx = H = xH$;若$x \notin H$,则$Hx \cap H = \emptyset, xH \cap H = \emptyset$,且此时有$G = H \cup Hx = H \cup xH$, 于是$Hx = xH$.总之有$Hx = xH$,即$H \lhd G$. □

注 10.1 $aH = Ha$只是集合相等,绝不意味着元素乘积可以交换.

定理 10.1 设$H \leq G$.下列叙述等价:

(1) $aH = Ha, \forall a \in G$;

(2) $aHa^{-1} = H, \forall a \in G$;

(3) $aHa^{-1} \subseteq H, \forall a \in G$;

(4) $aha^{-1} \in H, \forall a \in G, \forall h \in H$.

例 10.6 设$H \leq G$,称$N(H) = \{x \in G | xH = Hx\}$为$H$在$G$中的正规化子.则$H \lhd N(H) \leq G$.

由此可以看出,$N(H)$是将H作为不变子群的G的最大的子群.特别地, 若$H \lhd G$,则$N(H) = G$.

例 10.7 设$H \leq G, N \leq G$.则

(1) $H \lhd G \Rightarrow H \cap N \lhd N$;

(2) $H \lhd G$ *and* $N \lhd G \Rightarrow H \cap N \lhd G$;

(3) $H \lhd G \Rightarrow HN \leq G$ *and* $H \lhd HN$;

(4) $H \lhd G$ *and* $N \lhd G \Rightarrow HN \lhd G$;

(5) $H \lhd G$ *and* $N \lhd G$ *and* $H \cap N = \{e\} \Rightarrow \forall h \in H, n \in N, hn = nh$.

例 10.8 设$G = S_4, H = \{(1), (12)(34), (13)(24), (14)(23)\}, N = \{(1), (1234)\}$,则$H \lhd G, N \lhd H$,但$N \not\lhd G$.这说明正规子群没有传递性.

引理 10.1 设$H \lhd G$,则S_l中的运算$(aH)(bH) = (ab)H$是一个代数运算,即若$aH = a'H, bH = b'H$,则$(ab)H = (a'b')H$.

定理 10.2 设$H \lhd G$,则S_l关于运算$(aH)(bH) = (ab)H$作成一个群.

定义 10.2 一个群G的一个不变子群H的陪集所作成的群叫做G关于H的商群,记为G/H.

由于$|\ G/H\ |$等于H在G中的指数,根据Lagrange定理可得

推论 10.1 设$H \lhd G$,则$\dfrac{|G|}{|H|} = |\ G/H\ |$.

§11 同态与不变子群

定义 11.1 设$\varphi : G \longrightarrow \bar{G}$是群同态映射,称$ker\varphi = \{x \in G \mid \varphi(x) = \bar{e}\}$为$\varphi$的核.

性质 11.1 设$\varphi : G \longrightarrow \bar{G}$是群同态,则$ker\varphi \lhd G$.

性质 11.2 设$\varphi : G \longrightarrow \bar{G}$是群同态,则$\varphi$为单同态$\Leftrightarrow ker\varphi = \{e\}$.

定理 11.1 设$N \lhd G$,则有群满同态$\varphi : G \longrightarrow G/N; x \longmapsto xN$.

注 11.1 *1.* 定理中的同态通常称为自然同态;

2. 自然同态的同态核为N;

3. 群G的每个商群都是G的同态象,进而可由商群的性质得到G的一些性质;

4. 由下面的定理还可以看出,G的每个同态象也只能是G的商群*(*在同构的意义下*)*,这两个定理合称为第一同态定理.

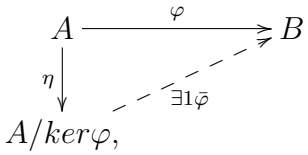
定理 11.2 设G与$\bar{G}$是同态的群:$G \overset{\varphi}{\sim} \bar{G}$且$ker\varphi = N$,则$G/N \cong \bar{G}$.

证 由$N \lhd G$得商群G/N.定义$\phi : G/N \longrightarrow \bar{G}; gN \longmapsto \varphi(g)$,则由定义即得$G/N \cong \bar{G}$. □

例 11.1

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong R^*.$$

性质 11.3 设$\varphi : A \longrightarrow B$是群同态映射,则存在唯一的群单同态$\bar{\varphi} : A/ker\varphi \longrightarrow B$使下图可换:



且$\bar{\varphi}$满$\Leftrightarrow$ φ满.

证 注意到φ是群同态,$N = \ker\varphi \lhd A$,有自然同态$\eta : A \longrightarrow A/N$,且$\bar{\varphi} : A/N \longrightarrow B$; $gN \longmapsto \varphi(g)$满足条件. □

通常称$\bar{\varphi}$为φ的导出同态.

定义 11.2 设$\phi : A \longrightarrow B$.称$\phi(S) = \{y \in B \mid \exists x \in S \ni \phi(x) = y\}$为$A$的子集$S$在$\phi$下的象; 称$\phi^{-1}(T) = \{x \in A \mid \exists y \in T \ni \phi(x) = y\}$为$B$的子集$T$ 在ϕ下的原象.

定理 11.3 设$\phi : A \longrightarrow B$.是群同态满射,则

(1) $H \leq A \Rightarrow \phi(H) \leq B$;

(2) $H \lhd A \Rightarrow \phi(H) \lhd B$;

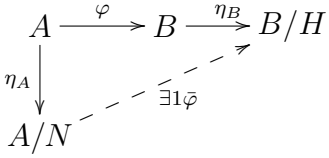
(3) $H \leq B \Rightarrow \phi^{-1}(H) \leq A$且$ker\phi \leq \phi^{-1}(H)$;

(4) $H \lhd B \Rightarrow \phi^{-1}(H) \lhd A$且$ker\phi \leq \phi^{-1}(H)$.

第一同态定理是说,若$A \overset{\varphi}{\twoheadrightarrow} B$,则$A/\ker\varphi \cong B$,其中$\ker\varphi = \varphi^{-1}(e_B)(= \varphi^{-1}(\{e_B\}))$.我们现在来推广这一定理,将$\{e_B\}$换成$B$的不变子群.

定理 11.4 (群的第二同态定理) 设$A \overset{\varphi}{\twoheadrightarrow} B, H \lhd B$,则$A/N \cong B/H$,其中$N = \varphi^{-1}(H)$.

证 由$H \lhd B$知$N \lhd A$,于是$A/N, B/H$都有意义.于是有交换图



注意到$N = \ker(\eta_B\varphi)$,由同态基本定理即得结论. □

作业p.74 1,2,4 p.79 2,3

练习与思考题

1. 设G是一个有限群,A和B是G的两个非空子集.证明:如果$|A|+|B|>G$, 则$G=AB$.特别地,若$|A|>|G|/2$,则$G=A^2$.

2. 证明:若群G中有惟一的2阶元素,则这个2阶元素必是G的一个中心元.

3. 设G是一个群,且$|G|>1$.

   (1) 证明:若G中除单位元外其余元素的阶都相同,则这个相同的阶不是无限就是素数.

   (2) 说明这样的两种群是存在的.

4. 设a,b是群G中的元素,且$|a|=s,|b|=t,ab=ba$.证明:

   (1) $|ab||[s,t]$;

   (2) 对$[s,t]$的任一正因数h,G中有阶是h的元素.

5. 设a是群G中的一个元素,且$|a|=mn,(m,n)=1$.证明:$\exists 1 b,c\in G\ni a=bc,bc=cb,|b|=m,|c|=n$.

6. 证明:交换群中所有有限阶元素作成一个群.

7. 求S_3的所有子群.

8. 设H是群G的一个非空子集,且$H^2=H$.

   (1) H是否为G的一个子群?

   (2) 当H有限时,$H\leq G$.

9. 设$H\leq G,a\in G$.证明:$aHa^{-1}\leq G$, 且$H\cong aHa^{-1}$.

10. 设$H,K\leq G$.证明:

    (1) $H\cap K\leq G$;

    (2) $H\cup K\leq G\Rightarrow H\cup K=HK$;

    (3) $H\cup K\leq G\Leftrightarrow H\subseteq K$ or $K\subseteq H$.

11. 设G是一个$2n$阶交换群.证明:如果n是一个奇数,则G有且仅有一个2阶子群.

12. 设$H,K\leq G$,且$|H|=m,|K|=n$.证明:若$(m,n)=1$,则$H\cap K=\{e\}$. 反之,若$H\cap K=\{e\}$,是否一定有$(m,n)=1$?

13. 设G是一个$2p$(p为素数)阶有限非交换群.证明:

    (1) G一定有一个p阶子群;

    (2) G的元素可写成$e, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b$的形式.

14. 设G为群,$H \leq K \leq G$.证明;$(G : H) = (G : K)(K : H)$.

15. 设$N \lhd G$,且$(G : N) = m$,则$\forall a \in G, a^m \in N$.

16. 证明:四元数群$G = \{\pm 1, \pm i, \pm j, \pm k\}$ (其中$i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik$) 是非交换群且每个子群都是正规子群.该群被称为Hamilton 群.

17. 证明:

    (1) 无限循环群的自同构只有两个;

    (2) n阶循环群的自同构有$\varphi(n)$个,即小于n且与n互素的正整数个数.

18. 证明:在同构的意义下,4阶群只有两个,一个是循环群,另一个是Klain四元群$K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$.

19. 求S_5中阶为2的元素.

执一而万物治

—庄子

第三章 环与域

§1 加群、环的定义

本节主要包括以下内容:

1 环的概念;

2 两个重要的环;

3 环的简单性质.

一、环的定义与例子

定义 1.1 设$(R,+,\cdot)$是具有两个代数运算的代数体系,如果这个代数体系满足:

(1) $(R,+)$是一个加法交换群;

(2) $(R,\cdot)$是一个半群;

(3) R的乘法"$\cdot$"对加法"$+$"满足左右分配律,即对$\forall a,b,c\in R$有

$$a(b+c)=ab+ac \quad 且 \quad (b+c)a=ba+ca$$

则称$(R,+,\cdot)$是一个环,简记为R.

例 1.1 $(\mathbb{Z},+,\cdot)$是一个环,习惯上称之为整数环,记为$\mathbb{Z}$.

同样有有理数环$\mathbb{Q}$,实数环$\mathbb{R}$,复数环$\mathbb{C}$.这几个环都由数组成,称为数环.

例 1.2 偶数集$2\mathbb{Z}=\{\cdots,-4,-2,0,2,4,\cdots\}$对于通常的加法和乘法是一个环.

例 1.3 设$\mathbb{Z}[i]=\{a+bi\mid \forall a,b\in\mathbb{Z}\}$,则$\mathbb{Z}[i]$按复数的通常的加法和乘法构成一个环,这个环叫做高斯整数环.

例 1.4 设F是一个数域,由F上一切多项式组成的集合$F[x]=\{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \mid a_i\in F, n\in\mathbb{N}\}$关于多项式通常的加法与乘法构成一个环,这个环$(F[x],+.\cdot)$称为关于$x$的一元多项式环,或一元多项式环.

[注] 将本例中的数域F换成任一个数环,也能构成多项式环,如$\mathbb{Z}[x]$ 叫做整系数多项式环.

例 1.5 数域F上的全部n阶方阵组成的集合$M_n(F)=\{A=(a_{ij}) \mid a_{ij}\in F, 1\le i,j\le n\}$关于矩阵的加法和乘法构成一个环,这个环$(M_n(F),+,\cdot)$叫做$n$阶矩阵环.

[注] 将本例中的数域F换成任一个数环,也能构成多项式环,如用偶数环$2\mathbb{Z}[x]$替换F得环

$$M_n(2\mathbb{Z})=\{A=(a_{ij}|a_{ij}\in 2\mathbb{Z}, 1\le i,j\le n\}.$$

二、两个重要的环

例 1.6 模n的剩余类环$(\mathbb{Z}_n,+,\cdot)$.

例 1.7 加群G的自同态环$(End(G),+,\cdot)$.

三、环的简单性质

设R是一个环,则对$\forall a,b,c\in R, n,m\in\mathbb{N}^*$, 有如下性质:

1 $c(a-b)=ca-cb \quad \& \quad (a-b)c=ac-ab$;

2 $0a=a0=0$;

3 $(-a)b=a(-b)=-ab$;

4 $(-a)(-b)=ab$;

5 若$a_1,a_2,\cdots,a_m\in R$,则$\sum\limits_{i=1}^{m}=a_1+a_2+\cdots+a_m$;

6 $(\sum\limits_{i=1}^{m}a_i)(\sum\limits_{j=1}^{n}b_j)=\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n}a_ib_j$;

7 $(na)b=a(nb)=n(ab)\overset{def}{=}nab$;

8 $a^m=\underbrace{aa\cdots a}_{m}, a^ma^n=a^{m+n}, (a^m)^n=a^{mn}$;

9 $(-n)a=\underbrace{(-a)+(-a)+\cdots+(-a)}_{n}, n(a+b)=na+nb, (n+m)a=na+ma, (nm)a=n(ma)$.

§2 交换律、单位元、零因子、整环

本节主要包括以下内容:

1 交换环的概念与简单性质;

2 无零因子环;

3 有单位元的环,整环.

一、交换环

定义 2.1 如果环$(R,+,\cdot)$关于乘法满足交换律,即$\forall a,b\in R, ab=ba$, 则称R为交换环.

例 2.1 数环、偶数环、高斯整数环、一元多项式环都是交换环.

当$n>1$时,$M_n(F)$不是交换环.

例 2.2 如果环$(R,+,\cdot)$的加法群是循环群,则R是交换环.

设R是交换环,$\forall a,b\in R$,有

1 $\forall n\in\mathbb{N},(ab)^n=a^nb^n$;

2 $(a\pm b)^2=a^2\pm 2ab+b^2,\ a^2-b^2=(a+b)(a-b), a^3\pm b^3=(a\pm b)(a^2\mp ab+b^2)$;

3 $(a+b)^n=a^n+C_n^1a^{n-1}b+C_n^2a^{n-2}b^2+\cdots+C_n^{n-1}ab^{n-1}+b^n$.

二、无零因子环

定义 2.2 设R是环,如果R中元$a\neq 0, b\neq 0$,但$ab=0$,则称a是R的一个左零因子, b是R的一个右零因子.

注 2.1 *1* R有左零因子$\Leftrightarrow$ R有右零因子;

2 R的左零因子未必是右零因子,例如,取$R=\left\{\begin{pmatrix} a & b\\ 0 & 0\end{pmatrix}\mid a,b\in\mathbb{R}\right\}$, 则$\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}$是$R$的右零因子, 但不是左零因子;

3 若R为交换环,则R的每个左(右)零因子都是右(左)零因子;

4 若环R中的元素a既是左零因子又是右零因子,则称a为R的零因子.

定义 2.3 若环R中没有左零因子,则称R为无零因子环.

定理 2.1 设R是一个环,则

(1) R中没有左零因子$\Leftrightarrow$ R中有左消去律;

(2) R中没有右零因子$\Leftrightarrow$ R中有右消去律.

推论 2.1 设R是一个环,则下列叙述等价:

(1) R中无左零因子;

(2) R中无右零因子;

(3) R中满足左消去律;

(4) R中满足右消去律.

由于R是无零因子环$\Leftrightarrow \forall a(\neq 0), b(\neq 0) \in R^*, ab \neq 0$(即$R^*$是封闭的) $\Leftrightarrow$ R^* 是封闭的$\Leftrightarrow$ R^*是乘法半群.故有

推论 2.2 R是无零因子环$\Leftrightarrow$ $(R^*, \cdot)$是半群.

例 2.3 设$A \in M_n(F)(n \geq 2)$,则A是左(右)零因子$\Leftrightarrow$ $|A| = 0$.

例 2.4 $\mathbb{Z}_n$是无零因子环$\Leftrightarrow$ n为素数.

定理 2.2 设$(R, +, \cdot)$是一个无零因子环,则加群$(R, +)$中每个非零元素的阶彼此相同.并且,当这个阶有限时必为素数.

证 (1) 若R中每个元素的阶都是无限时,R中元素的阶都相同;

(2) 若有$a \in R, |a| = n \in \mathbb{N}$,则$\forall b(\neq 0) \in R, 0 = (na)b = a(nb)$,所以$|b| = m|n$;同样可得$n|m$,故$m = n$.由$b$的任意性即知$R$中每个非零元素的阶都相同;

(3) 若R中非零元素的阶n是合数,则有$1 < n_1, n_2 < n$,使$n = n_1 n_2$,于是对$a(\neq 0), b(\neq 0) \in R$有$0 = n(ab) = (n_1 a)(n_2 b)$,但$1 < n_1, n_2 < n \Rightarrow n_1 a \neq 0, n_2 b \neq 0$,所以$n_1 a$是左零因子,$n_2 b$是右零因子,这与$R$是无零因子环相矛盾. □

三、有单位元的环

定义 2.4 若环$(R, +, \cdot)$中有元素e,使$\forall a \in R$都有$ea = ae = a$,则称这个元素为R的单位元.记为1_R.

注 2.2 *(1)* 环中的单位元未必是整数*1*;

(2) 并不是每个环都有单位元;

(3) 若环中有单位元,则这个单位元是惟一的.

定义 2.5 设R是有单位元1_R的环,$a \in R$.若有$b \in R$使$ab = ba = 1_R$,则称a是R中的可逆元, 并称b为a的逆元.

注 2.3 *(1)* 只有在有单位元的环中才能谈论逆元的问题;

(2) 即使在有单位元的环中,也不保证每个元素都有逆元;

(3) 若元a可逆,则a的逆元素是惟一的,记为a^{-1}.

性质 2.1 设R是有单位元的环,R中所有可逆元构成的集合为$R^\bullet = \{a \in R | a可逆\}$,则$R^\bullet$是一个乘法群.

定义 2.6 设R是环,若满足

(1) R是交换环;

(2) R有单位元;

(3) R是无零因子环,

则称R为整环.

例 2.5 整数环、多项式环、模p(p为素数)的剩余类环都是整环.
偶数环、矩阵环、模n(n为合数)的剩余类环都不是整环.

§3 除环、域

本节主要介绍除环与域的概念

一、除环

定义 3.1 设R是环,若满足

(1) R中有非零元;

(2) R有单位元;

(3) R^*中每个元素都可逆(于是$R^* = R^\cdot$),

则称R为除环.

性质 3.1 *(1)* 除环是无零因子环,反之不然;

(2) 若R是除环,则R^*是一个乘法群;

(3) 非零环R是除环$\Leftrightarrow$ R^*是乘法群;

(4) 有限的非零环R是除环$\Leftrightarrow$ R是无零因子环.

二、域

定义 3.2 若环R是交换除环,则称R为域,记为F.

由于域F为除环,所以$(F^*,+,\cdot)$是乘法群,因而对$\forall a,b\in F^*$方程:

$$ax=b \text{ 与 } \qquad ya=b$$

在F^*中有惟一解$x=a^{-1}b, y=ba^{-1}$.但F为域,所以$a^{-1}b=ba^{-1}\overset{def}{=}\frac{b}{a}$,并称$\frac{b}{a}$为"$b$除以$a$所得的商" (或"$a$除$b$的商").

在域F中,$\frac{b}{a}(a(\neq 0),b\in F)$有下列性质

(1) 若$a\neq 0, c\neq 0$,则$\frac{b}{a}=\frac{d}{c}\Leftrightarrow ad=bc$;

(2) $\frac{b}{a}\pm\frac{d}{c}=\frac{bc\pm ad}{ac}$;

(3) $\frac{b}{a}\cdot\frac{d}{c}=\frac{bd}{ac}$;

(4) $\frac{b}{a}/\frac{d}{c}=\frac{bc}{ad}$.

定理 3.1 设R是一个有限的非零环,则R是域$\Leftrightarrow$ R是整环.

p. 89 1,2,5 p. 93 1,2,5

§4 无零因子环的特征

本节主要介绍环的特征的概念

定义 4.1 设R为任意环,如果存在正整数n,使对$\forall a\in R$,都有$na=0$,则称这样的最小正整数n为环R的特征,记为$char(R)$.如果不存在这样的正整数,则称R的特征为无穷大,记为$char(R)=\infty$.

例 4.1 $char(\mathbb{Z}) = \infty, char(F(x)) = \infty,$
$char(M_n(F)) = \infty.$
$char(\mathbb{Z}_n) = n.$

注 4.1 *(1)* 若环R的加群中有一个元素的阶为∞,则$char(R)=\infty$;

(2) 若环R的加群中每个元素都是有限阶的且最大的阶为n,则$char(R) = n$;

(3) 存在环R,使得加群$(R,+)$中既有无穷阶的元素又有有限阶的元素*(*如$R = \mathbb{Z}_n \times \mathbb{Z}, (a,b) + (c,d) = (a+c, b+d), (a,b)(c,d) = (0,0)$*)*;

(4) 存在环R,使得加群$(R,+)$中每个元素都是有限阶的,但不存在最大的阶*(*如$R = \{x \in \mathbb{C} | \exists n \in \mathbb{N} \ni x^n = 1)\}, x \oplus y = xy, x \otimes y = 1$*)*.

例 4.2 若R中每个元素都是幂等元*(*即$\forall a \in R, a^2 = a$*)*且$R \neq \{0\}$, 则R是特征为*2*的交换环.

注 4.2 $\forall a \in R$,由$2a = (2a)^2 = 4a^2 = 4a = 2a + 2a$得$2a = 0$, 再由$R \neq \{0\}$得$charR=2$,于是对$\forall a, b \in R, a + b = (a + b)^2 = a^2 + b^2 + ab + ba$,即$ab = -ba$,但$a = -a$,所以$ab = ba$.

在第二节,我们已经证明了

定理 4.1 设$(R,+,\cdot)$是一个无零因子环,则加群$(R,+)$中每个非零元素的阶彼此相同.并且,当这个阶有限时必为素数.

所以有

推论 4.1 整环,除环和域的特征或是无限大,或是一个素数.

练习 1 *1* 设$a(\neq 0) \in R$,若a不是零因子, 则$char(R)=|a|$;

2 若域F的阶为偶数,则$char(F)=2$.

§5 子环、环的同态

本节主要包含以下内容:

1 子环的定义,尤其是子整环,子除环和子域的定义.

2 环同态映射的定义与基本性质.

3 环同构的应用–挖补定理.

定义 5.1 设S是环R的非空子集,如果S关于R中的加法和乘法作成一个环,则称S为R的一个子环, 同时称R为S的扩环.

等价地,有

定义 5.2 设$S(\neq \emptyset) \subseteq (R,+,\cdot)$.若$S$满足

(1) $(S,+)$是$(R,+)$的子群*(*即$\forall a,b \in S, a-b \in S$*)*;

(2) $(S,\cdot)$对乘法封闭*(*即$\forall a,b \in S, ab \in S$*)*

则称S是R的子环.

类似地,可以定义子整环,子除环和子域:

定义 5.3 设R是整环,$S(\neq \emptyset) \subseteq R$,若$\forall a,b \in S, a-b \in S, ab \in S$, 且$S$中有单位元, 则称$S$是$R$的子整环.

定义 5.4 设R是除环,$S(\neq \emptyset) \subseteq R$,若

(1) $\forall a,b \in S, a-b \in S, ab^{-1} \in S$;

(2) $S \neq \{0\}$,且S中有单位元*(*即$(S^*,\cdot)$是一个乘法群*)*,

则称S是R的子除环.

定义 5.5 若S既是R的子整环也是R的子除环,则称S是R的子域.

例 5.1 *1* 对任意环R,零环$\{0\}$和R是R的子环,这两个环称为R的平凡子环.

2 偶数环$2\mathbb{Z}$是整数环的子环,但不是子整环.

3 $\mathbb{Z}[x]$是$F[x]$的子环,其中F是数域.

4 $S=\{[0],[2],[4]\}$是$\mathbb{Z}_6$的子域,但$\mathbb{Z}_6$不是整环,并且S与$\mathbb{Z}_6$的单位元不相等.

5 设$S_1 = \left\{ \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}, n \in \mathbb{Z} \right\}$,

$S_2 = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \alpha \in \mathbb{C} \right\}$,

$S_3 = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \alpha,\beta \in \mathbb{Z} \right\}$.

则S_1是$M_2(\mathbb{C})$的子整环,S_2是$M_2(\mathbb{C})$的子域, S_3是$M_2(\mathbb{C})$的子除环,但$M_2(\mathbb{C})$不是整环,不是除环,更不是域.

由此可以看出,子环具有很多奇怪的性质,总之有

性质 5.1 设S是R的子环,则

(1) R有单位元,S未必有单位元;

(2) R没有单位元,S可能有单位元;

(3) R不是交换环,S可能是交换环;

(4) R和S都有单位元,但它们的单位元可能不一致;

(5) R不是整环(除环、域),S可能是整环(除环、域);

(6) R是整环(除环、域),S未必是整环(除环、域).

性质 5.2 设R为环,记$C(R)=\{a\in R|\forall x\in R, ax=xa\}$,则$C(R)$是$R$的子环, 这个子环叫做$R$的中心,并且若$R$是交换环,则$C(R)=R$.

性质 5.3 设R_1和R_2都是环,则$R_1\cap R_2$是R_1和R_2的子环.

定义 5.6 设φ是环$(R,+,\cdot)$到环$(\bar{R},\bar{+},\bar{\cdot})$的映射.若有

$$\varphi(a+b)=\varphi(a)\bar{+}\varphi(b), \varphi(a\cdot b)=\varphi(a)\bar{\cdot}\varphi(b), \forall a,b\in R$$

则称φ是一个环同态映射,如果φ 满射(单射、双射),则称φ为环满同态(环单同态、环同构).当φ是环同态满射时,称R与$\bar{R}$同态,记为$R\sim\bar{R}$.

由定义即得

定理 5.1 设$(A,+,\cdot),(\bar{A},\bar{+},\bar{\cdot})$是两个代数系统,如果$\varphi$是$A$ 到$\bar{A}$的满射,且对$\forall a,b\in A, \varphi(a+b)=\varphi(a)\bar{+}\varphi(b), \varphi(a\cdot b)=\varphi(a)\bar{\cdot}\varphi(b)$, 则当$(A,+,\cdot)$是环时,$(\bar{A},\bar{+},\bar{\cdot})$也是环.

定理 5.2 设$R\overset{\varphi}{\sim}\bar{R}$是环同态满射,则

(1) $\varphi(0_R)=0_{\bar{R}}$;

(2) $\varphi(1_R)=1_{\bar{R}}$;

(3) $\varphi(-a)=-\varphi(a)$;

(4) 若R是交换环,则$\bar{R}$也是交换环.

例 5.2 *1* $\varphi:\mathbb{Z}\to\mathbb{Z}_6; n\mapsto[n]$为环满同态, $\mathbb{Z}$是整环,但$\varphi(2)$是$\mathbb{Z}_6$中的零因子.这说明:非零因子的象可能是零因子.

2 设$R=\mathbb{Z}\times\mathbb{Z}=\{(a,b)|a,b\in\mathbb{Z}\}, R$ 中的加法和乘法均为分量的加法和乘法,则R是一个环,R到$\mathbb{Z}$的投射$\pi_1:R\to\mathbb{Z};(a,b)\mapsto a$是环同态满射,这个同态满射使$R$ 中零因子的象不是零因子.

定理 5.3 若$R\overset{\varphi}{\cong}\bar{R}$是环同构,则$R$是整环*(*除环,域*)*当且仅当$\bar{R}$是整环*(*除环,域*)*.

由此可以得到

引理 5.1 设$(R,+,\cdot)$是一个环,$\varphi:R\to A$是一个双射*(A*为集合*)*,则可以给集合A定义加法和乘法,使得φ成为R到A的同构.

定理 5.4 (挖补定理) 设S是环$(R,+,\cdot)$的一个子环,$B=R-S$.$\bar{S}$也是环且$S\overset{\varphi}{\cong}\bar{S}, B\cap S=\emptyset$.则存在环$\bar{R}$,满足:*(1)* $R\cong\bar{R}$; *(2)* $\bar{S}$是$\bar{R}$的子环.

证 1 设$S=\{a_S,b_S,c_S,\cdots\}\overset{\varphi}{\to}\bar{S}=\{\bar{a_S},\bar{b_S},\bar{c_S},\cdots\}; x_S\mapsto\bar{x_S}$.记$B=\{a,b,c,\cdots\}$. 作$f:R\to\bar{R}; x\mapsto\begin{cases}\bar{x_S}, & \text{若}x\in S;\\ x & \text{若}x\in B.\end{cases}$ 则f为双射.

由引理,可为$\bar{R}$定义加法$\bar{+}$和乘法$\bar{\cdot}$,使$\bar{R}$为环且$R\overset{f}{\cong}\bar{R}$.

设S与$\bar{S}$中的加法和乘法分别记为$+,\cdot$,下证:在$\bar{S}$内,$+$与$\bar{+}$是一致的,$\cdot$与$\bar{\cdot}$是一致的.

$\forall\bar{x}_S,\bar{y}_S\in\bar{S},\bar{x}_S+\bar{y}_S=\bar{z}_S\in\bar{S}$, 则有$x_S,y_S,z_S\in S$使$\varphi(x_S)=\bar{x}_S,\varphi(y_S)=\bar{y}_S,\varphi(z_S)=\bar{z}_S$,于是$\bar{x}_S\bar{+}\bar{y}_S=\varphi(x_S)\bar{+}\varphi(y_S)=f(x_S)\bar{+}f(y_S)=f(x_S+y_S)=f(z_S)=\varphi(z_S)=\bar{z}_S$, 这说明在$\bar{S}$中$\bar{+}$与$+$是一致的.

同理可证,在$\bar{S}$中$\bar{\cdot}$与$\cdot$也是一致的.所以,$\bar{S}$ 是$\bar{R}$的子环. □

§6 多项式环

本节主要包含以下内容:

1 多项式环的定义.

2 未定元存在定理.

设R_0是有单位元1_{R_0}的交换环,R是R_0的子环且$1_{R_0}\in R$.任取定$\alpha\in R_0$,考察R_0中含R与α的最小子环:

$R[\alpha]=\{f(\alpha)=\sum_{i=0}^{n}a_i\alpha^i\mid a_i\in R, n\in\mathbb{N}\}$,

显然有
$f(\alpha)=\sum\limits_{i=0}^{n}a_i\alpha^i=a_0+a_1\alpha+\cdots+a_n\alpha^n\in R_0.$

定义 6.1 如上形式的$f(\alpha)$叫做R上关于α的一个多项式,a_i叫做多项式$f(\alpha)$的系数.

$R[\alpha]$作成一个环(R_0的子环),还需指出$R[\alpha]$中的运算:
$\forall f(\alpha)=\sum\limits_{i=0}^{n}a_i\alpha^i, g(\alpha)=\sum\limits_{j=0}^{m}b_j\alpha^j$,不妨设$m\le n, b_{m+1}=b_{m+2}=\cdots=b_n=0$, 运算为

$$f(\alpha)+g(\alpha)=\sum_{i=0}^{n}(a_i+b_i)\alpha^i,$$

$$f(\alpha)\cdot g(\alpha)=(\sum_{i=0}^{n}a_i\alpha^i)(\sum_{j=0}^{m}b_j\alpha^j)=\sum_{k=0}^{n+m}c_k\alpha^k$$

其中$c_k=\sum\limits_{i+j=k}a_ib_j$.

定义 6.2 环$R[\alpha]$叫做R上的α的多项式环.

由于$R[\alpha]$中多项式$f(\alpha)$的表达形式未必惟一(例如,$R=\mathbb{Z},\alpha=\sqrt{2}\in R_0=\mathbb{R}$,则在$\mathbb{Z}[\sqrt{2}]$中有$0=0+0(\sqrt{2})^2=-2+(\sqrt{2})^2$,即0的表达式不惟一),就是说:上述定义的多项式环中会出现一种现象:$f(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0$,但系数$a_0,a_1,a_2,\ldots,a_n$不全为零.这与高等代数中的零多项式的定义相矛盾.因此, 我们有必要对α作进一步讨论.

定义 6.3 R_0中的一个元素α叫做R上的一个未定元(超越元),如果在R中找不到不全为零的元素$a_0,a_1,a_2,\ldots,a_n$使$\sum\limits_{i=0}^{n}a_i\alpha^i=0$.否则,称$\alpha$为$R$上的代数元.习惯上,记$R$上的未定元为$x$.

定义 6.4 设$f(\alpha)=a_0+a_1x+a_2x^2+\cdots+a_nx^n(a_n\neq 0)$为环$R$上的一元多项式, 则非负整数$n$叫做这个多项式的次数, 多项式0没有次数.

R上未定元的多项式才可定义次数,但对给定的环,未定元未必存在.例如,设$R_0=\mathbb{Q},R=\mathbb{Z}$的未定元不存在.

定理 6.1 (未定元存在定理) 设R是有单位元的交换环,则存在R的扩环R_0,使得R_0中含有R的未定元.

证明思路 1 *(1)* 记$P=\{(a_0,a_1,a_2,\cdots)\mid a_i\in R$, 只有有限个$a_i\neq 0\}$, 其运算为:$(a_0,a_1,a_2,\cdots)+(b_0,b_1,b_2,\cdots)=(a_0+b_0,a_1+b_1,a_2+b_2,\cdots),(a_0,a_1,a_2,\cdots)\cdot(b_0,b_1,b_2,\cdots)=(c_0,c_1,c_2,\cdots)$,
其中$c_k=\sum\limits_{i+j=k}a_ib_j$.则$P$是有单位元$(1,0,0,\cdots)$的交换环.

(2) P中全体形为$(a,0,0,\cdots)$的元素作成与R同构的子环$\bar{R}$,且$(P-\bar{R})\cap R=\emptyset$,由挖补定理得到一个新的环$R_0$,使得$R$是$R_0$的子环且$R_0\cong P,R_0$的单位元就是$R$中单位元$1_R$.

(3) 记$x=(0,1,0,0,\cdots)$,则x是R上的未定元.

例 6.1 设F为整环,R为F的子环,如果F中的每个元素都是R上的代数元, 则F是一个域.

设R_0是有单位元的交换环,R是R_0的子环且$1_{R_0} \in R$.任取R_0中n个元素$\alpha_1, \alpha_2, \cdots, \alpha_n$,首先作$R$上$\alpha_1$的多项式环$R[\alpha_1]$,再作$R[\alpha_1]$上$\alpha_2$的多项式环$R[\alpha_1][\alpha_2], \ldots$,最后作$R[\alpha_1][\alpha_2]\cdots[\alpha_{n-1}]$上$\alpha_n$的多项式$R[\alpha_1]\cdots[\alpha_n]$.

$\forall f(\alpha_1, \ldots, \alpha_n) \in R[\alpha_1]\cdots[\alpha_n]$,有$f(\alpha_1, \ldots, \alpha_n) = \sum a_{i_1 i_2 \cdots i_n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}$,其中系数$a_{i_1 i_2 \cdots i_n} \in R$ 只有有限个$\neq 0$.

定义 6.5 上述描述的每个$f(\alpha_1, \ldots, \alpha_n)$称为$R$上的$\alpha_1, \ldots, \alpha_n$多元多项式,而每个$a_{i_1 i_2 \cdots i_n}$叫作$f(\alpha_1, \ldots, \alpha$数.习惯上,$R$上$\alpha_1, \ldots, \alpha_n$的多元多项式环$R[\alpha_1]\cdots[\alpha_n]$记作$R[\alpha_1, \ldots, \alpha_n]$.

多元多项式环中的加法和乘法运算为

$$
\begin{aligned}
&(\sum_{i_1 i_2 \cdots i_n} a_{i_1 i_2 \cdots i_n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}) + \\
&+(\sum_{j_1 j_2 \cdots j_n} b_{j_1 j_2 \cdots j_n} \alpha_1^{j_1} \alpha_2^{j_2} \cdots \alpha_n^{j_n}) \\
&= (\sum_{i_1 i_2 \cdots i_n} (a_{i_1 i_2 \cdots i_n} + b_{i_1 i_2 \cdots i_n}) \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}) \\
&(\sum_{i_1 i_2 \cdots i_n} a_{i_1 i_2 \cdots i_n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}) \\
&(\sum_{j_1 j_2 \cdots j_n} b_{j_1 j_2 \cdots j_n} \alpha_1^{j_1} \alpha_2^{j_2} \cdots \alpha_n^{j_n}) \\
&= (\sum_{k_1 k_2 \cdots k_n} c_{k_1 k_2 \cdots k_n} \alpha_1^{k_1} \alpha_2^{k_2} \cdots \alpha_n^{k_n})
\end{aligned}
$$

其中$c_{k_1 k_2 \cdots k_n} = \sum_{i_m + j_m = k_m} a_{i_1 i_2 \cdots i_n} b_{j_1 j_2 \cdots j_n}$

多元多项式环中也存在着表示不惟一的问题,因此要定义无关未定元.

定义 6.6 R_0中n个元$x_1, x_2, \cdots, x_n$叫做R上的无关未定元,如果它们满足:R上的任一个关于$x_1, x_2, \cdots, x$多项式为零$\Leftrightarrow$该多项式的系数全为零.

容易证明

定理 6.2 设R是一个有单位元的交换环,对任意正整数n,存在R上的无关未定元$x_1, x_2, \cdots, x_n$,使多项式环$R[x_1, x_2, \cdots, x_n]$存在.

定理 6.3 设$\alpha, x \in R_0, R$是R_0的子环,x为R上的未定元,则$R[x] \sim R[\alpha]$.

一般地,有

定理 6.4 设$R[x_1, x_2, \ldots, x_n]$和$R[\alpha_1, \alpha_2, \ldots, \alpha_n]$都是有单位元的交换环$R$上的多项式环,且$x_1, x_2, \ldots, x_n$的无关未定元,而$\alpha_1, \alpha_2, \ldots, \alpha_n$是$R_0$中的任意元,则$R[x_1, x_2, \ldots, x_n] \sim R[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

推论 6.1 在$R[x]$中,设$u(x) = f(x) + g(x), v(x) = f(x) \cdot g(x)$,则在$R[\alpha]$中有$u(\alpha) = f(\alpha) + g(\alpha), v(\alpha) = f(\alpha) \cdot g(\alpha)$.

作业

p. 97 1 p. 101 2,3,4

p. 109 2

§7 理想

本节主要包括以下内容:

1 理想的定义;

2 单环的概念;

3 生成理想的概念及其中元素的表示形式;

4 主理想和特殊情况下主理想的结构.

设N是环R的子环,则$(N,+)\leq(R,+)$,
且由$(R,+)$是可换群可知$N\lhd R$, 于是有商群$R/N=\{a+N\mid\forall a\in R\}$,商群中的加法为$(a+N)+(b+N)=(a+b)+N$.

对于R/N,是否可以再定义一个乘法使R/N成为环?

如果R/N成为环,必有

$$(a+N)(b+N)=ab+N. \tag{$*$}$$

要使$(*)$式成立,N该满足什么条件呢?

由于$ab+N\subseteq ab+N+aN+bN=(a+N)(b+N)$,所以,$(*)$成立的关键是$(a+N)(b+N)\subseteq ab+N$.由此可以得到

性质 7.1 对$\forall a,b\in R$,

$$(a+N)(b+N)=ab+N\Leftrightarrow aN\subseteq B且Nb\subseteq N.$$

所以,R的子环N满足$\forall a,b\in R,aN,Nb\subseteq N$是很重要的.因为, 由此可以在商群$(R/N,+)$中定义乘法,使$\forall a,b\in R,(a+N)(b+N)=ab+N$.

定义 7.1 设N是R的子环.

(1) 如果$\forall a\in R$,有$aN\subseteq N$,则称N是R的一个左理想;

(2) 如果$\forall a\in R$,有$Na\subseteq N$,则称N是R的一个右理想;

(3) 如果$\forall a,b\in R$,有$aN\subseteq N,Nb\subseteq N$, 则称$N$是$R$的一个理想.

本节主要讨论理想.N是R的理想是指:N首先是R的子环;其次,$\forall a,b\in R, aN\subseteq N, Nb\subseteq N$.于是有

定义 7.2 设N是R的非空子集,如果

(1) $\forall a,b\in N, a-b\in N, ab\in N$;

(2) $\forall r\in R, rN\subseteq N, Nr\subseteq N$,

则称N为R的一个理想.

等价地,有

定义 7.3 设$N(\neq\emptyset)\subseteq R$,如果

(1) $\forall a,b\in N, a-b\in N$;

(2) $\forall r\in R, \forall n\in N, rn, nr\in N$,

则称N为R的一个理想,记为$N\lhd R$.

例 7.1 对任意环R,有*0(*零理想*)*$\lhd R$(单位理想)$\lhd R$.这两个理想统称为R的平凡理想.而R的其它理想*(*如果存在的话*)*,叫做R的真理想.

例 7.2 $2\mathbb{Z}\lhd\mathbb{Z}$.

例 7.3 设R是数环,则$N=\left\{\begin{pmatrix} a & 0\\ 0 & a\end{pmatrix}\mid \forall a\in R\right\}$是$M_2(R)$的子环,但$N\not\lhd M_2(R)$.

定理 7.1 除环*(*或域*)*R只有平凡理想.

定义 7.4 只有平凡理想的环称为单环.

显然,除环和域都是单环.

性质 7.2

- 若N是有单位元的环R的理想,且$1_R\in N$,则$N=R$;
- 若$N_1,N_2\lhd R$,则$N_1+N_2\overset{def}{=}\{a+b|a\in N_1,b\in N_2\}\lhd R$,这个理想通常称为理想$N_1$与$N_2$的和理想;
- 若$N_1,N_2\lhd R$,则$N_1N_2=\{a_1b_1+a_2b_2+\cdots+a_nb_n|a_i\in N_1,b_i\in N_2\}\lhd R$,这个理想通常称为理想$N_1$与$N_2$的积理想;
- 若$N_i\lhd R, i\in I$,则$\cap_{i\in I}N_i\lhd R$.

设R为环,$S(\neq\emptyset)\subseteq R,\Omega=\{A|A\lhd R$ 且$S\subseteq A\}$. 则$\cap_{A\in\Omega}A\lhd R$, 这个理想叫做由子集S生成的理想,记为(S), S叫做(S)的生成子集.显然,(S)是R中包含S的理想中最小的一个.当$S=\{a_1,a_2,\cdots,a_n\}$ 是有限集时,记$(S)=(a_1,a_2,\cdots,a_n)(=\sum_{i=1}^{n}(m_ia_i+x_ia_iy_i+r_ia_i+a_is_i)$,其中$m_i\in\mathbb{Z},\forall x_i,y_i,r_i,s_i\in R)$.特别地,

定义 7.5 由环R中一个元素a生成的理想(a)叫做R的主理想.

当R是有单位元的交换环时,$(a)=\{ra|r\in R\}$.

例 7.4 已知$\mathbb{Z}[x]$是整环,$(2,x)=\{2f(x)+xg(x)|f(x),g(x)\in R[x]\}=\{a_nx^n+\cdots+a_1x+2a_0|a_i\in\mathbb{Z}\}\lhd\mathbb{Z}[x]$. 但$(2,x)$不是$\mathbb{Z}[x]$的主理想.

事实上,若$\exists f(x)\in\mathbb{Z}[x]$ 使$(2,x)=(f(x))$, 则有$2=g(x)f(x),x=h(x)f(x)$, 于是$f(x),g(x)$都是非零常数,$x=h(x)a$,故$|a|=1$, 所以$1\in(2,x)$,这是不可能的.

§8 剩余类环、同态与理想

本节的主要内容是环的同态基本定理与对应定理.

设I是环R的理想,则对于加法来说,I是R的正规子群,于是I的陪集$a+I,b+I,c+I,\cdots$作成R的一个分类,这个分类叫做模I的剩余类.这个分类也相当于给出了R的元素间的一个等价关系:$a\sim b\Leftrightarrow a-n\in I$, 这个等价关系也记为$a\equiv b\pmod I$(或$a\equiv b(I)$).

R模I的剩余类的集合记为R/I,这是一个加法群.对$\forall a+I,b+I\in R/I$, 定义

$$(a+I)\cdot(b+I)=ab+I,$$

则这个定义是有意义的,并且$(R/I,\cdot)$作成一个半群, R/I中的乘法对加法满足左右分配律,所以,$(R/I,+,\cdot)$是一个环.

定义 8.1 设R为环,$I\lhd R$.称$(R/I,+,\cdot)$为R关于理想I的剩余类环 (商环),R/I中的元素叫做模I的剩余类.

例 8.1 设$R=\mathbb{Z},I=(6)=6\mathbb{Z}$,则$R/I=\mathbb{Z}_6$.

例 8.2 设$R=\mathbb{Z}_6[x],I=(1+x)$,则$R/I\cong\mathbb{Z}_6$.

例 8.3 设$R=\mathbb{Z}_6[x],I=(x)$,则$R/I\cong\mathbb{Z}_6$.

定义 8.2 设$\varphi:R_1\to R_2$为环同态,称R_2中零元的完全原象$\varphi^{-1}(0)=\{a\in R_1|\varphi(a)=0\}$为$\varphi$的核,记为$ker\varphi$.

定理 8.1 设$\varphi:R\to\bar{R}$为环同态满射,$I=ker\varphi$.则

(1) $I \lhd R$;

(2) $R/I \cong \bar{R}$.

定理 8.2 设R是环,$I \lhd R$.则有环同态$\varphi : R \to R/I$使φ是环满同态且$ker\ \varphi = I$.称这样的φ为环的自然同态.

上面的两个定理合称为环的同态基本定理.

定理 8.3 设$\varphi : R \to \bar{R}$为是环同态映射,则

(1) 若S是R的子环,则$\varphi(S)$是$\bar{R}$的子环;

(2) 若I是R的理想且φ为满射,则$\varphi(I)$是$\bar{R}$的理想;

(3) 若$\bar{S}$是$\bar{R}$的子环,则$\varphi^{-1}(\bar{S})$是R的子环;

(4) 若$\bar{S}$是$\bar{R}$的理想,则$\varphi^{-1}(\bar{S})$是R的理想.

作业

p. 113 2,5 p. 116 3

§9 最大理想

本节主要包括以下内容:

1 最大理想的概念和判断最大理想的方法;

2 通过最大理想获得域的方法;

3 素理想的概念和基本性质.

注 9.1 本教材中的"最大理想"在很多书中被称为"极大理想".为了与教材一致,我们仍用"最大理想"这个名词.

事实上,本教材中的"最大"是"极大"的意思,就是没有谁比它大(而"最大"应该是比谁都大的意思,这是本教材的一个缺陷).

整数12有因数1,2,3,4,6,4和6是12的"最大" (极大)因数.一般地,a是n的"最大" 因数当且仅当n/a是素数.本节主要是将这种思想应用到环上来.

定义 9.1 设I是环R的一个理想,且$I \neq R$,如果R除了R和I外,没有能包含I的其他理想,则称I是R的一个最大理想.

验证R的理想I是最大理想一般有两步:

(1) $I \neq R$(当$1_R \in R$时,通常证明$1_R \notin I$);

(2) 若$(I \subsetneq) J \lhd R$,则$J = R$.

例 9.1 *1* 设$R = \mathbb{Z}, p$是素数,则由p生成的理想$I = (p)$是R的最大理想.

2 设$R = \mathbb{Q}, p$是素数,则由p生成的理想$I = (p)$不是R的最大理想.

3 设R是非零环,则R为单环当且仅当零理想$\{0\}$是最大理想.

4 设R是偶数环,$I = 4\mathbb{Z} \lhd R$,则I是R的最大理想.

引理 9.1 设$I(\neq R) \lhd R$,则剩余类环R/I为单环$\Leftrightarrow$ I是R的最大理想.

引理 9.2 设R是有单位元$1_R(\neq 0)$的交换环,则R为域$\Leftrightarrow$ R为单环.

定理 9.1 设R是有单位元$1_R(\neq 0)$的交换环,$I \lhd R$,则R/I为域$\Leftrightarrow$ I是R的一个极大理想.

定义 9.2 设$I \lhd R$,若$\forall a, b \in R$,由$ab \in R$必有$a \in R$或$b \in R$,则称I为R的一个素理想.

例 9.2 设p是素数,则(p)与$\{0\}$都是$\mathbb{Z}$的素理想.

性质 9.1 设R是环,则

(1) R是素理想;

(2) 零理想是素理想$\Leftrightarrow$ R是无零因子环.

§10 商域

本节主要介绍由无零因子交换环来构造商域的方法.

定理 10.1 设R是无零因子交换环,则存在一个域Q,使R成为Q的一个子环,且$Q=\left\{\frac{a}{b}\mid a,b(\neq 0)\in R\right\}$.

定义 10.1 设R是环而Q是包含R的一个域,如果$Q=\left\{\left[\frac{a}{b}\right]\mid a,b(\neq 0)\in R\right\}$,则称$Q$为$R$的商域.

定理 10.2 设$R\neq 0$,且F为包含R的域,则F必包含R的商域.

定理 10.3 若环R与环$\bar{R}$同构,则它们各自的商域也同构.

注 10.1 这两个定理是说,环R可能会有两个"不同"的商域,但在同构的意义下,每个环最多只有一个商域.

作业

p. 119 1 p. 124 1,2

练习与思考题

1. 证明:对有单位元的环来说,加法适合交换律可以由定义中其它条件推出.
2. 如果环R中每个元素x都满足$x^2=x$,则称R为布尔(Bool)环.证明: 对布尔环R中每个元素x,y都有$x+x=0, xy=yx$.
3. 举出不同环,分别满足下列条件:
   (a) 既无左单位元,也无右单位元;
   (b) 只有左单位元,而无右单位元;
   (c) 只有右单位元,而无左单位元.

4. 对于下列情形,分别给出一个具体例子:

   (a) 环R有单位元,而它的一个子环S无单位元;

   (b) 环R无单位元,而它的一个子环S有单位元;

   (c) 环R及其子环都有单位元,但这两个单位元不相等.

5. 环R中的元素a称为拟正则的,若有$a' \in R$使$a + a' + aa' = 0$. 证明:

   (a) 幂零元是拟正则元;

   (b) 若R有单位元1,则a是拟正则元当且仅当存在$a' \in R$使$(1 + a)(1 + a') = 1$.

6. 问:一个环是否可以与其真子环同构?

7. 证明:实数域的自同构只有恒等自同构.

8. 证明:从$\mathbb{Z}[i]$到$\mathbb{Z}[x]$的同态映射只有零同态.

9. 证明:整数环$\mathbb{Z}$的不同的子环不同构.

10. 设R是可换环,$M, N \lhd R$.证明:$N \subseteq r(N) = \{a|a \in R$ 且有$a^n \in N\} \lhd R$,其中n是与a有关的正整数.$r(N)$称为理想N的根理想. 并且有$r(M \cap N) = r(M) \cap r(N)$.

11. $\mathbb{Z}_m$与$\mathbb{Z}_n$同态当且仅当$n|m$.

12. 设S是环R的非空子集.证明:$l(S) = \{x \in R|xS = \{0\}\}$是$R$的左理想, 且存在$R$的右理想$K$使$l(S) = l(K)$.

13. 设R是一个阶大于1的有限环.证明:如果R无零因子,则R是一个除环.

14. 设R是阶大于1且有单位元的可换环.证明:R是域当且仅当R到任意环的非零同态都是单同态.

15. 证明:(x)与$(2, x)$都是多项式环$\mathbb{Z}[x]$的素理想.

16. 设$I \lhd R$.证明:I是R的极大理想当且仅当R/I是单环.

第一次世界大战是化学家的战争;

第二次世界大战是物理学家的战争;

未来的世界大战如果发生,

—-那将是数学家的战争.

—-佚名

第四章 整环里的因子分解

从代数的观点来看,初等数论是研究整数环$\mathbb{Z}$的学科.首先是整除性, 然后是由此派生出来的一系列概念:因子和倍数,公因子和公倍数,最大公因子和最小公倍数,以及欧几里得除法算式等.

整数通常可分解成一些更小的整数之积,不能再分解的最小单位就是素数.而作为初等数论的基石—-算术基本定理是说:每个大于等于2的整数可以(不计次序)惟一地分解成素数的积.本章试图将$\mathbb{Z}$中的上述概念和性质推广到任意整环上去.这种推广是从整除性开始的.

§1 素元、惟一分解

本节主要应该掌握素元的概念与惟一分解的意义.

定义 1.1 设R是整环,$a,b\in R$,若有$c\in R$使$a=bc$,则称a被b整除. 如果a能被b整除,则称b为a的因子,并用符号$b\mid a$来表示;如果b不能整除a,用符号$b\nmid a$来表示.

定义 1.2 若ε是整环R中有逆元的元素,则称ε为R的一个单位.

设$a,b\in R$,若$b=\varepsilon a$,则称b为a的相伴元.

由单位的定义,显然有

定理 1.1 两个单位的乘积是单位,单位的逆元也是单位.

定义 1.3 单位以及元a的相伴元叫做a的平凡因子.其余的a的因子,如果还有的话,叫做a的真因子.

定义 1.4 如果整环R的元素p既不是零元,也不是单位,并且p只有平凡因子,则称p为R的一个素元.

定理 1.2 单位与素元的乘积是素元.

定理 1.3 整环中一个不等于零的元a有真因子$\Leftrightarrow a=bc, b$和c 都不是单位.

推论 1.1 若$a(\neq 0)$有真因子$b, a=bc$,则c也是a的真因子.

定义 1.5 称整环R中的元素a在R中有惟一分解,如果

(1) a在R中能分解成素元的乘积,即$a=p_1p_2\cdots p_r$ *(其中p_i是R的素元);*

(2) 若又有$a=q_1q_2\cdots q_s$ *(其中q_i是R的素元),*

则$r=s$,并且适当调整p_i与q_j的次序后有$q_i=\varepsilon_i p_i$(其中ε_i是R的单位).

例 1.1 4在$R=\{a+b\sqrt{-3}\mid a,b\in\mathbb{Z}\}$不具有惟一分解性.

§2 惟一分解环

本节主要应该掌握惟一分解环的概念、惟一分解定理及其证明.

定义 2.1 一个整环R称为惟一分解环,如果R的既不等于零又不是单位的元都有惟一分解.

定理 2.1 一个惟一分解环有以下性质:

(ⅲ) 若一个素元p能整除ab,则p能整除a或b.

反之,有

定理 2.2 如果一个整环满足以下性质:

(i) R中的每个既不是零元也不是单位的元素a都有一个分解$a=p_1p_2\cdots p_r$(其中p_i是R的单位);

(ⅱ) 如果R的一个素元p能整除ab,则p能整除a或b,

则R一定是一个整环.

定义 2.2 元c叫做元$a_1,a_2,\ldots,a_n$的公因子,如果c能同时整除$a_1,a_2,\ldots,a_n$.

元$a_1,a_2,\ldots,a_n$的一个公因子d叫做$a_1,a_2,\ldots,a_n$ 的最大公因子,如果d能够被$a_1,a_2,\ldots,a_n$的每一个公因子c 整除.

定理 2.3 一个惟一分解环R的两个元a和b在R中一定有最大公因子.a和b的最大公因子d和d'只能差一个单位因子:$d' = \varepsilon d$ (其中ε是单位).

由归纳法可以得到

定理 2.4 一个惟一分解环R的n个元$a_1, a_2, \ldots, a_n$在R中一定有最大公因子. $a_1, a_2, \ldots, a_n$的两个最大公因子只能差一个单位因子.

定义 2.3 如果一个惟一分解环的元素$a_1, a_2, \ldots, a_n$的最大公因子是单位,则称$a_1, a_2, \ldots, a_n$互素.

作业

p. 130 1,2 p. 135 2

§3 主理想环

本节的目的是证明主理想环一定是惟一分解环,主要应该掌握主理想环的概念、性质与应用.

定义 3.1 如果整环R的每个理想都是主理想,则称R为主理想环.

为了证明主理想环是惟一分解环,我们先要证明两个引理.

引理 3.1 设R是一个主理想环,若序列$a_1, a_2, a_3, \ldots$ $(a_i \in R)$中每一个元素都是其前面一个元素的真因子,则这个序列一定是一个有限序列.

注 3.1 考虑主理想

$$(a_1), (a_2), \cdots, (a_n), \cdots$$

有主理想的升链

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots$$

记$I = \cup_{i=1}^{\infty}(a_i)$,则$I$也是$R$的理想.于是存在$d \in R$使$I = (d)$,又由$d \in I$可知存在$n$,使$d \in (a_n)$.我们断言:$a_n$是序列$a_1, a_2, a_3, \ldots$(其中每一个元素都是其前面一个元素的真因子)的最后一个元素.

事实上,若a_{n+1}是a_n的真因子,则

$$a_{n+1} \mid a_n, a_n \mid d \mid a_{n+1}$$

于是$a_{n+1} = ca_n = cc'a_{n+1}$,再由$R$是整环知$cc' = 1$,因而$a_{n+1}$与$a_n$相伴,这与$a_{n+1}$是$a_n$的真因子相矛盾.

引理 3.2 如果R是主理想环,则R的素元p生成一个最大理想.

证 设理想I满足$(p) \subsetneqq I \subseteq R$,则有$d \in R$使$I = (d)$, 且$d$不是$p$的相伴元.由$p \in (d)$即$p = dc, c \in R - R^{\cdot}$,有$p \mid c$, 于是$d \in R^{\cdot}$,所以$I = R$.

定理 3.1 (主要定理) 主理想环R是惟一分解环.

证(主要定理的证明) 首先证明:R中的每个既不是零元也不是单位的元素a都有一个分解.事实上, 若a不能写成有限个素元的乘积,则a不是素元,于是可得a的真因子的无穷序列$a_1, a_2, a_3, \ldots$,其中每一个元素都是其前一个元素的真因子. 这与R是主理想环相矛盾.

再证:若$p \mid ab$则$p \mid a$或$p \mid b$.由$ab \in (p)$知,在剩余类环$R/(p)$中,$[a][b] = [ab] = 0$.但(p)是R的最大理想,$I/(p)$是域,有$[a] = 0$或$[b] = 0$,即$p \mid a$或$p \mid b$.

§4 欧氏环

本节的目的是证明欧氏环一定是惟一分解环,主要应该掌握欧氏环的概念、性质与应用.

定义 4.1 如果整环R满足

(1) 存在映射$\varphi : R \to \mathbb{N}$;

(2) 给定R的一个非零元a, R的任何元b都可以写成$b = qa + r (q, r \in R)$ 的形式,其中$r = 0$或$\varphi(r) < \varphi(a)$,

则称R为欧氏环.

例 4.1 整数环$\mathbb{Z}$是欧氏环.

定理 4.1 (主要定理) 欧氏环R是主理想环,因而是惟一分解环.

由此我们已经得到

$$\boxed{\text{欧氏环}} \subset \boxed{\text{主理想环}} \subset \boxed{\text{惟一分解环}}$$

事实上,有

$$\boxed{\text{欧氏环}} \subsetneqq \boxed{\text{主理想环}} \subsetneqq \boxed{\text{惟一分解环}}$$

推论 4.1 整数环是主理想环,因而是惟一分解环.

另外一种常见的欧氏环是一个域上的多项式环.为证明这个结论,需要

引理 4.1 假设$R[x]$是整环R上的一元多项式环,$R[x]$的元

$$g(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

的最高次项系数a_n是R的一个单位,则$R[x]$中的每个多项式$f(x)$都可以写成

$$f(x)=q(x)g(x)+r(x)\quad (q(x),r(x)\in R[x])$$

的形式,其中$r(x)=0$或$\deg r(x)<\deg g(x)$.

证 只需证$\deg f(x)>\deg g(x)$的情形. 设$f(x)=b_mx^m+\cdots+b_0, f_1(x)=f(x)-a_n^{-1}b_mx^{m-n}$,考虑到$\deg f_1(x)<\deg f(x)$,由数学归纳法即得证.

定理 4.2 一个域F上的一元多项式环$F[x]$是一个欧氏环.

作业

p. 138 1 p. 141 1,2,3

§5 多项式环的因子分解

本节的目的是证明:如果R是惟一分解环,则$R[x]$也是惟一分解环.

由此可以得到: 如果R是一个惟一分解环,则$R[x_1,x_2,\cdots,x_n]$是惟一分解环.

我们已经知道,域F上的多项式环$F[x]$是欧氏环,当然是惟一分解环. 本节将证明:惟一分解环R上的多项式环$R[x]$也是惟一分解环.

本节中的环R均指惟一分解环,Q为R的分式域.称只有平凡因子的多项式为素多项式,素多项式也叫做不可约多项式,有真因子的多项式叫做可约多项式.

定义 5.1 如果$R[x]$中多项式$f(x)$的系数的最大公因子是单位,则称$f(x)$为本原多项式.

我们有以下事实:

(1) R的单位是$R[x]$的仅有的单位.

(2) 一个本原多项式$\neq 0$.

(3) 若本原多项式$f(x)$可约,则$f(x)=g(x)h(x)$, 其中$f(x)$和$g(x)$的次数都大于0,因而都小于$f(x)$的次数.

我们先来看本原多项式的几个性质.

引理 5.1 若$f(x)=g(x)h(x)$,则$f(x)$是本原多项式$\Leftrightarrow$ $g(x)$和$h(x)$都是本原多项式.

证 ($\Leftarrow$).设$g(x)=a_0+a_1x+\cdots$, $h(x)=b_0+b_1x+\cdots$ 是两个本原多项式,若$f(x)=c_0+c_1x+\cdots(\neq 0)$不是本原多项式,则$c_0,c_1,\cdots$有非0的最大公因子$d(\notin R^{\cdot})$,再由$R$是惟一分解环知有素元$p|d$,于是$p|c_i$,从而有$p$整除所有的$a_i$或$p$整除所有的$b_j$,这与$g(x),h(x)$ 都是本原多项式相矛盾.

引理 5.2 $\forall f(x)(\neq 0)Q[x]$,存在$R[x]$中的本原多项式$f_0(x)$和$a,b\in R$使$f(x)=\frac{b}{a}f_0(x)$.且在相伴的意义下,$f_0(x)$是惟一的.

证 设$f(x)=\frac{b_0}{a_0}+\frac{b_1}{a_1}x+\cdots+\frac{b_n}{a_n}x^n, a_i,b_i\in R$.记$a=a_0a_1\cdots a_n$,则$f(x)=\frac{1}{a}(c_0+c_1x+\cdots+c_nx^n)$. 设$c_0,c_1,\cdots,c_n$的最大公因子为$b$,则$f(x)=\frac{b}{a}f_0(x)$,且$f_0(x)$ 为$R[x]$中的本原多项式.

若又有$f(x)=\frac{d}{c}g_0(x)$,其中$c,d\in R, g_0(x)$为$R[x]$中的本原多项式, 则$bcf_0(x)=adg_0(x)\overset{记}{=}h(x)\in R[x]$.由$f_0(x)$与$g_0(x)$ 均为本原多项式可知,ad,bc均为$h(x)$的系数的最大共因子,所以,$\exists\varepsilon\in R^{\cdot}$使$bc=\varepsilon ad$,即有$\varepsilon f_0(x)=g_0(x)$.

引理 5.3 设$f(x)$是$R[x]$中的一个本原多项式,则$f(x)$在$R[x]$中可约$\Leftrightarrow$ $f(x)$在$Q[x]$中可约.

证 ($\Leftarrow$).设$f(x)=g(x)h(x), g(x),h(x)$均为$Q[x]$中的本原多项式.于是有$R[x]$中的本原多项式$g_0(x),h_0(x)$以及$a,b,c,d\in R$使$g(x)=\frac{b}{a}g_0(x), h(x)=\frac{d}{c}h_0(x)$,并且$g_0(x)h_0(x)$为本原多项式,所以$f(x)=\frac{bd}{ac}g_0(x)h_0(x)=(\varepsilon g_0(x))h_0(x)$,且$\varepsilon g_0(x), h_0(x)$都不是$R[x]$中的单位,故$f(x)$在$R[x]$中可约.

引理 5.4 设$f(x)$是$R[x]$中的一个本原多项式,且$\partial(f(x))>0$,则$f(x)$在$R[x]$中有惟一分解.

证 1 易知$f(x)$可以写成不可约的本原多项式的积$f(x)=p_1(x)p_2(x)\cdots p_s(x)$.

若又有$f(x)=q_1(x)q_2(x)\cdots q_t(x)$,其中$q_i(x)$是$R[x]$中的不可约的本原多项式.则$p_i(x),q_j(x)$均为$Q[x]$中的不可约多项式,由$Q[x]$ 是惟一分解环可知,$s=t$且可以假定$p_i(x)=\varepsilon_iq_i(x)$,其中$\varepsilon_i(=\frac{b_i}{a_i}, a_i,b_i\in R)$是$Q$中的单位,由引理2的证明可知$\varepsilon_i$为$R$中的单位,所以$p_i(x)=\varepsilon q_i(x)$.

定理 5.1 若R是惟一分解环,则$R[x]$也是.

证 设$f(x)$是$R[x]$中不是零也不是单位的一个多项式,若$f(x)$是本原多项式或$\partial(f(x))=0$则定理已证.以下假设$f(x)=df_0(x)$,其中d不是R的单位, $f(x)$是次数大于零的本原多项式.

由引理,$f(x)$有分解$f(x)=p_1\cdots p_mp_1(x)\cdots p_s(x)$,其中$p_i$是$R$中的素元,$p_j(x)$是$R[x]$中的不可约的本原多项式.若$f(x)$在$R[x]$中又能分解成不可约多项式的积$f(x)=q_1\cdots q_nq_1(x)\cdots q_t(x)$,则$q_i$是的素元,$q_j(x)$是$R[x]$中的不可约的本原多项式.

由引理1及引理2的证明可得$p_1\cdots p_m=\varepsilon q_1\cdots q_n$,所以$p_1(x)\cdots p_s(x)=q_1(x)\cdots q_t(x)$,再由$R$是惟一分解环及引理4可得:$m=n$,且可假定$p_i$与$q_i$相伴,$s=t$,且可假定$p_i(x)$与$q_i(x)$相伴.

由数学归纳法容易证明

定理 5.2 若R是惟一分解环,则$R[x_1,x_2,\cdots,x_n]$也是,其中$x_1,x_2,\cdots,x_n$是R上的无关未定元.

§6 因子分解与多项式的根

本节主要研究整环R上一元多项式的因子分解与根的关系.

由代数基本定理我们知道,复数域上的一元n次多项式有n个根.这个结论在一般的数域中并不成立.本节我们将研究整环上一元多项式的根的问题,本节中的环R均指整环.首先给出多项式的根的定义

定义 6.1 设$f(x) \in R[x]$,若存在$a \in R$使$f(a) = 0$,则称a为多项式$f(x)$的根.

由整环上多项式的带余除法,易知有

定理 6.1 $f(a) = 0 \Leftrightarrow (x-a)|f(x)$.

定理6.1可推广为

定理 6.2 R的k个不同的元$a_1, \cdots, a_k$都是$f(x)$的根$\Leftrightarrow (x-a_1)\cdots(x-a_k)$.

由此易得

推论 6.1 若$\partial(f(x)) = n$,则$f(x)$则R中至多有n个根.

一般地,

定义 6.2 若有$a \in R$使$(x-a)^k|f(x), k(>1) \in \mathbb{Z}$,则称$a$为$f(x)$的一个重根.

研究重根需要导数的概念

定义 6.3 由多项式$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$惟一决定的多项式$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$叫做$f(x)$的导数.

容易验证导数的如下性质

性质 6.1 *(1)* $(f(x)+g(x))' = f'(x) + g'(x)$.

(2) $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$.

(3) $(f^k(x)) = kf^{k-1}(x)f'(x)$.

关于重根,我们有

定理 6.3 $f(x)$的根a是重根$\Leftrightarrow (x-a) \mid f'(x)$.

推论 6.2 设$R[x]$是惟一分解环.$a(\in R)$是$f(x)$的重根$\Leftrightarrow x-a$ 能整除$f(x)$与$f'(x)$的最大公因子.

作业

p. 150 2

总复习

第一章 基本概念

1 映射;单射;满射;双射;

2 同态;同构(自同构);

3 等价关系与分类;商集.

第二章 群论

1 群(有限群)的定义;

2 群同态的性质;

3 变换群;Caylay定理;

4 置换群;置换的表示;

5 循环群的结构;

6 子群的(3个)判定定理与性质;生成子群;

7 子群的陪集;陪集的性质;Lagrange定理;

8 不变(正规)子群及其判定;商群;

9 同态基本定理;对应定理.

第三章 环与域

1 环;零因子;整环;

2 除环;域;

3 无零因子环的特征与性质;

4 子环;环的同态;挖补定理;

5 多项式环;

6 理想;生成理想;

7 剩余类环;环的同态基本定理与对应定理;

8 “最大”理想及其性质;商域.

第四章 整环里的因子分解

1 单位;素元;相伴元;惟一分解;

2 惟一分解环的2个定义;公因子;最大公因子;

3 主理想环的概念与性质;

4 欧氏环的概念与性质;

5 本原多项式;惟一分解环上多项式环的因式分解;

6 因子分解与多项式的根.

习题

第一章 §10 Ex 1,3

第二章 §1 Ex 3 §2 Ex 1,4 §5 Ex 2 §6 Ex 1 §7 Ex 2,3,4 §8 Ex 4,5 §9 Ex 2,3 §10 Ex 3

第三章 §2 Ex 5 §4 Ex 1 §5 Ex 3，4 §6 Ex 2 §7 Ex 1

第四章 §1 Ex 2，3 §2 Ex 3 §6 Ex 1，2

练习与思考题

1. 证明:在环$\mathbb{Z}[\sqrt{5}i]=\{a+b\sqrt{5}i|a,b\in\mathbb{Z}\}$中, $2+\sqrt{5}i$不能整除3.

2. 设$\alpha\in\mathbb{Z}[i]$,且$|\alpha|^2=p$是素数.证明:α是$\mathbb{Z}[i]$中的不可约元.反之如何?

3. 证明:环$\mathbb{Z}[\sqrt{2}i]$是主理想环.

4. 证明:x^2+1是多项式环$\mathbb{Z}[x]$中的不可约元,但$\mathbb{Z}[x]/(x^2+1)$ 不是域.