引　论　章

内容要点

1. 代数问题的特点,代数学研究的对象与特点.

2. 域、环、群(半群)的定义与相互联系.

3. 群、环、域的基本运算性质:消去律(加法与乘法)及零因子、单位元(零元)和逆元(负元)的唯一性、广义结合律、方幂和倍数.

4. 一般域上关于多项式理论、线性方程组理论、线性空间与线性变换的理论的定理.

读后注

1. 引论章§1的设置是体现总导引中第1点思想.

2. 引论章的§2是贯彻总导引中第三点思想.本教材主要讲群、环、域三个运算系统.本章第一节初步体现了研究代数运算系统的必要性.而§2中从人们熟悉的数域,整数环等例子为背景先引入一般域和环的定义.然后才引入只有一个运算的系统:群(半群).研究它们的基本性质时发现群是更基本的运算系统.这样在后面几章中就是先讲群,后讲域、环.于是群中的一些运算性质,如剩余类(陪集),商群,同态定理等都能在讲域、环时应用.这种次序安排下,逻辑关系清楚,且数学处理上可以简便些、而§2中先按域、环、群次序引入定义却是更适合人们的认知顺序.

3. §2最后的定理非常重要.其一是引入一般域这种运算系统就是为了能应用这个定理.其二,在本教材的开始就引入这个定理是为了使本教材的结构比以前教材有较大的变化.以前教材在群论一章之后必须以很大篇幅讲环,主要是讲因式分解唯一性定理.这几乎成了以前师范院校近世代数课程的主要部分.而更有应用更有兴趣的域论部分就无法讲授.我们的处理可以在本教材的第二、三章大量地讲域(特别是有限域)及其应用.而环只作为铺垫,占很少部分.其中用到的多项式及线性空间的性质全可由上面所述的定理所提供.这种处理使本教材的面貌焕然一新.

思考练习题（非必作题）

1．在一般域上叙述和证明除法算式(带余除法)成立．

2．一般域上非常数多项式都是一些不可约多项式的乘积．

3．设

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=b_1 \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=b_2 \\ \cdots\cdots\cdots\cdots \\ a_{s1}x_1+a_{s2}x_2+\cdots+a_{sn}x_n=b_s \end{cases}$$

是域 F 上的线性方程组．试给出“这个方程组是相关或无关的”，“这个方程组的极大无关部分组”的定义．证明这个方程组与它的极大无关部分组同解．

习　题

以下各题中有＊者为必作题，其余为选作题．

＊1．判断下列哪些是集合 A 上的代数运算．

(1) A＝所有实数，A 上的除法．

(2) A 是平面上全部向量，用实数和 A 中向量作数量乘法(倍数)．

(3) A 是空间全部向量，A 中向量的向量积(或外积，叉乘)．

(4) A＝所有实数，A 上的一个二元实函数．

＊2．给定集合 $F_2=\{1,0\}$，定义 F_2 上两个代数运算加法和乘法，用下面的加法表，乘法表来表示：

＋	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

例如，0＋1＝1，在加法表中＋号下的 0 所在的行与＋号右边的 1 所在的列相交处的元就是 1；1×0＝0，在乘法表中×号下的 1 所在的行与×号右边的 0 所在的列相交处的元是 0．

试验证上述加法、乘法都有交换律、结合律，且乘法对于加法有分配律．

＊3．设 R 是环．证明下述性质：$\forall\ a,b,c\in R$，

(1) $a+b=a$，则 $b=0$，　　(2) $-(a+b)=(-a)-b$，

(3) $-(a-b)=(-a)+b$，　　(4) $a-b=c$，则 $a=c+b$，

(5) $a0=0$,　　(6) $-(ab)=(-a)b=a(-b)$,

(7) $(-a)(-b)=ab$　　(8) $a(b-c)=ab-ac$.

4. R 是环,$a_1,a_2,\cdots,a_m,b_1,b_2,\cdots,b_n\in R$,则

$$\left(\sum_{i=1}^{m}a_i\right)\left(\sum_{j=1}^{n}b_j\right)=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j.$$

*5. R 是环,验证:对所有非负整数 m,n,$\forall\ a,b\in R$,有

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

若 a,b 交换,则 $(ab)^m=a^mb^m$.

*6. R 是环,$a,b\in R$,a,b 交换,证明二项定理:

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\cdots+\binom{n}{k}a^{n-k}b^k+\cdots+b^n,$$

其中

$$\binom{n}{k}=C_n^k=\frac{n(n-1)\cdots(n-k+1)}{1\cdot2\cdots k}$$

7. R 是环,$a_1,a_2,\cdots,a_m\in R$,分别有乘法逆元素 $a_1^{-1},\cdots,a_m^{-1}$,则 $a_1\cdots a_m$ 的逆元素为 $a_m^{-1}a_{m-1}^{-1}\cdots a_2^{-1}a_1^{-1}$.若 $a_1,\cdots,a_m$ 两两交换,则 $a_1a_2\cdots a_m$ 有逆元素的充要条件是 $a_1,\cdots,a_m$ 皆有逆元素.

8. R 是环,$a,b\in R$.证明

$c(1-ab)=(1-ab)c=1\Rightarrow(1-ba)d=d(1-ba)=1$,

其中 $d=1+bca$.即若 $1-ab$ 在 R 内可逆,则 $1-ba$ 也可逆.元素 $1+adb$ 等于什么?

9. $M_n(F)$为域 F 上全体 $n\times n$ 阵作成的环,$n\geqslant2$.举出其中零因子的例子.

习题答案与解答

1. (1) 否,(2)否,(3)是,(4)是.

2. 证明　由于 $a+b$ 和 $b+a$,$a+(b+c)$和$(a+b)+c$ 中 1,0 出现的次数分别相同,它们的和就分别相等,故 F_2 中加法交换律和结合律成立.

由于 ab 和 ba,$a(bc)$和$(ab)c$ 中如有 0 出现,其积为零,否则其积为 1,故这两对积分别相等,于是 F_2 中乘法交换律和结合律成立.

对 $a(b+c)$和 $ab+ac$,若 $a=0$,这两式子都为零;若 $a=1$,这两式子都为 $b+c$,对这两种情形两式子都相等,故 F_2 中乘法对加法的分配律成立.

3. (1) 对 $a+b=a=a+0$ 用加法消去律,得 $b=0$.

(2) 由于$[(-a)-b]+a+b=(-a)+[-b+(a+b)]=(-a)+a=0$,

由负元的定义知$(-a)-b=-(a+b)$.

(3)在(2)中将 b 换为 $-b$,就得 $-(a-b)=(-a)+b$.

(4)对 $a-b=c$ 两边加上 b,左边$=(a-b)+b=a$,右边$=c+b$,故 $a=c+b$.

(5) $a\cdot 0+a=a\cdot 0+a\cdot 1=a(0+1)=a$.用加法消去律得 $a\cdot 0=0$.

(6) $(-a)b+ab=(-a+a)b=0\cdot b=0$,故 $-ab=(-a)b$.将上式 a,b 互换就得 $-ab=a(-b)$.

(7) $(-a)(-b)=-(a(-b))=-(-ab)=ab$.

(8) $a(b-c)=a(b+(-c))=ab+a(-c)=ab-ac$.

4. $\sum_{i=1}^{m}a_i\sum_{j=1}^{n}b_j=(a_1+\cdots+a_m)\sum_{j=1}^{n}b_j=a_1\sum_{j=1}^{n}b_j+\cdots+a_m\sum_{j=1}^{n}b_j=\sum_{j=1}^{n}a_1b_j+\cdots+\sum_{j=1}^{n}a_mb_j=\sum_{i=1}^{m}\sum_{j=1}^{n}a_ib_j$.

5. 分几种情形

(i) $m+n=0$,但 m,n 不为零,不妨设 m 为正整数. a^ma^{-m} 为 m 个 a 及 m 个 a^{-1} 的乘积,由广义结合律知 $a^ma^{-m}=1=a^0=a^{m+(-m)}$.

(ii)若 m,n 中有零,不妨设 $m=0$,则左边$=a^{0+n}=a^n=a^0a^n=$右边.

(iii) m,n 皆为正整数,则 a^{m+n} 与 a^ma^n 皆为 $m+n$ 个 a 的积,由广义结合律知它们相等.

若 m,n 皆为负整数,则 a^{m+n} 与 a^ma^n 皆为 $-(m+n)$ 个 a^{-1} 的乘积,由广义结合律知它们相等.

(iv) m,n 中有正有负,且 $m+n\neq 0$,不妨设 m 与 $m+n$ 为异号.则由(iii) $a^{m+n}a^{-m}=a^{(m+n)-m}=a^n$,两边再乘上 $(a^{-m})^{-1}=a^m$(参看(i)),则 $a^{m+n}=a^ma^n$.

以上已证明了 $a^{m+n}=a^ma^n$ 及 $(a^m)^{-1}=a^{-m}$.

再由 $a^{mn}=a^{\overbrace{m+m+\cdots+m}^{n个}}=\overbrace{a^m\cdots a^m}^{n个}=(a^m)^n$,当 $n>0$;

$$a^{mn}=a^{(-m)(-n)}=a^{\overbrace{-m\cdots-m}^{(-n)个}}=\overbrace{a^{-m}\cdots a^{-m}}^{(-n)个}=\overbrace{(a^m)^{-1}\cdots(a^m)^{-1}}^{(-n)个}$$

$=(a^m)^n$,当 $n<0$;

又 $a^{m\cdot 0}=1=(a^m)^0$.

这就证明了 $a^{mn}=(a^m)^n$.

若 a,b 交换,当 $m=0$ 时,显然有 $a^mb^m=(ab)^m$.当 m 为正整数时,a^mb^m 与 $(ab)^m$ 都是 m 个 a,m 个 b 的乘积,由广义结合律知它们相等,当 m 为负整数时,$a^{-m}b^{-m}=(ab)^{-m}$,即 $(a^m)^{-1}(b^m)^{-1}=((ab)^m)^{-1}$.左边又是 $(a^mb^m)^{-1}$,

故 $a^m b^m=(ab)^m$.

6. 参照中学数学中对二项定理的证明.

7. 由$(a_1 a_2\cdots a_m)(a_m^{-1}a_{m-1}^{-1}\cdots a_2^{-1}a_1^{-1})=a_1 a_2\cdots a_{m-1}a_m a_m^{-1}a_{m-1}^{-1}\cdots a_1^{-1}=1$,故$(a_1 a_2\cdots a_m)^{-1}=a_m^{-1}\cdots a_2^{-1}a_1^{-1}$.

对第2个问题,上面一段正是证明了它的充分性.再证必要性.设 $a_1 a_2\cdots a_m\cdot u=1$,则任 i, $a_i(a_1\cdots a_{i-1}a_{i+1}\cdots a_m u)=1$,故每个 a_i 有逆元素.

8. $(1-ba)d=(1-ba)(1+bca)=1-ba+bca-babca=1-ba+b(1-ab)ca=1-ba+ba=1$,

$$d(1-ba)=(1+bca)(1-ba)=1-ba+bca-bcaba,$$
$$=1-ba+bc(1-ab)a=1-ba+ba=1.$$

即 $1-ba$ 在 R 内也可逆.

又由 $c(1-ab)=(1-ab)c=1$,得 $1+cab=1+abc=c$.故

$$1+adb=1+a(1+bca)b=1+ab+abcab=1+ab(1+cab)$$
$$=1+abc=c.$$

9. 当 $n\geqslant 2$ 时,取

$$A=\begin{pmatrix}1&1&0&\cdots&0\\0&0&0&\cdots&0\\\cdots&\cdots&\cdots&&\cdots\\0&0&0&\cdots&0\end{pmatrix}_{n\times n}\qquad B=\begin{pmatrix}1&0&\cdots&0\\-1&0&\cdots&0\\0&0&\cdots&0\\\cdots&\cdots&&\cdots\\0&0&\cdots&0\end{pmatrix}_{n\times n}$$

则 $A\neq 0$,$B\neq 0$,但 $AB=0$.A,B 皆为零因子.

第一章　群

内容要点

1．群的例子．

2．群的基本概念：群、子群、同态、同构、陪集、正规子群、商群、群阶、元的阶、群的方指数、循环群、交换群、奇(偶)置换、置换的轮换分解．

3．与群作用有关的概念：群作用及等价定义、轨道(等价类)、不变量及不变量的完全组、稳定子群、轨道长、共轭类．

4．重要结论：Lagrange 定理、Cayley 定理、类方程，群作为稳定子群的陪集的无交并、稳定子群的阶与轨道长的积等于群阶(有限群时)、同态基本定理、循环群及其子群的结构、有限交换群为循环群的充要条件、域中非零元的有限乘法子群是循环群、A_n($n\geqslant 5$)的单性、Burnside 关于轨道数的定理．

5．几个应用：图形的对称性群的计算(利用稳定子群)、晶体的对称性定律、轨道数的定理在一些组合计算问题中的应用．

6．解析几何、高等代数中有关群的例子、矩阵的各种变换与群作用的关系．

读后注

1．本章的一大特点也是本教材的一大特点是以群作用为主线来处理群论这一章的内容．在其它教材中群作用的概念和理论仅在群论的稍深入的部分出现．不少教材(例如为师范院校用的教材)甚至不涉及它．作者发现本章的内容(作为群论的引论内容)大量地与群作用有关：从图形的对称性群的分析引入群作用概念、用群作用的轨道引出陪集与共轭类的概念、Lagrange 定理和 Cayley 定理、群作用与高等代数中各种矩阵变换和几何学中的 Erlanger 纲领的联系、群作用的轨道长和稳定子群关系的结论用于推出类方程和化简图形的对称性群的计算、Burnside 关于轨道数的结论用于组合计算问题等基本上形成了本章内容从头到尾的一条主线．中间穿插着讲述了群的各个基本概念和基本性质．这样就体现了群作用的重要性．

2．读者还可进一步考察高等代数中与群和群作用有关的其它例子．本教材中将群作用与高等代数矩阵变换相联系，体现了用群作用的高观点去看待以前

的知识.

3. 任意域中非零元素的乘法有限子群是循环群.这是非常漂亮的结果,是群论结果的推论.它在有限域的结构中起重要作用.

4. 利用商群和同态基本定理可以搞清一些对象的构造和性质.读者可从教材内容和习题中举出几个例子来熟悉这种方法.

思考练习题(非必作题)

(1) 空间点阵绕一轴的转动若是它的对称性变换,则转角只有 $0,\pm\frac{\pi}{3},\pm\frac{\pi}{2},\pm\frac{2\pi}{3},\pi$.证明 只由这几个变换共能组五个群.

(2) 实对称 $n\times n$ 方阵可用正交矩阵作相似变换化为对角矩阵.这其中有什么群作用?试找出这个群作用下的不变量的完全组,给出两个 $n\times n$ 实对称方阵在同一轨道的充分必要条件.给出两个 $n\times n$ 实对称矩阵在一般的(不一定是正交矩阵下)相似变换下能够互变的充分必要条件.

§1 群的例子

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. 平面取定坐标系 Oxy,则平面仿射(点)变换 $\varphi:(x,y)^{\mathrm{T}}\longrightarrow(x',y')^{\mathrm{T}}$ (这里 T 是矩阵的转置,$(x,y)^{\mathrm{T}}$ 是一列的矩阵,即列向量)可写为

$$\begin{aligned} x'&=a_{11}x+a_{12}y+b_1,\\ y'&=a_{21}x+a_{22}y+b_2, \end{aligned}\tag{1}$$

其中行列式

$$\begin{vmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix}\neq 0.$$

证明平面上全体仿射变换对于变换的乘法成一个群,称为平面的仿射变换群.(可以把(1)写成矩阵形式,再进行证明).

*2. 平面上取定直角坐标系 Oxy,任意平面正交(点)变换 $\varphi:(x,y)^{\mathrm{T}}$ $(x',y')^{\mathrm{T}}$ 可写为

$$x' = a_{11}x + a_{12}y + b_1,$$
$$y' = a_{21}x + a_{22}y + b_2,$$

其中矩阵

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

是正交矩阵.用这种表示式证明平面上全体正交变换对于变换的乘法成为一个群,它是平面的正交变换群(见例 10).

*3. 平面上三个(不同的)点$(x_0, y_0)^T$,$(x_1, y_1)^T$,$(x_2, y_2)^T$(在习题 1 中同一坐标系 Oxy 下)共线当且仅当有实数 l,使$(x_2 - x_0, y_2 - y_0)^T = l(x_1 - x_0, y_1 - y_0)^T$.证明在习题 1 中的仿射变换 φ 下,有$(x'_2 - x'_0, y'_2 - y'_0)^T = l(x'_1 - x'_0, y'_1 - y'_0)^T$,故变换后的三点$(x'_0, y'_0)$,$(x'_1, y'_1)$,$(x'_2, y'_2)$也共线.

*4. 平面上二点$(x_1, y_1)^T$,$(x_2, y_2)^T$(在习题 2 中直角坐标系 Oxy 下)的距离为$|x_2 - x_1, y_2 - y_1| = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$.证明:在习题 2 中的正交变换 φ 下,变换前后两点的距离不变.注:只要证明$(x_2 - x_1)^2 + (y_2 - y_1)^2 = (x'_2 - x'_1)^2 + (y'_2 - y'_1)^2$.除直接计算外还可利用矩阵工具.实际上

$$\begin{pmatrix} x'_2 - x'_1 \\ y'_2 - y'_1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_2 - x_1 \\ y_2 - y_1 \end{pmatrix}.$$

又若把一个数看成 1×1 矩阵,则有

$$\begin{aligned} &(x_2 - x_1)^2 + (y_2 - y_1)^2 \\ &= (x_2 - x_1, y_2 - y_1)(x_2 - x_1, y_2 - y_1)^T \end{aligned}$$

及

$$\begin{aligned} &(x'_2 - x'_1)^2 + (y'_2 - y'_1)^2 \\ &= (x'_2 - x'_1, y'_2 - y'_1)(x'_2 - x'_1, y'_2 - y'_1)^T. \end{aligned}$$

5. 所有形为

$$\begin{matrix} a & b \\ 0 & a \end{matrix}$$

($a \neq 0$,a,b 皆为复数)的矩阵对于矩阵的乘法成为一个群.

*6. 令 G 是全部实数对(a, b),$a \neq 0$,的集合.在 G 上定义乘法为$(a, b)(c, d) = (ac, ad + b)$,$e = (1, 0)$,验证 G 是一个群.

*7. 设 G 是一个幺半群.若 G 的每个元 a 有右逆元,即有 $b \in G$,使 $ab = e$,则 G 是一个群.

*8. 设 G 是一个群.若 $\forall\, a, b$ 皆有$(ab)^2 = a^2 b^2$,则 G 是交换群.

9. 设群 G 的每个元素 a 都满足 $a^2 = e$,则 G 是交换群.

10. $G = \{z \in \mathbb{C}$(复数域)$\mid |z| = 1\}$对于复数的乘法成群.

11. $K=\left\{\begin{pmatrix}\alpha & \beta\\ -\beta & \bar{\alpha}\end{pmatrix}\middle|\ \alpha,\beta\in C\right.$，不同时为 0 ，其中 $\bar{\alpha},\beta$ 是 α,β 的共轭复数，则 K 在矩阵的乘法下成群.

12. 设 G 是非空的有限集合，G 上的乘法满足：$\forall\ a,b,c\in G$ 有

1）$(ab)c=a(bc)$；

2）$ab=ac\Rightarrow b=c$；

3）$ac=bc\Rightarrow a=b$；

则 G 是群.

*13. 证明(1)群中元 $a,a^2=e$ 当且仅当 $a=a^{-1}$.(2)偶数个元素的群都含有一个元 $a\neq e$，使得 $a^2=e$.

14. 证明任一个群 G 不能是两个不等于 G 的子群的并集.

15. 以 Q_p 记分母与某素数 p 互素的全体有理数组成的集合，证明它对于数的加法成为一个群.

16. 以 Q^p 记分母皆为 $p^i(i\geqslant 0,p$ 素数)的全体有理数的集合，证明它对数的加法成为群.

*17. 令

$$\rho=\begin{matrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{matrix},\quad \sigma=\begin{matrix}1&2&3&4&5&6\\2&3&1&5&6&4\end{matrix},$$

$$\tau=\begin{matrix}1&2&3&4&5&6\\6&2&1&3&5&4\end{matrix},$$

计算 $\rho\sigma,\sigma\tau,\tau\rho,\sigma^{-1},\sigma\rho\sigma^{-1}$.

*18. 设

$$\sigma=\begin{matrix}1&2&\cdots&n\\ \sigma(1)&\sigma(2)&\cdots&\sigma(n)\end{matrix},\quad \tau=\begin{matrix}1&2&\cdots&n\\ \tau(1)&\tau(2)&\cdots&\tau(n)\end{matrix}.$$

问

$$\sigma=\begin{matrix}\tau(1)&\tau(2)&\cdots&\tau(n)\\ ?&?&\cdots&?\end{matrix},\quad \tau^{-1}=\begin{pmatrix}?&?&\cdots&?\\ i_1&i_2&\cdots&i_n\end{pmatrix},$$

及

$$\tau\sigma\tau^{-1}=\begin{matrix}\sigma(1)&\sigma(2)&\cdots&\sigma(n)&1&2&\cdots&n&?&?&\cdots&?\\ ?&?&\cdots&?&\sigma(1)&\sigma(2)&\cdots&\sigma(n)&1&2&\cdots&n\end{matrix}$$

$$=?$$

*19. 将下列置换分解成不相交轮换的乘积：

$$\begin{matrix}1&2&3&4&5&6&7\\7&1&2&6&5&4&3\end{matrix},\qquad \begin{matrix}1&2&3&4&5&6&7&8&9&10\\2&4&5&9&7&10&8&3&1&6\end{matrix}.$$

然后再分解成对换的乘积，并说是奇或偶置换.

*20. 确定置换

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ n & (n-1) & \cdots & 2 & 1\end{pmatrix}$$

的奇偶性.

*21. 把(1 4 7)(7 8 10)(3 10 9)(9 4 2)(3 5 6)分解成不相交的轮换的乘积.

习题答案与解答

1. 写仿射点变换 $\varphi:(x,y)^{\mathrm{T}}\longmapsto(x',y')^{\mathrm{T}}$(这儿 T 是矩阵的转置)为矩阵形式

$$\begin{pmatrix}x'\\ y'\end{pmatrix}=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}+\begin{pmatrix}b_1\\ b_2\end{pmatrix}=A\begin{pmatrix}x\\ y\end{pmatrix}+\begin{pmatrix}b_1\\ b_2\end{pmatrix},$$

其中

$$|A|=\begin{vmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix}\neq 0.$$

设另一仿射点变换 ρ:

$$\begin{matrix}x'\\ y'\end{matrix}=B\begin{matrix}x\\ y\end{matrix}+\begin{pmatrix}c_1\\ c_2\end{pmatrix}$$

其中 $|B|\neq 0$.则 $(x,y)^{\mathrm{T}}$ 经 $\rho\varphi$ 变成

$$\rho\varphi\begin{matrix}x\\ y\end{matrix}=\rho\ \varphi\begin{matrix}x\\ y\end{matrix}=\rho\left(A\begin{matrix}x\\ y\end{matrix}+\begin{pmatrix}b_1\\ b_2\end{pmatrix}\right)=B\left(A\begin{matrix}x\\ y\end{matrix}+\begin{pmatrix}b_1\\ b_2\end{pmatrix}\right)+\begin{pmatrix}c_1\\ c_2\end{pmatrix}.$$

$$=BA\begin{matrix}x\\ y\end{matrix}+\left(B\begin{pmatrix}b_1\\ b_2\end{pmatrix}+\begin{pmatrix}c_1\\ c_2\end{pmatrix}\right).$$

由于 $|BA|=|B||A|\neq 0$,$\rho\varphi$ 仍是仿射点变换.

易证:仿射点变换 φ_1:

$$\begin{matrix}x'\\ y'\end{matrix}=A^{-1}\left(\begin{matrix}x\\ y\end{matrix}-\begin{pmatrix}b_1\\ b_2\end{pmatrix}\right)$$

正是 φ 的逆变换.而仿射点变换

$$\begin{matrix}x'\\ y'\end{matrix}=\begin{matrix}x\\ y\end{matrix}=\begin{matrix}1 & 0 & x\\ 0 & 1 & y\end{matrix}+\begin{matrix}0\\ 0\end{matrix}$$

是恒等变换,它是乘法单位元,又变换的乘法自然有结合律.故平面上全体仿射点变换对变换的乘法成为一个群.

2. 平面上正交点变换 φ 可写成矩阵形式

$$\begin{matrix}x'\\ y'\end{matrix}=A\begin{matrix}x\\ y\end{matrix}+\begin{pmatrix}b_1\\ b_2\end{pmatrix},$$

其中 A 为 2×2 正交矩阵，即满足 $AA^{\mathrm{T}}=A^{\mathrm{T}}A=I$（单位矩阵）.

正交矩阵的乘积是正交矩阵，正交矩阵的逆也是正交阵.利用这两个性质，完全类似于习题 1 中的论证，能证明本习题的结论.

3. 由题设有

$$\begin{pmatrix}x_2-x_0\\y_2-y_0\end{pmatrix}=l\begin{pmatrix}x_1-x_0\\y_1-y_0\end{pmatrix}.$$

在仿射点变换 φ：

$$\begin{matrix}x'\\y'\end{matrix}=A\begin{matrix}x\\y\end{matrix}+\begin{pmatrix}b_1\\b_2\end{pmatrix}$$

的变换下

$$\begin{pmatrix}x_i'\\y_i'\end{pmatrix}=A\begin{pmatrix}x_i\\y_i\end{pmatrix}+\begin{pmatrix}b_1\\b_2\end{pmatrix},\quad i=0,1,2.$$

故

$$\begin{pmatrix}x_2'-x_0'\\y_2'-y_0'\end{pmatrix}=\begin{pmatrix}x_2'\\y_2'\end{pmatrix}-\begin{pmatrix}x_0'\\y_0'\end{pmatrix}=A\begin{pmatrix}x_2\\y_2\end{pmatrix}-A\begin{pmatrix}x_0\\y_0\end{pmatrix}=A\begin{pmatrix}x_2-x_0\\y_2-y_0\end{pmatrix}$$

$$=A\left(l\begin{pmatrix}x_1-x_0\\y_1-y_0\end{pmatrix}\right)=lA\begin{pmatrix}x_1-x_0\\y_1-y_0\end{pmatrix}=l\begin{pmatrix}x_1'-x_0'\\y_1'-y_0'\end{pmatrix}.$$

由于 $|A|\neq0$，A 可逆.于是 φ 将不同的三点 $(x_i,y_i)^{\mathrm{T}}$ 变成不同的三点 $(x_i',y_i')^{\mathrm{T}}$，$i=0,1,2$.上面一串等式的最前端与最后端相等即表示这三点也共线.

4. 与第三题类似有

$$\begin{pmatrix}x_2'-x_1'\\y_2'-y_1'\end{pmatrix}=A\begin{pmatrix}x_2-x_1\\y_2-y_1\end{pmatrix}$$

其中 A 满足 $AA^{\mathrm{T}}=A^{\mathrm{T}}A=I$.

于是

$$(x_2'-x_1')^2+(y_2'-y_1')^2=(x_2'-x_1',y_2'-y_1')\begin{pmatrix}x_2'-x_1'\\y_2'-y_1'\end{pmatrix}$$

$$=A\begin{pmatrix}x_2-x_1\\y_2-y_1\end{pmatrix}^{\mathrm{T}}A\begin{pmatrix}x_2-x_1\\y_2-y_1\end{pmatrix}=(x_2-x_1,y_2-y_1)A^{\mathrm{T}}A\begin{pmatrix}x_2-x_1\\y_2-y_1\end{pmatrix}$$

$$=(x_2-x_1,y_2-y_1)\begin{pmatrix}x_2-x_1\\y_2-y_1\end{pmatrix}=(x_2-x_1)^2+(y_2-y_1)^2.$$

5. 略.

6. 略.

7. 对 $a\in G$，a 有右逆 b. b 又有右逆 a'，这时 a 为 b 的左逆. 由 $ba'=e=ab$，得到

$$a=a(ba')=(ab)a'=a',$$

可知 $a=a'$. 这样 $ba=ab=e$，即 b 是 a 的逆.

8. 由题设，$\forall\ a,b\in G$，$(ab)^2=abab=a^2b^2$. 对后一等号两边左乘 a^{-1}，右乘 b^{-1}，就得到 $ab=ba$.

9. $\forall\ a,b\in G$，有 $a^2=b^2=e$，故 $a^{-1}=a$，$b^{-1}=b$，又 $(ab)^2=abab=e$. 对后一个等号两边左乘 a，右乘 b，就得 $ba=ab$.

10. 略.

11. 略.

12. 设 $G=\{g_1,\cdots,g_s\}$. 由性质(2)，$\forall\ a\in G$，$\{ag_1,\cdots,ag_s\}\subseteq G$，且是 s 个不同的元，故 $\{ag_1,\cdots,ag_s\}=G$. 同样由性质(3)可得，$\{g_1a,\cdots,g_sa\}=G$. 设其中 $ag_i=a$，$g_ja=a$. 于是 $(g_1a)g_i=g_1a,\cdots,(g_sa)g_i=g_sa$；$g_j(ag_1)=ag_1,\cdots,g_j(ag_s)=ag_s$. 即 g_i 是 G 的右单位元，g_j 是 G 的左单位元，分别记为 e 及 e'，则 $e=e'e=e'$，即 G 有单位元 e.

类似于上面作法，由 $\{ag_1,\cdots,ag_s\}=G$，有 $b\in G$ 使 $ab=e$，由 $\{g_1a,\cdots,g_sa\}=G$，而有 $b'\in G$ 使 $b'a=e$. 于是 $b'=b'e=b'(ab)=(b'a)b=eb=b$，即 $\forall\ a\in G$ 有逆元. 又题设 G 有结合律，故是一个群.

13. 只证(2). 用反证法. 设 $\forall\ a\in G$，$a\neq e$ 有 $a^2\neq e$. 由(1)知 $a\neq a^{-1}$.

取 $a_1\in G\setminus\{e\}$，则 $a_1\neq a_1^{-1}\neq e$. 若 $G\setminus\{e\}$ 除了 $\{a_1,a_1^{-1}\}$ 外还有元素 a_2，于是 $a_2\neq a_2^{-1}$. 由于 a_1,a_1^{-1} 互为逆元素，若 $a_2^{-1}\in\{a_1,a_1^{-1}\}$ 则 $a_2=(a_2^{-1})^{-1}\in\{a_1,a_1^{-1}\}$. 这不可能，即 $a_2^{-1}\overline{\in}\{a_1,a_1^{-1}\}$. 故 $\{a_1,a_1^{-1},a_2,a_2^{-1}\}$ 是四个不同的元素. 设上面的步骤进行了 $k-1$ 步，得到 $2(k-1)$ 个元素 $\{a_1,a_1^{-1},\cdots,a_{k-1},a_{k-1}^{-1}\}\subseteq G\setminus\{e\}$. 同样论证 $G\setminus\{e\}$ 除了上述 $2(k-1)$ 个元素外要么没有元素了，要么同时有 a_k 及 a_k^{-1} 且 $a_k\neq a_k^{-1}$. 可知 $G\setminus\{e\}$ 要么等于 $\{a_1,a_1^{-1},\cdots,a_{k-1},a_{k-1}^{-1}\}$，要么有 $2k$ 个元素 $\{a_1,a_1^{-1},\cdots,a_k,a_k^{-1}\}\subseteq G\setminus\{e\}$. 因 $G\setminus\{e\}$ 只有有限个元素，必然在某个第 k 步停止，即 $G\setminus\{e\}=\{a_1,a_1^{-1},\cdots,a_k,a_k^{-1}\}$. 故 G 有 $2k+1$ 个，即奇数个元素，矛盾. 因此 G 中必有元素 $a\neq e$，$a^2=e$.

14. 设 G_1,G_2 皆为不等于 G 的子群，但 $G=G_1\cup G_2$. 因 $G_1\neq G$，可取到 $g_1\overline{\in}G_1$. 由 $G=G_1\cup G_2$，$g_1\in G_2$. 同样能取到 $g_2\overline{\in}G_2$，但 $g_2\in G_1$. 作 $g=g_1\cdot g_2$. 若 $g\in G_1$，因 $g_2\in G_1$，则 $g_1=g\cdot g_2^{-1}\in G_1$ 矛盾. 于是 $g\overline{\in}G_1$，同样 $g\overline{\in}G_2$，就得到 $g\overline{\in}G_1\cup G_2$ 与 $G=G_1\cup G_2$ 矛盾. 故不能有不等于 G 的两个子群 G_1,G_2 使得 $G=G_1\cup G_2$.

15. 略.

16. 略.

17. 略.

18. $\sigma=\begin{pmatrix}\tau(1) & \tau(2) & \cdots & \tau(n)\\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n))\end{pmatrix}$, $\tau^{-1}=\begin{pmatrix}\tau(i_1) & \tau(i_2) & \cdots & \tau(i_n)\\ i_1 & i_2 & & i_n\end{pmatrix}$

$\tau\sigma\tau^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \tau(\sigma(1)) & \tau(\sigma(2)) & \cdots & \tau(\sigma(n))\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}\begin{pmatrix}\tau(1) & \tau(2) & \cdots & \tau(n)\\ 1 & 2 & \cdots & n\end{pmatrix}$

$=\begin{pmatrix}\tau(1) & \tau(2) & \cdots & \tau(n)\\ \tau(\sigma(1)) & \tau(\sigma(2)) & \cdots & \tau(\sigma(n))\end{pmatrix}$.

19. 略.

20. 略.

21. 略.

§2 对称性变换与对称性群,晶体对称性定律

习 题

下列习题中打 * 者为必作题,其它为选作题.

*1. 计算下列图形的对称性群:

(1) 正五边形;

(2) 不等边矩形;

(3) 圆.

*2. 用 S_4 的全部变换去变 $x_1x_2+x_3x_4$,把变到的所有可能的多项式写出来.

*3. 用 S_3 去变 $x_1^3x_2^2x_3$ 能变出几个多项式,把它们全写出来.以 $x_1^3x_2^2x_3$ 为其中一项作出一个和,使它是对称多项式,并使其项数最少.

*4. 用不相交的轮换的乘积的形式写出 S_3, A_3, S_4, A_4 中的全部元素.

*5. S_4 中下列 4 个元素的集合

$$\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$

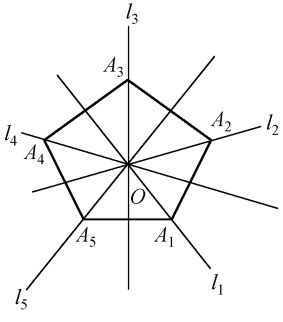
在置换乘法下成为一个群,记为 V_4.并且它是 A_4 的子群.

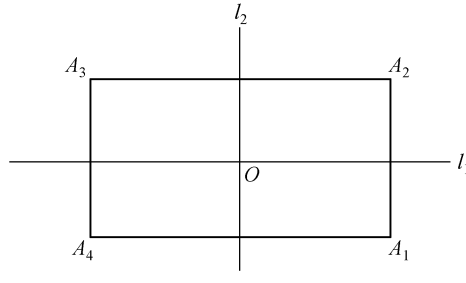
6. 求出正四面体 $A_1A_2A_3A_4$ 的对称性群.

习题答案与解答

1. (1) 令绕 O 反时针旋转 0°,72°,144°,216°,288°的 5 个旋转变换为 T_0,

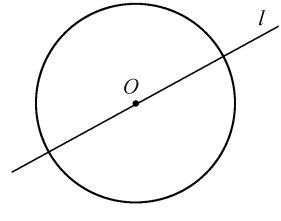
T_1，T_2，T_3，T_4，令平面对直线 l_1，l_2，l_3，l_4，l_5，的反射变换为 S_1，S_2，S_3，S_4，S_5，它们都是对称性变换.对于此正五边形的任一个对称性变换 T，它若将顶点 A_1 变成 A_i，则 $T_{i-1}^{-1}T$ 就将 A_1 变成 A_1.易知正五边形的保持 A_1 不动的对称性变换只有 T_0 和 S_1，即 $T_{i-1}^{-1}T=T_0$ 或 S_1，故 $T=T_{i-1}T_0=T_{i-1}$ 或 $T=T_{i-1}S_1$.故全部对称性变换为$\{T_{i-1}S_1, T_{i-1}, i=1,2,\cdots,5\}$，最多有 10 个元素.而前面已列出$\{T_{i-1}, S_i, i=1,2,3,4,5\}$共 10 个对称性变换，它们必须相等.





(2) 令绕 O 反时针旋转 0°，180°的旋转变换为 T_0，T_1，令平面对直线 l_1，l_2 的反射为 S_1，S_2.它们都是该矩形的对称性变换.使 A_1 分别变到 A_1，A_2，A_3，A_4 的对称性变换都只有一个，即分别为 T_0，S_1，T_1，S_2.故它们是全部的对称性变换.

(3) 令绕 O 反时针旋转任意角 θ 的旋转变换为 T_θ，令平面对过中心 O 的任意直线 l 的反射为 S_l.则圆的对称性变换群＝$\{T_\theta, 0\leqslant\theta<360°, S_l$，全部过中心 O 的直线 $l\}$



2. $x_1x_2+x_3x_4$，$x_1x_3+x_2x_4$，$x_1x_4+x_2x_3$.

3. 能变出 6 个单项式，即为：$x_1^3x_2^2x_3$，$x_1^2x_2^3x_3$，$x_1^3x_3^2x_2$，$x_1^2x_3^3x_2$，$x_2^3x_3^2x_1$，$x_2^2x_3^3x_1$.它们的和

$$x_1^3x_2^2x_3+x_1^2x_2^3x_3+x_1^3x_3^2x_2+x_1^2x_3^3x_2+x_2^3x_3^2x_1+x_2^2x_3^3x_1$$

是所要求的项数最少的多项式.

4. $S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$

$A_3=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$

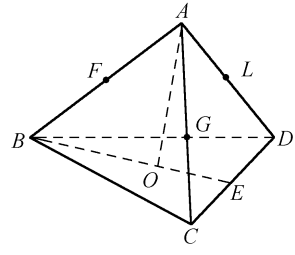
$S_4=\{(1),(1\ 2),(1\ 3),(1\ 4),(2\ 3),(2\ 4),(3\ 4),(1\ 2\ 3),(1\ 3\ 2),$
$(1\ 2\ 4),(1\ 4\ 2),(1\ 3\ 4),(1\ 4\ 3),(2\ 3\ 4),(2\ 4\ 3),$
$(1\ 2)(3\ 4),(1\ 4)(2\ 3),(1\ 3)(2\ 4),(1\ 2\ 3\ 4),(1\ 2\ 4\ 3),$
$(1\ 3\ 2\ 4),(1\ 3\ 4\ 2),(1\ 4\ 2\ 3),(1\ 4\ 3\ 2)\}$

$A_4=\{(1),(1\ 2\ 3),(1\ 3\ 2),(1\ 2\ 4),(1\ 4\ 2),(1\ 3\ 4)$

(1 4 3),(2 3 4),(2 4 3),(1 2)(3 4),(1 4)(2 3),(1 3)(2 4)}.

5. 略.

6. 正四面体为 $ABCD$,O 为△DBC 的中心,E,F,G,L 分别是 CD,AB,AC,AD 的中点,我们先找出使顶点 A 不动的全体对称性变换的集合 H.这些变换使△BCD 变为自己,H 限制在平面 BCD 上是△BCD 的对称性群.由此易确定出 $H=\{T_i, T_iS, i=1,2,3\}$,其中 T_1,T_2,T_3 是空间绕轴 AO 旋转(按某固定方向)转 0°,120°,240°的旋转变换,S 是空间对平面 ABE 的镜面反射.



再任选三个对称性变换 M_1,M_2,M_3,它们分别能将点 B,C,D 与 A 互变.例可取 M_1,M_2,M_3 是空间分别对平面 CDF,BGD,CBL 的镜面反射.与第 1 题(1)中的论证类似,可得正四面体 $ABCD$ 的对称性群 $G=\{T_i, T_iS, M_jT_i, M_jT_iS, i,j=1,2,3\}$.$G$ 有 24 个元.

§3 子群,同构,同态

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. 四个复数 1,−1,i,−i 的集合 U_4 构成非零复数的乘法群的子群.

*2. H_1,H_2,…,H_k,…都是群 G 的子群.证明

(1) $H_1 \cap H_2$ 是子群.

(2) $\bigcap_{i=1}^{\infty} H_i$ 是子群.

(3) 若 $H_1 \subset H_2 \subset \cdots \subset H_k \subset H_{k+1} \subset \cdots$,则 $\bigcup_{i=1}^{\infty} H_i$ 是子群.

*3. 设 G 是群.令 $Z(G)=\{a \in G \mid ag=ga, \forall\, g \in G\}$,则 $Z(G)$ 是 G 的子群.称为 G 的中心.

*4. G 是群,S 是 G 的非空子集.令

$$C_G(S)=\{a \in G \mid as=sa, \forall\, s \in S\},$$

$$N_G(S)=\{a \in G \mid aSa^{-1}=S\},$$

则它们都是 G 的子群,其中 $aSa^{-1}=\{asa^{-1} \mid \forall\, s \in S\}$.$C_G(S)$ 和 $N_G(S)$ 分别称

为 S 在 G 中的中心化子和正规化子.

5. 设 G 是群,H 是 G 的子群.(1)$a\in G$,则 aHa^{-1} 也是子群.(2)τ 是 G 的自同构,则 $\tau(H)$ 也是子群.

6. 证明§2 中习题 5 中 V_4 与上面习题 1 中 U_4 不同构.

*7. 证明正三角形 $A_1A_2A_3$ 的对称性群与 S_3 同构(将每个对称性变换与它引起的顶点的置换相对应).

8. 令

$$L=\left\{\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\middle|\ 0\leqslant\theta<2\pi\right\},\ M=\left\{\begin{pmatrix}e^{i\theta} & 0\\ 0 & e^{-i\theta}\end{pmatrix}\middle|\ 0\leqslant\theta<2\pi\right\}.$$

它们都在矩阵的乘法下成为群,并且相互同构.

9. 证明群 G 是交换群当且仅当映射

$$\begin{array}{ccc} G & & G\\ x & \longmapsto & x^{-1}\end{array}$$

是 G 的自同构.

10. 实数域R到习题 8 中群 L 的映射 φ:

$$\begin{array}{ccc} \mathrm{R} & & L\\ x & \longmapsto & \begin{matrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{matrix}\end{array},$$

其中 $x=2k\pi+\theta$,$0\leqslant\theta<2\pi$,是R的加群到群 L 的同态.

11. G 是群,S 是 G 的非空子集.令

$$H=\{t_1\cdots t_i\cdots t_k\mid\forall\ k\text{ 是正整数},t_i\text{ 或 }t_i^{-1}\in S\}.$$

证明 H 是子群且 $H=\langle S\rangle$.

*12. 整数加法群Z的子群一定是某个 $n\mathbb{Z}$($n\in\mathbb{Z}$).

13. 证明有理数加法群Q的任何有限生成的子群是循环群.

14. $G=${全体 2×2 整数元素的可逆矩阵},对矩阵乘法是否成为群?全体正实数元素的 2×2 可逆矩阵对矩阵乘法是否成为群?

*15. 群 G 的全部自同构在 G 上变换的乘法下成为群,称为 G 的自同构群,记为 Aut G.

习题答案与解答

1. 略.

2. (1)略.

(2)对 $a,b\in\bigcap\limits_{i=1}^{\infty}H_i$ 来证 $ab^{-1}\in\bigcap\limits_{i=1}^{\infty}H_i$.因 $a,b\in H_i$,H_i 是子群,故 $ab^{-1}\in$

H_i，$i=1,2,\cdots$，于是 $ab^{-1}\in\bigcap_{i=1}^{\infty}H_i$．故 $\bigcap_{i=1}^{\infty}H_i$ 是子群．

(3) 设 $a,b\in\bigcup_{i=1}^{\infty}H_i$，必有 k,l 使 $a\in H_k$，$b\in H_l$．不妨设 $k\leqslant l$．于是由 $H_k\subseteq H_l$ 得 $a,b\in H_l$，又 H_l 是子群，知 $ab^{-1}\in H_l\subseteq\bigcup_{i=1}^{\infty}H_i$．故 $\bigcup_{i=1}^{\infty}H_i$ 是子群．

3．略．

4．略．

5．略．

6．写 V_4 中的元为 a,b,c,e(单位元)，则有 $a^2=b^2=c^2=e$．而 U_4 中 4 个元为 $1,-1,i,-i$．假设 V_4 到 U_4 有同构 τ．不妨设 $\tau(a)=i$．由 $a^2=e$，$\tau(a^2)=\tau(e)=1$．但 $\tau(a)=i$，$i^2=-1$，$\tau(a)\tau(a)=-1$．故 $\tau(a^2)\neq\tau(a)\tau(a)$，$\tau$ 不保持乘法，矛盾．故 V_4 与 U_4 不同构．

7．§2 例 3 中已计算过正三角形$\triangle A_1A_2A_3$ 的对称性群 G 有 6 个元素．每个对称性变换引起顶点 A_1,A_2,A_3 的一个置换．这就引起了 G 到 S_3 的一个映射．易检验这 6 个变换引起 S_3 的全部 6 个不同的置换．故这映射是双射．又连续两次作对称性变换引起连续两次顶点的置换．即对称性变换的乘积引起对应的顶点置换的乘积，故这映射保持乘法．因此上述映射是对称性变换群 G 到 S_3 的同构．

8．略．

9．略．

10．略．

11．$\forall\ t_1\cdots t_k,x_1\cdots x_l\in H$，$t_i,x_i$ 或 $t_i^{-1},x_i^{-1}\in S$，则$(t_1\cdots t_k)(x_1\cdots x_l)^{-1}=t_1\cdots t_kx_l^{-1}\cdots x_{l-1}^{-1}\cdots x_1^{-1}$，其中 t_i 或 t_i^{-1}，x_i^{-1} 或$(x_i^{-1})^{-1}=x_i$ 都属于 S，故$(t_1\cdots t_k)(x_1\cdots x_l)^{-1}\in H$，即 H 是子群．

又设 H_1 是 G 的包含 S 的子群，则必含所有形为 $t_1\cdots t_k$ 的元素，其中 t_i 或 $t_i^{-1}\in S$，故 $H_1\supseteq H$，因而 H 是包含 S 的最小的子群．

12．设 H 是加法群Z 的子群，若 $H\neq0\cdot\mathbb{Z}$，则 H 中有非零整数 t．若 $t<0$，H 是子群，H 含 $-t$，它是正整数．故 H 中有正整数．取 n 为 H 中最小的正整数．任 $m\in H$，作除法算式，$m=nq+r$，其中 $r=0$ 或 $0<r<n$．但 $r=m-nq\in H$，若 $r\neq0$ 则与 n 的最小性矛盾．故 $r=0$，$m=nq$，即 $H\subseteq n\mathbb{Z}$．又 $n\in H$，$\forall\ l\in\mathbb{Z}$，$ln=\underbrace{n+\cdots+n}_{l\text{个}}$或 $ln=\underbrace{(-n)+\cdots+(-n)}_{-l\text{个}}\in H$，即有 $n\mathbb{Z}\subseteq H$．因此 $H=n\mathbb{Z}$．

13．设 $H=\left\langle\frac{q_1}{p_1},\cdots,\frac{q_s}{p_s}\right\rangle$是Q 的有限生成的加法子群．由第 12 题易知 $H=$

$\left\{\sum_{i=1}^{s} l_i \frac{q_i}{p_i} \middle| l_i \in \mathbf{Z}\right\}$. 取 $p_1, \cdots, p_s$ 的最小公倍数为 m, 则 $\frac{q_i}{p_i} = \frac{\frac{m}{p_i} q_i}{m}$, 令为 $\frac{Q_i}{m}$. 再令 $(Q_1, \cdots, Q_s) = n$, 则 $\frac{q_i}{p_i} = \frac{Q_i}{m} = \frac{n}{m}\left(\frac{Q_i}{n}\right)$, 令为 $\frac{n}{m} t_i$. 则 $(t_1, t_2, \cdots, t_s) = 1$. 取 $k_1, \cdots, k_s \in \mathbf{Z}$, 使 $k_1 t_1 + \cdots + k_s t_s = 1$. 于是 $\sum_{i=1}^{s} k_i \frac{n}{m} t_i = \frac{n}{m} \sum_{i=1}^{s} k_i t_i = \frac{n}{m} \in H$, 且任意 $\sum_{i=1}^{s} l_i \frac{q_i}{p_i} = \sum_{i=1}^{s} l_i t_i \frac{n}{m} = \frac{n}{m} \sum_{i=1}^{s} l_i t_i$. 这就证明了 $H = \left\langle \frac{n}{m} \right\rangle$ 是循环加法群.

14. $\begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$, $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}^{-1} = \frac{1}{2} \begin{matrix} 1 & 1 \\ -1 & 1 \end{matrix}$, 即 $\begin{matrix} 1 & -1 \\ 1 & 1 \end{matrix}^{-1}$ 不是整数矩阵, 故全体 2×2 整数元素的可逆矩阵不成为群.

取正实数矩阵

$$\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}, \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}^{-1} = \begin{matrix} 1 & -1 \\ 0 & 1 \end{matrix},$$

即正实数可逆矩阵的逆矩阵不是正实数矩阵. 故全体 2×2 正实数可逆矩阵不成为群.

15. 略.

§4 群在集合上的作用, 定义与例子

习 题

以下习题中打 * 者为必作题, 其余为选作题.

*1. V 是某域 F 上 n 维线性空间, $G = GL(V)$ 是 V 上全线性变换群. 令 M 为 V 的全部子空间的集合. 证明 G 在 M 上有群作用.

*2. G 是群. K, H 是 G 的子群. 作群直积 $K \times H$. 定义映射 $\circ$:

$$(K \times H) \times G \qquad G$$
$$((k, h), g) \longmapsto (k, h) \circ g = kgh^{-1}.$$

证明它是群 $K \times H$ 在集合 G 上的作用.

3. G 是正四面体 $A_1 A_2 A_3 A_4$ 的对称性群. 令 $M_1 = \{$四面体的顶点的集合$\}$, $M_2 = \{$四面体的四个面的集合$\}$, $M_3 = \{$四面体的六条棱的集合$\}$, 则 G 在 M_1, M_2, M_3 上分别有群作用.

*4. 令 G 是 $n \times n$ 实正交矩阵的群, M 是 $n \times n$ 实对称矩阵的集合. 证明下

述对应是一个映射

$$G\times M \qquad M$$
$$(P,A)\longmapsto P\circ A=PAP^{-1},$$

且是 G 在 M 上的群作用.

*5. 写域 F 上多项式 $f(x,y,z)=f(\boldsymbol{r})$,其中 $\boldsymbol{r}=(x,y,z)^{\mathrm{T}}$,取 M 为 F 上 x,y,z 的全部多项式的集合.G 为群 $GL_3(F)$.对 $A\in G$,令 $\boldsymbol{r}'=(x',y',z')^{\mathrm{T}}=A(x,y,z)^{\mathrm{T}}=A\boldsymbol{r}$.证明下述对应

$$(A,f)\longmapsto A\circ f=f(\boldsymbol{r}')=f(A\boldsymbol{r})$$

是 $G\times M \qquad M$ 的一个映射,且是 G 在 M 上的群作用.

6. 利用 Cayley 定理证明具有给定阶 n 的不同构的有限群只有有限个.

习题答案与解答

1. 略

2. (1)$K\times H$ 的单位元是(e,e),其中 e 是 G 的,也是 K 和 H 的单位元.$\forall g\in G$,$(e,e)\circ g=ege^{-1}=g$.

(2) $\forall k_1,k_2\in K$,$h_1,h_2\in H$,(k_1,h_1),$(k_2,h_2)\in K\times H$.$\forall g\in G$,$(k_1,h_1)\circ((k_2,h_2)\circ g)=(k_1,h_1)\circ(k_2 gh_2^{-1})=k_1k_2 gh_2^{-1}h_1^{-1}=(k_1k_2)g(h_1h_2)^{-1}=(k_1k_2,h_1h_2)\circ g=((k_1,h_1)(k_2,h_2))\circ g$.

由定义 $1'$,上面映射"$\circ$"是 $K\times H$ 在 G 上的群作用.

3. 略.

4. 首先证明

$$(P,A)\longmapsto P\circ A=PAP^{-1}$$

定义了 $G\times M$ 到 M 的映射.$\forall P\in G$,P 是 $n\times n$ 正交矩阵,故 $P^{-1}=P'$,对 $\forall A\in M$,A 是 $n\times n$ 实对称阵,有 $P\circ A=PAP^{-1}=PAP'$,是 $n\times n$ 实对称阵,故 $P\circ A\in M$,确定了 $G\times M$ 到 M 的映射.

易证这映射是 G 在 M 上的一个群作用.

5. 对 $A\in G=GL_3(F)$,$\forall f(\boldsymbol{r})$是 F 上 x,y,z 的多项式,$A\circ f=f(A\boldsymbol{r})$,$A\boldsymbol{r}=(x',y',z')^{T}$ 中 x',y',z'都是 x,y,z 的一次多项式,若设为

$$x'=a_{11}x+a_{12}y+a_{13}z$$
$$y'=a_{21}x+a_{22}y+a_{23}z$$
$$z'=a_{31}x+a_{32}y+a_{33}z,$$

其中 $a_{ij}\in F$.则 $f(A\boldsymbol{r})=f(x',y',z')=f(a_{11}x+a_{12}y+a_{13}z,a_{21}x+a_{22}y+a_{23}z,a_{31}x+a_{32}y+a_{33}z)$仍是 F 上 x,y,z 的多项式,故

$$(A,f)\longmapsto A\circ f=f(A\boldsymbol{r})$$

建立了 $G\times M$ M 的一个映射,易证它是 G 在 M 上的群作用.

6. Cayley 定理断言,有限群 G 同构于 G 上的变换群.设 G 的阶为 n,则 G 同构于 S_n 的子群.而 S_n 的子群只有限个,故只有有限个不同构的 n 阶群.

§5 群作用的轨道与不变量、集合上的等价关系

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. §4 习题 1 中的群作用有几条轨道?找出群作用的不变量与不变量的完全组.

*2. 找出 §4 习题 4 中群作用的不变量和不变量的完全组.

*3. (联系 §4 习题 2 中的群作用)令 $t\in G$,称 $KtH=\{kth\mid k\in K,h\in H\}$ 为 G 的一个 (K,H) 双陪集,则 G 的两个 (K,H) 双陪集或重合或不相交,且 G 是全部 (K,H) 双陪集的无交并.

习题答案与解答

1. V 中可逆线性变换若把某子空间 W 变成子空间 W_1,则把 W 的基变成 W_1 的基,故同一轨道上的子空间具有相同的维数,又设 V 的两个子空间 W 和 W_1,它们有同样维数 $k>0$,分别取 W 和 W_1 的基为 $\varepsilon_1,\cdots,\varepsilon_k;\varepsilon'_1,\cdots,\varepsilon'_k$.分别补充成 $\varepsilon_1\cdots\varepsilon_k\cdots\varepsilon_n;\varepsilon'_1\cdots\varepsilon'_k\cdots\varepsilon'_n$,使它们都是 V 的基.由线性代数知道必有 V 上可逆线性变换 $\boldsymbol{A}$,使 $\boldsymbol{A}\varepsilon_i=\varepsilon'_i$,$i=1,2,\cdots,n$.$\boldsymbol{A}$ 就将子空间 W 变成子空间 W_1.故 W 与 W_1 在同一条轨道上.

故对 $k=0,1,2,\cdots,n$,V 中全体 k 维子空间的集合 V_k 构成群作用的一条轨道.共有 $n+1$ 条轨道.子空间的维数是不变量,并构成不变量的完全组.

2. 对 A,B 皆为 $n\times n$ 实对称矩阵,若 A,B 在同一轨道上,即有 $n\times n$ 正交阵 P 使 $B=PAP^{-1}$,则它们有相同的特征值集合.反之,设 A,B 为具有相同特征值集合 $\{\lambda_1,\cdots,\lambda_n\}$($\lambda_i$ 是 k 重特征值就在集合中出现 k 次)的 $n\times n$ 实对称矩阵,它们都可用实正交矩阵化为对角阵,即有 $n\times n$ 正交阵 P_1,P_2 使

$$P_1 A P_1^{-1}=\begin{pmatrix}\lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n\end{pmatrix}= P_2 B P_2^{-1}.$$

于是$(P_2^{-1}P_1)A(P_2^{-1}P_1)^{-1}=B$，$P_2^{-1}P_1$仍为正交阵，故$A$，$B$在同一条轨道上.

以上说明，特征值的集合是群作用的不变量的完全组.而全部特征值的和，全部特征值的积，特征多项式都是群作用的不变量.

3. 实际上KtH是§4习题2中群作用下的一条轨道，两条轨道或重合或不相交，即两个(K,H)双陪集或重合或不相交，群作用集G是全体轨道的无交并也就是全体(K,H)双陪集的无交并.

§6 陪集，Lagrange定理，稳定化子，轨道长

习 题

以下习题中打＊者为必作题，其余为选作题.

＊1. G是群，H是G的子群.$x,y\in G$，则x，y属于H的同一左陪集当且仅当$x^{-1}y\in H$.

＊2. 群G作用于集合M上，$x\in M$.证明：(1)稳定化子$\mathrm{Stab}_G(x)$是子群.(2)设$g_1,g_2\in G$，则$g_1\circ x=g_2\circ x$当且仅当g_1，g_2属于$\mathrm{Stab}_G(x)$的同一左陪集.

＊3. V是域F上n维线性空间，取定V的一组基$\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n$.$V$上任一可逆线性变换A，设它在$\varepsilon_1,\cdots,\varepsilon_n$下矩阵为$A$，则建立起$GL(V)$到$GL_n(F)$的同构，$\mathrm{A}\longmapsto A$.于是群$GL_n(F)$通过$GL(V)$可作用于空间$V$上，进而可作用于$V$的子空间的集合$M$上.

(1) $GL_n(F)$在ε_1处的稳定化子由哪些元素组成？

(2) 令W是由$\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_k$，$k\leqslant n$，生成的子空间，$GL_n(F)$在$W$处的稳定化子由哪些元素组成？

＊4. 正四面体$A_1A_2A_3A_4$的对称性群G可作用在它的顶点的集合和它的面的集合上，也作用在它的棱的集合上.(1)试决定G在顶点A_1处的稳定化子；(2)求G在面$A_2A_3A_4$处的稳定化子；(3)求G在棱A_1A_2处的稳定化子.

5. 把正四面体$A_1A_2A_3A_4$的对称性群用顶点的置换表出.利用§6定理2中公式(2)写出它的对称性群的全部元素.再回到四面体上考察每个置换代表什

么正交变换.

6. G 是群,K 及 H 是 G 的子群.(1)令 M 是 G 中 H 的左陪集的集合.用 K 的元素对 M 的元素进行左乘,得下列映射$^{\circ}$:

$$K\times M\longrightarrow M$$
$$(k,tH)\longmapsto k^{\circ}tH=ktH,$$

证明这是 K 在 M 上的一个群作用.

(2)试决定这个群作用过 tH 的轨道及在 tH 处的稳定化子.并证明 $|KtH|=[K:K\cap tHt^{-1}]|H|$.

*7. S_3 中 $C_3=\{e,(1\ 2\ 3),(1\ 3\ 2)\}$ 组成 S_3 的子群.写出 S_3 中 C_3 的全部左陪集和全部右陪集.

*8. S_4 中写出子群 $S_3=\left\{\begin{pmatrix}1&2&3&4\\ i_1&i_2&i_3&4\end{pmatrix}\middle|\ i_1\,i_2\,i_3 \text{ 是 } 1\ 2\ 3 \text{ 的全部排列}\right\}$ 的全部左陪集.

9. G 是群,H 是子群.当 G 是交换群时,H 的任一左陪集都是一个右陪集.

*10. 写出Z中子群 $3\mathrm{Z}=\{3k\,|\,k\in\mathrm{Z}\}$ 的全部左陪集.

*11. 证明任意 $l,k\in\mathrm{Z}$ 属于 $n\mathrm{Z}$ 在Z中同一陪集的充分必要条件为 $l\equiv k(\mathrm{mod}\ n)$(*).写出Z中 $n\mathrm{Z}$ 的全部陪集.

12. S_3 作用在域 F 上全部多项式 $f(x_1,x_2,x_3)$ 的集合上.求 S_3 在 $x_1^3x_2^2x_3$ 和 $x_1x_2+x_2x_3$ 处的稳定化子及 S_3 作用下分别过 $x_1^3x_2^2x_3$ 和 $x_1x_2+x_2x_3$ 的轨道.

13. 有限群 G 称为 p 群,如果它的阶是素数 p 的方幂.证明 G 的非单位元子群的阶能被 p 除尽,及 G 对于其真子群(即不等于 G 的子群)的指数也被 p 除尽.

14. 有限群 G 为 p 群,则 G 的中心 $Z(G)\neq\{e\}$.(利用改进的类方程(7)).

15. $G=S_3$ 共轭作用于自身.求中心化子 $C_G(\sigma)$,其中 σ 分别是(1 2 3)和(1 2).

*16. 求 S_3 的含上题中(1 2 3)和(1 2)的共轭类.

*17. G 是素数 p 阶的群,则(1)G 除本身和单位元群以外没有其它子群.(2)$G=\langle a\rangle$,$\forall\ a\neq e$.即 G 是循环群.(见§3 定义4 前一段).

18. G 作用在集合 M 上.$x\in M$,$g\in G$,及 $g^{\circ}x=y$,则 $\mathrm{Stab}_G(y)=g\mathrm{Stab}_G(x)g^{-1}$.

19. G 是有限群,$H\subset K$ 皆是 G 的子群,则 $[G:H]=[G:K][K:H]$.

(*) $l\equiv k(\mathrm{mod}\ n)$表示 l 与 k 的差是 n 的倍数,或用 n 去除 l 及 k 所得的余数相同.

20. 有限群 G 是 p 群，$p \nmid m$. G 在 M 上有群作用，且 $|M| = m$，则 G 在 M 上有不动元.

21. 求 S_4 及 A_4 的全部共轭类.

习题答案与解答

1. 略.

2. (1) 设 $g_1, g_2 \in \mathrm{Stab}_G(x)$，$g_i \circ x = x$，$i=1,2$. 于是 $(g_1 g_2) \circ x = g_1 \circ (g_2 \circ x) = g_1 \circ x = x$，又 $g_1^{-1} \circ x = g_1^{-1} \circ (g_1 \circ x) = (g_1^{-1} g_1) \circ x = e \circ x = x$. 故 $g_1 g_2$ 及 $g_1^{-1} \in \mathrm{Stab}_G(x)$，即 $\mathrm{Stab}_G(x)$ 是 G 的子群.

(2) $g_1, g_2 \in G$，$g_1 \circ x = g_2 \circ x \Leftrightarrow x = g_1^{-1} \circ (g_1 \circ x) = g_1^{-1} \circ (g_2 \circ x) = (g_1^{-1} g_2) \circ x \Leftrightarrow g_1^{-1} g_2 \in \mathrm{Stab}_G(x)$，由第一题这等同于 g_1, g_2 属于 $\mathrm{Stab}_G(x)$ 的同一左陪集.

3. (1) 设 $A \in GL_n(F)$，$A \circ \varepsilon_1 = \varepsilon_1$. 这等价于

$$\mathrm{A}(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n) = (\varepsilon_1, *, \cdots, *) = (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n) \begin{pmatrix} 1 & * & \cdots & * \\ 0 & * & \cdots & * \\ \cdots & \cdots & & \cdots \\ 0 & * & \cdots & * \end{pmatrix}$$

故 $GL_n(F)$ 在 ε_1 处的稳定化子为

$$\left\{ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & & \cdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix} \right| \text{其中} \begin{vmatrix} a_{22} \cdots a_{2n} \\ \cdots\cdots \\ a_{n2} \cdots a_{nn} \end{vmatrix} \neq 0 \}$$

(2) $A \in W$ 处的稳定化子，则 A 所对应的线性变换 A 满足

$$\mathrm{A}\ \varepsilon_i = \sum_{j=1}^{k} a_{ji} \varepsilon_j, \qquad i = 1, 2, \cdots, k,$$

也即

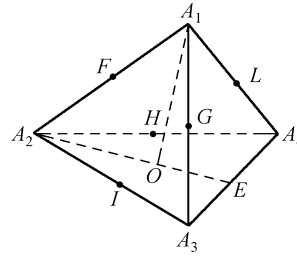
$$\mathrm{A}(\varepsilon_1, \cdots, \varepsilon_k, \cdots, \varepsilon_n) = (\varepsilon_1, \cdots, \varepsilon_k, \cdots, \varepsilon_n) \begin{pmatrix} a_{11} \cdots a_{1k} & \\ \cdots\cdots & * \\ a_{k1} \cdots a_{kk} & \\ \bigcirc & * \end{pmatrix}$$

故 $GL_n(F)$ 在 W 处的稳定化子为

$$\begin{pmatrix} a_{11}\cdots a_{1k} & & \\ \cdots\cdots & * & \\ a_{k1}\cdots a_{kk} & & \\ & a_{k+1,k+1}\cdots a_{k+1,n} & \\ \bigcirc & \cdots\cdots & \\ & a_{n,k+1}\cdots a_{nn} & \end{pmatrix} \text{ 其中 } \begin{vmatrix} a_{11}\cdots a_{1k} \\ \cdots\cdots \\ a_{k1}\cdots a_{kk} \end{vmatrix} \begin{vmatrix} a_{k+1,k+1}\cdots a_{k+1,n} \\ \cdots\cdots \\ a_{n,k+1}\cdots a_{nn} \end{vmatrix} \neq 0 .$$

4. (1),(2)中的稳定化子相同,可参考§2 第 6 题的结果.

(3) 令 A_1A_2 和 A_3A_4 的中点分别是 F,E,则 A_1A_2 的稳定化子由恒等变换、绕 FE 转 180°的旋转变换、对平面 A_1A_2E 以及对平面 A_3A_4F 的反射共四个变换组成.



5. 在§2 第 6 题中求正四面体 $A_1A_2A_3A_4$ 的对称性群的方法与§6 定理 2 中公式是一致的.那里求出对称性群有 24 个元素,全体对称性变换对应了顶点 A_1,A_2,A_3,A_4 的 24 个置换,正是 S_4 的全部元素.令 E、F、G、H、I、L 分别是棱 A_3A_4、A_1A_2、A_1A_3、A_2A_4、A_2A_3、A_1A_4 的中点,则顶点的置换与对称性变换的对应如下:

$\begin{matrix}1&2&3&4\\1&2&3&4\end{matrix}$ 恒等变换.

$\begin{matrix}1&2&3&4\\1&3&4&2\end{matrix}$ 绕 A_1O 旋转 120°.

$\begin{matrix}1&2&3&4\\1&4&2&3\end{matrix}$ 绕 A_1O 旋转 240°.

$\begin{matrix}1&2&3&4\\1&2&4&3\end{matrix}$ 对平面 A_1OA_2 的镜面反射.

$\begin{matrix}1&2&3&4\\1&4&3&2\end{matrix}$ 对平面 A_1OA_3 的镜面反射.

$\begin{matrix}1&2&3&4\\1&3&2&4\end{matrix}$ 对平面 A_1OA_4 的镜面反射.

$\begin{matrix}1&2&3&4\\2&1&3&4\end{matrix}$ 对平面 FA_3A_4 的镜面反射.

$\begin{matrix}1&2&3&4\\2&3&4&1\end{matrix}$ 先绕 A_1O 旋转 120°,再对平面 FA_3A_4 反射.

$\begin{matrix}1&2&3&4\\2&4&1&3\end{matrix}$ 先绕 A_1O 旋转 240°,再对平面 FA_3A_4 进行反射.

$\begin{matrix}1&2&3&4\\2&1&4&3\end{matrix}$ 绕 FE 轴旋转 $180°$.

$\begin{matrix}1&2&3&4\\2&4&3&1\end{matrix}$ 绕四面体过 A_3 的高线旋转 $120°$.

$\begin{matrix}1&2&3&4\\2&3&1&4\end{matrix}$ 绕四面体过 A_4 的高线旋转 $120°$.

$\begin{matrix}1&2&3&4\\3&2&1&4\end{matrix}$ 对平面 A_2GA_4 的镜面反射.

$\begin{matrix}1&2&3&4\\3&1&4&2\end{matrix}$ 先绕 A_1O 转 $120°$,再对平面 A_2GA_4 作反射.

$\begin{matrix}1&2&3&4\\3&4&2&1\end{matrix}$ 先绕 A_1O 转 $240°$,再对平面 A_2GA_4 作反射.

$\begin{matrix}1&2&3&4\\3&2&4&1\end{matrix}$ 绕四面体过 A_2 的高线旋转 $120°$.

$\begin{matrix}1&2&3&4\\3&4&1&2\end{matrix}$ 绕 GH 轴旋转 $180°$.

$\begin{matrix}1&2&3&4\\3&1&2&4\end{matrix}$ 绕四面体过 A_4 的高线旋转 $240°$.

$\begin{matrix}1&2&3&4\\4&2&3&1\end{matrix}$ 对平面 A_2LA_3 的反射.

$\begin{matrix}1&2&3&4\\4&3&1&2\end{matrix}$ 先绕 A_1O 转 $120°$再对平面 A_2LA_3 作反射.

$\begin{matrix}1&2&3&4\\4&1&2&3\end{matrix}$ 先绕 A_1O 转 $240°$再对平面 A_2LA_3 作反射.

$\begin{matrix}1&2&3&4\\4&2&1&3\end{matrix}$ 绕四面体过 A_2 的高线旋转 $240°$.

$\begin{matrix}1&2&3&4\\4&1&3&2\end{matrix}$ 绕四面体过 A_3 的高线旋转 $240°$.

$\begin{matrix}1&2&3&4\\4&3&2&1\end{matrix}$ 绕 IL 轴旋转 $180°$.

6.(1)略.(2)过 tH 的轨道为 $KtH=\{ktH\mid k\in K\}$,而在 tH 处的稳定化子为

$$\mathrm{Stab}_K(tH)=\{k\in K\mid ktH=tH\}=\{k\in K\mid (t^{-1}kt)H=H\}$$
$$=\{k\in K\mid (t^{-1}kt)\in H\}=\{k\in K\mid k\in tHt^{-1}\}=K\cap tHt^{-1}.$$

$$|KtH|=(KtH\text{ 中 }H\text{ 的左陪集的数目})\cdot|H|$$

$=(K$ 作用下过 tH 的轨道的长度$)\cdot|H|$

$=[K:\mathrm{Stab}_K(tH)]\cdot|H|=[K:K\cap tHt^{-1}]|H|$.

7. 略.

8. S_4 中 S_3 的左陪集为

$$S_3,\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}S_3,\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}S_3,\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}S_3.$$

9. 略

10. 略

11. 略

12. S_3 在 $x_1^3x_2^2x_3$ 处的稳定化子为$\{1\}$,在 $x_1x_2+x_2x_3$ 处的稳定化子为

$$\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}.$$

S_3 作用下过 $x_1^3x_2^2x_3$ 的轨道为$\{x_1^3x_2^2x_3,x_1^2x_2^3x_3,x_1^3x_3^2x_2,x_1^2x_3^3x_2,x_2^3x_3^2x_1,x_2^2x_3^3x_1\}$,而过 $x_1x_2+x_3x_4$ 的轨道为$\{x_1x_2+x_2x_3,x_2x_3+x_3x_1,x_2x_1+x_1x_3\}$.

13. 设$|G|=p^k,k>0$.对 H 为 G 的非单位元子群,则有 $|H|\mid|G|$.p^k 的不等于 1 的因子必被 p 整除,故 $p\mid|H|$.

又设 K 为 G 的真子群,$|K|\mid|G|$.$|G|=p^k$,$|K|$是 p^k 的不等于自己的因子,设为 p^l,$l<k$.由$[G:K]=p^{k-l}$及$k-l>0$,故 $p\mid[G:K]$.

14. 由改进的类方程

$$|G|=|Z(G)|+\sum_{i=1}^{m}[G:C_G(y_i)],$$

其中 $C_G(y_i)\neq G$.由 13 题,$p\mid[G:C_G(y_i)]$.又 $p\mid|G|$,故 $p\mid|Z(G)|$.即 $Z(G)\neq\{e\}$.

15. 令 $\sigma=(1\ 2\ 3)$,$\tau=(1\ 2)$,由计算得

$$C_G(\sigma)=\{e,(1\ 2\ 3),(1\ 3\ 2)\}$$

$$C_G(\tau)=\{e,(1\ 2)\}$$

16. 含(1 2 3)的共轭类为

$$\{(1\ 2\ 3),(1\ 3\ 2)\}.$$

含(1 2)的共轭类为

$$\{(1\ 2),(1\ 3),(2\ 3)\}.$$

17. (1) 设 H 是 G 的子群,则 $|H|\mid|G|$,因 $|G|=p$ 是素数,$|H|=1$ 或 p.当 $|H|=1$ 时 $H=\{e\}$.当 $|H|=p$ 时 $H=G$.

(2) 取 $a\neq e$,则$\langle a\rangle\neq\{e\}$.由(1),$\langle a\rangle=G$.

18. 设 $g\circ x=y$,则

$$h\circ y=y\Leftrightarrow h\circ(g\circ x)=g\circ x\Leftrightarrow(g^{-1}hg)\circ x=x.$$

即 $h\in \mathrm{Stab}_G(y)\Leftrightarrow g^{-1}hg\in \mathrm{Stab}_G(x)$.即 $g^{-1}\mathrm{Stab}_G(y)g=\mathrm{Stab}_G(x)$,或 $g\mathrm{Stab}_G(x)g^{-1}=\mathrm{Stab}_G(y)$.

19. 略.

20. 设 $O_1,O_2,\cdots,O_s$ 是 M 在 G 作用下的全部轨道,则 $|M|=\sum_{i=1}^{s}|O_i|$.若 G 在 M 上无不动元,则 $\forall i,|O_i|>1$.取 $x_i\in O_i$,由 $|G|=|\mathrm{Stab}_G(x_i)|\cdot|O_i|$,即有 $|O_i|\mid|G|$.$|G|=p^k$ 的因子不是1就是 p^l,$l>0$,故 $p\mid|O_i|$.由 $|M|=\sum_{i=1}^{s}|O_i|$,得 $p\mid|M|$ 与题设矛盾.故 G 在 M 上必有不动元.

21. 在 S_4 中有着同类型轮换分解的置换组成一个共轭类.故 S_4 中全部共轭类为:

$\{(1)\}$;$\{(1\ 2),(1\ 3),(1\ 4),(2\ 3),(2\ 4),(3\ 4)\}$;$\{(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$;$\{(1\ 2\ 3),(1\ 2\ 4),(1\ 3\ 2),(1\ 4\ 2),(1\ 3\ 4),(1\ 4\ 3)\}$;$\{(1\ 2\ 3\ 4),(1\ 2\ 4\ 3),(1\ 3\ 2\ 4),(1\ 3\ 4\ 2),(1\ 4\ 2\ 3),(1\ 4\ 3\ 2)\}$.

上述集合中只有第1,第3,第4个集合是在 A_4 中.$\{(1)\}$是 A_4 的一个类.由于

$$\tau=\begin{pmatrix}1&2&3&4\\ i_1&i_2&i_3&i_4\end{pmatrix}\quad 及\quad \begin{pmatrix}1&2&3&4\\ i_1&i_2&i_4&i_3\end{pmatrix}$$

皆能满足 $\tau(1\ 2)(3\ 4)\tau^{-1}=(i_1\ i_2)(i_3\ i_4)$.且这两个 τ 中必有一个为偶置换.故 $\{(i_1\ i_2)(i_3\ i_4)\}$与$(1\ 2)(3\ 4)$在 A_4 中组成一个共轭类.

又设 $\tau_1=\begin{pmatrix}1&2&3&4\\ j_1&j_2&j_3&j_4\end{pmatrix}$,则 $\tau_1(1\ 2\ 3)\tau_1^{-1}=(j_1\ j_2\ j_3)(j_4)=(i_1\ i_2\ i_3)(i_4)=\tau(1\ 2\ 3)\tau^{-1}$ 当且仅当 $i_4=j_4$ 且 $j_1\ j_2\ j_3$ 是 $i_1\ i_2\ i_3$ 的循环排列.这时 $j_1\ j_2\ j_3\ j_4$ 与 $i_1\ i_2\ i_3\ i_4$ 具有相同的奇偶性,同时置换 τ 与 τ_1 也具有相同的奇偶性.结果$(j_1\ j_2\ j_3)$与$(1\ 2\ 3)$在 A_4 中共轭当且仅当 τ_1 是偶置换,也即 $j_1\ j_2\ j_3\ j_4$ 是1 2 3 4的偶排列.由此可计算出$(1\ 2\ 3)$在 A_4 中所属的类是

$$\{(1\ 2\ 3),(1\ 3\ 4),(1\ 4\ 2),(2\ 4\ 3)\}$$

同样地算出$(1\ 3\ 2)$在 A_4 中所属的类是

$$\{(1\ 3\ 2),(1\ 2\ 4),(1\ 4\ 3),(2\ 3\ 4)\}.$$

加上前面算出的两个共轭类

$$\{(1)\};\{(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\},$$

A_4 共有4个类.

§7 循环群与交换群

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. G 是 n 阶循环群,$m \mid n$,则方程 $x^m = e$ 在 G 中恰有 m 个解.

*2. 循环群的同态象是循环群.

*3. G 有 n 阶循环子群当且仅当 G 有 n 阶元.再证:

(1) G 是素数 p 阶群,则 G 是循环群.

(2) G 是 $2p$ 阶非交换群,p 素数,则 G 必有 p 阶子群.

4. G 是交换群,$g, h \in G$. $o(g) = m$, $o(h) = n$, $(m, n) = 1$.证明:

(1) g, h 生成的子群 $\langle g, h\rangle = \langle gh\rangle$.

(2) $\langle g\rangle \cap \langle h\rangle = e$ 且 $\langle gh\rangle \cong \langle g\rangle \times \langle h\rangle$.

*5. $G = \langle a\rangle$ 是 n 阶循环群,则

(1) $\langle a^m\rangle = \langle a\rangle$ 当且仅当 $(m, n) = 1$.

(2) 当 $(m, n) = d$ 时,$\langle a^m\rangle = \langle a^d\rangle$.

6. G 的阶是 p 的方幂,p 是素数,则 G 中有 p 阶元.

7. G 是交换群,则 G 中有限阶元素的集合组成 G 的子群.

8. G 是群,则 $o(a) = o(a^{-1})$, $o(ab) = o(ba)$, $\forall\, c \in G$, $o(a) = o(cac^{-1})$.

9. $lZ \quad kZ \quad l, k]Z \quad lZ \quad kZ \quad l, k)Z \quad l, k]$ 为 l, k 的最小公倍数.

习题答案与解答

1. 设 $G = \langle a\rangle = \{a, a^2, \cdots, a^n = e\}$. 令 $q = \frac{n}{m}$. 设 $(a^i)^m = e$,作除法算式 $i = lq + r$, $r = 0$ 或 $0 < r < q$. 若 $r \neq 0$ 由 $a^{im} = a^{lmq} \cdot a^{rm} = a^{rm}$. 但 $0 < rm < mq = n$,故 $a^{im} = a^{rm} \neq e$. 矛盾,故 $r = 0$,即 $i = lq$. 由此 $(a^i)^m = e$ 当且仅当 $i = lq$. 这样的 i 恰有 $q, 2q, \cdots, mq = n$ 共 m 个,故 G 中 $x^m = e$ 恰有 m 个解.

2. 略.

3. 只证(2),G 中元素的阶是 $|G|$ 的因子,故 G 中的非单位元的阶只能为 2, p, $2p$. 若 G 有 $2p$ 阶元 a,则 $G = \langle a\rangle$,与 G 为非交换群矛盾. 若 G 的元全为 2 阶元,由 §1 习题 9,G 为交换群,这不可能. 故 G 中必有 p 阶元,即有 p 阶子群.

4. (1) 由引理 4, $o(gh)=mn$, 故 $|\langle gh\rangle|=mn$, 而 $\langle g,h\rangle=\{g^ih^j \mid 1\leqslant i\leqslant m, 1\leqslant j\leqslant m\}$, 有 $|\langle g,h\rangle|\leqslant mn$. 但 $\langle gh\rangle\subseteq\langle g,h\rangle$, 则 $mn=|\langle gh\rangle|\leqslant|\langle g,h\rangle|\leqslant mn$, 因此 $|\langle g,h\rangle|=|\langle gh\rangle|$, 即有 $\langle g,h\rangle=\langle gh\rangle$.

(2) 作 $\langle g\rangle\times\langle h\rangle\xrightarrow{\pi}\langle g,h\rangle=\langle gh\rangle$

$(g^i,h^j)\longmapsto g^ih^j$, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n$.

因 g,h 交换, π 是同态. 易见它是满同态. 又 $|\langle g\rangle\times\langle h\rangle|=mn=|\langle g,h\rangle|$, 故 π 是双射, 因而是同构.

设有 $g^i=h^j\in\langle g\rangle\cap\langle h\rangle$, 则 $g^ih^{n-j}=e$. 因 π 是同构, g^ih^{n-j} 的原象是 $(g^i,h^{n-j})=(e,e)$, 即有 $g^i=e$, 故 $\langle g\rangle\cap\langle h\rangle=\{e\}$.

5. (1) $\langle a^m\rangle=\langle a\rangle\Leftrightarrow a\in\langle a^m\rangle\Leftrightarrow\exists\, l$, 使 $a^{lm}=a$. 用除法算式 $lm=qn+r$, $0\leqslant r<n$. 若 $r\neq1$, 则 $a^{lm}=a^{qn}\cdot a^r=a^r\neq a$, 矛盾. 故

$$\langle a^m\rangle=\langle a\rangle\Leftrightarrow\exists\, l, \text{使 } a^{lm}=a, \text{且 } lm=qn+1.$$

$$\Leftrightarrow(m,n)=1.$$

(2) 设 $(m,n)=d$. 则有 l,q 使 $lm+qn=d$. 于是有 $a^{lm}=a^d$, 因而 $\langle a^d\rangle\subseteq\langle a^m\rangle$.

又由 $(m,n)=d$, $d\mid m$. $a^m=a^{sd}\in\langle a^d\rangle$, 即有 $\langle a^m\rangle\subseteq\langle a^d\rangle$, 故 $\langle a^m\rangle=\langle a^d\rangle$.

6. G 的元素的阶是 $|G|$ 的因子. 它的非单位元 a 的阶是 p^l, $l>0$. 于是 $a^{p^{l-1}}$ 的阶就为 p.

7. 令 $G_1=\{a\in G \mid a$ 是有限阶$\}$. $\forall\, a,b\in G_1$, 设 $o(a)=m$, $o(b)=n$. 则 $(ab)^{mn}=a^{mn}b^{mn}=e$. 故 $ab\in G_1$. 又 $a^m=e$, $(a^{-1})^m=a^m(a^{-1})^m=(aa^{-1})^m=e$, 故 $a^{-1}\in G_1$. 以上证明了 G_1 是 G 的子群.

8. 题 7 中已证 $o(a)=m$ 则 $(a^{-1})^m=e$. 故 $o(a^{-1})\leqslant o(a)$. 由于 a 与 a^{-1} 互为逆元, 故 $o(a)\leqslant o(a^{-1})$, 因此有 $o(a)=o(a^{-1})$.

再看

$$a^m=e\Rightarrow(c^{-1}ac)(c^{-1}ac)\cdots(c^{-1}ac)=c^{-1}a^mc=e\Rightarrow a^m=cec^{-1}=e.$$

(m 个)

由此即得 $o(a)=o(c^{-1}ac)$.

又 $ab=b^{-1}(ba)b$, 即得 $o(ab)=o(ba)$.

9. (1) 由 $l\mid[l,k]$, $[l,k]\mathbb{Z}\subseteq l\mathbb{Z}$. 同样有 $[l,k]\mathbb{Z}\subseteq k\mathbb{Z}$, 即得 $[l,k]\mathbb{Z}\subseteq l\mathbb{Z}\cap k\mathbb{Z}$.

设 $t\in l\mathbb{Z}\cap k\mathbb{Z}$, 于是 $l\mid t$, $k\mid t$. 但 $[l,k]=\frac{lk}{(l,k)}$ 于是 $\frac{l}{(l,k)}\Big|\frac{t}{(l,k)}$, $\frac{k}{(l,k)}\Big|\frac{t}{(l,k)}$. 而 $\left(\frac{l}{(l,k)},\frac{k}{(l,k)}\right)=1$, 即有 $\frac{l}{(l,k)}\frac{k}{(l,k)}\Big|\frac{t}{(l,k)}$. 于是 $\frac{lk}{(l,k)}\Big|t$, 则 $[l,k]\mid t$ 及 $t\in[l,k]\mathbb{Z}$. 因此 $l\mathbb{Z}\cap k\mathbb{Z}\subseteq[l,k]\mathbb{Z}$. 就得到 $l\mathbb{Z}\cap k\mathbb{Z}=$

$[l,k]\mathbb{Z}$.

(2) 由 $l\mathbb{Z}\subseteq(l,k)\mathbb{Z}$, $k\mathbb{Z}\subseteq(l,k)\mathbb{Z}$,得 $l\mathbb{Z}+k\mathbb{Z}\subseteq(l,k)\mathbb{Z}$.又有 $u,v\in\mathbb{Z}$ 使 $ul+vk=(l,k)$,得$(l,k)\mathbb{Z}\subseteq l\mathbb{Z}+k\mathbb{Z}$,就有$(l,k)\mathbb{Z}=l\mathbb{Z}+k\mathbb{Z}$.

§8 正规子群和商群

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. G 的指数为 2 的子群 H 是正规子群.

*2. G 的中心 $Z(G)$是正规子群.

3. 证明 S_3 中的子群 e,(1 2) 不是正规子群, e,(1 2 3),(1 3 2) 是正规子群.

*4. 证明 S_4 中 V_4(见 §2 习题 5)是正规子群.

5. $GL_n(F)$中子群 $SL_n(F)$是正规子群及全部 $n\times n$ 数量矩阵的集合组成正规子群.

6. G 是群,H_1,H_2,…,H_k,…皆为 G 的正规子群,则$\bigcap\limits_{i=1}^{\infty}H_k$ 是 G 的正规子群.

7. G 是群,H 是子群,则$\bigcap\limits_{x\in G}xHx^{-1}$是 G 的正规子群.

8. 证明 S_3 是唯一的非交换 6 阶群.

9. S_4 中 e,(1 2 3),(1 3 2) 是正规子群吗?

*10. 设 G 是有限群,$n\mid\mid G\mid$,且 G 中仅有一个 n 阶子群 H,则 H 是 G 的正规子群.

*11. 确定$\mathbb{Z}/3\mathbb{Z}$,$\mathbb{Z}/6\mathbb{Z}$ 的加法表.写出$\mathbb{Z}/n\mathbb{Z}$ 的全部元素.

*12. F_2 是二元域,确定 $F_2[x]/(x^2+1)F_2[x]$, $F_2[x]/(x^3+x^2+x+1)F_2[x]$的加法表. $f(x)$是域 F_2 上 n 次多项式,写出 $F_2[x]/f(x)F_2[x]$的全部元素.

13. F 是域,写出 $GL_n(F)/SL_n(F)$的全部元素.

14. $G=\{(a,b)\mid a,b\in\mathbb{R}\ ,a\neq0\}=\mathbb{R}^*\times\mathbb{R}$,其中$\mathbb{R}^*=\mathbb{R}\setminus\{0\}$,对乘法$(a,b)(c,d)=(ac,ad+b)$成为群(§1 习题 6).证明

$$K=\{(1,b)\mid b\in\mathbb{R}\}$$

是 G 的正规子群,且 $G/K\cong\mathbb{R}^*$ 的乘法群.

15. G 是群,H 是子群.$C_G(H)$及 $N_G(H)$分别是 H 的中心化子及正规化

子.(见§3 习题4)证明:

(1) $C_G(H)$是 $N_G(H)$的正规子群.

(2) $N_G(H)$到 H 的自同构群 Aut H 有同态映射

$$N_G(H)\longrightarrow \text{Aut } H$$

$$n\longmapsto \tau_n:\tau_n(h)=nhn^{-1},\forall\ h\in H.$$

(3) $\forall\ n_1,n_2\in N_G(H),\tau_{n_1}=\tau_{n_2}$当且仅当 $n_2\in n_1C_G(H)$.

(4) 映射

$$N_G(H)/C_G(H)\longrightarrow \text{Aut } H$$

$$nC_G(H)\longmapsto \tau_n$$

是群的单同态.

16. $G=\langle a\rangle$是 n 阶循环群,Z 是整数加法群.证明:

(1) 映射

$$\mathrm{Z}\xrightarrow{\tau}G$$

$$m\longmapsto a^m$$

是群同态.

(2) $\forall\ k,m\in\mathrm{Z}$,$\tau(k)=\tau(m)$当且仅当 $k\in m+n\mathrm{Z}$.

(3) 映射

$$\mathrm{Z}/n\mathrm{Z}\longrightarrow G=\langle a\rangle$$

$$m+n\mathrm{Z}\longmapsto a^m$$

是群同构.

17. G 是 p^2 阶群,p 是素数,则 G 是交换群.进而证明只有两个(不同构的)p^2 阶的群.(提示:若 $G\neq Z(G)$,则有 $g\overline{\in}Z(G)$,使 $G=\bigcup_{i=1}^{p}g^iZ(G)$).

18. 若 $G/Z(G)$是循环群,则 G 是交换群.

19. G 是群,H 是循环子群且在 G 中正规,则 H 的子群在 G 中都正规.

20. 令 D_n 是平面上正 n 边形的对称性群.当 n 为奇数时,$Z(D_n)$为$\{e\}$,当 n 为偶数时,$Z(D_n)$为 2 阶群.

21. G 是群,$H_1,H_2,\cdots,H_k,\cdots$是 G 的子群.K 是 G 的正规子群,$K\subset H_k$,$k=1,2,\cdots$,则

$$\bigcap_{k=1}^{\infty}(H_k/K)=\left(\bigcap_{k=1}^{\infty}H_k\right)/K.$$

习题答案与解答

1. $\forall\ a\in H$,自然有 $aH=H=Ha$.若 $a\overline{\in}H$,则 H 与 aH 是不同的左陪集.

再由指数$[G:H]=2$,H 在中只有两个左陪集.故 $G=H\cup aH$.由于 $a\overline{\in}H$,H 与 Ha 也是不同的右陪集,于是 $G=H\cup Ha$,aH 与 Ha 皆为 H 在 G 中的补集,即知 $aH=Ha$.这样,$\forall\ a\in G$ 皆有 $aH=Ha$.由命题 1 及正规子群的定义知 H 是 G 的正规子群.

2. 略.

3. 略.

4. 略.

5. 略.

6. 首先证,$\forall\ g\in G$,有 $g^{-1}\left(\bigcap_{i=1}^{\infty}H_i\right)g=\bigcap_{i=1}^{\infty}g^{-1}H_ig$.实际上,左端的任一元为 $g^{-1}hg$,$h\in\bigcap_{i=1}^{\infty}H_i$,由 $h\in H_i$,$i=1,2,\cdots$,知 $g^{-1}hg\in g^{-1}H_ig$,$i=1,2,\cdots$.故 $g^{-1}hg\in\bigcap_{i=1}^{\infty}g^{-1}H_ig$,即有 $g^{-1}\left(\bigcap_{i=1}^{\infty}H_i\right)g\subseteq\bigcap_{i=1}^{\infty}g^{-1}H_ig$.由 g 的任意性,用 g^{-1} 替代 g,并用 $g^{-1}H_ig$ 替代 H_i,则有 $g\left(\bigcap_{i=1}^{\infty}g^{-1}H_ig\right)g^{-1}\subseteq\bigcap_{i=1}^{\infty}g(g^{-1}H_ig)g^{-1}=\bigcap_{i=1}^{\infty}H_i$.再用 g^{-1} 左乘两端,及用 g 右乘两端就得到 $\bigcap_{i=1}^{\infty}g^{-1}H_ig\subseteq g^{-1}\left(\bigcap_{i=1}^{\infty}H_i\right)g$,即有 $g^{-1}\left(\bigcap_{i=1}^{\infty}H_i\right)g=\bigcap_{i=1}^{\infty}g^{-1}H_ig$.

由 H_i 是 G 的正规子群,$g^{-1}H_ig=H_i$.就得 $\forall\ g\in G$,$g^{-1}\left(\bigcap_{i=1}^{\infty}H_i\right)g=\bigcap_{i=1}^{\infty}H_i$,这证明了 $\bigcap_{i=1}^{\infty}H_i$ 是正规子群.

7. 首先对 $\forall\ g\in G$,易知有

$$gG=\{gx\mid x\in G\}=G.$$

再由习题 6 证明中的第一部分,可得

$$g\left(\bigcap_{x\in G}xHx^{-1}\right)g^{-1}=\bigcap_{x\in G}gxHx^{-1}g^{-1}=\bigcap_{x\in G}(gx)H(gx)^{-1}=\bigcap_{y\in G}yHy^{-1}$$

故 $\bigcap_{x\in G}xHx^{-1}$ 是 G 的正规子群.

8. 设 H 是 6 阶非交换群,我们证明 $H\cong S_3$.

H 非循环,故没有 6 阶元.它非交换,不能全是二阶元,故有三阶元 b.令 $K=\langle b\rangle$,它是三阶群.$[H:K]=2$,故 K 是 H 的正规子群,且有陪集分解 $H=K\cup aK$.于是

$$K=\{e,b,b^2\},\quad H=\{e,b,b^2,a,ab,ab^2\}.$$

可以断言 $a^{-1}ba\neq b$.否则由 $ab=ba$,就得出 H 是交换群,与假设矛盾.由 $a^{-1}ba\in K$(K 是正规子群),$a^{-1}ba\neq e$(为什么?),又不等于 b,知 $a^{-1}ba=b^2$.也就得到 $ba=ab^2$.

再证 $a^2=e$.若不相等,则 a 为三阶元,$a^2\neq e$.若 $a^2\in aK$,则有 $k\in K$ 使 $a^2=ak$.于是 $a=k\in K$ 与 $a\overline{\in}K$ 矛盾.若 $a^2\in K$ 则 $e=a^3=a\cdot a^2\in aK$ 也矛盾.故 $a^2=e$.同样可证$(ab^2)^2=(ab)^2=e$(由于 $aK=abK=ab^2K$).

建立双射 $H\longmapsto S_3$:

$$e\longmapsto(1),a\longmapsto\begin{matrix}1&2&3\\3&2&1\end{matrix},ab\longmapsto\begin{matrix}1&2&3\\2&1&3\end{matrix},ab^2\longmapsto\begin{matrix}1&2&3\\1&3&2\end{matrix}$$

$$b\longmapsto\begin{matrix}1&2&3\\2&3&1\end{matrix},b^2\longmapsto\begin{matrix}1&2&3\\3&1&2\end{matrix}.$$

它保持乘法,故是同构.

9. 略.

10. 略.

11. 略.

12. 只写出 $F_2[x]/f(x)F_2[x]$的全部元素为

$$F_2[x]/f(x)F_2[x]=\{a_0+a_1x+\cdots+a_{n-1}x^{n-1}+(f(x))\mid a_i\in F_2,i=0,1,\cdots,n-1\}.$$

13. $A,B\in GL_n(F)$,它们属于 $SL_n(F)$的同一陪集当且仅当有 $C\in SL_n(F)$ 使 $A=BC$.由此可推出 $|A|=|B||C|=|B|$.反之设 $A,B\in GL_n(F)$,$|A|=|B|$.则 $A=B(B^{-1}A)$,$|B^{-1}A|=|B|^{-1}|B|=1$.得 $B^{-1}A\in SL_n(F)$.故 $A,B\in GL_n(F)$属于 $SL_n(F)$的同一陪集当且仅当 $|A|=|B|\neq0$.

对 $r\in F^*=F\setminus\{0\}$,可取

$$R_r=\begin{pmatrix}r&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix}_{n\times n}.$$

则 $SL_n(F)$在 $GL_n(F)$中的全部陪集为

$$GL_n(F)/SL_n(F)=\{R_rSL_n(F)\mid r\in F^*\}$$

14. 略.

15. (1)取 $c\in C_G(H)$,$n\in N_G(H)$,只要证(ncn^{-1})与 H 中的元素都交换.任取 $h\in H$.因 $n^{-1}hn\in H$,$c(n^{-1}hn)c^{-1}=nhn^{-1}$.故$(ncn^{-1})h(ncn^{-1})^{-1}=n(c(n^{-1}hn)c^{-1})n^{-1}=n(n^{-1}hn)n^{-1}=h$.得证.

(2)对 $n\in N_G(H)$,易知 $\tau_n:\tau_n(h)=nhn^{-1}$,$\forall\,h\in H$,是 H 的自同构.故 $n\longmapsto\tau_n$ 是 $N_G(H)$到 $Aut(H)$的映射.又对 $n_1,n_2\in N_G(H)$,$\forall\,h\in H$,

$\tau_{n_1 n_2}(h)=(n_1 n_2)h(n_1 n_2)^{-1}=n_1(n_2 h n_2^{-1})n_1^{-1}=\tau_{n_1}\tau_{n_2}(h)$. 故 $\tau_{n_1 n_2}=\tau_{n_1}\tau_{n_2}$，即这映射是群 $N_G(H)$到 H 的自同构群 $Aut(H)$的同态.

(3) $\forall\ n_1, n_2\in N_G(H)$，$\tau_{n_1}=\tau_{n_2}\Leftrightarrow\forall\ h\in H$，$n_1 h n_1^{-1}=n_2 h n_2^{-1}\Leftrightarrow\forall\ h\in H$，$(n_1^{-1}n_2)h(n_1^{-1}n_2)=h\Leftrightarrow n_1^{-1}n_2\in C_G(H)\Leftrightarrow n_2\in n_1 C_G(H)$.

(4) 先说明 $nC_G(H)$ τ_n 与代表元 n 的选择无关.实际上，$\forall\ n_1\in nC_G(H)$，由(3)知 $\tau_{n_1}=\tau_n$.这样，映射

$$\begin{array}{ccc} N_G(H)/C_G(H) & \overset{\eta}{\longrightarrow} & Aut(H) \\ nC_G(H) & \longmapsto & \tau_n \end{array}$$

是有定义的.仍由(3)知，这是单射.又 $\eta(mC_G(H)nC_G(H))=\eta(mnC_G(H))=\tau_{mn}=\tau_m\tau_n=\eta(mC_G(H))\cdot\eta(nC_G(H))$.故 η 是群同态，且是单同态.

16. (1) $\tau(m_1+m_2)=a^{m_1+m_2}=a^{m_1}a^{m_2}=\tau(m_1)\tau(m_2)$，故 τ 是同态.

(2) $\forall\ k, m\in\mathbf{Z}$，$\tau(m)=\tau(k)\Leftrightarrow a^k=a^m\Leftrightarrow a^{k-m}=e\Leftrightarrow(k-m)\in n\mathbf{Z}\Leftrightarrow k\in m+n\mathbf{Z}$.

(3) 令

$$\begin{array}{ccc} \mathbf{Z}/n\mathbf{Z} & \overset{\eta}{\longrightarrow} & G=\langle a\rangle \\ m+n\mathbf{Z} & \longmapsto & \tau(m)=a^m. \end{array}$$

由(2)知，$m+n\mathbf{Z}\longmapsto\tau(m)$与代表元的选择无关，即这映射是有定义的.仍由(2)知，它是单射.

又 $\eta((m+n\mathbf{Z})+(k+n\mathbf{Z}))=\eta((m+k)+n\mathbf{Z})=\tau(m+k)=\tau(m)\tau(k)=\eta(m+n\mathbf{Z})\eta(k+n\mathbf{Z})$.故 η 是同态.η 显然是满射，故是同构.

17. G 是 p 群，由§6 习题 16 知 $Z(G)\neq\{e\}$.若 $Z(G)=G$，则 G 是交换群.当 $Z(G)\neq G$，则$[G:Z(G)]=p$.于是 $G/Z(G)$是 p 阶循环群.令$\langle\bar g\rangle=G/Z(G)$，$\bar g=gZ(G)$.$\langle\bar g\rangle=\langle\bar g, \bar g^2,\cdots,\bar g^{p-1},\bar g^p=\bar e\rangle$.于是 $G=\bigcup_{i=1}^{p}g^iZ(G)$.$G$ 的任何元素可写成 g^iz，$z\in Z(G)$.G 的两个元素 g^iz_1 和 g^jz_2，$z_1, z_2\in Z(G)$，就有 $g^iz_1g^jz_2=g^ig^jz_1z_2=g^jz_2g^iz_1$，即相互交换，故 G 为交换群.

$|G|=p^2$，G 有下列两种类型：

(1) G 中有 p^2 阶元 a，则 G 是 p^2 阶循环群.

(2) G 中非单位元皆为 p 阶.任取 $e\neq a\in G$，$\langle a\rangle$是 p 阶群，故 $G\setminus\langle a\rangle$中还有 $b\neq e$.$\langle b\rangle$也为 p 阶群，$\langle a\rangle\cap\langle b\rangle\neq\langle a\rangle$，而 p 阶群$\langle a\rangle$的真子群只有$\{e\}$.故$\langle a\rangle\cap\langle b\rangle=\{e\}$.此时作映射

$$\begin{array}{ccc} \langle a\rangle\times\langle b\rangle & \overset{\tau}{\longrightarrow} & G \end{array}$$

$$(a^i, b^j) \longmapsto a^i b^j$$

易知它是同态，再证它是单射．设 $\tau((a^i, b^j)) = \tau((a^l, b^m))$，即 $a^i b^j = a^l b^m$．于是 $a^{i-l} = b^{m-j}$．由$\langle a\rangle \bigcap \langle b\rangle = e$，得 $a^{i-l} = b^{m-j} = e$．于是 $a^i = a^l$，$b^m = b^j$．这证明了 τ 是单射．

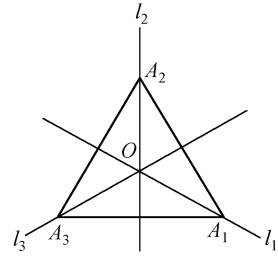
最后证明 τ 是满射，τ 的象集是 G 的子群．τ 的象中有$\langle a\rangle$及$\langle b\rangle$，多于 p 个元．$|G| = p^2$，G 的子群只有$\{e\}$，p 阶子群和 G 本身，故 τ 的象只能是 G 本身，这样 τ 是满射．

综合以上论证，τ 是同构．

18．设 $G/Z(G) = \langle \bar{g}\rangle$，$\langle \bar{g}\rangle = \langle \bar{g}^0, \bar{g}^1, \bar{g}^2, \cdots\rangle$．则 $G = \bigcup g^i Z(G)$．$\forall\ a, b \in G$，令 $a = g^i z_1$，$b = g^j z_2$，$z_1, z_2 \in Z(G)$．$ab = g^i z_1 g^j z_2 = g^i g^j z_1 z_2 = g^j z_2 g^i z_1 = ba$，故 G 是交换群．

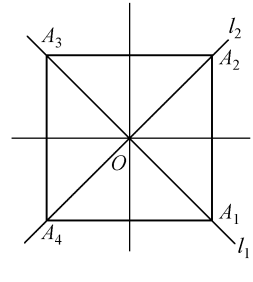
19．由§7 定理 3，循环群 H 中的同阶子群只有一个．设 K 是 H 中 q 阶子群，$\forall\ g \in G$，因 $K \subseteq H$，H 在 G 中正规，$g^{-1}Kg \subseteq H$．$g^{-1}Kg$ 是 H 中 q 阶子群，故 $g^{-1}Kg = K$，K 在 G 中正规．

20．令 O 为正 n 边形的中心，当 n 为奇数时，将它的顶点编号为 $A_1, A_2, \cdots, A_n$，令过 O, A_i 的直线为 l_i，$i = 1, 2, \cdots, n$ 共 n 个(例 $n = 3$，见图 1)．令平面对 l_i 的反射为 S_i，绕 O 反时针旋转$\frac{2i\pi}{n}$角的变换为 T_i，$i = 0, 1, 2, \cdots, n-1$．则它的对称性群 $D_n = \{T_i, T_i S_1, i = 0, 1, 2, \cdots, n-1\}$．可算出 $T_i S_1 T_i^{-1} = S_{i+1}$．这说明 S_1，除 T_0 外与任何 T_i 不交换．当然对 $i > 0$，T_i 也不与任何 $T_j S_1$ 交换，因此 T_i，$i > 0$ 及 $T_j S_1$，任何 j，都不是中心中的元素．故 $Z(D_n) = e$．



当 n 为偶数，仍将各顶点编号为 $A_1, A_2, \cdots, A_n$，中心记为 O．记直线 $A_1 OA_{\frac{n}{2}+1}$，$A_2 OA_{\frac{n}{2}+2}$，$\cdots$，$A_{\frac{n}{2}} OA_n$ 为 $l_1, l_2, \cdots, l_{\frac{n}{2}}$(例 $n = 4$，如图 2)．记平面上绕 O 反时针旋转$\frac{2i\pi}{n}$的变换为 T_i，$i = 0, 1, \cdots, n-1$．平面对 $l_1, l_2, \cdots, l_{\frac{n}{2}}$的反射分别记为 $S_1, S_2, \cdots, S_{\frac{n}{2}}$．则

$$D_n = \{T_i, T_i S_1, i = 0, 1, 2, \cdots, n-1\}.$$



易知 $T_i S_1 T_i^{-1} = S_{i+1}$，$i = 0, 1, \cdots, \frac{n}{2} - 1$．

$$T_i S_1 T_i^{-1} = S_{i+1-\frac{n}{2}},\ i = \frac{n}{2}, \frac{n}{2}+1, \cdots, n-1.$$

故除了 $T_0 S_1 T_0^{-1} = S_1$，$T_{\frac{n}{2}} S_1 T_{\frac{n}{2}}^{-1} = S_1$，即 S_1 与 T_0，$T_{\frac{n}{2}}$ 交换外，其它 T_i 与 S_1 皆不交换，当然对 $i \neq 0, \frac{n}{2}$，T_i 不与任何 $T_j S_1$ 交换．即 $T_i, i \neq 0, \frac{n}{2}$，$T_j S_1$ 都不是 $Z(D_n)$ 中的元素．$Z(D_n) = \{T_0, T_{\frac{n}{2}}\}$．

21．设 $\hbar \in \bigcap_{k=1}^{\infty} H_k / K$，其中 $h \in \bigcap_{k=1}^{\infty} H_k$．则 $h \in H_k$，$k = 1, 2, \cdots$．因此 $\hbar \in H_k / K$，于是 $\hbar \in \bigcap_{k=1}^{\infty} (H_k / K)$．即 $\bigcap_{k=1}^{\infty} H_k / K \subseteq \bigcap_{k=1}^{\infty} (H_k / K)$．

反之，对 $\hbar \in \bigcap_{k=1}^{\infty} (H_k / K)$，则 $\forall k$ 有 $\hbar \in H_k / K$．于是有 $h_k \in H_k$，$l_k \in K$，使 $h = h_k l_k$．故 $\forall k$ 有 $h \in H_k$，就有 $h \in \bigcap_{k=1}^{\infty} H_k$．即得 $\hbar \in \bigcap_{k=1}^{\infty} H_k / K$．由此 $\bigcap_{k=1}^{\infty} (H_k / K) \subseteq \bigcap_{k=1}^{\infty} H_k / K$，故两者相等．

§9　n 元交错群 A_n，A_n（$n \geqslant 5$）的单性

习　题

以下习题中打 * 者为必作题，其余为选作题．

*1．证明 S_n 可由 $(1\ 2), (1\ 3), \cdots, (1\ n)$ 生成，也可由 $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ 生成．

2．(1)求 $(1\ 2)$，$(3\ 4\ 5)$ 在 S_7 中的中心化子．

*(2) 证明 $\sigma = (1\ 2\ 3 \cdots n)$ 在 S_n 中的中心化子是 $\langle \sigma \rangle$ 及 σ 所在的共轭类中元素数目为 $(n-1)!$．

(3) 求 $(1\ 2)(3\ 4\ 5)(6)$ 在 S_6 中的中心化子的阶及其所在共轭类元素数目．

*3．G 是 S_n 的子群，则 G 中全部偶置换组成 G 的一个正规子群 H．若 G 中有奇置换，则 $[G : H] = 2$．

4．G 是 $2k$ 阶群，k 奇数，则 G 中有一个 k 阶的正规子群（提示：由 §4 中的定理 2(Cayley 定理)，G 同构于 S_{2k} 的一个子群．又由 §1 习题 13，这个子群有一个元 $a \neq e$，$a^2 = e$，分析这个置换的奇偶性）．

5．证明 $n \geqslant 3$ 时，S_n 的中心为 e．

*6．重新证明 A_5 是单群．

7．证明 A_4 中没有 6 阶子群．

习题答案与解答

1. 对 n 作归纳法,当 $n=2$ 时显然成立.设 $n-1$ 时已对,即 $1,2,\cdots,n-1$ 的任一置换是$(1\ 2),(1\ 3),\cdots,(1\ n-1)$的乘积.对 S_n 的任一置换,它是轮换的乘积.我们只要证明任一轮换是$(1\ 2),(1\ 3),\cdots,(1\ n)$的乘积就行.对含文字 n 的轮换$(i_1\cdots i_k\ n)$它等于$(i_1\ i_2\cdots i_k)(i_k\ n)=(i_1\cdots i_k)(1\ i_k)(1\ n)(1\ i_k)$.而$(i_1\cdots i_k)\in S_{n-1}$,可由$(1\ 2),(1\ 3),\cdots,(1\ n-1)$的乘积表出.故结论成立.这就完成了归纳法.后半题略证.

2. (1)求$(1\ 2)$在 S_7 中的中心化子.

设 $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\ \sigma(1)&\sigma(2)&\sigma(3)&\sigma(4)&\sigma(5)&\sigma(6)&\sigma(7)\end{pmatrix}$ 使 $\sigma(12)\sigma^{-1}=(12)$.上式左端$=(\sigma(1)\ \ \sigma(2))=(1\ \ 2)\Leftrightarrow\sigma\in S_2S_5$.其中 S_2 是文字 1,2 的对称群,S_5 是文字 3,4,5,6,7 的对称群.即$(1\ \ 2)$的中心化子是 S_2S_5.

类似地$(3\ \ 4\ \ 5)$的中心化子是 C_3S_4.其中 $C_3=\{(1),(3\ 4\ 5),(3\ 5\ 4)\}$,$S_4$ 是 1,2,6,7 四个文字上的对称群.

(2)先证 $\sigma=(1\ 2\cdots n)$的中心化子 $C_{S_n}(\sigma)=\langle\sigma\rangle$.

设 $\tau=\begin{pmatrix}1&2&\cdots&n\\ \tau(1)&\tau(2)&\cdots&\tau(n)\end{pmatrix}$ 满足 $\tau\sigma\tau^{-1}=\sigma$.即$(\tau(1)\ \tau(2)\cdots\tau(n))=(1\ 2\cdots n)$.故 $\tau(1)\ \tau(2)\cdots\tau(n)$是 $1\ \ 2\cdots n$ 的如下形式的排列 $k\ \ k+1\cdots n\ 1\ \cdots\ \ k-1$.因而 $\tau=\begin{pmatrix}1&2&\cdots&n-(k-1)&n-(k-2)&\cdots&n\\ k&k+1&\cdots&n&1&\cdots&k-1\end{pmatrix}$.即 $\tau=\sigma^{k-1}$,$1\leqslant k\leqslant n$.这证明了 $\tau\sigma\tau^{-1}=\sigma$ 当且仅当 $\tau\in\langle\sigma\rangle$,因此 $C_{S_n}(\sigma)=\langle\sigma\rangle$.

由于 $|\langle\sigma\rangle|=n$,σ 所在的共轭类中元素的数目为

$$[S_n:C_{S_n}(\sigma)]=\frac{n!}{n}=(n-1)!.$$

(3) $(1\ 2)(3\ 4\ 5)(6)$的中心化子是 S_2C_3.其中 S_2,C_3 如本题(1).

3. H 由 G 中全部偶置换组成,对 $\forall\ \sigma\in H,\tau\in G$,$\tau\sigma\tau^{-1}$仍为 G 中偶置换.故 $\tau H\tau^{-1}=H$,即 H 是 G 的正规子群.又若 G 中还有奇置换 τ,则 τH 中皆为奇置换.且对 G 中任一奇置换 τ_1,$\tau^{-1}\tau_1$ 必为偶置换,故 $\tau^{-1}\tau_1\in H$,因而 $\tau_1\in\tau H$.故 τH 是 G 中全部奇置换.由此 $G=H\cup\tau H$,$[G:H]=2$.

4. 考虑 G 在 G 上左乘的群作用,由 §4 的 Cayley 定理,这是群 G 到 G 上置换群的同构.后者是 $2k$ 个元的集合 G 上的 $|G|$个置换组成的 S_{2k}的子群.因 $|G|=2k$,故有 $g\in G$,$g\neq e$,但 $g^2=e$(§1 习题 13).考虑 g 左乘 G 所对应的全部置换.对任 $a\in G$,g 在 a,ga 这对元素上的作用构成二轮换,即对换,令 $a_1=$

$a, a_2 = ga_1 = ga$,则 $ga_2 = g^2 a_1 = a_1$.易知 g 在 $G \setminus \{a_1, a_2\}$上的左乘作用仍是封闭的,用归纳法可知 G 中 $2k$ 个元可逐个配对为 $a_1 a_2; a_3, a_4; \cdots; a_{2k-1}, a_{2k}$,并满足 $ga_{2l-1} = a_{2l}, ga_{2l} = g^2 a_{2l-1} = a_{2l-1}, l = 1, 2, \cdots, k$.即 g 在 G 上的左乘作用是 k 个对换的乘积.k 是奇数,故 g 对应奇置换.由习题 6,G 的左乘作用作成的置换群中有指数为 2 的正规子群.

5. 设 $\tau \in S_n$ 的中心,令 $\sigma = (1\ 2 \cdots n-1)(n)$.当然 τ 在 σ 的中心化子中.由 $\tau^{-1}\sigma\tau = \sigma$,就得 $(\tau(1)\tau(2)\cdots\tau(n-1))(\tau(n)) = (1\ 2 \cdots n-1)(n)$.再由 $n-1 \geqslant 2$,故 $\tau(n) = n$.适当更换 σ,可证明 $\tau(1) = 1, \tau(2) = 2, \cdots, \tau(n) = n$.即 $\tau = e$.

6. 按课文中的证明路线,只要证明 A_5 的非平凡正规子群 H 中有三轮换.我们按 H 中置换的不动元数目来进行分析.

H 中有非单位元置换 τ.若 τ 有四个不动元,则另一个元也为不动元,它就是单位元,不可能.若 τ 有三个不动元,则 τ 为对换或单位元.前者是奇置换,它不属于 H,这也不可能.若 τ 恰有两个不动元,只能是其它三个元的三轮换,故 H 中有三轮换.现设 τ 最多有一个不动元,τ 是偶置换,只能是五轮换,$\tau = (\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$或是两个不相交的对换的乘积,$\tau = (\alpha_1\ \alpha_2)(\alpha_3\ \alpha_4)$.令 $\varphi = (\alpha_3\ \alpha_4\ \alpha_5) \in A_5$,作 $\varphi\tau\varphi^{-1}$,它是 $\varphi\tau\varphi^{-1} = (\alpha_1\ \alpha_2\ \alpha_4\ \alpha_5\ \alpha_3)$或 $(\alpha_1\ \alpha_2)(\alpha_4\ \alpha_5)$,再作 $\tau^{-1}\varphi\tau\varphi^{-1}$,它就等于 $(\alpha_1)(\alpha_2\ \alpha_3\ \alpha_5)(\alpha_4)$或 $(\alpha_1)(\alpha_2)(\alpha_4\ \alpha_5\ \alpha_3)$它们都是三轮换且都属于 H.

7. 设 H 是 A_4 中的 6 阶子群.由习题 7 知 H 中有三阶正规子群 K,且 H 中有二阶元 h.于是 $H = K \cup hK$.若 $hk \in hK$ 为三阶元,则 $(hk)^3 = h^3 k_1 = e, k_1 \in K$.但 $h^2 = e$,于是 $hk_1 = e$,而得 $h \in K$.K 中无二阶元,矛盾.即 hK 中皆为二阶元.A_4 中仅有三个二阶元,$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$,加上 e 正好组成 H 中的 4 阶子群.但 $4 \nmid |H|$,矛盾.故 A_4 中没有 6 阶子群.

§10 同态基本定理

习 题

以下习题中打 * 者为必作题,其余为选作题.

1. F 是域.试证明 $GL_n(F)/SL_n(F) \cong F$.

2. S_4 有正规子群 $V_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.试写出 S_4/V_4 的全部元素,并建立一个同构映射

$$S_4/V_4 \qquad S_3 .$$

*3. G 是群，$Z(G)$是 G 的中心，则 $G/Z(G)$同构于 Aut G 的子群.进而，若 G 非交换，则 Aut G 是非循环群.

*4. $\mathbb{C}^*$是非零复数的乘法群. $U=\{e^{i\theta} \mid \theta$ 实数$\}$是$\mathbb{C}^*$中绝对值等于 1 的复数的子群，则$\mathbb{C}^*/U$ 同构于正实数的乘法群.

*5. R 是实数加法群，Z 是它的加法子群，则R /Z 同构于绝对值为 1 的复数的乘法群.

6. 设群 G 到群 $\bar{G}$ 有满同态 f.令 $N=\mathrm{Ker}\ f$.记 $f^{-1}(\bar{K})$为 $\bar{G}$ 的子集 $\bar{K}$ 对于 f 的原象.证明：

(1) 若 $\bar{K}$ 是 $\bar{G}$ 的子群，则 $N\subset f^{-1}(\bar{K})$.

(2) $\{G$ 的包含 N 的子群$\}$ $\overset{\varphi}{\longmapsto}$ $\{\bar{G}$ 的子群$\}$

$$H \longmapsto f(H)$$

是双射，且保持包含关系.

(3) 若 $\bar{K}$ 是 $\bar{G}$ 的正规子群，则 $f^{-1}(\bar{K})$是 G 的含 N 的正规子群. 于是

$\{G$ 的包含 N 的正规子群$\}$ $\overset{\varphi}{\longmapsto}$ $\{\bar{G}$ 的正规子群$\}$

$$K \longmapsto f(K)$$

是双射.

(4) 设 H 是 G 的正规子群，则有同构

$$G/f^{-1}(H)\cong \bar{G}/H .$$

(5) G 是群，N 是正规子群.令 $\bar{G}=G/N$. π 是自然同态

$$G \overset{\pi}{\longmapsto} G/N=\bar{G},$$

则 π 建立了$\{G$ 的含 N 的子群$\}$到$\{\bar{G}$ 的子群$\}$上的双射：$\pi(H)=\bar{H}=H/N$.且保持包含关系.同时建立了$\{G$ 的含 N 的正规子群$\}$到$\{\bar{G}$ 的正规子群$\}$上的双射.且有同构

$$G/H\cong \bar{G}/\bar{H}=G/N\big/H/N .$$

以上的结论称为第二同构定理.

7. G 是群，H 是子群，$[G:H]=n$.令 G 中 H 的左陪集的集合 $M=\{x_iH \mid i=1,2,\cdots,n, x_i\in G\}$.证明：

(1) $g\in G$, $gx_iH=x_iH$, $i=1,2,\cdots,n$ 当且仅当 $g\in\bigcap_{i=1}^{n} x_iHx_i^{-1}$.

(2) $\bigcap_{i=1}^{n} x_iHx_i^{-1}=\bigcap_{x\in G} xHx^{-1}$是 G 的正规子群.

(3) 映射 $G \overset{\varphi}{\longmapsto} S_n$($M$ 中 n 个元的置换群)

$$g\longmapsto\varphi(g):x_iH\longmapsto gx_iH,i=1,2,\cdots,n,$$

是群同态.

(4) $\forall g_1,g\in G,\varphi(g)=\varphi(g_1)$当且仅当 $g_1\in g(\bigcap\limits_{x\in G}xHx^{-1})$.

(5) 映射:$G/\bigcap\limits_{x\in G}xHx^{-1}$——$S_n$

$$g\bigcap_{x\in G}xHx^{-1}\longmapsto\varphi(g)$$

是群的单同态.即 $G/\bigcap\limits_{x\in G}xHx^{-1}$与 S_n 的一个子群同构.

(6) H 包含一个正规子群,它在 G 中的指数是 $n!$ 的因子.

8. G 是有限群,p 是 $|G|$的最小素因子.证明 G 的指数为 p 的任意子群皆为正规子群.

习题答案与解答

1. 由§8 习题 13 的证明可得所要的结论.

2. 计算 V_4 在 S_4 中的全部陪集:

$V_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}=\overline{(1)}$,

$(1\ 2)V_4=\{(1\ 2),(3\ 4),(1\ 4\ 2\ 3),(1\ 3\ 2\ 4)\}=\overline{(1\ 2)}$,

$(1\ 3)V_4=\{(1\ 3),(2\ 4),(1\ 4\ 3\ 2),(1\ 2\ 3\ 4)\}=\overline{(1\ 3)}$,

$(2\ 3)V_4=\{(1\ 4),(2\ 3),(1\ 2\ 4\ 3),(1\ 3\ 4\ 2)\}=\overline{(2\ 3)}$,

$(1\ 2\ 3)V_4=\{(1\ 2\ 3),(1\ 3\ 4),(2\ 4\ 3),(1\ 4\ 2)\}=\overline{(1\ 2\ 3)}$,

$(1\ 3\ 2)V_4=\{(1\ 3\ 2),(1\ 4\ 3),(2\ 3\ 4),(1\ 2\ 4)\}=\overline{(1\ 2\ 3)}$.

作映射:

$S_4/V_4=\{\overline{(1)},\overline{(1\ 2)},\overline{(1\ 3)},\overline{(2\ 3)},\overline{(1\ 2\ 3)},\overline{(1\ 3\ 2)}\}\longrightarrow S_3$

$\overline{(1)}\longmapsto(1),\overline{(1\ 2)}\longmapsto(1\ 2),\overline{(1\ 3)}\longmapsto(1\ 3),\overline{(2\ 3)}\longmapsto(2\ 3),\overline{(1\ 2\ 3)}\longmapsto(1\ 2\ 3),\overline{(1\ 3\ 2)}\longmapsto(1\ 3\ 2)$.

易知这是双射,又显然是同态,故是同构.

另一法:考虑 S_4 在$\{\sigma_1=(1\ 2)(3\ 4),\sigma_2=(1\ 3)(2\ 4),\sigma_3=(1\ 4)(2\ 3)\}$上的共轭作用.于是 S_4 到$\{\sigma_1,\sigma_2,\sigma_3\}$上的置换群 S_3 有同态 π,可算出:

$$\pi((1\ 2))=\begin{pmatrix}\sigma_1&\sigma_2&\sigma_3\\ \sigma_1&\sigma_3&\sigma_2\end{pmatrix},\pi((1\ 3))=\begin{pmatrix}\sigma_1&\sigma_2&\sigma_3\\ \sigma_3&\sigma_2&\sigma_1\end{pmatrix},$$

$$\pi((2\ 3))=\begin{pmatrix}\sigma_1&\sigma_2&\sigma_3\\ \sigma_2&\sigma_1&\sigma_3\end{pmatrix},$$

$$\pi((1\ 2\ 3))=\begin{pmatrix}\sigma_1 & \sigma_2 & \sigma_3\\ \sigma_3 & \sigma_1 & \sigma_2\end{pmatrix},\pi((1\ 3\ 2))=\begin{pmatrix}\sigma_1 & \sigma_2 & \sigma_3\\ \sigma_2 & \sigma_3 & \sigma_1\end{pmatrix},$$

$$\pi((1))=\begin{pmatrix}\sigma_1 & \sigma_2 & \sigma_3\\ \sigma_1 & \sigma_2 & \sigma_3\end{pmatrix}.$$

故 π 是满射,又 V_4 是交换群,它的元共轭作用于 $\sigma_1,\sigma_2,\sigma_3$ 上是恒等变换,即 $V_4\leqslant\mathrm{Ker}\,\pi$.

由 $S_4/\mathrm{Ker}\,\pi\cong S_3$,知 $|\mathrm{Ker}\,\pi|=|V_4|=4$,故 $\mathrm{Ker}\,\pi=V_4$.

3. 群 G 共轭作用于 G 自身是内自同构,这就将群 G 映射到 $\mathrm{Aut}\,G$ 之中.设此映射为 π,共轭作用决定 π 是同态.又

$g\in\mathrm{Ker}\,\pi\Leftrightarrow g$ 的共轭作用是恒等变换$\Leftrightarrow$对 $\forall\ a\in G$,有 $g^{-1}ag=a\Leftrightarrow a\in Z(G)$.

即 $\mathrm{Ker}\,\pi=Z(G)$,这样 $G/Z(G)=G/\mathrm{Ker}\,\pi\cong G$ 在 π 下的象,是 $\mathrm{Aut}\,G$ 的子群.

若 $\mathrm{Aut}\,G$ 是循环群,则 G 的象,因而 $G/Z(G)$是循环群,再由§8 习题 18,G 是交换群,矛盾,故 $\mathrm{Aut}\,G$ 是非循环群.

4. 中学数学中已学过,任意非零复数 $z=re^{i\theta}$,$r\neq0$ 是 z 的绝对值,θ 是实数.作映射

$$\mathbf{C}^*=\mathbf{C}\setminus\{0\}\xrightarrow{\pi}\mathbf{R}^+(\text{正实数乘法群})$$
$$z=re^{i\theta}\longmapsto r,$$

这是满射,且是同态.$z\in\mathrm{Ker}\,\pi\Leftrightarrow z$ 的绝对值 $r=1$.故 $\mathrm{Ker}\,\pi=U$.即$\mathbf{C}^*/U\cong\mathbf{R}^+$.

5. 每个绝对值为 1 的复数 z 可写成 $z=e^{i2\pi\theta}$,$0\leqslant\theta<1$.以 U 记这种复数的乘法群.作映射

$$\mathbf{R}\xrightarrow{\eta}U$$
$$\underset{0\leqslant\theta<1,k\in\mathbf{Z}}{r}=k+\theta\longmapsto e^{i\theta2\pi}.$$

这是同态:对 $r_1+r_2=k_1+k_2+\theta_1+\theta_2$.若 $\theta_1+\theta_2<1$,则 $\eta(r_1+r_2)=e^{i2\pi(\theta_1+\theta_2)}=e^{i2\pi\theta_1}e^{i2\pi\theta_2}=\eta(r_1)\eta(r_2)$;若 $\theta_1+\theta_2=1+\theta$,$0\leqslant\theta<1$,$r_1+r_2=k_1+k_2+1+\theta$,$\eta(r_1+r_2)=e^{i2\pi\theta}=e^{i2\pi(1+\theta)}=e^{i2\pi(\theta_1+\theta_2)}=e^{i2\pi\theta_1}e^{i2\pi\theta_2}=\eta(r_1)\cdot\eta(r_2)$.又 $r\in\mathrm{Ker}\,\eta\Leftrightarrow e^{i2\pi\theta}=1\Leftrightarrow\theta=0\Leftrightarrow r\in\mathbf{Z}$,即 $\mathrm{Ker}\,\eta=\mathbf{Z}$.因此

$$\mathbf{R}/\mathbf{Z}=\mathbf{R}/\mathrm{Ker}\,\eta\cong U.$$

6. (1) $N=\mathrm{Ker}f=f^{-1}(\bar{e})$,$\bar{e}$是 G 的单位元.对 K 是 G 的子群,$\bar{e}\in K$,显然 $f^{-1}(K)\supseteq f^{-1}(\bar{e})=N$.

(2) 令 $H=f(H)$,我们证 $H=f^{-1}(H)$.显然 $H\subseteq f^{-1}(H)$.现证 $f^{-1}(H)\subseteq H$.对任 $k\in f^{-1}(H)$,则 $f(k)\in H=f(H)$.于是有 $h\in H$ 使 $f(h)=f(k)$,即得 $f(h^{-1}k)=\bar{e}$.故 $h^{-1}k\in N$.由于 $N\subseteq H$,而有 $h^{-1}k\in H$,$k\in hH=H$.因此

$H=f^{-1}(H)$.这说明 φ 是单射.

再证 φ 是满射.对任 H 是 G 的子群,来证 $f^{-1}(H)$是 G 的子群.对 h_1, $h_2\in f^{-1}(H)$, $f(h_1)$,$f(h_2)\in H$.故 $f(h_1h_2)=f(h_1)f(h_2)\in H$,就有 $h_1h_2\in f^{-1}(H)$,又对 $f(h_1)\in H$,$f(h_1)^{-1}=f(h_1^{-1})\in H$.因此 $h_1^{-1}\in f^{-1}(H)$.以上就证明了 $f^{-1}(H)$是 G 的子群.

由于 $\varphi(f^{-1}(H))=f(f^{-1}(H))=H$,$\varphi$ 是满射.因此 φ 是双射.

保持包含关系是明显的.

(3) 设 K 是 G 的正规子群.对 $k\in f^{-1}(K)$,有 $f(k)\in K$.$\forall g\in G$, $f(g^{-1}kg)=f(g)^{-1}f(k)f(g)\in K$.即 $g^{-1}kg\in f^{-1}(K)$,$f^{-1}(K)$是正规子群.由(1),它包含 N,且 $\varphi(f^{-1}(K))=K$.

又若 K 是 G 的正规子群,$\varphi(K)=f(K)$是 G 的子群.对 G 的任一元素.由 f是满同态,必是 G 的某元 g 的象 $f(g)$.任意 K 的元 k,$f(k)\in f(K)$ 有 $f(g)^{-1}f(k)f(g)=f(g^{-1}kg)$,由 K 是 G 的正规子群,$g^{-1}kg\in K$,于是 $f(g)^{-1}f(k)f(g)\in f(K)$.因此 $f(K)$是 G 的正规子群,这证明了 φ 引起

$$\{G\text{ 的包含 }N\text{ 的正规子群}\}\to\{G\text{ 的正规子群}\}$$

间的满射.由(2)φ 引起单射.故这映射也是双射.

(4) $G\xrightarrow{f}G\xrightarrow{\eta}G/H$,因 f,η 皆为满同态,故 ηf 也是满同态.$g\in G$, $(\eta f)(g)=\eta f(g)=f(g)H$.由此有

$$g\in\mathrm{Ker}(\eta f)\Leftrightarrow f(g)\in H\Leftrightarrow g\in f^{-1}(H).$$

即有 $\mathrm{Ker}(\eta f)=f^{-1}(H)$.由同态基本定理有

$$G/f^{-1}(H)\cong G/H$$

(5) 当 f 为自然同态 $\pi:G\to G/N$ 时,利用(2),(3),(4)的结论,就得到(5)所要的结论.

7. (1) $g\in G$,$\forall i$,$gx_iH=x_iH\Leftrightarrow\forall i$,$gx_i\in x_iH\Leftrightarrow\forall i$,$g\in x_iHx_i^{-1}\Leftrightarrow g\in\bigcap_{i=1}^{n}x_iHx_i^{-1}$.

(2) $\forall x\in x_iH$,有 $h\in H$ 使 $x=x_ih$,故 $xHx^{-1}=x_ihHh^{-1}x_i^{-1}=x_iHx_i^{-1}$. 因此

$$\bigcap_{x\in G}xHx^{-1}=\bigcap_{i=1}^{n}\bigcap_{x\in x_iH}xHx^{-1}=\bigcap_{i=1}^{n}x_iHx_i^{-1}.$$

§8 习题 7 已证$\bigcap_{x\in G}xHx^{-1}$是正规子群.

(3) $\forall g_1,g_2\in G$,$\varphi(g_1g_2)(x_iH)=g_1g_2x_iH=g_1(g_2x_iH)=\varphi(g_1)(\varphi(g_2)(x_iH))=(\varphi(g_1)\varphi(g_2))(x_iH)$.故 $\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)$,$\varphi$ 是同态.

(4) $\forall g_1,g\in G$,$\varphi(g)=\varphi(g_1)$当且仅当$\forall i$,$\varphi(g)(x_iH)=\varphi(g_1(x_iH)$即

$gx_iH=g_1x_iH$ 当且仅当 $\forall\, i, g_1x_i\in gx_iH$ 当且仅当 $\forall\, i, g_1\in g(x_iHx_i^{-1})$,即 $g_1=gk, k\in\bigcap_{i=1}^{n}x_iHx_i^{-1}$ 当且仅当 $g_1\in g\bigcap_{i=1}^{n}x_iHx_i^{-1}=g\bigcap_{x\in G}xHx^{-1}$.

(5) 作映射

$$G\overset{\varphi}{\longrightarrow}S_n(M\text{ 中 }n\text{ 个元的置换})$$
$$g\longmapsto\varphi(g):x_iH\longmapsto gx_iH,\ i=1,2,\cdots,n.$$

$g\in\mathrm{Ker}\varphi$ 当且仅当 $\varphi(g)=\varphi(e)$ 当且仅当 $g\in\bigcap_{x\in G}xHx^{-1}$.即 $\mathrm{Ker}\varphi=\bigcap_{x\in G}xHx^{-1}$.

由同态基本定理

$$G/\bigcap_{x\in G}xHx^{-1}\cong\varphi(G)(\text{是 }S_n\text{ 的子群})$$

其同构映射是 $g\bigcap_{x\in G}xHx^{-1}\longmapsto\varphi(g)$.

(6) $\bigcap_{x\in G}xHx^{-1}$ 是同态核,当然是 G 的正规子群,又含于 H 中.且

$$G/\bigcap_{x\in G}xHx^{-1}\cong\varphi(G)$$

故 G 对此正规子群的指数等于 $\varphi(G)$ 的阶.但 $\varphi(G)$ 是 S_n 子群,它的阶是 $|S_n|=n!$ 的因子.

8. 设 G 的子群 H 满足 $[G:H]=p$.上题已证 $G:\bigcap_{x\in G}xHx^{-1}$ 是 $p!$ 的因子,但

$$G:\bigcap_{x\in G}xHx^{-1}=[G:H]\ H:\bigcap_{x\in G}xHx^{-1}=p\ H:\bigcap_{x\in G}xHx^{-1},$$

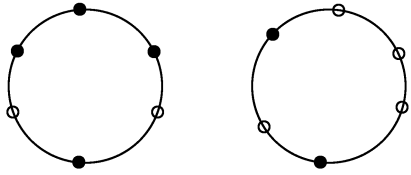
它需为 $p!$ 的因子,则 $H:\bigcap_{x\in G}xHx^{-1}$ 是 $(p-1)!$ 的因子.它又是 $|G|$ 的因子,则 $|G|$ 中最小素因子为 p,因此 $H:\bigcap_{x\in G}xHx^{-1}=1$.这证明了 $H=\bigcap_{x\in G}xHx^{-1}$ 是正规子群.

§11 轨道数的定理及其在计数问题中的应用

习 题

以下习题中打 * 者为必作题,其余为选作题.

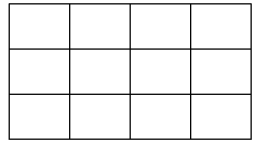
*1. 在一个圆手镯上串上六粒珠子,珠子可任意染白色或黑色.问能作出几种式样的手镯?(下图中列出两种式样的例子)



*2. 在一个正四面体的顶点上任意染黑色或白色,能作出几种式样?

*3. 将课文例 2 中的问题计算出答案.

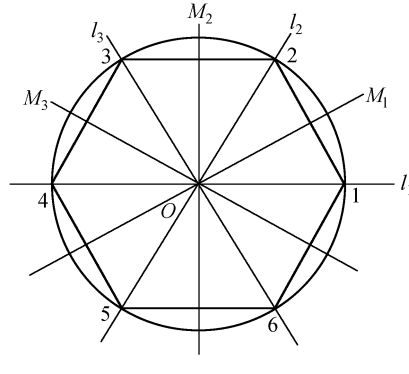
4. 下面图中,矩形板上有 12 个同样的矩形格子.将其中 5 个染红色,7 个染黄色.问能作出几种图板?若矩形板换成白布.将格子的正反面都染成同一颜色,五个染红色,7 个染黄色.问能染成几种图样?



5. 把 3 个红球,4 个白球,2 个篮球共 10 个球分成三堆,问有多少种分法?

习题答案与解答

1. 不妨把六个珠子放在手镯上的一个正六角形的顶点上.把绕 O 旋转 $0°$,$60°$,$120°$,$180°$,$240°$,$300°$ 的变换记为 T_0,T_1,T_2,T_3,T_4,T_5,把平面对直线 l_1,l_2,l_3,M_1,M_2,M_3 的反射变换记为 S_1,S_2,S_3,R_1,R_2,R_3.它们组成正六角形的对称性群 G.把六个珠子所有允许的串法(只许黑、白两色)组成集合 M.手镯经旋转 T_0,T_1,T_2,T_3,T_4,T_5 把一种串法变成另一种串法,这两种串法当然构成同一式样.而用六种反射之一将一种串法变成另一种串法相当于从背面去看手镯,这仍然构成同一式样.因此集合 M 中在群 G 作用下属同一轨道的串法是同一式样.故手镯的式样数等于 M 在 G 作用下的轨道数.



下面计算 G 的每个元在 M 上的不动点数.与课文中的例 1 类似可算出:

T_0 固定 M 中 64 种串法.

T_1,T_5 固定全黑,全白两种串法.

T_3 固定的串法中，顶点 1，4 上，顶点 2，5 上，顶点 3，6 上颜色分别相同．共有 8 种串法．

T_2，T_4 固定的串法中，顶点 1，3，5 上，顶点 2，4，6 上颜色分别相同．共有 4 种串法．

S_1 能固定的串法中顶点 2，6 上，顶点 3，5 上分别有相同颜色，顶点 1，4 上可任取颜色，共 16 种串法．同样地，S_2，S_3 也固定 16 种串法．

R_1 能固定的串法中，顶点 1，2 上，顶点 3，6 上，顶点 4，5 上分别有相同颜色．共 8 种串法、同样 R_2，R_3 也固定 8 种串法．

由 Burnside 定理，M 在群 G 作用下的轨道数也即在允许串法下手镯的式样数为

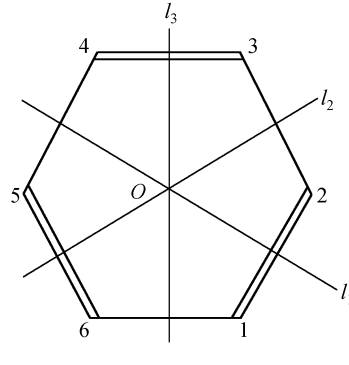
$$\frac{1}{12}(64+2\times2+8\times1+4\times2+16\times3+8\times3)=\frac{156}{12}=13(\text{种}).$$

2．正四面体的对称性群是顶点上的全体置换的群 S_4．令正四面体顶点上全体允许的着色法的集合为 M．下面计算 S_4 的各置换在 M 中的不动点数．

恒等置换(1)固定 M 中每种着色法．因每个顶点有黑白两种选择，四个顶点皆着色共有 2^4 种方法．

(1 2)固定的着色法在顶点 1，2 上有相同颜色，顶点 3，4 上可任意选择黑，白．共有 2^3 种方法．S_4 中有 6 个对换，都与(1 2)一样地固定 2^3 种着色方法．

(1 2)(3 4)它固定的着色方法在顶点 1 2 上和顶点 3，4 上分别有相同颜色，共有 2^2 种方法，同样(1 3)(2 4)，(1 4)(2 3)也固定 2^2 种着色方法．



(1 2 3)固定的着色法在顶点 1，2，3 上有相同颜色，顶点 4 上可任意选择黑，白．共有 2^2 种方法．同样地，S_4 中所有的三轮换(共 8 个)都固定 2^2 种着色方法．

(1 2 3 4)固定全着黑色和全着白色共两种方法．所有四轮换(共 6 个)都固定两种着色法．

正四面体顶点允许的着色方案的数目为：

$$\frac{1}{24}(16+6\times8+3\times4+8\times4+6\times2)=5(\text{种}).$$

3．这时的群 G 是由绕中心 O 旋转 0°，120°，240°的变换 T_0，T_1，T_2 及平面对直线 l_1，l_2，l_3 的反射 S_1，S_2，S_3 组成．令在 6 个顶点上任意配置 H 或 CH_3 的方法的集合为 M．则 G 在 M 上有群作用．在 G 作用下可以互变的配置方法作

出的化合物是相同的.故能得到的化合物的数目为 M 在 G 作用下的轨道数.现计算 G 的元在 M 上的不动元的数目.

T_0 固定 M 中每种配置方法,共 2^6 种.

T_1 固定的配置方法中须在顶点 1,3,5 上,顶点 2,4,6 上配置分别相同,故有四种方法.

T_2 与 T_1 在 M 中有同样多的不动元.

S_1 固定的配置方法必须在顶点 1,2 上,顶点 3,6 上,顶点 4,5 上配置分别相同.故有 8 种配置方法.S_2,S_3 也固定 8 种方法.

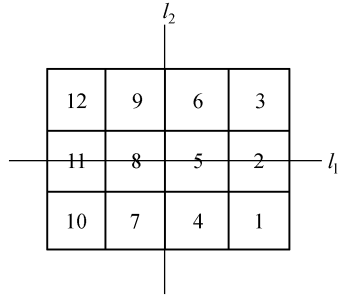
由 Burnside 定理,G 在 M 上的轨道数也即能作成的化合物数目为

$$\frac{1}{6}(2^6+2^2+2^2+2^3+2^3+2^3)=16(\text{种})$$

4. 第一种情形是板的反面没有图案,这问题中的群 G 由绕矩形中心旋转 0°及 180°的变换 T_0,T_1 组成.矩形板的图案数等于矩形板的允许染色法的集合 M 在 G 作用下的轨道数.先计算 G 的元在 M 中的不动元的数目.

T_0 固定全部的 M 中染色法.共 $C_{12}^5=792$ 种.

T_1 固定的染色法须在方格 1,12 上,方格 3,10 上,方格 4,9 上,方格 6,7 上,方格 5,8 上,方格 2,11 上分别有相同颜色.这是不允许的染色法,故 T_1 在 M 上没有不动元.



由 Burnside 定理,矩形板的图案数即 G 在 M 上的轨道数$=\frac{1}{2}(792+0)=396$(种).

第二种情形是板的正反面同样地染色.问题中 M 与第一情形一样.群 G 除了前面的 T_0,T_1 外还有矩形板绕 l_1 及 l_2 的旋转 180°的变换 S_1,S_2.

T_0 在 M 中的不动元有 792 个.

T_1 在 M 中的不动元数目为 0.

S_1 的不动元在方格 12,10 上,在方格 4,6 上,在方格 9,7 上,在方格 3,1 上分别有相同颜色,而在方格 2,5,8,11 上可任意选择颜色.有两种情形:

(i) 在方格 2,5,8,11 上有一格选黄色,而上面四对方格上选两对为黄色,共有 $C_4^1C_4^2=4\times6=24$ 种方法.

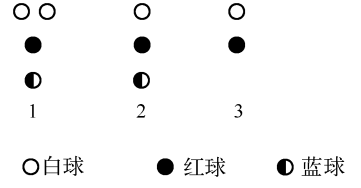
(ii) 在方格 2,5,8,11 上选三个黄色,在上面 4 对方格上选一对为黄色,共有 $C_4^3C_4^1=4\times4=16$ 种.

故 S_1 在 M 中的不动元数目为 40.

易计算 S_2 在 M 中没有不动元.结果矩形板(反面染同样颜色)的图案数为 $\frac{1}{4}(792+40)=208$(种).

5. 给三个堆编号为 1,2,3.这九个球在三个堆上的分配方法的集合为 M. 右图是分配方法的一个例子.群 G 是三个堆的置换作成的群.两个分配方法如能经 G 的元素互变,应为同一种分配方案.

先计算 $|M|$,它即为恒等置换在 M 中的不动元的数目.分别计算篮,红,白球在三个堆上的分配方法数.回忆,n 个东西放在 m 个抽屉中的方法数为 C_{n+m-1}^{m-1}.故篮球的分配方法数$=C_{2+2}^{2}=6$;红球的分配方法数$=C_{3+2}^{2}=10$;白球的分配方法数为 $C_{4+2}^{2}=15$.故三种球分配到三个堆上的方法数为 $6\times10\times15=900$.



(1 2) 固定的方法中篮球的分配方法只能在第三堆上放两个篮球或不放篮球,即两种;红球在第三堆上放 1 个或放三个,也是两种;白球在第三堆上放 2 个或 4 个或不放,共有三种.故(12)固定的方法共 $2\times2\times3=12$(种).

同样(1 3),(2 3)也固定 12 种.

(1 2 3)固定的方法中各球在三堆上的数目应相同,故它在 M 中没有不动元.同样(1 3 2)也没有.

结果三种球分成三堆,不相同的分配方案的数目即 G 在 M 上的轨道数为 $\frac{1}{3!}(900+3\times12+2\times0)=156$(种).

第二章　域　和　环

内容要点

1. 基本概念:域、子域、扩域、域的特征、素域.环、子环、理想、商环、同态、同构、同态基本定理.整环、极大理想.

2. 商环的应用例子:爱森斯坦判别法的证明(整数环上多项式性质的证明)可化归到整数环的剩余类域上.

3. 新域或新环的构造:复数域(作为实数域R上使 $x^2+1=0$ 有根的最小扩域);二元域;集合 S 在域 F 上生成的扩域;商环、剩余类环 $F[x]/(f(x))$(包括构造 F 上添加任意不可约多项式 $f(x)$ 的一个根的扩域)、$\mathbf{Z}/(n)$(包括构造 p 个元素的域);理想的和、积;环的直和;整环的分式域.

4. 域扩张的初步知识:代数扩张、有限扩张、单代数扩张、单超越扩张.

集合 S 在 F 上生成的扩域的三种刻画:

$$F(S)=\left\{\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_t)}{f_2(\alpha_1,\alpha_2,\cdots,\alpha_t)}\,\middle|\,\begin{array}{l}\forall\, t\in\mathbf{N}\text{(自然数)},\forall\,\alpha_1,\alpha_2,\cdots,\alpha_t\in S,\\ \forall\, f_i(x_1,x_2,\cdots,x_t)\in F[x_1,x_2,\cdots,x_t],i=1,2.\\ f_2(\alpha_1,\alpha_2,\cdots,\alpha_t)\neq 0\end{array}\right\}$$

$=$由 F 及 S 的元尽可能地多次作加减乘除所得的元素的集合

$=$含 F 及 S 的最小的域.

单扩张的构造:

$$F(\alpha)=\left\{\frac{f_1(\alpha)}{f_2(\alpha)}\,\middle|\,\forall\, f_1(x),f_2(x)\in F[x],f_2(\alpha)\neq 0\right\}.$$

若 α 为 F 上代数元,$f(x)$ 是以 α 为根的 F 上不可约多项式(α 的极小多项式),其次数为 n,则 $F(\alpha)$ 是 F 上 n 维线性空间,而 $1,\alpha,\cdots,\alpha^{n-1}$ 是它的一组基.

扩张次数$[E:F]$及性质:对域扩张 $E\supset H\supset F$ 有$[E:F]=[E:H][H:F]$.

5. 域的应用举例:(1) 二元域用于纠错码.(2) 域的扩张次数的性质用于否定三大几何作图难题(给出了用圆规直尺作图作出的量满足的条件).

6. 中国剩余定理.

读后注

1. 这一章讲域、环的基本概念.主要是讲各种造新域和新环的方法,环是为

域起铺垫的作用.本章的内容充分体现总导引第一点中的思想.

2. 体会造二元域的数学背景及如何用于构造纠一个错的码.思考一下能纠错的关键之点在哪里,随便指定一个矩阵 H 是否能起到纠错的作用?

3. 体会对圆规直尺作图问题进行分析中的几个步骤:(1)用解析几何知识分析出能用圆规直尺作图作出的量(长度)满足的方程;(2)用扩域的语言表达上述作出的量所在的范围;(3)用扩张次数的性质来表达作出的量满足的条件.

4. 这一章中我们充分地应用了引论章§2末尾的定理.即用了一般域上线性方程组、矩阵运算、线性空间、多项式等理论的大量性质.促进读者巩固高等代数的知识.

5. 与其它近世代数教材相比,本书中域的内容(包括下一章的有限域的内容)放到整环的因式分解唯一性理论之前,并且替代它而成为教材的核心部分.内容也改变很多,加入纠错码的例子和三大几何作图难题的讨论这些应用内容,而舍去了可分扩张及分裂域等内容.由于目标明确(参看总导引第一条)且有应用内容,增加了学习的生动性.

思考练习题(非必作题)

(1)造一个码长13,容量为 2^9 的能纠一个错的码集合.

(2)证明上面的码一般不能纠两个错.(举例:考察码子 $X=(0,0,0,0,0,0,0,0,0,0,0,0,0)^{\mathrm{T}}$ 错了两位成为 $Y=(1,1,0,0,0,0,0,0,0,0,0,0,0)^{\mathrm{T}}$.能否用书中所述的译码方法由 Y 恢复成 X?

§1 域的例子,复数域及二元域的构造,对纠一个错的码的应用

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. 令

$$\mathrm{C}_0=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a,b\in\mathrm{R}\right\},$$

则(1)C_0 对矩阵的加法和乘法成为域.

(2)C_0 中 $\mathrm{R}_0=\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a\in\mathrm{R}\right\}$ 是同构于R的子域.

(3) 干脆将R_0与R等同,将 $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ 写成 a,则可写

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = a + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

作映射

$$\begin{array}{ccc} C & \overset{\varphi}{} & C_0 \\ a+bi & \longmapsto & a+b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{array}, \forall\ a,b\in R,$$

则 φ 是域同构.

以下2—6题出现的运算是 F_2 中元素的运算.

*2. 计算

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

*3. 求

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}^{-1}.$$

*4. 解方程组

$$\begin{aligned} x_1+x_2+x_3+x_4+x_5+x_6 &= 1 \\ x_3+x_4+0+x_6 &= 0 \\ x_1+x_2+0+x_4 &= 1 \\ x_2+x_3+x_4 &= 0. \end{aligned}$$

*5. 计算

$$(x^4+x^3+x+1)^2,(x^3+x^2+1)(x^5+x^2+x+1).$$

*6. (1) 以 x^2+x+1 除 $x^6+x^4+x^3+1$,求商及余式.

(2) 求 x^2+x+1 与 $x^6+x^4+x^3+1$ 的最大公因式 $d(x)$.

(3) 求 $u(x),v(x)$,使

$$u(x)(x^2+x+1)+v(x)(x^6+x^4+x^3+1)=d(x).$$

* 7. 求作一个 13 位 0,1 序列的码集合,其容量为 2^9,有纠一个错的能力.

8. F 为素数特征 p 的域,$a,b,a_1,\cdots,a_n\in F$,则

(1) $(a+b)^p=a^p+b^p$,而且无论 p 为奇偶皆有 $(a-b)^p=a^p-b^p$.

(2) $(a+b)^{p^k}=a^{p^k}+b^{p^k}$.

(3) $(a_1+a_2+\cdots+a_n)^{p^k}=a_1^{p^k}+a_2^{p^k}+\cdots+a_n^{p^k}$.

(参见引论章习题 6)

(4) 映射 $\begin{array}{ccc} F & \overset{\varphi}{} & F, \\ a & \longmapsto & a^p \end{array}$

是 F 的自同态.且 φ 是同构当且仅当方程 $x^p-b=0$ 对所有 $b\in F$ 都有解.

习题答案与解答

1. 略.

2. $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

3. $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

4. $x_1=x_5+x_6+1$

$x_2=x_6+1$

$x_3=x_5+x_6$

$x_4=x_5+1$.

5. $x^8+x^6+x^2+1,x^8+x^7+x+1$.

6. (1) $x^6+x^4+x^3+1=(x^4+x^3+x^2+x)(x^2+x+1)+x+1$.

(2) $(x^6+x^4+x^3+1,x^2+x+1)=1$.

(3) $x(x^6+x^4+x^3+1)+(x^5+x^4+x^3+x^2+1)(x^2+x+1)=1$.

7. 令 $H=\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}_{4\times 13}$,

以 $HX_{13\times 1}=0$ 的解空间为码集.因秩 $H=4$,未知数的数目为 13,故解空间维数为 13−4=9.由于码集合是 F_2 上 9 维空间,共有 2^9 个解向量,即 2^9 个码子,码

集合的容量为 2^9.与课文中例 4 一样有纠一个错的能力.

8.(1) 由二项定理(参见引论章习题 6),

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} C_p^i a^i b^{p-i}.$$

当 $1 \leqslant i \leqslant p-1$ 时,

$$C_p^i = \frac{p(p-1)\cdots 2\cdot 1}{(p-i)!\,i!}.$$

而 $(p-i)!$ 及 $i!$ 中的素因子皆小于 p,故 $p \mid C_p^i$.题设 F 的特征为 p,故 $\sum_{i=1}^{p-1} C_p^i a^i b^{p-i} = 0$.这证明了

$$(a+b)^p = a^p + b^p.$$

对 $(a-b)^p = a^p + (-b)^p = a^p + (-1)^p b^p$.当 p 为奇素数时,$(-1)^p = -1$;当 $p=2$ 时,$(-1)^2 = 1 = -1$.故

$$(a-b)^p = a^p - b^p.$$

(2) $(a+b)^{p^k} = ((a+b)^p)^{p^{k-1}} = (a^p + b^p)^{p^{k-1}}$.利用归纳法可得 $(a+b)^{p^k} = (a^p)^{p^{k-1}} + (b^p)^{p^{k-1}} = a^{p^k} + b^{p^k}$.

(3) $(a_1 + a_2 + \cdots + a_n)^{p^k} = a_1^{p^k} + (a_2 + \cdots + a_n)^{p^k}$.利用归纳法可得 $(a_1 + \cdots + a_n)^{p^k} = a_1^{p^k} + a_2^{p^k} + \cdots + a_n^{p^k}$.

(4) $\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$.$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$.故 φ 为 F 的自同态.又 $\varphi(a-b) = (a-b)^p = a^p - b^p = \varphi(a) - \varphi(b)$,就有 $\varphi(a) = \varphi(b)$ 当且仅当 $a = b$.即 φ 是单射.

由以上论证,φ 是同构当且仅当 φ 是满射当且仅当对 $\forall\, b \in F$,有 $a \in F$ 使 $\varphi(a) = a^p = b$ 也即方程 $x^p - b = 0$ 有解.

§2 域的扩张,扩张次数,单扩张的构造

习 题

以下习题中打 * 者为必作题,其余为选作题.

1. $F \subset E$ 是域扩张.

(1) $\alpha_1, \alpha_2, \cdots, \alpha_s \in E$,则

$$F(\alpha_1, \alpha_2, \cdots, \alpha_s) = \left\{ \frac{f_1(\alpha_1, \cdots, \alpha_s)}{f_2(\alpha_1, \cdots, \alpha_s)} \,\middle|\, f_1, f_2 \in F[x_1, \cdots, x_s], f_2(\alpha_1, \cdots, \alpha_s) \neq 0 \right\}.$$

(2) $S\subset E$,则

$$F(S)=\bigcup_{\substack{S_0\subset S\\ S_0\text{有限集}}}F(S_0).$$

*2. 计算$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$,$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$.证明

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

*3. $F\subset E$ 是域扩张,且$[E:F]=p$ 是素数,则任意 $\alpha\in E\setminus F$,有 $E=F(\alpha)$.

*4. $E\supset F$ 为域扩张,$\alpha_1,\alpha_2,\cdots,\alpha_t\in E$,$[F(\alpha_i):F]=n_i$,$i=1,2,\cdots,t$,则 $[F(\alpha_1,\cdots,\alpha_t):F]\leqslant n_1n_2\cdots n_t$.

*5. $F\subset E$ 为有限次域扩张,则必为代数扩张.

*6. $F\subset E$ 为有限次域扩张,则有 $\alpha_1,\cdots,\alpha_t\in E$,使得 $E=F(\alpha_1,\cdots,\alpha_t)$.

7. $F\subset E$ 为域扩张,$S\subset E$ 且 S 中每个元皆是 F 上代数元,则 $F(S)$是 F 上代数扩张.进而,E 中全部代数元作成 F 的一个扩域.

*8. 令 $E=\mathbb{Q}(u)$.

(1) 设 $u^3-u^2+u+2=0$.试把$(u^2+u+1)(u^2-u)$和$(u-1)^{-1}$表成 au^2+bu+c 的形式,$a,b,c\in\mathbb{Q}$.

(2) 若 $u^3-2=0$,把$\frac{u+1}{u-1}$表成 au^2+bu+c 的形式,$a,b,c\in\mathbb{Q}$.

9. 令 $E=F(u)$,u 是极小多项式为奇数次的代数元.证明 $E=F(u^2)$.

10. 求$\sqrt[3]{2}+\sqrt{5}$在$\mathbb{Q}$ 上的极小多项式.

11. $E\supset F$,E 是环,F 是域,$s\in E$ 是 F 上代数元,则 s 可逆当且仅当有 F 上多项式 $f(x)$,其常数项不为零使 $f(s)=0$.并且 $s^{-1}=g(s)$,$g(x)$是 F 上多项式.

12. E 是 F 上的代数扩张,则 E 的含 F 的子环都是子域.

13. 设$[E:F]=n$,则不存在子域 G,使 $E\supset G\supset F$ 及$[G:F]$与 n 互素.

*14. $\mathbb{R}$(实数域)上任意代数扩张 E 若不为$\mathbb{R}$,则同构于$\mathbb{C}$.特别地,$\mathbb{R}$ 上除二次扩域外没有其它有限次扩域.(这正是 Hamilton 等数学家找不到“三维复数”的原因).

习题答案与解答

1. (1) 这几令 $S=\{\alpha_1,\cdots,\alpha_s\}$,按命题 2 下面一段的约定 $F(\alpha_1,\alpha_2,\cdots,\alpha_s)$就是 $F(S)$.命题 1 中的(2)式定义了 $F(S)$.易看出本题所设的集合与 $F(S)$的定义集合是一致的.

(2) 比较(1)的结果和命题 1 中(2)式在一般集合 S 下 $F(S)$的定义即得

$$F(S)=\{F(\alpha_1,\cdots,\alpha_k)\mid\forall\{\alpha_1,\alpha_2,\cdots,\alpha_k\}\subset S\}$$

$$= \bigcup_{\substack{S_0 \subset S \\ S_0 \text{有限集}}} F(S_0).$$

2. 易看出

$$Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2})(\sqrt{3}) = \{(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})\sqrt{3} \mid a_i, b_i \in Q\}.$$

我们来证 $1,\sqrt{3}$ 在 $Q(\sqrt{2})$ 上是线性无关的. 设 $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})\sqrt{3} = 0$, 若 $a_2 + b_2\sqrt{2} \neq 0$, 则

$$\sqrt{3} = \frac{-a_1 - b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} \in Q(\sqrt{2}).$$

令 $\sqrt{3} = a + b\sqrt{2}$, $a, b \in Q$. 将两边平方, 得到 $3 = a^2 + 2ab\sqrt{2} + b^2$. 因 $\sqrt{2}$ 不是有理数, 则 a, b 之一为零. 若 $a = 0$, 则 $3^2 = 2b^2 = \frac{2q^2}{p^2}$, $(p, q) = 1$. 又因左边为整数, 必须 $p^2 \mid 2$, 只能 $p = 1$, 由 $3^2 = 2q^2$, 必须 $2 \mid 3^2$, 这也不可能. 若 $b = 0$, 则 $3 = a^2$, $\sqrt{3} = a$ 是有理数, 这也不可能. 这些矛盾推出 $a_2 + b_2\sqrt{2} = 0$, $a_1 + b_1\sqrt{2}$ 也就为零, 说明 $1,\sqrt{3}$ 在 $Q(\sqrt{2})$ 上线性无关. 因而 $[Q(\sqrt{2})(\sqrt{3}) : Q(\sqrt{2})] = 2$. 结果

$$[Q(\sqrt{2})(\sqrt{3}) : Q] = [Q(\sqrt{2})(\sqrt{3}) : Q(\sqrt{2})][Q(\sqrt{2}) : Q] = 2 \times 2 = 4.$$

再证 $[Q(\sqrt{2}+\sqrt{3}) : Q] = 4$. 这只要证 $Q(\sqrt{2})(\sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$. 首先显然有 $Q(\sqrt{2}+\sqrt{3}) \subseteq Q(\sqrt{2},\sqrt{3})$. 又从 $\sqrt{3} - \sqrt{2} = \frac{1}{\sqrt{2}+\sqrt{3}}$ 得 $\sqrt{3} = \frac{1}{2}(\sqrt{3} - \sqrt{2} + \sqrt{3} + \sqrt{2}) = \frac{1}{2}\left(\frac{1}{\sqrt{3}+\sqrt{2}} + \sqrt{3} + \sqrt{2}\right) \in Q(\sqrt{2}+\sqrt{3})$. 同样可得 $\sqrt{2} \in Q(\sqrt{2}+\sqrt{3})$. 这就证明了 $Q(\sqrt{2},\sqrt{3}) \subseteq Q(\sqrt{2}+\sqrt{3})$. 于是 $Q(\sqrt{2},\sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$.

3. $[F(\alpha) : F] \mid [E : F]$, $[E : F] = p$. 故 $[F(\alpha) : F] = 1$ 或 p. 但 $\alpha \in E \setminus F$, $[F(\alpha) : F] > 1$. 故 $[F(\alpha) : F] = p$. 因此 $F(\alpha) = E$.

4. $[F(\alpha_1, \cdots, \alpha_t) : F] = [F(\alpha_1, \cdots, \alpha_t) : F(\alpha_1, \cdots, \alpha_{t-1})][F(\alpha_1, \cdots, \alpha_{t-1}) : F(\alpha_1, \cdots, \alpha_{t-2})] \cdots [F(\alpha_1) : F]$. 由于 α_i 在 F 中的极小多项式次数为 n_i. F 上的这个极小多项式也是 $F(\alpha_1, \cdots, \alpha_{i-1})$ 中的多项式, 这个次数 n_i 比 α_i 在 $F(\alpha_1, \cdots, \alpha_{i-1})$ 上的极小多项式的次数低. 故 $[F(\alpha_1, \cdots, \alpha_{i-1}, \alpha_i) : F(\alpha_1, \cdots, \alpha_{i-1})] \leqslant n_i$. 因而 $[F(\alpha_1, \cdots, \alpha_t) : F] \leqslant n_t n_{t-1} \cdots n_1 = n_1 n_2 \cdots n_t$.

5. $F \subseteq E$ 是 k 次扩张. 任一元 $\alpha \in E$, $1, \alpha, \cdots, \alpha^k$ 是 E 中 $k+1$ 个元, 必在 F 上线性相关. 即有 F 上不全为零的 $a_0, a_1, \cdots, a_k$ 使 $a_0 + a_1\alpha + \cdots + a_k\alpha^k = 0$. 由此知 α 满足 F 上的次数 $\leqslant k$ 的一个多项式. 故 α 是 F 上代数元, 因而 E 是 F 上代数扩张.

6. 取 E 的 F 基 $\alpha_1, \cdots, \alpha_t$, 则 $E = \sum_{i=1}^{t} l_i\alpha_i \mid l_i \in F \subseteq F(\alpha_1, \cdots, \alpha_t) \subseteq E$,

故 $E=F(\alpha_1,\cdots,\alpha_t)$.

7. 设 S 中每个元皆为 F 上代数元.对 $\alpha\in F(S)$,必有 $\alpha_1,\cdots,\alpha_k\in S$ 使 $\alpha=\frac{f_1(\alpha_1,\cdots,\alpha_k)}{f_2(\alpha_1,\cdots,\alpha_k)}\in F(\alpha_1,\cdots,\alpha_k)$.因 α_i 为代数元,令$[F(\alpha_i):F]=n_i$.由习题 4,$[F(\alpha_1,\cdots,\alpha_k):F]\leqslant n_1n_2\cdots n_k$.故 $F(\alpha_1,\cdots,\alpha_k)$是 F 上有限扩张,再由习题 5,它是 F 上代数扩张.这就证明了任意 $\alpha\in F(S)$是 F 上代数元,于是 $F(S)$也是 F 上代数扩张.

现令 E 中全体 F 上代数元的集合为 S.则 $F(S)$是代数扩张,$F(S)$中每个元皆为 F 上代数元.于是 $F(S)\subseteq S$,即有 $S=F(S)$.故 S 是 F 上扩域.

8.(1) $(u^2+u+1)(u^2-u)=u^4-u=(u+1)(u^3-u^2+u+2)-4u-2=-4u-2$.

由于$(u-1)(u^2+1)-(u^3-u^2+u+2)=3$,故$(u-1)(u^2+1)=3$.因此$(u-1)^{-1}=\frac{1}{3}(u^2+1)$.

(2) 由$(u-1)(u^2+u+1)=u^3-1=(u^3-2)+1=1$,故$\frac{u+1}{u-1}=(u+1)\cdot(u^2+u+1)=u^3+2u^2+2u+1=(u^3-2)+2u^2+2u+3=2u^2+2u+3$.

9. 设 $u^2=a\in F(u^2)$,则 $u^2-a=0$.故$[F(u):F(u^2)]\leqslant 2$.因$[F(u):F(u^2)]\mid[F(u):F]$,及$[F(u):F]=$奇数,$[F(u):F(u^2)]\neq 2$.所以$[F(u):F(u^2)]=1$,即 $E=F(u)=F(u^2)$.

另一证法,设 u 在 F 中极小多项式是$f(x)$.$f(x)$为 $2l+1$ 次,满足 $f(u)=0$,设为

$$a_{2l+1}u^{2l+1}+a_{2l}u^{2l}+\cdots+a_1u+a_0=0,a_i\in F,$$

则

$$u(a_{2l+1}u^{2l}+a_{2l-1}u^{2(l-1)}+\cdots+a_1)+(a_{2l}u^{2l}+\cdots+a_0)=0.$$

由 $f(x)$的极小性,第一括弧不为零,所以

$$u=\frac{a_{2l}u^{2l}+a_{2(l-1)}u^{2(l-1)}+\cdots+a_0}{a_{2l+1}u^{2l}+a_{2l-1}u^{2(l-1)}+\cdots+a_1}\in F(u^2).$$

故 $F(u)=F(u^2)$.

10. 令 $u=\sqrt[3]{2}+\sqrt{5}$.则$\sqrt[3]{2}=u-\sqrt{5}$,$(u-\sqrt{5})^3=2$.于是 $u^3-3\cdot u^2\cdot\sqrt{5}+3u(\sqrt{5})^2-(\sqrt{5})^3=u^3+15u-(3u^2+5)\sqrt{5}=2$.移项后得 $u^3+15u-2=(3u^2-5)\sqrt{5}$.两边平方,得到$(u^3+15u-2)^2=(3u^2-5)^2\cdot 5$.这是 u 满足的Q 上 6 次方程,故$[Q(u):Q]\leqslant 6$.

又$(u-\sqrt{5})^3=2$,可得 $\sqrt{5}\in Q(u)$.由$[Q(\sqrt{5}):Q]=2$,及$[Q(\sqrt{5}):Q]\mid[Q(u):Q]$,知$2\mid[Q(u):Q]$.而由$\sqrt[3]{2}=\sqrt{5}-u$ 知$\sqrt[3]{2}\in Q(u,\sqrt{5})=Q(u)$.又

$[Q(\sqrt[3]{2}):Q]=3$ 及 $[Q(\sqrt[3]{2}):Q]\mid[Q(u):Q]$，得 $3\mid[Q(u):Q]$．于是 $6\mid[Q(u):Q]$，因而 $[Q(u):Q]=6$．由于 $(u^3+15u-2)^2-(3u^2-5)^2\cdot 5=0$，故 6 次多项式 $(x^3+15x-2)^2-5(3x^2-5)^2$ 是 u 在 Q 上的极小多项式．

11．设 s 为可逆的代数元，则有 F 上多项式 $f(x)$，使

$$f(s)=a_k s^k+a_{k-1}s^{k-1}+\cdots+a_1 s+a_0=0,$$

其中 $k\geqslant 1$，$a_k\neq 0$．设 $a_0,a_1,\cdots,a_{k-1},a_k$ 中不为零的最小脚标为 i．则 $i\neq k$，否则 $a_k s^k=0$，由 s 可逆，得 $a_k=0$．矛盾．故 $i<k$．用 s^{-i} 乘它，则得 $a_k s^{k-i}+\cdots+a_i=0$．于是 $g(x)=a_k x^{k-i}+\cdots+a_i$ 满足 $g(s)=0$ 且常数项 $a_i\neq 0$．反之，设 s 满足某多项式方程

$$f(s)=a_k s^k+\cdots+a_1 s+a_0=0,$$

且 $a_0\neq 0$．令 $g(x)=-(a_k x^{k-1}+\cdots+a_1)$，则

$$g(s)\cdot s=a_0\neq 0.$$

故 $s^{-1}=\frac{1}{a_0}g(s).\frac{1}{a_0}g(x)$ 是 F 上多项式．

12．设 $E\supset H$ 是含 F 的子环．任取 $0\neq s\in H$．s 在 E 中有逆，由习题 11 知，$s^{-1}=g(s)$，$g(x)$ 是 F 上多项式．H 是子环，因此 $g(s)\in H$．故 H 是 E 的子域．

13．设 G 是域，使 $E\supsetneq G\supsetneq F$．则 $[G:F]\mid[E:F]$，故 $[G:F]$ 不能与 $n=[E:F]$ 互素．

14．设 $R\subset E$ 是代数扩张．任取 $\alpha\in E$，α 是 R 上不可约多项式 $f(x)$ 的根．R 上只有 1 次或 2 次不可约多项式．若为 1 次，则 $\alpha\in R$．若 E 中有 $\alpha\overline{\in}R$，则它是 R 上 2 次不可约多项式的根，设 α 满足 $\alpha^2+b\alpha+c=0$，$b,c\in R$．则 $\left(\alpha-\frac{b}{2}\right)^2=\frac{1}{4}(b^2-4c)$．因 $\alpha\overline{\in}R$，故 $b^2-4c<0$．因此 $\sqrt{b^2-4c}=\sqrt{4c-b^2}\,\sqrt{-1}\in R(\alpha)$，而有 $\sqrt{-1}\in R(\alpha)$．显然 $R(\sqrt{-1})=R(\alpha)$，即 $C\simeq R(\alpha)$．

又任 $\beta\in E$ 是 R 上代数元，由 C 是代数封闭域知 $R(\sqrt{-1})$ 也是．于是 $\beta\in R(\sqrt{-1})$，即得 $E=R(\sqrt{-1})$．

上面证明了代数扩域 $E\supset R$，只能是 $E=R$ 或 $E=R(\sqrt{-1})$．它们是 1 次和 2 次扩域，R 上没有 3 次扩域．

§3 古希腊三大几何作图难题的否定

习 题

以下习题中打 * 者为必作题，其余为选作题．

*1. 设已知量 a,b 及 r 皆大于 0 且 $a>b$.试用圆规直尺作图作出 $a\pm b$,ab,$\frac{a}{r}$,$\sqrt{r}$.

*2. 下列哪些量可以用圆规直尺作图作出:

(1) $\sqrt[4]{5+2\sqrt{6}}$　　(2) $\frac{2}{1+\sqrt{7}}$

(3) $1-\sqrt[5]{27}$

*3. 下列多项式中哪些多项式的实根可用圆规直尺作图作出:

(1) $x^2-7x-13$　　(2) x^4-5

(3) x^3-10x^2+1　　(4) x^5-9x^3+3

(5) x^4-2x-3

4. 证明:实数 α 可用圆规直尺作图作出当且仅当有实数的域的序列 $E_0\subset E_1\subset\cdots\subset E_{n-1}\subset E_n$,使 $\alpha\in E_n$,且$[E_i:E_{i-1}]=2$,$1\leqslant i\leqslant n$,其中 E_0 是已知量的域.

习题答案与解答

1. 运用中学几何作图知识来作出要求的量.

2. (1) 可以.

(2) 可以.

(3) 不可以.

证明　令 $x=\sqrt[5]{27}$,它满足 $x^5-27=0$.再令 $y+2=x$,则$(y+2)^5-27=y^5+5y^4\cdot 2+10y^3\cdot 2^2+10y^2\cdot 2^3+5y\cdot 2^4+2^5-27=y^5+10y^4+40y^3+80y^2+80y+5=0$.用艾森斯坦判别法,它是 y 的Q 上 5 次不可约多项式方程,$\sqrt[5]{27}-2$ 是它的根,于是$[Q(\sqrt[5]{27}-2):Q]=[Q(\sqrt[5]{27}):Q]=5$.若 $\sqrt[5]{27}$能用圆规直尺作图得到,则它落在Q 的某扩域 E 中,且$[E:Q]=2^l$.但$[Q(\sqrt[5]{27}):Q]\nmid[E:Q]$,故 $\sqrt[5]{27}$,因而 $1-\sqrt[5]{27}$不能落在这样的域中,它们不能这样作出.

3. (1) 可以.

(2) 可以,令 $x=\pm\sqrt[4]{5}=\pm\sqrt{\sqrt{5}}$. $\sqrt{5}$是可作的,故 $\sqrt{\sqrt{5}}$也可作.

(3) 我们证明 x^3-10x^2+1 是Q 上不可约多项式.实际上只有 ±1 可能是它的有理根,但它们不是.因此 x^3-10x^2+1 在Q$[x]$中没有一次因式,故不可约.令它的实根为 α,则$[Q(\alpha):Q]=3$.α 不属于Q 的任何扩张域 E,使 E 满足$[E:Q]=2^l$.故 α 不能用圆规直尺作图作出.

(4) 用艾森斯坦判别法,x^5-9x^3+3 在Q 上不可约.对它的实根 α,$[Q(\alpha):Q]=5$.与习题 1 中(3)的证明类似,知 α 不可作.

(5) $x^4-2x-3=(x+1)(x^3-x^2+x-3)$.第二个因式的有理根只可能是$\pm3,\pm1$,但都不是根.因而是Q上三次不可约多项式、与本题(3)的证明一样可知,它的实根不可作,但第一因式的根为-1,是可作的.

4. 课文中已证明由 E_0 作为已知量出发,用圆规直尺作图能作出的量 α 一定属于某个具有题目所设性质的扩域 E_n 中.

反之,设 α 属于具有上述性质的扩域 E_n 中.我们对 n 作归纳法.首先对 $\forall i$,$[E_i:E_{i-1}]=2$,即 E_i 是 E_{i-1} 上 2 维向量空间.取 $\beta_i\in E_i/E_{i-1}$.则 $1,\beta_i$ 对域 E_{i-1} 为线性无关,因而是 E_i 作为 E_{i-1} 上线性空间的基,故 $E_i=E_{i-1}(\beta_i)$.又 $\beta_i^2\in E_i$,它是 $1,\beta_i$ 的线性组合,因此有 $b_i,c_i\in E_{i-1}$ 使 $\beta_i^2+b_i\beta_i+c_i=0$,$\beta_i=\dfrac{-b_i\pm\sqrt{b_i^2-4c_i}}{2}$.$n=0$,$E_0$ 中的任一个量显然可用圆规和直尺经有限步作出.设 E_{n-1} 中任一量已可用圆规和直尺经有限步作出,即 b_n,c_n 可用有限步作出.于是 $b_n^2-4c_n$ 以至 β_n 皆能作出.E_n 中任一量 α 都是 $1,\beta_n$ 的线性组合 $\alpha=a+b\beta_n$,$a,b\in E_{n-1}$.a,b,β_n 皆能用圆规直尺经有限步作出,则 α 也能.完成了归纳法.

§4 环的例子,几个基本概念

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. 举出$\mathbf{Z}/6\mathbf{Z}=Z_6$中的零因子的例子.

*2. 令$\mathbf{Z}[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbf{Z}\}$,它是整环.$2\mathbf{Z}[\mathrm{i}]=\{2a+2b\mathrm{i}\}$是$\mathbf{Z}[\mathrm{i}]$的主理想.问$\mathbf{Z}[\mathrm{i}]/2\mathbf{Z}[\mathrm{i}]$中是否有零因子?

*3. 写出下列商环的全部元素.

(i) $Z_2=\mathbf{Z}/2\mathbf{Z}$,检查它与 F_2 是否同构.

(ii) $Z_3=\mathbf{Z}/3\mathbf{Z}$,检查是否是域.

(iii) $F_2[x]/(x^2+x+1)$,检查是否有零因子.

(iv) $Z_3[x]/(x^2+x+2)$,检查是否是域.

*4. R 是环.若 R 的加群是循环群,则(i)R 是交换环;(ii)R 的子环只有 R;(iii)当 R 的元素有无限多个时,它的任一理想也有无限多个元;(iv)当 R 的元素有限时,设 I 为它的理想,则 $|I|\,|\,|R|$;(v)R 的加法子群都是 R 的理想.

5. 找出Z_6,Z_8的全部理想.哪些是极大理想?对所有极大理想 K,写出Z_6/K及Z_8/K的全部元素、加法表和乘法表.

6．设 K 为交换环，M 是它的理想，M 作为 K 的加法子群满足$[K:M]=$素数，则商环 K/M 是域．

7．试将第一章§10 习题 6 中关于群同态的结论推广到环同态的情形．

8．设 $f(x)=f_1^{r_1}(x)f_2^{r_2}(x)\cdots f_k^{r_k}(x)$是域 F 上的不可约多项式的乘积，且 $f_1(x),\cdots,f_k(x)$互不相伴，令 $R=F[x]/(f(x))$是商环．

(i) 求出 R 的全体理想．

(ii) 这些理想中哪些是极大理想？

(iii) 设 $\bar{K}$ 是 R 的理想，K 是 $\bar{K}$ 在 $F[x]$中的原象．检验 $F[x]/K\cong R/\bar{K}$．

9．证明Z [i]/(1+i)是域．

习题答案与解答

1．2+6 Z $\neq 0$，3+6 Z $\neq 0$，都是Z_6中的零因子．

2．由$(1+i)^2=2i$，$((1+i)+2\,\mathrm{Z}\,[i])^2=2i+2\,\mathrm{Z}\,[i]=0$．故$(1+i)+2\,\mathrm{Z}\,[i]$是Z [i]/2 Z [i]中的零因子．

3．(i) $Z_2=\mathrm{Z}/2\,\mathrm{Z}=\{0+2\,\mathrm{Z},1+2\,\mathrm{Z}\}=\{\bar{0},\bar{1}\}$．它的加法表和乘法表如下：

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

，

×	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

．

建立映射

$$\begin{aligned} Z_2 &\longrightarrow F_2 \\ \bar{0} &\longmapsto 0 \\ \bar{1} &\longmapsto 1. \end{aligned}$$

这是双射，且保持加法和乘法．故是同构．

(ii) $Z_3=\mathrm{Z}/3\,\mathrm{Z}=\{\bar{0},\bar{1},\bar{2}\}$．

这是交换环，又$(\bar{1})^{-1}=\bar{1}$，$(\bar{2})^{-1}=\bar{2}$．故Z_3是域．

(iii) 因 $\bar{0},\bar{1}$ 不是 x^2+x+1 的根，故 x^2+x+1 在 $F_2[x]$上不可约．因此 $F_2[x]/(x^2+x+1)$是域，故无零因子．

(iv) 由于 $\bar{0},\bar{1},\bar{2}$ 都不是 x^2+x+2 的根，故它在$Z_3[x]$中不可约．因此 $Z_3[x]/(x^2+x+2)$是域．

4．由于 R 是加法循环群，可设 $R=\mathrm{Z}a$，$a\in R$．(i) R 中任意两元可写为 ma，na，而$(ma)(na)=mna^2=(na)(ma)$，故 R 是交换环．

(ii)设$1=ka$，又设 $a^2=la$．则 $a=1\cdot a=ka^2=kla=lka=l\cdot 1$．因 R的子

环含 1,就含有 $l1=a$.故子环含$\mathbf{Z}a=R$.即子环必是 R.

(iii) $R=\mathbf{Z}a$ 有无限多个元,则它是无限循环加群.于是当 $m,n\in\mathbf{Z}$,$m\neq n$ 时有 $ma\neq na$.设 I 是 R 的非零理想,它就是 R 的非零子加群,必为无限群.故 I 有无限个元.

(iv) 当 R 的元素有限时,它作为加群是有限循环群.而 R 的理想 I 是它的子加群,由 Lagrange 定理,知 $|I|\,|\,|R|$.

(v) 设 I 是 R 的加法子群,它也是循环群.设 $I=\mathbf{Z}(ka)$.任 $ma\in R$,$(ma)I=\mathbf{Z}(na)(ka)=\mathbf{Z}(mkla)\subseteq\mathbf{Z}(ka)=I$.故 I 是 R 的理想.

5. $\mathbf{Z}_6$ 的全部理想为$\mathbf{Z}_6$,$2\mathbf{Z}_6$,$3\mathbf{Z}_6$,$0\cdot\mathbf{Z}_6$.其中 $2\mathbf{Z}_6$,$3\mathbf{Z}_6$ 是$\mathbf{Z}_6$的极大理想.

$\mathbf{Z}_8$的全部理想为$\mathbf{Z}_8$,$2\mathbf{Z}_8$,$4\mathbf{Z}_8$,$0\cdot\mathbf{Z}_8$,其中 $2\mathbf{Z}_8$是极大理想.

$$\mathbf{Z}_6/2\mathbf{Z}_6=\{\bar{0},\bar{1}\},\mathbf{Z}_6/3\mathbf{Z}_6=\{\bar{0},\bar{1},\bar{2}\},$$

$$\mathbf{Z}_8/2\mathbf{Z}_8=\{\bar{0},\bar{1}\}.$$

它们的加法表和乘法表:

$\mathbf{Z}_6/2\mathbf{Z}_6$:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

,

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

.

$\mathbf{Z}_8/2\mathbf{Z}_8\cong\mathbf{Z}_6/2\mathbf{Z}_6$,它们有相同的加法表和乘法表.

$\mathbf{Z}_6/3\mathbf{Z}_6$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

6. K/M 是商环,作为加法商群$[K:M]=$素数.对 K 的任一理想 N,若 $M\subseteq N\subseteq K$、则从加法方面看 N/M 是K/M 的子群.后者是素数阶群,故 N/M 是单位元群或 K/M 本身.因此 $N=M$ 或 $N=K$,即 M 是 K 的极大理想.于是 K/M 是域.

7. 群同态的结论推广到环同态,结论如下:

设环 G 到环 $\bar{G}$ 有满同态 f.令 $N=\mathrm{Ker}f$.记 $f^{-1}(\bar{K})$为 $\bar{G}$ 的子集 $\bar{K}$ 对于 f 的原象.则

(1) 若 $\bar{K}$ 是 $\bar{G}$ 的子环,则 $N\subset f^{-1}(\bar{K})$,且 $f^{-1}(\bar{K})$是子环.

(2) 有映射

$$\{G\text{ 的含 }N\text{ 的子环}\}\overset{\varphi}{}\{\bar{G}\text{ 的子环}\}$$

$$H \longmapsto f(H).$$

它还是双射,且保持包含关系.

(3) 若 K 是 G 的理想,则 $f^{-1}(K)$是 G 的含 N 的理想,于是

$$\{G \text{ 的含 } N \text{ 的理想}\} \quad \{G \text{ 的理想}\}$$
$$K \longmapsto f(K)$$

是双射.

(4) 设 H 是 G 的理想,则有同构

$$G/f^{-1}(H) \cong G/H.$$

(5) G 是环,N 是理想.令 $\bar{G}=G/N$,π 是自然同态

$$G \overset{\pi}{\longrightarrow} G/N=\bar{G},$$

则 π 建立了$\{G$ 的含 N 的子环$\}$到$\{G$ 的子环$\}$上的双射:$\pi(H)=\bar{H}=H/N$,且保持包含关系.同时建立了$\{G$ 的含 N 的理想$\}$到$\{G$ 的理想$\}$上的双射,且有同构

$$G/H \cong \bar{G}/\bar{H}=G/N/H/N.$$

证明　由于环是加群,子环、理想是子加群,环同态的核正是加群同态的核.如能证明(i)若 H 是 G 的子环(或理想),则 $f(H)$是 G 的子环(或理想),(ii)H 是 G 的子环(或理想),则 $f^{-1}(H)$是 G 的包含 N 的子环(或理想).再利用群同态的结论就给出上面(1)到(5)的结论都成立.

对结论(i),易知子环(或理想)的满同态的象是子环(或理想),故成立.

对(ii),设 H 是子环(或理想),它是 G 的子加群,故 $f^{-1}(H)$是 G 的子加群.又对 $l,k\in f^{-1}(H)$(或取 $l\in G$),$f(l),f(k)\in H$(或 $f(l)\in G$).由 H 是子环(或理想),$f(l)f(k)=f(lk)\in H$,故 $lk\in f^{-1}(H)$.这证明了 $f^{-1}(H)$是 G 的子环(或理想).

8. (i) $F[x]$是主理想环,它的同态象 $R=F(x)/(f(x))$.由 7 题,R 的任一理想为 $J/(f(x))$,其中 J 为 $F[x]$的理想.J 为主理想,设为 $J=g(x)F[x]$.于是 R 的任一理想 I 必有形式:$I=g(x)F[x]/(f(x))$是 R 的一个主理想.令 $(g(x),f(x))=m(x)$,$g(x)=h(x)m(x)$.由$(h(x),f(x))=1$,有 $u(x)$,$v(x)\in F[x]$,使 $u(x)h(x)+v(x)f(x)=1$.即 $u(x)h(x)+(f(x))=1+(f(x))$.于是 $m(x)F[x]/(f(x))=u(x)h(x)m(x)F[x]/(f(x))\subseteq g(x)F[x]/(f(x))=I\subseteq m(x)F[x]/(f(x))$,故 $I=m(x)F[x]/(f(x))$.这说明 R 的任一理想必为 $m(x)F[x]/(f(x))$,其中 $m(x)|f(x)$.

再设 $I_i=m_i(x)F[x]/(f(x))$,$m_i(x)|f(x)$,$i=1,2$ 都是 R 的理想.来证 $I_1=I_2$ 当且仅当 $m_1(x)$与 $m_2(x)$相伴.

首先设 $m_1(x)=cm_2(x)$,$c\neq 0$ 是 F 的元,则

$I_1=m_1(x)F[x]/(f(x))=cm_2(x)F[x]/(f(x))=m_2(x)\cdot cF[x]/(f(x))=m_2(x)F[x]/(f(x))=I_2$.

反之,设 $I_1\subseteq I_2$.由 $m_1(x)+(f(x))\in I_1\subseteq I_2=m_2(x)F[x]/(f(x))$,有 $h_2(x)\in F[x]$使 $m_1(x)+(f(x))=m_2(x)h_2(x)+(f(x))$.进而有 $g_2(x)$使 $m_1(x)+g_2(x)f(x)=m_2(x)h_2(x)$.因 $m_2(x)|f(x)$,可得 $m_2(x)|m_1(x)$.当 $I_1=I_2$ 时,同样有 $m_1(x)|m_2(x)$.就证明了 $m_1(x),m_2(x)$相伴.

写 $g_{i_1\cdots i_k}(x)=(f_1(x))^{i_1}(f_2(x))^{i_2}\cdots(f_k(x))^{i_k}$,其中 $i_1,\cdots,i_k$ 可独立地遍取 $1\leqslant i_1\leqslant r_1$,$1\leqslant i_2\leqslant r_2$,$\cdots$,$1\leqslant i_k\leqslant r_k$.则$\{g_{i_1\cdots i_k}(x)\}$是 $f(x)$的全部不相伴的因式,而 $g_{i_1\cdots i_k}(x)F[x]/(f(x))$是 R 的全部的理想.

(ii)取 $J_i=f_i(x)F[x]/(f(x))$.由(i)第二部分的证明只有理想 $1\cdot F[x]/(f(x))$及 $f_i(x)F[x]/(f(x))$能包含 J_i.故 J_i 是 R 的极大理想.

R 的任一理想若非 J_i 之一和 R 本身,则它是 $m(x)F[x]/(f(x))$,其中 $m(x)$是 $f_1(x),\cdots,f_k(x)$中至少两项的乘积.设 $m(x)=f_i(x)f_j(x)\cdots$.则 $f_i(x)|m(x)$,但任意一个 $f_i(x)$与 $m(x)$不相伴.由(i)中第二部分的证明 $m(x)F[x]/(f(x))\subseteq J_i$,但它们不相等,故前者不是极大理想.因此 R 的全部极大理想为 J_i,$i=1,2,\cdots,k$.

(iii)设 $K=m(x)F[x]/(f(x))$是 R 的理想,其中 $m(x)|f(x)$.显然 $m(x)F[x]$在 R 中的象是 K.又任意 $g(x)\in F(x)$,若 $g(x)+(f(x))\in m(x)F[x]/(f(x))$,用(i)中第二部分的证明可得 $m(x)|g(x)$.故 $g(x)\in m(x)F[x]$.这证明了 K 在 $F[x]$中的原象 K 是 $m(x)F[x]$.作映射

$$\begin{array}{ccc} F[x]/m(x)F[x] & \overset{\pi}{\longrightarrow} & R/K \\ g(x)+m(x)F[x] & \longmapsto & [g(x)+(f(x))]+K. \end{array}$$

首先要证明它确实规定了映射,即象元与 $g(x)+m(x)F[x]$中的代表的选择无关,实际上 $g_1+m(x)F[x]=g_2+m(x)F[x]$当且仅当 $g_1-g_2\in m(x)F[x]$当且仅当$(g_1-g_2)+(f(x))\in m(x)F[x]/(f(x))=K$ 当且仅当$[g_1+(f(x))]$与$[g_2+(f(x))]$属于 K 的同一陪集当且仅当$[g_1+(f(x))]+K=[g_2+(f(x))]+K$.这就证明了映射是意义的,而且是单射.$\pi$ 显然是满射,因而是双射.

又

$$\begin{aligned}&\pi((g_1+m(x)F[x])+(g_2+m(x)F[x]))=\pi((g_1+g_2)+m(x)F[x])\\&=[(g_1+g_2)+(f(x))]+K=[(g_1+(f(x)))+(g_2+(f(x)))]+K\\&=(g_1+(f(x)))+K+(g_2+(f(x)))+K=\pi(g_1+m(x)F[x])\\&\quad+\pi(g_2+m(x)F[x]).\end{aligned}$$

同样可证 $\pi((g_1+m(x)F[x])(g_2+m(x)F[x]))=\pi(g_1+m(x)F[x])\pi(g_2+m(x)F[x])$.故 π 是环同构.

9. 先计算$Z[i]/(1+i)$的全部元素.

记剩余类 $a+bi+((1+i))$为 $\overline{a+bi}$,其中 $a,b\in Z$.我们有 $\overline{a+bi}=\overline{a-b+b(1+i)}=\overline{a-b}$.又$(1+i)^2=-2$,故 $\overline{2}=\overline{2+(1+i)^2}=\overline{0}$.于是

$$Z[i]/(1+i)=\{\overline{0},\overline{1}\}=\{0+((1+i)),1+((1+i))\}\cong Z_2.$$

故它是域.

§5 整数模 n 的剩余类环,素数 p 个元素的域

习 题

以下习题中打 * 者为必作题,其余为选作题.

1. 求出Z_8中可逆元的群及其乘法表.

*2. 求出Z_9中可逆元的群及其乘法表.

*3. 写出$Z_3[x]/(x^2+1)$的全部元素.求出 $\overline{x+1}$与全部元素的乘积以及它的逆元素.

*4. $4^{27}\equiv?\pmod 3$ $7^{123}\equiv?\pmod 5$ $8^{27}\equiv?\pmod 6$

*5. p 是素数,则域Z_p中全部元素是方程 $x^p-x=0$ 的全部根.因而映射

$$\begin{array}{ccc} Z_p & \longrightarrow & Z_p \\ a & \longmapsto & a^p \end{array}$$

是恒等自同构.

习题答案与解答

1. Z_8的可逆元群是$\{1+8Z,3+8Z,5+8Z,7+8Z\}$.乘法表略.

2. Z_9的可逆元群是$\{1+9Z,2+9Z,4+9Z,5+9Z,7+9Z,8+9Z\}$.乘法表略.

3. 记剩余类 $f(x)+((x^2+1))$为$\overline{f(x)}$.则

$Z_3[x]/(x^2+1)=\{\overline{0},\overline{1},\overline{2},\overline{x},\overline{x+1},\overline{x+2},\overline{2x},\overline{2x+1},\overline{2x+2}\}$.

$\overline{(x+1)}Z_3[x]/(x^2+1)=\{\overline{0},\overline{x+1},\overline{2(x+1)}\}$ $\overline{x+1}$的逆元素为$\overline{x+2}$

4. $4^{27}\equiv 1^{27}=1(\bmod 3)$.

$7^{123}\equiv 2^{123}\equiv 2^{120}\cdot 2^3(\bmod 5)$

$\equiv 2^3(\bmod 5)$(因 $2^4\equiv 1,2^{120}=(2^4)^{30}\equiv 1$)

$\equiv 3(\bmod 5)$.

$8^{27}\equiv((2^3)^3)^3\equiv(2^3)^3\equiv2^3\equiv2(\mathrm{mod}\ 6)$.

5. $\mathbf{Z}_p\setminus\{0\}$是 $p-1$ 阶乘法循环群,故任 $0\neq a\in\mathbf{Z}_p$,满足 $a^{p-1}=1$.于是 $a^p=a$.又 $0^p=0$,所以$\mathbf{Z}_p$中全部元是 $x^p-x=0$ 的全部根.这就证明了

$$\begin{array}{ccc}\mathbf{Z}_p & & \mathbf{Z}_p\\ a & \longmapsto & a^p\end{array}$$

是恒等自同构.

§6 $F[x]$模某个理想的剩余类环,添加一个多项式的根的扩域

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. $\mathbf{Z}_3[x]$中计算$(x^2+x+1)(x^3+2x+1)$及$(x^4+2x+1)(x^3+x+1)$

*2. 证明 x^2+1,x^3+2x+1 是$\mathbf{Z}_3[x]$中不可约多项式.问$\mathbf{Z}_3[x]/(x^2+1)$,$\mathbf{Z}_3[x]/(x^3+2x+1)$分别是几个元素的域.

3. 写出$\mathbf{Z}_3[x]/((x^2+1)(x^3+2x+1))$中的全部理想和极大理想.

*4. 证明$\mathbf{Q}[x]/(x^2-2)$与$\mathbf{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$都是域,且互相同构.

习题答案与解答

1. $(x^2+x+1)(x^3+2x+1)=x^5+x^4+1$.

$(x^4+2x+1)(x^3+x+1)=x^7+x^5+x^3+2x^2+1$.

2. x^2+1,x^3+2x+1 在$\mathbf{Z}_3$中无根,于是在$\mathbf{Z}_3[x]$中无一次因式,因此不可约.$\mathbf{Z}_3[x]/(x^2+1)$是有 9 个元的域,$\mathbf{Z}_3[x]/(x^3+2x+1)$是有 27 个元的域.

3. 用§4 习题 8,它的全部理想为零理想及

$\mathbf{Z}_3[x]/((x^2+1)(x^3+2x+1))$,$(x^2+1)\mathbf{Z}_3[x]/((x^2+1)(x^3+2x+1))$,$(x^3+2x+1)\mathbf{Z}_3[x]/((x^2+1)(x^3+2x+1))$.

后面两个理想是极大理想.

4. $\mathbf{Q}[x]/(x^2-2)$与$\mathbf{Q}(\sqrt{2})$都是域,略证.

作映射

$$\begin{array}{ccc}\mathbf{Q}[x] & \overset{\varphi}{} & \mathbf{Q}(\sqrt{2})\\ p(x) & \longmapsto & p(\sqrt{2})\end{array}$$

这是同态映射,且是满射.$\mathrm{Ker}\varphi=\{p(x)\mid p(\sqrt{2})=0\}$.由于 x^2-2 是$\sqrt{2}$的极小多项式,故 $\mathrm{Ker}\varphi=(x^2-2)\mathbb{Q}[x]=((x^2-2))$.由同态基本定理得

$$\mathbb{Q}[x]/((x^2-2))\cong\mathbb{Q}(\sqrt{2}).$$

§7 整环的分式域,素域

习 题

以下习题中打 * 者为必作题,其余为选作题.

1. 证明:有限整环是域.

*2. R 是交换环,$P\neq R$ 是 R 的理想,则$\frac{R}{P}$是整环当且仅当 P 有性质:若 $a,b\in R$ 满足 $ab\in P$,则 $a\in P$ 或 $b\in P$.有这种性质的理想 P 称为素理想.

*3. R 是交换环,则 R 的极大理想必为素理想.

*4. 设 $n\in\mathbb{Z}$,$n>1$,$\mathbb{Z}$ 中主理想$(n)=n\mathbb{Z}$ 是素理想当且仅当 n 是素数.

*5. 设 R 是一个域,则 R 的分式域就是自身.

*6. 令$\mathbb{Z}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$,$\mathbb{Q}(\sqrt{2})=\{\alpha+\beta\sqrt{2}\mid\alpha,\beta\in\mathbb{Q}\}$.证明$\mathbb{Q}(\sqrt{2})$是$\mathbb{Z}(\sqrt{2})$的分式域.

7. 令$\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}\}$,$\mathbb{Q}[\mathrm{i}]=\{\alpha+\beta\mathrm{i}\mid\alpha,\beta\in\mathbb{Q}\}\mathbb{Z}$.证明$\mathbb{Q}[\mathrm{i}]$是$\mathbb{Z}[\mathrm{i}]$的分式域.

8. 域 F 上多项式 $f(x)$的次数$\geqslant 1$.$F[x]$中主理想$(f(x))$是素理想当且仅当 $f(x)$是不可约多项式.

习题答案与解答

1. 设 R 是有限整环,$R=\{r_1,\cdots,r_t\}$.令 $r_t=0$.$\forall 0\neq r\in R$,当 $r_i\neq r_j$ 时有 $rr_i\neq rr_j$.故 $rr_1,\cdots,rr_{t-1}$是 R 的全部非零元,必有某 r_j 使 $rr_j=1$,即 r_j 为 r 的逆元.

R 的每个非零元都有逆,故是域.

2. 设 R/P 为整环.$\forall\ a,b\in R$,若 $ab\in P$,则$(a+P)(b+P)=ab+P=0$.于是 $a+P=0$ 或 $b+P=0$,即 $a\in P$ 或 $b\in P$.故 P 为素理想.

反之,设 P 是素理想,$\forall\ a,b\in R$,若 $ab\in P$ 则 $a\in P$ 或 $b\in P$.现设 R/P 中$(a+P)(b+P)=ab+P=0$.即 $ab\in P$,于是 $a\in P$ 或 $b\in P$,即 $a+P=0$ 或 $b+P=0$.故 R/P 是整环.

3. 设 I 是 R 的极大理想,则 R/I 是域,当然是整环.由习题 2,I 是素理想.

4. 设Z 中$(n)=nZ$ 是一个理想.若 n 不是素数,则 $n=ab$, a,b 为大于 1 的正整数.由于 a 和 b 都不是 n 的倍数,故 $a\overline{\in}(n)$, $b\overline{\in}(n)$.但 $ab=n\in(n)$,故(n)不是素理想,这就证明了(n)是素理想则 n 为素数.

当 n 是素数时,对 $ab\in(n)$,则 $n\mid ab$.若 $n\nmid a$,则$(n,a)=1$.于是 $n\mid b$.即 $a\in(n)$或 $b\in(n)$,(n)是素理想.

5. R 是域,则也是整环.它的分式域 F 以 R 为子环,且 F 中的元是 R 的元的商.由于 R 是域,它的元的商仍在 R 中,故 $R=F$.

6. 我们已知Q $(\sqrt{2})$是域.对任意 $\alpha+\beta\sqrt{2}\in$Q $(\sqrt{2})$,可写 $\alpha=\frac{a}{c}$, $\beta=\frac{b}{c}$, $a,b,c\in$Z .则 $\alpha+\beta\sqrt{2}=\frac{a+b\sqrt{2}}{c}$是Z $(\sqrt{2})$中两元素的商.又Z $(\sqrt{2})$中两元素的商为:

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(c-d\sqrt{2})(a+b\sqrt{2})}{c^2-2d^2}=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}\in\text{Q}(\sqrt{2}).$$

现在Z $(\sqrt{2})$是Q $(\sqrt{2})$的子环,且Q $(\sqrt{2})$是由Z $(\sqrt{2})$中两元素的商组成,故Q $(\sqrt{2})$是Z $(\sqrt{2})$的分式域.

7. 易证Q $[i]$是域.对任意 $\alpha+\beta i\in$Q $[i]$,可写 $\alpha=\frac{a}{c}$, $\beta=\frac{b}{c}$,则 $\alpha+\beta i=\frac{a+bi}{c}$是Z $[i]$中两元素的商.又Z $[i]$中两元素的商为$\frac{a+bi}{c+di}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i\in$Q $[i]$.即Q $[i]$由Z $[i]$的两元素的商组成.故Q $[i]$是Z $[i]$的分式域.

8. 完全可仿照习题 4 的证明.

设$(f(x))$是 $F[x]$中理想,$f(x)$的次数$\geqslant 1$.若 $f(x)=g(x)h(x)$, $g(x)$及 $h(x)$的次数皆大于等于 1,这时 $g(x)$, $h(x)$皆不是 $f(x)$的倍数,故 $g(x)$, $h(x)\overline{\in}(f(x))$,但 $g(x)h(x)\in(f(x))$.即$(f(x))$不是素理想.故若$(f(x))$是素理想,则 $f(x)$不可约.

反之,若 $f(x)$不可约.对 $g(x)h(x)\in(f(x))$,则有 $g(x)h(x)=f(x)k(x)$.若 $f(x)\mid g(x)$则 $g(x)\in(f(x))$.若$f(x)\nmid g(x)$,则$(f(x),g(x))=1$,于是 $f(x)\mid h(x)$.即有 $h(x)\in(f(x))$,故$(f(x))$是素理想.

§8 环的直和与中国剩余定理

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. 解同余方程组.

(i) $\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 5 \\ x\equiv 3 \pmod 7 \\ x\equiv 4 \pmod 9 \end{cases}$ (ii) $\begin{cases} x\equiv 5 \pmod 7 \\ x\equiv 4 \pmod 6 \end{cases}$

*2. 韩信点兵问题:有兵一队,若列 5 列纵队,则末行 1 人.成 6 列纵队,则末行 5 人.成 7 列纵队,则末行 4 人.成 11 列纵队,则末行 10 人.求兵数.

*3. $R_1,\cdots,R_s$ 是环.$U_1,\cdots,U_s$ 分别是它们的可逆元的群.证明 $R_1\oplus\cdots\oplus R_s$ 的可逆元群为 $U=U_1\times U_2\times\cdots\times U_s$(见第一章§4 定义 2).

4. 设 $n=m_1m_2\cdots m_s$,m_i 两两互素.令 $U(\mathbf{Z}_m)$表$\mathbf{Z}_m$的可逆元群,则$\mathbf{Z}/n\mathbf{Z}=\mathbf{Z}_n$的可逆元群同构于 $U(\mathbf{Z}_{m_1})\times\cdots\times U(\mathbf{Z}_{m_s})$.进而有,$\varphi(n)=\varphi(m_1)\varphi(m_2)\cdots\varphi(m_s)$,这里 $\varphi(n)$是欧拉函数.当 $n=p_1^{e_1}\cdots p_s^{e_s}$,$p_i$ 为不同素数时,$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)$.(见第二章§5 定义 1 及最后一段).

习题答案与解答

1. (i) 解为 157(mod 630)

(ii) 解为 40(mod 42)

2. 2111(mod 2310)

3. $(a_1,a_2,\cdots a_s)$是 $R_1\oplus\cdots\oplus R_s$ 的可逆元当且仅当有$(b_1,\cdots,b_s)$使$(a_1,\cdots,a_s)(b_1,\cdots,b_s)=(a_1b_1,\cdots,a_sb_s)=(1,\cdots,1)$当且仅当 $a_ib_i=1$,$i=1,2,\cdots,s$ 当且仅当 $a_i\in U_i$,$i=1,2,\cdots,s$ 当且仅当$(a_1,\cdots,a_s)\in U_1\times\cdots\times U_s$.

4. 这时$\mathbf{Z}_n\cong\mathbf{Z}_{m_1}\oplus\cdots\oplus\mathbf{Z}_{m_s}$.$\mathbf{Z}_m$的可逆元群 $U(\mathbf{Z}_n)=\{k+n\mathbf{Z}\mid(k,n)=1\}$.故$|U(\mathbf{Z}_n)|=\varphi(n)$.(见第二章§5 定义 1).

由习题 3,$U(\mathbf{Z}_n)\cong U(\mathbf{Z}_{m_1})\times\cdots\times U(\mathbf{Z}_{m_s})$.$|U(\mathbf{Z}_{m_i})|=\varphi(m_i)$,$i=1,2,\cdots,s$.故得 $\varphi(n)=\varphi(m_1)\cdots\varphi(m_s)$.

对素数幂 p^k,$1,2,\cdots,p^k-1$ 中与 p^k 不互素的数为 p 的所有倍数 lp,$1\leqslant l\leqslant p^{k-1}-1$.故此中与 p^k 互素的数共$(p^k-1)-(p^{k-1}-1)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right)$(个).即 $\varphi(p^k)=p^k\left(1-\frac{1}{p}\right)$.

当 $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 时,

$$\begin{aligned}\varphi(n)&=\varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_s^{e_s})\\&=p_1^{e_1}\cdots p_s^{e_s}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right).\end{aligned}$$

第三章　有限域及其应用

内容要点

1. 有限域中的元素的数目. p^n 元域的存在及唯一性,它的结构(Z_p上的 n 维向量空间、是 $x^{p^n}-x=0$ 的全部根、它的全部非零元组成乘法循环群),它的子域.

2. 有限域上不可约多项式的性质. F_q 上全部 n 次不可约多项式皆为 $x^{q^n}-x$ 的因子.不可约多项式 $f(x)(\neq cx)$的周期性.本原多项式及用于纠错码.

3. 移位寄存器序列(线性递归序列)

序列的数学刻画:引入 F_2 上向量空间 $V(F_2)=\{\boldsymbol{a}=(a_0,a_1,a_2,\cdots,)\mid a_i\in F_2\}$及 $V(F_2)$上左移变换 $L:L\boldsymbol{a}=(a_1,a_2,a_3,\cdots)$.对 F_2 上递归关系

$$a_{n+k}=c_{n-1}a_{(n-1)+k}+c_{n-2}a_{(n-2)+k}+\cdots+c_0a_k,\ k=0,1,2,\cdots \quad (*)$$

引入 F_2 上多项式

$$f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_0.$$

则 $V(F_2)$中向量 $\boldsymbol{a}$ 满足(*)(即 $\boldsymbol{a}$ 是满足(*)的线性递归序列)的充分必要条件是 $f(L)\boldsymbol{a}=\boldsymbol{0}$.

优美的理论结果:$\boldsymbol{0}\neq\boldsymbol{a}$ 的周期等于$f(x)$的周期(这时 $f(x)$必须是不可约多项式且 $f(x)\neq x$)

m 序列及其优美性质(参看习题)

读后注

1. §3 内容是总导引中第一点思想的又一体现.读者自己察看一下,§3 中共组织了两个运算系统.一个是 F_2 上的无限序列作成的线性空间 $V(F_2)$;一个是引入左移变换 L,组成了 $V(F_2)$上线性变换的多项式环.正是有这两个运算系统才能将线性递归序列的周期性与 F_2 上多项式的理论联系起来.

2. §1 及§2 内容是有限域及其上的多项式理论的一个简短而较全面的介绍.这在一般近世代数教材中少见.而§3 内容在这些教材中从未出现过.其中的应用使我们看到这些内容与当代信息技术有密切联系.实际上它们对今后更

大范围的应用来说也是基本的.

3.§3 内容是理论与实践相互促进的范例.正是分析移位寄存器序列性质的需要产生了理论的研究,理论的建立和优美的结果又解决了实践中的问题.这充分显示了理论的力量

思考练习题(非必作题)

读者试作出一个具体线性递归序列来验证一下§3 中关于周期性的结果.

§1 有限域的基本构造

习 题

*1. 验证 x^2+1 及 x^2+x+2 皆为$\mathbf{Z}_3[x]$上不可约多项式.写出下列两域

$$\mathbf{Z}_3[x]/(x^2+1) \quad 及 \quad \mathbf{Z}_3[x]/(x^2+x+2)$$

的加法表和乘法表.找出这两个域之间的同构对应.

*2. 作出$\mathbf{Z}_2[x]$,$\mathbf{Z}_3[x]$中所有的二次、三次、及两个四次不可约多项式.作出 2^2,2^3,2^4 个元的域.

*3. $f_1(x)$,$f_2(x)$都是$\mathbf{Z}_p[x]$上 m 次不可约多项式,则

$$\mathbf{Z}_p[x]/(f_1(x))\cong\mathbf{Z}_p[x]/(f_2(x)).$$

4. 作出一个 3^4 个元的域,并在其中找出一个 3^2 个元的子域.

*5. 设 $d\mid m$,证明

(1) $p^d-1\mid p^m-1$.

(2) $x^{p^d}-x\mid x^{p^m}-x$.

*6. 设 $F_{p^n}=\mathbf{Z}_p(\alpha)$.问 α 是乘法群 $F_p^{*n}=F_{p^n}\setminus\{0\}$的生成元吗?

习题答案与解答

1. x^2+1 及 x^2+x+2 在$\mathbf{Z}_3$上皆无根,故它们在$\mathbf{Z}_3[x]$中不可约.

$$\mathbf{Z}_3[x]/(x^2+1) \quad 及 \quad \mathbf{Z}_3[x]/(x^2+x+2)$$

都是域.我们略去它们的加法表和乘法表,只证明它们同构.

$$\mathbf{Z}_3[x]/(x^2+1)=\mathbf{Z}_3[\bar{x}],$$

其中 $\bar{x}=x+((x^2+1))$.$\bar{x}$ 满足$\mathbf{Z}_3$上 $x^2+1=0$.而

$$Z_3[x]/(x^2+x+2)=Z_3[\bar{\bar{x}}]$$

其中 $\bar{\bar{x}}=x+((x^2+x+2))$.$\bar{\bar{x}}$ 满足Z_3上 $x^2+x+2=0$.我们要找出$Z_3[\bar{\bar{x}}]$中的元素 α,满足方程 $x^2+1=0$.实际上由 $0=\bar{\bar{x}}^2+\bar{\bar{x}}+\bar{\bar{2}}=\bar{\bar{x}}^2+\bar{\bar{x}}+\bar{\bar{1}}+\bar{\bar{1}}=\bar{\bar{x}}^2+\bar{\bar{4}}\bar{\bar{x}}+\bar{\bar{4}}+\bar{\bar{1}}=(\bar{\bar{x}}+\bar{\bar{2}})^2+\bar{\bar{1}}$(在$Z_3$中 $\bar{\bar{4}}=\bar{\bar{1}}$).取 $\alpha=\bar{\bar{x}}+\bar{\bar{2}}$就适合 $\alpha^2+\bar{\bar{1}}=0$.由此$[Z_3(\alpha):Z_3]=2$.再由$Z_3(\alpha)\subseteq Z_3[\bar{\bar{x}}]$及$[Z_3[\bar{\bar{x}}]:Z_3]=2$,知$Z_3(\alpha)=Z_3[\bar{\bar{x}}]$.现作映射

$$\begin{array}{ccc} Z_3[x] & \overset{\varphi}{} & Z_3(\alpha)=Z_3[\bar{\bar{x}}]=Z_3[x]/(x^2+x+2) \\ p(x) & \longmapsto & p(\alpha) \end{array}$$

这是满同态,且 $\mathrm{Ker}\varphi=((x^2+1))$.由同态基本定理得同构

$$\begin{array}{ccc} Z_3[x]/(x^2+1) & & Z_3(\alpha) \\ p(\bar{x}) & & p(\alpha). \end{array}$$

其中 $\bar{x}=x+((x^2+1))$.

2. $Z_2[x]$中不可约多项式如下:

一次的:x,$x+1$,

二次的:x^2+x+1,

三次的:x^3+x^2+1,x^3+x+1,

四次的:x^4+x+1,x^4+x^3+1,$x^4+x^3+x^2+x+1$.

$Z_3[x]$中不可约多项式如下:

一次的:x,$x+1$,$x+2$,

二次的:x^2+1,x^2+x+2,x^2+2x+2,

三次的:x^3+2x+1,x^3+2x+2,x^3+x^2+2,x^3+x^2+x+2,x^3+x^2+2x+1,x^3+2x^2+1,x^3+2x^2+x+1,x^3+2x^2+2x+2,

四次的:x^4+2x^3+2,x^4+x^3+2,x^4+x^2+2x+1,x^4+2x^3+x+1,$x^4+x^3+x^2+2x+2$,x^4+2x^3+x+1,$x^4+2x^3+x^2+1$,$x^4+2x^3+x^2+2x+1$,$x^4+x^3+2x^2+2x+1$,$x^4+2x^3+x^2+x+2$,x^4+2x^2+2x+2,x^4+2x+2,x^4+x+2,x^4+2x^2+2,x^4+2x+2,x^4+x^2+2,x^4+x^2+x+1,x^4+x^2+2x+1.

找寻的步骤:(1) 列举出$Z_2[x]$($Z_3[x]$)中所有一次,二次,三次及四次多项式.(2) 一次多项式皆不可约.

(3) 检验$Z_2[x]$($Z_3[x]$)中哪些二次、三次多项式在Z_2(Z_3)中没有根,它们是不可约多项式.

(4) 检验$Z_2[x]$($Z_3[x]$)中哪些四次多项式在Z_2(Z_3)中没有根,又不是$Z_2[x]$($Z_3[x]$)中两个二次不可约多项式的乘积,则它们都是不可约多项式.

3. 它们都是 p^m 个元的有限域,由定理 3 知它们同构.

4. 取$Z_3[x]$中的四次不可约多项式 x^4+2x^2+2,则$Z_3[x]/(x^4+2x^2+2)$是

3^4 个元的域.

令 $\bar{x}=x+((x^4+2x^2+2))$,则 $\bar{x}^4+2\bar{x}^2+\bar{2}=(\bar{x}^2+\bar{1})^2+\bar{1}=0$.即 $\bar{x}^2+\bar{1}$ 是$Z_3[x]$中二次不可约多项式的根.于是有

$$Z_3[x]/(x^2+1)\cong Z_3(\bar{x}^2+\bar{1})\subseteq Z_3(\bar{x})=Z_3[x]/(x^4+2x^2+2)$$

这表明$Z_3(\bar{x}^2+\bar{1})$是$Z_3(\bar{x})$中的 3^2 个元的子域.

5.(1) $d\mid m$,令 $m=kd$.则 $p^m-1=p^{kd}-1=(p^d)^k-1=(p^d-1)(p^{d(k-1)}+p^{d(k-2)}+\cdots+p^d+1)$.故 $p^d-1\mid p^m-1$.

(2)令 $p^m-1=l(p^d-1)$.则 $x^{p^m-1}-1=x^{(p^d-1)l}-1=(x^{p^d-1}-1)(x^{(p^d-1)(l-1)}+x^{(p^d-1)(l-2)}+\cdots+x^{p^d-1}+1)$.故 $x^{p^d-1}-1\mid x^{p^m-1}-1$,即得 $x^{p^d}-x\mid x^{p^m}-x$.

6.不一定.例$Z_3[x]/(x^2+1)=F$.令 $\bar{x}=x+((x^2+1))$,它满足 $\bar{x}^2+\bar{1}=0$,当然有 $\bar{x}^4-\bar{1}=0$,即 $\bar{x}^4=\bar{1}$.但 F 是 3^2 个元的域,$F^*=F\setminus\{0\}$是 8 阶循环乘法群.故 $\bar{x}$ 不是 F^* 的生成元.

§2 有限域上不可约多项式及其周期,本原多项式及其对纠错码的应用

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1.验证$Z_3[x]/(x^2+1)$的非零元乘法群是循环群,找出生成元.x^2+1 是否本原多项式?

*2. x^3+x+1,x^4+x+1 是否$Z_2[x]$中的本原多项式?

*3.证明映射

$$\begin{array}{ccc} F_{p^m} & & F_{p^m} \\ a & \longmapsto & a^p \end{array}$$

是 F_{p^m}的自同构且保持 F_{p^m}中的素子域 F_p 中的元素不动.

4. $f(x)$是Z_p上 m 次不可约多项式.设 $\alpha\in F_{p^m}$是 $f(x)$的一个根,则 $\alpha,\alpha^p,\cdots,\alpha^{p^{m-1}}$ 是 $f(x)$的全部 m 个根.

5.设 $\beta\in F_{p^m}$,β 在Z_p上的极小多项式$f(x)$是 d 次的,则(1)β 属于 F_{p^m}中的一个 p^d 个元的子域.(2)$d\mid m$.

6.证明 F_{p^m}中元素 β 与 β^p 在Z_p上有相同的极小多项式.

*7. 设 α 是$Z_3[x]$中多项式 x^4+x+2 的一个根.把$Z_3(\alpha)$中全部元素用 $1,\alpha,\alpha^2,\alpha^3$ 的线性组合表示出来.并算出$\dfrac{1+\alpha+\alpha^3}{1+\alpha^2+\alpha^3}+\alpha+\alpha^2$.

8. 把 $x^{2^4}-x$, $x^{2^3}-x$ 分解成$Z_2[x]$上不可约多项式的乘积,把 $x^{3^3}-x$, $x^{3^2}-x$ 分解成$Z_3[x]$上不可约多项式的乘积.

*9. 取$Z_2[x]$中本原多项式 x^3+x+1.在多项式$\sum_{i=1}^{6} a_i x^{7-i}=a_1x^6+a_2x^5+\cdots+a_6x+a_7$ 与向量$(a_1,a_2,\cdots,a_7)$等同的约定下,作码集合

$$M=\{(x^3+x+1)(b_1x^3+b_2x^2+b_3x+b_4)\mid b_i\in Z_2\}.$$

(i) 取 $f(x)=x^6+x^4+c_1x^2+c_2x+c_3$,试决定 c_1,c_2,c_3 使 $f(x)$属于码集合 M.

(ii) 设 $f_1(x)=x^6+x^5+x^4+x^3+x^2+x+1$ 及 $f_2[x]=x^6+x^4+x^3+x^2+x+1$ 是接受到的向量,并设传输过程中最多错一位,试进行译码.

习题答案与解答

1. 令 $\bar{x}=x+((x^2+1))$.计算 $\bar{x}+2$ 的各方幂

$$\bar{x}+\bar{2},(\bar{x}+\bar{2})^2=\bar{x},(\bar{x}+\bar{2})^3=\bar{2}\bar{x}+\bar{2},$$
$$(\bar{x}+\bar{2})^4=\bar{2},(\bar{x}+\bar{2})^5=\bar{2}\bar{x}+\bar{1},(\bar{x}+\bar{2})^6=\bar{2}\bar{x},$$
$$(\bar{x}+\bar{2})^7=\bar{x}+\bar{1},(\bar{x}+\bar{2})^8=\bar{1}.$$

故 $\bar{x}+\bar{2}$ 生成了非零元素乘法群,它是 8 阶循环群.$\bar{x}$ 只是 4 阶元,它不是生成元,从而证明 x^2+1 不是本原多项式.

2. x^3+x+1 的周期是 $2^3-1=7$ 的因子.它不是 $x-1$ 的因子,故周期不为 1,只能是 7,所以它是本原多项式.

x^4+x+1 的周期是 $2^4-1=15$ 的因子.但 $x^4+x+1\nmid x-1,x^3-1,x^5-1$.故它的周期只能是 15.因此是本原多项式

3. $\forall\ a,b\in F_{p^m}$,有$(a+b)^p=a^p+b^p$ 及$(ab)^p=a^pb^p$ 故是 φ 同态.又由第二章§1 习题 8 知

$$(a-b)^p=a^p-b^p,$$

故这是单射.又上面的映射是有限集 F_{p^m} 中的单射,必是满射.因此是 F_{p^m} 的自同构.

由于子域 F_p 是 p 个元的域,由第二章§5 习题 5,知这映射是 F_p 上的恒等变换.

4. 设 $f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0$,$a_i\in Z_p$.因此 $a_i^p=a_i$(第二章§1 习题 8).

设 $a\in F_{p^m}$ 满足 $f(a)=0$，则 $f(a)^p=(a_m a^m+\cdots+a_0)^p=a_m^p a^{mp}+\cdots+a_1^p a^p+a_0^p=a_m(a^p)^m+\cdots+a_1 a^p+a_0=f(a^p)=0$．即 a^p 也是 $f(x)$ 的根．设 a，a^p，a^{p^2}，$\cdots$，a^{p^k} 中两两不同，$a^{p^{k+1}}$ 与前面某 a^{p^l} 相同．a_1，a^p，$\cdots$，a^{p^k} 是 $f(x)$ 的 k 个不同的根，故 $k\leqslant m$．又若 $1\leqslant l\leqslant k$．则 $a^{p^l}=(a^{p^{k+1-l}})^{p^l}$．因 $a\longrightarrow a^{p^l}$ 是 F_{p^m} 的自同构(习题 3)，上式两端元素的原象应相等，得 $a=a^{p^{k+1-l}}$．又 $k+1-l\leqslant k$，与 a，a^p，$\cdots$，a^{p^k} 中两两不同矛盾．故 $l=0$，即 $a=a^{p^{k+1}}$．

令 $g(x)=(x-a)(x-a^p)\cdots(x-a^{p^k})=x^k+b_1x^{k-1}+\cdots+b_k$．则 $b_1=-(a+a^p+\cdots+a^{p^k})$，$\cdots$，$b_k=(-1)^k a\cdot a^p\cdots a^{p^k}$，$b_1^p=(-1)^p(a^p+a^{p^2}+\cdots+a^{p^{k+1}})=-(a^p+\cdots+a^{p^k}+a)=b_1$，$\cdots$，$b_k^p=(-1)^{kp}a^p\cdot a^{p^2}\cdots a^{p^{k+1}}=(-1)^k a^p a^{p^2}\cdots a^{p^k}a=b_k$．任意 $b_i=(-1)^i$［a，a^p，$\cdots$，a^{p^k} 中任取 i 个的乘积之和］，$b_i^p=((-1)^i)^p$［a^p，a^{p^2}，$\cdots$，$a^{p^{k+1}}$ 中任取 i 个的乘积之和］$=(-1)^i$［a^p，a^{p^2}，$\cdots$，a^{p^k}，a 中任取 i 个的乘积之和］$=b_i$．即所有 b_i 满足 $x^p-x=0$，故所有 b_i 属于 F_{p^m} 的子域 $\mathbf{Z}_p$ 之中，因此 $g(x)$ 是 $\mathbf{Z}_p$ 上的多项式．因 $f(x)$，$g(x)$ 在 $F_{p^m}[x]$ 中有公因式 $(x-a)$，故 $f(x)$，$g(x)$ 在 $\mathbf{Z}_p[x]$ 中不互素，又 $f(x)$ 是 $\mathbf{Z}_p[x]$ 中不可约多项式，且 $g(x)$ 的次数 $\leqslant m$．故 $f(x)$ 与 $g(x)$ 是相伴的．因而 $k=m$，且 a，a^p，a^{p^2}，$\cdots$，a^{p^m} 是 $f(x)$ 的全部 m 个根．

5．因 $f(x)$ 是 β 在 $\mathbf{Z}_p$ 上的极小多项式，由第二章 §2 定理 4，$f(x)$ 在 $\mathbf{Z}_p[x]$ 中不可约．由 $f(\beta)=0$，有

$$F_{p^m}\supseteq\mathbf{Z}_p(\beta)\cong\mathbf{Z}_p[x]/(f(x)).$$

又 $f(x)$ 是 d 次的，故 $\mathbf{Z}_p(\beta)$ 是 p^d 个元的子域，再由定理 4 知 $d\mid m$．

6．设 F_{p^m} 的元 β 在 $\mathbf{Z}_p$ 上的极小多项式为 $f(x)$．由第二章 § 定理 4 知它在 $\mathbf{Z}_p[x]$ 中不可约．再由第 4 题，$f(\beta^p)=0$．这时 $f(x)$ 不可约，仍由第二章 § 定理 4，它是 β^p 在 $\mathbf{Z}_p$ 上的极小多项式．

7．由 §1 习题 2，知 x^4+x+2 是 $Z_3[x]$ 中不可约多项式．α 是它的根，故

$$Z_3(\alpha)=\{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3\mid a_0,a_1,a_2,a_3\in Z_3\}.$$

易计算知，$\alpha^2(\alpha^3+\alpha^2+1)-(\alpha+1)(\alpha^4+\alpha+2)=1$，即有 $\alpha^2(\alpha^3+\alpha^2+1)=1$．于是

$$\frac{1+\alpha+\alpha^3}{1+\alpha^2+\alpha^3}+\alpha+\alpha^2=\alpha^2(1+\alpha+\alpha^3)+\alpha+\alpha^2=\alpha^3+\alpha^2+2\alpha.$$

8．$x^{2^3}-x=x(x+1)(x^3+x+1)(x^3+x^2+1)$，

$x^{2^4}-x=x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$，

$x^{3^2}-x=x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$,

$x^{3^3}-x=x(x+1)(x+2)(x^3+2x+1)(x^3+2x+2)(x^3+x^2+2)(x^3+x^2+x+2)(x^3+x^2+2x+1)(x^3+2x^2+1)(x^3+2x^2+x+1)(x^3+2x^2+2x+2)$.

9. (i) 作除法算式,$x^6+x^4=(x^3+1)(x^3+x+1)+x+1$.取 $C_1=0, C_2=1, C_3=1, f(x)=x^6+x^4+x+1=(x^3+1)(x^3+x+1)$就属于码集合 M.

(ii) $f_1(x)=(x^3+x^2+1)(x^3+x+1)$,故传输过程中无错误.$f_2(x)=x^3(x^3+x+1)+x^2+x+1$.作计算:

$x(x^2+x+1)=x^3+x^2+x=(x^3+x+1)+x^2+1\equiv x^2+1,(\mathrm{mod}\, x^3+x+1)$,

$x^2(x^2+x+1)=x(x^2+1)=(x^3+x+1)+1\equiv 1,(\mathrm{mod}\, x^3+x+1)$,

即 $x^2(x^2+x+1)\equiv 1$.但 $x^2\cdot x^5=x^7\equiv 1$,故 $x^5\equiv x^2+x+1,(\mathrm{mod}\, x^3+x+1)$.这即说明 $f_2(x)$错在 x^5 项上,原来输出的码字应为 $f_2(x)+x^5=x^6+x^5+x^4+x^3+x^2+x+1$.

§3 线性移位寄存器序列

习 题

以下习题中打 * 者为必作题,其余为选作题.

1. F_p(p 为素数)上首项系数为 1 的 m 次本原多项式的个数为 $\varphi(p^m-1)/m$,这里 φ 是欧拉函数(参见第二章 §5).并算出$\mathbf{Z}_2$,$\mathbf{Z}_3$上三次、四次本原多项式的数目.

*2. 作出$\mathbf{Z}_2$上两个周期为 7 的 m 序列(写出 2 个周期的长度).

*3. 设 F_2 上序列 $\boldsymbol{a}=(a_0, a_1, a_2, \cdots)$的周期为 e.证明

(i) 若有 e'使 $a_{k+e'}=a_k, k=0,1,2,\cdots$,则 $e\mid e'$.

(ii) 若令 $S_0=(a_0,\cdots,a_{e-1}), S_1=(a_1,\cdots,a_e),\cdots, S_{e-1}=(a_{e-1},\cdots,a_{2e-2})$,则它们两两不同.

*4. 设 $f(x)$是 F_2 上 n 次不可约多项式,则

(i) $G(f)$是 F_2 上向量空间.

(ii) 对任意 $\boldsymbol{a}\in G(f)$.令 $S_{\boldsymbol{a}}=(a_0, a_1,\cdots, a_{n-1})$,称为 $\boldsymbol{a}$ 的初始状态向量.则$\forall\ \boldsymbol{a},\boldsymbol{b}\in G(f)$,$\boldsymbol{a}=\boldsymbol{b}$ 当且仅当 $S_{\boldsymbol{a}}=S_{\boldsymbol{b}}$.

(iii) $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_k,\boldsymbol{a}\in G(f), l_1,\cdots,l_k\in F_2$,则

$\boldsymbol{a}=l_1\boldsymbol{a}_1+\cdots+l_k\boldsymbol{a}_k$ 当且仅当 $S_{\boldsymbol{a}}=l_1S_{\boldsymbol{a}_1}+\cdots+l_kS_{\boldsymbol{a}_k}$.

于是 $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_k$ 线性相关当且仅当 $S_{\boldsymbol{a}_1},\cdots,S_{\boldsymbol{a}_k}$ 线性相关.

(iv) $G(f)$是 F_2 上 n 维空间.

5. 设 $f(x)$是 $F_2[x]$中 n 次本原多项式,$\boldsymbol{a}$ 是 $G(f)$中非零序列,即 m 序列,则

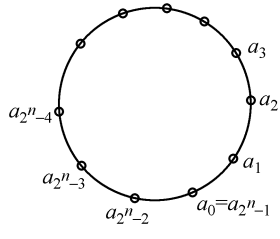
$$\boldsymbol{a}=\boldsymbol{a}_0,L\boldsymbol{a}=\boldsymbol{a}_1,\cdots,L^{2^n-2}\boldsymbol{a}=\boldsymbol{a}_{2^n-2}$$

是 $G(f)$中全部非零序列.进一步 $S_{\boldsymbol{a}_0},S_{\boldsymbol{a}_1},\cdots,S_{\boldsymbol{a}_{2^n-2}}$全不相同,它们是 F_2 上 n 元向量空间中全部非零向量.

6. 设

$$\boldsymbol{a}=(a_0,a_1,a_2,\cdots)$$

是 F_2 上周期为 2^n-1 的 m 序列.将 $\boldsymbol{a}$ 的一个周期$(a_0,a_1,\cdots,a_{2^n-2})$中的元



依次排在圆周上,并使 a_{2^n-2}与 $a_0=a_{a^n-1}$相邻,则 F_2 上的任一 k 元组$(1\leqslant k\leqslant n)$,

$$(b_1,b_2,\cdots,b_k)$$

在上述圆周中出现的次数为

$$2^{n-k},\quad \text{若}(b_1,b_2,\cdots,b_k)\neq(0,0,\cdots,0),$$

$$2^{n-k}-1,\quad \text{若}(b_1,b_2,\cdots,b_k)=(0,0,\cdots,0).$$

(考察有多少个 $S_{\boldsymbol{a}_i}$的前 k 个元正是 $b_1,b_2,\cdots,b_k$).

7. $\boldsymbol{a}$ 为 F_2 上周期为 2^n-1 的 m 序列,则在 $\boldsymbol{a}$ 的一个周期中 1 的数目为 2^{n-1},0 的数目为 $2^{n-1}-1$.

8. 对习题 2 中作出的 F_2 上周期为 7 的两个 m 序列的一个周期排成圆圈如习题 6,数出 1,0,01,10,101,110,出现的次数.

习题答案与解答

1. 考虑域 F_{p^m},它由 F_p 上多项式 $x^{p^m}-x$ 的全部根组成.将 $x^{p^m}-x$ 分解成 F_p 上不可约多项式的乘积.任一 F_p 上 m 次不可约多项式 $f(x)$都是它的因子,

故 $f(x)$在 F_{p^m}中有 m 个根.任取一根 α,则 $F_{p^m}=F_p(\alpha)\cong F_p[x]/(f(x))=F(\bar{x})$.其中 $\bar{x}=x+(f(x))$.由此知 $f(x)$是 F_p 上 m 次本原多项式当且仅当 $\bar{x}$ 是 p^m-1 阶乘法循环群 $F_p(\bar{x})\setminus\{0\}$的生成元当且仅当 α 是乘法循环群 $F_p(\alpha)\setminus\{0\}=F_{p^m}\setminus\{0\}$的生成元.

反之,任取 $F_{p^m}\setminus\{0\}$的任一生成元 α,则它必为 F_p 上某不可约多项式 $f(x)$的根,显然 $F_{p^m}=F_p(\alpha)\cong F_p[x]/(f(x))$.比较两边元素的数目,知 $f(x)$是 m 次不可约多项式.又 α 是乘法循环群 $F_{p^m}\setminus\{0\}$的生成元,前一段证明了 $f(x)$是 F_p上 m 次本原多项式.

m 次本原多项式都是 $x^{p^m}-x$ 的因式,后者无重根,故全体 m 次本原多项式在 F_{p_m}中的全体根也各不相重.设共有 k 个 m 次本原多项式,它们共有 mk 个根,前面证明了它们是 p^m-1 阶乘法循环群 $F_{p^m}\setminus\{0\}$的全部生成元.任取一个生成元 α,由第一章§7 习题 5 知 α^n 是生成元当且仅当$(n,p^m-1)=1$.故 $F_{p^m}\setminus\{0\}$的生成元的数目等于与 p^m-1 互素的且小于 p^m-1 的正整数的数目即 $\varphi(p^m-1)$.由于 $mk=\varphi(p^m-1)$,得 $k=\frac{1}{m}\varphi(p^m-1)$.

Z_2,Z_3上 3 次,4 次本原多项式的数目分别是$\frac{1}{3}\varphi(2^3-1)$,$\frac{1}{4}\varphi(2^4-1)$,$\frac{1}{3}\varphi(3^3-1)$,$\frac{1}{4}\varphi(3^4-1)$.用第二章§5 中关于 $\varphi(n)$的公式进行计算,得到

$$\frac{1}{3}\varphi(2^3-1)=\frac{1}{3}\varphi(7)=2,$$

$$\frac{1}{4}\varphi(2^4-1)=\frac{1}{4}\varphi(15)=\frac{1}{4}\varphi(3)\varphi(5)=2,$$

$$\frac{1}{3}\varphi(3^3-1)=\frac{1}{3}\varphi(26)=\frac{1}{3}\varphi(2)\varphi(13)=4,$$

$$\frac{1}{4}\varphi(3^4-1)=\frac{1}{4}\varphi(80)=\frac{1}{4}\varphi(16)\varphi(5)=\frac{1}{4}2^4\left(1-\frac{1}{2}\right)\cdot 4=8.$$

2. 取Z_2上的三次本原多项式 x^3+x+1(Z_2上的 3 次不可约多项式都是本原多项式).作线性递归序列$a=(a_0,a_1,a_2\cdots)$,其递归关系为

$$a_{k+3}=a_{k+1}+a_k,k=0,1,2,\cdots.$$

因 x^3+x+1 为本原多项式 ,它的周期,因而上述序列的周期为 $2^3-1=7$.

取 $a_0=1,a_1=a_2=0$.可计算出

a

取 $a_0=a_1=a_2=1$,可计算出

a

3.(i) 作除法算式 $e'=le+e_1,e_1=0$ 或$0<e_1<e$.若$0<e_1<e$,则对 $k=0$,

1,2,…有

$$a_{k+e_1}=a_{k+e_1+le}=a_{k+e'}=a_k .$$

即 e_1 也是a 的周期与 e 是极小周期矛盾.故 $e_1=0$,$e'=le$.

(ii) 若有 $0\leqslant i<j\leqslant e-1$,使 $S_i=S_j$.即

$$(a_i,a_{i+1},\cdots,a_{i+e-1})=(a_j,a_{j+1},\cdots,a_{j+e-1}).$$

当 $i\geqslant 1$,由 $a_{i+e-1}=a_{i-1}$,$a_{j+e-1}=a_{j-1}$,并把上面两端向量的前 $e-1$ 个分量都向右移一位,而最后一位分量移至第一位,得到的两向量仍相等,

$$(a_{i-1},a_i,\cdots,a_{(i-1)+e-1})=(a_{j-1},a_j,\cdots,a_{(j-1)+e-1}).$$

即 $S_{i-1}=S_{j-1}$.可继续这样做,结果得到 $S_0=S_{i-i}=S_{j-i}$.于是对任意 $0\leqslant t\leqslant e-1$ 有 $a_t=a_{t+(j-i)}$.而对任意 $k=0,1,2,\cdots$,作除法算式,设 $k=le+s$,$0\leqslant s\leqslant e-1$.则 $a_k=a_{k-le}=a_s=a_{s+(j-i)}=a_{s+le+(j-i)}=a_{k+(j-i)}$.即a 有周期 $j-i$.而 $0<j-i<e$,与 e 为极小周期矛盾.故任意 $0\leqslant i<j\leqslant e-1$,必有 $S_i\neq S_j$.

4. (i) $G(f)=\{a\in V(F_2)\mid f(L)a=0\}$.$\forall$ a b $\in G(f)$,则 $f(L)$a $f(L)$b$=0$.于是 $f(L)$(a b$)=f(L)$a$+f(L)$b a b $\in G(f)$.

又设 $l\in F_2$,a $G(f)$,$f(L)$(la $l(f(L)$a la $\in G(f)$.因此 $G(f)$是 $V(F_2)$的子空间.

(ii) $\forall$ a b $G(f)$,显然a b 推出 $S_a=S_b$.反之,设 $S_a=S_b$.对 $k=0$,1,2,…,有

$$a_{k+n}=c_{n-1}a_{k+(n-1)}+\cdots+c_1a_{k+1}+c_0c_k$$

$$b_{k+n}=c_{n-1}b_{k+(n-1)}+\cdots+c_1b_{k+1}+c_0b_k .$$

由 $S_a=S_b$,并在上式中令 $k=0$,则有 $a_n=b_n$.于是 $S_{La}=(a_1,a_2,\cdots,a_n)=(b_1,b_2,\cdots,b_n)=S_{Lb}$.但 $f(L)$La $Lf(L)$a$=0$,$f(L)$Lb$=Lf(L)$b 同样可证 $S_{L^2}a=S_{L^2}b$.归纳地可证,对任意 k 有 $S_{L^k}a=S_{L^k}b$.就得到对任意 k,$a_{k+n}=b_{k+n}$.加上 $S_a=(a_0,a_1,\cdots,a_{n-1})=(b_0,b_1,\cdots,b_{n-1})=S_b$,就证明了a b

(iii) a_i有初始向量 S_{a_i}.于是若a l_1 a $_1$+…+ l_ka $_k$,则显然 $S_a=l_1S_{a_1}+\cdots+l_kS_{a_k}$.

反之,设 $S_a=l_1S_{a_1}+\cdots+l_kS_{a_k}$.因 l_1 a $_1$+…+ l_ka $_k\in G(f)$,及 $S_{l_1a_1+\cdots+l_ka}=l_1S_{a_1}+\cdots+l_kS_{a_k}=S_a$.由(ii)a l_1 a $_1$+…+ l_ka $_k$.

特别地当a 时就得到 l_1 a $_1$+…+ l_ka $_k=0$ 当且仅当 $l_1S_{a_1}+\cdots+l_kS_{a_k}=0$.即有a $_1$,…,a $_k$线性相关当且仅当 S_{a_1},S_{a_2},…,S_{a_k}线性相关.

(iv) 考虑到可取 F_2 上 n 维向量空间的任一组基作初始向量,由递归关系 $f(L)$a 得到 $G(f)$中的一组序列a $_1$,…,a $_n$.而初始向量 S_{a_1},…,S_{a_n} 是 F_2 上 n 维向量空间的基.由(iii)a $_1$,…,a $_n$也线性无关.$\forall$ a $G(f)$,S_a是 S_{a_1},…,S_{a_n}的线性组合,再由(ii),a a$_1$,…,a $_n$的线性组合,故a$_1$,…,a $_n$是 $G(f)$的一组基,因

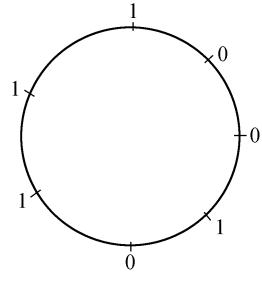
此 $G(f)$是 F_2 上 n 维线性空间.

5. $f(x)$为 F_2 上 n 次本原多项式,a　$G(f)$中非零序列,则其周期为 2^n-1.由习题 3(ii)知 $S_{a_0}, S_{a_1}, \cdots, S_{a_{2^n-2}}$互不相同,它们是 F_2 上 2^n-1 个非零的 n 维向量,但 F_2 上仅有 2^n-1 个非零的 n 维向量,故 $S_{a_1}, \cdots, S_{a_{2^n-2}}$是 F_2 上全部非零的 n 维向量.由习题 4(ii),$a_0, \cdots, a_{2^n-2}$ 是 $G(f)$中全部非零序列.

6. 设a　$a_0, a_1, a_2, \cdots)$是周期为 2^n-1 的 m 序列,由习题 5 知 $S_{a_0}, S_{a_1}, \cdots, S_{a_{2^n-2}}$是 F_2 上 2^n-1 个不同的,也即全部非零的 n 元向量.对 $1 \leqslant k \leqslant n$,$(b_1, b_2, \cdots, b_k)$每次出现必有某 $S_{a_i}=(b_1, b_2, \cdots, b_k, \cdots)$.因此它出现的次数正是这样的 S_{a_i}的数目.当$(b_1, b_2, \cdots, b_k) \neq (0, 0, \cdots, 0)$时,后面 $n-k$ 位分量可任意在 F_2 上取值,故这样的 S_a共 2^{n-k}个.若$(b_1, \cdots, b_k)=(0, 0, \cdots, 0)$,后面 $n-k$ 位分量除了不能全取零外可任意选取(因 S_{a_i}不能为零向量),故这样的 S_{a_i}共有 $2^{n-k}-1$ 个.

7. 在习题 6 中取 $k=1$.当$(b_1)=(1)$时,它出现的次数是 2^{n-1};当$(b_1)=(0)$时,它出现的次数是 $2^{n-1}-1$.

8. 习题 2 出现的周期为 7 的两个 m 序列各取一个周期,分别为 1001011 及 1110010.排成的圆圈是下列同样的圆圈.可见到 1 出现 $4(=2^{3-1})$次,0 出现 $3(=2^{3-1}-1)$次,01 出现 $2(=2^{3-2})$次,101 出现 $1(=2^{3-3})$次,110 出现 $1(=2^{3-3})$次.



第四章　有因式分解唯一性的环

内容要点

1. 基本概念:因子、倍元、相伴、不可约元、素元、因式分解及唯一性、公因子、最大公因子.

2. 整环成为唯一因分解环的充要条件.不是唯一因式分解环的例子.

3. 欧氏环及例子(Z ,域上多项式环,高斯整数环)

主理想环及其因式分解唯一性.

4. 交换环上的多项式环.唯一因式分解环上的多项式环仍是唯一因式分解环.

5. 几个典型环类的包含关系

欧氏环$\subsetneq$主理想环$\subsetneq$唯一因式分解环$\subsetneq$整环.

读后注

1. 在其它抽象代数教材中,由于内容的逻辑体系的需要,都是把本章内容作为主要内容放在域论内容之前.占用了大量教学用时,以致只能讲很少域论内容.为了教材内容现代化,为了写入应用内容和为应用所需的理论内容,我们把域论和域论的应用内容放在前面,而把本章内容放在最后.时间不够,可以少讲和不讲.这是教材内容的重要改革.

2. 本章§3 的内容是为说明一般域甚至交换环上多项式的存在性.多项式是一类运算系统.必须举出实例才能表明对它的讨论有意义.本书的第二章§6 及第三章§1 的内容都是以一般域上多项式的存在为前提的.

3. §4 中定理 1 的证明中又采用了将整系数作模 p 剩余类的方法.这个证明比以前教科书(包括本书第一版)中的证明有所简化.

4. 内容要点中第 5 点中的包含关系是严格的真包含关系,要能用例子说明此关系.

§1 整环的因式分解

习 题

以下习题中打 * 者为必作题,其余是选作题.

*1. 试说明整环中的零元,可逆元不能是不可约元的乘积.

*2. R 是整环,则它的素元是不可约元.

*3. R 是整环,则 $a\in R$ 是素元当且仅当主理想$(a)=aR$ 是非零素理想(第二章§7 习题 2).

4. 令整环

$$M=\{a+b\sqrt{3}\mathrm{i}\mid a,b\in\mathbf{Z}\}.$$

求出 M 的全部可逆元.证明它没有因式分解唯一性(举反例,有 M 中非零的不可逆元 a,它没有分解唯一性).

*5. 证明在环$\mathbf{Z}(\sqrt{-5})$中 $3(2+\sqrt{5}\mathrm{i})$和 9 没有最大公因子.

6. R 为整环.(1)$a,b\in R$,a,b 不同时为零,$a=a_1d$,$b=b_1d$,则 d 是 a,b 的最大公因子当且仅当 a_1,b_1 互素.(2)把 a,b 两个元素推广到任意 k 个元素的情形.

7. 设 M 是形为$\frac{m}{2^k}$(m 任意整数,k 非负整数)的全部有理数的集合,则它是 Q 的子环.找出 M 的全部可逆元和不可约元.

8. R 是唯一因式分解环.$a,b\in R$ 是互素的,且 $a\mid bc$,则 $a\mid c$.

*9. R 是唯一因式分解环,p 为不可约元,则 $R=R/(p)$为整环.

习题答案与解答

1. 设在整环 R 中有 $0=p_1p_2\cdots p_s$,p_i 是不可约元,于是 p_1 及 p_s 都是零因子,与 R 是整环矛盾.

又设可逆元 $u=p_1\cdots p_s$,p_i 是不可约元.并设 $uv=1$,则 $p_1p_2\cdots p_sv=1$,得出 p_1 是可逆元,与 p_1 非可逆矛盾.

2. 设 u 是素元,若 u 可约,则 $u=v_1v_2$,v_1,v_2 皆非可逆.于是 $u\mid v_1v_2$,u 又是素元,必有 $u\mid v_1$ 或 $u\mid v_2$.若 $u\mid v_1$,则 $v_1=uv$,某 $v\in R$.因此 $u=v_1v_2=u(vv_2)$.R是整环,$u\neq0$,用消去律得 $1=vv_2$.与 v_2 非可逆矛盾.同样 $u\mid v_2$ 也

有矛盾.故 u 不可约.

3. 设 aR 是非零素理想,故 a 是非零的非可逆元.对 $b,c\in R$,$a\mid bc$,则 $bc\in aR$.故 $b\in aR$ 或 $c\in aR$,即 $a\mid b$ 或 $a\mid c$,所以 a 是素元.

反之,设 a 是素元.$b,c\in R$,$bc\in aR$.于是 $a\mid bc$,有 $a\mid b$ 或 $a\mid c$.即 $b\in aR$ 或 $c\in aR$.又 a 是非零非可逆元,故 $aR\neq 0$ 及 $aR\neq R$,所以 aR 是非零素理想.

4. 设 $(a+b\sqrt{3}i)(c+d\sqrt{3}i)=1$,$a,b,c,d\in\mathbf{Z}$.对两端取复数模平方,得 $(a^2+3b^2)(c^2+3d^2)=1$.若 $b\neq 0$ 或 $d\neq 0$ 则 $3b^2\geqslant 3$ 或 $3d^2\geqslant 3$,左端必大于 1,不可能,所以 $b=0$,$d=0$,得到 $ac=1$,$a=\pm 1$.故 $a+b\sqrt{3}i$ 在 M 中可逆当且仅当 $b=0$,$a=\pm 1$.

4 在 M 中有两种分解:

$4=2\cdot 2=(1+\sqrt{3}i)(1-\sqrt{3}i)$.

下证 2,$1\pm\sqrt{3}i$ 皆为 M 中不可约元,实际上它们的模平方皆为 4.令它们中任一个为 α,设 $\alpha=\alpha_1\alpha_2$,α_1,α_2 皆非可逆.而 M 中非可逆元 $a+b\sqrt{3}i$,必有 $b\neq 0$,或 $a\neq\pm 1$,这时 $|a+b\sqrt{3}i|^2=a^2+3b^2\geqslant 3$.于是 $|\alpha_1|^2|\alpha_2|^2\geqslant 9$.而左端 $|\alpha|^2=4$,不能相等.故 2,$1\pm\sqrt{3}i$ 皆为不可约元,4 分解成 M 中的不可约元乘积的方式不唯一.

5. 要证明不存在 9 与 $3(2+\sqrt{5}i)$ 在 $\mathbf{Z}[\sqrt{5}i]$ 中的公因子 d,使得 9 与 $3(2+\sqrt{5}i)$ 的任一公因子皆是 d 的因子.

反设 $d=a+b\sqrt{5}i$,$a,b\in\mathbf{Z}$ 满足上述要求.由于 3 是 9 与 $3(2+\sqrt{5}i)$ 的公因子.故 $3\mid d$,即有 $c,e\in\mathbf{Z}$ 使 $a+b\sqrt{5}i=3(c+e\sqrt{5}i)$.于是 $a=3c$,$b=3e$.但 $d\mid 9$,两边取模平方得 $(3c)^2+5(3e)^2\mid 9^2$,则有 $c^2+5e^2\mid 3^2$.只有 $c=\pm 2$,$e=\pm 1$;$c=\pm 3$;$e=0$ 这几种情况适合这条件.故 $c+e\sqrt{5}i$ 的仅有的可能为 $\pm 2\pm\sqrt{5}i$,± 3.即 $d=a+b\sqrt{5}i$ 的仅有的可能为 $\pm 6\ \pm 3\sqrt{5}i$,± 9.

若 $d=\pm 6\pm 3\sqrt{5}i$,$d\mid 9$,$9=d\alpha$.取模平方 $9^2=|d|^2|\alpha|^2=9^2|\alpha|^2$.得 $|\alpha|=1$ 故 $\alpha=\pm 1$.$9=\pm d$,这不可能.

若 $d=\pm 9$,$d\mid 3(2+\sqrt{5}i)$,$3(2+\sqrt{5}i)=d\alpha$.取模平方,$9^2=|d|^2|\alpha|^2=9^2|\alpha|^2$.得 $|\alpha|=1$,$\alpha=\pm 1$.$3(2+\sqrt{5}i)=\pm d$ 也不可能.

故 9,$3(2+\sqrt{5}i)$ 在 $\mathbf{Z}[\sqrt{5}i]$ 中没有最大公因子.

6. (1) 这时 $d\neq 0$.设 a_1,b_1 不互素,则有 d_1 非可逆元是它们的公因子.则 dd_1 是 a,b 的公因子,而 d 为最大公因子,故 $dd_1\mid d$.有 $d_2\in R$,$dd_1d_2=d$.R 是整环,用乘法消去律得 $d_1d_2=1$,即 d_1 是可逆元,矛盾.故 a_1,b_1 互素.

反之,设 a_1,b_1 互素.又设 d_1 是 a,b 的最大公因子.则 $d\mid d_1$,有 $d_2\in R$ 使 $d_1=dd_2$.d_1 是 a,b 的因子,有 $a_2,b_2\in R$ 使 $a=d_1a_2=dd_2a_2=da_1$,及 $b=d_1b_2=dd_2b_2=db_1$.用消去律 $d_1a_2=a_1$,$d_2b_2=b_1$.于是 d_2 是 a_1,b_1 的公因

子.但 a_1, b_1 互素故 d_2 为可逆元.由此知 $d=d_1(d_2)^{-1}$ 也是 a, b 的最大公因子.

(2) 略.

7. 由于 M 中的元具有形式 $\frac{m}{2^k}$,它们的和,差,积仍为这种形式的元,故 M 是Q

设 $\frac{m}{2^k}$ 为 M 中可逆元,则有 $\frac{n}{2^l}$ 使 $\frac{m}{2^k}\frac{n}{2^l}=1$.故 m 必为 $\pm 2^t$, t 为非负整数.反之,对 $\frac{\pm 2^t}{2^k}$, k, t 皆非负整数,则 $\pm\frac{2^k}{2^t}$ 属于 M,且 $\frac{\pm 2^t}{2^k}\cdot\frac{\pm 2^k}{2^t}=1$,故在 M 中可逆.因此

$$M \text{ 中可逆元集}=\left\{\frac{\pm 2^t}{2^k}\,\middle|\, t, k \text{ 皆非负整数}\right\}.$$

由此易知,M 中非可逆元集 $=\left\{\frac{m}{2^k}\,\middle|\, m \text{ 是具有奇素数因子的非负整数}\right\}$.

下面证明 $\frac{m}{2^k}$ 为 M 中不可约元当且仅当 $m=\pm p\cdot 2^t$,其中 p 为奇素数, t 为非负整数.

先设 $\frac{m}{2^k}$, $m=\pm p\cdot 2^t$, p 为奇素数.若 $\frac{m}{2^k}=\frac{m_1}{2^{k_1}}\cdot\frac{m_2}{2^{k_2}}$,则 $m_1\cdot m_2=\pm p\cdot 2^{t_1}$.因此 m_1, m_2 中的一个只是 2 的非负方幂,于是 $\frac{m_1}{2^{k_1}}\cdot\frac{m_2}{2^{k_2}}$ 中有一个是可逆元.因此 $\frac{m}{2^k}$ 是不可约元.

再设 $\frac{m}{2^k}$, $m=p_1 p_2 m_1$, p_1, p_2 皆为奇素数,可以相同, m_1 为整数.则 $\frac{m}{2^k}=\frac{p_1}{2^0}\cdot\frac{p_2 m_1}{2^k}$,右端是 M 中两个非可逆元的乘积.因此 $\frac{m}{2^k}$ 为 M 中可约元.故若 $\frac{m}{2^k}$ 在 M 中不可约,必须 $m=\pm p\cdot 2^t$,其中 p 为奇素数, t 非负整数,证毕.

8. 设 $bc=ad$,将 b, c 分解成不可约因式的乘积 $b=p_1\cdots p_s$, $c=p_{s+1}\cdots p_t$.再将 a, d 分解成不可约因式的乘积 $a=q_1\cdots q_r$, $d=q_{r+1}\cdots q_l$.由 $bc=ad$,及因式分解唯一性知 $t=l$,及有 1,2,…, t 的一个排列 $i_1 i_2\cdots i_t$,使 p_{i_j} 与 q_j 相伴.对 $1\leqslant j\leqslant r$, q_j 是 a 的不可约因子,则 p_{i_j} 不在 $p_1, \cdots, p_s$ 之中,否则 a 与 b 有公因子 p_{i_j},与它们互素矛盾.这样 $p_{i_1}\cdots p_{i_r}$ 必出现在 c 的分解中,它与 $a=q_1\cdots q_r$ 相伴,故 $a\mid c$.

9. R 为唯一因式分解环,由 §1 定理 1 及定义 2 知它的不可约元 p 为素元.设 $\bar{c}, \bar{d}$ 是 R 的两个非零元,来证 $\bar{c}\bar{d}\neq\bar{0}$,即 R 是整环.反证法设 $\overline{cd}=\bar{c}\bar{d}=\bar{0}$,

则 $p \mid cd$、因 p 为素元,则或 $p \mid c$ 或 $p \mid d$,即或 $\bar{c}=\bar{0}$ 或 $\bar{d}=\bar{0}$.矛盾.故 $\overline{cd} \neq \bar{0}$,$R$ 为整环.

§2 欧氏环,主理想整环

习 题

以下习题中打 * 者为必作题,其余为选作题.

*1. 主理想环的商环是主理想环.

*2. R 是主理想环,a 为 R 中不可约元,则

(i)(a)为极大理想;(ii) a 为素元;

(iii)每个非 0 素理想(见第二章 §7 习题 2)是极大理想;

(iv) $R/(a)$是域.

3. 证明 $M=\{a+b\sqrt{2}\,i \mid a,b \in \mathbf{Z}\}$是欧氏环(仿例 1).

*4. p 是素数.令 $R=\left\{\dfrac{a}{b} \,\middle|\, a,b \in \mathbf{Z},(b,p)=1\right\}$.

(i)证明 R 是整环;

(ii)求出 R 的所有可逆元;

(iii)证明 R 的所有非可逆元组成 R 的唯一极大理想;

(iv)上述极大理想是主理想;

(v)求出 R 的全部理想.

*5. 找出高斯整数环$\mathbf{Z}\quad\{a+b\mathrm{i} \mid a,b \in \mathbf{Z}\}$的全部可逆元.

*6. 高斯整数环的元素 a 满足 $\delta(a)=$素数,则 a 为不可约元.

7. R 是欧氏环,求证

(i)若 $\varepsilon \in R^{*}=R \setminus \{0\}$,则 ε 是 R 中可逆元当且仅当 $\forall\, a \in R^{*}$ 有 $\delta(\varepsilon) \leqslant \delta(a)$.

(ii)设 $a \in R^{*}$,a 不可逆.若对所有不可逆元 $b \in R^{*}$ 都有 $\delta(a) \leqslant \delta(b)$,则 a 是 R 中不可约元.

8. $R=\left\{\dfrac{1}{2}a+\dfrac{1}{2}b\sqrt{19}\mathrm{i} \,\middle|\, a,b \in \mathbf{Z}\right\}$,则 R 是主理想环但不是欧氏环(参看 Motzkin,The Euclidean algorithm,Bull.Amer.Math.Soc.55.1142—1146(1949).或参看张勤海著《抽象代数》(科学出版社,2004)中推论 2.4.14 及命题 2.4.16).

9. R 是主理想环.d 是 R 中非零元,则 R 中只有有限个不同的素理想包含

(d)(提示:$(d)\subset(k)\Rightarrow k\mid d$).

习题答案与解答

1. 设 R 为主理想环,$R=R/I$ 为商环.任取一个理想 N,令 $N=\{r\in R\mid \bar{r}=r+I\in N\}$.易证它是 R 的理想并包含 I(参见第二章§4 习题 8).R 是主理想环,故有 $N=aR$.于是 $N=\bar{a}R$,即 R 是主理想环.

2. (i) 设有 $(a)\subset M\subset R$,M 为 R 的理想.故有 $b\in M$ 使 $M=(b)$.$a\in(b)$,有 $a=br$,$r\in R$.因 a 不可约,b,r 中必有可逆元,若 b 可逆,则 $(b)=R$;若 r 可逆,则 $(a)=(b)$.故 (a)是极大理想.

(ii) 主理想环是唯一因式分解环,它的不可约元皆为素元.

(iii) 设 (b)是非零素理想,由§1 习题 3,b 为素元.因而是不可约元.由(i),(b)为极大理想.

(iv) 由(i),(a)为极大理想,故 $R/(a)$为域.

3. 仿例 1,令 δ:

$$M^{*}\longrightarrow \mathbf{Z}^{+}(\text{非负整数集})$$

$$\delta(a+b\sqrt{2}\,i)=a^{2}+2b^{2}.$$

当 $a+b\sqrt{2}\,i\neq 0$,$\delta(a+b\sqrt{2}\,i)\geqslant 1$,具有性质

(i) $\delta(\alpha\beta)=\delta(\alpha)\delta(\beta)\geqslant\delta(\beta)$,$\forall\,\alpha,\beta\in M^{*}$.

(ii) $\forall\,\alpha,\beta\in M$,$\beta\neq 0$,我们证明有 $q,r\in R$ 使得 $\alpha=q\beta+\gamma$,且 $\gamma=0$ 或 $\delta(\gamma)<\delta(\beta)$.

证明　对 $\alpha\in M$ 及 $\beta\in M^{*}$,可写 $\alpha\beta^{-1}=a+b\sqrt{2}\,i$,这几 $a,b\in\mathbf{Q}$ 选最接近 a,b 的整数 k,l 使 $a=k+\nu$,$b=l+\mu$,其中 $|\mu|\leqslant\frac{1}{2}$,$|\nu|\leqslant\frac{1}{2}$.则

$$\alpha=\beta[(k+\nu)+(l+\mu)\sqrt{2}\,i]=\beta[k+l\sqrt{2}\,i]+\beta(\nu+\mu\sqrt{2}\,i).$$

令 $q=k+l\sqrt{2}\,i$,$\gamma=\beta(\nu+\mu\sqrt{2}\,i)=\alpha-\beta q\in M$.则 $\alpha=q\beta+\gamma$,且若 $\gamma\neq 0$,

$$\delta(\gamma)=|\gamma|^{2}=|\beta|^{2}\,|\nu+\mu\sqrt{2}\,i|^{2}\leqslant|\beta|^{2}\left(\frac{1}{4}+\frac{2}{4}\right)=\frac{3}{4}\,|\beta|^{2}<\delta(\beta).$$

故 $M=\{a+b\sqrt{2}\,i\mid a,b\in\mathbf{Z}\}$是欧氏环.

4. (i) 设 $\frac{a_1}{b_1},\frac{a_2}{b_2}\in R$,$(b_i,p)=1$,$i=1,2$.于是 $(b_1b_2,p)=1$,$\frac{a_1a_2}{b_1b_2}\in R$,$\frac{a_1}{b_1}\pm\frac{a_2}{b_2}=\frac{b_2a_1\pm b_1a_2}{b_1b_2}\in R$.故 R 是 $\mathbf{Q}$ 的子环,因而是整环.

(ii) $(b,p)=1$.若 $\frac{a}{b}$ 在 R 中可逆,存在 $\frac{c}{d}\in R$ 使 $\frac{a}{b}\frac{c}{d}=1$.这时 $(b,p)=(d,p)=1$,故 $(bd,p)=1$.由 $ac=bd$,于是 $(a,p)=1$.

反之，$\frac{a}{b}\in R$，若$(a,p)=1$，则$\frac{b}{a}\in R$，$\frac{a}{b}\cdot\frac{b}{a}=1$.即$\frac{a}{b}$在 R 中可逆.故

R 中可逆元集$=\left\{\frac{a}{b}\,\middle|\,a,b\in\mathbf{Z},(b,p)=(a,p)=1\right\}$.

(iii) 由(ii)知$\frac{a}{b}\in R$ 非可逆当且仅当$(b,p)=1$ 及 $p\mid a$.

令 $M=\{R$ 中非可逆元$\}$.$\forall\frac{a}{b},\frac{c}{d}\in M$，即有 $p\mid a,p\mid c$.$\frac{a}{b}\pm\frac{c}{d}=\frac{bc\pm ad}{db}$，这时$(db,p)=1$，$p\mid bc\pm ad$.故$\frac{a}{b}\pm\frac{c}{d}$非可逆，属于 M.

又$\forall\frac{a}{b}\in M,\frac{c}{d}\in R$，$\frac{c}{d}\cdot\frac{a}{b}=\frac{ac}{db}$.这时$(db,p)=1$ 及 $p\mid ac$，故$\frac{c}{d}\cdot\frac{a}{b}$是非可逆元，属于 M.这就证明了 M 是 R 的理想.

设 M_1 是 R 的真理想，则 M_1 中元皆为 R 中的非可逆元，故 $M_1\subset M$，即 M 为 R 的唯一的极大理想.

(iv) 易知 $M=\left\{\frac{a}{b}\,\middle|\,(b,p)=1,p\mid a\right\}=pR$，故为主理想.

(v) 设 M_1 是 R 的任一非零理想，$M_1\subset M$.任意$0\neq\frac{a}{b}\in M_1$，$(b,p)=1$，$p\mid a$.令 M_1 的全体元$\frac{a}{b}$中使$p^l\mid a$的最小的 l 值为 k，$k\geqslant 1$，则 $M_1\subseteq p^kR$.又设 M_1 中具有 p^k 因子的元是$\frac{p^kc}{d}$，$(d,p)=(c,p)=1$.则 $p^k=\frac{p^kc}{d}\cdot\frac{d}{c}\in M_1$，于是 $p^kR\subseteq M_1$，即有 $M_1=p^kR$.

也易知任一 p^kR 也是 R 的理想.故 R 的全部理想是 p^kR，$k=0,1,2,\cdots$，及零理想.

5. 设 $a+bi$ 是$\mathbf{Z}[i]$中可逆元，则有 $c+di\in\mathbf{Z}[i]$使$(a+bi)(c+di)=1$.两边取模平方就得$(a^2+b^2)(c^2+d^2)=1$.只能 $a^2+b^2=1$，有四个可能 $a=\pm1,b=0$；$a=0,b=\pm1$.$\mathbf{Z}[i]$中只有四个可逆元$\pm1,\pm i$.

6. 设 $a\in\mathbf{Z}[i]$，$\delta(a)=$素数.若 $a=bc,b,c\in\mathbf{Z}[i]$.因 $\delta(a)=|a|^2$，故 $\delta(a)=\delta(b)\delta(c)$.由于 $\delta(a)$为素数，$\delta(b)$或 $\delta(c)=1$.由习题 5，知 b 或 c 为可逆元.故 a 为$\mathbf{Z}[i]$中不可约元.

7. 设 ε 是 R 中可逆元，则有 $\varepsilon r=1$.对 $a\in R^*$，有 $\varepsilon ra=a$，由 δ 的性质知 $\delta(a)\geqslant\delta(\varepsilon)$.

反之，对 $\varepsilon\in R^*$，若$\forall\,a\in R^*$ 皆有 $\delta(a)\geqslant\delta(\varepsilon)$.用欧氏环的定义，对 $1,\varepsilon$ 有 $q,r\in R$ 使

$$1=q\varepsilon+r,\ r=0\text{ 或 }\delta(r)<\delta(\varepsilon).$$

且若 $r\neq0$，则 $\delta(r)<\delta(\varepsilon)$，这与题设矛盾.故 $r=0$，得 $1=q\varepsilon$，即 ε 为可逆元.

(ii) 设 a 有题设的性质，若 $a=bc$，b,c 皆非可逆.设有 q,r 使

$b=qa+r$，

$r=0$ 或 $\delta(r)<\delta(a)$.若 $r=0$，则 $b=qa=qbc$.用消去律有 $1=qc$ 与 c 非可逆矛盾.若 $r\neq 0$，且非可逆，则 $\delta(a)>\delta(r)$与题设 $\delta(a)\leqslant\delta(r)$矛盾.故 r 为可逆元.由 $b-qa=b-qbc=b(1-qc)=r$，可得 b 为可逆元，与 b 非可逆矛盾.故 a 为 R 的不可约元.

8. 不作要求，可参看所列文献.

9. R 为主理想环，若某一素理想包含(d)，可设该理想为(k).设 $d=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$，$p_1,\cdots,p_s$ 是不相伴的不可约元或素元.(k)是素理想，$(d)\subseteq(k)$，则(k)不为零.由习题 3 知 k 为素元，又 $k\mid d$，知 k 与 $p_1,\cdots,p_s$ 之一相伴，故(k)为(p_i)之一，$1\leqslant i\leqslant s$.

§3 交换环上多项式环

习 题

以下习题中打 * 者为必作题，其余为选作题.

*1. R 是整环，则 $R[x]$中可逆元一定是 R 中可逆元.

2. 设 R 是有限域.令

$$R_1=\{R\text{ 到 }R\text{ 的全部映射的集合}\}.$$

R_1 上有加法和乘法：$f_1,f_2\in R_1$，令$\forall\ a\in R$，

$$(f_1+f_2)(a)=f_1(a)+f_2(a),$$
$$(f_1\cdot f_2)(a)=f_1(a)f_2(a).$$

易知 R_1 在这两个运算下成环.其单位元 e 为：$\forall\ a\in R$，$e(a)=1$.

对$\forall\ r\in R$，作 R_1 中映射 $f_{(r)}$：$f_{(r)}(a)=r$，$\forall\ a\in R$.它们组成 R_1 的子环，并与 R 同构.干脆记成 R，于是 R_1 是 R 的扩环，并将 $f_{(r)}$记成 r.

令 u 是 R 的恒等映射：$u(a)=a$，$\forall\ a\in R$.证明 u 不是 R 上不定元.

*3. Z 是整数环，则 $a+b\mathrm{i}$，$a,b\in$Z，不是Z 上不定元.

习题答案与解答

1. 设 $f(x)\in R[x]$，在 $R[x]$中可逆，则有 $g(x)\in R[x]$使 $f(x)g(x)=1$.在整环 $R[x]$中，多项式相乘则次数相加.故必有$\partial(f(x))=\partial(g(x))=0$.即 $f(x)=a_0$，$g(x)=b_0$，皆为 R 中元，且 $a_0b_0=1$.故 $f(x)=a_0$ 是 R 中可逆元.

2. 先证明 $R_1 \supseteq R_0 = \{f_{(r)} \mid r \in R\}$ 是 R_1 的子环并与 R 同构.实际上

$$(f_{(r_1)} \pm f_{(r_2)})(a) = (r_1 \pm r_2) = f_{(r_1 \pm r_2)}(a),$$

$$(f_{(r_1)} \cdot f_{(r_2)})(a) = f_{(r_1)}(a) f_{(r_2)}(a) = r_1 r_2 = f_{(r_1 r_2)}(a).$$

即 $f_{(r_1)} \pm f_{(r_2)} = f_{(r_1 \pm r_2)}$, $f_{(r_1)} f_{(r_2)} = f_{(r_1 r_2)}$, R_0 对加,减,乘是封闭的,故是 R_1 的子环.

作映射

$$\begin{array}{ccc} R_0 & & R \\ f_{(r)} & \longmapsto & r \end{array}$$

它显然环同构.把 $f_{(r)}$ 干脆与 r 等同.则 R_1 是 R 的扩环.

现设 $R = F_{p^n}$. $\forall\ a \in R$ 满足 $a^{p^n} - a = 0$. $u^{p^n}(a) = a^{p^n}$, $u(a) = a$,即有 $(u^{p^n} - u)(a) = 0$, $\forall\ a \in R$.故 $u^{p^n} - u = 0$,这即说 u^{p^n}, u 在 R 上线性相关, u 不是 R 上不定元.

3. 令 $u = a + bi$,则 $(u-a)^2 + b^2 = 0$, $a, b \in \mathbf{Z}$.这是 u^2, u, 1 在 $\mathbf{Z}$ 上的一个线性关系,故 u 不是 $\mathbf{Z}$ 上不定元.

§4 唯一因式分解环上的多项式环

习 题

以下习题中打 * 者是必作题,其余为选作题.

下面的环 R 都是唯一因式分解环.

*1. $R[x]$的正次数多项式若是不可约元,一定是本原多项式.

*2. $f(x), g(x) \in R[x]$. $g(x)$的首项系数为 1,则有 $q(x), r(x) \in R[x]$,使

$$f(x) = g(x)q(x) + r(x),$$

其中 $r(x)$或者为零或者$\partial(r(x)) < \partial(g(x))$.

*3. $f(x) \in R[x], c \in R$ 是$f(x)$的一个根,则$(x-c) \mid f(x)$.

*4. $R[x]$中的 n 次多项式$f(x)$在 R 中最多有 n 个不同的根.于是 $f(x) = a_n x^n + \cdots + a_0$ 在 R 中若有多于 $n+1$ 个根,必是零多项式.

习题答案与解答

1. 设 $f(x)$各系数的最大公因子为 d,则 $f(x) = dg(x)$. $g(x)$为正次数必

不可逆.因 $f(x)$不可约,故 d 是 $R[x]$中可逆元.由§3 习题 1,d 是 R 中可逆元.故 $f(x)$是 $R[x]$中本原多项式.

2. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$,$g(x)=x^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$,$m\geqslant 0$.我们对 n 作归纳法.

当 $n=0$ 时是显然的.设次数$\leqslant n-1$ 时已对.若 $n<m$,$f(x)=0g(x)+f(x)$,$f(x)$就是要求的 $r(x)$.若 $n\geqslant m$.作 $f(x)-a_nx^{n-m}g(x)$,此中两多项式的首项都是 a_nx^n,两者相消.这个差多项式若为零,则 $f(x)=a_nx^{n-m}g(x)+0$,命题已对.若差多项式不为零,其次数已小于 n.用归纳假设有 $q(x)$,$r(x)$使 $f(x)-a_nx^{n-m}g(x)=q(x)g(x)+r(x)$,就有 $f(x)=(a_nx^{n-m}+q(x))g(x)+r(x)$,其中 $r(x)=0$ 或$\partial(r(x))<\partial(g(x))$.完成了归纳法.

3. 用$(x-c)$去除 $f(x)$,由习题 2 可得

$$f(x)=(x-c)q(x)+r,$$

这时 $r\in R$.两边用 c 代入,$0=f(c)=(c-c)q(c)+r$.故 $r=0$.即得 $f(x)=(x-c)q(x)$,$(x-c)\mid f(x)$.

4. 这时 $R[x]$是唯一因式分解环.设 $f(x)$有 $n+1$ 个不同的根 $\alpha_1,\alpha_2,\cdots,\alpha_n,\alpha_{n+1}$.由习题 3,$(x-\alpha_i)\mid f(x)$,$i=1,2,\cdots,n+1$.先设 $f(x)=(x-\alpha_1)q_1(x)$.用 α_2 代入得 $0=(\alpha_2-\alpha_1)q_1(\alpha_2)$.因 $\alpha_2\neq\alpha_1$,知 $q_1(\alpha_2)=0$.仍由习题 3,$q_1(x)=(x-\alpha_2)q_2(x)$,于是 $f(x)=(x-\alpha_1)(x-\alpha_2)q_2(x)$.同样 α_3 代入,得 $q_2(\alpha_3)=0$.于是 $q_2(x)=(x-\alpha_3)q_3(x)$.这样可得 $f(x)=(x-\alpha_1)q_1(x)=(x-\alpha_1)(x-\alpha_2)q_2(x)=\cdots=(x-\alpha_1)\cdots(x-\alpha_n)q_n$.因 $f(x)$是 n 次的,这时 q_n 必为 R 中非零元.再用 α_{n+1}代入,左端为 $f(\alpha_{n+1})$等于零,右端$(\alpha_{n+1}-\alpha_1)\cdots(\alpha_{n+1}-\alpha_n)q_n\neq 0$,矛盾.故 $f(x)$最多有 n 个不同的根.因此 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 若有 $n+1$ 个不同的根,必为零多项式.