代数学引论题解

Focus[1]

2017 年 3 月 17 日

[1]北京大学数学科学学院

第一章　代数基本概念

1. 如果在群G中,对于任意元素a,b,有$(ab)^2=a^2b^2$,证明G为交换群

证明　对于任意$a,b\in G$,由于$(ab)^2=a^2b^2$,即$abab=aabb\Rightarrow ab=ba$,从而$G$为Abel群 □

2. 如果在群G中,每个元素a都适合$a^2=e$,证明G为交换群

证明　由于$a^2=e$对$\forall a\in G$成立,因此,对任意$a,b\in G$,有$(ab)^2=a^2b^2$.由第一题的结论知G为Abel群 □

3. 设G是一个非空的有限集合,其中定义了一个乘法ab,适合条件

(i) $a(bc)=a(bc)$;

(ii) $ab=ac\Rightarrow b=c$;

(iii) $ac=bc\Rightarrow a=b$;

证明G在这个乘法下成一群

证明　设$G=\{a_1,\cdots,a_n\}$,由条件(ii)知,对$\forall x\in G,xa_1,\cdots,xa_n$两两不同,$\forall x\in G,a_1x,\cdots,a_nx$也两两不同,从而它们均构成了$G$ 中元素的一个排列.

特别地,考虑a_1,知存在$e\in G$,使得$ea_1=a_1$.从而对$a_k\in G$,设$a_kb=a_1$,从而$(ea_k)b=e(a_kb)=ea_1=a_1=a_kb$,从而$ea_k=a_k$. 从而$G$中存在左单位元$e$.

由于对于$\forall x\in G$,存在y,使得$yx=e$,从而每个元素均存在左逆,从而G在这个乘法下构成一个群 □

4. 设G是一个非空集合并在G内定义了一个乘法ab.证明:如果乘法满足结合律,并且对于任一对元素$a,b\in G$,下列方程

$$ax=b\quad 和\quad ya=b$$

分别在G内恒有解,则G在这乘法下成一群.

证明　任取$a\in G$,知存在$e\in G$,使得$ea=a$,对于$\forall b\in G$,由于存在$y\in G$使得$b=ay$,从而$eb=e(ay)=(ea)y=ay=b$. 从而G中存在左单位元,而由条件显然每个元素均存在左逆,从而G在此乘法下构成一个群 □

5. 在S_3中找两个元素x,y,适合$(xy)^2\neq x^2y^2$

解　由第一题,只需找两个元素不交换即可.

而事实上,$(12)(13)=(132),(13)(12)=(123)$即满足条件 □

6. 对于$n>2$,作一个$2n$阶的非交换群

解　考虑二面体群$D_n=\{e,\tau,\cdots,\tau^{n-1},\sigma,\sigma\tau,\cdots,\sigma\tau^{n-1}|\sigma^2=e,\tau^n=e,\sigma\tau=\tau^{-1}\sigma\}$ 不是阿贝尔群

事实上,有$\sigma\tau\neq\tau\sigma$,这是由于$\sigma\tau=\tau^{-1}\sigma$,而当$n>2$时,$\tau^{-1}\neq\tau$ □

7. 设G是一群,$a,b\in G$,如果$a^{-1}ba=b^r$,其中r为一正整数,证明$a^{-i}ba^i=b^{r^i}$

证明　对i使用数学归纳法,假设k时成立,下面考虑$k+1$的情形.

由于$a^{-k}ba^k=b^{r^k}$,从而$(a^{-k}ba^k)^r=(b^{r^k})^r$.即$a^{-k}b^ra^k=b^{r^{k+1}}$.又由于$a^{-1}ba=b^r$,从而$b^{r^{k+1}}=a^{-k}b^ra^k=a^{-k}(a^{-1}ba)a^k=a^{-(k+1)}ba^{k+1}$.

从而由归纳原理知原命题成立 □

8. 证明：群G为一交换群当且仅当映射$x\mapsto x^{-1}$是一个同构映射.

证明　若G为交换群,从而对$\forall x,y\in G,x^{-1}y^{-1}=y^{-1}x^{-1}=(xy)^{-1}$,而该映射显然为双射,从而题中所述的映射为同构映射.

另一方面,若上述映射为同构映射,则对$\forall x,y\in G,x^{-1}y^{-1}=(xy)^{-1}$,两边取逆得$xy=yx$,从而$G$为交换群 □

9. 设S为群G的一个非空子集合,在G中定义一个关系$a\sim b$当且仅当$ab^{-1}\in S$,证明这是一个等价关系的充分必要条件为S是一个子群

证明　若S是一个子群,则有$aa^{-1}=e\in S$,从而$a\sim a$满足自反性.而若$a\sim b$,即$ab^{-1}\in S$.从而$(ab^{-1})^{-1}=ba^{-1}\in S$, 即$b\sim a$,满足对称性.并且,若$a\sim b,b\sim c$,即$ab^{-1}\in S,bc^{-1}\in S$,则$(ab^{-1})(bc^{-1})=ac^{-1}\in S$,从而$a\sim c$, 满足传递性.从而$\sim$是一个等价关系

另一方面,若$\sim$是一个等价关系,对任取$x\in S$,$x\sim x$,从而$xx^{-1}=e\in S$,又由于$xe^{-1}=x$,结合$x,e\in S$,知$x\sim e$,于是,对任意$x,y\in S$,$x\sim e,y\sim e\Rightarrow x\sim y\Rightarrow xy^{-1}\in S$,从而$S$为子群. □

10. 设n为一正整数,$n\mathbb{Z}$为整数加法群$\mathbb{Z}$ 的一个子群,证明：$n\mathbb{Z}$与$\mathbb{Z}$同构

证明　考虑映射$f:\mathbb{Z}\to n\mathbb{Z},a\mapsto na$.显然$f$是一个同构映射 □

11. 证明：在S_4中,子集合

$$B=\{e,(12)(34),(13)(24),(14)(23)\}$$

是一个子群，并且B与U_4不同构

证明　记$a=(12)(34),b=(13)(24),c=(14)(23)$,则容易验证$a^2=b^2=c^2=e,ab=c,bc=a,ca=b$,从而$B$对乘法封闭,是$S_4$的子群.

而$a^2=b^2=c^2=e$,故任意元素的阶均为1或2,但在U_4中,i 为4阶元,故B与U_4不同构. □

12. 证明:如果在一阶为$2n$的群中有一个n阶子群,它一定是正规子群.

证明　记原来的群为G,子群为H,我们证明对$\forall g\in G,gH=Hg$.

事实上,若$g\in H$,则$gH=Hg=H$,而又由于对某个$g\notin H,G=H\cup gH=H\cup Hg$.从而对于$\forall g\notin H,gH=Hg$,从而$H$正规 □

13. 设群G的阶为一偶数,证明G中必有一元素$a\neq e$适合$a^2=e$

证明　对每个$a\in G$,将a与a^{-1}分为一组.若除了e以外,a与a^{-1}均不相同.则每一组都有2个元素,这将导致$|G|$是一个奇数,矛盾! □

14. 令

$$A=\begin{pmatrix}0&1\\1&0\end{pmatrix},B=\begin{pmatrix}\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}&0\\0&\mathrm{e}^{-\frac{2\pi\mathrm{i}}{n}}\end{pmatrix}$$

证明集合$\{B,B^2,\cdots,B^n,AB,AB^2,\cdots,AB^n\}$在矩阵的乘法下成一个群,而这个群与群$D_n$同构

证明　由矩阵的几何意义,显然同构.若严格证明则考虑相应的同构映射即可. □

15. 设i为一正整数.如果群G中任意元素a,b都适合$(ab)^k=a^kb^k,k=i,i+1,i+2$,证明$G$为交换群

证明　由于$a^{i+1}b^{i+1}=(ab)^{i+1}=(ab)^i(ab)=a^ib^iab$,等式两端左端消去$a^i$,右边消去$b$,得到$ab^i=b^ia$.

用$i+1$代替i,于是也有$ab^{i+1}=b^{i+1}a$,于是$ab^{i+1}=b^{i+1}a=b(b^ia)=b(ab^i)$，等式两端右端消去$b^i$,得$ab=ba$对$\forall a,b\in G$成立,从而$G$为交换群 □

16. 在群$SL_2(\mathbb{Q})$中,证明元素

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

的阶为4,元素

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

的阶为3,而ab为无限阶元素

证明　直接计算可得,$a^2=-1,a^3=-a,a^4=1,b^2=\begin{pmatrix}-1&-1\\1&0\end{pmatrix},b^3=\begin{pmatrix}1&0\\0&1\end{pmatrix}=1$

从而a,b的阶分别为3, 4,而$ab=\begin{pmatrix}1&1\\0&1\end{pmatrix}$,从而$(ab)^k=\begin{pmatrix}1&k\\0&1\end{pmatrix}$. 故为无限阶元素 □

17. 如果G为一交换群,证明G中全体有限阶元素组成一子群

证明　记全体有限阶元素构成的集合为S

只需证明对$a,b\in S\Rightarrow ab^{-1}\in S$.事实上,若$a,b$为有限阶元素,设阶分别为$m,n$.从而$(ab^{-1})^{mn}=a^{mn}(b^{-1})^{mn}=e$ 也为有限阶元素 □

18. 如果群G只有有限多个子群,证明G为有限群

证明　利用反证法,假设G是一个无限群,下面证明G有无穷多个子群

若G中每个元素的阶均有限,则由单个元素生成的循环群有无穷多个,矛盾！若G有一个元素a阶为无穷,则考虑$a,a^2,a^3,\cdots$生成的子群,它们两两不同且均为G的子群,也导致矛盾！从而原命题得证 □

19. 写出群D_n的全部正规子群

解　由$D_n=\{e,\tau,\cdots,\tau^{n-1},\sigma,\sigma\tau,\cdots,\sigma\tau^{n-1}|\sigma^2=e,\tau^n=e,\sigma\tau=\tau^{-1}\sigma\}$, 记$R_n=\{e,\tau,\cdots,\tau^{n-1}\}$,令$S$为$D_n$的一个正规子群,我们分两种情况讨论所有可能的$S$:

(i) 若某个$\sigma\tau^k\in S(0\le k\le n-1)$,若$S$ 正规,则$\tau^l\cdot\sigma\tau^k\cdot\tau^{-l}\in S$对$\forall 1\le l\le n-1$ 成立.即$\sigma\tau^{k-2l}\in S(\forall 1\le l\le n-1)$.于是,若$n$为奇数,则$\sigma\tau^{k-2l}$取遍所有$D_n-R_n$ 的元素,又由于$\sigma\cdot\sigma\tau^k=\tau^k$ 因此$\tau^k\in S(\forall 0\le k\le n-1)$,此时$S=D_n$.若$n$为奇数,则$\sigma\tau^{k-2l}$ 可以只取遍D_n-R_n.的一半,由τ指数为奇数和偶数的情况生成了两个子群$\{e,\tau^2,\tau^4,\cdots,\tau^{n-2},\sigma,\sigma\tau^2,\sigma\tau^4,\cdots,\sigma\tau^{n-2}\}$ 与$\{e,\tau^2,\tau^4,\cdots,\tau^{n-2},\sigma\tau,\sigma\tau^3,\cdots,\sigma\tau^{n-1}\}$ 容易验证,它们均为D_n的子群,又由于指数为2,从而为正规子群

(ii) 若任何$\sigma\tau^k$均不属于S,从而S为$R_n=\{e,\tau,\cdots,\tau^{n-1}\}$的某个子群,即$S=\{e,\tau^k,\cdots,\tau^n\}$, 其中$k$ 为某个整除n的正整数.而此时,对任何$a\in D_n$,我们验证S必然正规,即$asa^{-1}\in S$对$\forall s\in S$成立.

事实上,若$a\in R_n$,显然成立.若$a=\sigma\tau^l$, 记$s=\tau^r$,则$a^{-1}sa=\tau^{-l}\sigma\tau^r\sigma\tau^l=\tau^{-l}\tau^{-r}\tau^l=\tau^{-r}\in S$.故$S$正规. □

20. 设H,K为G的子群,证明HK也为G的子群当且仅当$HK=KH$

证明　当HK是子群时,从而$(HK)^{-1}=HK$,而$(HK)^{-1}=K^{-1}H^{-1}=KH$,从而$HK=KH$

另一方面,当$HK=KH$时,对任意$a,b\in HK,ab^{-1}\in HKK^{-1}H^{-1}=HKKH=HKH=HHK=HK$,从而$HK$为子群. □

21. 设H,K为有限群G的子群,证明：

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}$$

证明　我们在$H\times K$上定义等价关系$(h_1,k_1)\sim(h_2,k_2)\Leftrightarrow h_1k_1=h_2k_2$.我们证明每个等价类均有$|H\cap K|$个元素.

事实上,命题即为对每个$hk\in HK$,有多少个形如$h'k'\in HK$的元素,满足$hk=h'k'$.而若$hk=h'k'\Rightarrow h^{-1}h'=kk'^{-1}\Rightarrow h^{-1}h'\in H\cap K$故不同的$h$至多有$|H\cap K|$个.而对于每个$r\in H\cap K$令$h'=hr,k=r^{-1}k$,故$h'k'=hk$.从而这样就证明了每个等价类均有$|H\cap K|$个元素.

于是$|HK|=\dfrac{|H|\cdot|K|}{|H\cap K|}$ □

22. 设M,N是群G的正规子群.证明:

(i) $MN=NM$

(ii) MN是G的正规子群

(iii) 如果$M\cap N=\{e\}$,则MN/N与M同构

证明　(i) 由于N为正规子群,从而对$\forall m,mN=Nm$于是$\bigcup\limits_m mN=\bigcup\limits_m Nm\Rightarrow MN=NM$

(ii) 由上一道题的结论知,MN为G的子群.而对任意$g\in G,gMN=MgN=MNg$,从而MN为G的正规子群.

(iii) 由于$N\lhd G$,从而$N\lhd MN$.由于$M\cap N=\{e\}$,从而对于每个$g\in MN$,g可以唯一地表示为mn的形式.且$mn=nm$. 其中$m\in M,n\in N$.考虑映射

$$f:MN\to N:mn\mapsto m$$

显然f是满射.下面证明f是群同态.事实上,对$a,b\in MN$,记$a=m_1n_1,b=m_2n_2$

$$f(ab)=f(m_1n_1m_2n_2)=f(m_1m_2n_1n_2)=m_1m_2=f(m_1n_1)f(m_2n_2)=f(a)f(b)$$

于是,由第一同构定理

$$MN/\operatorname{Ker}f\cong\operatorname{Im}f\Rightarrow MN/N\cong M$$ □

23. 设G是一个群,S是G的一个非空子集合.令

$$C(S)=\{x\in G|xa=ax,\text{对一切}a\in S\},N(S)=\{x\in G|x^{-1}Sx=S\}$$

证明：

(i) $C(S),N(S)$都是G的子群

(ii) $C(S)$是$N(S)$的正规子群

证明　(i) 先证$C(S)$是G的子群,事实上,对$y\in C(S)$,由于$ya=ay,\forall a\in S$ 从而$ay^{-1}=y^{-1}a,\forall a\in S$,从而对任意$a\in S$因此,对$x,y\in C(S)$,有$xy^{-1}axay^{-1}=axy^{-1}$,于是$xy^{-1}\in C(S)$，从而得出$C(S)$为$G$的子群.

再证$N(S)$是G的子群.对$y\in N(S)$,我们有$y^{-1}Sy=S$,从而$ySy^{-1}=S$,对$x,y\in N(S)$,$x^{-1}ySy^{-1}x=x^{-1}Sx=S$, 故$xy^{-1}\in N(S)$,于是$N(S)$为$G$的子群.

(ii) 对$\forall x \in N(S), c \in C(S)$,下面证明$x^{-1}cx \in C(S)$.事实上,由于$x \in N(S)$,故对任意$a \in S$,存在$b$使得$xa = bx$, 从而$ax^{-1} = x^{-1}b$对于任意$a \in S, x^{-1}cxa = x^{-1}cbx = x^{-1}bcx = ax^{-1}cx$,因此$C(S) \lhd N(S)$ □

24. 证明任意一个2阶群与乘法群$\{1,-1\}$同构.

证明　考虑二阶群G的非单位元a,其阶只能为2,考虑同构映射$f : a \mapsto -1, e \mapsto 1$即可. □

25. 试定出所有互不同构的4阶群.

解　记此群为G,由于每个元素的阶都整除4,分两种情况讨论.

(i) 存在4阶元.从而G为循环群.同构于乘法群U_4

(ii) 每个非单位元均为2阶元,此时任意两个非单位元的乘积只能等于第三个元素.从而,该群与$\mathbb{Z}_2 \oplus \mathbb{Z}_2$同构. □

26. 若p为素数,证明:任何两个p阶群均同构.

证明　对于p阶群G,考虑非单位元a,故a的阶整除p且大于1,故只能为p,此时$G = \{e, a, \cdots, a^{p-1}\}$,从而$G \cong \mathbb{Z}_p$.因此,任何$p$阶群均与$\mathbb{Z}_p$ 同构. □

27. 设$\mathbb{Z}$为整数环,在集合$S = \mathbb{Z} \times \mathbb{Z}$上定义

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b) \cdot (c,d) = (ac+bd, ad+bc)$$

证明S在这两个运算下构成一具有单位元素的环.

证明　事实上,该单位元素为$(1,0)$,其余自行验证即可. □

28. 在整数集$\mathbb{Z}$上重新定义加法“$\oplus$”与乘法“$\odot$”为

$$a \oplus b = ab, \qquad a \odot b = a + b$$

试问Z在这两个运算下是否成一环.

解　由于不满足结合律$a \odot (b \oplus c) = a \odot b \oplus a \odot c$,从而不构成环结构 □

29. 设L为一具有单位元素的环,在L中定义:

$$a \oplus b = a + b - 1$$
$$a \odot b = a + b - ab$$

证明在新定义的运算下,L仍成具有单位元素的环,并且与原来的环同构.

证明　按照环的定义,容易验证L在所定义一环,考虑映射

$$\varphi : L \to L, a \mapsto 1 - a$$

则

$$\varphi(a) + \varphi(b) = (1-a) + 1 - b = 1 + (1 - a - b) = \varphi(a \oplus b)$$
$$\varphi(a)\varphi(b) = (1-a)(1-b) = 1 - (a + b - ab) = \varphi(a \odot b)$$

从而φ为环同态.又显然φ既单又满,故φ为同构映射.从而L在所定义的运算下与原来的环同构. □

30. 给出环L与它的一个子环S的例子,它们分别具有下列性质

1) L具有单位元素,但S无单位元素

2) L没有单位元素,但S有单位元素

3) L,S都有单位元素,但不相同

4) L不交换但S交换

解　1) 取$L=\mathbb{Z}$,$S=2\mathbb{Z}$满足条件

2) 考虑L为$\mathbb{Z}_{18}$的子环$\{0,3,6,9,12,15\}$,无单位元,但$\{0,9\}$作为其子环就有9这个单位元.

3) 与上面相同,考虑$L=\mathbb{Z}_{18}$, $S=\{0,9\}$

4) 取L为$M_n(\mathbb{R})$为实数域上的n阶矩阵环$(n\geq 2)$,而S为所有对角矩阵构成的矩阵环.故S交换. □

31. 环L中的元素e_L称为左单位,如果对所有的$a\in L$,

$$e_La=a;$$

元素e_R称为一个右单位,如果对所有$a\in L$,

$$ae_R=a;$$

证明：

(i) 如果L既有左单位又有右单位,则L具有单位元素

(ii) 如果L有左单位,L无零因子,则L具有单位元素

(iii) 如果L有左单位,但没有右单位,证明L至少有两个左单位

证明　(i) 设左单位为e_L,右单位为e_R.从而$e_Le_R=e_L$且$e_Le_R=e_R$.从而左右单位相等.它就是L的单位元素

(ii) 设该左单位为e_L,结合L无零因子知,对任意非零元$a\in L, ae_La=a(e_La)=a^2\Rightarrow(ae_L-a)a=0\Rightarrow ae_L=a$.于是$e_L$也是右单位.

(iii) 设e_L为左单位,由于e_L不是右单位.从而存在$a\in L$,使得$ae_L=b\neq a$,从而$be_L=ae_Le_L=ae_L=b$,于是$(a-b)e_L=0$,对于任意$r\in L, (a-b)r=(a-b)e_Lr=0$,于是$(a-b+e_L)r=r$对$\forall r\in L$成立.于是$a-b+e_L$也是左单位. □

32. 设F为一域,证明F无非平凡的双边理想.

证明　设I是F的一个非零理想,考虑非零元$a\in I$,由于$a^{-1}\in F$,于是$aa^{-1}=1\in I\Rightarrow I=F$.从而$F$无非平凡的双边理想. □

33. 如果L是一交换环,$a\in L$.

(i) 证明$La=\{ra|r\in L\}$是一双边理想.

(ii) 举例说明,如果L非交换,则La不一定是双边理想.

证明　(i) 容易验证La是一个子环.对$\forall r\in L$,$rLa=(rL)a\subset La$,由于L交换,从而La为左理想也是右理想.即为双边理想.

(ii) 取$L=M_2(\mathbb{R}), a=\begin{pmatrix}1&0\\1&0\end{pmatrix}$,此时$La=\begin{pmatrix}x&0\\y&0\end{pmatrix}$, $x,y\in\mathbb{R}$.但La不是右理想,事实上,例如

$$\begin{pmatrix}1&0\\1&0\end{pmatrix}\cdot\begin{pmatrix}1&1\\0&0\end{pmatrix}=\begin{pmatrix}1&1\\1&1\end{pmatrix}$$ □

34. 设I是交换环L的一个理想,令

$$\operatorname{rad}I=\{r\in L|r^n=I\text{对某个正整数}n\},$$

证明$\operatorname{rad}I$也是一理想.$\operatorname{rad}I$叫做I的**根**.

证明　先验证$\operatorname{rad}I$是子环.事实上,对任意$a,b\in\operatorname{rad}I$显然$ab\in\operatorname{rad}I$.而设$a^n\in I,b^m\in I$,从而$(a-b)^{m+n}\in I$,故$a-b\in\operatorname{rad}I$

对$a\in\operatorname{rad}I,r\in L$,设$a^n\in I$,故由于$L$交换,$(ra)^n=r^na^n\in I$,于是$ra\in\operatorname{rad}I$,从而$\operatorname{rad}I$也是理想. □

35. 设L为一具有单位元素的交换环.如果L没有非平凡的理想,则L是一域.

证明　只需证明每个非零元可逆.对非零元$a\in L$,考虑La,由33题知La为理想.故$La=L$,于是存在$b\in L$,使得$ba=1$.于是L是一域. □

36. $\mathbb{Q}$为有理数域,$M_n(\mathbb{Q})$为n阶有理系数全矩阵环.证明:$M_n(\mathbb{Q})$无非平凡的理想.(这种环称为**单环**)

证明　设某个非零矩阵$A\in K$,其中K是一理想.下面证明：$K=M_n(\mathbb{Q})$

事实上,不妨设A的矩阵元$a_{ij}\neq 0$,于是$E_{sj}AE_{is}\in K$对$\forall 1\le s\le n$成立(E_{ij}代表只有第i行第j列为1,其余均为0的矩阵). 而$E_{sj}AE_{is}$ 满足只有第s 行第s列为a_{ij},其余位置均为0,从而

$$\sum_{s=1}^{n}E_{sj}AE_{is}=a_{ij}I_n\in K$$

因此,$I_n\in K\Rightarrow K=M_n(\mathbb{Q})$ □

37. 设L为一环,a为L中一非零元素.如果有一非零元素b使$aba=0$,证明a是一左零因子或一右零因子.

证明　否则,若a既非左零因子,又非右零因子.从而$aba=0\Rightarrow ba=0\Rightarrow b=0$.矛盾! □

38. 环中元素x称为一**幂零元素**,如果有一正整数n使$x^n=0$.设a为具有单位元素的交换环中一幂零元素,证明$1-a$可逆.

证明　事实上,由于$(1-a)(1+a+\cdots+a^{n-1})=1-a^n$,故当$a$幂零时,设$a^m=0$从而$1-a^m=1$.因此

$$(1-a)(1+a+\cdots+a^{m-1})=(1+a+\cdots+a^{m-1})(1-a)=1$$

从而$1-a$可逆. □

39. 证明：在交换环中，全体幂零元素的集合是一理想.

证明　设$a,b\in L$幂零,再设$a^m=b^n=0$,从而$(a-b)^{m+n}=0,(ab)^m=0$,从而全体幂零元素构成一子环.

设$r\in L$,对于a幂零,设$a^m=0$,$(ra)^m=0$,故ra幂零.从而全体幂零元素构成一理想. □

40. 设L为一具有单位元素的有限环.证明由$xy=1$可得$yx=1$.

证明　设$L=\{a_1,\cdots,a_n\}$,考虑$ya_1,\cdots,ya_n$,由于$xya_i=a_i$,故ya_i两两不同,因此存在z,使得$yz=1$.

而$z=(xy)z=x(yz)=x$,从而$yx=1$ □

41. 在一具有单位元素的环中,如果对元素a,b有$ab=1$但$ba\neq 1$,则有无穷多个元素x,适合$ax=1$.

证明　由$ab=1$知,$aba=a\Rightarrow a(1-ba)=0$而$1-ba\neq 0$,从而$1-ba+a$也是$a$的一个右逆.下面证明若$a$有不止一个右逆,则$a$无穷多个右逆.事实上,我们有

定理1 (Kaplansky)　在幺环R中,若某个元素a有不止一个右逆,则a一定有无穷多个右逆

下面给出证明:若a只有有限多个右逆,记作$x_1,\cdots,x_n$,考虑$a(1+x_1-x_1a),a(1+x_2-x_1a),\cdots,a(1+x_n-x_1)a$,其中$1+x_1-x_1a,\cdots,1+x_n-x_1a$ 两两不同.故它们构成$x_1,\cdots,x_n$的一个排列,于是存在某个i,$1+x_1-x_ia=x_1\Rightarrow x_ia=1$,于是$x_j=(x_ia)x_j=x_i(ax_j)=x_i$,故这将推出$n=1$,矛盾! 从而原命题得证. □

42. 设L为至少有两个元素的环.如果对于每个非零元素$a\in L$都有唯一的元素b使得

$$aba=a$$

证明:

(i) L无零因子

(ii) $bab=b$

(iii) L有单位元素

(iv) L是一个体

注　第(ii)问中,$bab=b$是指若a,b满足$aba=a$,那么也一定满足$bab=b$

证明　(i) 若某个$x\in L$是L的零因子.则存在$z\neq 0$,使得$xz=0$.从而$x(y+z)x=xyx+xzx=xyx=x$.与y的唯一性矛盾.从而L无零因子.更一般地,也得到L既无左零因子也无右零因子.

(ii) 由$aba=a$,两边同乘b,得到$abab=ab\Rightarrow a(bab-b)=0\Rightarrow bab=b$

(iii) 设a,b满足条件$aba=a$.下面去证明ab就是这个环的单位元素.事实上,对任意$c\neq 0\in L$,我们去证明$cab=abc=c$.

证明一:由条件,存在$d\in L$,使得$cdc=c$,存在$d_1\in L$,使得$cabd_1cab=cab$.两边消去ab,得到$cabd_1c=c=cdc\Rightarrow d=abd_1$. 从而$cdcab=cab$,于是$dcab=ab$.右乘$ab$,得$dcabab=abab$.又由于$abab=ab$,于是$dcab=abab\Rightarrow(dc-ab)ab=0\Rightarrow dc=ab$. 从而根据$cdc=c\Rightarrow cab=c$.同理可证$abc=c$.于是$ab$就是$L$的单位元

证明二:由$aba=a\Rightarrow abac=ac\Rightarrow bac=c$,同理也有$abc=c$

(iv) 设L中的单位元为1,于是对每个$a\neq 0\in L$,存在$b\in L$,$aba=a\Rightarrow aba=a1\Rightarrow a(ba-1)=0\Rightarrow ba=1$.同理$ab=1$.故每个非零元可逆.于是$L$为一体. □

43. 令$C[0,1]$为全体定义在闭区间$[0,1]$上的连续函数构成的环,证明:

(i) 对于$C[0,1]$的非平凡理想I,一定有一实数θ,$0\leq\theta\leq 1$,使$f(\theta)=0$对所有的$f(x)\in I$成立;

(ii) $f(x)\in C[0,1]$是一零因子当且仅当点集

$$\{x\in[0,1]|f(x)=0\}$$

包含一个开区间.

证明　(i) 利用反证法.对非零理想I,如果对于任意$x_0\in[0,1]$.存在$f\in I$,使得$f(x_0)\neq 0$.将使得$f(x_0)\neq 0$的某一个函数f记作f_{x_0}.下面证明只能有$I=C[0,1]$

由f_{x_0}连续性,知存在x的某个邻域$U(x_0,\delta_{x_0})$,使得在$U(x_0,\delta_{x_0})\cap[0,1]$上,$|f(x)-f(x_0)|\leq\dfrac{|f(x_0)|}{2}$. 对每个$x\in[0,1]$, 考虑$U(x,\delta_x)$.它们构成$[0,1]$的一个覆盖,由有限覆盖定理知存在一个有限覆盖$U_{x_k}(k=1,\cdots,n)$.考虑$g_{x_k}\in C[0,1]$使得$g_{x_k}f_{x_k}$在$[0,1]$上非负且在$U(x_k,\delta_{x_k})$上为正.(这总是可以取到的).由于$I$ 为理想,从而

$$F(x)=\sum_{k=1}^{n}f_{x_k}(x)g_{x_k}(x)\in I$$

但$F(x)$在$[0,1]$上恒正,从而$\dfrac{1}{F(x)}\in C[0,1]$.因此$F(x)\cdot\dfrac{1}{F(x)}\in I$.从而导致$I=C[0,1]$为平凡理想.矛盾!

(ii) 记$A=\{x\in[0,1]|f(x)=0\}$一方面,当A含有一开区间时,记为(a,b)考虑一$g(x)$,使得$g(x)$在$(a+\varepsilon,b-\varepsilon)$上为正,$[0,1]-(a,b)$上为0即可.

另一方面,若A不含开区间,且$g\in C[0,1]$满足$fg=0$,下面证明$g=0$.反之,若g满足某个$g(x_0)\neq 0$,由g的连续性知必存在x_0的某个邻域,使得g在这个邻域内恒不为0.但由于A不含开区间,从而这个邻域内有某个x',使得$f(x')\neq 0$.从而$f(x')g(x')\neq 0$.矛盾! □

44. 令$F=\mathbb{Z}/p\mathbb{Z}$为p个元素的域.求

(i) 环$M_n(F)$的元素的个数

(ii) 群$GL_n(F)$的元素的个数

解　(i) $M_n(F)$中的每个元素有p种选法,从而$|M_n(F)|=p^{n^2}$

(ii) 由于矩阵$A\in GL_n(F)\iff A$的列向量在F中线性无关.下面利用这个性质来求出$GL_n(F)$的元素个数

事实上,第一列的向量有p^n-1种选法,而后第二列就不能选在第一列生成的子空间里,有p^n-p种选法,类似地,第三列有p^n-p^2种选法.依次这样下去我们得到

$$|GL_n(F)|=\prod_{k=0}^{n-1}(p^n-p^k)$$ □

45. 设K是一体,$a,b\in K$,a,b不等于0,且$ab\neq 1$.证明**华罗庚恒等式**:

$$a-(a^{-1}+(b^{-1}-a)^{-1})^{-1}=aba$$

证明

$$\begin{aligned}
&a-(a^{-1}+(b^{-1}-a)^{-1})^{-1}=aba\\
\iff&1-(1+(b^{-1}-a)^{-1}a)^{-1}=ba\\
\iff&1-ba=(1+(b^{-1}-a)^{-1}a)^{-1}\\
\iff&(1-ba)^{-1}=1+(a^{-1}b^{-1}-1)^{-1}
\end{aligned}$$

记$ab=x$,只需证明$(1-x)^{-1}=1+(x^{-1}-1)^{-1}$,而

$$\begin{aligned}
&(1-x)^{-1}=1+(x^{-1}-1)^{-1}\\
\iff&(1-x)(1+(x^{-1}-1)^{-1})=1\\
\iff&1-x+(x^{-1}-1)^{-1}-x(x^{-1}-1)=1\\
\iff&x=(x^{-1}-1)^{-1}-x(x^{-1}-1)^{-1}\\
\iff&x(x^{-1}-1)=1-x
\end{aligned}$$ □