问题求解（三）第11周作业

黄奕诚161220049

November 13, 2017

TJ Chapter 16

1

(a)$7\mathbb{Z}$是环，但不是域;
(b)$\mathbb{Z}_{18}$是环，但不是域;
(c)$\mathbb{Q}(\sqrt{2})$是域;
(d)$\mathbb{Q}(\sqrt{2},\sqrt{3})$是域;
(e)$\mathbb{Z}[\sqrt{3}]$是环，但不是域;
(f)R不是环;
(g)$\mathbb{Z}[i]$是环，但不是域;

3

a

由于
$1\times 1\%10=1$,
$3\times 7\%10=1$,
$7\times 3\%10=1$,
$9\times 9\%10=1$,
因此单元为1,3,7,9

b

由于
$1\times 1\%12=1$,
$5\times 5\%12=1$,
$7\times 7\%12=1$,
$11\times 11\%12=1$,
因此单元为1,5,7,11

c

由于
$1\times 1\%7=1$,
$2\times 4\%7=1$,
$3\times 5\%7=1$,
$4\times 2\%7=1$,
$5\times 3\%7=1$,
$6\times 6\%7=1$,
因此单元为1,2,3,4,5,6

d

可逆(行列式不等于0)的二阶矩阵都是单元.

e

与(d)相同，可穷举如下：$\begin{bmatrix}1&1\\0&1\end{bmatrix}$，$\begin{bmatrix}1&0\\0&1\end{bmatrix}$，$\begin{bmatrix}0&1\\1&0\end{bmatrix}$，$\begin{bmatrix}1&0\\1&1\end{bmatrix}$，$\begin{bmatrix}0&1\\1&1\end{bmatrix}$，$\begin{bmatrix}1&1\\1&0\end{bmatrix}$

12

Proof. 首先证明$\mathbb{Z}[\sqrt{3}i]$是可交换环:
加法交换律、加法结合律易证，零元即为0(此时$a=b=0$)，逆元即为相反数，乘法结合律、分配律也满足，对于乘法交换律，$(a_1+b_1\sqrt{3}i)(a_2+b_2\sqrt{3}i)=(a_1a_2-3b_1b_2)+(a_2b_1+a_1b_2)\sqrt{3}i=(a_2+b_2\sqrt{3}i)(a_1+b_1\sqrt{3}i)$，知其满足乘法交换律，故是可交换环.
此时，对于任意的非零元素$x\in\mathbb{Z}[\sqrt{3}i]$，若$xy=xz$，则$(a_1+b_1\sqrt{3}i)(a_2+b_2\sqrt{3}i)=(a_1+b_1\sqrt{3}i)(a_3+b_3\sqrt{3}i)$，可得$(a_1+b_1\sqrt{3}i)[a_2-a_3+(b_2-b_3)\sqrt{3}i]=0$，因为$x$非零，故有$(a_2-a_3)+(b_2-b_3)\sqrt{3}i=0$，有$a_2=a_3$且$b_2=b_3$，因此$y=z$，于是可证得$\mathbb{Z}[\sqrt{3}i]$是integral domain. □

17

Proof. 因为R是有单位元的环，所以存在$1\in R$，对任意的$a\in R$都有$1\cdot a=a$，由Proposition 16.1(2)可

知$(-1)a=-(1\cdot a)=-a$，得证. □

18

Proof. 由$ab+(-a)b=b(a-a)=b0=0$，得$-ab=(-a)b$，同理可得$-ab=a(-b)$，因此对于$(-a)(-b)$，有$(-a)(-b)=-(a(-b))=-(-ab)=ab$，得证. □

24

Proof. 先证明充分性：如果满足(a)(b)(c)三个条件，欲证S是R的子环，即证S在R的操作下仍然是一个环.首先，S是R的非空子集，其次S满足的三个条件及乘法分配律恰好能推得环的定义.
再证明必要性.如果H是R的子环，由于需要存在零元，故非空.又由乘法交换律易得$rs\in S$，再由加法交换律以及负元存在性可知$r-s\in S$，由此得证. □

32

Proof. 若R是一个单位元为0的环，则可知对于任意的$a\in R$，都有$0a=a0=a$，又因为$0a=a0=0$，因此可得$a=0$，由此R为单元素集合$\{0\}$. □

34

Proof. 首先，由$Z(R)$定义中的$a\in R$可知$Z(R)$是R的子集.另外，对任意$r\in R$，有$0r=r0=0$，因此$0\in Z(R)$，故$Z(R)\neq\emptyset$.其次，对于$a,b\in Z(R)$，则对任意$r\in Z(R)$，都有$ar=ra$且$br=rb$，于是两者相减可得$(a-b)r=r(a-b)$，故$a-b\in Z(R)$.两者相乘可得$arbr=rarb$，即$a(rb)r=(ra)(rb)$，即$a(br)r=(rr)(ab)$，即$(ab)r^2=r^2(ab)$，所以$ab\in Z(R)$，由此可证得$Z(R)$是R的子环.又因为对于$a,b\in Z(R)$，便有$b\in R$，必然有$ab=ba$，因此$Z(R)$是R的可交换子环. □

35

Proof. 1.对于$x,y\in\mathbb{Z}_{(p)}$，$x+y=\frac{a_1}{b_1}+\frac{a_2}{b_2}=\frac{a_1b_2+a_2b_1}{b_1b_2}$，易知$a_1b_2+a_2b_1\in\mathbb{Z}$并且$b_1b_2\in\mathbb{Z}$.又因为$gcd(b_1,p)=gcd(b_2,p)=1$，所以$gcd(b_1b_2,p)=1$，因此对加法封闭.
2.对于$x,y\in\mathbb{Z}_{(p)}$，$xy=\frac{a_1a_2}{b_1b_2}$，有$a_1a_2\in\mathbb{Z},b_1b_2\in\mathbb{Z},gcd(b_1b_2,p)=1$，因此对乘法封闭.
3.对于加法交换律、结合律，乘法结合律、分配律，由有理数的性质显然得到.
4.单位元为0，负元为相反数.
因此，$\mathbb{Z}_{(p)}$是环. □

36

Disprove

Proof. 对于矩阵集合$\mathbb{M}_2(\mathbb{Z}_2)$的子环$\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&1\\1&0\end{bmatrix},\begin{bmatrix}0&1\\1&1\end{bmatrix}\}$来说，它显然是一个integral domain，但元素个数4，不为素数，无法与Z_p同构，因此不成立. □

39

Proof. 对于integral domain来说，不能存在zero divisors，也即假若$rs=0$，则必有$r=0$或$s=0$.对于$x^2=x$，有$x^2-x=0$，即$x(x-1)=0$，得到$x=0$或$x=1$，所以integral domain唯一的幂等元是0和1.
幂等元不等于0，1的环的例子：$\mathbb{M}_2(\mathbb{R})$，此时二元幂等矩阵有无数个. □

40

Proof. 由模线性方程推论知：方程$ax\equiv b(\mod n)$有解当且仅当$gcd(a,n)|b$，而在条件中，$gcd(a,n)|d$并且$gcd(b,d)=1$，由此b无法被$gcd(a,n)$整除，因此原方程无解. □