# Problem Solving: Homework 3.11

Name: Chen Shaoyuan Student ID: 161240004

November 13, 2017

## 1 [TJ] Exercise 16-1

All of the sets except (f) are rings. Multiplication is not closed in (f).

(c), (d), (h) are fields, because they are commutative and the multiplicative inverses exist for all nonzero elements.

## 2 [TJ] Exercise 16-3

(a) 1, 3, 7, 9;

(b) 1, 5, 7, 11;

(c) 1, 2, 3, 4, 5, 6;

(d) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(\mathbb{Z}), ad \neq bc$;

(e) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

## 3 [TJ] Exercise 16-12

For every two $a+b\sqrt{3}i, c+d\sqrt{3}i \in \mathbb{Z}[\sqrt{3}i]$. their product is $(ac-3bd^2)+(ad+bc)\sqrt{3}i$, so multiplication is closed. Also $(\mathbb{Z}[\sqrt{3}i],+)$ is an abelian group, and the associative property for multiplication and the distribution property hold, so $\mathbb{Z}[\sqrt{3}i]$ is a ring. Furthermore, since the multiplication is commutative, it is a commutative ring.

The element $1 \in \mathbb{Z}[\sqrt{3}i]$ is the identity. For every two nonzero elements in $\mathbb{Z}[\sqrt{3}i]$, their product is also nonzero, so it is an integral domain.

## 4 [TJ] Exercise 16-17

Since we have $1+(-1)=0$, multiplying $a$ on both sides, the lhs becomes

$$(1+(-1))a = 1a+(-1)a = a+(-1)a$$

the rhs becomes $0a$. Since we have $0+0a = 0a = (0+0)a = 0a+0a$, and $(R,+)$ is a group, we cancel $0a$ on both sides and obtain

$$0a = 0$$

hence $a+(-1)a = 0$. Also, we have $a+(-a)=0$, which means

$$a+(-1)a = a+(-a)$$

cancelling $a$ on both sides gives

$$(-1)a = -a$$

## 5 [TJ] Exercise 16-18

We have proved in Exercise 16-17 that $(-1)a=-a$. Likewise we can prove that $a(-1)=-a$. So we have

$$(-a)(-b) = (a(-1))((-1)b) = a((-1)(-1))b$$

and we only have to prove $(-1)(-1)=1$. Recall that $0a=0$ for all $a$, which we have proved in Exercise 16-17, and we have

$$\begin{aligned} 0 = 0(-1) &= (1+(-1))(-1) = (-1)+(-1)(-1) \\ &= (-1)+1 \end{aligned}$$

So $(-1)(-1)=1$.

## 6 [TJ] Exercise 16-24

The necessity is immediate from the definition of a ring. So we only have to prove the sufficiency.

First, let's consider the condition (c). Let $r=s$ be arbitrary element in $S \neq \varnothing$, we have $r-s=0 \in S$, so the addition identity is in $S$. For every $s \in S$, let $r=0$, we get that $-s \in S$, i.e. the additive inverse of every element in $S$ is still in $S$. For every two elements $h,g \in S$, we have $h+g = h-(-g) \in S$, so the addition is closed. Therefore, $(S,+)$ is a subgroup of $(R,+)$. Furthermore, since addition is commutative in $R$, $(S,+)$ is actually an abelian group.

Note that (b) guarantees that the multiplication is closed in $S$. The associative and distributive property still hold in $S$. So $S$ is a subring of $R$.

## 7 [TJ] Exercise 16-32

For every element $s$ in $R$, we have

$$s = 1s = 0s = 0$$

so every element of $R$ is 0, i.e. $R = \{0\}$.

## 8 [TJ] Exercise 16-34

Since the addition identity 0 is commutative in multiplication ,so $0 \in R$. For every $a \in Z(R)$, since $ar = ra$ for all $r \in Z(R)$, we have $(-a)r = r(-a)$, so $-a \in Z(R)$. Also, if $a, b \in Z(R)$, we have $ar = ra$, $br = rb$, by the distributive property we have $(a+b)r = r(a+b)$, i.e. $a+b \in Z(R)$. So $(Z(R),+)$ is a subgroup of $(R,+)$. Moreover, $(Z(R),+)$ is an abelian subgroup of $(R,+)$ since + is commutative.

For every $a, b \in Z(R)$, we have $ar = ra$, $br = rb$ for all $r \in R$. Hence, $abr = arb = rab$ for all $r \in R$, i.e. $ab \in Z(R)$. The associative and distributive property still holds in $Z(R)$. So $Z(R)$ is a subring of $R$. Furthermore, by the definition of $Z(R)$, multiplication is commutative in $Z(R)$, i.e. $Z(R)$ is a commutative subring of $R$.

## 9 [TJ] Exercise 16-35

The commutative and associative property for addition, the associative property for multiplication and the distributive property hold in $\mathbb{Z}_p$.

For every $g = a/b, h = c/d \in \mathbb{Z}_p$, we have

$$a+b = a/b + c/d = (ad+bc)/bd$$

$$ab = ac/bd$$

since $\gcd(b,p) = \gcd(d,p) = 1$, $p$ is not a divisor of $b$ and $d$, so $p$ is not a divisor of $bd$, too. This means the addition and multiplication is closed in $\mathbb{Z}_p$.

The identity 0 can be written as $0/1$, so $0 \in \mathbb{Z}_p$. For every $g = a/b \in \mathbb{Z}_p$, $-g = -a/b \in \mathbb{Z}_p$. By the definition of the ring, $\mathbb{Z}_p$ is a ring.

## 10 [TJ] Exercise 16-35

No. Consider the following algebraic structure on $\mathbb{Z}_4$ with addition and multiplication defined as

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 0 | 3 | 2 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 2 | 1 | 0 |

| $\times$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 3 | 1 |
| 3 | 0 | 3 | 1 | 2 |

It is easy to verify that $(\mathbb{Z}_4, +, \times)$ is a finite integral domain of order 4, which is impossible to be isomorphic to any $\mathbb{Z}_p$.

## 11 [TJ] Exercise 16-39

In integral domain, we have

$$\begin{aligned} x^2 &= x \\ x^2 &= 1x \\ x^2 - 1x &= 0 \\ (x-1)x &= 0 \end{aligned}$$

So $x - 1 = 0$ or $x = 0$, i.e the only idempotents in an integral domain are 0 and 1.

Consider $\mathbb{M}_2(\mathbb{R})$, all $2 \times 2$ matrices with real entries, we have

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

which means $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0$ is an idempotent.

## 12 [TJ] Exercise 16-40

Assume, to the contrary that this equation has a solution $x = x_0$. Since $\gcd(a,n) = d$, there exists integers $p, q$, such that $a = pd, n = qd$, and the equation becomes

$$pdx \equiv b \pmod{qd}$$

Since $x = x_0$ is a solution to this equation, there must exist integer $k$, such that

$$b = kqd + pdx_0 = (kq + px_0)d$$

This means that $b$ is a multiple of $d$, which contradicts $\gcd(b,d) = 1$.