

§ 5.1. Homework Problems.

1. b. $R = \left\{ \frac{m}{n} \in \mathbb{Q} : n \text{ is even} \right\}$.

Claim: R is not a ring.

Proof: $\forall \frac{m}{n} \in R, n \text{ even} \Rightarrow m \text{ odd} \Rightarrow \frac{m}{n} \neq 1$
 $\Rightarrow 1 \notin R \Rightarrow R$ is not a subring.

1. d. $R = \left\{ \frac{m}{n} \in \mathbb{Q} : \gcd(n, k) = 1 \right\}$.

Claim: R is a subring of \mathbb{Q} .

Proof: Clearly, $1 \in R$. Let $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in R$.

$$\bullet \frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$$

$$\gcd(n_1, k) = \gcd(n_2, k) = 1 \Rightarrow \gcd(n_1 n_2, k) = 1$$

\Rightarrow the denominator d in lowest terms is coprime to k
since $d \mid n_1 n_2$; hence, $(R, +)$ is closed.

$\bullet \frac{m_1}{n_1} \cdot \frac{m_2}{n_2} \in R$, so (R, \cdot) is closed; the reasoning is the same as for $(R, +)$.

It follows that R is a subring of \mathbb{Q} .

$$2a. A = \{ m + n\sqrt{2} : m, n \in \mathbb{Z}; n \text{ even} \},$$

Claim: A is a subring of \mathbb{R} .

Proof: 0 is even $\Rightarrow 1 = 1 + 0 \cdot \sqrt{2} \in A$

Also, $\forall a \in A, -a \in A$. Now, let $m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in A$.

We have:

$$\bullet (m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2}) = (m_1 + m_2) + \underbrace{(n_1 + n_2)}_{\text{even}}\sqrt{2} \in A$$

$$\bullet (m_1 + n_1\sqrt{2})(m_2 + n_2\sqrt{2}) = (m_1 m_2 + 2n_1 n_2) + \underbrace{(m_1 n_2 + m_2 n_1)}_{\text{even}}\sqrt{2} \in A$$

Hence, A is a subring of \mathbb{R} .

$$2b. B = \{ m + n\sqrt{2} : m, n \in \mathbb{Z}; m \text{ odd} \}.$$

Claim: B is not a subring of \mathbb{R} .

Proof: Let $m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in B$.

$$(m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2}) = \underbrace{(m_1 + m_2)}_{\text{even}} + (n_1 + n_2)\sqrt{2} \notin B$$

(odd + odd)

$(B, +)$ not closed \Rightarrow not a subring.

2e. $E = \{ m + nu : m, n \in \mathbb{Z}; u = \frac{1 + \sqrt{3}}{2} \}$.

Claim: E is not a subring of \mathbb{R} .

Proof:

Observe that $u \in E$, but that

$$u^2 = \left(\frac{1 + \sqrt{3}}{2} \right)^2 = \frac{1 + 2\sqrt{3} + 3}{4} = 1 + \frac{\sqrt{3}}{2} = u + \frac{1}{2} \notin E.$$

Hence, (E, \times) not closed, so E is not a subring of \mathbb{R} .

2f. $F = \{ m + nv : m, n \in \mathbb{Z}, v = \frac{1 + \sqrt{5}}{2} \}$.

Claim: F is a subring of \mathbb{R} .

Proof: First, note that $1 \in F$ and $\forall f \in F$, we have $-f \in F$.

Now, let $m_1 + n_1 v, m_2 + n_2 v \in F$. Observe that

$$v^2 = \left(\frac{1 + \sqrt{5}}{2} \right)^2 = \frac{1 + 2\sqrt{5} + 5}{4} = 1 + \frac{1 + \sqrt{5}}{2} = 1 + v$$

$\bullet (m_1 + n_1 v) + (m_2 + n_2 v) = (m_1 + m_2) + (n_1 + n_2) v \in F \Rightarrow (F, +)$ is closed.

$\bullet (m_1 + n_1 v)(m_2 + n_2 v) = m_1 m_2 + (n_1 m_2 + m_1 n_2) v + n_1 n_2 v^2$

$= m_1 m_2 + n_1 n_2 + (n_1 m_2 + n_1 m_2 + m_1 m_2) v \in F \Rightarrow (F, \times)$ is closed.

Hence, F is a subring of \mathbb{R} .

$$\textcircled{4} \quad R = \{m+n\sqrt{2} : m, n \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{2}].$$

$$\textcircled{a} \quad \text{Show: } m+n\sqrt{2} \in R^\times \iff m^2 - 2n^2 = \pm 1.$$

Proof (\implies) let $m+n\sqrt{2} \in R^\times$. Then $\exists x+y\sqrt{2} \in R$

with $(m+n\sqrt{2})(x+y\sqrt{2}) = 1$. We claim that

$(m-n\sqrt{2})(x-y\sqrt{2}) = 1$. To see this, observe that

$$(m+n\sqrt{2})(x+y\sqrt{2}) = \cancel{m^2+2n^2} \quad mx+2ny + (nx+my)\sqrt{2} = 1$$

$\implies mx+2ny = 1; \quad nx+my = 0$. It follows that

$$(m+n\sqrt{2})(x-y\sqrt{2}) = mx+2ny - (nx+my)\sqrt{2} = 1 - 0 \cdot \sqrt{2} = 1,$$

as claimed. Now, $(m+n\sqrt{2})(x+y\sqrt{2}) = 1$
 $(m-n\sqrt{2})(x-y\sqrt{2}) = 1 \quad \Bigg\} \implies$

$$1 = (m+n\sqrt{2})(m-n\sqrt{2})(x+y\sqrt{2})(x-y\sqrt{2}) = \underbrace{(m^2-2n^2)}_{\in \mathbb{Z}} \underbrace{(x^2-2y^2)}_{\in \mathbb{Z}}$$

$$\implies m^2 - 2n^2 = \pm 1.$$

(\impliedby) Suppose that $m^2 - 2n^2 = (m+n\sqrt{2})(m-n\sqrt{2}) = \pm 1$.

$$\bullet (m+n\sqrt{2})(m-n\sqrt{2}) = 1 \implies m+n\sqrt{2} \in R^\times; \quad (m+n\sqrt{2})^{-1} = m-n\sqrt{2}.$$

$$\bullet (m+n\sqrt{2})(m-n\sqrt{2}) = -1 \xrightarrow{\times(-1)} (m+n\sqrt{2})(-m+n\sqrt{2}) = 1$$

$$\implies m+n\sqrt{2} \in R^\times; \quad (m+n\sqrt{2})^{-1} = -m+n\sqrt{2}.$$

4b. Show that $1 + \sqrt{2} \in \mathbb{R}^*$ has infinite order.

Proof: First, note that $(1 + \sqrt{2})(1 - \sqrt{2}) = 1^2 - 2 \cdot 1 = -1$

$\implies 1 + \sqrt{2} \in \mathbb{R}^*$. Now, $1 + \sqrt{2} > 1 \implies \forall n \geq 1, (1 + \sqrt{2})^n > 1$

$\implies 1 + \sqrt{2}$ has infinite order.

4c. Show that 1 and -1 are the only ~~finite~~ units in \mathbb{R} with finite order.

Proof: $\mathbb{R} = \mathbb{R} \implies u \in \mathbb{R}^*$ has $|u| = 1 \iff u = \pm 1$.

• $|u| > 1$: As in part (b), $\forall n \geq 1, |u|^n > 1$, so u has ∞ order. ($|u|^n \rightarrow \infty$ as $n \rightarrow \infty$).

• $|u| < 1$: Then $\forall n \geq 1, 0 < |u|^n < 1$, so u has ∞ order ($|u|^n \rightarrow 0$ as $n \rightarrow \infty$).

7. Suppose that $u \in R^{\times}$ and that $a \in R$ is nilpotent.

Show that $u-a \in R^{\times}$.

Proof: $a \in R$ is nilpotent $\implies \exists n \geq 1$ such that $a^n = 0$.

$u \in R^{\times} \implies \forall m \in \mathbb{Z}, u^m \in R$.

Consider: $V = u^{-1} + au^{-2} + \dots + a^{n-1}u^{-n} = \sum_{i=1}^n a^{i-1}u^{-i} \in R$.

We have:

$$(u-a)V = uV - aV = \underbrace{(1 + au^{-1} + \dots + a^{n-1}u^{-n+1})}_{= uV}$$

$$- \underbrace{(au^{-1} + \dots + a^{n-1}u^{-1} + a^n u^n)}_{= aV} = 1 + a^n u^n = 1 \text{ since } a^n = 0.$$

Therefore, $u-a \in R^{\times}$.

Alternative: Let $v' = 1 + a + \dots + a^{n-1} \in R$. } *

Then $(1-a)v' = 1 - a^n = 1 \implies 1-a \in R^{\times}$

Note: $(u^{-1}a)^n = u^{-n}a^n = 0 \implies u^{-1}a$ is nilpotent.

* $\implies 1 - u^{-1}a \in R^{\times}$. Consider:

$$u(1 - u^{-1}a) = u - a \in R^{\times}$$

\uparrow
 $\in R^{\times}$, a group under mult.

⑧ Let R be a commutative ring such that $\forall a \in R, a^2 = a$.

Show that $a+a=0 \forall a \in R$.

Proof: $(a+a)^2 = a+a = 2a$
 $(a+a)^2 = (2a)^2 = 4a^2 = 4a$ } $\Rightarrow 4a = 2a \Rightarrow 2a = 0$.

11. Suppose that $\forall a \in R, a^2 = a$. Show that R is commutative.

Proof: Let $x, y \in R$. To show: $xy = yx$.

Hypothesis $\Rightarrow x^2 = x; y^2 = y; (x+y)^2 = x+xy$.

Prob # 8 $\Rightarrow \forall a \in R, a+a=0$; hence $a = -a$.

We have $\boxed{yx = -yx}$. Now, compute:

$$(x+y)^2 = x^2 + xy + yx + y^2 \underset{\substack{\uparrow \\ x^2=x, y^2=y}}{=} x + xy + yx + y$$

$(x+y)^2 = x+xy$. Hence, we have $x + xy + yx + y = x + xy$

$$\begin{array}{l} x \\ \longrightarrow \\ -y \end{array} xy + yx = 0 \Rightarrow xy = -yx \underset{\substack{\text{by } * \\ \downarrow}}{=} yx.$$

14. Define \oplus, \odot on \mathbb{Q} : $\forall a, b \in \mathbb{Q}$,

$$\left. \begin{array}{l} \bullet a \oplus b = a + b \\ \bullet a \odot b = 2ab \end{array} \right\} \text{ show that } (\mathbb{Q}, \oplus, \odot) \text{ is a comm. ring.}$$

Proof: First, note that (\mathbb{Q}, \oplus) is an abelian group.

Properties of (\mathbb{Q}, \odot) :

(i) closure: $\forall a, b \in \mathbb{Q}$, $a \odot b = 2ab \in \mathbb{Q}$

(ii) identity: $\forall a \in \mathbb{Q}$, $a \odot \frac{1}{2} = 2a\left(\frac{1}{2}\right) = a$; $\left. \begin{array}{l} \frac{1}{2} \odot a = 2\left(\frac{1}{2}\right)a = a. \end{array} \right\} \Rightarrow \frac{1}{2} \text{ (in } \odot) = \frac{1}{2}.$

(iii) associativity: $\forall a, b, c \in \mathbb{Q}$,

$$a \odot (b \odot c) = a \odot (2bc) = 2(a)(2bc) = 4abc. \left. \begin{array}{l} \end{array} \right\} \text{ equal.}$$

$$(a \odot b) \odot c = (2ab) \odot c = 2(2ab)(c) = 4abc$$

(iv) commutativity: $\forall a, b \in \mathbb{Q}$, $a \odot b = 2ab$; $\left. \begin{array}{l} b \odot a = 2ba = 2ab \end{array} \right\} \text{ equal.}$

Distributivity:

$$\left. \begin{array}{l} \bullet a \odot (b \oplus c) = a \odot (b+c) = 2(a)(b+c) = 2ab + 2ac \\ \bullet (a \odot b) \oplus (a \odot c) = (2ab) \oplus (2ac) = 2ab + 2ac. \end{array} \right\} \text{ equal.}$$

15. Define \oplus, \ominus on \mathbb{Z} by, $\forall a, b \in \mathbb{Z}$:

$$\left. \begin{aligned} a \oplus b &= a + b - 1 \\ a \ominus b &= a + b - ab \end{aligned} \right\} \text{Is } (\mathbb{Z}, \oplus, \ominus) \text{ a comm. ring?}$$

Claim: $(\mathbb{Z}, \oplus, \ominus)$ is a comm. ring.

(I) (\mathbb{Z}, \oplus) properties.

(i) closure: $\forall a, b \in \mathbb{Z}, a \oplus b = a + b - 1 \in \mathbb{Z}$.

(ii) identity: $\forall a \in \mathbb{Z}, \left. \begin{aligned} 1 \oplus a &= 1 + a - 1 = a \\ a \oplus 1 &= a + 1 - 1 = a \end{aligned} \right\} \rightarrow 1_{(\mathbb{Z}, \oplus)} = 1$.

(iii) inverse: let $m \in \mathbb{Z}$. $m \oplus (-m+2) = m + (-m+2) - 1 = 1$
 $(-m+2) \oplus m = -m+2 + m - 1 = 1$

$\Rightarrow \ominus m = -m+2$.

(iv) associativity: let $a, b, c \in \mathbb{Z}$.

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2$$

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = (a + b - 1) + c - 1 = a + b + c - 2$$

(v) commutativity: let $a, b \in \mathbb{Z}$.

$$a \oplus b = a + b - 1;$$

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

(i) - (v) hold

$\Rightarrow (\mathbb{Z}, \oplus)$ is an abelian group.

(II) (\mathbb{Z}, \oplus) properties.

(i) closure: $\forall a, b \in \mathbb{Z}, a \oplus b = a + b - ab \in \mathbb{Z}$.

(ii) identity: $\forall a \in \mathbb{Z}, a \oplus 0 = a + 0 - (a)(0) = a;$
 $0 \oplus a = 0 + a - (0)(a) = a. \} \Rightarrow 1_{(\mathbb{Z}, \oplus)} = 0.$

(iii) associativity: $\forall a, b, c \in \mathbb{Z},$

$$(a \oplus b) \oplus c = (a + b - ab) \oplus c = (a + b - ab) + c - (a + b - ab)c$$
$$= a + b + c - ab - ac - bc + abc$$

$$a \oplus (b \oplus c) = a \oplus (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$$
$$= a + b + c - ab - ac - bc + abc.$$

(iv) commutativity: $\forall a, b \in \mathbb{Z}, a \oplus b = a + b - ab$
 $b \oplus a = b + a - ba = a + b - ab.$

Distributivity: let $a, b, c \in \mathbb{Z}$

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - a(b + c + 1)$$
$$= a + b + c - ab - ac + a - 1 = 2a + b + c - ab - ac - 1.$$

$$(a \oplus b) \oplus (a \oplus c) = (a + b - ab) \oplus (a + c - ac)$$
$$= (a + b - ab) + (a + c - ac) - 1 = 2a + b + c - ab - ac - 1$$

All axioms ~~are~~ satisfied $\Rightarrow (\mathbb{Z}, \oplus, 0)$ is a comm. ring.

Let F be a finite field.

① Show that \exists prime p such that $\forall a \in F, pa = 0$.

Proof: $|F| \geq 2 \Rightarrow \exists$ prime $p \mid |F|$.

F is an additive abel. group $\xrightarrow{\text{(Cauchy)}}$ $\exists a \neq 0$ in F

with order p : $pa = 0$. Now, let $b \in F$. We have:

$pab = (pa)b = 0 \cdot b = 0$. But also, note that $pab = (pb)a$.

Hence, we have: $(pb)a = 0$. Since $a \neq 0$ and F is an int. domain, it follows that $pb = 0$.

② Suppose that F has q elements. Show that $\exists n \geq 1$

Proof: Part ① $\Rightarrow \exists$ prime p such that $\forall a \in F$, $pa = 0$. Hence, every $a \in F$ has additive order dividing p . with $q = p^n$.

Now, suppose that a prime $l \mid q = |F|$. Cauchy's Theorem

$\Rightarrow \exists b \neq 0$ in F with add. order l . But also, b has

add. order dividing p , so $l \mid p$. Since l and p are

prime, we must have $l = p$. It follows that $\exists n \geq 1$

for which $|F| = q = p^n$.