Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
HW #1 Solutions

Section 18:
2) $(16)(3) = 48 = 16$ in $\mathbb{Z}_{32}$.

6) $(-3, 5)(2, -4) = (-6, -20) = (2, 2)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{11}$.

8) $\mathbb{Z}^+$ is not a ring as it is not even a group under addition. For instance, 1 has no additive inverse.

10) $2\mathbb{Z} \times \mathbb{Z}$ is a commutative ring but it has no unity and it is not a field (for instance, $(2, 1)$ has no multiplicative inverse).

11) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a commutative ring with unity, but is not a field. For instance, 2 has no multiplicative inverse.

12) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field and thus also a commutative ring with unity. The key point to see that it is a field is that

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

13) The set of purely imaginary numbers is not even a ring as it is not closed under multiplicative. For instance, $i \cdot i = -1$ which is not purely imaginary.

16) The units in $\mathbb{Z}_5$ are $\{1, 2, 3, 4\}$. To see this, note that $1 \cdot 1 = 4 \cdot 4 = 2 \cdot 3 = 1$.

18) For R a ring with unity, write $R^\times$ for the units in R. Then for R and S rings, we have that $(R \times S)^\times = R^\times \times S^\times$ (check this!). Thus,

$$(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z})^\times = \mathbb{Z}^\times \times \mathbb{Q}^\times \times \mathbb{Z}^\times.$$

The only units in $\mathbb{Z}$ are 1 and -1 while $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ as $\mathbb{Q}$ is a field. Thus,

$$(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z})^\times = \{\pm 1\} \times (\mathbb{Q} - \{0\}) \times \{\pm 1\}.$$

27) The reasoning here is flawed as it assumes that the ring is an integral domain. From $(X - I_3)(X + I_3) = 0$ one cannot deduce $X = I_3$ or $X = -I_3$ as this ring has zero divisors. As an explicit counter-example, the matrix $X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ satisfies $X^2 = I_3$ but X is neither the identity or its negative.

33)

a. True

b. False. For example, $R = 2\mathbb{Z}$ is a ring without a multiplicative identity.

c. False. For example, $R = \mathbb{Z}_2$ is a ring with unity, but only has 1 unit.

d. False. For example, $R = \mathbb{Q}$ is a ring with unity, but has infinitely many units.

e. True, this is possible. Consider $F = \mathbb{Q}$ and $R = 2\mathbb{Z}$ which is a subring of F but not a field.

f. False, but silly as this is a subjective question. They are important because they give the link between $+$ and $\cdot$.

g. True (by definition)

h. True (see #37)

i. True (by definition)

j. True (by definition)

37) We need to check that multiplication on U is closed, associative, has an identity element and that every element has an inverse. As $U \subseteq R$, we immediately see that multiplication on U is associative as it is on R. The element 1 is the identity element of U. If $u \in U$, then by definition there exists $v \in R$ such that $uv = vu = 1$. But then it is clear that v is itself a unit (and thus $v \in U$). Hence, $u^{-1} = v \in U$. Lastly, we need to check that U is closed under multiplication. Let u_1 and u_2 be elements of U. By definition, there exists v_1 and v_2 such that $u_1v_1 = v_1u_1 = u_2v_2 = v_2u_2 = 1$. Thus,

$$(u_1u_2)(v_2v_1) = u_1 \cdot 1 \cdot v_1 = u_1v_1 = 1$$

and

$$(v_2v_1)(u_1u_2) = v_2 \cdot 1 \cdot u_2 = v_2u_2 = 1.$$

Hence, u_1u_2 is a unit and multiplication is closed on U. This proves that U is a group under multiplication.

44)

a. Let a and b be idempotents in R. We need to check that ab is an idempotent. We compute

$$(ab)^2 = abab = aabb = a^2b^2 = 1 \cdot 1 = 1.$$

Thus ab is an idempotent. (Note that we used the commutativity of R in the middle step above.)

b. If (a, b) is idempotent in $\mathbb{Z}_6 \times \mathbb{Z}_{12}$, then $(a, b)^2 = (a, b)$ and thus $a^2 = a$ in $\mathbb{Z}_6$ and $b^2 = b$ in $\mathbb{Z}_{12}$. The idempotents in $\mathbb{Z}_6$ are $\{0, 1, 3, 4\}$ while the idempotents in $\mathbb{Z}_{12}$ are $\{0, 1, 4, 9\}$. Hence the idempotents in $\mathbb{Z}_6 \times \mathbb{Z}_{12}$ are $\{0, 1, 3, 4\} \times \{0, 1, 4, 9\}$.

55) Let R be a Boolean ring and let $a, b \in R$. We then have

$$\begin{aligned} a + b &= (a + b)^2 \\ &= (a + b)(a + b) \\ &= a^2 + ba + ab + b^2 \\ &= a + ba + ab + b. \end{aligned}$$

Subtracting, then yields

$$ab = -ba.$$

This looks wrong because of the minus sign! But note that since this equation is true for all a and b, we can take $b = 1$. Then we have $a = -a$ for all a. In particular, $-ba = ba$ and thus $ab = ba$ for all a and b. Hence, R is commutative.

Section 19:

3) $3x = 2$ in $\mathbb{Z}_7$ implies $x = 3$ while in $\mathbb{Z}_{23}$ we have that $x = 16$.

14) $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ -1 & -1 \end{pmatrix} = 0.$

17)

a. False. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ and thus has no zero divisors.

b. True

c. False. $n\mathbb{Z}$ has characteristic 0

d. False. The map $x \mapsto nx$ is not an isomorphism.

e. True

f. True

g. False. Consider $R = \mathbb{Z} \times \mathbb{Z}$. Then $\mathbb{Z}$ is an integral domain but $(1, 0) \cdot (0, 1) = (0, 0)$.

h. True

i. False. $n\mathbb{Z}$ has no unity for $n > 1$ which is required for a domain.

j. False. $\mathbb{Z}$ is not a field!

29) Let the characteristic of D equal x. Assume x is not 0 and not a prime. Note that it is not possible that $x = 1$ as in this case we would have that $1 = 0$ in D and hence D is the zero ring which is not a domain. Hence, x is composite and we can write $x = mn$ and $0 < m, n < x$. We then know that

$$0 = mn \cdot 1 = (m \cdot 1)(n \cdot 1).$$

Since D is a domain, we must have that $m \cdot 1 = 0$ or $n \cdot 1 = 0$. But this is impossible as x is smallest positive integer such that $x \cdot 1 = 0$. This contradiction implie that x is either 0 or prime.