
Assignment 1 – Solutions

1. Give examples for each of the following (you need not prove the required properties):

- (a) A non-commutative ring with no multiplicative identity.
- (b) A non-commutative ring with multiplicative identity.
- (c) A commutative ring with no multiplicative identity.
- (d) A commutative ring with multiplicative identity that is not an integral domain.
- (e) An integral domain that is not a UFD.
- (f) A ring that is not a PID, but in which all ideals are principal.

Solution:—

- (a) The ring of 2×2 matrices with entries from $2\mathbb{Z}$, with the usual matrix operations.
 - (b) The ring of 2×2 matrices with entries from \mathbb{Z} , with the usual matrix operations.
 - (c) $2\mathbb{Z}$
 - (d) $\mathbb{Z}/4\mathbb{Z}$
 - (e) $\mathbb{Z}[\sqrt{-5}]$
 - (f) $\mathbb{Z}/4\mathbb{Z}$
-

2. Define new operations of \mathbb{Z} by: $x \oplus y = x + y + 1$ and $x \odot y = xy + x + y$.

- (a) Prove that with respect to these operations \mathbb{Z} forms a ring.
- (b) Prove that $(\mathbb{Z}, \oplus, \odot)$ is isomorphic to $(\mathbb{Z}, +, \times)$ (i.e., \mathbb{Z} with the usual operations).

Solution:—

- (a) Using standard properties of the integers we have:

$$\begin{aligned} (x \oplus y) \oplus z &= (x + y + 1) \oplus z = (x + y + 1) + z + 1 = x + (y + z + 1) + 1 = x \oplus (y \oplus z) \\ (x \oplus -1) &= x \\ (x \oplus (-x - 2)) &= -1 \\ x \oplus y &= x + y + 1 = y + x + 1 = y \oplus x \end{aligned}$$

Therefore (\mathbb{Z}, \oplus) forms an abelian group, with (additive) identity $0_R = -1$ and (additive) inverse of x given by $-x - 2$. We also have:

$$\begin{aligned} (x \odot y) \odot z &= (x \odot y)z + (x \odot y) + z = (xy + x + y)z + xy + x + y + z \\ &= xyz + xz + yz + xy + x + y + z \\ &= x(yz + y + z) + x + yz + y + z \\ &= x(y \odot z) + x + y \odot z = x \odot (y \odot z) \end{aligned}$$

and

$$\begin{aligned} x \odot (y \oplus z) &= x \odot (y + z + 1) = x(y + z + 1) + x + (y + z + 1) = xy + xz + x + x + y + z + 1 \\ &= (xy + x + y) + (xz + x + z) + 1 = (x \odot y) \oplus (x \odot z) \end{aligned}$$

which, as \odot is clearly commutative, gives

$$(y \oplus z) \odot x = x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z) = (y \odot x) \oplus (z \odot x)$$

Having verified all the defining axioms, we conclude that $R = (\mathbb{Z}, \oplus, \odot)$ is a (commutative) ring.

(b) Let $\varphi : (\mathbb{Z}, +, \times) \rightarrow (\mathbb{Z}, \oplus, \odot)$ be the map given by $\varphi(x) = x - 1$. Then φ is a ring homomorphism since

$$\begin{aligned}\varphi(x + y) &= x + y - 1 = (x - 1) + (y - 1) + 1 \\ &= \varphi(x) \oplus \varphi(y)\end{aligned}$$

and

$$\begin{aligned}\varphi(xy) &= xy - 1 = (x - 1)(y - 1) + x + y - 2 = (x - 1)(y - 1) + (x - 1) + (y - 1) \\ &= \varphi(x) \odot \varphi(y)\end{aligned}$$

It is clear that the map φ is a bijection, and hence that it is an isomorphism.

3. Let $a, b \in R$ be two elements in a commutative ring R . Show carefully that

$$R/(a, b) \cong (R/\langle a \rangle)/\langle b + \langle a \rangle \rangle$$

Solution:—

For clarity, I'll write $\langle a \rangle$ for the ideal $(a) \triangleleft R$, $\langle a, b \rangle$ for $(a, b) \triangleleft R$ and $\langle b + \langle a \rangle \rangle$ for $(b + (a)) \triangleleft R/\langle a \rangle$. Let $\varphi : R/\langle a \rangle \rightarrow R/\langle a, b \rangle$ be the map given by $\varphi(r + \langle a \rangle) = r + \langle a, b \rangle$. This is well-defined since

$$r + \langle a \rangle = s + \langle a \rangle \implies r - s \in \langle a \rangle \implies r - s \in \langle a, b \rangle \implies r + \langle a, b \rangle = s + \langle a, b \rangle.$$

It is a homomorphism since

$$\varphi((r + \langle a \rangle)(s + \langle a \rangle)) = \varphi(rs + \langle a \rangle) = rs + \langle a, b \rangle = (r + \langle a, b \rangle)(s + \langle a, b \rangle) = \varphi(r + \langle a \rangle)\varphi(s + \langle a \rangle)$$

and

$$\begin{aligned}\varphi((r + \langle a \rangle) + (s + \langle a \rangle)) &= \varphi(r + s + \langle a \rangle) = r + s + \langle a, b \rangle = (r + \langle a, b \rangle) + (s + \langle a, b \rangle) \\ &= \varphi(r + \langle a \rangle) + \varphi(s + \langle a \rangle)\end{aligned}$$

As φ is clearly surjective, from the first isomorphism theorem we have $(R/\langle a \rangle)/\ker \varphi \cong R/\langle a, b \rangle$. The required result then follows since

$$\begin{aligned}r + \langle a \rangle \in \ker \varphi &\iff \varphi(r + \langle a \rangle) = 0 \iff r + \langle a, b \rangle = 0 + \langle a, b \rangle \iff r \in \langle a, b \rangle \\ &\iff r = xa + yb \quad \text{for some } x, y \in R \\ &\iff r + \langle a \rangle = yb + \langle a \rangle \quad \text{for some } y \in R \\ &\iff r + \langle a \rangle = (y + \langle a \rangle)(b + \langle a \rangle) \quad \text{for some } y \in R \\ &\iff r + \langle a \rangle \in \langle b + \langle a \rangle \rangle\end{aligned}$$

4. Let R be a commutative ring with multiplicative identity, let I be an ideal in R . Let

$$J = \{x \in R \mid \exists n \in \mathbb{N} \text{ such that } x^n \in I\}$$

Show that J is an ideal in R . (J is called the radical of I .)

Solution:—

Let $J = \{x \in R \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$. Let $x, y \in I$, and let $m, n \in \mathbb{N}$ be such that $x^m \in I$ and $y^n \in I$. The set J is non-empty since I , being an ideal, is non-empty and $I \subseteq J$. To see that J is an ideal:

$$\begin{aligned} (x - y)^{m+n} &= \sum_{i=0}^{m+n} \binom{m+n}{i} x^i (-y)^{m+n-i} \\ &= \sum_{i=0}^m \binom{m+n}{i} x^i (-y)^{m+n-i} + \sum_{i=m+1}^{m+n} \binom{m+n}{i} x^i (-y)^{m+n-i} \\ &= \left(\sum_{i=0}^m \binom{m+n}{i} x^i (-y)^{m-i} \right) (-1)^n y^n + \left(\sum_{i=m+1}^{m+n} \binom{m+n}{i} x^{i-m} (-y)^{m+n-i} \right) x^m \\ &\in I \quad \text{(Since } I \text{ is an ideal and } y^n, x^m \in I.) \end{aligned}$$

Therefore $(x - y) \in J$. Also, if $r \in R$, then $(rx)^m = r^m x^m \in I$ since I is an ideal and $x^m \in I$. Therefore $rx \in J$. Hence J is an ideal.

5. Let R be a commutative ring with 1, and suppose that every element $x \in R$ satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in R is maximal.

Solution:—

Let $P \triangleleft R$ be a prime ideal. Then R/P is an integral domain. We will show that R/P is a field, which implies that P is maximal. We need to show that every non-zero element in R/P is a unit. Let $x \in R \setminus P$ and consider $\bar{x} = x + P \in R/P$. Let n be such that $x^n = x$. Then $\bar{x}^n = (x + P)^n = x^n + P = x + P = \bar{x}$. Since R/P is an integral domain the cancellation law implies that $\bar{x}^{n-1} = 1$. Therefore $\bar{x} \cdot \bar{x}^{n-2} = 1$ and \bar{x} is a unit.

6. Let R be a UFD. Let $a, b \in R$ be two elements which are not both zero. An element $m \in R$ is a least common multiple of a and b (denoted $\text{lcm}(a, b)$) if it satisfies:

1: $a|m$ and $b|m$;

2: if $m' \in R$ is such that $a|m'$ and $b|m'$, then $m|m'$.

(a) Prove that $\text{lcm}(a, b)$ exists and is unique up to multiplication by a unit.

(b) Let m be a lcm of a and b , and let d be a gcd of a and b . Prove that md is an associate of ab .

Solution:—

(a) **Existence:** If either is zero, then $m = 0$ satisfies the definition. So assume that neither is zero. If a , say, is a unit, then $m = b$ satisfies the definition. So we assume that neither a nor b is a unit. Since R is a UFD, we have irreducible decompositions: $a = a_1 \dots a_t$ and $b = b_1 \dots b_n$. By rearranging the factors if necessary, we can assume that there is a $k \leq \min\{t, n\}$ such that $a_i \sim b_i$ for $1 \leq i \leq k$ and $a_i \not\sim b_j$ for $i, j > k$. Let $m = ab_{k+1} \dots b_n$. Clearly $a|m$. We also have that $b|m$ since $m \sim ba_{k+1} \dots a_t$. If $m' \in R$ is such that $a|m'$ and $b|m'$, then $m|m'$ since $a|m'$, $b_{k+1} \dots b_n|m'$ and a and $b_{k+1} \dots b_n$ are relatively prime. It follows that m is a least common multiple of a and b .

Uniqueness: If $n \in R$ also satisfies the definition, we have $m|n$ and $n|m$ which implies that n is an associate of m .

- (b) If either is zero, then $\text{lcm}(a, b) \text{gcd}(a, b) = ab = 0$. If a , say, is a unit, then $\text{lcm}(a, b) \sim b$ and $\text{gcd}(a, b) \sim 1$, so $\text{lcm}(a, b) \text{gcd}(a, b) \sim b \sim ab$. Assuming both are non-zero and non-unit and with the notation of the previous part, observe that $a_1 \dots a_k$ is a gcd of a and b . It is clearly a common divisor, and if d' is some other common divisor, then the irreducible decomposition of d' must contain each of the irreducibles a_1, \dots, a_k (up to associates). It follows that $d \sim a_1 \dots a_k$, and $md \sim ma_1 \dots a_k \sim ba_{k+1} \dots a_t a_1 \dots a_k = ba$

7. Let R be the following subset of \mathbb{Q} :

$$R = \{x \in \mathbb{Q} \mid x = \frac{a}{b}, \text{ for some } a, b \in \mathbb{Z}, \text{ with } b \text{ not divisible by } 3\}.$$

- (a) Show that R is a subring of \mathbb{Q} .
 (b) Describe the units of R .
 (c) Show that every proper ideal in R has the form $\langle 3^k \rangle$ (i.e., the ideal in R generated by 3^k) for some positive $k \in \mathbb{Z}$ (depending on the ideal).
 (d) Show that $R/\langle 3 \rangle$ is a field.

Solution:—

- (a) Let a/b and α/β be elements of R . Then 3 does not divide $b\beta$ since $3|b\beta \implies 3|b$ or $3|\beta$ as 3 is prime. Let $[c/d]$ denote the reduced fraction equal to c/d , and note that $[c/d] \in R$ if 3 does not divide d (the converse is false). Then

$$(a/b) - (\alpha/\beta) = [(a\beta - \alpha b)/(b\beta)] \in R$$

and

$$(a/b)(\alpha/\beta) = [(a\alpha)/(b\beta)] \in R$$

So R is a subring of \mathbb{Q} .

- (b) If $3 \nmid a$, then a/b is a unit since $b/a \in R$ and $(a/b)(b/a) = 1$. These are the only units in R because if $3|a$ and $(a/b)(\alpha/\beta) = 1$ then $a\alpha = b\beta$ but 3 divides $a\alpha$ and not $b\beta$. So the units in R are given by $\{a/b \in R \mid 3 \nmid a\}$.
 (c) Let I be a proper ideal in R . As I is proper it has more than one element and contains no units. As I contains no units, 3 divides the numerator of each element in I (by the previous part of the question). For each $a/b \in R$ let $\nu(a/b)$ denote the exponent of 3 in the prime factorisation of a . Then for all $a/b \in I$ we have $\nu(a/b) \geq 1$. Let $k \geq 1$ be given by $k = \min\{\nu(a/b) \mid a/b \in I, \text{gcd}(a, b) = 1\}$. Then 3^k divides the numerator of each element in I , and $I \subset \langle 3^k \rangle$. For the reverse inclusion note that there exists an element in I of the form $(3^k \alpha)/\beta$ where $3 \nmid \alpha$, as otherwise $\nu(a/b) \geq k + 1$ for all $a/b \in I$. So $\beta/\alpha \in R$ and $3^k = \beta/\alpha(3^k \alpha/\beta) \in I$ since I is an ideal in R . The inclusion $\langle 3^k \rangle \subset I$ follows from $3^k \in I$.
 (d) It follows from the previous part that the ideal $\langle 3 \rangle$ is maximal since $\langle 3 \rangle \supseteq \langle 3^k \rangle$ for any $k \geq 1$. (In fact it is the only maximal ideal in R .) Since the ideal $\langle 3 \rangle$ is maximal, $R/\langle 3 \rangle$ is a field.

8. (a) Show that the following are irreducible in $\mathbb{Q}[x]$:
 i. $x^2 + x + 1$ ii. $x^5 + 7x + 7$ iii. $x^5 + 3x + 2$
 (b) Factorise the polynomial $x^3 + x + 1$ into irreducible factors in:
 i. $\mathbb{Z}_2[x]$ ii. $\mathbb{Z}_3[x]$

Solution:—

- (a) i. Since the polynomial has no roots in \mathbb{Q} , it has no linear factors. If it were reducible, it would have linear factors, as it is a quadratic.
 ii. Irreducible by Eisenstein's criterion (with $p = 7$).
 iii. If the polynomial had a linear root, it would have a root in \mathbb{Q} and therefore a root in \mathbb{Z} that divides 2. Since there is no such root, the polynomial has no linear factors. Suppose there is a factorisation of the form:

$$x^5 + 3x + 2 = (x^2 + bx + a)(x^3 + \gamma x^2 + \beta x + \alpha)$$

with $a, b, \alpha, \beta, \gamma \in \mathbb{Z}$. Then

$$\begin{aligned} \gamma + b &= 0 \\ \beta + b\gamma + a &= 0 \\ \alpha + b\beta + a\gamma &= 0 \\ b\alpha + a\beta &= 3 \\ a\alpha &= 2 \end{aligned}$$

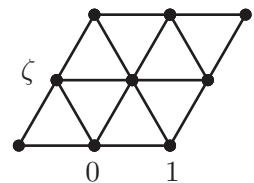
So $(a, \alpha) \in \{(1, 2), (-1, -2), (2, 1), (-2, -1)\}$. Suppose $(a, \alpha) = (1, 2)$. Then we obtain $b^2 - b - 1 = 0$, which is not possible for $b \in \mathbb{Z}$. The other three possibilities for (a, α) lead to similar contradictions.

- (b) i. Since it has no roots in \mathbb{Z}_2 , it has no linear factors. The cubic polynomial is therefore irreducible.
 ii. The element $1 \in \mathbb{Z}_3$ is a root of the polynomial, so $(x - 1) = (x + 2)$ is a factor. Division gives $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$. The quadratic factor is irreducible since it has no roots in \mathbb{Z}_3 .

9. Show that $\mathbb{Z}[\zeta]$ is a Euclidean Domain, where $\zeta = e^{2\pi i/3}$.

Solution:—

$\mathbb{Z}[\zeta] = \{m + n\zeta + k\zeta^2 \mid m, n, k \in \mathbb{Z}\} = \{m + n\zeta \mid m, n \in \mathbb{Z}\}$ since $1 + \zeta + \zeta^2 = 0$. The elements of $\mathbb{Z}[\zeta]$ are those complex numbers that lie on the (infinite) triangular lattice indicated on the right. Every element of \mathbb{C} is within $\frac{1}{\sqrt{3}}$ of an element of $\mathbb{Z}[\zeta]$. Define $\sigma : \mathbb{Z}[\zeta] \rightarrow \mathbb{N}$ by $\sigma(m + n\zeta) = |m + n\zeta|^2 = m^2 - mn + n^2$. Let $a, b \in \mathbb{Z}[\zeta]$ with $b \neq 0$. Define $c = a/b \in \mathbb{C}$, and choose $q \in \mathbb{Z}[\zeta]$ satisfying $|c - q| \leq \frac{1}{\sqrt{3}}$. Then $a = cb = qb + (c - q)b$. Let $r = (c - q)b$. Note that $r = a - qb$ is an element of $\mathbb{Z}[\zeta]$, and $\sigma(r) = |(c - q)b|^2 = |c - q|^2|b|^2 = |c - q|^2\sigma(b) \leq \frac{1}{3}\sigma(b) < \sigma(b)$.



10. Use the Euclidean algorithm to find a gcd in $\mathbb{Q}[x]$ of

$$f(x) = x^4 - x^3 + 2x^2 - x + 1 \quad \text{and} \quad g(x) = x^4 + x^3 + 2x^2 + x + 1$$

and write it as a $\mathbb{Q}[x]$ -linear combination of f and g .

Solution:—

$$g = f + (2x^3 + 2x)$$

$$f = \frac{1}{2}(x-1)(2x^3 + 2x) + (x^2 + 1)$$

$$2x^3 + 2x = 2x(x^2 + 1) + 0$$

It follows that the gcd is $x^2 + 1$, and that

$$\begin{aligned} x^2 + 1 &= f - \frac{1}{2}(x-1)(2x^3 + 2x) \\ &= f - \frac{1}{2}(x-1)(g-f) \\ &= \left(1 + \frac{1}{2}(x-1)\right)f - \frac{1}{2}(x-1)g \\ &= \frac{1}{2}(x+1)f - \frac{1}{2}(x-1)g \end{aligned}$$
