Algebra III: Rings and Modules
Solutions for In-class Test 1, Autumn Term 2022-23

John Nicholson

1. Let R be a ring and let $I, J \subseteq R$ be two-sided ideals.

   (a) Define what it means for a subset $I \subseteq R$ to be a two-sided ideal. **(2 marks)**

   (b) Define the quotient ring R/I and prove carefully that it is a ring. **(6 marks)**

   (c) Prove that the map $\psi : R \to R/I$, $r \mapsto r + I$ is a ring homomorphism. **(2 marks)**

   (d) Prove that $I \cap J \subseteq R$ is a two-sided ideal. **(2 marks)**

   (e) Prove that $I/(I \cap J) = \{a + (I \cap J) : a \in I\} \subseteq R/(I \cap J)$ is a two-sided ideal. **(2 marks)**

   (f) Hence show that $(R/(I \cap J))/(I/(I \cap J))$ and R/I are isomorphic as rings. You may not assume the Third Isomorphism Theorem. **(6 marks)**

Solution: (a) I is a two-sided ideal if the addition operation in R restricts to I and makes I into an abelian subgroup and, for all $r \in R$ and $a \in I$, we have $r \cdot a \in I$ and $a \cdot r \in I$ where $\cdot$ denotes multiplication in the ring R.

(b) For each $a \in R$, let $a + I = \{a + x : x \in I\}$ which we view as a subset of R. As a set, define $R/I = \{a + I : a \in R\}$ to be collection of subsets of R (i.e. $a + I = b + I$ if they are the same as sets). Define addition and multiplication operations by:

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = (ab + I).$$

To see these operations are well-defined, first note that $a + I = b + I$ if and only if $a - b \in I$.

$+$ well-defined: Suppose $a + I = a' + I$, $b + I = b' + I$. Then $a - a', b - b' \in I$. Since I is an abelian subgroup of R under addition, we have $(a + b) - (a' - b') = (a - a') + (b - b') \in I$. Hence $(a + b) + I = (a' + b') + I$.

$\cdot$ well-defined: Again suppose $a + I = a' + I$, $b + I = b' + I$. Then $a - a', b - b' \in I$. It suffices to show that $ab - a'b' \in I$ by the same argument as above. We have $ab - a'b' = (a - a')b + a'(b - b')$. Since I is a two-sided ideal, we have that $(a - a')b, a'(b - b') \in I$ and so $ab - a'b' = (a - a')b + a'(b - b') \in I$. **(4 marks: definition, check it is well defined)**

We now check that R/I is a ring with these operations and with $0 := 0 + I$ and $1 := 1 + I$.

$(R/I, +)$ an abelian group: The fact that the operation is commutative and associative follows immediately since $+_R$ is commutative and associative. We have $(0 + I) + (a + I) = a + I$ so $0 + I$ is the additive identity. Given $a + I$, we have an inverse $(-a) + I$.

$(R/I, \cdot)$ a monoid: The fact that the operation is associative follows since $\cdot_R$ is associative. We have $(1 + I) \cdot (a + I) = a + I = (a + I) \cdot (1 + I)$ so $1 + I$ is a multiplicative identity.

Distributivity follows from the fact that $\cdot_R$ and $+_R$ satisfy distributivity.

(2 marks: check it is a ring)

(c) $\psi(0) = 0 + I$ and $\psi(1) = 1 + I$ so it preserves the additive/multiplicative identities.

Let $a, b \in R$. Then $\psi(a+b) = (a+b)+I = (a+I)+(b+I)$ and $\psi(ab) = ab+I = (a+I)\cdot(b+I)$.

(d) The addition operation restricts to $I \cap J$: if $a, b \in I \cap J$, then $a+b \in I$ (since $a, b \in I$ and I a two-sided ideal) and $a+b \in J$ (since $a, b \in J$ and J a two-sided ideal) and so $a+b \in I \cap J$.

If $a \in I \cap J$, then $-a \in I$ and $-a \in J$ similarly and so $-a \in I \cap J$. $0 \in I$, $0 \in J$ implies $0 \in I \cap J$. Hence $I \cap J$ is an abelian subgroup.

Let $r \in R$ and $a \in I \cap J$. Since $a \in I$ and I a two-sided ideal we have $r \cdot a, a \cdot r \in I$. Similarly $r \cdot a, a \cdot r \in J$ and so $r \cdot a, a \cdot r \in I \cap J$.

(e) Since $I \cap J \subseteq R$ is a two-sided ideal, $R/(I \cap J)$ is a ring (by (b)).

$I/(I \cap J)$ is an abelian subgroup: The operation restricts to $I/(I \cap J)$ since $a, b \in I$ implies $a + b \in I$ and $-a \in I$ (as I is an abelian subgroup of R). That is, given $a' = a + (I \cap J), b' = b + (I \cap J) \in I/(I \cap J)$, we have $a' + b', -a' \in I/(I \cap J)$. Since $0_R \in I$, we have $0_R + (I \cap J) \in I/(I \cap J)$.

The fact I is closed under the left and right R-action implies the same is true for $I/(I \cap J)$.

(f) Let $\psi : R/(I \cap J) \to R/I$ be the map $r+(I \cap J) \mapsto r+I$. To see this is well-defined note that, if $a+(I \cap J) = b+(I \cap J)$, then $a-b \in I \cap J \subseteq I$. So $a-b \in I$ and this implies that $a+I = b+I$. To see this is a ring homomorphism, note that $\psi(0+(I \cap J)) = 0+I$ and $\psi(1+(I \cap J)) = 1+I$. We have $\psi(a + b + (I \cap J)) = a + b + I = (a + I) \cdot (b + I) = \psi(a + (I \cap J)) \cdot \psi(b + (I \cap J))$ and similarly for $\psi(ab + (I \cap J))$. **(2 marks: correct map, check it is well-defined)**

We now claim that $\ker(\psi) = I/(I \cap J)$. Let $a' = a + (I \cap J) \in R$. Then $a' \in \ker(\psi)$ if and only if $\psi(a') = a + I = 0 + I$ if and only if $a = a - 0 \in I$ if and only if $a' \in I/(I \cap J)$.

(2 marks: compute kernel)

Now recall the following result from lectures (the First Isomorphism Theorem).

Theorem: Let R, S be a rings and let $\psi : R \to S$ be a ring homomorphism. Then $\ker(\psi) \subseteq R$ is a two-sided ideal, $\text{im}(\psi) \leq S$ is a subring and there is a ring isomorphism $R/\ker(\psi) \cong \text{im}(\psi)$.

Above we have a ring homomorphism $\psi : R/(I \cap J) \to R/I$ with $\ker(\psi) = I/(I \cap J)$. Note that ψ is surjective: given any $a + I \in R/I$ for $a \in R$, we simply have $a + I = \psi(a + (I \cap J))$. In particular, $\text{im}(\psi) = R/I$. Hence $(R/(I \cap J))/(I/(I \cap J)) \cong R/I$ as required.

(2 marks: state and apply first isomorphism theorem)

2. Define what it means for a ring R to be a:

   (a) Integral Domain (ID) **(1 mark)**

   (b) Euclidean Domain (ED) **(1 mark)**

   (c) Principal Ideal Domain (PID) **(1 mark)**

   (d) Unique Factorisation Domain (UFD). **(1 mark)**

   Prove the following:

   (e) If R is a Euclidean Domain, then R is a Principal Ideal Domain. **(3 marks)**

   For each of the following rings R determine (with proof) whether or not R is an ID, whether or not R is a ED, whether or not R is a PID and whether or not R is a UFD.

   (1 mark shared across f, g, h)

   (f) $(\mathbb{Z}/4\mathbb{Z})[X]$ **(2 marks)**

   (g) $\mathbb{Z}[\omega] = \{a + b\omega + c\omega^2 : a, b, c \in \mathbb{Z}\}$ where $\omega = e^{2\pi i/3} \in \mathbb{C}$. **(5 marks)**

   (h) $\mathbb{Q}[X, Y]$ **(5 marks)**

   Solution: (a) A ring R is an integral domain if it is commutative, non-zero and, for all $a, b \in R$ with $ab = 0$ we have either $a = 0$ or $b = 0$.

   (b) A ring R is a Euclidean domain if it is an integral domain and if there exists a function $\phi : R \backslash \{0\} \to \mathbb{Z}_{\geq 0}$ (called the Euclidean function) such that (i) For all $a, b \in R$ with $b \neq 0$, we have $\phi(ab) \geq \phi(a)$, (ii) For all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and $\phi(b) > \phi(r)$.

   (c) A ring R is a principal ideal domain if it is an integral domain and if, for every ideal $I \subseteq R$, there exists an element $a \in R$ such that $I = (a)$, i.e. I is a principal ideal.

   (d) A ring R is a unique factorisation domain if: (i) For every non-zero non-unit $a \in R$, there exists $n \geq 1$ and irreducibles $p_1, \cdots, p_n \in R$ such that $a = p_1 \cdots p_n$, (ii) Given $n, m \geq 1$ and irreducibles $p_1, \cdots, p_n, q_1, \cdots, q_m \in R$ such that $p_1 \cdots p_n = q_1 \cdots q_m$, we have $n = m$ and there exists a bijection $\sigma : \{1, \cdots, n\} \to \{1, \cdots, n\}$ such that, for all $1 \leq i \leq n$, p_i is an associate of $q_{\sigma(i)}$.

   (e) Let $\phi : R \to \mathbb{Z}_{\geq 0}$ be a Euclidean function and let $I \subseteq R$ be an ideal. We claim that I is principal.

   If $I = \{0\}$, then $I = (0)$. Assume $I \neq \{0\}$ so that $I \setminus \{0\}$ is a non-empty set. By the well-ordering principle, there exits $b \in I \setminus \{0\}$ such that $\phi(b) \in \mathbb{Z}_{\geq 0}$ is minimal. Let $a \in I$. Then, since R is a Euclidean domain with function ϕ and $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$ and $\phi(b) > \phi(r)$. Since I is an ideal, $r = a - qb \in I$. Since $\phi(b)$ is minimal, this implies that $r = 0$ and so $a = qb$, i.e. $a \in (b)$. Hence $I = (b)$.

   (1 mark shared across f, g, h: stating anywhere that PID $\Rightarrow$ UFD and correctly applying the implications ED $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ ID)

   (f) Let $f = 2 \in (\mathbb{Z}/4\mathbb{Z})[X]$, i.e. the constant polynomial with constant term $2 = 2 + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$. We have $f \neq 0$ but $f^2 = 4 = 0 \in (\mathbb{Z}/4\mathbb{Z})[X]$. Hence $(\mathbb{Z}/4\mathbb{Z})[X]$ is not an ID. By definition, this implies it is not an ED, PID or UFD.

   (g) We claim that $\mathbb{Z}[\omega] \leq \mathbb{C}$ is an ED with Euclidean function $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_{\geq 0}$ given by $z \mapsto z\bar{z} = |z|^2$. Given $z = a + b\omega + c\omega^2$, we need to check that $\psi(z) \in \mathbb{Z}_{\geq 0}$. We have $|z|^2 = (a + b\omega + c\omega^2)(a + c\omega + b\omega^2) = (a^2 + b^2 + c^2) + (ab + bc + ca)(\omega + \omega^2) = a^2 + b^2 + c^2$.

(1 mark: checking it is an ED with good choice of ϕ, show ϕ lands in $\mathbb{Z}_{\geq 0}$)

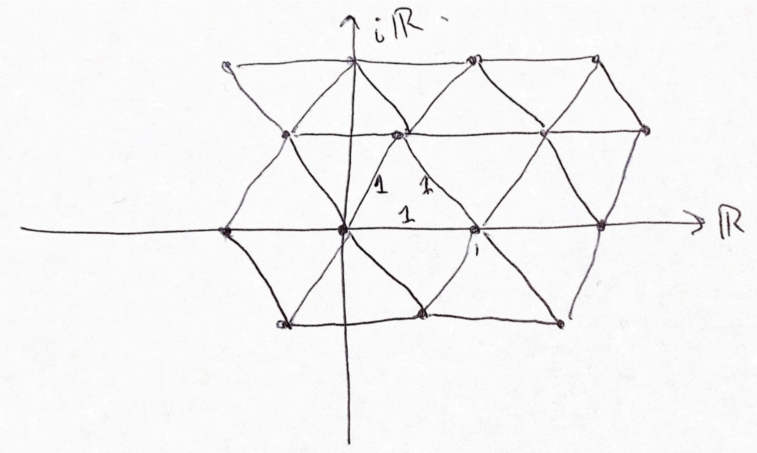
We will now check conditions (i) and (ii) from our definition.

(i) Give $z_1, z_2 \in \mathbb{Z}[\omega]$, we have $\phi(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 |z_2|^2 = \phi(z_1)\phi(z_2)$, i.e. ϕ is a ring homomorphism. Note that $\bar{\omega} = \omega^2 = -\omega$. Let $z_1, z_2 \in \mathbb{Z}[\omega]$ with $z_2 \neq 0$. Then $\phi(z_2) \neq 0$ and so $\phi(z_2) \geq 1$. Hence we have $\phi(z_1 z_2) = \phi(z_1) \cdot \phi(z_2) \geq \phi(z_1)$.

(1 mark: checking property (i))

(ii) Let $z_1, z_2 \in \mathbb{Z}[\omega]$ with $z_2 \neq 0$. Then $\frac{z_1}{z_2} \in \mathbb{C}$.

We claim that, given any $z \in \mathbb{C}$, there exists $z' \in \mathbb{Z}[\omega]$ such that $|z - z'| < 1$. To see this, note that $\omega = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and so $\mathbb{Z}[\omega]$ gives the following lattice when viewed as a subset of $\mathbb{C}$:



This splits the regions into small triangles of side lengths 1. If $z \in \mathbb{Z}[\omega]$, we can take $z' = z$ so that $|z - z'| = 0$. If $z \notin \mathbb{Z}[\omega]$, then it lies in the interior of one of these triangles and picking $z' \in \mathbb{Z}[\omega]$ to be any of the three vertices gives $|z - z'| < 1$.

(2 marks: correct picture drawn or described, some justification for "$|z - z'| < 1$")

By applying this in the situation above, there exists $q \in \mathbb{Z}[\omega]$ such that $|\frac{z_1}{z_2} - q| < 1$, i.e. that $|z_1 - z_2 q|^2 < |z_2|^2$. Let $r = z_1 - z_2 q$. Then $r \in \mathbb{Z}[\omega]$ and $\phi(z_2) = |z_2|^2 > |r|^2 = x(r)$, as required.

(1 marks: stating "given any $z \in \mathbb{C}$, there exists $z' \in \mathbb{Z}[\omega]$ such that $|z - z'| < 1$" and completing the argument from this point)

Finally recall the following result from lectures.

Theorem: If R is a PID, then R is a UFD.

Hence, combining with (e), we have a chain of implications ED $\Rightarrow$ PID $\Rightarrow$ UFD $\Rightarrow$ ID. In particular, $\mathbb{Z}[\omega]$ is an ED, PID, UFD and ID.

(h) Recall the following two results from lectures.

Theorem: If F is a field, then $F[X]$ is an ED.

Theorem: If R is a UFD, then $R[X]$ is a UFD.

The first result implies that $\mathbb{Q}[X]$ is an ED. By the chain of implications stated in (g), $\mathbb{Q}[X]$ must be a UFD. The second result then implies that $\mathbb{Q}[X, Y] = (\mathbb{Q}[X])[Y]$ is a UFD. Hence it is also an ID.

(2 marks: proof that $\mathbb{Q}[X, Y]$ is a UFD, stating the right results from lectures)

We claim that $\mathbb{Q}[X,Y]$ is not a PID. By the chain of implications stated in (g), this implies it is not an ED either.

For ease of notation, write $R = \mathbb{Q}[Y]$ so that $R[X] = \mathbb{Q}[X,Y]$. Given $f \in R[X]$, let $\deg(f) \in \mathbb{N} \cup \{-\infty\}$ denote the degree viewed as a polynomial in X. The second result above implies that R is an ED so it is certainly an ID. Since R is an ID, we have $\deg(fg) = \deg(f) + \deg(g)$ for $f, g \in R[X]$.

Let $I = (X,Y) \subseteq R[X]$. We claim that I is proper. If $I = R[X]$, then $1 \in I$ and so there exists $f, g \in R[X]$ such that $1 = fX + gY$. However fX and gY both have constant term 0. Comparing constant terms then leads to a contradiction.

(1 mark: stating an ideal which works (i.e. which is not principal), checking it is proper)

We now claim that I is not principal. Suppose $I = (f)$ for some $f \in R[X]$. Then $X, Y \in (f)$ implies there exists $g, h \in R[X]$ such that $fg = X$ and $fh = Y$. The second implies $\deg(f) + \deg(h) = \deg(Y) = 0$. Since $h \neq 0$ (since otherwise $Y = 0$), we have that $\deg(f) \leq 0$ and so $f = a$ is a constant polynomial, i.e. $f \in R \subseteq R[X]$. Since $fg = X$, we have $\deg(g) = 1$. It follows that $g = bX$ for some $b \in R$ (e.g. write $g = a_0 + a_1 X$ and compare coefficients using that R is an integral domain). This gives $X = abX$ and $ab = 1$ which implies that $f = a \in R^\times$. But then $I = R[X]$ since I contains a unit. This is a contradiction and so I is not principal. Hence $\mathbb{Q}[X,Y] = R[X]$ is not a PID, as required.

(2 marks: showing the ideal is not principal, both marks requires no major detail to be missing such as stating that $R = \mathbb{Q}[Y]$ is an ID and that "if R is an ID, then $\deg(fg) = \deg(f) + \deg(g)$ for $f, g \in R[X]$", though I would not expect a proof of this second fact)