# Algebra III: Rings and Modules
# Solutions for Problem Sheet 3, Autumn Term 2022-23

John Nicholson

1. Prove that the two definitions of ring localisation given in lectures are equivalent. That is, let $R$ be a commutative ring and let $S \subseteq R$ be a multiplicative submonoid. Show that there is a unique commutative ring $R'$ such that there exists a map $\iota : R \to R'$ which satisfies:

   (i) $\iota(S) \subseteq (R')^\times$, i.e. everything in $S$ gets mapped to a unit in $R'$.

   (ii) For all commutative rings $A$ and maps $\varphi : R \to A$ with $\varphi(S) \subseteq A^\times$, there exists a unique $\widetilde{\varphi} : R' \to A$ such that $\varphi = \widetilde{\varphi} \circ \iota$.

   **Solution**: Existence follows by the definition given in lectures and results on problem sheet 2, i.e. we take $R' = S^{-1}R$ and $\iota : R \to S^{-1}R$. We will show uniqueness.

   Suppose $R_1$ and $R_2$ both have this property with maps $\iota_1 : R \to R_1$ and $\iota_2 : R \to R_2$. It suffices to show that $R_1 \cong R_2$ as rings. Consider the case $R' = R_1$. Since $(A, \varphi) = (R_2, \iota_2)$ satisfy the conditions of (ii), there exists a unique map $f : R_1 \to R_2$ such that $\iota_2 = f \circ \iota_1$. Similarly there exists a unique map $g : R_2 \to R_1$ such that $\iota_1 = g \circ \iota_2$. This implies that $\iota_1 = (g \circ f) \circ \iota_1$. We claim that $g \circ f = \mathrm{id}_{R_1}$. To see this, consider the ring $R_1$ and note that $(A, \varphi) = (R_1, \mathrm{id}_{R_1})$ satisfy the conditions of (ii). This implies that $\mathrm{id}_{R_1}$ is the unique map such that $\iota_1 = \mathrm{id}_{R_1} \circ \iota_1$. Hence $g \circ f = \mathrm{id}_{R_1}$. Similarly we have $f \circ g = \mathrm{id}_{R_2}$. This implies that $f$ is a ring isomorphism and so $R_1 \cong R_2$ as required.

2. Let $R$ be a unique factorisation domain, let $F$ denote its field of fractions and let

   $$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X].$$

   Show that, if $\frac{p}{q} \in F$ is a root of $f$ for $p, q \in R$ with $\gcd(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$ in $R$. [This is a generalisation of the Rational Root theorem.]

   **Solution**: Let $f = c(f) f_1$ where $f_1$ is primitive. Then $\frac{p}{q} \in F$ is a root of $f_1$. Since $F[X]$ is Euclidean domain, this means we can write $f_1 = (qX - p)g$ for some $g \in F[X]$. Since $f_1$ is primitive and reducible in $F[X]$, it must be reducible in $R[X]$ by Gauss' lemma. It follows that $f_1 = (qX - p)g$ for some $g \in R[X]$ (this follows from the proof of Gauss' lemma but can also be seen directly). If $g = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$, then $f_1$ has constant term $-pb_0$ and leading term $qb_{n-1}$. Since $f = c(f) f_1$, we have that $-pb_0 \mid a_0$ and $qb_{n-1} \mid a_n$. Hence $p \mid a_0$ and $q \mid a_n$ as required.

   Note that an elementary solution is also possible.

3. Show that the following polynomials are irreducible in $\mathbb{Q}[X, Y]$:

$$3X^3Y^3 + 7X^2Y^2 + Y^4 + 2XY + 4X, \qquad 2X^2Y^3 + Y^4 + 4Y^2 + 2XY + 6.$$

**Solution**:
$3X^3Y^3+7X^2Y^2+Y^4+2XY+4X$: This can be rewritten as $Y^4+3X^3Y^3+7X^2Y^2+2XY+4X$; we regard it as a polynomial in $Y$ with coefficients in $\mathbb{Q}[X]$. Note that it is monic, that each of the coefficients other than the leading one lies in the prime ideal $\langle X\rangle$, and that the "constant term" $4X$ does not lie in $\langle X\rangle^2$. Thus this polynomial is irreducible by Eisenstein's criterion.

$2X^2Y^3 + Y^4 + 4Y^2 + 2XY + 6$: This is monic in $Y$, and this is irreducible in $\mathbb{Q}[X, Y]$ if, and only if, it is irreducible in $\mathbb{Q}(X)[Y]$. Since $\mathbb{Z}[X]$ has field of fractions $\mathbb{Q}(X)$, and is a UFD, this polynomial is irreducible in $\mathbb{Q}(X)[Y]$ if and only if it is irreducible in $\mathbb{Z}[X][Y]$. But as a polynomial in $\mathbb{Z}[X][Y]$ this polynomial is Eisenstein mod (2), so it is irreducible.

4. We say a polynomial in $\mathbb{Z}[X, Y]$ is *primitive* if the greatest common divisor of its (integer) coefficients is one. Show that:

   (i) If $f, g \in \mathbb{Z}[X, Y]$ are primitive, then $fg$ is primitive.

   (ii) If $f \in \mathbb{Z}[X, Y]$ is primitive, then $f \in \mathbb{Z}[X, Y]$ is irreducible if and only if $f \in \mathbb{Q}[X, Y]$ is irreducible. [This is the analogue of Gauss' lemma for multivariate polynomials.]

**Solution**: (i) We first show (following the single variable setting) that if $P(X, Y)$ and $Q(X, Y)$ are primitive in $\mathbb{Z}[X, Y]$ (that is, their coefficients have GCD one) then so is their product. Suppose that $p$ is a prime in $\mathbb{Z}$ that divides every coefficient of the product $P(X, Y)Q(X, Y)$. Then we have that $P(X, Y)Q(X, Y) = 0$ in $\mathbb{Z}/p\mathbb{Z}[X, Y]$. Since the latter is a domain, we must have that either $P(X, Y)$ or $Q(X, Y)$ is zero mod $p$, contradicting the fact that $P(X, Y)$ and $Q(X, Y)$ are primitive.

(ii) Suppose we have $P(X, Y) = Q(X, Y)R(X, Y)$ in $\mathbb{Z}[X, Y]$. Then (considering this as a factorisation in $\mathbb{Q}[X, Y]$) we see by irreducibility of $P(X, Y)$ that at least one factor is a unit in $\mathbb{Q}[X, Y]$, hence a nonzero constant. WLOG assume $Q(X, Y)$ is this factor; then $Q(X, Y)$ lies in $\mathbb{Q}$ and $\mathbb{Z}[X, Y]$, so $Q(X, Y)$ must be an integer $d$. But then $d$ divides each coefficient of $P(X, Y)$, so must be equal to $\pm 1$.

Now suppose that $P(X, Y)$ is an irreducible (thus primitive) polynomial in $\mathbb{Z}[X, Y]$, and that we have a factorization $P(X, Y) = Q(X, Y)R(X, Y)$ in $\mathbb{Q}[X, Y]$. Let $q$ and $r$ be rational numbers such that $qQ(X, Y)$ and $rR(X, Y)$ are primitive polynomials with integer coefficients. Then $qrP(X, Y) = qQ(X, Y)rR(X, Y)$, so by the previous paragraph $qrP(X, Y)$ is a primitive rational multple of $P(X, Y)$. Thus $qr = \pm 1$. Thus $P(X, Y) = \pm qQ(X, Y)rR(X, Y)$ is a factorization of $P(X, Y)$ in $\mathbb{Z}[X, Y]$, so one of $qQ(X, Y)$ or $rR(X, Y)$ is equal to $\pm 1$. But then one of $Q(X, Y)$ or $R(X, Y)$ is constant, so $P(X, Y)$ is irreducible in $\mathbb{Q}[X, Y]$.

5. For each of the following elements $\alpha \in \mathbb{C}$ determine whether $\alpha$ is an algebraic integer and, if so, compute its minimal polynomial $f_\alpha$.

$$(1 + \sqrt{3})/2, \quad 2\cos(2\pi/7), \quad (1 + i)\sqrt{3}, \quad \sqrt{5}/\sqrt{7}, \quad i + \sqrt{3}.$$

**Solution**: $(1 + \sqrt{3})/2$: Not an algebraic integer. If so, then $\alpha(1 - \alpha) = \frac{1^2-3}{4} = -\frac{1}{2}$ is an algebraic integer. This is a contradiction since the algebraic integers in $\mathbb{Q}$ are $\mathbb{Z}$.

$2\cos(2\pi/7)$: We claim that $f_\alpha = X^3 + X^2 - 2X - 1$. Let $\zeta_7 = e^{2\pi i/7}$ so that $\alpha = \zeta_7 + \zeta_7^{-1}$. Then $\alpha^2 = \zeta_7^2 + \zeta_7^{-2} + 2$ and $\alpha^3 = \zeta_7^3 + \zeta_7^{-3} + 3\alpha$. Hence have $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$. So

$f_\alpha \mid X^3 + X^2 - 2X - 1$. But $X^3 + X^2 - 2X - 1$ is irreducible since, by the rational root theorem and the fact that $\pm 1$ are not roots, it has no linear factors.

$(1+i)\sqrt{3}$: We claim that $f_\alpha = X^4 + 36$. We have $\alpha^2 = -2i \cdot 3 \Rightarrow \alpha^4 = -36$, so $f_\alpha \mid X^4 + 36$. Since $X^4 + 36$ is monic, all rational roots are in $\mathbb{Z}$ by the rational root theorem (i.e. question 2). Clearly it has no integer roots and so $X^4 + 36$ has no linear factors. Hence, if $f_\alpha$ is not an associate of $X^4 + 36$, it has degree two. But $X^4 + 36 = (X^2 + 6i)(X^2 - 6i)$. This is a factorisation in $(\mathbb{Z}[i])[X]$ which is a UFD since $\mathbb{Z}[i]$ is a UFD (this follows from the fact it is an ED). $X^2 + 6i$ and $X^2 - 6i$ are irreducible in $(\mathbb{Z}[i])[X]$ since their roots are not in $\mathbb{Z}[i]$. Since $f_\alpha$ has degree two and no roots in $\mathbb{Z}[i]$, it must be irreducible in $(\mathbb{Z}[i])[X]$ and so, since $(\mathbb{Z}[i])[X]$ is a UFD, it must be an associate of $X^2 + 6i$ or $X^2 - 6i$ which is a contradiction.

[A much better way to prove this would be to prove that the rational minimal polynomial has degree 4 since the field $\mathbb{Q}(\alpha)$ has degree 4. This follows from the fact that it has distinct subfields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{3})$. However, this material was not included in the course.]

$\sqrt{5}/\sqrt{7}$: Not an algebraic integer. If so, then $\alpha^2 = \frac{5}{7}$ is an algebraic integer. This is a contradiction since the algebraic integers in $\mathbb{Q}$ are $\mathbb{Z}$.

$i + \sqrt{3}$: We claim that $f_\alpha = X^4 - 4X^2 + 16$. We have $\alpha^2 = 2 + 2i\sqrt{3} \Rightarrow (\alpha^2 - 2)^2 = -12 \Rightarrow \alpha^4 - 4\alpha^2 + 16 = 0 \Rightarrow f_\alpha \mid X^4 - 4X^2 + 16$. The fact this is irreducible follows by a similar argument to the case $\alpha = (1+i)\sqrt{3}$.

6. Let $R$ be a commutative ring. Show that $R$ is Noetherian if and only if every ideal $I \subseteq R$ is finitely generated.

   **Solution**: ($\Leftarrow$): Suppose every ideal of $R$ is finitely generated. Given the chain $I_1 \subseteq I_2 \subseteq \cdots$, let:

$$I = \bigcup_{i \geq 1} I_i$$

   This is an ideal (e.g. we proved this in lectures). We know $I$ is finitely generated, say $I = (r_1, \cdots, r_n)$, with $r_i \in I_{k_i}$. Let

$$K = \max_{i=1,\cdots,n} \{k_i\}.$$

   Then $r_1, \cdots, r_n \in I_K$. So $I_K = I$. So $I_K = I_{K+1} = I_{K+2} = \cdots$.

   ($\Rightarrow$): To prove the other direction, suppose there is an ideal $I \lhd R$ that is not finitely generated. We pick $r_1 \in I$. Since $I$ is not finitely generated, we know $(r_1) \neq I$. So we can find some $r_2 \in I \setminus (r_1)$.

   Again $(r_1, r_2) \neq I$. So we can find $r_3 \in I \setminus (r_1, r_2)$. We continue on, and then can find an infinite strictly ascending chain

$$(r_1) \subseteq (r_1, r_2) \subseteq (r_1, r_2, r_3) \subseteq \cdots.$$

   So $R$ is not Noetherian.

7. Let $R$ be a commutative ring. Give a proof or counterexample to each of the following statements:

   (i) If $R$ is Noetherian, then $R$ is an integral domain.

   (ii) If $R[X]$ is Noetherian, then $R$ is Noetherian. [The converse to Hilbert's basis theorem.]

   (iii) Let $S \subseteq R$ be a multiplicative submonoid. If $R$ is Noetherian, then $S^{-1}R$ is Noetherian.

**Solution**: (i) False. For example, take $\mathbb{Z}/6\mathbb{Z}$. This is not an integral domain but it is Noetherian since it is a finite ring and all finite rings are Noetherian.

(ii) True. Let $I_1 \subseteq I_2 \subseteq \dots$ be an infinite increasing sequence of ideals of $R$, and for each integer $k$, let $J_k$ be the subset of $R[X]$ consisting of polynomials all of whose coefficients lie in $I_k$. Then $J_1 \subseteq J_2 \subseteq \dots$ is an infinite increasing sequence of ideals of $R[X]$, so it is eventually stable. But since $I_k = J_k \cap R$, this means the $I_k$ are also eventually stable.

(iii) True. Recall from lectures that every ideal of $S^{-1}R$ is of the form $S^{-1}I = \{\frac{i}{s} : i \in I, s \in S\}$ for some ideal $I \subseteq R$. Suppose $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain in $S^{-1}R$. Then this implies that there exists ideals $J_i \subseteq R$ such that $I_i = S^{-1}J_i$ for all $i \geq 1$. Since $I_i \subseteq I_{i+1}$ for all $i$, we have $J_i \subseteq J_{i+1}$ for all $i$. Since $R$ is Noetherian, there exists $N$ such that $J_{i+N} = J_N$ for all $i \geq 0$. This then implies that $I_{i+N} = I_N$ for all $i \geq 0$. Hence $S^{-1}R$ is Noetherian.

8. Let $R$ and $S$ be rings. Show that every $(R\times S)$-module $M$ is isomorphic to a product $M_1 \times M_2$, where $M_1$ is an $R$-module and $M_2$ is an $S$-module, and the $(R \times S)$-module structure on $M_1 \times M_2$ is given by $(r, s) \cdot (m_1, m_2) = (rm_1, sm_2)$.

**Solution**: Let $e_1 = (1, 0)$ and $e_2 = (0, 1)$ in $R \times S$, and set $N_1 = e_1M$, $N_2 = e_2M$. Although a priori $N_1$ and $N_2$ are $(R \times S)$-modules, we note that $(r, s)e_1m = (r, 0)m$ and $(r, s)e_2m = (0, s)m$, so that "multiplication by $(r, s)$" depends only on $r$ on $N_1$ and only on $s$ on $N_2$. Give $N_1$ the structure of an $R$-module by setting $re_1m = (r, 0)e_1m$ and similarly give $N_2$ the structure of an $S$-module.

We then have maps $N_1 \times N_2 \to M$ and $M$ to $N_1 \times N_2$ that take $(n_1, n_2)$ to $n_1 + n_2$ and $m$ to $(e_1m, e_2m)$. It is easy to see that these are inverse to each other and define homomorphisms of $(R \times S)$-modules, so we have our desired isomorphism.

9. Let $R$ be a ring. An $R$-module is $M$ said to be *cyclic* if $M$ it is generated by one element, and *simple* if $M$ has no $R$-submodules other than 0 and $M$.

   (i) Show that any cyclic $R$ module is isomorphic to $R/I$ for some ideal $I$ of $R$.

   (ii) Show that any simple $R$-module is cyclic.

   (iii) Show that $M$ is a simple $R$-module if and only if $M$ is isomorphic to $R/I$ for some maximal ideal $I$ of $R$.

**Solution**: (i) Let $m$ generate $M$, and consider the map $R \to M$ of $R$-modules taking 1 to $m$ (and thus taking $r$ to $rm$ for all $r \in R$). It is clear that this is a surjective homomorphism of $R$-modules, and its kernel is an $R$-submodule (i.e. ideal) $I$ of $R$. We thus get an isomorphism $R/I \cong M$.

(ii) Let $M$ be simple and $m \in M$ nonzero. The submodule of $M$ generated by $m$ is then nonzero, so must be all of $M$.

(iii) By part (i), we must show that $R/I$ is simple if, and only if, $I$ is maximal. Let $f : R \to R/I$ be the natural quotient map. Then given any submodule $J$ of $R/I$, its preimage $f^{-1}(J)$ is an ideal of $R$ containing $I$. This gives a bijection between the ideals of $R$ containing $I$ and the submodules of $R/I$. In particular we see that $R/I$ is simple if, and only if, the only ideals containing $I$ are $I$ itself and the unit ideal; that is, if and only if $I$ is maximal.

10. Let $R$ be a ring and $M$ an $R$-module. Define the *endomorphism ring* of $M$ to be set $\mathrm{End}_R(M) := \{f : M \to M \mid f \text{ is an } R\text{-module homomorphism}\}$ with pointwise addition and multiplication given by function composition. The *automorphism group* of $M$, denoted by $\mathrm{Aut}_R(M)$, is defined to be the group of units of $\mathrm{End}_R(M)$.

    (i) Show that the two definitions of $R$-module given in lectures are equivalent. That is, for an abelian group $M$, show that the structure $\cdot : R \times M \to M$ of a left $R$-module on $M$ is the same information as a ring homomorphism $\varphi : R \to \mathrm{End}(M)$.

    (ii) Show that a $\mathbb{Z}$-module is the same thing as an abelian group. Deduce that, for for an abelian group $M$, we have $\mathrm{End}(M) \cong \mathrm{End}_{\mathbb{Z}}(M)$ and $\mathrm{Aut}(M) \cong \mathrm{Aut}_{\mathbb{Z}}(M)$.

    (iii) Let $G$ be a group and $M$ an abelian group. Show that an $R[G]$-module structure on $M$ is equivalently an $R$-module structure on $M$ and a homomorphism $\varphi : G \to \mathrm{Aut}_R(M)$.

    (iv) Let $G$ be a group. Show that a $\mathbb{Z}[G]$-module is equivalently an abelian group $M$ with a $G$-action, i.e. group homomorphism $G \to \mathrm{Aut}(M)$. [We often call this a $G$-module.]

    [Hint: To show that two definitions are equivalent, we need to establish a one-to-one correspondence. For example, you could show that (a) for every abelian group $A$, there exists a $\mathbb{Z}$-module $M_A$, (b) For every $\mathbb{Z}$-module $M$, there exists an abelian group $A(M)$, (c) $A(M_A) \cong A$ as abelian groups and $M_{A(M)} \cong M$ as $\mathbb{Z}$-modules.]

    **Solution**: (i) If $R \times M \to M$ is a left module structure, then we have first to check that $\varphi(a)(m) := a \cdot m$ defines an element $\varphi(a) \in \mathrm{End}(M)$, i.e., that $\varphi(a)$ is additive (as we recall from group theory, this is enough to be a group endomorphism). It follows from the distributivity axioms of a left $R$-module that $\varphi(a)$ is additive, as desired. Next we check that $\varphi$ is a homomorphism. It follows from the other distributivity axiom that $\varphi(a+b) = \varphi(a) + \varphi(b)$, and from the associative axiom that $\varphi(ab) = \varphi(a)\varphi(b)$. Finally the unit axiom implies that $\varphi(1) = \mathrm{Id}_M$.

    Similarly, if $\varphi$ is a ring homomorphism, then the same argument in reverse shows that $a \cdot b = \varphi(a)(m)$ defines an action. Finally, we note that if we apply the map (def 1) $\Rightarrow$ (def 2) and then (def 2) $\Rightarrow$ (def 1) we get the original action back, and similarly in the other direction we get the homomorphism back.

    (ii) Given an abelian group $A$, define $M_A$ to be the $\mathbb{Z}$-module with abelian group $A$ and with action $\mathbb{Z} \to \mathrm{End}(A)$ the unique ring homomorphism $n \mapsto \underbrace{\mathrm{id}_A + \cdots \mathrm{id}_A}_{n}$. Given an $\mathbb{Z}$-module $M$, let $A(M)$ denote its underlying abelian group. By definition, we have $A(M_A) \cong A$ as abelian groups. Finally, $M \cong M_{A(M)}$ are isomorphic as $\mathbb{Z}$-modules with the $\mathbb{Z}$-actions are determined by maps $\mathbb{Z} \to \mathrm{End}(A)$ which are unique.

    (iii) By part (i), an $R[G]$-module structure on $M$ is a map $\varphi : R[G] \to \mathrm{End}(M)$. Restricting this map to $R$ gives an $R$-modules structure on $M$. Since $G \subseteq R[G]^\times$, we have that $\varphi(G) \subseteq \mathrm{End}(M)^\times = \mathrm{Aut}(M)$. Hence, by restricting to $G$, we get a map $\varphi\mid_G : G \to \mathrm{Aut}(M)$. We want to show this lands in $\mathrm{Aut}_R(M)$. For $g \in G$, $\varphi(g) : M \to M$ is an abelian group homomorphism and we want to show that $\varphi(g)(r \cdot m) = r \cdot \varphi(g)(m)$. By definition, we have $r \cdot m = \varphi(r)(m)$ and $r \cdot \varphi(g)(m) = \varphi(r)(\varphi(g)(m))$. We have:

    $$\begin{aligned}\varphi(g)(r \cdot m) &= \varphi(g)(\varphi(r)(m)) = (\varphi(g) \cdot_{\mathrm{End}(M)} \varphi(r))(m) = \varphi(gr)(m) \\ &= \varphi(rg)(m) = (\varphi(r) \cdot_{\mathrm{End}(M)} \varphi(g))(m) = \varphi(r)(\varphi(g)(m)) = r \cdot \varphi(g)(m)\end{aligned}$$

    since $\varphi$ is multiplicative and since $r, g \in R[G]$ commute. Hence $\varphi$ restricts to a map $\varphi\mid_G : G \to \mathrm{Aut}_R(M)$.

Given an $R$-module structure on $M$ given by $h : R \to \mathrm{End}(M)$ and a homomorphism $f : G \to \mathrm{Aut}_R(M) \subseteq \mathrm{End}(M)$, define $\widehat{f} : R[G] \to \mathrm{End}(M)$ by $\sum r_i g_i \mapsto \sum h(r_i) \cdot_{\mathrm{End}(M)} f(g_i)$. It can be easily verified that this is a ring homomorphism.

Given $f : G \to \mathrm{Aut}_R(M)$, it is clear that $\widehat{f} \mid_G = f$. It also needs to be verified that, given $\varphi : R[G] \to \mathrm{End}(M)$, we have $\widehat{\varphi \mid_G} = \varphi$.

(iv) This is essentially immediate from (ii) and (iii).

+11. If $R$ is a ring, the *formal power series ring* $R[[X]]$ is the ring with elements

$$f = a_0 + a_1 X + a_2 X^2 + \cdots ,$$

where each $a_i \in R$. This has addition and multiplication the same as for polynomials, but without upper limits. Show that, if $R$ is Noetherian, then $R[[X]]$ is Noetherian.

**Solution not provided.** You may continue to work on this throughout the term and contact me to discuss ideas and/or hand in a solution. Remember that this problem is optional and may be significantly more challenging than the other problems.