Algebra III: Rings and Modules
Solutions for In-Class Test 2, Autumn Term 2022-23

John Nicholson

1. (a) Give the definition of:
   - (i) Algebraic integer. (1 mark)
   - (ii) Field of fractions. (1 mark)
   - (iii) $\mathbb{Z}[\alpha]$ where α is an algebraic integer. (1 mark)

   (b) Let $\beta \in \mathbb{C}$ be an algebraic integer such that $R = \mathbb{Z}[\beta]$ is a unique factorisation domain, let $\alpha \in \mathbb{C}$ be the root of a monic polynomial in $R[X]$ and let $F = \mathrm{Frac}(R)$.
   - (i) Prove that there exists a unique monic polynomial $f_{\alpha,\beta} \in F[X]$ such that, for all polynomials $f \in F[X]$ which have α as a root, we have $f_{\alpha,\beta} \mid f$ in $F[X]$. (5 marks)
   - (ii) Prove that there exists a unique monic polynomial $g_{\alpha,\beta} \in R[X]$ such that, for all polynomials $f \in R[X]$ which have α as a root, we have $g_{\alpha,\beta} \mid f$ in $R[X]$. Furthermore, show that $f_{\alpha,\beta} = g_{\alpha,\beta}$. (10 mark)
   - (iii) Let $\beta_1, \beta_2 \in \mathbb{C}$ be algebraic integers such that $R_1 = \mathbb{Z}[\beta_1]$ and $R_2 = \mathbb{Z}[\beta_2]$ are unique factorisation domains and suppose $\alpha \in \mathbb{C}$ is both a root of a monic polynomial in $R_1[X]$ and a root of a monic polynomial in $R_2[X]$. Give examples to show that f_{α,β_1} and f_{α,β_2} need not have the same degree. (2 marks)

   (Total: 20 marks)

Solution: (a) (i) $\alpha \in \mathbb{C}$ is an algebraic integer if it is the root of a monic polynomial $f \in \mathbb{Z}[X]$.

(ii) Let R be an integral domain. Then the field of fractions, denoted by $\mathrm{Frac}(R)$, is defined as the localisation $S^{-1}R$ where $S = R \setminus \{0\}$.

(iii) Let $\alpha \in \mathbb{C}$ be an algebraic integer. Then $\mathbb{Z}[\alpha]$ is defined as the smallest subring $R \le \mathbb{C}$ such that $\alpha \in R$ and $\mathbb{Z} \subseteq R$.

(b) (i) We will use the following two results from lectures:

Theorem: Let F be a field. Then $F[X]$ is a Euclidean domain.

Theorem: If R is Euclidean domain, then R is a principal ideal domain.

Since $F = \mathrm{Frac}(R)$ is a field, the above results imply that $F[X]$ is a principal ideal domain. **(1 mark: deducing that $F[X]$ is a PID from known statements)**

Now let $I = \{f \in F[X] : f(\alpha) = 0\}$. Then $I \subseteq F[X]$ is an ideal. To see this, note that $\psi : F[X] \to F$, $f \mapsto f(\alpha)$ is a ring homomorphism with $\ker(\psi) = I$, and kernels of ring homomorphisms are ideals. (Alternatively, we could just check that I is an ideal directly.) **(1 mark: considering the right I and proving it is an ideal)**

Since I is an ideal and $F[X]$ is a principal ideal domain, we have that $I = (h)$ for some $h \in F[X]$. Since α is the root of a monic polynomial in $R[X]$, we know that $I \neq \{0\}$ and so

$h \neq 0$. Suppose h has leading coefficient $a \in F \setminus \{0\} = F^\times$. Then $f_{\alpha,\beta} := a^{-1}h$ is monic. Since $a \in F^\times$, we have that $I = (h) = (af_{\alpha,\beta}) = (f_{\alpha,\beta})$. Hence, for all $f \in F[X]$ such that $f(\alpha) = 0$, we have that $f \in (f_{\alpha,\beta})$ and so $f_{\alpha,\beta} \mid f$ as required. **(2 mark: using the facts above to complete the proof, including checking that f is monic)**

To show that $f_{\alpha,\beta}$ is unique, suppose $g \in F[X]$ is monic and also has this property. Then $I = (f_{\alpha,\beta}) = (g)$ and so $g = af_{\alpha,\beta}$ for some $a \in F^\times$. Since g and $f_{\alpha,\beta}$ and both monic, comparing leading coefficients implies that $a = 1$ and so $g = f_{\alpha,\beta}$. **(1 mark for uniqueness)**

(ii) There are two main solutions I expect students to come up with. Since R is UFD, we can define the content $c(f) \in R$ of a polynomial $f \in R[X]$. We will use the following result from lectures. **(1 mark: acknowledging that we need UFD to define content)**

Lemma: If $f, g \in R[X]$, then $c(fg) = c(f) \cdot c(g)$ (where equality is up to associates).

(1 mark: stating a lemma of this type, or at least applying it consistently)

Solution 1: We will show that $f_{\alpha,\beta} \in R[X]$ and that it satisfies the required property. Thus, we complete both parts of the question simultaneously.

Let $d \in R \setminus \{0\}$ be such that $df_{\alpha,\beta} \in R[X]$ is primitive. Let $f \in R[X]$ be such that $f(\alpha) = 0$. By (i), there exists $h \in F[X]$ such that $f = h \cdot df_{\alpha,\beta}$. We now claim that $h \in R[X]$. Suppose $a \in R \setminus \{0\}$ is such that $ah \in R[X]$. Then $af = (ah) \cdot (df_{\alpha,\beta})$. Taking contents yields $a \cdot c(f) = c(ah)$ since $df_{\alpha,\beta}$ is primitive. This implies that $ah = a\bar{h}$ for some $\bar{h} \in R[X]$ and so $h = \bar{h} \in R[X]$ since $a \neq 0$ and R is an integral domain. Hence $df_{\alpha,\beta} \mid f$ for all $f \in R[X]$ with $f(\alpha) = 0$. **(5 mark for showing an R-multiple of $f_{\alpha,\beta}$ works)**

Now let $f_0 \in R[X]$ be a monic polynomial such that $f_0(\alpha) = 0$. Since $df_{\alpha,\beta} \mid f_0$ in $R[X]$, we can write $f = h \cdot (df_{\alpha,\beta})$ for $h \in R[X]$. Suppose h has leading coefficient $b \in R \setminus \{0\}$. Since f and $f_{\alpha,\beta}$ are both monic, comparing leading coefficients gives that $1 = bd$. Hence $d \in R^\times$ and so $f_{\alpha,\beta} = d^{-1} \cdot (df_{\alpha,\beta}) \in R[X]$. In particular, $g_{\alpha,\beta} := f_{\alpha,\beta}$ satisfies all the necessary conditions. **(2 mark for correctly utilising the monic polynomial f_0)**

Uniqueness follows similarly to in part (i). If $g \in R[X]$ also has this property, then $g \mid g_{\alpha,\beta}$ and $g_{\alpha,\beta} \mid g$ and so g and $g_{\alpha,\beta}$ are associates. Since they are both monic, then implies that $g = g_{\alpha,\beta}$. **(1 mark for uniqueness)**

Solution 2: We will mimic the proof from lectures in the case $\beta = 1$. Let $I = \{f \in R[X] : f(\alpha) = 0\}$. Since α is the root of a monic polynomial in $R[X]$, we know that $I \neq \{0\}$. Let $h \in I$ denote a non-zero polynomial of minimal degree. If h has content $d = c(h)$, then $h = dg$ where $g \in R[X]$ is primitive and $h(\alpha) = d \cdot g(\alpha) = 0$ implies $g(\alpha) = 0$ and so $g \in I$.

(1 mark for showing we can take g to have minimal degree and be primitive)

Let $f \in I$. By the theorem above, $F[X]$ is a Euclidean domain and so there exists $q, r \in F[X]$ such that $f = qg + r$ where $\deg(r) < \deg(g)$. Since $f(\alpha) = g(\alpha) = 0$, we have $r(\alpha) = 0$. If $a \in R \setminus \{0\}$ is such that $ar \in R[X]$, this implies that $ar \in I$. Hence $r = 0$, otherwise this contradicts the fact that g has minimal degree in I among non-zero polynomials. This gives that $f = qg$. **(2 mark for working in $F[X]$, using that it is an ED, proving $r = 0$)**

Let $b \in R \setminus \{0\}$ be such that $aq \in R[X]$. Then $af = (aq) \cdot g$. Taking contents, using the lemma above, yields $a \cdot c(f) = c(aq)$. So $aq = a\bar{q}$ for $\bar{q} \in R[X]$. Since $a \neq 0$ and R is an integral domain, we get $q = \bar{q} \in R[X]$.

(1 mark for showing that $q \in R[X]$ using contents)

Finally, by assumption, there exists $f_0 \in R[X]$ monic such that $f_0(\alpha) = 0$. Since $g \mid f_0$ in $R[X]$, we can write $f = h \cdot g$ for $h \in R[X]$. Suppose g has leading coefficent a and h has leading coefficient $b \in R \setminus \{0\}$. Since f is monic, comparing leading coefficients gives that $1 = ab$. Hence $a \in R^\times$ and so $g_{\alpha,\beta} := a^{-1} \cdot g \in R[X]$ and has the required properties.

(2 mark for correctly utilising the monic polynomial f_0)

Uniqueness follows similarly to in part (i). If $g' \in R[X]$ also has this property, then $g' \mid g_{\alpha,\beta}$ and $g_{\alpha,\beta} \mid g'$ and so g' and $g_{\alpha,\beta}$ are associates. Since they are both monic, then implies that $g' = g_{\alpha,\beta}$. **(1 mark for uniqueness)**

We now claim that $f_{\alpha,\beta} = g_{\alpha,\beta}$. It follows from the definition of $g_{\alpha,\beta}$ that $g_{\alpha,\beta} \mid f_{\alpha,\beta}$. Given this, $g_{\alpha,\beta}$ is also a monic polynomial in $F[X]$ satisfying the same properties as $f_{\alpha,\beta}$. Hence, by uniqueness in (ii), we have that $f_{\alpha,\beta} = g_{\alpha,\beta}$. **(1 mark for last part)**

(iii) Let $\beta_1 = i$ and $\beta_2 = 1$. Then $R_1 = \mathbb{Z}[i]$ and $R_2 = \mathbb{Z}$ are both UFDs. Let $\alpha = i$. Then α is a root of the monic polynomial $X - i \in R_1[X]$ and the monic polynomial $X^2 + 1 \in R_2[X]$. Since $f_{\alpha,\beta_1} \mid X - i$ is monic, we must have $f_{\alpha,\beta_1} = X - i$. Similarly, f_{α,β_2} is monic and has $f_{\alpha,\beta_2} \mid X^2 + 1$. Since $\alpha \notin R_2$, α is not the root of a degree one polynomial and so $\deg(f_{\alpha,\beta_2}) \geq 2$. Hence $f_{\alpha,\beta_2} = X^2 + 1$ since f_{α,β_2} is monic.

(2 mark for stating examples which work)

2. (a) Define what it means for an R-module to be:

(i) Simple. (ii) Finitely generated. (iii) Free. (3 marks)

(b) Determine, with proof, all implications which exist between properties (i), (ii) and (iii) for all rings R. That is, for all $a, b \in \{\mathrm{i}, \mathrm{ii}, \mathrm{iii}\}$ with $a \neq b$, prove that $(a) \Rightarrow (b)$ for all rings R or find a counterexample which demonstrates that $(a) \not\Rightarrow (b)$. (7 marks)

(c) Give a proof or counterexample to each of the following statements:

(i) A non-trivial R-module M is simple and free if and only if $M \cong R$. (2 marks)

(ii) An R-module M is finitely generated if and only if there exists a surjective R-module homomorphism $f : R^n \twoheadrightarrow M$ for some integer $n \geq 1$. (2 marks)

(iii) A non-trivial R-module M is simple if and only if M is isomorphic to R/I for some prime ideal I of R. (3 marks)

(iv) If an R-module M has finitely many R-submodules, then M is finitely generated. (3 marks)

(Total: 20 marks)

Solution: (a) (i) An R-module M is simple if it has no R-submodules other than $\{0\}$ and M.

(ii) An R-module M is finitely generated if there exist $m_1, \cdots, m_n \in M$ such that $M = R \cdot m_1 + \cdots + R \cdot m_n$.

(iii) An R-module is free if there exists a set S such that $M \cong R^{(S)}$, where $R^{(S)} := \bigoplus_{i \in S} R$. (Any definition of free module is acceptable.)

(b) Simple $\Rightarrow$ Finitely generated: True if $R = \{0\}$, so assume $R \neq \{0\}$. Consider $R \cdot 1 \subseteq M$, the R-submodule generated by $1 \in M$. Since $R \neq \{0\}$, we have $0 \neq 1$ and so $R \cdot 1 \neq \{0\}$. Since M is simple, this implies that $R \cdot 1 = M$. Hence M is finitely generated (by the set $\{1\}$).

All five other implications fail. Many examples are possible. In all the examples below, we take $R = \mathbb{Z}$ so that R-modules are abelian groups and R-submodules are abelian subgroups.

Finitely generated $\not\Rightarrow$ Simple: $M = \mathbb{Z}/4$ is finitely generated since $M = \mathbb{Z} \cdot 1$. However, M is not simple since $N = \{0, 2\}$ is a proper abelian subgroup.

Simple or Finitely generated $\not\Rightarrow$ Free: $M = \mathbb{Z}/2$ is finitely generated since $M = \mathbb{Z} \cdot 1$ and is simple since its only abelian subgroups are $\{0\}$ and $\mathbb{Z}/2$. If M is free, then $M \cong \mathbb{Z}^{(S)}$ for some set S. Since M is finite, we must have $S = \emptyset$. But $\mathbb{Z}^{\emptyset} = \{0\}$ and $M \neq \{0\}$. Hence M is not free.

Free $\not\Rightarrow$ Simple or Finitely generated. $M = \mathbb{Z}^{(\mathbb{N})}$ is free. Recall the following result from lectures:

Proposition: Let R be a non-trivial ring. Then $R^{(S)}$ is a finitely generated R-module if and only if S is finite.

Since $R = \mathbb{Z}$ is non-trivial and $S = \mathbb{N}$ is infinite, this implies that M is not finitely generated. We also know that M is not simple since simple implies finitely generated, as shown above.

(1 mark for all the implications being correct, 1 mark for each of the six proofs)

(c) (i) False. Let $R = \mathbb{Z}$. Then $M := \mathbb{Z}$ is not a simple $\mathbb{Z}$-module since $2\mathbb{Z}$ is a proper R-submodule.

(1 mark for example which works, 1 mark for proving it works - note that not much needs to be done for examples with $R = \mathbb{Z}$)

(ii) True. If $M = Rm_1 + Rm_2 + \cdots + Rm_n$, we define $f : R^n \to M$ by

$$(r_1, \cdots, r_n) \mapsto r_1 m_1 + \cdots + r_n m_n.$$

It is clear that this is an R-module homomorphism. This is by definition surjective. So done.

Conversely, given a surjection $f : R^n \twoheadrightarrow M$, we let

$$m_i = f(0, 0, \cdots, 0, 1, 0, \cdots, 0),$$

where the 1 appears in the ith position. We now claim that $M = Rm_1 + Rm_2 + \cdots + Rm_n$. So let $m \in M$. As f is surjective, we know $m = f(r_1, r_2, \cdots, r_n)$ for some r_i. We then have

$$\begin{aligned}
&f(r_1, r_2, \cdots, r_n) \\
&= f((r_1, 0, \cdots, 0) + (0, r_2, 0, \cdots, 0) + \cdots + (0, 0, \cdots, 0, r_n)) \\
&= f(r_1, 0, \cdots, 0) + f(0, r_2, 0, \cdots, 0) + \cdots + f(0, 0, \cdots, 0, r_n) \\
&= r_1 f(1, 0, \cdots, 0) + r_2 f(0, 1, 0, \cdots, 0) + \cdots + r_n f(0, 0, \cdots, 0, 1) \\
&= r_1 m_1 + r_2 m_2 + \cdots + r_n m_n.
\end{aligned}$$

So the m_i generate M. **(1 mark for each direction)**

(iii) False. By the problem sheet, the corresponding statement is true with prime ideals replaced by maximal ideals. To find a counterexample, we need to work over a ring R where prime ideals are not all maximal (i.e. not a PID). **(1 mark for any having this idea)**

Let $R = \mathbb{Z}[X]$ and $I = (X)$. Then $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ as rings. Since $\mathbb{Z}$ is an integral domain, this implies that I is a prime ideal. Let $M := \mathbb{Z}[X]/(X)$, which is an $\mathbb{Z}[X]$-module. Then $M \cong \mathbb{Z}$ as abelian groups and M has the trivial R-action. In particular, M has a non-proper R-submodule $N := 2M$ which is $2\mathbb{Z}$ with the trivial R-action.

(1 mark for an example which works, 1 mark for proving it works)

Alternatively we could note that, since $\mathbb{Z}$ is not a field, this implies that I is not maximal and, in fact, we have $(X) \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$. It then suffices to check that $M := R/I$ has a non-proper R-submodule $(2, X)/(X)$.

(iv) True. Suppose for contradiction that M is not finitely generated. This implies $M \neq \{0\}$, so pick $m_1 \in M \setminus \{0\}$. Since M is not finitely generated, there exists $m_2 \in M \setminus (R \cdot m_1)$. Continuing like this gives an infinite sequence $m_1, m_2, \cdots$ in M such that

$$m_{i+1} \notin R \cdot m_1 + \cdots R \cdot m_i.$$

(2 marks for this construction, or something equivalent)

Let $M_i := R \cdot m_1 + \cdots R \cdot m_i$. Then $M_i \leq M$ is an R-submodule for each i and $m_{i+1} \notin M_i$ implies $M_1 \subsetneq M_2 \subsetneq \cdots$. Hence M_i has infinitely many distinct R-submodules.

(1 mark for carefully checking this works, or something equivalent)