A3: Algebra II

Mathematical Institute, University of Oxford
Hilary Term 2015

Part A Algebra II, examination questions and solutions.

1. Let R be a ring.

a) [8 marks] Let $a, b \in R$. We say that a and b are associate if there is a unit $u \in R^\times$ such that $a = ub$.

- *i)* Show that if a and b are associate then $\langle a \rangle = \langle b \rangle$.
- *ii)* A ring in which the converse holds is called an *associator ring*. Show an integral domain is an associator ring.
- *iii)* What are the ideals in $\mathbb{Z}/4\mathbb{Z}$? Show that $\mathbb{Z}/4\mathbb{Z}$ is an associator ring which is not an integral domain.

b) [5 marks] Show that if R_1 and R_2 are associator rings then so is $R_1 \oplus R_2$.

c) [6 marks] Let R be a PID, p a prime element in R and k a positive integer. Show that $S = R/p^kR$ is an associator ring.

d) [6 marks] If R is a PID, and $\phi\colon R \to S$ is a surjective ring homomorphism, then S is an associator ring.

Solution: Part $a)$: [BW] part $i)$: If $a = ub$ then $a \in \langle b \rangle$ so that $\langle a \rangle \subset \langle b \rangle$. But then $b = u^{-1}a$ similarly shows that $\langle b \rangle \subseteq \langle a \rangle$, so that $\langle a \rangle = \langle b \rangle$ as required. For part $ii)$: if $\langle a \rangle = \langle b \rangle$ then there are $u, v \in R$ such that $a = u.b$ and $b = v.a$. But then $a = u.(va)$ so that $a(1 - uv) = 0$ and hence since R is an integral domain, either $a = 0$ or u, v are units. In the latter case a and b are clearly associates, while in the former $b \in \langle 0 \rangle = \{0\}$ so that $b = 0$ also and hence again a, b are associates. For part $iii)$ let $R = \mathbb{Z}/4\mathbb{Z}$. We have $R^\times = \{1 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$, so that $R = 1.R = 3.R$ and $2R = \{0 + 2\mathbb{Z}, 2 + 2\mathbb{Z}\}$. Thus the only ideals in R are $\{0\}, 2R$ and R. Clearly R is thus an associator ring, because if $I = \langle a \rangle = \langle b \rangle$ then if $I = R$, a and b are units and hence associates, if $I = 2R$, then $a = b = 2 + 4\mathbb{Z}$ (as this is the only nonzero element in the ideal!) Finally if $I = \{0\}$ then $a = b = 1.b = 0$ are again associates. Since $(2 + 4\mathbb{Z})^2 = 0 + 4\mathbb{Z}$, clearly $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.

Part $b)$ [S]: Suppose that $I = \langle (a_1, a_2) \rangle = \langle (b_1, b_2) \rangle \subseteq R_1 \oplus R_2$. Then $I \cap R_1 = a_1R_1 = b_1R_1$, and $I \cap R_2 = a_2R_2 = b_2R_2$, and thus since R_1 and R_2 are associator rings, there are units $u_1 \in R_1$ with $a_1 = u_1b_1$, $a_2 = u_2b_2$, so that $(a_1, a_2) = (u_1, u_2)(a_2, b_2)$. Since $(u_1, u_2).(u_1^{-1}, u_2^{-1}) = (1, 1)$ we see that $(u_1, u_2) \in S^\times$ so that (a_1, b_1) and (a_2, b_2) are associates as required.

Part $c)$: [S] Suppose that $I = \langle a + p^kR \rangle = \langle b + p^kR \rangle$. Note we may assume $a, b \in R$ are both nonzero. If $q\colon R \to R/p^kR$ denotes the quotient map, $q^{-1}(I) = Ra + p^kR = gR$ where g is by definition a highest common factor of a and p^k. Since p is a prime element and R is a UFD, the highest common factor g must be (up to a unit) p^l for some $l \in \mathbb{Z}$ with $0 \leq l \leq k$, and we may write $a = cp^l$, where $p \nmid c$. Since $I = \langle b + p^kR \rangle$ also, we similarly have $b = dp^l$, where $p \nmid d$. But then c and p^k are coprime, so that $Rc + Rp^k = R$ and we may write $1 = \alpha.c + \beta.p^k$ and so $\alpha.c + p^kR = 1 + p^kR$ so that $c + p^kR$ is a unit in R/p^kR, and hence $a + p^kR$ and $p^l + p^kR$ are associates. By symmetry $b + p^kR$ and $p^l + p^kR$ are also associates, and hence $a + p^kR$ and $b + p^kR$ are associates as required.

Variant: As in part $a)$ if $\bar{a}, \bar{b} \in S$ have $\langle \bar{a} \rangle = \langle \bar{b} \rangle$ then there exist $\bar{r}, \bar{s}$ such that $\bar{a} = \bar{r}\bar{b}$ and $\bar{b} = \bar{s}\bar{a}$, so that $\bar{a} = \bar{a}(1 - \bar{r}\bar{s})$. Taking representatives $a, b, r, s \in R$ corresponding to $\bar{a}, \bar{b}, \bar{r}, \bar{s}$ respectively, we see that $p^k | a(1 - rs)$. But then since R is a UFD either p^k divides a, in which case $\bar{a} = 0$ and we are done trivially, or $p | 1 - rs$ and hence clearly p does not divide r or s. But the r, s are coprime of p and hence also p^k, so that by Bezout's Lemma (which holds as R is a PID) there exist $\alpha_1, \alpha_2, \beta_1, \beta_2 \in R$ with $\alpha_1.a + \alpha_2.p^k = 1$ and $\beta_1.b + \beta_2.p^k = 1$. But then $\bar{r}$ and $\bar{s}$ are units in R/p^kR and so $\bar{a}$ and $\bar{b}$ are associates. (Note that in contrast to part $a)$ it does *not* follow that $\bar{r}, \bar{s}$ are inverses of each other: for example in $\mathbb{Z}/4\mathbb{Z}$ above, one has $2 = 3.2 = 1.2$.)

Part $d)$:[N – see below.] Let $J = \ker(\phi)$. Then $J = \langle c \rangle$ for some $c \in R$. Since $S \cong R/cR$ it is enough to prove that R/cR is an associator ring. If $c = 0$ then $R \cong S$ so that S is an associator ring by part $a)$. If $J = R$ then S is the zero ring, which is trivially an associator ring. We may thus assume that c is a nonzero nonunit, and hence since R is a PID and so UFD, we may write $c = p_1^{n_1} \dots p_k^{n_k}$ a product of distinct primes, where $k \geq 1$ and $n_i \geq 1$ for each i, $(1 \leq i \leq k)$. We proceed by induction on k. If $k = 1$ then we are done by part c). If we know the claim for k and $c = \prod_{i=1}^{k+1} p_i^{n_i}$, then by the Chinese Remainder Theorem, (noting that $p_1^{n_1}$ and $d = \prod_{j=2}^{k+1} p_j^{n_j}$ are coprime) we have $R/cR \cong R/p_1^{n_1} \oplus R/dR$, which is an associator ring by part b), as $p_1^{n_1}$ and d both have k or fewer distinct prime factors. $\square$

Note that the Chinese Remainder Theorem argument in part d) is exactly what is used in deducing the primary decomposition form of the structure theorem from the canonical form, so the argument is one they have seen in lectures in a different context.

2. $a)$ [5 marks] State a structure theorem for finitely generated modules over an Euclidean domain, and define the *rank* of such a module. Use it to show that if R is an Euclidean domain and M is a finitely generated torsion-free module, then M is free. [5]

$b)$ [6 marks] The rational numbers $\mathbb{Q}$ are an abelian group under addtition and hence are a $\mathbb{Z}$-module. Show that any two elements of $\mathbb{Q}$ are linearly dependent. Hence or otherwise show that any nonzero finitely generated submodule M of $\mathbb{Q}$ is free of rank 1. [6]

$c)$ [8 marks] Find a basis for the submodule of $\mathbb{Q}$ generated by $\{\frac{2}{5}, \frac{3}{7}, \frac{1}{2}\}$. [8]

$d)$ [6 marks] Show that $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-module. [6]

Solution: Part $a)$: [BW] The structure theorem (in canonical form, they might state the primary decomposition form instead) states that if M is a finitely generated module over an Euclidean domain R, then there exist nonzero non-units $c_1, c_2 \ldots, c_k \in R$ (unique up to units) and a unique non-negative integer s such that $c_1|c_2|\ldots|c_k$ and

$$M \cong R^s \oplus R/c_1R \oplus \ldots R/c_kR.$$

The rank of M is defined to be the integer s. If M is torsion free then in the decomposition above we must have $k = 0$ (as every element of the summand $m \in R/c_1R$ has $c_1 \in \text{Ann}_R(m)$, and hence is torsion). But then $M \cong R^s$ is free as required.

Part $b)$: [N] If $p, q \in \mathbb{Q}$ we may write $p = a/b, q = c/d$ where $b, d \in \mathbb{Z}_{>0}$ and $a, b \in \mathbb{Z}$. But then clearly we have

$$(bc).p - (ad).q = ac - ac = 0,$$

so that p and q are linearly dependent provided bc and ad are not both zero. But since b, d are nonzero, this last happens only if $c = a = 0$, so $p = q = 0$ and then $1.p + 0.q = 0$ is a nontrivial linear dependence. Suppose that $M \subseteq \mathbb{Q}$ is a nonzero finitely generated submodule of $\mathbb{Q}$. Then since $\mathbb{Q}$ is torsion-free (it's a field, so an integral domain, so certainly torsion-free as a $\mathbb{Z}$-module, *i.e.* Abelian group) M is also and so it follows from the first part that M is free. On the other hand we have just seen that $\mathbb{Q}$ has no linearly independent sets of size larger than 1, hence if M is nonzero it must be free of rank one.

Part $c)$: [S] Let $M = \langle\frac{1}{2}, \frac{2}{5}, \frac{3}{7}\rangle$. Clearly M is a submodule of $\mathbb{Z}.(\frac{1}{70})$, and the reverse inclusion follows if we can write $\frac{1}{70} = \frac{a}{2} + \frac{2b}{5} + \frac{3c}{7}$ for some $a, b, c \in \mathbb{Z}$, or equivalently if we can write $1 = 35a + 14b + 30c$, which is clear possible as this set has h.c.f. equal to 1, or more explicitly because $1 = 3.35 - 3.30 - 14$. Thus $\frac{1}{70}$ is a basis for M as required. (*You could adapt this strategy to give a proof of part ii) that did not use the structure theorem.*)

Part $d)$: [N] For the last part, if $\mathbb{Q}$ were finitely generated, by the previous part if would be free of rank one. But then we would have $\mathbb{Q} = \mathbb{Z}.(\frac{m}{n})$ for some $\frac{m}{n} \in \mathbb{Q}$. But since $\frac{1}{n+1} \notin \mathbb{Z}.(\frac{m}{n})$ as $\frac{1}{n+1} < |\frac{a.m}{n}|$ for any $a \in \mathbb{Z}$, this is impossible, and hence $\mathbb{Q}$ is not finitely generated as required. $\square$

3. Let $P \subset \mathbb{Z}[t]$ be a nonzero prime ideal such that $P \cap \mathbb{Z} = \{0\}$.

$a)$ [6 marks] Define the *content* $c(f)$ of a nonzero polynomial $f \in \mathbb{Z}[t]$. Define the content of nonzero polynomial $g \in \mathbb{Q}[t]$ and show that it is well-defined.

Show that if $g_1, g_2 \in \mathbb{Q}[t]\backslash\{0\}$ then $c(g_1.g_2) = c(g_1).c(g_2)$.

[*You may assume, without proof, that* $c(f.g) = c(f).c(g)$ *for* $f, g \in \mathbb{Z}[t]$.]

$b)$ [8 marks] Let

$$\tilde{P} = \{\frac{1}{n}.f : n \in \mathbb{Z}_{>0}, f \in P\} \subseteq \mathbb{Q}[t].$$

Show that $\tilde{P}$ is an ideal in $\mathbb{Q}[t]$, and that $\tilde{P} \cap \mathbb{Z}[t] = P$.

$c)$ [7 marks] Show that there is a polynomial $f \in \mathbb{Z}[t]$ with content equal to 1 such that $\tilde{P} = \langle f \rangle_{\mathbb{Q}[t]}$. Deduce that $P = \langle f \rangle_{\mathbb{Z}[t]}$ is a principal ideal in $\mathbb{Z}[t]$.

[*You may assume, without proof, that* $\mathbb{Q}[t]$ *is a principal ideal domain. Note also that if* R *is a ring, and* $r \in R$ *then we write* $\langle r \rangle_R$ *for the ideal in* R *generated by* r.]

$iv)$ [4 marks] Give, with proof, an example of a prime ideal in $\mathbb{Z}[t]$ which is not principal.

Solution: Part $a)$ [BW]: If $f \in \mathbb{Z}[t]$, and $f = \sum_{i=0}^{n} a_i t^i$ then we set $c(f) = \text{h.c.f.}\{a_i : 1 \leq i \leq n\}$. It follows that we may write $f = c(f).f_1$ where $f_1 \in \mathbb{Z}[t]$ has $c(f_1) = 1$, and this property uniquely determines $c(f)$ (provided we insist $c(f) > 0$.)

If $f \in \mathbb{Q}[t]$ is nonzero then we define $c(f)$ to be the unique positive $\alpha \in \mathbb{Q}_{>0}$ such that $f = \alpha.f_1$ where $f_1 \in \mathbb{Z}[t]$ has $c(f) = 1$. To see that such an α exists, pick any $N \in \mathbb{Z}_{>0}$ such that $N.f \in \mathbb{Z}[t]$ (take for example the product of the denominators of the coefficients of f) and set $\alpha = c(N.f)/N$ (where $N.f \in \mathbb{Z}[t]$, so that $c(N.f)$ is already well-defined). It is then clear that $\alpha \in \mathbb{Q}_{>0}$ and that $\alpha^{-1}f = Nf/c(Nf)$ has content 1 as required. To see that α is unique, suppose that $f = \alpha_1 f_1 = \alpha_2 f_2$ where $\alpha_1, \alpha_2 \in \mathbb{Q}_{>0}$ and $f_1, f_2 \in \mathbb{Z}[t]$ have $c(f_1) = c(f_2) = 1$. Then for $i = 1, 2$ write $\alpha_i = m_i/n_i$ where $m_i, n_i \in \mathbb{Z}_{>0}$, so we have $(n_2 m_1) f_1 = (n_1 m_2) f_2$. But now by the multiplicativity of the content in $\mathbb{Z}[t]$ (viewing $n_2 m_1, n_1 m_2 \in \mathbb{Z}[t]$ as constant polynomials) we have $c(n_2 m_1).c(f_1) = c(n_1 m_2)c(f_2)$. But if $n \in \mathbb{Z} \subset \mathbb{Z}[t]$, clearly $c(n) = |n|$, and hence $n_2 m_1 = n_1 m_2$, that is, $\alpha_1 = \alpha_2$ as required.

Finally suppose that $f, g \in \mathbb{Q}[t]$ are nonzero polynomials. Picking $N_1, N_2 \in \mathbb{Z}_{>0}$ such that $N_1.f, N_2.g \in \mathbb{Z}[t]$, clearly $N_1 N_2 (f.g) = (N_1.f)(N_2.g) \in \mathbb{Z}[t]$, and so by the above we have

$$c(f.g) = c(N_1 N_2.fg)/N_1 N_2 = c(N_1 f)c(N_2 g)/N_1 N_2 = (c(N_1 f)/N_1).(c(N_2 g)/N_2) = c(f).c(g).$$

Part $b)$ [N – *simple application of definitions and results in course.*]: Clearly $\tilde{P}$ is nonempty, as if $f \in P$ then $f = \frac{1}{1}.f \in \tilde{P}$. To check that $\tilde{P}$ is an ideal, note that if $\frac{1}{n}f, \frac{1}{m}g \in \tilde{P}$ then

$$\frac{1}{n}.f - \frac{1}{m}.g = \frac{1}{n.m}(m.f - n.g) \in \tilde{P},$$

as clearly $m.f - n.g \in P$ since P is an ideal. Thus $\tilde{P}$ is an abelian subgroup of $(\mathbb{Q}[t], +)$. If $\frac{1}{n}f \in \tilde{P}$ and $g \in \mathbb{Q}[t]$, then as above we can write $g = \frac{1}{m}.h$ for some $h \in \mathbb{Z}[t]$, $m \in \mathbb{Z}_{>0}$ and then $g.(\frac{1}{n}.f) = \frac{1}{m.n}(h.f) \in \tilde{P}$ and $h.f \in P$ since P is an ideal in $\mathbb{Z}[t]$.

Now consider $\tilde{P} \cap \mathbb{Z}[t]$. As already noted, $P \subseteq \tilde{P}$ and so certainly $P \subseteq \tilde{P} \cap \mathbb{Z}[t]$. But if $\frac{1}{n}f \in \mathbb{Z}[t]$ where $f \in P$ and $n \in \mathbb{Z}_{>0}$ it follows that $n.(\frac{1}{n}.f) = f \in P$ and so since P is prime either $n \in P$ or $\frac{1}{n}.f \in P$. But $P \cap \mathbb{Z} = \{0\}$ and $n > 0$ so we must have $\frac{1}{n}.f \in P$ and $\tilde{P} \cap \mathbb{Z}[t] = P$ as required.

Part $c)$: [S] Since $\mathbb{Q}[t]$ is a PID, $\tilde{P}$ is principal, so it has a generator g say, and $g = c(g).f$ where $f \in \mathbb{Z}[t]$ has content 1, so (as $c(f)$ is a unit in $\mathbb{Q}[t]$) $\tilde{P}$ has a generator with content 1 as required. We claim P is generated by f: indeed if $g \in P \subseteq \tilde{P}$ we can write $g = h.f$ for some $h \in \mathbb{Q}[t]$, but then $c(h) = c(h).1 = c(h).c(f) = c(g) \in \mathbb{Z}$ so $h \in \mathbb{Z}[t]$. (Note that it follows from the existence and uniqueness of the content in $\mathbb{Q}[t]$ that a nonzero element $f \in \mathbb{Q}[t]$ lies in $\mathbb{Z}[t]$ if and only if $c(f) \in \mathbb{Z}$.) Moreover as $f \in \mathbb{Z}[t] \cap \tilde{P}$ by the previous part it lies in P, so $P = \langle f \rangle$ as required.

Minor variant: Since $P = \tilde{P} \cap \mathbb{Z}[t]$, it is enough to show that $\tilde{P} \cap \mathbb{Z}[t] = \langle f \rangle_{\mathbb{Q}[t]} \cap \mathbb{Z}[t] = \langle f \rangle_{\mathbb{Z}[t]}$. But if $h \in \mathbb{Q}[t]$ is such that $h.f \in \mathbb{Z}[t]$, then taking contents we see $c(h.f) = c(h).c(f) = c(h) \in \mathbb{Z}[t]$ so that $h \in \mathbb{Z}[t]$ and hence $\langle f \rangle_{\mathbb{Q}[t]} \cap \mathbb{Z}[t] \subseteq \langle f \rangle_{\mathbb{Z}[t]}$. Since the reverse inclusion is immediate we are done.

Part d) [S] Consider the ideal $I = \langle 2, t\rangle$. Then I is the kernel of the surjective homomorphism $\mathbb{Z}[t] \to \mathbb{Z}/2\mathbb{Z}$ given by $\sum_{i=0}^{n} a_i t^i \mapsto a_0 \mod 2$, and hence is a maximal (therefore prime) ideal. If it was generated by a single element f, then if $2 = a.f$ for some a implies $\deg(f) = 0$ (since $\mathbb{Z}$ is an integral domain so degrees of polynomials add) and $f = c$ divides 2. But then either $c = \pm 2$ or $c = 1$. In the former case $t \notin \langle \pm 2\rangle$ while in the latter we would have $I = \mathbb{Z}[t]$ both of which give a contradiction.

Note that this is also an example of how a UFD differs from a PID: in any UFD it makes sense to define highest common factors, but Bezout's Lemma fails – in the above example in $\mathbb{Z}[t]$ the highest common factor of 2 and t is 1, but 1 is not a linear combination of 2 and t.

□