Final Honour School of Mathematics Part A

Rings and Modules
Tom Sanders
Checked by: Konstantin Ardakov

26/01/2022

Do not turn this page until you are told that you may do so

1. (a) [15 marks] Let R be a commutative ring.

   (i) Show that if R is an integral domain with the ACCP then R is a factorisation domain.

   (ii) We say that $x \in R$ is *irreducible* if $\langle x \rangle$ is maximal amongst proper principal ideals. State which of the following elements are irreducible in the given rings and briefly justify your answers:

$$3 + 2\sqrt{2} \text{ in } \mathbb{Z}[\sqrt{2}]; \quad 25 \text{ in } \mathbb{Z}_{10}; \quad 2 \text{ in } \mathbb{Z}[\sqrt{-5}].$$

   (iii) Show that if R is a PID then every non-unit in R has an irreducible factor.

   (iv) Show that R is a field if and only if 0 is irreducible.

(b) [10 marks] Let $\overline{\mathbb{Z}}$ be the set of $\alpha \in \mathbb{C}$ for which there is a monic polynomial $p \in \mathbb{Z}[X]$ such that $p(\alpha) = 0$.

   (i) Show that $\alpha \in \overline{\mathbb{Z}}$ if and only if the $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ is finitely generated.

   (ii) Hence show that $\overline{\mathbb{Z}}$ is a subring of $\mathbb{C}$.
   [*Hint: you may assume that a submodule of a finitely generated module over a PID is also finitely generated.*]

   (iii) Show that $\overline{\mathbb{Z}}$ does not contain any irreducible elements.

[5 marks] B (a) (i) Write $\mathcal{F}$ for the set of elements in R^* that have factorisation into irreducibles so that all units and irreducible elements are in $\mathcal{F}$. $\mathcal{F}$ is closed under multiplication, by design and since R is an integral domain.
Were $\mathcal{F}$ not to be the whole of R^* then there would be some $x_0 \in R^* \setminus \mathcal{F}$. Now create a chain iteratively: at step i suppose we have $x_i \in R^* \setminus \mathcal{F}$. Since x_i is not irreducible and not a unit there is $y_i|x_i$ with $y_i \not\sim 1$ and $y_i \not\sim x_i$; let $z_i \in R^*$ be such that $x_i = y_i z_i$. If $z_i \sim x_i$, then $z_i \sim y_i z_i$ and by cancellation $1 \sim y_i$, a contradiction. We conclude $y_i, z_i \not\sim x_i$.
Since $\mathcal{F}$ is closed under multiplication we cannot have both y_i and z_i in $\mathcal{F}$. Let $x_{i+1} \in \{y_i, z_i\}$ such that $x_{i+1} \notin \mathcal{F}$; by design $x_{i+1}|x_i$ and $x_{i+1} \not\sim x_i$. This process produces a sequence $\dots|x_2|x_1|x_0$ in which $x_i \not\sim x_{i+1}$ for all $i \in \mathbb{N}_0$ contradicting the ACCP.

[4 marks] B (ii) $3+2\sqrt{2}$ has $3-2\sqrt{2}$ as a multiplicative inverse so is a unit in $\mathbb{Z}[\sqrt{2}]$ and hence not irreducible. $25 \equiv 5 \pmod{10}$ and $\langle 5\rangle$ is maximal amongst principal ideals in $\mathbb{Z}_{10}$ and so irreducible. 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, since if $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then $4 = (a^2+5b^2)(c^2+5d^2)$ and so $b = d = 0$, and hence $a = \pm 1$ or $c = \pm 1$.

[3 marks] S (iii) (In the notes we prove that a PID has the ACCP so they may choose to reproduce that and then apply the first part.) Let $x \in R \setminus U(R)$. Then $\langle x\rangle$ is proper and so by Krull's Theorem it is contained in a maximal ideal I. Since R is a PID $I = \langle d\rangle$, and in particular $\langle d\rangle$ is maximal amongst proper principal ideals so d is irreducible, and since $x \in I = \langle d\rangle$ we have $d|x$ as required.

[3 marks] S (iv) If R is a field then the only ideals are $\{0\}$ and R and so $\{0\}$ is maximal amongst principal ideals, and hence 0 is irreducible. On the other hand if $\{0\}$ is maximal amongst principal ideals and $x \in R^*$ then $\{0\} \subsetneq \langle x\rangle$ and so by maximality $\langle x\rangle = R$. Since R is commutative there must be $y \in R$ such that $xy = 1$, and again since R is commutative it is a field.

[4 marks] N (b) (i) For the first part, 'only if' follows since $1, \alpha, \alpha^2, \dots$ generate $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$-module, but the degree d, say, monic p of which α is a root gives an inductive way of writing α^i as a $\mathbb{Z}$-linear combination of $1, \alpha, \dots, \alpha^{d-1}$ for $i \geqslant d$. For 'if', suppose that $p_1, \dots, p_k \in \mathbb{Z}[\alpha]$ generate $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$-module. Then α^d is a $\mathbb{Z}$-linear combination of $p_1, \dots, p_k$ for all $d \in \mathbb{N}_0$ and in particular for some $d > \max\{\deg p_1, \dots, \deg p_k\}$. This gives a monic satisfied by α as required.

[3 marks] N (ii) Suppose that $\alpha, \beta \in \overline{\mathbb{Z}}$. Then there are generators $p_1, \dots, p_k \in \mathbb{Z}[\alpha]$ and $q_1, \dots, q_m \in \mathbb{Z}[\beta]$. But $\mathbb{Z}[\alpha+\beta]$ and $\mathbb{Z}[\alpha\beta]$ are both contained in the $\mathbb{Z}$-module generated by $\alpha^i\beta^j$ for $i, j \in \mathbb{N}_0$, which in turn is generated by the finite set $\{p_i q_j : 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant m\}$. Hence $\mathbb{Z}[\alpha+\beta]$ and $\mathbb{Z}[\alpha\beta]$ are submodules of a finitely generated $\mathbb{Z}$-module, and so themselves finitely generated. Finally, $\mathbb{Z}[\alpha] = \mathbb{Z}[-\alpha]$ and 1 is a root of $X-1$ and so $\overline{\mathbb{Z}}$ is a ring by the subring test.

[3 marks] N (iii) If $\alpha \in \overline{\mathbb{Z}}$ then then α is a root of some monic p and so $\sqrt{\alpha}$ is the root

of the monic $p(X^2)$. Suppose that $\alpha \in \overline{\mathbb{Z}}$ is irreducible. Then $\alpha \not\sim 1$, but since $\alpha = \sqrt{\alpha} \times \sqrt{\alpha}$ we have $\sqrt{\alpha} \sim 1$ or $\sqrt{\alpha} \sim \alpha$. If $\sqrt{\alpha} \sim 1$ then $\alpha \sim 1$, a contradiction; therefore $\sqrt{\alpha} \sim \alpha$. If $\sqrt{\alpha} \neq 0$ then $\sqrt{\alpha} \sim 1$ again a contradiction, so $\sqrt{\alpha} = 0$ and hence $\alpha = 0$. By a iv we conclude that $\overline{\mathbb{Z}}$ is a field. However, 2 does not have an inverse in $\overline{\mathbb{Z}}$ since if $2\alpha = 1$ and $p \in \mathbb{Z}[X]$ is a monic then $2^d p(\alpha) = (2\alpha)^d + 2q(2\alpha)$ for some $q \in \mathbb{Z}[X]$, so $p(\alpha) \neq 0$. Hence $\overline{\mathbb{Z}}$ is not a field and it has no irreducible elements.

2. (a) [7 marks] Show that if R is an integral domain with non-zero characteristic p then p is prime and R is a vector space over $\mathbb{F}_p$ in such a way that multiplication on R is bilinear.

(b) [4 marks] Show that if p is a prime and R is a ring of order p^2 then either $R \cong \mathbb{Z}_{p^2}$ or there is a polynomial $q \in \mathbb{F}_p[X]$ such that $R \cong \mathbb{F}_p[X]/\langle q \rangle$.

(c) [6 marks] Let $p \equiv 3 \pmod 4$ be prime.

(i) Show that if $d \in \mathbb{F}_p$ is not a square then $d = -x^2$ for some $x \in \mathbb{F}_p^*$.

(ii) Show that if $q \in \mathbb{F}_p[X]$ is a degree 2 irreducible polynomial then

$$\mathbb{F}_p[X]/\langle q \rangle \cong \mathbb{F}_p[X]/\langle X^2 + 1 \rangle.$$

(d) [8 marks]

(i) Show that if R is a Euclidean domain then there is a prime $p \in R$ such that if $q : R \to R/\langle p \rangle$ is the quotient map then $U(q(R)) = q(U(R))$. [*Hint: consider the minimal values of the Euclidean function.*]

(ii) Show that $A := \mathbb{R}[X, Y]/\langle X^2 + Y^2 + 1 \rangle$ is not a Euclidean domain. [*You may assume that $U(A) = \mathbb{R}^*$, and also that the $\mathbb{R}$-vector space $A/\langle p \rangle$ is finite-dimensional for any non-zero prime $p \in A$.*]

[7 marks] B

(a) Let $\chi_R : \mathbb{Z} \to R$ be the unique homomorphism from the integers, and suppose that R has characteristic p. If $p = ab$ for $a, b \geqslant 1$ then $0_R = \chi_R(p) = \chi_R(a)\chi_R(b)$, and since R is an integral domain we conclude that $\chi_R(a) = 0$ or $\chi_R(b) = 0$; say the former. Then by definition $a \geqslant p$ and so $a = p$ and $b = 1$. We conclude that p is prime.

The kernel of χ_R contains p and is an ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID it has the form $\langle N \rangle$ for some $N \in \mathbb{N}_0$, but then $N|p$, whence $N = 1$ or $N = p$. If $N = 1$ then $1_R = \chi_R(1) = \chi_R(0) = 0_R$ contradicting the non-triviality of R. We conclude that $N = p$ and the ring $\mathbb{Z}/\langle p \rangle$ is the field $\mathbb{F}_p$ which is a field. By the First Isomorphism Theorem there is then an injective ring homomorphism $\mathbb{F}_p \to R$ which induces an $\mathbb{F}_p$-vector space structure on the additive group of R in such a way that right multiplication is $\mathbb{F}$-linear. Since multiplication is commutative, it is $\mathbb{F}$-bilinear.

[4 marks] S

(b) The additive order of 1 must divide p^2. It cannot be 1 since the ring is not trivial. If it is p^2 then $R \cong \mathbb{Z}_{p^2}$. The characteristic p case is what remains. In this case R is a vector space over $\mathbb{F}_p$, and for reasons of size must have a basis of size 2. Take $1 \in R$ which is non-zero and extend this to an $\mathbb{F}_p$-basis by some element x. Let $a, b \in \mathbb{F}_p$ be such that $x^2 = ax + b$, then the map $\mathbb{F}_p[X] \to R; f \mapsto f(x)$ is a surjective ring homomorphism. The kernel contains $\langle X^2 - aX - b \rangle$, and since $\mathbb{F}_p[X]/\langle X^2 - aX - b \rangle$ is 2-dimensional over $\mathbb{F}_p$, R is 2-dimensional, and the given homomorphism is $\mathbb{F}_p$-linear.

[3 marks] N

(c) (i) The map $\mathbb{F}_p^* \to \mathbb{F}_p^*; x \mapsto x^2$ is a homomorphism of the multiplicative group, and its image has index at most 2 since degree 2 polynomials over an integral domain have at most 2 roots, and at least 2 since -1 is not a square modulo p for congruence reasons. Since cosets partition a group, if Q are the quadratic residues in $\mathbb{F}_p^*$ then $-Q$ is the set of non-residues as required.

[3 marks] S

(ii) Since q is a quadratic there are $a, b, c \in \mathbb{F}_p$ with $a \neq 0$ such that $q(X) = aX^2 + bX + c$ by completing the square (since p is odd) $q(X) = a((X - b/2a)^2 + \Delta)$ for $\Delta = c - b^2/4a^2$. Since q is irreducible it has no root so $-\Delta$ is not a square, so by c(i) we have $\Delta = d^2$ for $d \neq 0$. Hence $q(X) = ad^2((X/d - b/2ad)^2 + 1)$. Dilating ideals by a unit does not change them so the map $\mathbb{F}_p[X]/\langle q \rangle \to \mathbb{F}_p[X]/\langle X^2 + 1 \rangle f \mapsto f(dX + b/2ad)$ is an isomorphism.

[5 marks] N

(d) (i) Let f be a Euclidean function on R and $p \in R$ have $f(p)$ minimal over all nonzero non-units. Then if $x \in R^* \setminus U(R)$, then either $p|x$ or there is $r \in R^*$ with $x = bp + r$ and $f(r) < f(p)$. By minimality of $f(p)$ we have $r \in U(R)$ and hence $x + \langle p \rangle \in U(q(R))$. It follows that $U(q(R)) \cap q(R^* \setminus U(R))) \subset q(U(R))$, and hence $U(q(R)) \subset q(U(R))$. Units remain units under quotienting which is the other direction.

Finally, p is prime, because it is not a unit, and if $p|xy$ and $p \not| x$ then by the above $p|(bp + r)y$ for $r \in U(R)$, but then $p|ry|y$ as required.

[3 marks] N

(ii) Let p be as in d(i). Then $A/\langle p\rangle$ contains elements x, y with $x^2+y^2+1=0$. It is also an integral domain that is finite dimensional over $\mathbb{R}$ and so $A/\langle p\rangle$ is a field and hence $A/\langle p\rangle = U(A/\langle p\rangle)\cup\{0\} = \mathbb{R}^*\cup\{0\} = \mathbb{R}$, but there are no $X, Y \in \mathbb{R}$ with $X^2+Y^2+1=0$.

3. (a) [15 marks]

(i) Show that if R is a Euclidean domain then every $A \in M_{n,m}(R)$ is equivalent by elementary operations to a diagonal matrix.

(ii) Show that if R is a commutative ring and $A, B \in M_{n,m}(R)$ are both in Smith Normal Form with A equivalent to B then $A_{i,i}$ is an associate of $B_{i,i}$ for all i. State clearly any results you use.

(iii) Show that if $R = M_2(\mathbb{F})$ for a field $\mathbb{F}$ and $R^n \cong R^m$ as R-modules then $n = m$.

(b) [10 marks] Let U, V and W be vector spaces over $\mathbb{F}$ and let $R := \mathrm{End}_{\mathbb{F}}(V)$.

(i) Show that the map $R \times L(U,V) \to L(U,V)$ which sends (ϕ, ψ) to $\phi \circ \psi$ is well-defined and gives the commutative group $L(U,V)$ of $\mathbb{F}$-linear maps $U \to V$ the structure of an R-module.

(ii) Write down an R-linear isomorphism $\alpha : L(U,V) \oplus L(W,V) \to L(U \oplus W, V)$.

(iii) Show that if $V = \mathbb{F}[X]$ considered as an $\mathbb{F}$-vector space, then V is $\mathbb{F}$-linearly isomorphic to $V \oplus V$.

(iv) Deduce that $R \cong R^2$ as R-modules.

[8 marks] B (a) (i) Let $\mathcal{A}_k$ be those matrices $B \sim_{\mathcal{E}} A$ with the additional property that whenever $i < k$ and $j \neq i$, or $j < k$ and $i \neq j$, we have $B_{i,j} = 0$. We shall show by induction that $\mathcal{A}_k$ is non-empty for $k \leqslant \min\{m,n\}$; $\mathcal{A}_1$ contains A and so is certainly non-empty.

Let f be a Euclidean function for R, and suppose that $\mathcal{A}_k \neq \emptyset$ and $k < \min\{m,n\}$. Let $B \in \mathcal{A}_k$ be a matrix with $f(B_{k,k})$ minimal. First we show that $B_{k,k}|B_{k,i}$ for all $i > k$: if not, there is some $i > k$ with $B_{k,i} = qB_{k,k} + r$ with $f(r) < f(B_{k,k})$ and we apply the elementary operations $c_i \mapsto c_i - c_k q$ and $c_k \leftrightarrow c_i$ to get a matrix $B' \in \mathcal{A}_k$ with $B'_{k,k} = B_{k,i} - qB_{k,k} = r$, but $f(B'_{k,k}) = f(r) < f(B_{k,k})$ which contradicts the minimality in our choice of B. Similarly, but with row operations in place of column operations, $B_{k,k}|B_{i,k}$ for all $i > k$.

For $k < i \leqslant m$ let q_i be such that $B_{k,i} = B_{k,k}q_i$. Apply elementary column operations $c_{k+1} \mapsto c_{k+1} - c_k q_{k+1}, \dots, c_m \mapsto c_m - c_k q_m$ to get a matrix B'. For $k < i \leqslant n$ let p_i be such that $B_{i,k} = p_i B_{k,k}$. Apply elementary row operations $r_{k+1} \mapsto r_{k+1} - p_{k+1} r_k, \dots, r_n \mapsto r_n - p_n r_k$ to B' to get a matrix B''. Then $B'' \sim_{\mathcal{E}} B' \sim_{\mathcal{E}} B \sim_{\mathcal{E}} A$ and $B'' \in \mathcal{A}_{k+1}$. The inductive step is complete. It follows that $\mathcal{A}_{\min\{m,n\}} \neq \emptyset$; any B in this set is diagonal and equivalent to A.

[4 marks] S (ii) This is on problem sheet 4. I am expecting them to quote the uniqueness theorem and the fact that equivalent matrices produce isomorphic presentations, so $R^m/\operatorname{Im} L_A \cong R^m/\operatorname{Im} L_B$, and since both A and B are diagonal with, say, entries $a_1, \dots, a_k$ and $b_1, \dots, b_k$ (where $k = \min\{n,m\}$) we have $\operatorname{Im} L_A = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle \times \{0\} \times \cdots \times \{0\}$ where there are $m - k$ copies of $\{0\}$. Moreover, $a_1|a_2|\cdots|a_k$ so $\langle a_1 \rangle \supset \cdots \supset \langle a_k \rangle \supset \langle 0 \rangle \supset \cdots \supset \langle 0 \rangle$. Similarly for $\operatorname{Im} L_B$, and it follows by the uniqueness theorem that $a_i \sim b_i$ for all i as required.

[3 marks] S (iii) If $R = M_2(\mathbb{F})$ then R is $\mathbb{F}$-linearly isomorphic to $\mathbb{F}^4$, and if R^n is R-linearly isomorphic to R^m then the underlying $\mathbb{F}$-vector spaces are $\mathbb{F}$-linearly isomorphic, and so $\mathbb{F}^{4n}$ is $\mathbb{F}$-linearly isomorphic to $\mathbb{F}^{4m}$ and hence $4n = 4m$ and so $n = m$.

[3 marks] S (b) (i) The map is well-defined because the composition of linear maps is linear. The multiplicative identity in $\operatorname{End}_{\mathbb{F}}(V)$ is the identity function and so $1_R.\psi = \psi$; $\phi \in \operatorname{End}_{\mathbb{F}}(V)$ is additive and so $(\phi.(\psi + \pi))(x) = \phi(\psi(x) + \pi(x)) = \phi(\psi(x)) + \phi(\pi(x)) = (\phi.\psi)(x) + (\phi.\pi)(x)$ for all $x \in V$; $((\phi + \phi').\psi)(x) = (\phi + \phi')(\psi(x)) = \phi(\psi(x)) + \phi'(\psi(x)) = (\phi.\psi)(x) + (\phi'.\psi)(x)$ for all $x \in V$; and finally $(\phi \circ \phi').\psi = (\phi \circ \phi') \circ \psi = \phi \circ (\phi' \circ \psi) = \phi.(\phi'.\psi)$ since functional composition is associative.

[2 marks] S (ii) In the first case, the map $\alpha : L(U,V) \oplus L(W,V) \to L(U \oplus W, V); (\phi, \psi) \mapsto (u + w \mapsto \phi(u) + \psi(w))$ is a well-defined R-linear isomorphism.

[2 marks] N (iii) The map $\beta : \mathbb{F}[X] \oplus \mathbb{F}[X] \to \mathbb{F}[X]; p \mapsto p(X^2) + q(X^2)X$ is an $\mathbb{F}$-linear bijection.

[3 marks] N (iv) Let $U = W = V$ in the isomorphism α and note that the map $R \to R^2; \phi \mapsto$

$\alpha^{-1}(\phi \circ \beta)$ is well-defined and an R-linear bijection and the claim is proved.