A3: Rings and Modules

Sheet III — HT21

III.1. Consider the commutative group $\mathbb{C}$ as a vector space over the field $\mathbb{C}$ with the scalar multiplications $\mathbb{C}\times\mathbb{C}\to\mathbb{C}; (z,w)\mapsto zw$ and $\mathbb{C}\times\mathbb{C}\to\mathbb{C}; (z,w)\mapsto \overline{z}w$; are these two vector spaces isomorphic?

Suppose that R is a commutative ring and $\pi : R \to R$ is a non-injective ring homomorphism. Show that $R\times R\to R; (r,x)\mapsto \pi(r)x$ is a scalar multiplication giving R the structure of an R-module. Is this module isomorphic to the R-module on R given by the scalar multiplication $R\times R\to R; (r,x)\mapsto rx$?

III.2. Suppose that R is an integral domain and not a field. Give, with proof, an example of a proper submodule of R that is linearly isomorphic to R.

III.3. Suppose that $\mathbb{F}$ is a field. Show that the $\mathbb{F}[X]$-modules $\mathbb{F}[X]/\langle p\rangle$ and $\mathbb{F}[X]/\langle q\rangle$ are $\mathbb{F}[X]$-linearly isomorphic if and only if $p\sim q$.

Suppose that $A\in M_n(\mathbb{F})$ has minimal polynomial $m\in\mathbb{F}[X]$. Show that $\mathbb{F}[A]\cong\mathbb{F}[X]/\langle m\rangle$ as $\mathbb{F}[X]$-modules, and that if m is not equal to the characteristic polynomial of A then $\mathbb{F}[A]$ is *not* isomorphic to the endomorphism $\mathbb{F}[X]$-module $\mathbb{F}^n$ induced by the linear map $\mathbb{F}^n\to\mathbb{F}^n; v\mapsto vA$.

III.4. Suppose that $\phi : N\to M$ is a surjective R-linear map. Show that if N is finitely generated then so is M; and on the other hand if M and $\ker\phi$ are finitely generated then N is finitely generated.

III.5. In this question we view $\mathbb{Q}$ as a $\mathbb{Z}$-module. Does $\mathbb{Q}$ have a generating set? Does $\mathbb{Q}$ have a finite generating set? Does $\mathbb{Q}$ have a minimal generating set, meaning a (possibly infinite) generating set S such that no proper subset of S generates $\mathbb{Q}$?

III.6. Let $R := \{p\in\mathbb{Q}[X] : p(0)\in\mathbb{Z}\}$ and $I := \{p\in R : p(0)=0\}$. Explain briefly why R is a ring and I is an ideal in R. Show that I is *not* finitely generated as an R-module.

III.7. Suppose that $p\in\mathrm{Int}(\mathbb{Z})$ is such that for all $z\in\mathbb{Z}$, either 2 divides $p(z)$ or 3 divides $p(z)$. Show that the quantifiers may be reversed *i.e.* that either for all $z\in\mathbb{Z}$ we have 2 divides $p(z)$, or for all $z\in\mathbb{Z}$ we have 3 divides $p(z)$.

III.8. Let R be the ring $\mathbb{Z}[\sqrt{-5}]$ and I be the ideal $\langle 2, 1+\sqrt{-5}\rangle$ in R. Show that I^2 is R-module isomorphic to R^2. Is there some $n\in\mathbb{N}_0$ such that I is R-module isomorphic to R^n?

Mathematical Institute, University of Oxford
Tom Sanders: tom.sanders@maths.ox.ac.uk

III.9. [Optional] The aim of the question is to give an example of a ring which is a PID but not a Euclidean Domain. Let $A := \mathbb{R}[X][Y]/\langle Y^2 + X^2 + 1\rangle$, which has the structure of an $\mathbb{R}[X]$-module such that multiplication in A is $\mathbb{R}[X]$-bilinear, and write $\tilde{Y}$ for the image of Y under the quotient map $\mathbb{R}[X][Y] \to A$.

(a) Show that $\{1, \tilde{Y}\}$ is a basis for A as an $\mathbb{R}[X]$-module and that the map

$$A \to A; f = p.1 + q.\tilde{Y} \mapsto \overline{f} := p.1 - q.\tilde{Y}$$

is an $\mathbb{R}[X]$-linear ring isomorphism. Hence show that A is an integral domain and $U_0 := U(A) \cup \{0\}$ is a subring of A which is isomorphic to $\mathbb{R}$. Show also that there is no ring homomorphism $A \to \mathbb{R}$.

If $f = p.1 + q.\tilde{Y} \in A$ then we write $|f|^2 := p^2 + q^2(X^2 + 1) \in \mathbb{R}[X]$ and a calculation shows that $f\overline{f} = |f|^2.1$. Furthermore, since $\mathbb{R}$ is a subring of $\mathbb{R}[X]$, A also has the structure of an $\mathbb{R}$-vector space such that multiplication in A is $\mathbb{R}$-bilinear.

(b) Show that if $g \in \mathbb{R}[X]^*$ has degree d then $A/\langle g.1\rangle$ is $2d$-dimensional as an $\mathbb{R}$-vector space. Given this, for $f \in A^*$ show by considering the map $A/\langle f\overline{f}\rangle \to A/\langle f\rangle; g + \langle f\overline{f}\rangle \mapsto g + \langle f\rangle$ or otherwise that $A/\langle f\rangle$ is $\deg |f|^2$-dimensional as an $\mathbb{R}$-vector space.

(c) Show that if I is a maximal ideal in A then there are elements $\alpha, \beta, \gamma \in \mathbb{R}$ such that $I = \langle(\alpha + \beta X).1 + \gamma.\tilde{Y}\rangle$, and hence use Exercise II.6 to show that A is a PID.

[*Hint: You may assume that any finite degree field extension of* $\mathbb{R}$ *has degree at most* 2 *for the first part. It is in fact enough for our purposes to show that the maximal ideals in* A *are principal and this can be achieved without this assumption by slightly more work.*]

(d) Show that A is *not* a Euclidean domain.

Tom Sanders: tom.sanders@maths.ox.ac.uk