A3: RINGS AND MODULES, EXAMPLES SHEET 1

TOM SANDERS

Feedback to tom.sanders@maths.ox.ac.uk. My thanks to Richard Earl for many of the problems.

1. Show that $2\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic as (additive) groups, but that the only ring homomorphism $2\mathbb{Z} \to 3\mathbb{Z}$ is the zero map.

2. Write $C(\mathbb{R})$ for the set of continuous functions $\mathbb{R} \to \mathbb{R}$ and $L(\mathbb{R})$ for the set of linear maps $\mathbb{R} \to \mathbb{R}$ *i.e.* the maps of the form $x \mapsto ax$.

- (i) Show that $C(\mathbb{R})$ is a ring when endowed with addition defined by pointwise addition and multiplication defined by pointwise multiplication. Is $L(\mathbb{R})$ a subring of $C(\mathbb{R})$ with these operations?
- (ii) $C(\mathbb{R})$ with operations as in (i) is actually a unital ring – what is the multiplicative identity? What is the subring of $C(\mathbb{R})$ generated by the map $\iota : \mathbb{R} \to \mathbb{R}; x \mapsto x$? What is the unital subring generated by the map ι?
- (iii) What are the zero-divisors of $C(\mathbb{R})$ with operations as in (i)?
- (iv) Is $C(\mathbb{R})$ a ring when endowed with addition defined by pointwise addition and multiplication defined by functional composition? Is $L(\mathbb{R})$ a ring with these operations?

3. Suppose that

$$A := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \text{ and } C := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Show that $\mathbb{R}[A, B] = \mathbb{R}[A, C] = \mathbb{R}[B, C]$; denote this ring $\mathbb{H}$. It is called the ring of quaternions. Show that $\{I, A, B, C\}$ is a basis for $\mathbb{H}$ as a real vector space. Show that the only zero divisor in $\mathbb{H}$ is the zero matrix.

[Hint: it may help to consider $(\delta I - \alpha A - \beta B - \gamma C)(\delta I + \alpha A + \beta B + \gamma C)$*.]*

4. Show that if A is a 2×2 matrix with real coefficients then $\mathbb{R}[A]$ is isomorphic to one of $\mathbb{R}$, $\mathbb{R} \times \mathbb{R}$, $\mathbb{R}[X]/\langle X^2 \rangle$, or $\mathbb{C}$.

5. Show that there is no surjective unital ring homomorphism $\phi : \mathbb{Z}[X] \to \mathbb{Q}$ *i.e.* that $\mathbb{Q}$ does *not* arise as a unital quotient of $\mathbb{Z}[X]$. Does it arise as a not-necessarily-unital

Last updated: 4^{th} February, 2020.

quotient?

[Hint: it may help to consider a prime not in the denominator of the image of X.]

6. The aim of this question is to identify the group structure of $\mathbb{Z}[\sqrt{2}]$.

(i) Show that if $a + b\sqrt{2}$ is a unit then[1] $2b^2 - a^2 \in \{-1, 1\}$.
(ii) Show that $1 + \sqrt{2}$ is the smallest unit bigger than 1.
(iii) Show that the map $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}) \to U(\mathbb{Z}[\sqrt{2}]); (n, v) \mapsto (-1)^v(\sqrt{2} + 1)^n$ is a well-defined isomorphism of groups.

7. Show that the set of polynomials in $\mathbb{C}[X]$ mapping the integers to the integers is a subring of $\mathbb{Q}[X]$. Is it a subring of $\mathbb{Z}[X]$?

Suppose that p is a polynomial mapping integers to integers 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 $p(z)$.

Mathematical Institute, University of Oxford, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom

Email address: tom.sanders@maths.ox.ac.uk

[1]The equation $x^2 - 2y^2 = 1$ is an instance of something called Pell's equation.