RINGS AND MODULES HT19 – SHEET THREE

UFDs. Gauss's Lemma and Eisenstein's Criterion. Introduction to Modules.

1. (i) Let $K\colon F$ be a field extension of finite degree. Show that every element of K is algebraic over F.
(ii) Let $\mathbb{A}$ denote the set of elements in $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Show $\mathbb{A}$ is a subfield of $\mathbb{C}$. [Use the tower law.]
(iii) Show that $\mathbb{A}$ is the union of all the subfields L of $\mathbb{C}$ which are finite degree extensions of $\mathbb{Q}$.
(iv) By considering roots of the equation $x^n = 2$ for $n \geqslant 1$, or otherwise, prove that $\mathbb{A}\colon \mathbb{Q}$ does not have finite degree.

2. In each of the following UFDs, factorize the given elements into irreducible elements.
(i) $36x^3 - 24x^2 - 18x + 12$ in $\mathbb{Z}[x]$.
(ii) $x^6 - 1$ in $\mathbb{Z}_7[x]$.
(iii) $32 + 9i$ in $\mathbb{Z}[i]$.
(iv) $x^3 + y^3$ in $\mathbb{Q}[x, y]$.
(v) $2\pi^2 + 3\pi + 1$ in $\mathbb{Q}[\pi]$.

3. Investigate the irreducibility of the following polynomials over $\mathbb{Q}$.

(i) $x^3 - 3$, (ii) $x^{17} + 7x^{11} + 14x^2 + 21$, (iii) $x^4 + 4x^3 + 12x^2 + 16x + 15$, (iv) $x^6 + x^3 + 1$.

4. A *Bézout domain* is an integral domain in which the sum of two principal ideals is principal.
(i) Give an example of a UFD which is not a Bézout domain.
(ii) Show that a Bézout domain which is a UFD is a PID.
(iii) Show that the ring of holomorphic functions on $\mathbb{C}$ is not a UFD.
(iv) [Optional and harder] Show that the ring of holomorphic functions on $\mathbb{C}$ is a Bézout domain. [You may assume that, given a sequence (z_n) of complex numbers with no limit point and a specification of the Taylor coefficients at z_n up to some finite degree, there is a holomorphic function f on $\mathbb{C}$ with, for each z_n, the specified Taylor coefficients and no further zeros than already specified.]

5. (i) Given a ring R, thought of as an R-module, what are the submodules of R? Justify your answer.
(ii) Show that $\mathbb{Q}$, as a module over $\mathbb{Z}$, is not finitely-generated (i.e. is not generated by any finite set).
(iii) Show that $M_1 = \mathbb{R}[x]/\langle x\rangle$ and $M_2 = \mathbb{R}[x]/\langle x-1\rangle$ are isomorphic as rings but are not isomorphic as $\mathbb{R}[x]$-modules.

6. (i) Show that the set $\{6, 10, 15\}$ generates $\mathbb{Z}$ as a $\mathbb{Z}$-module, but that no proper subset of $\{6, 10, 15\}$ generates $\mathbb{Z}$.

(ii) For what values of a in the Gaussian integers $\mathbb{Z}[i]$ do $(2, 1)$ and $(2 + i, a)$ form a basis for $\mathbb{Z}[i]^2$?

7. Let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

(i) Show that $\mathbb{R}[A]$ and $\mathbb{R}[B]$ are isomorphic as $\mathbb{R}[x]$-modules. What is the dimension of $\mathbb{R}[A]$ as a real vector space?
(ii) Given a vector space over F and a linear map $T\colon V \to V$, explain how T defines V as a $F[x]$-module.
(iii) Given a $F[x]$-module V, explain why V is a vector space over F and show that there is a linear map $T\colon V \to V$ defining V as a $F[x]$-module.
(iv) With $V = \mathbb{R}^3$, let M and N respectively denote the $\mathbb{R}[x]$-modules defined by A and B. Are M and N isomorphic as $\mathbb{R}[x]$-modules?
(v) What are submodules of M?

8. Consider the quotient $\mathbb{Z}$-module

$$M = \frac{\mathbb{Z}^3}{\langle (3, 3, 1), (2, 2, 2)\rangle}.$$

(i) Is M free?
(ii) Show that $\langle (3, 3, 1), (2, 2, 2)\rangle = \langle (1, 1, -1), (0, 0, 4)\rangle$.
(iii) Find an element of infinite order in M. Justify your answer.
(iv) Find a non-zero element of finite order in M. Justify your answer.
(v) Show that M is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}_4$.

9. (Optional) (i) Let A be an abelian group. Show that the endomorphisms of A (the homomorphisms $A \to A$) form a ring with an identity under addition and composition.
(ii) Let M be an R-module. Show how this induces a ring homomorphism $\rho\colon R \to \mathrm{End}(M)$ such that $\rho(1_R) = id$.
(iii) Show, conversely, given an abelian group M and a ring homomorphism $\rho\colon R \to \mathrm{End}(M)$ with $\rho(1_R) = id$, how to give M the structure of an R-module.