RINGS AND MODULES HT19 – SHEET TWO

Ideals in R and R/I. Prime and maximal ideals. Euclidean Domains. PIDs. Field extensions. Tower law.

1. Let I, J, K be ideals in a ring R. Show that

$$I(JK) = (IJ)K \qquad \text{and} \qquad I(J+K) = IJ + IK.$$

2. Let R be a commutative ring with unity. Define the terms *irreducible element* and *prime element*.

(i) Show that in an integral domain every prime element is irreducible.

(ii) Prove that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

(iii) Describe the irreducible elements of the following rings:
(a) the ring $\mathbb{C}[x]$ of polynomials in x with coefficients in $\mathbb{C}$.
(b) the ring $\mathbb{R}[x]$ of polynomials in x with coefficients in $\mathbb{R}$.
(c) the ring of all numbers of the form $2^a b$ where a and b are integers (with the usual addition and multiplication).
(d) the ring of holomorphic functions on $\mathbb{C}$.

(iv) Show that the polynomial $x^3 - 3$ is irreducible over $\mathbb{Z}_7$ but factorises into linear factors over $\mathbb{Z}_7[y]/\langle y^3 - 3\rangle$.

3. For each of the following rings and ideals, say whether the ideal is principal, prime, maximal. In each case determine the quotient ring R/I and justify your answers.

(i) $R = \mathbb{Z}[x]$ and $I = \langle x \rangle$.
(ii) $R = \mathbb{Q}[x]$ and $I = \langle x^2 - 4, x^3 - 8\rangle$.
(iii) $R = \mathbb{C}[x]$ and $I = \langle x^2 + 1\rangle$,
(iv) $R = \mathbb{Z}^2$ and $I = \{(a, b) : a \in 2\mathbb{Z} \text{ and } b \in 3\mathbb{Z}\}$.

4. Suppose that R is an integral domain containing a field K. Then we may view R as a K-vector space. Show that if R is finite dimensional as a K-vector space then it must be a field. Deduce that if I is a prime ideal in $K[x, y]$ of finite codimension (i.e. such that the quotient $K[x, y]/I$ is finite dimensional) then I is maximal. Is every ideal in $K[x, y]$ of finite codimension necessarily prime?

5. Let R be a principal ideal domain. Prove directly (that is without using the theory of unique factorization) that
(i) R is Noetherian: if $I_1, I_2, I_3, \ldots$ are ideals of R such that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ then there is an N such that $I_n = I_N$ for all $n \geqslant N$.
(ii) R is a Bézout domain: any two elements x, y of R have a highest common factor h such that $ux + vy = h$ for some $u, v \in R$.

6. Let $p = 4n+1$ be a prime in $\mathbb{Z}$. Prove that $(p-1)! \equiv -1 \bmod p$ and that $((2n)!)^2 \equiv (4n)! \bmod p$. Hence show that

$$((2n)! - i)((2n)! + i) \in p\mathbb{Z}[i],$$

and that p is not prime in $\mathbb{Z}[i]$.

Deduce that p is the sum of two squares in $\mathbb{Z}$.

Can a prime of the form $4n + 3$ be expressed as the sum of two squares?

7. (i) Determine the minimal polynomials of the following $\alpha \in \mathbb{C}$ each of which is algebraic over $\mathbb{Q}$.

$$i\sqrt{3}, \qquad \sqrt[4]{2}, \qquad \frac{1}{2}\left(-1 + i\sqrt{3}\right), \qquad 2\cos(2\pi/5), \qquad e^{2\pi i/5}.$$

(ii) Determine the degrees of each of the following field extensions.

$$\left|\mathbb{Q}(\sqrt{6}) : \mathbb{Q}\right|, \qquad \left|\mathbb{Q}(e^{\pi i/4}) : \mathbb{Q}\right|, \qquad \left|\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}\right|, \qquad \left|\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q}\right|.$$

8. (Optional) Use the Euclidean algorithm to find the hcf h of $z_1 = 109 + 3i$ and $z_2 = 15 + 70i$ in $\mathbb{Z}[i]$.

Determine $u, v \in \mathbb{Z}[i]$ such that $h = uz_1 + vz_2$.

9. (Optional) Give an example of an irreducible quadratic over $\mathbb{Z}_3$. Hence, give an example of the finite field F_9 of order 9. Find all the generators for F_9^* justifying your answers.

Given $\xi \in F_9 \backslash \mathbb{Z}_3$ determine the possible minimal polynomials of ξ over $\mathbb{Z}_3$.