A3: Rings and Modules
Sheet II — HT21

II.1. Show that if R is an integral domain and $x \sim y$ then there is $z \in U(R)$ such that $x = zy$. Show that if $x, y \in \mathbb{Z}_4$ and $x \sim y$ then there is a unit z such that $x = zy$.

II.2. Suppose that $\mathbb{F}$ is a field. What are the ideals of the product ring $\mathbb{F}^2$? Is $\mathbb{F}^2$ a PID? Show that $\mathbb{F}^2$ has exactly one proper subring if and only if $\mathbb{F}$ has no proper subrings.

II.3. Let T be the ring of polynomials in $\mathbb{F}[X]$ in which the coefficient of X is zero, so that T is an integral domain. What are the units of T? Show carefully that if $p(X) \mid X^j$ in T then $p(X) \sim X^i$ in T for some i, and $i, j - i, j \in \{0, 2, 3, \dots\}$. Hence show that X^2 is irreducible but not prime in T; X^3 and X^2 have a greatest common divisor; and that $\langle X^3 \rangle \cap \langle X^2 \rangle$ is not principal in T.

II.4. Show that if R is a commutative ring with ideals I, J, and K then $I \cap J + I \cap K \subset I \cap (J + K)$. Show that if $R = \mathbb{Z}[X]$, $I = \langle 2 \rangle$, $J = \langle X + 1 \rangle$ and $K = \langle X - 1 \rangle$, then $I \cap J + I \cap K \subsetneq I \cap (J + K)$. Show that if R is a PID then $I \cap (J + K) = I \cap J + I \cap K$ for all ideals I, J, and K.

II.5. Suppose that R is an infinite integral domain with finitely many units in which every non-unit has an irreducible factor. By emulating Euclid's proof that there are infinitely many primes show that R contains infinitely many irreducible elements.

II.6. Suppose that R is an integral domain with the ACCP in which every maximal ideal is principal. Show that R is a PID.

II.7. Factorise the following into irreducible elements in the given rings and decide whether your factorisation is a unique factorisation into irreducibles.

(a) $36X^3 - 24X^2 - 18X + 12$ in $\mathbb{Z}[X]$;

(b) 6 in $\mathbb{Z}[\sqrt{-5}]$;

(c) $X^5 + X^2 + 1$ in $\mathbb{F}_2[X]$;

(d) X^5 in T, the ring from Exercise II.3.

II.8. Show that $\mathbb{Z}[X]$ has the ACCP, and that every irreducible element in $\mathbb{Z}[X]$ is prime. Hence conclude that $\mathbb{Z}[X]$ is a UFD.

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

II.9. [Optional] Suppose that $\mathbb{F}$ is a finite field of size q. For $n \in \mathbb{N}_0$ let $\Pi_n(X)$ be the product of all monic polynomials in $\mathbb{F}[X]$ of degree exactly n, and for $n \in \mathbb{N}$ let $I_n(X)$ be the product of all monic irreducible polynomials with degree *dividing* n.

(a) Explain why $\deg \Pi_n = nq^n$.

(b) Suppose that $n > 1$ and there are no monic irreducible polynomials of degree n. Show that

$$\deg I_n < q^{2\lfloor n/2 \rfloor}.$$

(c) Suppose that P is an irreducible monic polynomial of degree d. Show that the power of P dividing Π_n is

$$\sum_{k=1}^{\lfloor n/d \rfloor} q^{n-kd},$$

and hence that

$$I_n(X) = \frac{\Pi_n(X)}{\Pi_{n-1}(X)^q}.$$

(d) Combine these ingredients to show that for all $n \in \mathbb{N}$ there is an irreducible polynomial of degree n, and so conclude that for every prime p and $n \in \mathbb{N}$ there is a field of order p^n.

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