Oxford University Department of Mathematics

Rings and Arithmetic 1 (Paper A1): Michaelmas Term 2005

Commutative rings with 1, subrings. Integral domains, fields. polynomial rings. Units. Ideals and quotient rings

1. Which of the following are rings, which not?

(i) $\mathbb{N}$ with the usual addition and multiplication;

(ii) $\mathbb{Z}$ with the usual addition and multiplication;

(iii) $\mathbb{Q}$ with the usual addition and multiplication;

(iv) $\mathbb{Z}$ with addition given by $a \oplus b := a + b + 1$, multiplication $a \otimes b := ab + a + b$;

(v) $\mathbb{R}^2$ with the usual addition and with multiplication given by $(x_1, y_1) \times (x_2, y_2) := (x_1x_2, x_1y_2 + y_1x_2)$.

2. Let X be a set. Define 'addition' and 'multiplication' on its power set $\mathcal{P}X$ by $u+v := (u \cup v) \setminus (u \cap v)$ and $uv := u \cap v$. Prove that this turns $\mathcal{P}X$ into a commutative ring with 1 in which $x^2 = x$ for all elements x.

3. Let Π be a set of prime numbers. An integer n is said to be a Π-number if all its prime factors lie in Π. Define $\mathbb{Z}_\Pi := \{m/n \in \mathbb{Q} \mid m,\ n \text{ are co-prime and } n \text{ is a } \Pi\text{-number}\}$.

(i) Show that $\mathbb{Z}_\Pi$ is a subring of $\mathbb{Q}$.

(ii) Now let $R \leqslant \mathbb{Q}$. Let $m/n \in R$, with m, n co-prime. Let p be a prime divisor of n. Show that $p^{-1} \in R$. [You may find it helpful to recall from Mods that since m and p are co-prime there exist $a, b \in \mathbb{Z}$ such that $am + bp = 1$.] Deduce that $\mathbb{Z}_{\{p\}} \leqslant R$. Prove that there exists a unique set Π of prime numbers such that $R = \mathbb{Z}_\Pi$.

4. (a) Prove that if R is an integral domain then the ring $R[x]$ of polynomials with coefficients from R is an integral domain. Deduce that there is an infinite integral domain of characteristic 2.

(b) Find the units in $R[x]$.

5. Show that a finite integral domain is a field.

6. Let R, S be commutative rings with unity. Recall that $U(R)$ is the group of units of R, and that $R \times S$ is the ring consisting of all pairs (x, y) (for $x \in R$ and $y \in S$) with componentwise addition and multiplication. Identify $U(R \times S)$ in terms of $U(R)$ and $U(S)$.

7. An element x of a ring R is said to be *nilpotent* if $x^k = 0$ for some positive integer k; it is said to be *idempotent* if $x^2 = x$. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ will be denoted $\mathbb{Z}_n$. Let's abuse language a little and use m to denote both an integer m and the member of $\mathbb{Z}_n$ that it represents.

(i) Show that m is a unit in $\mathbb{Z}_n$ if and only if m, n are coprime.

(ii) Show that m is a zero-divisor in $\mathbb{Z}_n$ if and only if m, n are not coprime.

(iii) Identify the nilpotent elements of $\mathbb{Z}_{12}$. [What about $\mathbb{Z}_n$ in general?]

(iv) Identify the idempotent elements of $\mathbb{Z}_{12}$. [What about $\mathbb{Z}_n$ in general?]