Algebra III: Rings and Modules
Problem Sheet 2, Autumn Term 2022-23

John Nicholson

1. Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:

$$\mathbb{Z}[X], \quad \mathbb{Z}[X]/(X^2+1), \quad \mathbb{F}_2[X]/(X^2+1), \quad \mathbb{F}_2[X]/(X^2+X+1), \quad \mathbb{F}_3[X]/(X^2+X+1).$$

2. Given a set $X \subseteq \mathbb{Z}$ of prime numbers, let $S(X) \subseteq \mathbb{Z}$ be the set consisting of 1 and the $n \geq 2$ all of whose prime factors are in X.

   (i) Prove that $S(X)$ is a submonoid of $(\mathbb{Z}, \cdot)$.

   (ii) Let $R_X = S(X)^{-1}\mathbb{Z}$ denote the localisation of the integers at the set $S(X)$. Prove that if X' is another set of prime numbers, then $R_X \cong R_{X'}$ if and only if $X = X'$.

   (iii) Prove that every subring of $\mathbb{Q}$ is of the form R_X for some set of prime numbers X, realising $(a, b) \in R_X$ as the fraction $\frac{a}{b}$.

   (iv) Show that there exists a countable integral domain R (i.e. the set R is countable) for which there exists uncountably many subrings which are distinct up to ring isomorphism.

3. Let R be a commutative ring and let $S \subseteq R$ be a multiplicative submonoid.

   (i) Let $\iota : R \to S^{-1}R$ be the map $a \mapsto (a, 1)$. Show that ι is injective if and only if S contains no zero divisors or zero. Show further that ι is an isomorphism if and only if $S \subseteq R^\times$.

   (ii) Let $I \subseteq R$ be an ideal. Show that I is prime if and only if $R \setminus I \subseteq R$ is a multiplicative submonoid. Deduce that $R \setminus \{0\} \subseteq R$ is a multiplicative submonoid if and only if R is an integral domain.

4. A ring R is *simple* if it is non-trivial and its only two-sided ideals are $\{0\}$ and R. The *centre* of a ring R is the subset $Z(R) \subseteq R$ of elements $x \in R$ such that $xy = yx$ for all $y \in R$.

   (i) Let R be any non-trivial ring. Find two nilpotent elements $x, y \in M_2(R)$ such that $x + y$ and xy are both not nilpotent. [Compare with Problem 2 on Problem Sheet 1.]

   (ii) Let $R = F$ be a field. Prove that $M_n(F)$ is simple.

   (iii) Let R be a ring. Prove that the centre of $M_n(R)$ is $Z(R) \cdot I_n$ where I_n denotes the $n \times n$ identity matrix, i.e. the diagonal matrices whose diagonal entries are all equal to some $x \in Z(R)$.

5. Let d be an integer which is not a square.

   (i) Show that, in $\mathbb{Z}[\sqrt{d}]$, if I is any nonzero ideal, then $\mathbb{Z}[\sqrt{d}]/I$ is finite. [Hint: If $a+b\sqrt{d} \in I$, show that $a^2 - b^2 d \in I$ as well. Then show that $|\mathbb{Z}[\sqrt{d}]/(m)| = m^2$ if $m \geq 1$.]
   (ii) Show that every nonzero prime ideal in $\mathbb{Z}[\sqrt{d}]$ is maximal.
   (iii) Now suppose $\mathbb{Z}[\sqrt{d}]$ is a UFD. Then show that, for every irreducible $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then $\mathbb{Z}[\sqrt{d}]/(a + b\sqrt{d})$ is a field.
   (iv) Is $\mathbb{Z}[\sqrt{5}]$ a Euclidean domain? [Hint: Show that $\mathbb{Z}[\sqrt{5}]/(2) \cong (\mathbb{Z}/2)[X]/(X^2)$.]

6. Let R be a UFD and let $f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ be primitive (i.e. $\gcd(a_0, \cdots, a_n) = 1$) with $a_n \neq 0$. Let $p \in R$ be irreducible (hence prime) and such that $p \nmid a_n$, $p \mid a_i$ for all $0 \leq i < n$ and $p^2 \nmid a_0$.

   (i) Prove that f is irreducible in $R[X]$. This is *Eisenstein's criterion*. [Hint: If f factorises in $R[X]$, what would an induced factorisation in $R[X]/(p) \cong (R/(p))[X]$ look like?]
   (ii) Use Eisenstein's criterion to show that $3X^5 + 12X^3 + 18$ is irreducible over $\mathbb{Q}$.
   (iii) Show that the UFD hypothesis is not needed if we replace p by a prime ideal P and the conditions $p \mid a_i$ by $a_i \in P$ and $p^2 \nmid a_0$ by $a_0 \notin P^2$.

7. Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:

$$X^4 + 2X + 2, \quad X^4 + 18X^2 + 24, \quad X^3 - 9, \quad X^3 + X^2 + X + 1, \quad X^4 + 1, \quad X^4 + 4.$$

8. Find the factorisations of $X^{13} + X$, $X^{16} + 1$, and $X^8 + X^4 + 1$ into irreducibles in $\mathbb{F}_2[X]$.

9. An element e of a ring R is said to be *idempotent* if $e^2 = e$ and $er = re$ for all $r \in R$ (this is often called a *central idempotent*). A nonzero idempotent e is called *primitive* if for any other idempotent e', one has either $e'e = 0$ or $e'e = e$. We will call a ring R with no idempotents other than zero or one *indecomposable*.

   (i) Show that if R and S are rings, then $R \times S$ is not indecomposable unless either R or S is the zero ring.
   (ii) Let e be an idempotent element of R other than zero or one. Show that one has an isomorphism:
$$R \cong R/(e) \times R/(1-e).$$
   (iii) Show that if e is a primitive idempotent then $R/(1-e)$ is indecomposable.
   (iv) Show that a nonzero idempotent e is primitive if and only if e cannot be expressed as $e_1 + e_2$, with e_1, e_2 nonzero idempotents such that $e_1 e_2 = 0$.
   (v) Let R be a ring with finitely many idempotent elements. Show that the number of idempotents is 2^d for some positive integer d, and that R is isomorphic to a product:
$$R \cong R_1 \times R_2 \times \cdots \times R_d,$$
   with each R_i indecomposable. Conclude that R has exactly d primitive idempotents.

10. For each integer $n \geq 1$, show that there exists an ideal in $\mathbb{Z}[X]$ which is generated by $n+1$ elements but not by n elements.

+11. Let p be a prime. Is it true that every ideal in $\mathbb{Z}[C_p]$ is a principal if and only if $\mathbb{Z}[\zeta_p]$ is a principal ideal domain? [Here C_p denotes the cyclic group of order p and $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$ denotes the pth roots of unity.]