IB Groups, Rings and Modules: Example Sheet 2

All rings in this course are commutative with a multiplicative identity.

1. Prove that the product $R_1 \times R_2$ of the rings R_1, R_2 is a ring under componentwise addition and multiplication.

2. (i) Let R be a ring. Recall that $r \in R$ is a *unit* if it has a multiplicative inverse in R. Show that the set of units in R is a group under multiplication.
(ii) An element r of R is *nilpotent* if $r^n = 0$ for some $n \geq 1$. Show that if r is nilpotent, then r is not a unit, but that both $1 + r$ and $1 - r$ are units.
(iii) Prove that the nilpotent elements form an ideal in R.
(iv) If $a \in R$, show that $1 + aX$ is a unit in the polynomial ring $R[X]$ if and only if a is nilpotent.

3. Show that if I and J are ideals in the ring R, then so is $I \cap J$, and the quotient $R/(I \cap J)$ is isomorphic to a subring of the product $R/I \times R/J$.

4. (i) Suppose that $f : R \to S$ is a ring homomorphism. Show that if J is an ideal in S, then $f^{-1}(J) = \{a \in R \,|\, f(a) \in J\}$ is an ideal in R.
(ii) What are the ideals in the ring $\mathbb{Z}$? What are the ideals in the quotient ring $\mathbb{Z}/n\mathbb{Z}$?
(iii) For which values of n and m is there a ring homomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$? Is the homomorphism unique?

5. What are the subrings of the ring $\mathbb{Z}/12\mathbb{Z}$? What are the units in $\mathbb{Z}/12\mathbb{Z}$? What are the ideals in $\mathbb{Z}/12\mathbb{Z}$? Is $\mathbb{Z}/12\mathbb{Z}$ a principal ideal domain?
[Remember that a subring must contain the multiplicative identity of the ring, and that a principal ideal domain must be an integral domain.]

6. (i) Suppose $f(X) \in R[X]$ is a polynomial with coefficients in the ring R and $a \in R$ is such that $f(a) = 0$; show that $f(X) = (X - a)g(X)$ for some $g(X) \in R[X]$. Deduce that if R is an integral domain, then a polynomial $f(X) \in R[X]$ of degree n has at most n roots in R.
(ii) How many roots has $X^2 - 1$ in the ring $\mathbb{Z}/8\mathbb{Z}$? How many roots has $2X^2 - 2X$ in the ring $\mathbb{Z}/4\mathbb{Z}$? In how many essentially different ways can you factorize $(X^2 - 1) \in R[X]$ into irreducibles when $R = \mathbb{Z}/8\mathbb{Z}$?

7. Let R be an integral domain and F be its field of fractions. Suppose that $\phi : R \to K$ is an injective ring homomorphism from R to a field K. Show that ϕ extends to an injective homomorphism $\bar{\phi} : F \to K$ from F to K. What happens if we do not assume that ϕ is injective?

8. (i) Show that the ideal $(2, X)$ in $\mathbb{Z}[X]$ is not a principal ideal.
(ii) Let R be any ring. Show that the ring $R[X]$ is a principal ideal domain if and only if R is a field.

9. Let $\mathbb{F}_p$ be the field of p elements. Show that $\mathbb{F}_p[X]/(X^3 + X + 1)$ is a field if $p = 2$ but not if $p = 3$.

10. (i) Show that the set of all subsets of a given set S is a ring with respect to the operations of symmetric difference and intersection. Note that in this ring $a^2 = a$ for all elements a. Describe the principal ideals in this ring.
(ii) Let R be any ring satisfying $a^2 = a$ for all elements a in R. Prove that R has characteristic 2, and that, for each prime ideal P, the ring R/P is isomorphic to the field of two elements. Show that any ideal of R generated by two elements is in fact a principal ideal, and deduce the same for every finitely generated ideal. Give an example to show that R may have an ideal which is not a principal ideal.

11. An element a of a ring is *idempotent* if $a^2 = a$. Show that the element $e = (1, 0)$ of $R_1 \times R_2$ is idempotent. Let the ring R contain an idempotent e other than 0 or 1. Show that $e' = 1 - e$ is also an idempotent, and that $ee' = 0$. Show that the principal ideal eR generated by e is a ring with identity e. Show that R is isomorphic to the product ring $eR \times e'R$.

Additional Questions

12. (i) Show that a finite subgroup of the multiplicative group of a field is cyclic.
[You can use the structure theorem for finite abelian groups - a non-cyclic group will contain a subgroup $C_p \times C_p$ for some prime p.]
(ii) Find a generator for the multiplicative group of the fields $\mathbb{Z}/p\mathbb{Z}$ of p elements for $p = 5$ and $p = 7$.
(iii) Show for odd p that -1 is a square modulo p if and only if p is congruent to 1 modulo 4.

13. A sequence $\{a_n\}$ of rational numbers is a *Cauchy sequence* if $|a_n - a_m| \to 0$ as $m, n \to \infty$, and $\{a_n\}$ is a *null sequence* if $a_n \to 0$ as $n \to \infty$. Quoting any standard results from Analysis, show that the Cauchy sequences with componentwise addition and multiplication form a ring C, and that the null sequences form a maximal ideal N.
Deduce that C/N is a field, with a subfield which may be identified with $\mathbb{Q}$. Explain briefly why the equation $x^2 = 2$ has a solution in this field.

14. Let ϖ be a set of prime numbers. Write $\mathbb{Z}_\varpi$ for the collection of all rationals m/n (in lowest terms) such that the only prime factors of the denominator n are in ϖ.
(i) Show that $\mathbb{Z}_\varpi$ is a subring of the field $\mathbb{Q}$ of rational numbers.
(ii) (More challenging?) Show that any subring R of $\mathbb{Q}$ is of the form $\mathbb{Z}_\varpi$ for some set ϖ of primes.
(iii) Given (ii), what are the maximal subrings of $\mathbb{Q}$?

15. Let F be a field, and let $R = F[X, Y]$ be the polynomial ring in two variables.
(i) Let I be the principal ideal generated by the element $X - Y$ in R. Show that $R/I \cong F[X]$.
(ii) What can you say about R/I when I is the principal ideal generated by $X^2 + Y$?
(iii) [Harder] What can you say about R/I when I is the principal ideal generated by $X^2 - Y^2$?

16. Recall that $\mathbb{F}_p$ is the field with p elements. Show that in the polynomial ring $\mathbb{F}_p[X]$ the polynomials

$$\prod_{r=0}^{p-1}(X - r) \qquad \text{and} \qquad X^p - X$$

have the same p distinct roots, and hence must be equal.
Deduce Wilson's Theorem that $(p-1)! \equiv -1 \pmod{p}$.
Can you calculate the sum

$$\sum_{\substack{r \neq s \\ r,s \neq 0}}^{p-1} rs \pmod{p} \ ?$$

Comments and corrections should be sent to `brookes@dpmms.cam.ac.uk`.