

### Groups Rings and Modules: Example Sheet 2 of 4

All rings in this course are commutative with a 1.

1. Let  $\omega = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$ , let  $R = \{a + b\omega : a, b \in \mathbb{Z}\}$ , and let  $F = \{a + b\omega : a, b \in \mathbb{Q}\}$ . Show that  $R$  is a subring of  $\mathbb{C}$ , and that  $F$  is a subfield of  $\mathbb{C}$ . What are the units of  $R$ ?
2. An element  $r$  of a (non-zero) ring  $R$  is called *nilpotent* if  $r^n = 0$  for some  $n$ .
  - (i) What are the nilpotent elements of  $\mathbb{Z}/6\mathbb{Z}$ ? Of  $\mathbb{Z}/8\mathbb{Z}$ ? Of  $\mathbb{Z}/24\mathbb{Z}$ ? Of  $\mathbb{Z}/180\mathbb{Z}$ ?
  - (ii) Show that if  $r$  is nilpotent then  $r$  is not a unit, but  $1 + r$  and  $1 - r$  are units.
  - (iii) Show that the set of nilpotent elements form an ideal  $N$  in  $R$ . What are the nilpotent elements in the quotient ring  $R/N$ ?
3. Let  $r$  be an element of a ring  $R$ . Show that the polynomial  $1 + rX \in R[X]$  is a unit if and only if  $r$  is nilpotent. Is it possible for the polynomial  $1 + X$  to be a product of two non-units?
4. Let  $I_1 \subset I_2 \subset I_3 \subset \dots$  be ideals in a ring  $R$ . Show that the union  $I = \bigcup_{n=1}^{\infty} I_n$  is also an ideal. If each  $I_n$  is proper, explain why  $I$  must be proper.
5. Show that if  $I$  and  $J$  are ideals in the ring  $R$ , then so is  $I \cap J$ , and the quotient ring  $R/(I \cap J)$  is isomorphic to a subring of the product  $R/I \times R/J$ . Show further that if there exist  $x \in I$  and  $y \in J$  with  $x + y = 1$  then  $R/(I \cap J) \cong R/I \times R/J$ . What does this result say when  $R = \mathbb{Z}$ ?
6. Let  $R$  be an integral domain. Show that a polynomial in  $R[X]$  of degree  $d$  can have at most  $d$  roots. Deduce that the natural ring homomorphism from  $R[X]$  to the ring of all functions  $R \rightarrow R$  is injective if and only if  $R$  is infinite. Give also an example of a monic quadratic polynomial in  $(\mathbb{Z}/8\mathbb{Z})[X]$  that has more than two roots.
7. Write down a prime ideal in  $\mathbb{Z} \times \mathbb{Z}$  that is not maximal. Explain why in a finite ring all prime ideals are maximal.
8. Explain why, for  $p$  a prime number, there is a unique ring of order  $p$ . How many rings are there of order 4?
9. Let  $R$  be an integral domain and  $F$  be its field of fractions. Suppose that  $\phi : R \rightarrow K$  is an injective ring homomorphism from  $R$  to a field  $K$ . Show that  $\phi$  extends to an injective homomorphism  $\Phi : F \rightarrow K$ . What happens if we do not assume that  $\phi$  is injective?
10. An element  $r$  of a ring  $R$  is called *idempotent* if  $r^2 = r$ .
  - (i) What are the idempotent elements of  $\mathbb{Z}/6\mathbb{Z}$ ? Of  $\mathbb{Z}/8\mathbb{Z}$ ? Of  $\mathbb{Z}/24\mathbb{Z}$ ? How many idempotents are there in  $\mathbb{Z}/180\mathbb{Z}$ ?
  - (ii) Show that if  $r$  is idempotent then so is  $r' = 1 - r$ , and that  $rr' = 0$ . Show also that the ideal  $(r)$  is naturally a ring, and that  $R$  is isomorphic as a ring to  $(r) \times (r')$ .

11. 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  $(X - Y)$  in  $R$ . Show that  $R/I \cong F[X]$ .
  - (ii) Describe  $R/I$  when  $I = (X^2 + Y)$ .
  - (iii) Describe  $R/I$  when  $I = (X^2 - Y^2)$ . Is it an integral domain? Does it have nilpotent or idempotent elements?

### Further Questions

12. Give an example of an abelian group which is not the additive group of some ring; is every abelian group the additive group of some ideal in some ring?
13. Suppose a ring  $R$  has the property that for each  $x \in R$  there is a  $n \geq 2$  such that  $x^n = x$ . Show that every prime ideal of  $R$  is maximal.
14. This question illustrates a construction of the real numbers, so you should avoid mentioning them in your answer.

A sequence  $\{a_n\}$  of rational numbers is a *Cauchy sequence* if  $|a_n - a_m| \rightarrow 0$  as  $m, n \rightarrow \infty$ , and  $\{a_n\}$  is a *null sequence* if  $a_n \rightarrow 0$  as  $n \rightarrow \infty$ . Quoting any standard results from Analysis, show that the set of 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, which contains a subfield which may be identified with  $\mathbb{Q}$ . Explain briefly why the equation  $x^2 = 2$  has a solution in this field.

15. Let  $\varpi$  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  $\varpi$ .
- (i) Show that  $\mathbb{Z}_\varpi$  is a subring of the field  $\mathbb{Q}$  of rational numbers.
  - (ii) Show that any subring  $R$  of  $\mathbb{Q}$  is of the form  $\mathbb{Z}_\varpi$  for some set  $\varpi$  of primes.
  - (iii) Given (ii), what are the maximal subrings of  $\mathbb{Q}$ ?
16. (i) Show that the set  $\mathcal{P}(S)$  of all subsets of a given set  $S$  is a ring with respect to the operations of symmetric difference and intersection. Describe the principal ideals in this ring. Show that the ideal  $(A, B)$  generated by elements  $A, B$  is in fact principal.
- (ii) A ring  $R$  is called *Boolean* if every element of  $R$  is idempotent. Prove that every finite Boolean ring is isomorphic to a power-set ring  $\mathcal{P}(S)$  for some set  $S$ . Give an example to show that this need not remain true for infinite Boolean rings.