Rings and Fields Problems

1. Let R be the set of continuous functions from $[0,\infty[$ to $\mathbb{R}$, with ordinary addition of functions and with a multiplication $*$ given by

$$(f*g)(t)=\int_0^t f(u)g(t-u)du \ \ \forall\ t\geq 0,\ f,\ g\in R.$$

Show that R is a commutative ring. Show that R has no multiplicative identity. (*Hint.* Consider $(f*g)(0)$.)

2. (a) Define *ring.*

(b) Which of the following are rings? In each case (other than (v) and (viii)) state explicitly the operations you think it natural to use for $+$ and $\times$. For each object which is not a ring name a condition in your definition of 'ring' which it does not satisfy.

(i) upper triangular 3×3 real matrices;

(ii) orthogonal 3×3 real matrices;

(iii) $\mathbb{N}$;

(iv) $\mathbb{Z}_{12}$;

(v) $\mathbb{R}^3$ with ordinary vector addition and cross-product multiplication (i.e., $(a_1,a_2,a_3)\times(b_1,b_2,b_3)=(a_2b_3-a_3b_2,a_3b_1-a_1b_3,a_1b_2-a_2b_1)$):

(vi) symmetric 3×3 real matrices;

(vii) the set $\mathcal{P}\mathbb{N}$ of all subsets of $\mathbb{N}$;

(viii) $\mathbb{Z}$ with ordinary addition and the mutiplication $*$, where $m*n=m+n-mn$.

3. (a) Define *ring, subring.*

(b) Let $(G,+)$ be an abelian group. Show that the set of group homomorphisms from G to itself is a ring under suitable operations (to be described explicitly).

(c) Let V be a vector space over a field F. Show that the set of linear maps from V to itself is a subring of the ring of homomorphisms of the additive group $(V,+)$ to itself.

4. Define *ideal.* (a) Describe (with proof) the construction of the quotient ring R/I where R is a ring and I is an ideal of R.

(b) If R is a ring and $a\in R$, under what circumstances is $aR=\{ar:r\in R\}$ an ideal of R?

(c) If R is a ring and $M_n(R)$ is the ring of $n\times n$ matrices with coefficients in R, show that any ideal of $M_n(R)$ is of the form $M_n(I)$ where I is an ideal of R.

(d) Let R be the ring of 2×2 matrices with integer coefficients. Let I be the set of matrices in R all of whose coefficients are even. How many elements does R/I have? Is R/I commutative? (Justify your answer.)

5. (a) Define *homomorphism* (between rings), *subring, ideal, isomorphism* (of rings).

(b) Describe (without proof) the construction of the quotient ring R/I where R is a ring and I is an ideal of R.

(c) Show that if R and S are rings and $\phi:R\to S$ is a homomorphism then $I=\{r:\phi(r)=0\}$ is an ideal of R and $\phi[R]=\{\phi(r):r\in R\}$ is a subring of S.

(d) Show that R/I is isomorphic to $\phi[R]$. (*Hint.* For $s\in\phi[R]$ set $\theta(s)=\{r:\phi(r)=s\}$. Show that $\theta(s)=r+I$ whenever $\phi(r)=s$. Show that $\theta:\phi[R]\to R/I$ is an isomorphism.)

6. Define *ideal, ring of polynomials* over a given ring.

Describe (without proof) the quotient ring R/I where R is a ring and I is an ideal of R.

Let R be the ring of polynomials over the field $\mathbb{R}$. Let $I\subseteq R$ be the ideal of multiples of the polynomial x^2. Show that the quotient R/I can be identified with the vector space $\mathbb{R}^2$ for a suitable multiplication, to be described.

7. (a) Let R be any ring. Let e be a suitable symbol and set $R_1=\{ne+a:n\in\mathbb{Z},a\in R\}$. Show that with appropriate definitions of $+$ and $\times$ (to be described) R_1 is a ring with $\mathbf{1}$ in which R is embedded as a subring.

(b) Show that (i) if R is commutative, so is R_1 (ii) if R is an integral domain, so is R_1.

(c) Give an example in which R is commutative and without zero divisors, but R_1 is not an integral domain.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

8. (a) Define *ring, ideal, integral domain.*

(b) Show that $R = C([0,1])$, the set of continuous real-valued functions on $[0,1]$, is a ring with $\mathbf{1}$. (Explicitly describe the operations $+$, $\times$ you use and give clear statements of any theorems in analysis on which you rely.) Is it an integral domain? Justify your answer.

(c) Define $e \in R$ by setting $e(t) = t$ for $t \in [0,1]$. Let I be the ideal eR. Is R/I an integral domain? Justify your answer.

(d) Show that $J = \{f : f \in R,\ f(0) = 0\}$ is an ideal of R. Show that R/J is isomorphic to a familiar field.

[Standard theorems concerning quotient rings may be used without proof but should be clearly stated.]

9. (a) What is meant by saying that a ring R has a '$\mathbf{1}$' or 'unity'? Show that a ring can have at most one $\mathbf{1}$. In a ring with a $\mathbf{1}$, what is an *invertible element* or 'unit'? Show that an invertible element can have at most one inverse, and that the invertible elements of a ring with $\mathbf{1}$ form a group.

(b)(i) Define *integral domain, field.*

(ii) Show that a finite integral domain is a field.

(iii) Give an example of an integral domain which is not a field, and explain the point at which the argument you gave in (ii) fails when applied to your example.

10. Define *ring, integral domain, field.*

Explain, with proof, how the field of fractions of an integral domain is constructed.

Describe the field of fractions of the ring $\{m + ni : m, n \in \mathbb{Z}\}$ of Gaussian integers.

11. 11. Let R be a ring. Explain what is meant by the ring $R[x]_\infty$ of formal power series with coefficients in R, and prove that it is a ring.

If F is a field, show that every element of $F[x]_\infty$ is of the form $x^n e$ where e is an invertible element of $F[x]_\infty$. Hence show that $F[x]_\infty$ is a Euclidean domain.

12. Define *integral domain, Euclidean domain, ideal.* Show that if R is a Euclidean domain and I is an ideal of R then I is of the form aR for some $a \in R$.

Which of the following are integral or Euclidean domains?

(i) matrices of the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, where $a, b \in \mathbb{R}$;

(ii) $\mathbb{Z}$;

(iii) the ring $\mathbb{R}[x]$ of polynomials over $\mathbb{R}$;

(iv) the ring $\mathbb{Z}[x]$ of polynomials over $\mathbb{Z}$;

(v) the ring $\mathbb{R}[x, y]$ of polynomials in two variables over $\mathbb{R}$;

(vi) the subring $2\mathbb{Z}$ of $\mathbb{Z}$.

Justify your answers.

13. (a) Define *ring, ideal, principal ideal.*

(b) Let X be a set. Show that the set $\mathcal{P}X$ of subsets of X is a ring under suitable operations (to be described explicitly). Does $\mathcal{P}X$ have a multiplicative identity?

(c) Show that every ideal of $\mathcal{P}X$ is principal.

14. (a) Explain (with an outline of the proof) how the polynomial ring $R[x]$ is constructed from a ring R.

(b) Define *principal ideal domain.* Show that if $R[x]$ is a principal ideal domain then R is a field.

15. (a) Define *principal ideal domain.* Show that if R is a principal ideal domain and $a_1, \ldots, a_k \in R$ then there are $r_1, \ldots, r_k \in R$ such that $r_1 a_1 + \ldots + r_k a_k$ is a factor of every a_j.

(b) Let $\mathbf{A}$ be an $n \times n$ complex matrix, where $n \geq 2$. Show that there is a non-zero irreducible polynomial $p \in \mathbb{C}[x]$ such that $p(\mathbf{A}) = \mathbf{0}$. Expressing p as $(x - \lambda_1)^{m_1} \ldots (x - \lambda_k)^{m_k}$, where each $\lambda_j \in \mathbb{C}$ and each $m_j \geq 1$, show that $\mathbb{R}^n = U_1 \oplus \ldots \oplus U_k$, where $U_j = \{\mathbf{u} : \mathbf{u} \in \mathbb{R}^n,\ (\mathbf{A} - \lambda_j \mathbf{I})^{m_j}(\mathbf{u}) = \mathbf{0}\}$. Show that $\mathbf{A}\mathbf{u} \in U_j$ whenever $j \leq k$, $\mathbf{u} \in U_j$.

16. Let R be a principal ideal domain.
(a) Show that for any a, $b \in R$ there are r, $s \in R$ such that $ar + bs$ is a factor of both a and b.
(b) Show that if $p \in R$ is irreducible then the quotient ring R/pR is a field.
(c) Set $R = \{m + n\omega : m, n \in \mathbb{Z}\}$ where $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{C}$. Give a formula for a Euclidean valuation on R (you need not show that it is a valuation) and show that $\zeta = 2 + \omega$ is a prime in R. Describe the field $R/\zeta R$.

17. Set $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{C}$, $R = \{m + n\omega : m, n \in \mathbb{Z}\} \subseteq \mathbb{C}$.
(a) Show that R is a subring of $\mathbb{C}$.
(b) Show that R is a Euclidean domain.
(c) Show that 2 and $2 + \omega$ are irreducible in R.
(d) Describe the field $R/2R$, giving its addition and multiplication tables.

18. (a) Define *unique factorisation domain.* Show that an integral domain R is a unique factorisation domain iff (i) irreducibles in R are prime (ii) every non-zero non-invertible element of R is expressible as a product of irreducibles.
(b)(i) Give an example (with proof) of an integral domain R in which every non-zero non-invertible element of R is expressible as a product of irreducibles, but R is not a unique factorisation domain;
(ii) give an example (with proof) of an integral domain in which there are no irreducible elements (so that every irreducible is prime) but R is not a field (so is not a unique factorisation domain).

19. (a) Define *integral domain, principal ideal domain.* Describe (without proof) the construction of the field of fractions of an integral domain.
(b) State the Unique Factorisation Theorem for principal ideal domains.
(c) Let R be a principal ideal domain, F its field of fractions. Suppose $x \in F$ is of the form $q/p_1^{k_1} \dots p_r^{k_r}$ where $q \in R$ and $p_1, \dots, p_r$ are distinct irreducible elements of R. Show that x is expressible as

$$\sum_{j=1}^{r} \frac{q_j}{p_j^{k_j}},$$

where $q_1, \dots, q_r \in R$.
(d) Illustrate (c) by expressing $\frac{17}{60}$ in the form $\frac{l}{3} + \frac{m}{4} + \frac{n}{5}$ where l, m, $n \in \mathbb{Z}$.

20. Let R be a Euclidean domain with Euclidean valuation ν, and F its field of fractions. Show that any element of F is uniquely expressible in the form

$$a + \sum_{j=1}^{n} \frac{q_j}{p_j^{k_j}}$$

where $a \in R$, $q_1, \dots, q_n \in R \setminus \{0\}$, $p_1, \dots, p_n \in R$ are irreducible elements of R, $k_1, \dots, k_n \geq 1$ are integers and $\nu(q_j) < \nu(p_j)$ for every j. (It is understood that n may be 0.) Illustrate your proof by tracing it step-by-step through the representation of

$$\frac{x^4 - x^3 + 3x^2 - x + 1}{x^5 + x^3}$$

as partial fractions in the field of rational functions with integer coefficients.

21. Define *Euclidean domain, principal ideal domain.* State the Unique Factorisation Theorem for principal ideal domains.
Let R be the ring of Gaussian integers, viz. $\{m + ni : m, n \in \mathbb{Z}\}$. Show that R is a Euclidean domain. Show that an element $m + ni$ of R is irreducible in R iff *either* $m^2 + n^2$ is a prime in $\mathbb{Z}$ *or* one of $|m|$, $|n|$ is zero and the other is a prime in $\mathbb{Z}$ which is not the sum of two squares in $\mathbb{Z}$.

22. Define *Euclidean domain, irreducible* element of an integral domain, *prime* element of an integral domain, *principal ideal domain.*

Show that primes are always irreducible, and that in a principal ideal domain irreducible elements are prime.

State the Unique Factorisation Theorem for principal ideal domains.

Let R be the set $\{m + n\omega : m,\, n \in \mathbb{Z}\} \subseteq \mathbb{C}$ where $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Show that R is a subring of $\mathbb{C}$ and is a Euclidean domain.

Express 6 as a product of prime factors in R.

23. (a) Let R be an integral domain. Show that if $a^2 = b^2$ in R then $a = \pm b$.

(b) Let F be a finite field. Show that the product of the non-zero elements of F is -1. (*Hint.* Collect them, as far as possible, into inverse pairs.)

(c) Let $p \in \mathbb{N}$ be a prime. Show that $(p-1)! \cong -1 \bmod p$.

(d) Let $p \in \mathbb{N}$ be a prime of the form $4m + 1$ where $m \in \mathbb{N}$; set $q = (p-1)/2$. Show that $(q!)^2 \cong -1 \bmod p$.

(e) Let R be the ring $\{m + ni : m,\, n \in \mathbb{Z}\}$ of Gaussian integers. Is R is a unique factorisation domain? Justify your answer.

(f) Let $p \in \mathbb{N}$ be a prime of the form $4m + 1$ where $m \in \mathbb{N}$. Show that p is not a prime in R. (*Hint.* Find $n,\, k$ such that $(n - i)(n + i) = kp$.) Hence show that p is expressible as the $a^2 + b^2$ where $a,\, b \in \mathbb{Z}$. (*Hint.* Show that p has a non-trivial factor $r \in R$ and consider $|r|^2$.)

24. Define *Euclidean domain, irreducible* element. Show that if R is a Euclidean domain then any two elements $a,\, b \in R$ have a greatest common divisor (in a sense which you should explain).

Show that the ring $R = \{m + ni : m,\, n \in \mathbb{Z}\}$ of Gaussian integers is a Euclidean domain. Find the greatest common divisor in R of $3 + i$ and 5. Show that 3 and 7 are irreducible in R.

25. (a) Define the terms *integral domain, irreducible element, unique factorisation domain, prime element, greatest common divisor.*

(b) Show that in an integral domain all primes are irreducible and that in a unique factorisation domain all irreducibles are prime.

(c) Give an example (with proof) of an integral domain which is not a unique factorisation domain.

(d) Show that in a unique factorisation domain R

(i) any non-zero $a_1, \dots, a_k \in R$ have a greatest common divisor in R;

(ii) if d is a greatest common divisor of $a_1, \dots, a_k$ and $b \in R \setminus \{0\}$ then bd is a greatest common divisor of $ba_1, \dots, ba_k$.

26. (a) Let R be a unique factorisation domain and F its field of fractions. Show that if a polynomial with coefficients in R is irreducible in $R[x]$ then it is irreducible in $F[x]$.

(b) For each of the following polynomials either find a factorisation in $\mathbb{Q}[x]$ or show that it is irreducible in $\mathbb{Q}[x]$:

(i) $x^2 + \frac{1}{2}x + 1$;

(ii) $x^3 + \frac{3}{4}x + \frac{1}{2}$;

(iii) $x^4 + x^3 + x^2 + x + 1$.

Are any of these polynomials irreducible in $\mathbb{C}[x]$? Justify your answer.

27. Define *unique factorisation domain.* Let R be a unique factorisation domain and F its field of fractions.

(a) Recall that a polynomial is *primitive* if its coefficients have no non-trivial common factor. Show that if $p,\, q$ are primitive polynomials in the polynomial ring $R[x]$ then their product pq is also primitive.

(b) Show that $p \in R[x]$ is irreducible in $R[x]$ iff it is primitive and irreducible in $F[x]$.

28. Define *integral domain, Euclidean domain, principal ideal domain, unique factorisation domain.* For each of the following rings state exactly which of the four definitions it satisfies; briefly justify your answers.

(i) $\mathbb{R}$;
(ii) $\mathbb{Q}[x]$;
(iii) $\mathbb{C}[x, y]$;
(iv) $\mathbb{Z}$;
(v) $\mathbb{Z}[x]$;
(vi) $\mathbb{Z}_{12}$;
(vii) $\mathbb{Z}_{13}$.

29. A field F is *of characteristic 2* if $1 + 1 = 0$.

(a) Let F be a field which is not of characteristic 2 and $K \subseteq F$ a subfield of F. Suppose that every element of K has a square root in F. Show that every polynomial over K of degree 2 is reducible in $F[x]$.

(b) Show that if F is a finite field of characteristic 2 then every element of F has a square root, but there is a quadratic of the form $x^2 + ax + 1$ which is irreducible in $F[x]$.

30. Define *ring, ideal, integral domain.*

Prove that a finite integral domain is a field.

Describe a field with four elements, giving its addition and multiplication tables.

31. (a) Define *irreducible element* in a ring. List the irreducible quadratics and cubics in the ring $\mathbb{Z}_2[x]$ of polynomials over the field $\mathbb{Z}_2$.

(b) Is $x^4 + x^2 + 1$ irreducible in $\mathbb{Z}_2[x]$? Is $x^4 + x + 1$ irreducible in $\mathbb{Z}_2[x]$? Justify your answers.

32. Give the addition and multiplication tables of the field $\mathbb{Z}_3$.

Show that $p = x^2 + a$ is irreducible in the ring $R = \mathbb{Z}_3[x]$ for just one value of $a \in \mathbb{Z}_3$; what is it?

Give a list of the elements of the field $F = R/pR$. Show that the group $F \setminus \{0\}$ is cyclic and find a generator for it.

33. Let F be a finite field. Show that there is a quadratic with coefficients in F which is irreducible in $F[x]$.

(*Hint.* If $1 + 1 \neq 0$, show that not every element of F is a square. If $1 + 1 = 0$, show that not every element of F is of the form $x(x + 1)$.)

Find such quadratics for the fields $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

34. Define *subfield.*

Suppose that F is a field and $K \subseteq F$ is a subfield. Let $c \in F$ be such that c is a root of a quadratic with coefficients in K. Show that $L = \{a + bc : a, b \in K\}$ is a subfield of F. Show that if $x^3 + px + q$ is a cubic with coefficients in K which has no root in K then it has no root in L.

Hence show that there is no straight-edge-and-compasses construction of an angle of $10°$.