ALGEBRA QUALIFYING EXAM PROBLEMS
RING THEORY

Nic Beike

June 28, 2022

Contents

1 Ring Theory

1.1 General Ring Theory

1. Give an example of each of the following

   (a) An irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$

   (b) A polynomial in $\mathbb{Z}[x]$ that is not irreducible in $\mathbb{Z}[x]$ but is irreducible in $\mathbb{Q}[x]$

   (c) A non-commutative ring of characteristic p, p a prime

   (d) A ring with exactly 6 inverible elements

   (e) An infinite non-commutative ring with only finitely many ideals.

   (f) An infinite non-commutative ring with non-zero characteristic.

   (g) An integral domain which is not a unique factorization domain.

   (h) A unique factorization domain that is not a principal ideal domain

   (i) A principal ideal domain that is not a Euclidean domain.

   (j) A Euclidean domain other than the ring of integers of a field.

   (k) A finite non-commutative ring.

   (l) A commutative ring with a sequence $\{P_n\}_{n=1}^{\infty}$ of prime ideals such that P_n is properly contained in P_{n+1} for all n.

   (m) A non-zero prime ideal of a commutative ring that is not a maximal ideal.

   (n) An irreducible element of a commutative ring that is not a prime element.

   (o) An irreducible element of an integral domain that is not a prime element.

   (p) A commutative ring that has exactly one maximal ideal and is not a field.

   (q) A non-commutative ring with exactly two maximal ideals.

2. (a) How many units does the ring $\mathbb{Z}/60\mathbb{Z}$ have? Explain your answer.

   (b) How many ideals does the ring $\mathbb{Z}/60\mathbb{Z}$ have? Explain your answer.

   Proof. For (a), we can use the fact that a is a unit if $\gcd(a,n)=1$. Thus $\mid U_{60} \mid=\mid \{1,7,11,13,17,19,23,29,31,37,41,43,47,53,57,59\} \mid= 16$.

   For (b) use the fact that $\mathbb{Z}/d\mathbb{Z}$ is an ideal of $\mathbb{Z}/n\mathbb{Z}$ when $d \mid n$. So let $D=\{d \in \mathbb{Z}/60\mathbb{Z} : d \mid 60\} = \{2^x \cdot 3^y \cdot 5^z : 0 \le x \le 2, 0 \le y \le 1, 0 \le z \le 1\}$. Thus the number of ideals is equal to $\mid D \mid = 3 \cdot 2 \cdot 2 = 12$ □

3. How many ideals does the ring $\mathbb{Z}/90\mathbb{Z}$ have? Explain your answer.

   Proof. Use the fact that $\mathbb{Z}/d\mathbb{Z}$ is an ideal of $\mathbb{Z}/n\mathbb{Z}$ when $d \mid n$. Let $D=\{d \in \mathbb{Z}/90\mathbb{Z} : d \mid 90\} = \{2^x \cdot 3^y \cdot 5^z : 0 \le x \le 1, 0 \le y \le 2, 0 \le z \le 1\}$. Then the number of ideals is equal to $\mid D \mid = 2 \cdot 3 \cdot 2 = 12$. □

4. Denote the set of inverible elements of the ring $\mathbb{Z}_n$ by U_n.

   (a) List all the elements of U_{18}.

   (b) Is U_{18} a cyclic group under multiplication? Justify your answer.

   Proof. Use the fact that a is a unit if $\gcd(a,18)=1$. So the invertible elements of $\mathbb{Z}_{18}$ are $U_{18}=\{1,5,7,11,13,17\}$. Note that $\langle 5 \rangle = \{5,7,17,13,11,1\} = U_{18}$. Therefore U_{18} is cyclic. □

5. Denote the set of inverible elements of the ring $\mathbb{Z}_n$ by U_n.

   (a) List all the elements of U_{24}.

   (b) Is U_{24} a cyclic group under multiplication? Justify your answer.

Proof. Use the fact that a is a unit if $\gcd(a, 24) = 1$. So the invertible elements of $\mathbb{Z}_{18}$ are $U_{24} = \{1, 5, 7, 11, 13, 17, 19, 23\}$. Note that $x^2 = 1$ for all $x \in U_{24}$. Therefore U_{24} is not cyclic. $\square$

6. Find all positive integers n having the property that the group of units of $\mathbb{Z}/n\mathbb{Z}$ is an elementary abelian 2-group.

7. Let $U(R)$ denote the group of units of a ring R. Prove that if m divides n, then the natural ring homomorphism $\mathbb{Z}_n \to \mathbb{Z}_m$ maps $U(\mathbb{Z}_n)$ onto $U(\mathbb{Z}_m)$. Give an example that shows that $U(R)$ does not have to map onto $U(S)$ under a surjective ring homomorphism $R \to S$.

8. If p is a prime satisfying $p \equiv 1(\text{mod } 4)$, then p is a sum of two squares.

9. If $(\div)$ denotes the Legendre symbol, prove Euler's Critereon: if p is a prime and a is any integer relatively prime to p, then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$

10. Let R_1 and R_2 be commutative rings with identities and let $R = R_1 \times R_2$. Show that every ideal I of R is of the form $I = I_1 \times I_2$ with I_i an ideal of R_i for $i = 1, 2$.

Proof. Let I be an ideal fo $R = R_1 \times R_2$. Define $I_1 = \{r \in R_1 : \exists s \in R_2 \text{ where } (r, s) \in I\}$ and $I_2 = \{s \in R_2 : \exists r \in R_1 \text{ where } (r, s) \in I\}$.

Note that if $r \in I_1$, then there exists $s \in R_2$ such that $(r, s) \in I$. Thus $(a, 1_{R_2})(r, s) = (ar, s) \in I$, and so $ar \in I_1$. Thus I_1 is an ideal of R_1. By a similar argument, we can see that I_2 is an ideal of R_2. Now it is clear that $I \subseteq I_1 \times I_2$.

To show the reverse inclusion, suppose that $r \in I_1$, and $s \in I_2$ such that $(r, s) \in I_1 \times I_2$. Since $r \in I_1$, then there is an $s' \in I_2$ such that $(r, s') \in I$. Also since $s \in I_2$, then there exists an $r' \in I_2$ such that $(r', s) \in I$. Now we see that $(1_R, s)(r, s') = (r, ss') \in I$, and $(1_R, s')(r', s) = (r', ss') \in I$. Thus $(r, ss') - (r', ss') + (r', s) = (r, s) \in I$. Therefore $I_1 \times I_2 \subseteq I$ so $I = I_1 \times I_2$, as desired. $\square$

11. Show that a non-zero ring R in which $x^2 = x$ for all $x \in R$ is of characteristic 2 and is commutative.

Proof. Let $x \in R$ and note that $x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$. Thus $x + x = 0$, so R has characteristic zero.

Now let $x, y \in R$. Then $x+y = (x+y)^2 = x^2+xy+yx+y^2$. Rearranging terms gives $0 = xy+yx$. Now $xy = xy+xy+yx = (xy+xy)+yx = 0+yx = yx$. Thus we conclude that R is commutative. $\square$

12. Let R be a finite commutative ring with more than one element and no zero-divisors. Show that R is a field.

Proof. Define $\phi : R \to R$ by $\phi(r) = xr$ for all $r \in R$ and a fixed nonzero element $x \in R$. Suppose that for two elements $r, s \in R$, $\phi(r) = phi(s)$. Then we have $xr = xs$ or $xr - xs = 0$ or $x(r - s) = 0$. Since x is nonzero and R has no zero divisors, we see that $r - s = 0$, and so $r = s$. Thus the map ϕ is injective. Since we are mapping from $R \to R$, then ϕ must also be surjective and thus bijective.

First we show that R has an identity element. By the surjectivity of ϕ there must be an element $e \in R$ such that $x = \phi(e) = ex$. Now let $b \in R$. Then by the surjectivity of ϕ there is an element $y_b \in R$ such that $b = \phi(y_b) = y_b x$. Now we have $b = y_b x = y_b e x = (y_b x)e = be$. Thus $e = 1$ since it fixes every element in R.

Now again by the surjectivity of ϕ, we must have some $r \in R$ such that $\phi(r) = rx = 1$. Thus x is a unit and since the choice of x was arbitrary (except for the restriction of x being nonzero), we conclude that R must be a field. $\square$

13. Determine for which integers n the ring $\mathbb{Z}/n\mathbb{Z}$ is a direct sum of fields. Prove your answer.

14. Let R be a subring of a field F such that for each x in F either $x \in R$ or $x^{-1} \in R$. Prove that if I and J are ideals of R, then either $I \subseteq J$ or $J \subseteq I$.

Proof. Suppose $I \nsubseteq J$. It suffices to show that $J \subseteq I$. Since $I \nsubseteq J$, then there is a nonzero $a \in I \setminus J$. If $b \in J$, we want to show that $b \in I$.

If $b = 0$, then we are done since I is an ideal, and must contain zero. Now suppose $b \neq 0$. Then there is an inverse $b^{-1} \in F$ and so $ab^{-1} \in F$. Thus either $ab^{-1} \in R$ or $ba^{-1} \in R$. If $ab^{-1} \in R$, then $a = ab^{-1}b \in J$, a contradiction.

Thus it must be the case that $ba^{-1} \in R$, and so $b = ba^{-1}a \in I$. Therefore $b \in I$ and $J \subseteq I$, as desired. □

15. The *Jacobson Radical* $J(R)$ of a ring R is defined to be the intersection of all maximal ideals of R. Let R be a commutative ring with 1 and let $x \in R$. Show that $x \in J(R)$ if and only if $1 - xy$ is a unit for all y in R.

    Proof. Suppose that $x \in J(R)$. Then $x \in I_i$ where I_i is a maximal ideal. Then $xy \in I_i$ for all i, and so $xy \in J(R)$. Thus xy is quasiregular and so $1 - xy$ is a unit for all y in R.

    Now suppose that $1-xy$ is a unit for all $y \in R$ and $x \notin J(R)$. Then there exists a maximal ideal M such that $x \notin M$. Thus $\langle x \rangle + M = R$. So there exists a $y \in R$ and $m \in M$ such that $xy + m = 1$. Thus $m = 1 - xy \in M$ is a unit. So we must have $M = R$, but this is a contradiction to the maximality of M. □

16. Let R be any ring with identity, and n any positive integer. If $M_n(R)$ denotes the ring or $n \times n$ matrices with entries in R, prove that $M_n(I)$ is an ideal of $M_n(R)$ whenever I is an ideal of R, and that every ideal of $M_n(R)$ has this form.

17. Let m, n be positive integers such that m divides n. Then the natural map $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $a + (n) \mapsto a + (m)$ is a surjective ring homomorphism. If U_n, U_m are the units of $\mathbb{Z}_n$ and $\mathbb{Z}_m$, respectively, show that $\phi : U_n \to U_m$ is a surjective group homomorphism.

18. Let R be a ring with the ideals A and B. Let $R/A \times R/B$ be the ring with coordinate-wise addition and multiplication. Show the following.

    (a) The map $R \to R/A \times R/B$ given by $r \mapsto (r + A, r + B)$ is a ring homomorphism.

    (b) The homomorphism is part (a) is surjective if and only if $A + B = R$.

19. Let m and n be relatively prime integers.

    (a) Show that if c and d are any integers, then there is an integer x such that $x \equiv c (\text{mod } m)$ and $x \equiv d (\text{mod } n)$.

    (b) Show that $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic as rings.

20. Let R be a commutative ring with 1 and let I and J be ideals of R such that $I + J = R$. Show that $R/(I \bigcap J) \cong R/I \oplus R/J$.

21. Let R be a commutative ring with identity and let $I_1, I_2, \cdots, I_n$ be pairwise co-maximal ideals of R (i.e, $I_i + I_j = R$ if $i \neq j$). Show that $I_i + \bigcap_{j \neq i} I_j = R$ for all i.

22. Let R be a commutative ring, not necessarily with identity, and assume there is some fixed positive integer n such that $nr = 0$ for all $r \in R$. Prove that R embeds in a ring S with identity so that R is an ideal of S and $S/R \cong \mathbb{Z}/n\mathbb{Z}$.

23. Let R be a ring with identity 1 and $a, b \in R$ such that $ab = 1$. Denote $X = \{x \in R \mid ax = 1\}$. Show the following.

    (a) If $x \in X$, then $b + (1 - x) \in X$.

    (b) If $\phi : X \to X$ is the mapping given by $\phi(x) = b + (1 - xa)$, then ϕ is one-to-one.

    (c) If X has more than one element, then X is an infinite set.

24. Let R be a commutative ring with identity and define $U_2(R) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in R \right\}$. Prove that every R-automorphism of $U_2(R)$ is inner.

25. Let $\mathbb{R}$ be the field of real numbers and let F be the set of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -3b & a \end{bmatrix}$, where $a, b \in \mathbb{R}$ Show that F is a field under the usual matrix operations.

26. Let R be the ring of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ where a and b are real numbers. Prove that R is isomorphic to $\mathbb{C}$, the field of complex numbers.

27. Let p be a prime and let R be the ring of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ pb & a \end{bmatrix}$, where $a, b \in \mathbb{Z}$. Prove that R is isomorphic to $\mathbb{Z}[\sqrt{p}]$.

28. Let p be a prime and F_p the set of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where $a, b \in \mathbb{Z}_p$.
    (a) Show that F_p is a commutative ring with identity.
    (b) SHow that F_7 is a field.
    (c) Show that F_{13} is not a field.

29. Let $I \subseteq J$ be right ideals of a ring R such that $J/I \equiv R$ as right R-modules. Prove that there exists a right ideal K such that $I \cap K = (0)$ and $I + K = J$.

30. A ring R is called simple if $R^2 \neq 0$ and 0 and R are its only ideals. Show that the center of a simple ring is 0 or a field.

31. Give an example of a field F and a one-to-one ring homomorphism $\phi : F \to F$ which is not onto. Verify your example.

32. Let D be an integral domain and let $D\left[x_1, x_2, \ldots, x_n\right]$ be the polynomial ring over D in the n indeterminates $x_1, x_2, \ldots, x_n$. Let
$$V = \begin{bmatrix} x_1^{n-1} & \ldots & x_1^2 & x_1 & 1 \\ x_2^{n-1} & \ldots & x_2^2 & x_2 & 1 \\ \vdots & & \vdots & \vdots & \vdots \\ x_n^{n-1} & \ldots & x_n^2 & x_n & 1 \end{bmatrix}.$$
Prove that the determinant of V is $\prod_{1 \leq i < j \leq n} (x_i - x_j)$.

33. Let $R = C[0, 1]$ be the set of all continuous real-valued functions on $[0, 1]$. Define addition and multiplication on R as follows. For $f, g \in R$ and $x \in [0, 1]$,
$$(f + g)(x) = f(x) + g(x) \text{ and } (fg)(x) = f(x)g(x).$$
    (a) Show that R with these operations is a commutative ring with identity.
    (b) Find the units of R.
    (c) If $f \in R$ and $f^2 = f$, then $f = 0_R$ of $f = 1_R$.
    (d) If n is a positive integer and $f \in R$ is such that $f^n = 0_R$, then $f = 0_R$

34. Let S be the ring of all bounded, continuous functions $f : \mathbb{R} \to \mathbb{R}$, where $\mathbb{R}$ is the set of real numbers. Let I be the set of functions f in S such that $f(t) \to 0$ as $\mid t \mid \to \infty$.
    (a) Show that I is an ideal of S.
    (b) Suppose $x \in S$ is such that there is an $i \in I$ with $ix = x$. Show that $x(t) = 0$ for all sufficiently large $\mid t \mid$.

35. Let $\mathbb{Q}$ be the field of rational numbers and $D = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
    (a) Show that D is a subring of the field of real numbers.
    (b) Show that D is a principal ideal domain.
    (c) show that $\sqrt{3}$ is not an element of D.

36. Show that if p is a prime such that $p \equiv 1 (\text{mod } 4)$, then $x^2 + 1$ is not irreducible in $\mathbb{Z}_p[x]$.

37. Show that if p is a prime such that $p \equiv 4 (\text{mod } 4)$, then $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$.

38. Show that if p is a prime such that $p \equiv 1 (\text{mod } 6)$, then $x^3 + 1$ splits in $\mathbb{Z}_p[x]$.

1.2 Prime, Maximal, and Primary Ideals

39. Let R be a non-zero commutative ring with 1. Show that an ideal M of R is maximal if and only if R/M is a field.

    Proof. By the correspondence theorem, M is a maximal ideal of R if and only if 0 is a maximal ideal of R/M. Also, it is known that a commutative ring is a field if and only if 0 is a maximal ideal. Thus the result follows. □

40. Let R be a commutative ring with 1. Show that an ideal P of R is prime if and only if R/P is an integral domain.

    Proof. First let P be a prime ideal of R. Then R/P is a prime ring. Let $a, b \in R/P$ such that $ab = 0$. Then we can say that $(a)(b) = 0$ where (a) and (b) are ideals generated by a and b respectively in R/P. But then we know that either $(a) = 0$ or $(b) = 0$ since R/P is a prime ring. Therefore, we must have $a = 0$ or $b = 0$ and so R/P is an integral domain.

    Now suppose that R/P is an integral domain. Suppose A and B are ideals such that $AB = 0$. Then pick $a_1 \in A$. Then, since R/P is an integral domain, we have $a_1 b_i = 0$ for all $b_i \in B$ or $a_1 = 0$. Continuing in this way, we must have either $A = 0$ or $B = 0$. Thus R/P is prime so P is a prime ideal □

41. (a) Let R be a commutative ring with 1. Show that if M is a maximal ideal of R then M is a prime ideal of R.

    (b) Give an example of a non-zero prime ideal in a ring R that is not a maximal ideal.

    Proof. For (a) since M is a maximal ideal then R/M is a field and thus an integral domain. Since R/M is an integral domain, then M is a prime ideal of R.

    For (b) note that $\mathbb{Z}[x]/(x) \equiv \mathbb{Z}$ so (x) is a prime ideal of $\mathbb{Z}[x]$ but (x) is not maximal in $\mathbb{Z}[x]$ since $\mathbb{Z}$ is not a field. □

42. Let R be a non-zero ring with identity. Show that every proper ideal of R is contained in an maximal idea.

    Proof. Let $I \subsetneq R$ be a proper ideal. Define the set $P = \{A \mid I \subseteq A \subsetneq R \text{ is an ideal of } R\}$. Let $\mathcal{C}$ be a chain of ideals in P. Then $U_{\mathcal{C}} = \bigcup_{A \in \mathcal{C}} A$ is an ideal of R containing I and is an upper bound for $\mathcal{C}$. Notice that $1 \notin U_{\mathcal{C}}$ since 1 was not in any of the ideals from $\mathcal{C}$ as the ideals in $\mathcal{C}$ are proper in R. Thus we have that $U_{\mathcal{C}} \in P$. Now we can apply Zorn's Lemma. So there exists a maximal element $\mathscr{A}$ of the set P. It follows that $I \subseteq \mathscr{A} \subsetneq R$ and so I is contained in the maximal ideal $\mathscr{A}$.

    □

43. Let R be a commutative ring with 1 and P a prime ideal of R. Show that if I and J are ideals of R such that $I \cap J \subseteq P$ and $J \nsubseteq P$, then $I \subseteq P$.

    Proof. Suppose that I and J are ideals of R such that $I \cap J \subseteq R$ but $JnsubseteqP$. Then there is some element $x \in J$ such that $x \notin P$.

    Let $y \in I$, then $xy \in I$ and $xy \in J$. Thus $xy \in P$. Since P is prime, we must have $x \in P$ or $y \in P$. We know that $x \notin P$ so it must be the case that $y \in P$. Since $y \in I$ was arbitrary, it follows that $I \subseteq R$. □

44. Let $M_1 \neq M_2$ be two maximal ideals in the commutative ring R and let $I = M_1 \cap M_2$. Prove that R/I is isomorphic to the direct sum of two fields.

45. Let R be a non-zero commutative ring with 1. Show that if I is an ideal of R such that $1 + a$ is a unit in R for all $a \in I$, then I is contained in every maximal ideal of R.

Proof. Let I be an ideal of R such that $1+a$ is a unit in R for all $a \in I$. If $a \in I$ the we know that $-a \in I$. Thus $1-a$ is a unit in R for all $a \in I$. It follows that every element of I is quasiregular. It is known that the Jacobson Radical, $J(R)$, is maximal with respect to every element being quasiregular. Thus $I \subseteq J(R) \subseteq \bigcap_{\{M \mid M \text{ is maximal in } R\}} M$, as desired. □

46. Let R be a commutative ring with identity. Suppose R contains an idempotent element a other that 0 or 1. Show that every prime ideal of R contains an idempotent element other that 0 or 1. (An element $a \in R$ is idempotent if $a^2 = a$)

47. Let R be a commutative ring with 1.

    (a) Prove that (x) is a prime ideal in $R[x]$ if and only if R is an integral domain.

    (b) Prove that (x) is a maximal ideal in $R[x]$ if and only if R is a field.

    Proof. Note that (x) is an ideal of $R[x]$ and $R[x]/(x) \equiv R$. Then (a) and (b) follow trivially. □

48. Find all values of a in $\mathbb{Z}_3$ such that the quotient ring

$$\mathbb{Z}_3[x]/(x^3 + x^2 + ax + 1)$$

    is a field. Justify your answer.

49. Find all values of a in $\mathbb{Z}_5$ such that the quotient ring

$$\mathbb{Z}_5[x]/(x^3 + 2x^2 + ax + 3)$$

    is a field. Justify your answer.

50. Let R be a commutative ring with identity and let U be maximal among non-finitely generalted ideals of R. Prove U is a prime ideal.

51. Let R be a commutative ring with identity and let U be a maximal among non-principal ideals of R. Prove U is a prime ideal.

    Proof. Let $U \subseteq R$ be maximal among non-principal ideals. Suppose U is not prime. Then there exists $a, b \in R \setminus U$ such that their product $ab \in U$. Then we have that $U \subsetneq U + (a)$. Since U is properly contained in $U + (a)$, then $U + (a)$ is principal. So $U + (a) = (c)$ for some $c \in R$.

    Now define the set $V = \{x \in R \mid cx \in U\}$. Clearly we have $U \subseteq V$. Also we can say $u + ra = c$ for some $u \in U$ and $r \in R$. Then $b(u + ra) = bu + r(ab) = bc$. So it follows that $bc \in U$ since $bu \in U$ and $r(ab) \in U$. Thus $b \in V$ and we can conlude that $U \subsetneq V$. Now we can say that $V = (d)$ for some $d \in R$.

    Let $u \in U$. Then $u = cy$ for some $y \in R$. Then $y \in V$. So we can say that $y = dz$ for some $z \in R$. Thus $u = c(dz)$ and so $u \in (cd)$. Hence $U \subseteq (cd)$. Also since $d \in V$ then $cd \in U$ and so $(cd) \subseteq U$. But then we have $U = (cd)$, a contradiction and so U is a prime ideal. □

52. Let R be a non-zero commutative ring with 1 and S a multiplicative subset of R not containing 0. Show that if P is maximal in the set of ideals of R not intersecting S, then P is a prime ideal.

    Proof. Let S be a multiplicative set not containing 0. Let $P \subseteq R \setminus S$ be maximal. Suppose that P is not a prime ideal. Then there exists elements $a, b \in R \setminus P$ such that $ab \in P$. Then $P + (a) \cap S \neq \emptyset$ and $P + (b) \cap S \neq \emptyset$. So there exists elements $p, q \in P$ and $s, t \in R$ such that $p + as \in S$ and $q + bt \in S$. Thus we can say that $(p + as)(q + bt) = (pq) + as(q) + (p)bt + (ab)st \in P \cap S = \emptyset$, a contradiction. □

53. Let R be a non-zero commutative ring with 1.

    (a) Let S be a multiplicative subset of R not containing 0 and let P be maximal in the set of ideals of R not intersecting S. Show that P is a prime ideal.

    (b) Show that the set of nilpotent elements of R is the intersection of all prime ideals.

Proof. For (a), let S be a multiplicative set not containing 0. Let $P \subseteq R \setminus S$ be maximal. Suppose that P is not a prime ideal. Then there exists elements $a, b \in R \setminus P$ such that $ab \in P$. Then $P + (a) \cap S \neq \emptyset$ and $P + (b) \cap S \neq \emptyset$. So there exists elements $p, q \in P$ and $s, t \in R$ such that $p + as \in S$ and $q + bt \in S$. Thus we can say that $(p + as)(q + bt) = (pq) + as(q) + (p)bt + (ab)st \in P \cap S = \emptyset$, a contradiction.

For (b), let $r \in R$ be nilpotent. Then $r^n = 0$ for some $n \in \mathbb{N}$. Since $r^n = 0 \in P$ for all prime ideals $P \subseteq R$, then $r \in P$ for all prime ideals. Therefore $r \in \bigcap_{\{P | P \subseteq R \text{ is a prime ideal}\}} P$.

Now suppose $r \in \bigcap_{\{P | P \subseteq R \text{ is a prime ideal}\}} P$. Suppose r is not nilpotent.

Then we can define $\mathcal{R} = \{r^n \mid n \in \mathbb{N}\}$. Now define $\mathcal{M} = \{I \subseteq R \setminus \mathcal{R} \mid I \text{ is an ideal of } R\}$. Now let $\mathcal{C}$ be a chain of ideals of $\mathcal{M}$. Then note that $U = \bigcup_{\{U_c \in \mathcal{C}\}} U_c$ is an ideal, an upper bound for $\mathcal{C}$ and $U \cap \mathcal{R} = \emptyset$ since $U_c \cap \mathcal{R} = \emptyset$ for all $U_c \in \mathcal{C}$. Thus $U \in \mathcal{M}$ and by Zorn's lemma $\mathcal{M}$ has a maximal element say M.

Now we want to show that M is a prime ideal and arrive at a contradiction. Suppose $a, b \in R \setminus M$. Then $M \subsetneq M + (a)$ and $M \subsetneq M + (b)$. So $M + (a) \notin \mathcal{M}$ and $M + (b) \notin \mathcal{M}$. So there exists $m, n \in \mathbb{N}$ such that $r^n \in M + (a)$ and $r^m \in M + (b)$. Then $r^{m+n} \in M + (ab) \notin \mathcal{M}$. Therefore $ab \notin M$ and so M is prime, a contradiction to r being contained in all prime ideals of R.

□

54. Let R be a commutative ring with identity and let $x \in R$ be a non-nilpotent element. Prove that there exists a prime ideal P of R such that $x \notin P$.

55. Let R be a commutative ring with identity and let S be the set of all elements of R that are *not* zero-divisors. Show that there is a prime ideal P such that $P \cap S$ is empty. (Hint: Use Zorn's Lemma)

56. Let R be a commutative ring with identity and let $\mathcal{C}$ be a chain of prime ideals of R. Show that $\bigcup_{P \in \mathcal{C}} P$ and $\bigcap_{P \in \mathcal{C}} P$ are prime ideals of R.

57. Let R be a commutative ring and P be aa prime ideal of R. Show that there is a prime ideal $P_0 \subseteq P$ that does not properly contain any prime ideal.

58. Let R be a commutative ring with 1 such that every x in R there is an integer $n > 1$ (depending on x) such that $x^n = x$. Show that every prime ideal of R is maximal.

59. Let R be a commutative ring with 1 in which every ideal is a prime ideal. Prove that R is a field. (Hint: For $a \neq 0$ consider the ideals (a) and (a^2).)

60. Let D be a principal ideal domain. Prove that every nonzero prime ideal of D is a maximal ideal.

61. Show that if R is a finite commutative ring with identity, then every prime ideal of R us a maximal ideal.

62. Let $R = C[0, 1]$ be the ring of all continuous real-valued functions on $[0, 1]$, with addition and multiplication defined as follows. For $f, g \in R$ and $x \in [0, 1]$,
$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x).$$
Prove that if M is a maximal ideal of R, then there is a real number $x_0 \in [0, 1]$ such that $M = \{f \in R \mid f(x_0) = 0\}$.

63. Let R be a commmutative ring with identity, and let $P \subset Q$ be prime ideals of R. Prove there exists prime ideals P^*, Q^* satisfying $P \subseteq P^* \subset Q^* \subseteq Q$, such that there are no prime ideals strictly between P^* and Q^*. (Hint: Fix $x \in Q \setminus P$ and show that there exists a prime ideal P^* containing P, contained in Q and maximal with respect to not containing x.)

64. Let R be a commutative ring eith 1. An ideal I of R is called a *primary* ideal if $I \neq R$ and for all $x, y \in R$ with $xy \in I$, either $x \in R$ or $y^n \in R$ for some integer $n \geq 1$.
    (a) Show that an ideal I of R is primary if and only if $R/I \neq 0$ and every zero-divisor in R/I is nilpotent.
    (b) Show that if I is a primary ideal of R then the radical $\mathrm{Rad}(I)$ of I is a prime ideal. (Recall that $\mathrm{Rad}(I) = \{x \in R \mid x^n \in I \text{ for some } n\}$.)

1.3 Commutative Rings

65. Let R be a commutative ring with identity. Show that R is an integral domain if and only if R is a subring of a field.

66. Let R be a commutative ring with identity. Show that if x and y are nilpotent elements of R then $x + y$ is nilpotent and the set of all nillpotent elements is an ideal in R.

67. Let R be a commutative ring with identity. An ideal I of R is *irreducible* if it cannot be expressed as the intersection of two ideals of R neither of which is contained in the other. Show the following.

    (a) If P is a prime ideal then P is irreducible.

    (b) If x is a non-zero element of R, then there is an ideal I_x, maximal with respect to the property that $x \notin I_x$, and I_x is irreducible.

    (c) If every irreducible ideal of R is a prime ideal, then 0 is the only nilpotent element of R.

68. Let R be a commutative ring with 1 and let I be an ideal of R satisfying $I^2 = \{0\}$. Show that if $a + I \in R/I$ is an idempotent element of R/I, then the coset $a + I$ contains an idempotent element of R.

69. Let R be a commutative ring with identity that has exactly one prime ideal P. Prove the following

    (a) R/P is a field.

    (b) R is isomorphic to R_p, the ring of quotients of R with respect to the multiplicative set $R \setminus P = \{s \in R \mid s \notin P\}$

70. Let R be a commutative ring with identity and $\sigma : R \to R$ a ring automorphism.

    (a) Show that $F = \{r \in R \mid \sigma(R) = r\}$ is a subring of R and the identity of R is in F.

    (b) Show that if σ^2 is the identity map on R, then each element of R is the root of a monic polynomial of degree two in $F[x]$.

71. Let R be a commutative ring with identity that has exactly three ideals $\{0\}$, I, and R.

    (a) Show that if $a \notin I$, then a is a unit of R.

    (b) Show that if $a, b \in I$ then $ab = 0$

72. Let R be a commutative ring with 1. Show that if u is a unit in R and n is nilpotent, then $u + n$ is a unit.

73. Let R be a commutative ring with identity. Suppose that for every $a \in R$, either a or $1 - a$ is invertible. Prove that $N = \{a \in R \mid a \text{ is not invertible}\}$ is an ideal of R.

74. Let R be a commutative ring with 1. Show that the sum of any two principal ideals of R is principal if and only if every finitely generated ideal of R is principal.

75. Let R be a commutative ring with identity such that not every ideal is a principal ideal.

    (a) Show that there is an ideal I maximal with respect to the property that I is not a principal ideal.

    (b) If I is the ideal of part (a), show that R/I is a principal ideal ring.

76. Recall that if $R \subseteq S$ is an inclusion of commutative rings (with the same identity) then an element $s \in S$ is *integral over* R if s satisfies some monic polynomial with coefficients in R. Prove the equivalence of the following statements.

    (a) s is integral over R.

    (b) $R[s]$ is finitely generated as an R-module.

    (c) There exists a faithful $R[s]$ module which is finitely generated as an R-module.

77. Recall that if $R \subseteq S$ is an inclusion of commmutative rings (with the same identity) then S is an *integral* extension of R if every element of S satisfies some monic polynomial with coefficients in R. Prove that if $R \subseteq S \subseteq T$ are commutative rings with the same identity, then S is integral over R and T if and only if T is integral over R.

78. Let $R \subseteq S$ be commutative domains with the same identity, and assime that S is an integral Extension of R. Let I be a nonzero ideal of S. Prove the $I \cap R$ is a nonzero ideal of R.

1.4 Domains

79. Suppose R is a domain and I and J are ideals of R such that IJ is principal. Show that I (and by symmetry J) is finitely generated.

    [Hint: If $IJ = (a)$, then $\sum_{i=1}^{n} x_i y_i$ for some $x_i \in I$ and $y_i \in J$. Show the x_i generate I.]

80. Prove that if D is a Euclidean Domain, then D is a Principal Ideal Domain.

81. Show that if p is a prime such that there is an integer b with $p = b^2 + 4$, then $\mathbb{Z}[\sqrt{p}]$ is not a unique factorization domain.

82. Show that if p is a prime such that $p \equiv 1 (\text{mod } 4)$, then $\mathbb{Z}[\sqrt{p}]$ is not a unique factorization domain.

83. Let $D = \mathbb{Z}(\sqrt{5}) = \{m + n\sqrt{5} \mid m, n \in \mathbb{Z}\}$ - a subring of the field of real numbers and necessarily an integral domain (you need not show this) - and $F = \mathbb{Q}(\sqrt{5})$ its field of fractions. Show the following:

    (a) $x^2 + x - 1$ is irreducible in $D[x]$ but not in $F[x]$.

    (b) D is not a unique factorization domain.

84. Let $D = \mathbb{Z}(\sqrt{21}) = \{m + n\sqrt{21} \mid m, n \in \mathbb{Z}\}$ and $F = \mathbb{Q}(\sqrt{21})$, the field of fractions. Show the following:

    (a) $x^2 - x - 5$ is irreducible in $D[x]$ but not in $F[x]$.

    (b) D is not a unique factorization domain.

85. Let $D = \mathbb{Z}(\sqrt{-11}) = \{m + n\sqrt{-11} \mid m, n \in \mathbb{Z}\}$ and $F = \mathbb{Q}(\sqrt{-11})$, the field of fractions. Show the following:

    (a) $x^2 - x + 3$ is irreducible in $D[x]$ but not in $F[x]$.

    (b) D is not a unique factorization domain.

86. Let $D = \mathbb{Z}(\sqrt{13}) = \{m + n\sqrt{13} \mid m, n \in \mathbb{Z}\}$ and $F = \mathbb{Q}(\sqrt{13})$, the field of fractions. Show the following:

    (a) $x^2 + 3x - 1$ is irreducible in $D[x]$ but not in $F[x]$.

    (b) D is not a unique factorization domain.

87. Let D be an integral domain and F a subring of D that is a field. Show that if each element of D is algebraic over F, then D is a field.

88. Let R be an integral domain containing the subfield F and assume that R is finite dimensional over F when viewed as a vector space over F. Prove that R is a field.

89. Let D be an integral domain.

    (a) For $a, b \in D$ define a *greatest common divisor* of a and b.

    (b) For $x \in D$ denote $(x) = \{dx \mid d \in D\}$. Prove that if $(a) + (b) = (d)$, then d is a greatest common divisor of a and b.

90. Let D be a principal ideal domain.

(a) For $a, b \in D$, define a *least common multiple* of a and b.

(b) Show that $d \in D$ is a least common multiple of a and b if and only if $(a) \cap (b) = (d)$.

91. Let D be a principal ideal domain and let $a, b \in D$.

    (a) Show that there is an element $d \in D$ that satisfies the properties

        i. $d \mid a$ and $d \mid b$ and
        ii. if $e \mid a$ and $e \mid b$ then $e \mid d$

    (b) Show that there is an element $m \in D$ that satisfies the properties

        i. $a \mid m$ and $b \mid m$ and
        ii. if $a \mid e$ and $b \mid e$ then $m \mid e$.

92. Let R be a principal ideal domain. Show that if (a) is a nonzero ideal in R, then htere are only finitely many ideals in R containing (a).

93. Let D be a unique factorization domain and F its field of fractions. Prove that if d is an irreducible element in D, then there are no $x \in F$ such that $x^2 = d$.

94. Let D be a Euclidean domain. Prove that every non-zero prime ideal is a maximal ideal.

95. Let π be an irreducible element of a principal ideal domain R. Prove that π is a prime element (that is, $\pi \mid ab$ implies $\pi \mid a$ or $\pi \mid b$).

96. Let D with $\phi : D \setminus \{0\} \to \mathbb{N}$ be a Euclidean domain. Suppose $\phi(a + b) \leq \max\{\phi(a), \phi(b)\}$ for all $a, b \in D$. Prove that D is either a field or isomorphic to a polynomial ring over a field.

97. Let D be an integral domain and F its field of fractions. Show that if g is an isomorphism of D onto itself, then there is a unique isomorphism h of F onto F such that $h(d) = g(d)$ for all $d \in D$. $(h\mid_D = g)$.

98. Let D be a unique factorization domain such that if p and q are irreducible elements of D, then p and q are associates. Show that if A and B are ideals of D, then either $A \subseteq B$ or $B \subseteq A$.

99. Let D be a unique factorization domain and p a fixed irreducible element of D such that if q is any irreducible element of D, then q is an associate of p. Show the following.

    (a) If d is a nonzero element of D, then d is uniquely expressible in the form up^n, where u is a unit of D and n is a non-negative integer.

    (b) D is a Euclidean domain.

100. Prove that $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.

101. Show that the ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean ring and compute the greatest common divisor of $5 + i$ and 13 using the Euclidean algorithm.

1.5 Polynomial Rings

102. Show that the polynomial $f(x) = x^4 + 5x^2 + 3x + 2$ is irreducible over the field of rational numbers.

103. Let D be an integral domain and $D[x]$ the polynomial ring over D. Suppose $\phi : D[x] \to D$ is an isomorphism such that $\phi(d) = d$ for all $d \in D$. Show that $\phi(x) = ax + b$ for some $a, b \in D$ and that a is a unit of D.

104. Let $f(x) = a_0 + a_1x + \ldots + a_kx^k + \ldots + a_nx^n \in \mathbb{Z}[x]$ and p a prime such that $p \mid a_i$ for $i = 1, \ldots, k-1$, $p \nmid a_k$, $p \nmid a_n$, and $p^2 \nmid a_0$. Show that $f(x)$ has an irreducible factor in $\mathbb{Z}[x]$ of degree at least k.

105. Let D be an integral domain and $D[x]$ the polynomial ring over D in the indeterminate x. Show that if every nonzero prime ideal of $D[x]$ is a maximal ideal, then D is a field.

106. Let R be a commutative ring with 1 and let $f(x) \in R[x]$ be nilpotent. Show that the coefficients of f are nilpotent.

107. Show that if R is an integral domain and $f(x)$ is a unit in the polynomial ring $R[x]$, then $f(x)$ is in R.

108. Let D be a unique factorization domain and F its field of fractions. Prove that if $f(x)$ is a monic polynomial in $D[x]$ and $\alpha \in F$ is a root of f, then $\alpha \in D$.

109. (a) Show that $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$.
   (b) Show that $x^4 + 1$ is not irreducible in $\mathbb{Z}_3[x]$.

110. Let $F[x, y]$ be the polynomial ring over a field F in two indeterminates x, y. Show that the ideal generated by $\{x, y\}$ is not a principal ideal.

111. Let F be a field. Prove that the polynomial ring $F[x]$ is a PID and that $F[x, y]$ is not a PID.

112. Let D be an integral domain and let c be an irreducible element in D. Show that the ideal (x, c) generated by x and c in the polynomial ring $D[x]$ is not a principal ideal.

113. Show that if R is a commutative ring with 1 that is not a field. then $R[x]$ is not a principal ideal domain.

114. (a) Let $\mathbb{Z}[\frac{1}{2}] = \left\{\frac{a}{2^n} \mid a, n \in \mathbb{Z}, n \geq 0\right\}$, the smallest subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and $\frac{1}{2}$. Let $(2x-1)$ be the ideal of $\mathbb{Z}[x]$ generated by the polynomial $2x - 1$. Show that $\mathbb{Z}[x]/(2x-1) \cong \mathbb{Z}[\frac{1}{2}]$.
   (b) Find an ideal I of $\mathbb{Z}[x]$ such that $(2x-1) \subsetneq I \subsetneq \mathbb{Z}[x]$

1.6 Non-commutative Rings

115. Let R be a ring with identity such that the identity map is the only ring automorphism of R. Prove that the set N of all nilpotent elements of R is an ideal of R.

116. Let p be a prime. A ring S is called a *p-ring* if the characteristic of S is a power of p. Show that if R is a ring with identity of finite characteristic, then R is isomorphic to a finite direct product of p-rings for distinct primes.

117. If R is any ring with identity, let $J(R)$ denote the Jacobson radical of R. Show that if e is any idempotent of R, then $J(eRe) = eJ(R)e$.

118. If n is a positive integer and F is any field, let $M_n(F)$ denote the ring of $n \times n$ matrices with entries in F. Prove that $M_n(F)$ is a simple ring. Equivalently, $\mathrm{End}_F(V)$ is a simple ring if V is a finite dimensional vector space over F.

119. Let R be a ring.
   (a) Show that there is a unique smallest (with respect to inclusion) ideal A such that R/A is a commutative ring.
   (b) Give an example of a ring R such that for every proper ideal I, R/I is not commutative. Verify your example.
   (c) For the ring $R = \left\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z}\right\}$ with the usual matrix operations, find the ideal of A of part (a).

120. A ring R is *nilpotent-free* if $a^n = 0$ for $a \in R$ and some positive integer n implies $a = 0$.
   (a) Suppose there is an ideal I such that R/I is nilpotent-free. Show there is a unique smallest (with respect to inclusion) ideal A such that R/A is nilpotent-free.
   (b) Give an example of a ring R such that for every proper ideal I, R/I is not nilpotent-free. Verify your example.
   (c) Show that if R is a commutative ring with identity, then there is a proper ideal I of R such that R/I is nilpotent-free, and find the ideal A of part (a).

1.7 Local Rings, Localization, Rings of Fractions

121. Let R be an integral domain. Construct the field of fractions F of R by defining the set F and the two binary operations, and show that the two operations are well-defined. Show that F has a multiplicative identity element and that every nonzero element of F has a multiplicative inverse.

122. A *local* ring is a commutative ring with 1 that has a unique maximal ideal. Show that a ring R is local if and only if the set of non-units in R is an ideal.

123. Let R be a commutative ring with $1 \neq 0$ in which the set of nonunits is closed under addition. Prove that R is local, i.e., has a unique maximal ideal.

124. Let D be an integral domain and F its field of fractions. Let P be a prime ideal in D and $D_P = \{ab^{-1} \mid a, b \in D, b \notin P\} \subseteq F$. Show that D_P has a unique maximal ideal.

125. Let R he a commutative ring with identity and M a maximal ideal of R. Let R_M be the ring of quotients of R with respect ot the multiplicative set $R \setminus M = \{s \in R \mid s \notin M\}$. Show the following.
    (a) $M_M = \{\frac{a}{s} \mid a \in M, s \notin M\}$ is the unique maximal ideal of R_M.
    (b) The fields R/M and R_M/M_M are isomorphic.

126. Let R be an integral domain, S a multiplicative set, and let $S^{-1}R = \{\frac{r}{s} \mid r \in R, s \in S\}$ (contained in the field of fractions of R). Show that if P is a prime ideal of R, then $S^{-1}P$ is either a prime ideal of $S^{-1}R$ or else equals $S^{-1}R$.

127. Let R be a commutative ring with identity and P a prime ideal of R. Let R_P be the ring of quotients of R with respect to the set $R \setminus P = \{s \in R \mid s \notin P\}$. Show that R_P/P_P is the field of fractions of the integral domain R/P.

128. Let D be an integral domain and F its field of fractions. Denote by $\mathcal{M}$ the set of all maximal ideals of D. For $M \in \mathcal{M}$, let $D_M = \{\frac{a}{s} \mid a, s \in D, s \notin M\} \subset F$. Show that $\bigcap_{M \in \mathcal{M}} D_M = D$.

129. Let R be a commutative ring with 1 and D a multiplicative subset of R containing 1. Let J be an ideal in the ring of fractions $D^{-1}R$ and let
$$I = \left\{a \in R \mid \frac{a}{d} \in J \text{ for some } d \in D\right\}.$$
    Show that I is an ideal of R.

130. Let D be a principal ideal domain and let P be a non-zero prime ideal. Show that D_P, the localization of D at P, is a principal ideal domain and has a unique irreducible element, up to associates.

1.8 Chains and Chain Conditions

131. Let R be a commutative ring with identity. Prove that any non-empty set of prime ideals of R contains maximal *and* minimal elements.

132. Let R be a commutative ring with 1. We say R satisfies the *ascending chain condition* if whenever $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is an ascending chain of ideals, there is an integer N such that $I_k = I_N$ for all $k \geq N$. Show that R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

133. Define *Noetherian ring* and prove that if R is Noetherian, then $R[x]$ is Noetherian.

134. Let R be a commutative Noetherian ring with identity. Prove that there are only finitely many *minimal* prime ideals of R.

135. Let R be a commutative Noetherian ring in which every 2-generated ideal is principal. Prove that R is a Principal Ideal Domain.

136. Let R be a commutative Noetherian ring with identity and let I be an ideal in R. Let $J = \text{Rad}(I)$. Prove that there exists a positive integer n such that $j^n \in I$ for all $j \in J$.

137. Let R be a commutative Noetherian domain with identity. Prove that every nonzero ideal of R conatains a product of nonzero *prime* ideals of R.

138. Let R be a ring satisfying the *descending chain condition* on right ideals. If $J(R)$ denotes the Jacobson radical of R, prove that $J(R)$ is nilpotent.

139. Show that if R is a commutative Noetherian ring with identity, then the polynomial ring $R[x]$ is also Noetherian.

140. Let P be a nonzero prime ideal of the commutative Noetherian domain R. Assume P is principal. Prove that there does not exist a prime ideal Q satisfying $(0) < Q < P$.

141. Let R be a commutative Noetherian ring. Prove that every nonzero ideal A of R contains a product of prime ideals (not necessarily distinct) each of which contains A.

142. Let R be a commutative ring with 1 and let M be an R-module that is not Artinian (Noetherian, of finite composition length). Let $\mathcal{I}$ be the set of ideals I of R such that there exists and R-submodule N of M with the property that N/NI is not Artinian (Noetherian, of finite composition length, respectively). Show that if $A \in \mathcal{I}$ is a maximal element of $\mathcal{I}$, then A is a prime ideal of R.