Exercises for Basic Algebra (MA 419)
IIT Mumbai, M.K. Keshari

1. If G is a group such that $(a.b)^i = a^i.b^i$ for three consecutive integers i, and for all $a, b \in G$, then G is abelian.

   Give an example to show that if the above holds for only two consecutive integers, then G may not be abelian.

2. Suppose H is a subgroup of G such that whenever $Ha \neq Hb$ then $aH \neq bH$. Prove that $gHg^{-1} \subset H$ for all $g \in G$.

3. If H is a subgroup of finite index in G, prove that there is only a finite number of distinct subgroups in G of the form aHa^{-1}.

4. If H is of finite index in G, prove that there is a subgroup N of G contained in H and of finite index in G such that $aNa^{-1} = N$ for all $a \in G$. Can you give an upper bound for the index of this N in G?

5. Let G be a finite group whose order is not divisible by 3. Suppose that $(ab)^3 = a^3b^3$ for all $a, b \in G$. Show that G is abelian.

6. Let G be an abelian group which has elements of order m, n. Show that G has an element of order $\mathrm{lcm}(m, n)$.

7. If an abelian group has subgroups of order m, n, then it has a subgroup of order $\mathrm{lcm}(m, n)$.

8. Let $U_n = (\mathbb{Z}/n\mathbb{Z})^\times$. Show that U_8, U_{20} are not cyclic groups, $U_9, U_{17}, U_{18}, U_{25}, U_{27}$ are cyclic groups.

   For what values of n, U_n is cyclic?

9. Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = 1$ is atmost n for every positive integer n. Prove that G must be a cyclic group.

10. Every subgroup of an abelian group is normal. Is the converse true?

11. Give an example of three groups $E \subset F \subset G$, where E is normal in F, F is normal in G, but E is not normal in G.

12. Let $U = \{xyx^{-1}y^{-1} | x, y \in G\}$ and G' is the subgroup generated by U, called the "commutator subgroup" of G. Prove that G' is a normal subgroup of G and G/G' is abelian. Further, if G/N is abelian then $G' \subset N$. Also, if $H < G$ and H contains G', then H is normal in G.

13. A subgroup C of G is called a "characteristic subgroup" of G if $\sigma(C) \subset C$ for all automorphism σ of G. Prove that a characteristic subgroup of G must be normal.

    Show that the converse may not hold.

14. Let $E \subset F \subset G$ be groups such that E is characteristic subgroup of F and F is normal in G, then E is normal in G.

15. Every finite group having more than two elements has a non-trivial automorphism.

16. Let G be a group of order $2n$. Suppose half the elements of G are of order 2, and the other half form a subgroup H of order n. Prove that H is of odd order and is an abelian subgroup of G.

17. If $a > 1$ is an integer then $n/\varphi(a^n - 1)$, where φ is the Euler function.

18. Let G be a group of order pq, $p > q$ are primes. Prove that
    (i) G has a subgroup of order p and a subgroup of order q,
    (ii) If $q \not| p-1$, then G is cyclic,
    (iii) Given two primes p, q such that $q/(p-1)$, $\exists$ a non-abelian group of order pq,
    (iv) any two non-abelian group of order pq are isomorphic.

19. (i) For $n \geq 3$, the subgroup generated by 3-cycles is A_n.
    (ii) A_5 has no non-trivial normal subgroup.
    (iii) Any proper subgroup of A_5 has order atmost 12.

20. List all the conjugate classes in D_{2n} and verify the class equation.

21. If G is a group of order p^n and H is a proper subgroup of G. Show that $\exists x \in G - H$ such that $xHx^{-1} = H$.

22. If G is a group of order p^n, p : prime, and N is a non-trivial normal subgroup of G, then $Z(G) \cap N \neq 1$.

23. Let G be a group of order pqr, $p < q < r$ primes. Prove that
    (i) the r-Sylow subgroup is normal in G,
    (ii) G has a normal subgroup of order qr,
    (iii) if $q \not| (r-1)$, the q-Sylow subgroup of G is normal in G.

24. If G is a group of order p^2q, p, q : primes, then G has a non-trivial normal subgroup. Further either a $p-$Sylow subgroup or a q-Sylow subgroup of G must be normal in G.

25. If P is a p-Sylow subgroup of G, then $N_G(N_G(P)) = N_G(P)$.

26. Let G be a finite abelian group such that it contains a subgroup $H_0 \neq 1$ which lies in every subgroup $H \neq 1$. Prove that G must be cyclic. What can you say about the order of G?

27. Let $G = A \times A$, where A is cyclic of order p : prime. Find the number of automorphism of G.

28. Let G be a finite abelian group with elements $a_1, \ldots, a_n$. Prove that $a_1 a_2 \ldots a_n$ is an element whose square is identity. Further, if G has no element of order 2 or more than one element of order 2, then $a_1 a_2 \ldots a_n = 1$. Prove that if p is a prime integer, then $(p-1)! = -1 \bmod (p)$ (Wilson's theorem).

29. Give an example of a non-abelian group G such that $(xy)^3 = x^3 y^3$ for all $x, y \in G$.

30. A group can not be written as the set theoretic union of two proper subgroups.

31. (a) If G is a finite group and if P is a p-Sylow subgroup of G, prove that P is the only p-Sylow subgroup in $N_G(P)$.
(b) If P is a p-Sylow subgroup of G and if $a^{p^k} = 1$, then if $a \in N_G(P)$, then $a \in P$.

32. Every group of order < 60 either is of prime order of has a non-trivial normal subgroup.

33. The normalizer of a proper subgroup A of a p-group G contains A properly.

34. If p, q are primes and $|G| = p^a q$, then G has a non-trivial normal subgroup.

35. Let G be a group which acts on a set A. Prove that if $a, b \in A$ and $b = g.a$ for some $g \in G$, then $G_b = gG_a g^{-1}$, where G_a is the stabilizer of a. Deduce that if G acts transitively on A, then the kernel of the action is $\cap_{g \in G} g G_a g^{-1}$.

36. Let G be a permutation group on the set A, i.e. $G < S_A$. Let $\sigma \in G$ and $a \in A$. Prove that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then $\cap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1$.

37. Assume that G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and $a \in A$. Deduce that $|G| = |A|$.

38. List the elements of S_3 as $1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$ and label them with integers $1, \ldots, 6$. Exhibit the image of each element of S_3 under the left regular representation of S_3 into S_6.

39. Let Q_8 be the quaternion group of order 8.
(a) Prove that Q_8 is isomorphic to a subgroup of S_8.
(b) Prove that Q_8 is not isomorphic to a subgroup of S_n for $n \leq 7$. (If Q_8 acts on any set A of order ≤ 7, show that the stabilizer of any point must contain the subgroup (-1).)

40. Prove that if H has finite index n in G, then there is a normal subgroup K of G with $K \subset H$ and $|G : K| \leq n!$.

41. Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

42. Prove that every non-abelian group of order 6 has a non-normal subgroup of order 2. Use this to classify groups of order 6. (Produce an injective homomorphism into S_3).

43. Let G be a finite group and let $\pi : G \to S_G$ be the left regular representation. Prove that if $x \in G$ has order n and $|G| = mn$, then $\pi(x)$is a product of m n-cycles. Deduce that $\pi(x)$ is an odd permutation iff $|x|$ is even and $|G|/|x|$ is odd.

44. Prove that if $S \subset G$ and $g \in G$, then $gN_G(S)g^{-1} = N_G(gSg^{-1})$ and $gC_G(S)g^{-1} = C_G(gSg^{-1})$.

45. If the center of G is of index n, prove that every conjugacy class has atmost n elements.

46. Let $\sigma = (1, 2, 3, 4, 5) \in S_5$. Find $\tau \in S_5$ such that $\tau\sigma\tau^{-1} = \sigma^{-1}$.

47. Assume H is a proper subgroup of the finite group G. Prove $G \neq \cup_{g\in G}\, gHg^{-1}$.

48. Let G be a transitive permutation group on the finite set A with $|A| > 1$. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$. (Such a σ is called "fixed point free".)

49. Let $g_1, \ldots, g_r$ be representatives of the conjugacy classes of the finite group G and assume there elements commute pairwise. Prove that G is abelian.

50. If G is a group of odd order, then for $x \neq 1 \in G$, x and x^{-1} are not conjugate in G.

51. Show that for $n = 2k$, the conjugacy classes in D_{2n} are the following: $\{1\}, \{r^k\}, \{r^{\pm 1}\}, \ldots,$ $\{r^{\pm(k-1)}\}, \{sr^{2b} | b = 1, \ldots, k\}$. Give the class equation for D_{2n}.

52. Show that for $n = 2k + 1$, the conjugacy classes in D_{2n} are the following: $\{1\}, \{r^{\pm 1}\}, \ldots,$ $\{r^{\pm k}\}, \{sr^b | b = 1, \ldots, n\}$. Give the class equation for D_{2n}.

53. If H is the unique subgroup of a given order in a group G, then H is the characteristic subgroup of G.

54. Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of D_{12} and $S_3 \times S_3$.

55. Show that a Sylow p-subgroup of D_{2n} is cyclic and normal for every odd prime p.

56. Exhibit all Sylow 3-subgroups of A_4 and S_4.

57. Exhibit two distinct Sylow 2-subgroups of S_5 and an element of S_5 that conjugates one into other.

58. If G is a simple group of order 60, then $G \xrightarrow{\sim} A_5$.

59. If G is a non-abelian simple group of order < 100, then $G \xrightarrow{\sim} A_5$.

60. (a) If $|G| = 105$, then G has normal Sylow 5-subgroup and a normal Sylow 7-subgroup.
(b) If $|G| = 200$, then G has a normal Sylow 5-subgroup.
(c) If $|G| = 56$, then G has a normal Sylow p-subgroup for some prime $p/|G|$.

61. If $|G| = 6545, 1365, 2907, 132, 462$, then G has a non-trivial normal subgroup, i.e. G is not simple.

62. If $|G| = 231$, then $Z(G)$ contains a Sylow 11-subgroup of G and a Sylow 7-subgroup is normal in G.

63. If $|G| = 105$ and a 3-Sylow subgroup of G is normal in G, then G is abelian.

64. How many elements of order 7 must be there in a simple group of order 168.

65. Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If P is a normal subgroup of H and H is a normal subgroup of K, then P is normal in K. Deduce that if $P \in Syl_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$ (i.e. normalizers of Sylow p-subgroups are self-normalizing).

66. Let P be a normal Sylow p-subgroup of G and let H be any subgroup of G. Then $P \cap H$ is the unique Sylow p-subgroup of H.

67. Let R be a normal p-subgroup of G (not necessarily a Sylow subgroup).
   (a) Prove that R is contained in every Sylow p-subgroup of G.
   (b) If S is another normal p-subgroup of G, then RS is also a normal p-subgroup of G.
   (c) The subgroup $O_p(G)$ which is generated by all normal p-subgroups of G is the unique largest normal p-subgroup of G and equals the intersection of all Sylow p-subgroups of G.
   (d) Let $\overline{G} = G/O_p(G)$. Then $O_p(\overline{G}) = \overline{1}$.

68. Prove that if p is a prime and P is a subgroup of S_p of order p, then $|N_{S_p}(P)| = p(p-1)$. (Argue that every conjugate of P contains exactly $p-1$ p-cycles and use the formula for the number of p-cycles to compute the index of $N_{S_p}(P)$ in S_p.)

69. Prove that if p is a prime and P is a subgroup of S_p of order p, then $N_{S_p}(P)/C_{S_p}(P) \xrightarrow{\sim} \mathrm{Aut}(P)$.

70. Prove that if $\sigma \in \mathrm{Aut}(G)$ and φ_g is conjugation by g, then $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. (The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the "outer automorphism group of G.)

71. Prove that under any automorphism of D_8, r has atmost 2 possible images and s has at most 4 possible images. Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.

72. Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G, then $H \subset Z(G)$. Deduce that G is abelian in this case.

73. Show that $Z(G_1 \times \ldots \times G_n) = Z(G_1) \times \ldots \times Z(G_n)$.

74. Let A, B be finite groups and let p be a prime. Prove that any Sylow p-subgroup of $A \times B$ is of the form $P \times Q$, where $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. Prove that $n_p(A \times B) = n_p(A).n_p(B)$.

75. Let $\pi \in S_n$. Prove that $\varphi_\pi : G_1 \times \ldots \times G_n \to G_{\pi^{-1}(1)} \times \ldots \times G_{\pi^{-1}(n)}$ defined by $\varphi_\pi(g_1, \ldots, g_n) = (g_{\pi^{-1}(1)}, \ldots, g_{\pi^{-1}(n)})$ is an isomorphism.

76. Let $G_1 = \ldots = G_n$ and $G = G_1 \times \ldots \times G_n$. Show that $\varphi_\pi \in \mathrm{Aut}(G)$. Show that the map $\pi \mapsto \varphi_\pi$ is an injective homomorphism of S_n into $\mathrm{Aut}(G)$.

77. Let p be a prime. Let A and B be two cyclic groups of order p with generators x and y respectively. Let $E = A \times B$ be the elementary abelian group of order p^2. Prove that the distinct subgroups of E of order p are $< x >, < xy >, < xy^2 >, \ldots, < xy^{p-1} >, < y >$. (there are $p+1$ of them.)

78. Let p be a prime. Find the number of subgroups of order p in the elementary abelian group E_{p^n}.

79. Let $G = A_1 \times \ldots \times A_n$ and let B_i be a normal subgroup of A_i. Prove that $B = B_1 \times \ldots \times B_n$ is a normal subgroup of G and $G/B \xrightarrow{\sim} (A_1/B_1) \times \ldots \times (A_n/B_n)$.

80. Find the number of non-isomorphic abelian groups of order 100, 576, 1155, 42875, 2704. Further, give the list of their invariant factors.

81. For $x, y \in G$, prove that $[y, x] = [x, y]^{-1}$. Deduce that for any subsets A, B of G, $[A, B] = [B, A]$.

82. Find the commutator subgroups of S_4 and A_4.

83. Prove that if p is a prime and P is a non-abelian group of order p^3, then $P' = [P, P] = Z(P)$.

84. Prove that if $G = HK$, where H, K are characteristic subgroups of G with $H \cap K = 1$, then $\mathrm{Aut}(G) \xrightarrow{\sim} \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Deduce that if G is an abelian group of finite order then $\mathrm{Aut}(G)$ is isomorphic to the direct product of the automorphism groups of its Sylow subgroups.

85. Prove that D_{8n} is not isomorphic to $D_{4n} \times Z_2$.

86. If A, B are normal subgroups of G such that G/A and G/B are both abelian, prove that $G/(A \cap B)$ is abelian.

87. Prove that if K is normal in G, then $K' = [K, K]$ is normal in G.

88. Prove that the center of a ring is a subring and the center of a division ring is a field.

89. Show that if R is a commutative ring and $x \in R$ is nilpotent, then (i) either $x = 0$ or x is a zero divisor, (ii) rx is nilpotent for all $r \in R$, (iii) $1 + x$ is a unit in R, (iv) sum of a nilpotent element and a unit is a unit.

90. A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative and the only Boolean rings that are integral domain is $\mathbb{Z}/2\mathbb{Z}$.

91. Let I be any nonempty index set and let R_i be a ring for each $i \in I$. Prove that the direct product $\prod_{i\in I} R_i$ is a ring under componentwise addition and multiplication.

92. Let R be the collection of sequences $(a_1, a_2, \ldots)$ of integers $a_1, a_2, \ldots$ where all but finitely many of the a_i's are 0. Prove that R is a ring under componentwise addition and multiplication which does not have an identity element. (R is called the direct sum of infinitely many copies of $\mathbb{Z}$).

93. Give an example of an infinite Boolean ring.

94. Let D be a square free integer and let $\mathcal{O}$ be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. For any positive integer n prove that $\mathcal{O}_n := \mathbb{Z}[nw] = \{a + bnw | a, b \in \mathbb{Z}\}$ is a subring of $\mathcal{O}$ containing the identity. Prove that $|\mathcal{O} : \mathcal{O}_n| = n$ as abelian groups. Conversely prove that a subring of $\mathcal{O}$ containing the identity and having finite index n is equal to $\mathcal{O}_n$. ($\mathcal{O}_n$ is called the order of conductor n in the field $\mathbb{Q}(\sqrt{D})$ and $\mathcal{O}$ is called the maximal order in $\mathbb{Q}(\sqrt{D})$.)

95. Let $A = \mathbb{Z}\times\mathbb{Z}\times\ldots$ be the direct product of infinite copies of $\mathbb{Z}$ and let R be the ring of all group homomorphisms from A to itself. Let $\varphi, \psi \in R$ defined by $\varphi(a_1, a_2, \ldots) = (a_2, a_3, \ldots)$ and $\psi(a_1, a_2, \ldots) = (0, a_1, a_2, \ldots)$.
(i) Prove that $\varphi\psi$ is identity of R but $\psi\varphi$ is not identity of R.
(ii) Exhibit infinitely many right inverses for φ.
(iii) Find a nonzero element $\pi \in R$ such that $\varphi\pi = 0$ but $\pi\varphi \neq 0$.
(iv) Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\varphi = 0$ (so φ is a left zero divisor but not a right zero divisor).

96. Let R be a commutative ring with 1. Define the set $R[[x]]$ of "formal power series" in the indeterminate x with coefficients from R to be all formal infinite sums $\sum_0^\infty a_n x^n$. Define the addition and multiplication as $\sum_0^\infty a_n x^n + \sum_0^\infty b_n x^n = \sum_0^\infty (a_n + b_n)x^n$ and $(\sum_0^\infty a_n x^n).(\sum_0^\infty b_n x^n) = \sum_0^\infty c_n x^n$ where $c_n = \sum_0^n a_k b_{n-k}$.
(i) Prove that $R[[x]]$ is a commutative ring with 1.
(ii) Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \ldots$.
(iii) Prove that $\sum_0^\infty a_n x^n$ is a unit in $R[[x]]$ iff a_0 is a unit in R.

97. If R is an integral domain then show that $R[[x]]$ is also an integral domain.

98. Let F be a field and define the ring $F((x))$ of "formal Laurent series" with coefficients from F by $F((x)) = \{\sum_{n\geq N}^\infty a_n x^n | \, a_n \in F, N \in \mathbb{Z}\}$. (Every element of $F((x))$ is a power series in x plus a polynomial in $1/x$.) Prove that $F((x))$ is a field.

99. Prove that the center of the ring $M_n(R)$ is the set of scalar matrices (R is commutative ring with 1).

100. Let $G = \{g_1, \ldots, g_n\}$ be a finite group. Prove that the element $N = g_1 + \ldots + g_n \in Z(RG)$.

101. Let $\mathcal{K} = \{k_1, \ldots, k_m\}$ be a conjugacy class in the finite group G.
(i) Prove that the element $x = k_1 + \ldots + k_m \in Z(RG)$. [Hint: Check that $gxg^{-1} = x$ for all $g \in G$]
(ii) Let $\mathcal{K}_1, \ldots, CK_r$ be the conjugacy classes of G and for each $\mathcal{K}_i$, let x_i be the element of RG that is the sum of the members of $\mathcal{K}_i$. Prove that $\alpha \in RG$ is in $Z(RG)$ iff $\alpha = a_1x_1 + \ldots + a_rx_r$ for some $a_i \in R$.

102. Find all ring homomorphisms from $\mathbb{Z}/20\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

103. Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

104. Show that every two-sided ideal of $M_n(R)$ is equal to $M_n(J)$ for some ideal J of R. [Hint: Show that the set of entries of matrices in an ideal of $M_n(R)$ form an ideal of R.]

105. Let $\varphi : R \to S$ be a ring homomorphism. (i) Prove that if J is an ideal of S, then $\varphi^{-1}(J)$ is an ideal of R.
(ii) Prove that if φ is surjective and I is an ideal of R, then $\varphi(I)$ is an ideal of S. Give an example where this fails if φ is not surjective.

106. The "characteristic" of a ring is the smallest positive integer n such that $1 + \ldots + 1 = 0$ (n times). If no such n exists, characteristic of R is 0. E.g. characteristic of $\mathbb{Z}/n\mathbb{Z}$ is n and characteristic of $\mathbb{Z}$ is 0.
(i) Prove the the map $\mathbb{Z} \to R$ defined as $k \mapsto k.1$ is a ring homomorphism with kernel $n\mathbb{Z}$, where n is the characteristic of R.
(ii) Determine the characteristic of the rings $\mathbb{Q}, \mathbb{Z}[x], \mathbb{Z}/n\mathbb{Z}[x]$.
(iii) Prove that if R is commutative and has characteristic a prime p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

107. Prove that a nonzero Boolean ring has characteristic 2.

108. Prove that an integral domain has characteristic 0 or a prime p.

109. Let R be commutative. Show that the set of nilpotent elements form an ideal, called the nil radical of R.

110. Assume R is commutative and $p(x) = a_nx^n + \ldots + a_1x + a_0 \in R[x]$.
(i) Prove that $p(x)$ is a unit in $R[x]$ iff a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent in R.
(ii) $p(x)$ is nilpotent in $R[x]$ iff $a_0, \ldots, a_n$ are nilpotent in $R[x]$.

111. Let R be a ring in which $x^3 = x$ for all $x \in R$. Show that R is commutative.

112. If R is a finite commutative ring with unity, then every prime ideal of R is maximal.

113. Let L_j be the left ideal of $M_n(R)$ consisting of arbitrary entries in the j^{th} column and zero elsewhere and let $E_{i,j}$ be the element of $M_n(R)$ with 1 at (i, j) entry and zero elsewhere. Prove that $L_j = M_n(R)E_{ij}$ for any i.

114. (i) Prove that every prime ideal is a maximal ideal in a Boolean ring.
(ii) Every finitely generated ideal in a Boolean ring is principal.

115. Let R be commutative and for each $a \in R$, there is a positive integer n such that $a^n = a$. Prove that every prime ideal of R is maximal.

116. Prove that the nilradical of a commutative ring R is equal to the intersection of all the prime ideals of R.

117. Let R be a commutative ring with $1 \neq 0$. If $a \in R$ is nilpotent then $1 - ab$ is a unit for all $b \in R$.

118. Let R be commutative and I an ideal of R. Define radical of I as $\text{rad}(I) = \{r \in R | r^n \in I$ for some $n > 0\}$. Prove that $\text{rad}(I)$ is an ideal of R containing I and $\text{rad}(I)/I$ is the nil radical of R/I.

119. An ideal I is called a radical ideal if $rad(I) = I$. Show every prime ideal of R is a radical ideal. Show $n\mathbb{Z}$ is a radical ideal of $\mathbb{Z}$ iff n is the product of distinct primes in $\mathbb{Z}$.

120. Let R be commutative and I an ideal. Define $\text{Jac}(I)$ as intersection of all maximal ideals containing I. $\text{Jac}(0)$ is called the Jacobson radical of R.
(i) Show that $\text{Jac}(I)$ is an ideal of R containing I.
(ii) Show that $\text{rad}(I) \subset \text{Jac}(I)$.
(iii) Describe $\text{Jac}(n\mathbb{Z})$ in terms of the prime factorization of n.

121. Let R be the ring of continuous functions from $[0,1]$ to $\mathbb{R}$ and for $c \in [0,1]$, define M_c as the set of all elements of R which vanishes at c.
(i) Show that M_c is a maximal ideal of R. Conversely, if M is any maximal ideal of R, there is some $c \in [0,1]$ such that $M = M_c$.
(ii) If $b, c \in [0,1]$ are distinct, then $M_c \neq M_b$.
(iii) Show that M_c is not equal to the ideal generated by $(x - c)$.
(iv) Prove that M_c is not a finitely generated ideal.

122. Let R be the ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and for each $c \in \mathbb{R}$, let M_c be the maximal ideal $\{f \in R | f(c) = 0\}$.
(i) Let I be the collection of functions f in R with compact support, i.e $f(x)$ vanishes for $|x|$ sufficiently large. Show that I is an ideal of R and is not a prime ideal.
(ii) Let M be a maximal ideal of R containing I, then $M \neq M_c$ for any $c \in \mathbb{R}$.

123. Let R be an integral domain and let D be a non-empty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R.

124. Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p (F_0 is called the "prime subfield" of F). Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

125. If F is a field, prove that the field of fractions of $F[[x]]$ (the ring of formal power series in the indeterminate x and coefficients in F) is the ring $F((x))$ of formal Laurent series. Show that the field of fractions of the power series ring $\mathbb{Z}[[x]]$ is "properly" contained in $\mathbb{Q}((x))$ (e.g. e^x).

126. * Prove that $\mathbb{R}$ contains a subring A with $1 \in A$ and A maximal (under inclusion) w.r.t. the property that $1/2 \notin A$ (Use Zorn's lemma). Let K be the field of fractions of A in $\mathbb{R}$.
(i) Show that $\mathbb{R}$ is algebraic over K. (If t is transcendental over K, then $1/2 \notin A[t]$)
(ii) Show that A is integrally closed in $\mathbb{R}$. (Show that $1/2$ is not in the integral closure of A in $\mathbb{R}$) (iii) Deduce that $\mathbb{R} = K$. Hence $\mathbb{R}$ is the quotient field of a proper subring.

127. An element $e \in R$ is called an "idempotent" if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \xrightarrow{\sim} Re \times R(1-e)$. Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$.

128. (i) Let R, S be rings with 1. Prove that every ideal of $R \times S$ is of the form $I \times J$ for some ideals I, J of R, S respectively.
(ii) If R, S are non-zero rings, then $R \times S$ is never a field.
(iii) Let R be a finite Boolean ring. Prove that $R \xrightarrow{\sim} \prod_1^n \mathbb{Z}/2\mathbb{Z}$.

129. Solve the simultaneous system of congruences (i) $x = 1 \bmod 8$, $x = 2 \bmod 25$, $x = 3 \bmod 81$ and (ii) $y = 5 \bmod 8$, $y = 12 \bmod 25$, $y = 47 \bmod 81$.

130. Let $f_1(x), \ldots, f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, \ldots, n_k$ be integers which are pairwise comaximal. Use Chinese remainder theorem to prove that there exists a polynomial $f(x)$ with integer coefficients and of degree d with $f(x) = f_1(x) \bmod n_1, \ldots, f(x) = f_k(x) \bmod n_k$. Show that if $f_i(x)$ are monic then we can choose monic $f(x)$.

131. Let m, n be positive integers with n dividing m. Prove that the natural surjective ring projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is also surjective on the units $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$

132. Let (a) $a = 13, n = 20$, (b) $a = 69, n = 89$. Show that a, n are coprime. Find the inverse of a mod n.

133. Let R be a Euclidean domain. Let m be the minimum ineger in the set of norms of non-zero elements of R. Prove that every non-zero element of R of norm m is a unit. Deduce that a non-zero element of norm 0 is a unit.

134. Let R be a Euclidean domain. Prove that if $\gcd(a, b) = 1$ and a/bc then a/c. More generally, if a/bc with non-zero b, c, then $a/gcd(a, b)$ divides c.

135. Let $R = \mathbb{Z}$ and consider the Diophantine equation $ax + by = N$ where a, b are non zero. Suppose x_0, y_0 is a solution. Prove that the full set of solutions of this equation is given by $x = x_0 + m\frac{b}{(a,b)}$ and $y = y_0 - m\frac{a}{(a,b)}$ as $m \in \mathbb{Z}$. [If x, y is a solution, then $a(x - x_0) = b(y_0 - y)$ and use previous exercise.]

136. Find all integer solutions of $17x + 29y = 31$.

137. Find a generator for the ideal $(85, 1 + 13i)$ in $\mathbb{Z}[i]$, i.e. $\gcd(85, 1 + 13i)$ by the Euclidean algorithm.

Theorem The only negative values of D for which the ring of integers $\mathcal{O}$ is PID if $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$.

138. (i) For $D = -1, -2, -3, -7, -11$, $\mathcal{O}$ is a Euclidean domain wrt field norm N. [Modify the proof for $D = -1$]
(ii) For $D = -43, -67, -163$, $\mathcal{O}$ is not a Euclidean domain with respect to any norm. [Modify the proof for $D = -19$]

139. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any non-zero ideal I.

140. Let $a, b \in R$ be non zero. A "least common multipal" of a, b is an element $e \in R$ such that (i) $a/e, b/e$ and (ii) if $a/e', b/e'$ then e/e'.
(a) Prove that $\text{lcm}(a, b)$ if exists, is a generator for the unique largest principal ideal contained in $(a) \cap (b)$.
(b) Any two non-zero elements in a Euclidean domain have a lcm which is unique upto multiplication by a unit.
(c) In a Euclidean domain, $\text{lcm}(a, b) = ab/gcd(a, b)$.

141. Show that any two non-zero elements of a PID have a least common multiple.

142. Let R be an integral domain. Prove that R is a PID if (i) any two non-zero elements $a, b \in R$ have a gcd which can be written in the form $ra + sb$ for $r, s \in R$ and (ii) if $a_1, a_2, \ldots$ are non zero elements of R such that $a_{i+1}|a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n > N$.

143. Let $R = \mathbb{Z}[\sqrt{-5}]$. Let $I_2 = (2, 1+\sqrt{-5}), I_3 = (3, 2+\sqrt{-5})$ and $I_3' = (3, 2-\sqrt{-5})$ be ideals of R. (i) Prove that above ideals are non-principal.
(ii) Show that $I_2^2 = (2)$, $I_2 I_3 = (1 - \sqrt{-5})$ and $I_2 I_3' = (1 + \sqrt{-5})$. Conclude $(6) = I_2^2 I_3 I_3'$.

144. Show that an integral domain R, in which every prime ideal is principal, is a PID.

145. If R is PID and D is a multiplicatively closed subset of R, then $D^{-1}R$ is also a PID.

146. Prove that the rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(y^2 - x^2)$ are not isomorphic for any field F.

147. Let R be an integral domain and let i, j be relatively prime integers. Prove that $(x^i - y^j)$ is a prime ideal in $R[x, y]$.

148. (i) Let F be a field. Prove that $F[x]$ contains infinitely many primes.
(ii) Determine all the ideals of $\mathbb{Z}[x]/(2, x^2 + 1)$.

149. Determine the gcd of $a(x) = x^3 - 2$ and $b(x) = x + 1$ in $\mathbb{Q}[x]$ and write the gcd as a linear combination of $a(x)$ and $b(x)$.

150. Prove that if $f(x), g(x) \in \mathbb{Q}[x]$ with $fg \in \mathbb{Z}[x]$, then the product of any coefficient of $f(x)$ with any coefficient of $g(x)$ is an integer.

151. For a field F, let R be the set of all $f(x) \in F[x]$ with coefficient of x equals 0. Then R is not a UFD.

152. (i) Show that the polynomials $x^4 + 4x^3 + 6x^2 + 2x + 1$ and $\frac{(x+2)^p - 2^p}{x}$ p a prime, are irreducible in $\mathbb{Z}[x]$.
(ii) Prove that $x^{n-1} + x^{n-2} + \ldots + 1$ is irreducible over $\mathbb{Z}$ iff n is a prime.

153. Show that the additive and multiplicative groups of a field F are never isomorphic.