Algebra First Year Examination Exercises

1. State and prove Cayley's Theorem about finite groups.
2. (a) Compute the order of the general linear group $\mathrm{GL}_n(\mathbb{Z}_p)$, with p a prime number.

   (b) Calculate the order of the subgroup $\mathrm{SL}_n(\mathbb{Z}_p)$ of matrices which have determinant 1.
3. (a) Prove that two elements of the symmetric group S_n are conjugate if and only if their cycle types are the same.

   (b) Is this true for the alternating groups? Justify your answer.
4. Prove that if $|G| = 12$ and G has 4 Sylow 3-subgroups, then $G \cong A_4$. (Hint: let G act by conjugation on the 4 Sylow 3-subgroups.)
5. Let p and q be prime numbers, and suppose that $p < q$. If G is a group of order pq and p does not divide $q - 1$, show that G must be cyclic.
6. Recall that a group G is called a *p-group* (p a prime number) if for each $g \in G$, $g^{p^i} = 1$, for some positive integer i.

   Prove that if G is a finite p-group, then its center is not trivial. Then use this fact to prove that every finite p-group is nilpotent.
7. Suppose that $\phi : G \longrightarrow H$ and $\theta : G \longrightarrow K$ are homomorphisms between groups. Assume that ϕ is surjective. Show that if $Ker(\phi)$ is contained in $Ker(\theta)$ then there is a unique homomorphism $\theta^* : H \longrightarrow K$ such that $\theta^* \cdot \phi = \theta$.
8. Prove that if G is a finite group then any subgroup of index 2 is normal.
9. Prove that any subgroup of a cyclic group is cyclic.
10. Find all the automorphisms of order 3 of $\mathbb{Z}_{91}$. (Hint: How can $\mathbb{Z}_3$ act nontrivially on $\mathbb{Z}_{91}$?) Does $\mathbb{Z}_{91}$ have any automorphisms of order 5? Explain.
11. Suppose that G is a nonabelian group of order 21. Prove:

    (a) $Z(G) = \{e\}$;

    (b) G has an automorphism which is not inner.
12. Let $\mathrm{GL}_2(\mathbb{Z}_3)$ act on the four one-dimensional subspaces of $\mathbb{Z}_3^2$ by $g(Span\{v\}) = Span\{gv\}$, where $g \in \mathrm{GL}_2(\mathbb{Z}_3)$ and $v \in \mathbb{Z}_3^2$. Prove that this action induces a surjective homomorphism of $\mathrm{GL}_2(\mathbb{Z}_3)$ onto S_4 whose kernel is the subgroup of all scalar matrices.
13. Let p be a prime number and n be a positive integer. Prove that the general linear group $\mathrm{GL}_n(\mathbb{Z}_p)$ is isomorphic to the automorphism group of $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (n times).
14. Suppose that $\phi : G \longrightarrow H$ is a surjective homomorphism of groups. Prove the following about the assignment $\phi^* : N \mapsto \phi^{-1}(N)$. Assume that it maps subgroups to subgroups.

    (a) ϕ^* is a bijection between the lattice of subgroups of H and the set of subgroups of G that contain $Ker(\phi)$.

    (b) $N_1 \subseteq N_2$ if and only if $\phi^*(N_1) \subseteq \phi^*(N_2)$.

    (c) $\phi^*(N)$ is normal in G if and only if N is normal in H.

15. Let G be a finite group acting on the set S. Suppose that H is a normal subgroup of G so that for any $s_1, s_2 \in S$ there is a unique $h \in H$ so that $hs_1 = s_2$. For each $s \in S$, let $G_s = \{ g \in G : gs = s \}$. Prove
    (a) $G = G_s H$, and $G_s \cap H = \{e\}$;
    (b) if H is contained in the center of G, then G_s is normal and G is (isomorphic to) a direct product of G_s and H.
16. Suppose that G is a group and H is a proper subgroup of index k. Show that
    (a) $g * (xH) = gxH$ defines a group action of G on the set $\Omega = (G/H)_l$ of left cosets of H;
    (b) the kernel of the induced homomorphism into the permutation group on Ω is the intersection of all the conjugates of H.
    (c) Now suppose that G is simple and that $k > 1$ is the index of H. Then show that G is isomorphic to a subgroup of S_k.
17. Prove that a group of order 30 must have a normal subgroup of order 15.
18. Classify the groups of order 70.
19. Show that if G is a subgroup of S_n (n a natural number) containing an odd permutation, then half the elements of G are odd and half are even.
20. Use 19 to prove that if G is a group of order $2m$, with m odd, then G cannot be simple, and, indeed, contains a subgroup of index 2.
21. Classify the groups of order $4p$, where $p \geq 5$ is prime.
22. Let p be an odd prime number.
    (a) Prove that in $\mathrm{GL}_2(\mathbb{Z}_p)$ every element A of order 2, $A \neq -I$, is conjugate to the diagonal matrix U, for which $U_{11} = -1$ and $U_{22} = 1$.
    (b) Now classify the groups of order $2p^2$, for which the Sylow p-subgroups are *not* cyclic.
23. (a) Prove that there are exactly four homomorphisms from $\mathbb{Z}_2$ into $Aut(\mathbb{Z}_8)$.
    (b) Show that these yield four pairwise nonisomorphic semidirect products.
24. Prove that S_4 contains no non–abelian simple groups.
25. Use the result of 24 to prove that if G is a nonabelian simple group, then every proper subgroup of G has index at least 5.
26. Prove that D_{2n} is nilpotent if and only if n is a power of 2. (Hint: Use the ascending central chain; recall that if there is an even number number of vertices n, then $Z(D_{2n}) \neq \{e\}$.
27. Let G be the group of all 3 by 3 upper triangular matrices, with entries in $\mathbb{Z}$, and diagonal entries equal to 1. Prove that the commutator of G is its center.
28. Let P be a Sylow p-subgroup of H and $H \leq K$. If P is normal in H and H is normal in K, prove that P is normal in K. Deduce that if $P \in Syl_p(G)$ then $N_G(P)$ is selfnormalizing.
29. Prove that if G is a finite group, and each Sylow p-subgroup is normal in G, then G is a direct product of its Sylow subgroups.

30. Classify the abelian groups of order $2^5 \cdot 5^2 \cdot 17^3$.

31. Prove that $(\mathbb{Q}, +)$, the additive group of rational numbers is not cyclic.

32. Prove that $Aut(\mathbb{Z}_k)$ is isomorphic to the group $U(k)$ of integers i, with $1 \leq i < k$, which are relatively prime to k, under multiplication modulo k.

33. Give examples of each of the following, with a brief explanation in each case:

    (a) A solvable group with trivial center.

    (b) An abelian p-group which is isomorphic to one of its proper subgroups and also one of its proper homomorphic images.

    (c) An abelian group having no maximal subgroups.

    (d) A direct product of nilpotent groups which is not nilpotent.

    (e) A semidirect product of abelian groups which is not nilpotent.

    (f) A finite nonabelian group in which every proper subgroup is cyclic.

34. Each three-cycle in S_n has $\frac{1}{3}n(n-1)(n-2)$ conjugates. Prove this and conclude from it that A_4 is the only subgroup of S_4 of order 12.

35. Prove that A_5 is a simple group.

36. For $n \geq 5$, prove that A_n is the only proper, nontrivial normal subgroup of S_n.

37. Let G be a finite group. Call $x \in G$ a *non-generator* if for each subset $Y \subseteq G$, if $G = < Y \cup \{x\} >$ then $G = < Y >$. Prove:

    (a) The subset $\Phi(G)$ of all non-generators of G form a subgroup of G.

    (b) $\Phi(G)$ is the intersection of all maximal subgroups of G.

    (c) Conclude from (b) that $\Phi(G)$ is normal.

    (d) What is the Frattini subgroup of S_n? Explain. (Consider the stabilizers of a single letter.

38. State and prove the Orbit-Stabilizer Theorem.

39. Show that if G is a simple abelian group then it is cyclic of prime order.

40. For the additive group of rational numbers $(\mathbb{Q}, +)$, show that the intersection of any two nontrivial subgroups is nontrivial.

41. Show that the group $(\mathbb{Q}, +)$ of additive rational numbers has no maximal subgroups. (Hint: Use the lattice isomorphism theorem (Exercise 14) and Exercise 39.)

42. The *commutator subgroup* G' of a group G is defined as the subgroup generated by the set

$$\{ x^{-1}y^{-1}xy \, : \, x, y \in G \}.$$

    Prove that:

    (a) Show that G' is a normal subgroup of G.

    (b) Show that G/G' is abelian.

(c) Show that if $\phi : G \longrightarrow H$ is a homomorphism into the abelian group H, then there exists a unique homomorphism $\hat{\phi} : G/G' \longrightarrow H$ such that $\hat{\phi}(G'x) = \phi(x)$, for each $x \in G$.

43. Suppose that G is a group and H is a normal subgroup. Prove that $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. (Hint: let G act on H by conjugation.)

44. Let G be a group of 385 elements. Prove that the Sylow 11-subgroups are normal, and that any Sylow 7-subgroup lies in the center.

45. Describe all the groups of 44 elements, up to isomorphism. (Hint: use semidirect products.)

46. Suppose that $|G| = 105$. If G has a normal Sylow 3-subgroup, prove that it must lie in the center of G.

47. Let G and H be the cyclic groups of orders n and k, respectively. Prove that the number of homomorphisms from G to H is the sum of all $\phi(d)$, where d runs over all common divisors of n and k, and ϕ denotes the Euler ϕ-function.

48. Let R be the ring of all n by n matrices with integer entries. Prove that the matrix $a \in R$ is invertible if and only if its determinant is ± 1. (Would you believe: Cramer's Rule?)

49. Using Zorn's Lemma, prove that each non-zero commutative ring with an identity has maximal ideals.

50. Using Zorn's Lemma, prove that in each non-zero commutative ring with identity minimal prime ideals exist.

51. Consider $A = \mathbb{R}^{\mathbb{N}}$, the ring of all real valued sequences, under pointwise operations. Prove:

    (a) for each $n \in \mathbb{N}$, $M_n = \{f \in A : f(n) = 0\}$ is a maximal ideal of A;

    (b) there exist maximal ideals besides the M_n $(n \in \mathbb{N})$. (Zorn's Lemma)

52. Suppose that A is a commutative ring with identity. Suppose that $a \in A$ is not nilpotent. Prove that there is a prime ideal that fails to contain a. Use this to show that the set of all nilpotent elements of A is the intersection of all the prime ideals of A.

53. Let F be a field, and $A = F[[X]]$ denote the ring of formal power series in one variable. Prove the following:

    (a) The units of A are precisely the power series whose constant term is nonzero.

    (b) Suppose that $k \geq 1$ is an integer. Let I_k denote the set of all power series $\sum_{n=0}^{\infty} a_n X^n$ for which $a_0, \ldots, a_{k-1}$ are all zero. Each I_k is an ideal of A.

    (c) If J is a nonzero proper ideal of A, then $J = I_m$, for some $m \geq 1$.

54. Prove the Divison Algorithm for the ring $\mathbb{Z}[i]$ of Gaussian integers.

55. Let D be an integer which is not a square in $\mathbb{Z}$. Consider the subring $\mathbb{Z}[\sqrt{D}] = \{\, a + b\sqrt{D} : a, b \in \mathbb{Z} \,\}$; (do not prove it is a subring.) Define $N(a + b\sqrt{D}) = a^2 - Db^2$. Assume that $N(xy) = N(x)N(y)$, for all $x, y \in \mathbb{Z}[\sqrt{D}]$. Prove that

    (a) $a + b\sqrt{D}$ is a unit of $\mathbb{Z}[\sqrt{D}]$ if and only if $N(a + b\sqrt{D}) = \pm 1$.

    (b) If $D < -1$, prove that the units of $\mathbb{Z}[\sqrt{D}]$ are precisely ± 1.

56. A ring R is *boolean* if it has an identity and $x^2 = x$, for each $x \in R$. Prove:

    (a) Every boolean ring has characteristic 2 and is commutative.

    (b) Assume R is a boolean ring. Prove that every prime ideal is maximal.

57. A ring R is *boolean* if it has an identity and $x^2 = x$, for each $x \in R$. Assume the preceding exercise. Use the Chinese Remainder Theorem to prove that every finite boolean ring has 2^n elements, for a suitable non-negative integer n.

58. Suppose that A is a non-zero commutative ring with identity. Let $n(A)$ denote the set of nilpotent elements of A; you may assume here that it is an ideal. Prove the equivalence of the following three statements:

    (a) Every nonunit of A is nilpotent.

    (b) $A/n(A)$ is a field.

    (c) A has exactly one prime ideal.

59. Prove the Chinese Remainder Theorem: if A is a commutative ring with identity, and I and J are comaximal ideals of A, then $IJ = I \cap J$, and the homomorphism $\phi : A \to A/I \times A/J$, by $\phi(a) = (a + I, a + J)$ is surjective.

60. Let D be an integral domain. Prove that the ring $D[T]$ of polynomials over D in one indeterminate is a principal ideal domain if and only if D is a field.

61. Let A be a commutative ring with 1. Suppose that I and J are ideals of A. Prove that

    (a) Prove that $IJ \subseteq I \cap J$, and give an example where equality does not hold.

    (b) Suppose that A is the (ring) direct product of two fields. Show that $IJ = I \cap J$, for any two ideals I and J of A.

62. Suppose that D is an integral domain. A polynomial $f(X)$ over D is *primitive* if the greatest common divisor of its coefficients is 1.

    Prove the following form of Gauss' Lemma: *If D is a unique factorization domain, then the product of any two primitive polynomials over D is primitive.*

63. Let A be an integral domain, and P be a prime ideal of A. Define A_P to be the subset of the quotient field K of A, consisting of all fractions whose denominator is not in P. Prove that

    (a) A_P is a subring of K;

    (b) A_P has exactly one maximal ideal; identify it.

64. (a) Define *Euclidean domain* and *principal ideal domain.*

    (b) Prove that any Euclidean domain is a principal ideal domain.

65. Convince that the polynomial rings $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ have the same field of fractions, but the power series rings $\mathbb{Z}[[X]]$ and $\mathbb{Q}[[X]]$ do not.

66. Consider the polynomial $X^2 + 1$ over the field $\mathbb{Z}_7$. Prove that $E = \mathbb{Z}_7[X]/(X^2 + 1)$ is a field of 49 elements.

67. Let n be a natural number; prove that the polynomial

$$\Phi_n(X) = \frac{X^n - 1}{X - 1}$$

is irreducible over the ring $\mathbb{Z}$ precisely when n is prime.

68. Prove that $X^2 + Y^2 - 1$ is irreducible in $\mathbb{Q}[X, Y]$.

69. Give examples of the following, and justify your choices:

    (a) A unique factorization domain which is not a principal ideal domain.

    (b) A local integral domain with a *nonzero* prime ideal that is not maximal.

    (c) An integral domain in which the uniqueness provision of "unique factorization" fails.

70. Suppose that F is a field and G is a finite multiplicative subgroup of $F \setminus \{0\}$. Prove that G is cyclic.

71. Suppose that F is a field and $q(X) = a_0 + a_1 X + \cdots a_{n-1}X^{n-1} + X^n$ is an irreducible polynomial in $F[X]$. Prove that $E = F[X]/(q(x))$ is a field which is an n dimensional vector space over F.

72. Let R be a ring with identity and M be an R-module. An element $x \in M$ is called a *torsion element* if $rx = 0$, for some nonzero $r \in R$. Let $T(M)$ denote the subset of all torsion elements of M.

    (a) If R is an integral domain show that $T(M)$ is a submodule of M.

    (b) Give an example to show that $T(M)$, in general, is not a submodule of M.

73. Suppose that A is a commutative ring with identity, and I is an ideal of A.

    (a) For each positive integer n, prove that

    $$A^n/IA^n \cong A/I \times \cdots \times A/I;$$

    (b) Use (a) to prove that if $A^m \cong A^n$, where m and n are positive integers, then $m = n$. (You may use the corresponding fact for fields.)

74. Prove that $\mathbb{Q}$, the additive group of the rationals, is not a free abelian group. (Hint: The rank of $\mathbb{Q}$ is one.)

75. Suppose that G is an abelian group, generated by x_1, x_2, x_3, x_4, and subject to the relations:

$$4x_1 - 2x_2 - 2x_3 = 0;\ 8x_1 - 12x_3 + 20x_4 = 0;\ 6x_1 + 4x_2 - 16x_4 = 0.$$

Write G as a direct product of cyclic groups.

76. Let R be a commutative ring with identity. If F is a free R-module of rank $n < \infty$, then show that $\mathrm{Hom}_R(F, M) \cong M^n$, for each R-module M.

77. Let V be a vector space over the field F. Suppose that U_1 and U_2 are finite dimensional subspaces of V. Prove that $dim(U_1) + dim(U_2) = dim(U_1 \cap U_2) + dim(U_1 + U_2)$.

78. Suppose that $T : V \longrightarrow W$ is a linear transformation between vector spaces over the same field F. Prove that T is one to one precisely when it maps linearly independent sets to linearly independent sets.

79. Suppose that $T : V \longrightarrow V$ is a linear transformation on the vector space V. Call T a *projection* if $T^2 = T$. Prove that if T is a projection then $V = Ker(T) \oplus Im(T)$.

    Give an example to show that the converse of the above proposition is false.

80. Suppose that V is a finite dimensional vector space over the field F and that $T : V \longrightarrow W$ is a linear transformation into a vector space W over F. Prove that $dim(V) = dim(Ker(T)) + dim(Im(T))$. (Caution: The finite dimensionality of $Im(T)$ must be established.)

81. Obtain a formula for the number of one dimensional subspaces of an n dimensional vector space over the field $\mathbb{Z}_p$ of p elements (p is a prime number). Justify your choice.

82. (a) Define: *Irreducible module* over a ring R with identity 1.

    (b) Now assume that R is commutative as well. Prove that the R-module M is irreducible if and only if $M \cong R/I$, where I is a maximal ideal of R. Use this to classify the irreducible $\mathbb{Z}$-modules.

83. (a) Define: *Irreducible module* over a ring R with identity 1.

    (b) Prove Schur's Lemma: *Suppose that M is an irreducible module; then every nonzero endomorphism of M is an automorphism.* Show how one concludes from this that $End(M)$ is a division ring, when M is irreducible.

84. Let R be a ring with identity. Suppose that $\phi : M \longrightarrow F$ is a surjective R-homomorphism and that F is a free R-module. Prove that $M = Ker(\phi) \oplus N$, where $N \cong F$.

85. Let R be a principal ideal domain and M be a torsion R-module. Define *primary module* and prove that M is isomorphic to a direct sum of primary R-modules.

86. Suppose that V is a finite dimensional vector space over the field F and that T is a linear transformation on V, so that the induced module action of $F[X]$ on V defines a cyclic module with cyclic vector w. Prove:

    (a) The set $\{ w, Tw, T^2w, \ldots, T^kw \}$ is a basis for a suitable k.

    (b) Compute the matrix of T relative to this basis, pointing out the relationship which the entries of this matrix and k have to the monic polynomial in $F[X]$ that generates the annihilator of w.

    (c) Compute the characteristic polynomial of the matrix in (b).

87. Suppose that T is a linear transformation on a finite dimensional vector space V, over the field F. Prove that T is diagonalizable if and only if $m_T(X)$, the minimum polynomial of T, can be factored as

$$m_T(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_k),$$

    where the $\lambda_i \in F$ $(i = 1, \ldots, k)$ are distinct.

88. Suppose that A is a nilpotent 6×6 matrix, with entries in a field. Find all possible Jordan forms of A, justifying your arguments.

89. Prove that in $\mathrm{GL}_2(\mathbb{Q})$ all the elements of order four are conjugate. (Hint: Consider the rational canonical form of such an element.)

90. Suppose that V is a vector space of dimension 7 over the field of real numbers $\mathbb{R}$, and T is a linear transformation on V which satisfies $T^4 = I$. Compute the following:

    (a) the possible minimum polynomials of T, and the characteristic polynomial that goes with each choice;

    (b) the possible Rational Canonical Forms of T.

91. Suppose that V is a finite dimensional vector space over $\mathbb{Q}$, and T is an invertible linear transformation on V for which $T^{-1} = T^2 + T$. Prove:

    (a) The dimension of V is a multiple of 3.

    (b) If the dimension is 3, prove that all such transformations are similar.

92. Consider: *All 3 × 3 matrices $A \neq I$ with real entries, such that $A^3 = I$ are similar over* $\mathbb{R}$. Prove or disprove by example.

93. Prove, over any field F, that if two 2×2 matrices or two 3×3 matrices have the same minimum and characteristic polynomials then they are similar matrices.

    Give an example which shows that this is false for matrices of greater dimension.

94. On a vector space V of dimension 8 over the field $\mathbb{Q}$, T is a linear transformation for which the minimum polynomial is
$$m_T(X) = (X^2 + 1)^2(X - 3).$$
    Determine all possible Rational Canonical Forms. Justify your answer.

95. A *projection* is a linear transformation $P : V \to V$ on a vector space V for which $P^2 = P$. Assume that V has finite dimension and prove the following:

    (a) Any projection is diagonalizable.

    (b) Two projections have the same diagonal form if and only if their kernels have the same dimension.

96. Prove that there are exactly two conjugacy classes of 5×5 matrices with entries in $\mathbb{Q}$ for which $T^8 = I$ and $T^4 \neq I$.

97. T is a linear transformation on the n dimensional space V, over the field F, and there is a basis $\{v_1, \ldots, v_n\}$ for V for which $Tv_i = v_{i+1}$, for $i = 1, 2, \ldots, n-1$, and $Tv_n = v_1$. As a module over $F[X]$ with the action induced by T, show that

    (a) V is a cyclic module but not irreducible.

    (b) If $F = \mathbb{Q}$ and n is a prime number prove that V is the direct sum of two irreducible $F[X]$-submodules, of dimensions 1 and $n-1$, respectively, over $\mathbb{Q}$. (Hint: Find the minimum polynomial of T.)

98. (a) Define the terms *eigenvector* and *eigenvalue* of a linear transformation T.

    (b) Prove that a set of eigenvectors of T for which the corresponding eigenvalues are distinct must be linearly independent.

99. Find one representative of each conjugacy class of elements of order 2 in the group $\mathrm{GL}_5(\mathbb{Z}_2)$ of invertible 5×5 matrices with entries in the field of integers mod 2.

100. Let $\mathrm{GL}_4(\mathbb{Z}_3)$ denote the group of all invertible 4 by 4 matrices with entries in $\mathbb{Z}_3$, the field of three elements. Use rational canonical forms to determine the number of conjugacy classes of elements of order 4. Give the rational canonical form for each class.

101. Over $\mathbb{Q}$, compute the Jordan canonical form J of

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Then find a matrix S such that $J = SAS^{-1}$.

102. Over $\mathbb{Q}$, consider the following matrix:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Answer the following:

(a) Prove that A is diagonalizable.

(b) Is the $\mathbb{Q}[T]$-module structure on $\mathbb{Q}^4$ by A, via $f(T)v = f(A)v$ cyclic? Explain.

103. Let $\mathbb{C}$ be the field of complex numbers. Prove that each irreducible $\mathbb{C}[T]$-module is isomorphic to $\mathbb{C}$.

104. Prove that if F is a finite field, then there is a prime number p and a natural number n, so that F has p^n elements.

105. Suppose that F is a subfield of K and K a subfield of L, so that the dimensions $[K : F]$ and $[L : K]$ are finite. Prove that $[L : F]$ is also finite and that

$$[L : F] = [L : K][K : F].$$

106. Determine the dimension over $\mathbb{Q}$ of the extension $\mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$. Justify your arguments.

107. Prove that $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Conclude that $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$, and find a monic irreducible polynomial over $\mathbb{Q}$ satisfied by $\sqrt{3} + \sqrt{5}$.

108. Suppose that F is a field whose characteristic is not 2. Assume that $d_1, d_2 \in F$ are not squares in F. Prove that $F(\sqrt{d_1}, \sqrt{d_2})$ is of dimension 4 over F if $d_1 d_2$ is not a square in F and of dimension 2 otherwise.

109. Suppose that $[F(u) : F]$ is odd; prove that $F(u) = F(u^2)$.

110. Let L be a field extension of F. Prove that the subset E of all elements of L which are algebraic over F is a subfield of L containing F.

111. Determine the splitting field of $X^4 - 2$ over $\mathbb{Q}$. It suffices to describe it as the subfield of $\mathbb{C}$, the field of complex numbers, generated by certain well-identified elements. Justify your choices.

112. Suppose that F is a field. For $f(X) = a_nX^n + \cdots + a_1X + a_0 \in F[X]$, define the *derivative* $D_Xf(X)$ by

$$D_Xf(X) = na_nX^{n-1} + \cdots + 2a_2X + a_1.$$

Prove the following: In a splitting field of $f(X)$, u is a multiple root of $f(X)$ if and only if u is a root of the derivative of $f(X)$.

113. Assume the existence and uniqueness, up to isomorphism, of the splitting field of a polynomial over an arbitrary base field. Let p be a prime number. Now consider the polynomial $X^{p^n} - X$ over the field $\mathbb{Z}_p$ of p elements. Let K_{p^n} be its splitting field. Prove that K_{p^n} has p^n elements. (Hint: Consider the set of all roots of $X^{p^n} - X$.)

Now consider any field F having p^n elements. Prove that $F \cong K_{p^n}$. (Hint: Use the fact that the multiplicative group of nonzero elements of F is cyclic.)