Algebra Qualifying Examination Exercises on Ring Theory

1. Definitions
   (a) Define the characteristic of a ring.
   (b) Define a norm on a ring; define a Euclidean domain.
   (c) Define: von neumann regular ring, boolean ring, noetherian ring, the a.c.c. on ideals, Principal Ideal Domain, Bézout domain, U.F.D., clean ring.
   (d) State Zorn's Lemma.
   (e) Define a complete lattice.
   (f) Define $\mathrm{Aut}(E|F)$ for fields $F \leq E$.
   (g) Define an F-vector space. Define a basis.
2. Prove that an arbitrary intersection of ideals is an ideal.
3. Prove that the set of all ideals of a commutative ring with identity is a complete lattice. For ideals I, J explicitly state what $I \wedge J$ and $I \vee J$ are.
4. Using Zorn's Lemma, prove that each commutative ring with an identity has maximal ideals.
5. Using Zorn's Lemma, prove that in each commutative ring with identity minimal prime ideals exist.
6. (a) Define a maximal ideal and prime ideal.

   (b) Let R be a commutative ring with identity and M an ideal of R. Prove that M is a maximal ideal if and only if R/M is a field.

   (c) Let R be a commutative ring with identity and P an ideal of R. Prove that P is a prime ideal if and only if R/P is an integral domain.

   (d) Conclude that a maximal ideal is prime.
7. Let R be a commutative ring with identity. Prove that R is a field if and only if the only two ideals of R are itself and $\{0\}$.
8. Prove that in a Principal Ideal Domain every irreducible element generates a prime ideal and that it is a maximal ideal.
9. 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)
10. 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.
11. 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.

12. Define a boolean ring. Prove:

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

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

    (c) Prove that a homomorphic image of a boolean ring is boolean.

    (d) Classify the boolean rings which are integral domains.

    (e) Prove that a direct product of boolean rings is boolean.

    (f) Use the Chinese Remainder Theorem to prove that every finite boolean ring has 2^n elements, for a suitable positive integer n.

13. Define a von Neumann regular ring. Assume that R is a such a ring. Prove:

    (a) Prove that a homomorphic image of a boolean ring is boolean.

    (b) Prove that every prime ideal is maximal.

    (c) Classify the von Neumann regular rings which are integral domains.

    (d) Prove that a direct product of von Neumann regular rings is von Neumann regular.

14. Suppose that A is a 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.

15. 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.

16. Let R be a commutative ring with identity. Prove that the following are equivalent:

    (i) R is an integral domain.

    (ii) $R[x]$ is an integral domain.

    (iii) For all $f, g \in R[x]$, deg fg = deg f + deg g.

17. Let R be an integral domain. Prove that the following are equivalent:

    (i) R is a field.

    (ii) $R[x]$ is an Euclidean Domain.

    (iii) $R[x]$ is an Principal Ideal Domain.

    (iv) $R[x]$ is a Bézout domain.

18. 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.

19. 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.*

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

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

21. 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.

22. 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.

23. Prove that $X^2 + Y^2 - 1$ is irreducible in $\mathbb{Q}[X, Y]$. (Hint: Translate by a suitable quantity and then apply the general form of Eisenstein's Criterion.)

24. Prove that a ring is P.I.D. if and only if it is noetherian and a Bézout domain.

25. Prove that a ring is P.I.D. if and only if it is a U.F.D. and a Bézout domain.

26. Prove that a ring is noetherian if and only if it satisfies the a.c.c. condition on ideals.

27. State and prove Eisenstein's Criterion.

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

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

    (b) A Principal Ideal Domain which is not Euclidean.

    (c) A Bézout domain which is not a Principal Ideal Domain.

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

30. Suppose F is a field and that $f(x) \in F[x]$ is an irreducible polynomial of degree n. Explain why $K = F[x]/(f(x)))$ is a field extension of F. Moreover, K is an F-vector space. Prove that the set $\{1 + (f(x)), x + (f(x)), \cdots, x^{n-1} + (f(x))\}$ is a basis for K as an F-vector space. Conclude that $[K : F] = n$.

31. Construct a field $\mathbb{C}$ such that $\mathbb{R} \leq \mathbb{C}$, $[\mathbb{C} : \mathbb{R}] = 2$, and so that the polynomial $f(x) = x^2 + 1$ has a solution in $\mathbb{C}$.

32. 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.)

33. 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.

34. 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

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

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

36. 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 $\sqrt{3} + \sqrt{5}$.

37. 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.

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

39. 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.

40. 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.

41. Suppose that F is a field. For $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in F[X]$, define the *derivative* $D_X f(X)$ by

$$D_X f(X) = n a_n X^{n-1} + \cdots + 2a_2 X + a_1.$$

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 $f(X)$.

42. 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.)

43. 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 $m \geq 1$.

44. Suppose F is a field and that $f(x) \in F[x]$ is an irreducible polynomial of degree n. Explain why $K = F[x]/(f(x)))$ is a field extension of F. Moreover, K is an F-vector space. Prove that the set $\{1 + (f(x)), x + (f(x)), \cdots, x^{n-1} + (f(x))\}$ is a basis for K as an F-vector space. Conclude that $[K : F] = n$.

45. Construct a field $\mathbb{C}$ such that $\mathbb{R} \leq \mathbb{C}$, $[\mathbb{C} : \mathbb{R}] = 2$, and so that the polynomial $f(x) = x^2 + 1$ has a solution in $\mathbb{C}$.

46. State the Rational Root Test.

47. State and prove Eisenstein's Irreducibility Criterion

48. State the definition of a polynomial. Explain why for any $f(x) \in F[x]$, $f(x)$ is a product of irreducible polynomials.

49. Given an irreducible polynomial $f(x) \in F[x]$ construct a field K containing a root of $f(x)$.

50. State the definition of a splitting field of a polynomial.

51. Given $F \leq K$, define $[K : F]$.

52. Given $F \leq K$ state the definition of what it means for K to be an algebraic extension field of F.

53. For a given extension $F \leq K$ with $\alpha \in K$ state what it means for a to be algebraic (transcendental) over F.

54. Suppose $F \leq K$ and $\alpha \in K$ algebraic over F. Define the minimum polynomial of α over F. Explain why it is unique.

55. Suppose $F \leq K \leq L$. Prove that $[L : F] = [L : K][K : F]$.

56. Suppose $F \leq K$ and $\alpha, \beta \in K$. Define $F(a)$ and $F(\alpha, \beta)$.

57. Suppose $F \leq K$ and $\alpha \in K$. Prove that α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.

58. Given $F \leq K$. Let $T = \{\alpha \in K : \alpha \text{ is algebraic over } F\}$. Prove that T is a subfield of K containing F.

59. Prove that if $[K : F] < \infty$, then K is an algebraic extension of F. Is the converse true?

60. Determine minimum polynomials. Determine splitting fields of polynomials e.g. $f(x) = x^p - 2$.

61. Construct the cyclotomic field of n^{th} roots of unity over $\mathbb{Q}$. Determine its dimension over $\mathbb{Q}$.

62. Prove that a polynomial has α as a multiple root if and only if its α is a root of its formal derivative.

63. State and prove the Freshman's Dream.

64. (a) Let F be any field. Prove that a polynomial has a multiple root α if and only if α is also a root of $D_x f(x)$, the derivative of $f(x)$.
    (b) Use (a) to show that if $F = \mathbb{Z}_p$, then the polynomial $f(x) = x^{p^n} - x \in F[x]$ is separable and therefore has exactly p^n roots.

(c) Use the Freshman's Dream to show that the roots of $f(x)$ form a subfield, say E, of the splitting field of $f(x)$ containing F and hence is the splitting field.

(d) Determine $[E : F]$.

65. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$. Do the same for $1 + i$.
66. Let p be prime. Determine the splitting field and Galois Group of $x^p - 2$.
67. Let $\alpha = \sqrt{2 + \sqrt{2}}$. Determine the minimum polynomial of α over $\mathbb{Q}$, say $m_\alpha(x)$. Determine the splitting field of $m_\alpha(X)$ and determine its Galois group.
68. Determine the splitting field of $x^4 + x^2 + 1$.
69. Determine the Galois Group over $\mathbb{Q}$ of $x^4 - 14x^2 + 9$.
70. Let E be an algebraic field extension over F and $\sigma \in \text{Aut}(E/F)$. Show that if $\alpha \in E$ is a root of $f(x) \in F[x]$, then so is $\sigma(\alpha)$.
71. Determine the Galois group of $x^4 - 25$.
72. Show that $x^5 - x - 1$ is irreducible.
73. Determine the Galois Group of $x^3 - 3x + 1$.
74. Classify the possible Galois Groups of a quadratic polynomial over $\mathbb{Q}$. Classify the possible Galois Groups of a cubic polynomial over $\mathbb{Q}$.
75. State Gauss' Lemma.
76. Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not field isomorphic.
77. Determine $\text{Aut}(\mathbb{R}/\mathbb{Q})$.
78. Suppose F is a finite field of characteristic p. Prove that $|F| = p^n$ for some $n \in \mathbb{N}$.
79. Suppose $f(x) \in \mathbb{Q}[x]$. Prove that if $z \in \mathbb{C}$ is a root of $f(x)$, then so is its complex conjugate $\bar{z} \in \mathbb{C}$.
80.
81.
82.
83.
84.
85.
86.
87.
88.
89.