ANNA ADARSH COLLEGE FOR WOMEN (AUTONOMOUS)
End Semester Examination, Apr/May- 2026

Max. Marks: 75 **TIME:3 Hrs**

PART- A (10 × 1 = 10 Marks)
Answer all questions.

1. Define a Field.
   Field is a commutative ring.
2. Define degree of K over F.
   The degree of K over F is the dimension of K as a vector space over F.
3. Define Algebraic over F.
   An element a ∈ K is said to be algebraic over F if there exist elements α_0 , α_1 , ... , αn in F, not all 0, such that $\alpha_0 a_n + \alpha_1.a_{n-1} + \cdot \cdot \cdot + \alpha n=0$
4. State the reminder theorem.
   If p(x) ∈ F[x] and if K is an extension of F, then for any element b∈ K,p(x) = (x - b)q(x) + p(b) where q(x) ∈ K[x] and where deg q(x) deg p(x) -1
5. Define splitting field over F.
   If f(x) ∈ F[x], a finite extension E of F is said- to be a splitting field over F for f(x) if over E (that is, in E[x]), but not over any proper subfield of E, f (x) can be factored as a product of linear factors.
6. Determine the degrees of the splitting fields of the polynomial $x^7 - 1$ over F .
7. Define Algebraic of degree n.
   The element a ∈ K is said to be algebraic of degree n over F if it satisfies a nonzero polynomial over F of degree n but no nonzero polynomial of lower degree.
8. Define Algebraic extension of F.
   The extension K of F is called an algebraic extension of F if every element in K is algebraic over F.
9. Define Algebraic number.
   A complex number is said to be an algebraic number if it is algebraic over the field of rational numbers.
10. Define solvable group.
    A group G is said to be solvable if we can find a finite chain of subgroups $G = N_0 \supset N_1 \supset N_2 \supset \bullet \bullet \bullet \supset N_k = (e)$, where each N_i is a normal subgroup of Ni-l and such that every factor group N_{i-1}/N_i is abelian.
11. Define simple extension of F.
    The extension K of F is a simple extension of F if K = F (α) ·· for some a in K.
12. Define the norm N(x).
    If x ∈ Q then the norm of x, denoted by N(x), is defined by N(x) = xx*.

PART - B (5 × 5 = 25 Marks)
Answer any FIVE questions.

13. Prove that if the element a∈K is algebraic over F if and only if F(a) is a finite extension of F.
    Proof
    Suppose that F(a) is a finite extension of F and that [F(a) :F] = m. Consider the elements 1, a, a^2 , ••• , a^m; they are all in F(a) and are m + 1 in number. By Lemma these elements are linearly dependent over F. Therefore, there are elements α_1 ... , α_n in F, not all 0, such that $\alpha_0 + \alpha_1 a^1 + \ldots , \alpha_n a^m = 0$. Hence a is algebraic over F and satisfies the nonzero polynomial $p(x) = \alpha_0 + \alpha_1 x^1 + \ldots , \alpha_n x^m \cdot$ in F[x] of degree at most m = [F(a) :F]. This proves the "if" part of the theorem. Now to the "only if" part. Suppose that a in K is algebraic over F. By

14. If a and b in K are algebraic over F then prove that a ± b, ab and a/b (if b≠0) are algebraic over F.

Proof

Suppose that a is algebraic of degree m over F while b is algebraic of degree n over F. By Theorem 5.1.3 the subfield T = F(a) of K is of degree mover F. Now b is algebraic of degree n over F, a fortiori it is algebraic of degree at most n over T which contains F. Thus the subfield W = T (b) of K, again by Theorem 5.1.3, is of degree at most n overT. But [W:F] = [W: T][T:F] by Theorem 5.1.1; therefore, [W:F] ~ mn and so W is a finite extension of F. However, a and b are both in W, whence all of a ± b, ab, and ajb are in W. since [W:F] is finite, these elements must be algebraic over F, thereby proving the theorem.

15. Prove that a polynomial of degree *n* over a field can have at most *n* roots in any extension field.

Proof

We proceed by induction on n, the degree of the polynomial p(x). If p(x) is of degree 1, then it must be of the form αx + β where α, β are in a field F and where α≠0. Any a such that p(a) = 0 must then imply that αx + β = 0, from which we conclude that α = (-β/α). That is, p(x) has the unique root - β/α, whence the conclusion of the lemma certainly holds in this case. Assuming the result to be true in any field for all polynomials of degree less than n, let us suppose that p(x) is of degree n over F. Let K be any extension of F. If p(x) has no roots in K, then we are certainly done, for the number of roots in K, namely zero, is definitely at most n. So, suppose that p(x) has at least one root a E K and that a is a root of multiplicity m. Since (x - a)m I p(x), m :::;;; n follows. Now $p(x) = (x - a)^m q(x)$, where q(x) ∈ K[x] is of degree n - m. From the fact that $(x - a)^{m+1}$,V p(x), we get that (x- a) _.r q(x), whence, by the corollary a is not a root of q(x). If b ≠a is a root, in K, of p(x), then $0 = p(b) = (b - a)^m q(b)$; however, since b - a =1= 0 and since we are in a field, we conclude that q(b) = 0. That is, any root of p(x), in K, other than a, must be a root of q(x). Since q(x) is of degree n - m < n, by our induction hypothesis, q(x) has at most n - m roots in K, which, together with the other root a, counted m times, tells us that p(x) has at most m + (n - m) = n roots in K. This completes the induction and proves the lemma.

16. Examine that G(K,F) is a subgroup of the group of all automorphisms of K.

Proof

K contains field of rational numbers F_0 , since K is of characteristic 0, and it is easy see that the fixed field of any group of automorphisms of K, being a field, contain F_0 • Hence, every rational number is left fixed by every · automorphism of K.

17. Explain that the fixed field of G is a subfield of K.

Proof

Let a, b be in the fixed field of G. Thus for all (J E G, (J(a) = a (J(b) = b. But then (J(a ± b) = (J(a) ± (J(b) = a ± b and (J(ab) = u(b) = ab; hence a ± b and ab are again in the fixed field of G. If 0, then (J(b- 1) = (J(b) - 1 = b- 1, hence b- 1 also falls in the fixed of G. Thus we have verified that the fixed field of G is indeed a subfield of K.

18. Infer that K is a normal extension of F iff K is the splitting field of some polynomial over F.

Proof

Suppose that K is a normal extension of F; K = F(a). Consider the polynomial $p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a))$ over K, where σ_1, σ_2 , ••• , σ_n are all the elements of G(K, F). Expanding P(x) we see that $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + (-1)^n \alpha_n$ where $\alpha_1 \ldots, \alpha_n$ are the elementary symmetric functions in a = u1 (a), u2 (a), ... , U 11 (a), But then $\alpha_1 \ldots, \alpha_n$ are each invariant with respect to every u ∈ G (K, F), whence by the normality of K over F, must all be in F. Ther

19. Show that for every prime number p and every positive integer m there exists a field having p^m elements.

Proof

Consider the polynomial $x^{Pm} - x$ in $J_p[x]$, the ring of polynomials in x over Jp, the field of integers mod p. Let K be the splitting field of this polynomial. In K let $F = \{a \in K / a^{Pm} = a\}$. The elements of F are thus the roots of $x^{Pm} - x$, which are distinct;

whence F has p^m elements. We now claim that F is a field. If a, b∈F then $a^{Pm} = a$, $b^{Pm} = b$ and so $(ab)^{Pm} = a^{Pm}b^{pm} = ab$; thus ab∈ F. Also since the characteristic is p, $(a \pm b)Pm = aPm \pm bPm = a \pm b$, hence $a \pm b \in F$. Consequently, F is a subfield of K and so is a field. Having exhibited the field F having pm elements we have proved,

SECTION – C (4 X 10 = 40 Marks)

Answer any FOUR Questions

20. Show that [L:F]=[L:K][K:F], where L is a finite extension of K and K is a finite extension of F, then L is a finite extension of F.

Proof

Proof. The strategy we employ in the proof is to write down explicitly a basis of L over F. In this way not only do we show that L is a finite extension of F, but we actually prove the sharper result and the one which is really the heart of the theorem, namely that $[L:F] = [L:K][K:F]$.

Suppose, then, that $[L:K] = m$ and that $[K:F] = n$. Let $v_1, \ldots, v_m$ be a basis of L over K and let $w_1, \ldots, w_n$ be a basis of K over F. What could possibly be nicer or more natural than to have the elements $v_i w_j$, where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, serve as a basis of L over F? Whatever else, they do at least provide us with the right number of elements. We now proceed to show that they do in fact form a basis of L over F. What do we need to establish this? First we must show that every element in L is a linear combination of them with coefficients in F, and then we must demonstrate that these mn elements are linearly independent over F.

Let t be any element in L. Since every element in L is a linear combination of $v_1, \ldots, v_m$ with coefficients in K, in particular, t must be of this form. Thus $t = k_1 v_1 + \cdots + k_m v_m$, where the elements $k_1, \ldots, k_m$ are all in K. However, every element in K is a linear combination of $w_1, \ldots, w_n$ with coefficients in F. Thus $k_1 = f_{11}w_1 + \cdots + f_{1n}w_n, \ldots, k_t = f_{i1}w_1 + \cdots + f_{in}w_n, \ldots, k_m = f_{m1}w_1 + \cdots + f_{mn}w_n$, where every f_{ij} is in F.

Substituting these expressions for $k_1, \ldots, k_m$ into $t = k_1 v_1 + \cdots + k_m v_m$, we obtain $t = (f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m$ Multiplying this out, using the distributive and associative laws, we finally arrive at $t = f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n$. Since the f_{ij} are in F, we have realized t as a linear combination over F of the elements $v_i w_j$. Therefore, the elements $v_i w_j$ do indeed span all of L over F, and so they fulfill the first requisite property of a basis.

21. Explain the number e is transcendental.

Proof

Proof. In the proof we shall use the standard notation $f^{(i)}(x)$ to denote the ith derivative of $f(x)$ with respect to x.

Suppose that $f(x)$ is a polynomial of degree r with real coefficients. Let $F(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + \cdots + f^{(r)}(x)$. We compute $(d/dx)(e^{-x}F(x))$; using the fact that $f^{(r+1)}(x) = 0$ (since $f(x)$ is of degree r) and the basic property of e, namely that $(d/dx)e^x = e^x$, we obtain $(d/dx)(e^{-x}F(x)) = -e^{-x}f(x)$.

The mean value theorem asserts that if $g(x)$ is a continuously differentiable, single-valued function on the closed interval $[x_1, x_2]$ then

$$\frac{g(x_1) - g(x_2)}{x_1 - x_2} = g^{(1)}(x_1 + \theta(x_2 - x_1)), \qquad \text{where} \quad 0 < \theta < 1.$$

We apply this to our function $e^{-x}F(x)$, which certainly satisfies all the required conditions for the mean value theorem on the closed interval $[x_1, x_2]$ where $x_1 = 0$ and $x_2 = k$, where k is any positive integer. We then obtain that $e^{-k}F(k) - F(0) = -e^{-\theta_k k}f(\theta_k k)k$, where θ_k depends on k and is some real number between 0 and 1. Multiplying this relation through by e^k yields $F(k) - F(0)e^k = -e^{(1-\theta_k)k}f(\theta_k k)k$. We write this out explicitly:

$$\begin{aligned} F(1) - eF(0) &= -e^{(1-\theta_1)}f(\theta_1) = \varepsilon_1, \\ F(2) - e^2F(0) &= -2e^{2(1-\theta_2)}f(2\theta_2) = \varepsilon_2, \\ &\vdots \\ F(n) - e^nF(0) &= -ne^{n(1-\theta_n)}f(n\theta_n) = \varepsilon_n. \end{aligned} \tag{1}$$

Suppose now that e is an algebraic number; then it satisfies some relation of the form

$$c_n e^n + c_{n-1}e^{n-1} + \cdots + c_1 e + c_0 = 0, \tag{2}$$

where $c_0, c_1, \ldots, c_n$ are integers and where $c_0 > 0$.

In the relations (1) let us multiply the first equation by c_1, the second by c_2, and so on; adding these up we get $c_1F(1) + c_2F(2) + \cdots + c_nF(n) - F(0)(c_1e + c_2e^2 + \cdots + c_ne^n) = c_1\varepsilon_1 + c_2\varepsilon_2 + \cdots + c_n\varepsilon_n$.

In view of relation (2), $c_1e + c_2e^2 + \cdots + c_ne^n = -c_0$, whence the above equation simplifies to

$$c_0F(0) + c_1F(1) + \cdots + c_nF(n) = c_1\varepsilon_1 + \cdots + c_n\varepsilon_n. \tag{3}$$

22. Prove that the polynomial f(x)∈F[x] has a multiple root if and only if f(x) and f'(x) have a nontrivial common factor.

Proof

Before proving the lemma proper, a related remark is in order, namely, iff (x) and g(x) in F[x] have a nontrivial common factor in K[x], for K an extension of F, then they have a nontrivial common factor in F [x]. For, were they relatively prime as elements in F [x], then we would be able to find two polynomials a(x) and b(x) in F[x] such that a(x)f(x) + b(x) g(x) = 1. Since this relation also holds for those elements viewed as elements of K[x], in K[x] they would have to be relatively prime. Now to the lemma itself. From the remark just made, we may assume, without loss of generality, that the roots off (x) all lie in F (otherwise extend F to K, ·the splitting field of f(x)). But this that f(x) and f'(x) have the common factor x- ex, thereby proving the lemma in one direction. On the other hand, if f (x) has no multiple root, since the roots are all distinct. However, if f (x) and f' (x) have a nontrivial common factor, they have a common root, namely, any root of this common factor. The net result is that f(x) and f'(x) have no nontrivial

common factor, and so the lemma has been proved in the other direction,

23. Analyze that G(K,F) is a finite group and its order o(G(K,F)) satisfies o(G(K,F))≤ [K:F] where K is a finite extension of F.

Proof

Let [K:F] = n and suppose that u_1, ••• , u_n is a basis of K over F. Suppose we can find n + 1 distinct automorphisms n G(K, F). By the corollary to Theorem the system of n homogeneous linear equations in the n + 1 unknowns x_1, ... , x_{n+1}

Since every element in F is left fixed by each ui and since an arbitrary element t in K is of the form $t = \alpha_1 u_1 + \cdots + \alpha_n u_n$ with α_1 ... , α_n in F, then from the system of equations (1) we get $a_1\sigma_1(t) + \cdots + a_{n+1}\sigma_{n+1}(t) = 0$ for all t ∈K. But this contradicts the result of Theorem

24. Deduce that the Galois group over F of p(x) is a solvable group if p(x)∈F[x] is solvable by radicals over F.

Proof

Let K be the splitting field of p(x) over F; the Galois group of p(x) over F is G(K, F). Since p(x) is solvable by radicals, there exists a sequence of fields. we pointed out, without loss of generality we may assume that F_k is a normal extension of F. As a normal extension of F, F_k is also a normal extension of any intermediate field, hence F_k is a normal extension of each F_i. each Fi is a normal extension of F_{i-1} and since F_k is normal over F_{i-1} , by $G(F_k$, Fi) is a normal subgroup in G. As we just remarked, each subgroup in this chain is a normal subgroup in the one preceding it. Since Fi is a normal extension of Fi_ 1, by the fundamental theorem of Galois theory G(K, F) itself must then he a solvable group. Since G (K, F) is the Galois group of p(x) over F the theorem has been prove.

25. State and prove Wedderburn's theorem.

Proof

Let K be a finite division ring and let Z = {z ∈ K I zx = xz for all x ∈ K} be its center. If Z has q elements then, as in the proof of Lemma 7.1.1, it follows that K has qn elements. Our aim is to prove that Z = K, or, equivalently, that n = 1. If a ∈ K let N(a) = {x ∈ K / xa =ax}. N(a) clearly contains Z, and, as a simple check reveals, N(a) is a subdivision ring of K. Thus N(a) contains ~(a) elements for some integer n(a). We claim that n(a) In. For, the nonzero elements of N(a) form a subgroup of order qn(a) - 1 of the group of nonzero elements, under multiplication, of K which has qn - 1 elements. By Lagrange's theorem qn - 1 is a divisor ·of~ - 1; but this forces n(a) to be a divisor of n In the group of nonzero elements of K we have the conjugacy relation namely a is a conjugate of b if a = x- 1bx for some x =f. 0 in K. the number of elements in K conjugate to a is the index of the normalizer of a in the group of nonzero elements of K. Therefore the number of conjugates of a in K is (qn - 1)/(qn(a) - 1). Now a E Z if and only if n(a) = n, thus by the class equation

****

.