CMI Algebra IV Endsem
09:30-12:30, Saturday, 22 April 2023

Write clearly at the start of the answer book: *Algebra 4 Endsem, your name and roll number*. Number the pages. **Justify your answers, but keep them short; make sure you have time to deal with the more serious questions.**

Maximum Marks 60/65

(1) [4] Consider the following 2×2 matrix

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

(a) Consider its action on $\mathbb{R}^2$. What is the minimal polynomial? What is the characteristic polynomial? Is there a cyclic vector?

(b) Consider its action on $\mathbb{C}^2$. What is the minimal polynomial? What is the characteristic polynomial? Is there a cyclic vector?

(2) [2] A finite domain is a field. (commutative)

(3) [3] Let p be an *odd* prime, and $q = p^n$. Prove that exactly half the elements of $\mathbb{F}_q^*$ are squares. Prove that, on the other hand, every element of $\mathbb{F}_{2^n}$ is a square.

(4) [8] Find the irreducible (monic) polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$. You will find that this has integral coefficients. Show that this polynomial is reducible modulo p for every prime p.

(5) [3+3] (a) Prove that $f, g \in K[t]$ are relatively prime iff they have no common zeroes in any extension L of K. (b) Let f be a nonconstant polynomial in $K[t]$. Prove that f and f' are coprime in $K[t]$ iff f has no multiple roots in any extension L.

(6) [2] Let f be a nonconstant polynomial in $K[t]$ and suppose that L has *deg* f distinct roots in L. Prove that if $\tilde{L}$ is another extension in which f splits into linear factors:

$$f(t) = c\prod_i (t - \tilde{\alpha}_i) \in \tilde{L}[t]$$

Then the roots $\tilde{\alpha}_i$ also have multiplicity one.

(7) [4] Let $K/\mathbb{Q}$ be a degree 4 extension such that it has no intermediate fields. Give an example of such an extension. Can K be Galois over $\mathbb{Q}$?

(8) [12] Find the Galois groups of:

(a) $x^3 - 10$ over $\mathbb{Q}(\sqrt{2})$.

(b) $x^4 + 2$ over $\mathbb{F}_3$.

(9) [4] Let E/F be a finite Galois extension of fields of characteristic zero. Prove that there exists a primitive element.

(10) [4] Prove that if L/K is a finite (not necessarily separable!) extension, then $|Aut(L/K)|$ divides $[L : K]$.

(11) [16] For an integer $n \geq 3$ consider the cyclotomic extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$.

(a) Prove that any Galois transformation of $\mathbb{Q}(\mu_n)/\mathbb{Q}$ permutes the primitive n^{th} roots of unity. Give an example of a permutation of the set of primitive n^{th} roots which is *not* implemented by a Galois transformation of $\mathbb{Q}(\mu_n)/\mathbb{Q}$.

(b) Prove that every intermediate field $\mathbb{Q}(\mu_n)/F/\mathbb{Q}$ is Galois over $\mathbb{Q}$.

From now on let $n = p$, an odd prime.

(c) How many intermediate fields $\mathbb{Q}(\mu_p)/F/\mathbb{Q}$ exist?

(d) Calculate the trace and norm of ξ_p where ξ_p is a nontrivial p^{th} root.

(e) Prove the existence of a normal basis of $\mathbb{Q}(\mu_p)$.