Math 535
Solutions to the Final Exam

Tuesday, May 7, 2024

Part I (30 minutes)

Briefly define the following six terms:

1. splitting field of a polynomial

   Solution: If $f(x) \in k[x]$ is a polynomial, an extension field E of k is called a splitting field for $f(x)$ if $f(x)$ factors into linear factors over E, but not over any proper subfield of E.

2. character of a representation

   Solution: The character of a representation $\rho\colon G \to \mathrm{End}_k(V)$ is the function $\chi_V\colon G \to k$ defined by $\chi_V(g) = \mathrm{tr}_V\, \rho(g)$.

3. degree of a field extension

   Solution: The degree of a field extension $k \subseteq E$ is the dimension of E as a k-vector space.

4. complex of A-modules

   Solution: A complex of A-modules is a collection of A-modules M_n, indexed by $n \in \mathbb{Z}$, and a collection of homomorphisms $d_n\colon M_n \to M_{n-1}$, such that $d_n \circ d_{n+1} = 0$ for all $n \in \mathbb{Z}$.

5. minimal polynomial of an endomorphism

   Solution: The minimal polynomial of an endomorphism $T\colon V \to V$ is the monic polynomial $m(x) \in k[x]$ of least degree for which $m(T) = 0$.

6. Galois extension

   Solution: A field extension $k \subseteq E$ is a Galois extension if $E^{\mathrm{Aut}_k(E)} = k$.

Give examples for the following four phenomena:

1. A finite field extension that is not Galois

   Solution: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$

2. A 2×2-matrix with entries in $\mathbb{Q}$ that is not diagonalizable

   Solution: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

3. A module over the ring $\mathbb{Z}$ that is flat but not free

   Solution: $\mathbb{Q}$

4. An irreducible representation of the group S_3 of dimension ≥ 2

   Solution: The subrepresentation $V = \{\, a \in \mathbb{C}^3 \mid a_1 + a_2 + a_3 = 0 \,\}$ inside the permutation representation of S_3 on $\mathbb{C}^3$.

It is enough to describe each example very briefly; you do *not* need to prove that your example works.

Part II (135 minutes)

1. Determine whether or not $i = \sqrt{-1}$ belongs to the field $\mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$. Justify your answer.

   Solution: The polynomial $x^3 + x + 1$ has no roots in $\mathbb{Q}$, and so it is irreducible (for degree reasons). This means that $\mathbb{Q}(\alpha)$ is an extension of degree 3 over $\mathbb{Q}$. Therefore it cannot contain the field $\mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$, because 2 does not divide 3.

2. Let $f(x) = x^4 - 5x^2 + 6$. Determine the Galois group G of $f(x)$ over $\mathbb{Q}$. List all subgroups of G and the intermediate fields that they correspond to under the Galois correspondence.

   Solution: We have

   $$f(x) = (x^2 - 2)(x^2 - 3) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3}),$$

   and so the splitting field of $f(x)$ is $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know that this has degree 4 over $\mathbb{Q}$. Being the splitting field of a polynomial over $\mathbb{Q}$, the field extension $\mathbb{Q} \subseteq E$ is normal and separable, and therefore a Galois extension. It follws that $G = \mathrm{Gal}(E/\mathbb{Q})$ is a group of order 4. Because every element of the Galois group has to permute the two roots $\pm\sqrt{2}$ of the polynomial $x^2 - 2$ (and the two roots $\pm\sqrt{3}$ of the polynomial $x^2 - 3$), the four elements of G must be e, g, h, and gh, where g is the automorphism that swaps $\pm\sqrt{2}$ and leaves $\sqrt{3}$ fixed, and where h is the automorphism that swaps $\pm\sqrt{3}$ and leaves $\sqrt{2}$ fixed. So $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

There are five subgroups of G, namely

$$\{e\}, \quad G, \quad \{e,g\}, \quad \{e,h\}, \quad \{e,gh\}.$$

Their fixed fields are the five subfields

$$E, \quad \mathbb{Q}, \quad \mathbb{Q}[\sqrt{3}], \quad \mathbb{Q}[\sqrt{2}], \quad \mathbb{Q}[\sqrt{6}].$$

3. Consider the matrix

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

Determine the characteristic polynomial, the minimal polynomial, and the Jordan canonical form of A.

Solution: The characteristic polynomial is

$$f_A(x) = \det(xI_4 - A) = (x-1)^4,$$

due to A being upper triangular. We have $\ker(A - I_4) = \langle e_1, e_2 \rangle$ and

$$(A - I_4)(e_3) = e_1 \quad \text{and} \quad (A - I_4)(e_4) = e_1 + e_2,$$

and so $(A - I_4)^2 = 0$; this shows that the minimal polynomial is

$$m_A(x) = (x-1)^2.$$

Since $\ker(A - I_4)$ has dimension 2, there are exactly two Jordan blocks, so both must be of size 2. So the Jordan canonical form is

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

4. Determine the degree of the field extension $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ over $\mathbb{Q}$, and find an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

Solution: Consider the two subfields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{2})$. They have degree 2 respectively 3 over $\mathbb{Q}$, and so $(K : \mathbb{Q})$ must be divisible by both 2 and 3. This gives $(K : \mathbb{Q}) \geq 6$. From the chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) = K,$$

we see that $(K\colon \mathbb{Q}) \leq 6$, and so $(K\colon \mathbb{Q}) = 6$.

For the second part, we can use $\alpha = \sqrt{3} \cdot \sqrt[3]{2}$. With this choice,

$$\alpha^3 = 6\sqrt{3} \quad \text{and} \quad \alpha^4 = 18\sqrt[3]{2}$$

and therefore $\sqrt{3}$ and $\sqrt[3]{2}$ belong to $\mathbb{Q}(\alpha)$. This gives $K = \mathbb{Q}(\alpha)$.

5. Let V be a finite-dimensional $\mathbb{Q}$-vector space. Let $T\colon V \to V$ be a nonzero endomorphism. Suppose that the only linear subspaces $W \subseteq V$ with $T(W) \subseteq W$ are the trivial ones $W = V$ and $W = \{0\}$. Prove that the characteristic polynomial of T must be irreducible.

   Solution: Suppose by contradiction that $f_T(x)$ has a nontrivial factorization $f_T(x) = g(x)h(x)$. According to the Cayley-Hamilton theorem, we have $g(T)h(T) = f_T(T) = 0$, which means that $\operatorname{im} h(T) \subseteq \ker g(T)$. The subspace $\ker g(T)$ is invariant under T, and so either $\ker g(T) = V$ or $\ker g(T) = \{0\}$. In the first case, we get $g(T) = 0$; in the second case, $g(T)$ is invertible, and so we get $h(T) = 0$. After swapping the two factors, if necessary, we may therefore assume that $g(T) = 0$.

   Write $g(x) = a_k x^k + \cdots + a_1 x + a_0$, with $a_k \neq 0$. Because T is nonzero, there is a vector $v \in V$ such that $Tv \neq 0$. Now consider the subspace

   $$W = \langle v, Tv, T^2 v, \ldots, T^{k-1} v \rangle \neq \{0\}.$$

   It is invariant under T because $a_k T^k v + \cdots + a_1 T v + a_0 v = g(T)v = 0$ shows that $T^k v \in W$. Since $\dim W \leq k < \deg f_T(x) = \dim V$, we have $W \neq V$, which is a contradiction.

6. Let $k \subseteq E$ be a Galois extension of degree n, let p be a prime number that divides n, and write $n = p^e m$, where $(m, p) = 1$.

   (a) Show that there is an intermediate field $k \subseteq F \subseteq E$ that has degree m over k.

   (b) Show that if F is Galois over k, then F is the unique subfield of E of degree m.

   Solution: Let $G = \operatorname{Gal}(E/k)$ be the Galois group of the extension. According to the Galois correspondence, subfields of E of degree m over k are in bijection with subgroups of G of index m. Any subgroup of this kind has order $m/n = p^e$, hence is exactly a Sylow p-subgroup of G. In (a), we can therefore choose any Sylow p-subgroup $S \subseteq G$ and let $F = E^S$. In (b), F is Galois if and only if S is a normal subgroup of G; according to the Sylow theorems, this happens exactly when there is a unique Sylow p-subgroup, hence a unique subfield of degree m.

7. Let G be a finite group, and let $\rho \colon G \to \mathbb{C}^*$ be a linear character. Find a 1-dimensional subrepresentation of the regular representation $\mathbb{C}[G]$ whose character is the given ρ.

   Solution: The (unique) 1-dimensional subrepresentation of this kind is spanned by the vector
$$v_\rho = \sum_{h \in G} \frac{1}{\rho(h)} [h] \in \mathbb{C}[G].$$
   Indeed, for any $g \in G$, we have
$$g \cdot v_\rho = \sum_{h \in G} \frac{1}{\rho(h)} [gh] = \sum_{h \in G} \frac{1}{\rho(g^{-1}h)} [h] = \sum_{h \in G} \frac{\rho(g)}{\rho(h)} [h] = \rho(g) v_\rho,$$
   due to the fact that $\rho \colon G \to \mathbb{C}^*$ is a group homomorphism. Since the trace of multiplication by $\rho(g)$ on a 1-dimensional vector space is the number $\rho(g)$, the character of this representation is exactly ρ.

8. Let A be a commutative ring with 1, and let
$$0 \longrightarrow M \xrightarrow{\ i\ } N \xrightarrow{\ p\ } F \longrightarrow 0$$
   be a short exact sequence of A-modules. Show that if F is free, then $N \cong M \oplus F$.

   Solution: By the mapping property of free modules, there is a morphism of A-modules $s \colon F \to N$ such that $p \circ s = \mathrm{id}$.
$$\begin{array}{ccccc} & & F & & \\ & \overset{s}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}} & & \\ N & \xrightarrow{\ p\ } & F & \longrightarrow & 0 \end{array}$$
   Now consider the morphism of A-modules
$$f \colon M \oplus F \to N, \quad f(x, y) = i(x) + s(y).$$
   It is easy to see that f is injective: if $f(x, y) = i(x) + s(y) = 0$, then $y = p(s(y)) = p(i(x) + s(y)) = 0$, and because i is injective, it follows that $x = 0$. To show that f is also surjective, let $z \in N$ be an arbitrary element. Set $y = p(z) \in F$. Then
$$p(z - s(y)) = y - y = 0,$$
   and since $\ker p = \operatorname{im} i$, there is an element $x \in M$ such that $z - s(y) = i(x)$. But then $f(x, y) = i(x) + s(y) = z$, as needed. This proves that f is bijective, hence an isomorphism of A-modules.