MATH 314, SPRING 2025 PRACTICE FINAL

Each problem is worth 10 points.

Problem 1. Find, with proof, a description of the tangent space at the identity of the group $SL_n(\mathbb{R})$ of $n \times n$ real matrices of determinant 1.

Solution. Using the formula for an $n \times n$ matrix A, $\det e^{At} = e^{t \operatorname{tr} A}$ and $\frac{d}{dt}e^{At} = Ae^{At}$ it follows that all of the matrices of trace 0 are in the tangent space, so we need to check that no other matrices occur. Let $g(t) = (a_{ij}(t))$ be a smooth mapping into $SL_n(\mathbb{R})$ with $g(0) = I$. We have $\det g(t) = 1 = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}(t) ... a_{n\sigma(n)}(t)$ and so

$$0 = \frac{d}{dt} \det g(t) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \sum_{k=1}^{n} a_{1\sigma(1)}(t) ... a'_{k\sigma(k)}(t) ... a_{n\sigma(n)}(t)$$

Using $g(0) = I$, only $\sigma = id$ survives the sum, and $0 = a'_{11}(0) + ... + a'_{nn}(0)$ or $\operatorname{tr} g'(0) = 0$.

Problem 2. Given a group G, a 1-dimensional character of G is a group homomorphism $\chi : G \to \mathbb{C}$. The dual group of Abelian G is $\hat{G}$, the group of 1-dimensional characters under multiplication of functions. Given a finite abelian group $G = (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_k\mathbb{Z})$ prove that given integers $b_1, ..., b_k$, there is a character $\chi_b(a_1, ..., a_k) = e^{2\pi i(\frac{a_1 b_1}{d_1} + \cdots + \frac{a_k b_k}{d_k})}$ and that all characters arise this way. Hence or otherwise prove G and $\hat{G}$ are isomorphic.

Solution. Given the group $H = \mathbb{Z}/d\mathbb{Z}$, the function for $b \in \mathbb{Z}$, $a \mapsto e^{2\pi i ab/d}$ defines a character χ_b, since the function is d-periodic, and hence well-defined, and $\chi(0) = 1$, $\chi(a + a') = \chi(a)\chi(a')$, $\chi(-a) = 1/\chi(a)$. These are all different characters by testing at 1. It follows in the same way that χ_b in the statement of the problem is a character, and all of these characters are distinct by testing on $(1, 0, ...0), (0, 1, 0, ..., 0), ..., (0, 0, ..., 1)$. Since the sum of the squares of the dimensions of the irreducible representations equals the order of the group, these are all characters, as we've already found $|G|$ characters. The symmetry of the definition of χ_b in a and b means G and $\hat{G}$ are isomorphic.

Problem 3. Give the proof that an odd prime p is the sum of two squares if and only if $p \equiv 1 \bmod 4$.

Solution. We consider $\mathbb{Z}[x]/(p, x^2+1)$ in two ways, using $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]/(p)$. We have p is the sum of two squares if and only if $(p) = (a+bi)(a-bi)$ is the product of principal ideals, which is equivalent to (p) is not prime in $\mathbb{Z}[i]$, which means $\mathbb{Z}[i]/(p)$ is not a field, which is equivalent to $x^2 + 1$ is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$, which is equivalent to -1 is a square mod p. As (-1) has order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, this is equivalent to there is an order 4 element in $\mathbb{Z}/(p-1)\mathbb{Z}$ which is equivalent to $p \equiv 1 \bmod 4$.

Problem 4. Given variables $x_1, ..., x_n$ write $\delta(x_1, ..., x_n) = (x_1 - x_2)(x_1 - x_3)...(x_{n-1} - x_n)$. Prove that if $\sigma \in S_n$ permutes the x_i, σ acts on δ by multiplying it by the sign of σ. Hence or otherwise explain that if K/F is the splitting field of a cubic irreducible polynomial f with Galois group S_3 then the discriminant of f is not a square in F.

Solution. We have $\sigma\delta = (x_{\sigma(1)} - x_{\sigma(2)})...(x_{\sigma(n-1)} - x_{\sigma(n)})$, in which each factor $x_i - x_j$ or $x_j - x_i$ appears exactly once. Hence $\sigma\delta = (-1)^{\operatorname{inv}\sigma}\delta$ where $\operatorname{inv}\sigma = \#\{i < j : \sigma(i) > \sigma(j)\}$ so $\sigma\delta = \operatorname{sgn}(\sigma)\delta$. Since δ is the square root of the discriminant, if the Galois group is S_3 it does not act by only even permutations of the roots of f, so δ is not fixed by Galois and the square root of the discriminant is not in the base field.

Problem 5. Give the proof that the multiplicative group of a finite field is cyclic. (Hint: the group is a finite abelian group, use the structure theorem.)

Solution. We know that in the fields F_q of q elements, $F_q^\times$ is an Abelian group of order $q-1$ and so $x^{q-1} = 1$ for all $x \neq 0$. Let $F_q^\times \equiv (\mathbb{Z}/d_1\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/d_k\mathbb{Z})$, $d_1|d_2|...|d_k$. Then $x^{d_k} = 1$ for all $x \in F_q^\times$. As F_q is a field this has at most d_k roots, so $d_k \geq q-1$. By considering the orders of the groups $d_k = q-1$ and this is the only factor occurring in the direct sum.

Problem 6. Given an $n \times n$ complex matrix A, its characteristic polynomial is $P_A(x) = \det(xI - A)$. Using Jordan normal form, prove $P_A(A) = 0$.

Solution. Write $\mathbb{R}^n = V_1 \oplus \cdots \oplus V_k$ where A acts on the subspace V_i as a Jordan block, $\dim V_i = m_i$,

$$A|_{V_i} = \begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i \end{pmatrix}_{m_i \times m_i}.$$

Thus $P_A(x) = (x-\lambda_1)^{m_1} \cdots (x-\lambda_k)^{m_k}$. Given $v \in V$ write $v = v_1+v_2+\cdots+v_k$ where $v_i \in V_i$. Then $P_A(A)v_i = (A - \lambda_1 I)^{m_1} \cdots (A - \lambda_k I)^{m_k} v_i$ and since the factors commute, it suffices to check $(A - \lambda_i I)^{m_i} v_i = 0$. This is the same as

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}_{m_i \times m_i}^{m_i} = 0,$$

which is true.