Notes

- PMATH 445/745 requires a solid foundation in linear algebra, group theory and ring theory. This assignment is meant to help you identify any weak points in your background. I've also added some commentary in purple to indicate how the problems below are relevant to this course.
- Hopefully most of the material below will be somewhat familiar. However, I suspect that some things will be unfamiliar—either because you've actually never seen them before or because the perspective taken here is new to you. (Or you've forgotten that you've seen them.)
- I'm happy to discuss any of these problems during office hours. Please stop by!

Problems

Q1. Homs, Ends and Auts. If A and B are algebraic 'objects', we write

- $\mathrm{Hom}(A, B)$ for the set of all homomorphisms from A to B;
- $\mathrm{End}(A) = \mathrm{Hom}(A, A)$ for the set of **endomorphisms** of A; and
- $\mathrm{Aut}(A)$ for the set of **automorphisms** of A, i.e. *invertible* endomorphisms $A \to A$ whose inverses are also endomorphisms.

By defining appropriate (and "natural") operations, show:

(a) If V and W are F-vector spaces, then $\mathrm{Hom}(V, W)$ is an F-vector space.

(b) If V is an F-vector space, then $\mathrm{End}(V)$ is a ring.

(c) If G is a group, then $\mathrm{Aut}(G)$ is a group.

I just want you to know what Hom, End and Aut are. The set of homs between representations is a prominent object in representation theory. Endomorphism rings play a central role in the algebraic approach to representation theory. Automorphism groups are the targets for group actions and representations.

Q2. Exact sequences. Given algebraic objects A, B, C (e.g. groups, rings, vector spaces, ...), a **short exact sequence** is a diagram of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0 \tag{$*$}$$

where $f\colon A \to B$ and $g\colon B \to C$ are homomorphisms (of the appropriate type, e.g. group homs if we're working with groups) such that

- f is injective. (We say $(*)$ is exact at A or that the piece $0 \to A \xrightarrow{f} B$ is exact.)
- g is surjective. (We say $(*)$ is exact at C or that the piece $B \xrightarrow{g} C \to 0$ is exact.)
- $\ker g = \mathrm{im}\, f$. (We say $(*)$ is exact at B or that the piece $A \xrightarrow{f} B \xrightarrow{g} C$ is exact.)

(a) Suppose $(*)$ is a short exact sequence of groups (or rings or vector spaces). Show that $B/f(A) \cong C$. [Frequently this is written sloppily as $B/A \cong C$, where A is being viewed as a subset of B via the injection $f\colon A \to B$.]

(b) Show that if

$$0 \to U \to V \to W \to 0$$

is a short exact sequence of vector spaces, then $V \cong U \times W$. Show by way of example that the analogous statement is false for groups. [**Hint:** S_3 contains a normal subgroup of order 3.]

This is also just lingo. It won't be *that* important in our course, but every math student should know what a short exact sequence is.

Q3. Matrix groups. Let $M_n(F)$ be the ring of $n \times n$ matrices with entries in the field F. The ring operations are addition and multiplication of matrices. Inside this ring, we can find several interesting multiplicative groups.

(a) The **general linear group** is $GL_n(F) = \{A \in M_n(F)\colon A \text{ is invertible}\}$. Prove that $GL_n(F)$ is a group under multiplication.

(b) If V is an F-vector space, we define $GL(V) = \{T\colon V \to V\colon T \text{ is an invertible linear map}\}$. Show that this is a group under composition and prove that, if $\dim V = n$, $GL(V)$ is isomorphic to $GL_n(F)$.

(c) The **special linear group** is $SL_n(F) = \{A \in GL_n(F)\colon \det(A) = 1\}$. Prove that $SL_n(F)$ is a subgroup of $GL_n(F)$. [**Hint:** A quick way would be to note that det is a homomorphism.]

(d) If F comes equipped with some extra linear algebraic structure (e.g. a bilinear form) then we can examine subgroups of $GL_n(F)$ that preserve that form.

(i) Let $F = \mathbb{C}^n$ and let $\langle\ ,\ \rangle$ be the standard Hermitian inner product. The (standard) **unitary group** is $U_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C})\colon \langle A\vec{x}, A\vec{y}\rangle = \langle \vec{x}, \vec{y}\rangle\}$. Prove that $U_n(\mathbb{C}) = \{A \in GL_n(\mathbb{C})\colon A^* = A^{-1}\}$, where A^* is the conjugate transpose of A and deduce that $U_n(\mathbb{C})$ is a subgroup of $GL_n(\mathbb{C})$.

(ii) Let $F = \mathbb{R}^n$ and let $\langle\ ,\ \rangle$ be the dot product. The (standard) **orthogonal group** is $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R})\colon \langle A\vec{x}, A\vec{y}\rangle = \langle \vec{x}, \vec{y}\rangle\}$. Prove that $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R})\colon A^T = A^{-1}\}$ and deduce that $O_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

Given a group, we'll want to "represent" it as a matrix group; this is the basic idea of representation theory. Furthermore, matrix groups themselves turn out to have interesting representations, so they sort of play a dual role in the subject. Speaking of duals...

Q4. Dual spaces. Let V be a vector space over a field F. Its dual space is the set V^* of linear maps $f\colon V \to F$. (That is, $V^* = \mathrm{Hom}(V, F)$.) Addition and scalar multiplication of linear maps turn V^* into a vector space. In this problem, assume that V is finite-dimensional.

(a) Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for V. For each i, define an element $v_i^* \in V^*$ by $v_i^*(v_j) = \delta_{ij}$ (Kronecker delta). Show that $\mathcal{B}^* = \{v_1^*, \ldots, v_n^*\}$ is a basis for V^*; this is called the **dual basis** corresponding to $\mathcal{B}$. Conclude that $V \cong V^*$. [**Note:** This isomorphism is *non-canonical*, i.e., it depends on a choice of basis. It also needs V to be finite-dimensional, since in the infinite-dimensional setting $V \not\cong V^*$.]

(b) Let $\mathcal{B}$ be a basis for V and let $\mathcal{B}^*$ be the dual basis for V^* as in part (a). Given $v \in V$ and $f \in V^*$, let $[v]_\mathcal{B}$ be the coordinate vector of v represented as a column, and let $[f]_{\mathcal{B}^*}$ be the coordinate vector of f represented as a *row*. Show that

$$f(v) = [f]_{\mathcal{B}^*}[v]_\mathcal{B},$$

where the product of the $1 \times n$ row and the $n \times 1$ column on the right side, which results in a 1×1 matrix, is being identified with a scalar. [**Note:** This shows that we can interpret elements of V^* as row vectors.]

(c) Show that a vector $v \in V$ is zero if and only if $f(v) = 0$ for all $f \in V^*$. [**Hint:** If $v \neq 0$, extend $\{v\}$ to a basis for V.]

(d) **Duality pairing.** Given $v \in V$ and $f \in V^*$, we often denote the value $f(v)$ by $\langle v, f\rangle$. This defines a *non-degenerate* bilinear mapping $\langle\ ,\ \rangle\colon V \times V^* \to F$ which we refer to as the duality pairing between V and V^*. [Non-degenerate means: if $\langle v, f\rangle = 0$ for all $f \in V^*$ then $v = 0$; and if $\langle v, f\rangle = 0$ for all $v \in V$ then $f = 0$. Be sure to confirm that $\langle\ ,\ \rangle$ satisfies these two properties.]

Show that for each linear map $T\colon V \to V$, there is a unique linear map $T^*\colon V^* \to V^*$ that satisfies

$$\langle T(v), f\rangle = \langle v, T^*(f)\rangle .$$

Show also that the $\mathcal{B}^*$-matrix of T^* is the transpose of the $\mathcal{B}$-matrix of T. [**Hint:** The pairing actually defines $T^*(f)$ for you. Convince yourself that the the (i, j)th entry of $[T^*]_{\mathcal{B}^*}$ is $\left\langle e_i, T^*(e_j^*)\right\rangle$.]

As mentioned above, homs between representations are generally important, and homs to F are particularly important.

Q5. Invariant subspaces. Let $T\colon V \to V$ be a linear map. A subspace $U \subseteq V$ is said to be T**-invariant** if $T(U) \subseteq U$. In this problem, assume that V is finite-dimensional.

(a) Suppose U is T-invariant. Let $\mathcal{B}_U$ be a basis for U and extend it to a basis $\mathcal{B}$ for V. Show that the matrix $[T]_\mathcal{B}$ is block upper-triangular:

$$[T]_\mathcal{B} = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}.$$

Specifically, the upper-left block is the $\dim U \times \dim U$ matrix $[T|_U]_{\mathcal{B}_U}$.

(b) Suppose that $V = U \oplus W$ where both U and W are T-invariant. Let $\mathcal{B}_U$ and $\mathcal{B}_W$ be bases for U and W and set $\mathcal{B} = \mathcal{B}_U \cup \mathcal{B}_W$. Show that in this case $[T]_{\mathcal{B}}$ is block diagonal:

$$[T]_{\mathcal{B}} = \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}.$$

[**Special case:** If V is the direct sum of eigenspaces then $[T]_{\mathcal{B}}$ is diagonal.]

This will help us understand the decomposition of representations into smaller pieces.

Q6. Simultaneous diagonalizability. A family of matrices $\{A_i\}_{i=1}^m$ in $M_n(F)$ is simultaneously diagonalizable if there is a matrix P such that $P^{-1}A_iP$ is diagonal for all i. Show that a commuting family (i.e. $A_iA_j = A_jA_i$) of diagonalizable matrices is simultaneously diagonalizable. [**Hint:** Suppose E_λ is an eigenspace for A_i. What can you say about A_jE_λ?]

This will help us understand representations of finite abelian groups.

Q7. A diagonalizability criterion. Let F be an algebraically closed field. A matrix $A \in M_n(F)$ is diagonalizable if and only if there exists a non-zero polynomial $f(x) \in F[x]$ *with no repeated roots* such that $f(A) = 0$. Use this to show that if $A \in M_n(F)$ satisfies $A^k = I$ for some $k \in \mathbb{Z}_{>0}$ such that $\operatorname{char} F \nmid k$ (see below for $\operatorname{char} F$), then A is diagonalizable.

Not hugely important, but will be nice to know.

Q8. Facts about S_n. Prove:

(a) S_n is generated by transpositions (2-cycles).

(b) $a, b \in S_n$ are conjugate if and only if they have the same cycle type.

(c) If the cycle decomposition of $a \in S_n$ contains k_1 1-cycles, k_2 2-cycles, and so on, then the size of the conjugacy class in S_n containing a is equal to

$$\frac{n!}{1^{k_1}k_1!2^{k_2}k_2!\cdots n^{k_n}k_n!}.$$

We're going to explore the representation theory of S_n in the course.

Q9. char F. The **characteristic** of a field F, denoted by $\operatorname{char} F$, is the smallest positive integer n such that

$$\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0 \text{ in } F$$

provided such an integer n exists; otherwise we define the characteristic of F to be 0.

(a) Show that the characteristic of a field is either 0 or a prime number.

(b) Show that if $\operatorname{char} F = 0$ then F contains a copy of $\mathbb{Q}$. Otherwise, if $\operatorname{char} F = p$, then F contains a copy of $\mathbb{F}_p$, the finite field of size p.

[**Hint:** The slick proof is to consider the ring homomorphism $f : \mathbb{Z} \to F$ defined by sending 1 to 1. Then $\mathbb{Z}/\ker f$ sits inside F as an integral domain. What does this say about $\ker f$?]

Some parts of representation theory get weird if the underlying field has positive characteristic. We will want to be vaguely aware of this.