Math 561/661 **Fall 2018**
Homework 4 **Drew Armstrong**

---

1. Permutation Matrices. Let S_n be the group of permutations of the set $\{1, 2, \ldots, n\}$, and for each permutation $f \in S_n$ let $[f] \in \mathrm{Mat}_n(\mathbb{Q})$ be the matrix whose i, j-entry is 1 if $f(j) = i$ and 0 if $f(j) \neq i$.

(a) If $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{R}^n$ is the standard basis, prove that $[f]\mathbf{e}_i = \mathbf{e}_{f(i)}$ for all $i \in \{1, \ldots, n\}$.
(b) Use (a) to prove that the function $f \mapsto [f]$ is a group homomorphism $S_n \to O(n)$.
(c) Let $\det : O(n) \to \{\pm 1\}$ be the determinant. Use (b) to prove that $\varphi(f) := \det[f]$ is a group homomorphism $\varphi : S_n \to \{\pm 1\}$.
(d) Show that the kernel of φ is the alternating subgroup $A_n \subseteq S_n$ which was defined on the first homework. [Hint: If $t \in S_n$ is a transposition then $\varphi(t) = -1$.]
(e) Use the First Isomorphism Theorem and Lagrange's Theorem to conclude that

$$\#A_n = n!\,/\,2.$$

2. Dimension of a Vector Space. Let $(\mathbb{F}, +, \times, 0, 1)$ be a field (of "scalars") and let $(V, +, \mathbf{0})$ be an abelian group (of "vectors"). We say that V is a *vector space over* $\mathbb{F}$ if there exists a function $\mathbb{F} \times V \to V$ denoted by $(a, \mathbf{u}) \mapsto a\mathbf{u}$ that satisfies four axioms:

- For all $\mathbf{u} \in V$ we have $1\mathbf{u} = \mathbf{u}$.
- For all $a, b \in \mathbb{F}$ and $\mathbf{u} \in V$ we have $(ab)\mathbf{u} = a(b\mathbf{u})$.
- For all $a, b \in \mathbb{F}$ and $\mathbf{u} \in V$ we have $(a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$.
- For all $a \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in V$ we have $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$.

(a) In this case prove that $0\mathbf{u} = \mathbf{0}$ for all $\mathbf{u} \in V$ and $a\mathbf{0} = \mathbf{0}$ for all $a \in \mathbb{F}$.
(b) **Steinitz Exchange.** For all vectors $\mathbf{u}_1, \ldots, \mathbf{u}_m \in V$ we define their *span* as the set

$$\mathbb{F}(\mathbf{u}_1, \ldots, \mathbf{u}_m) := \{a_1\mathbf{u}_1 + \cdots + a_m\mathbf{u}_m : a_1, \ldots, a_m \in \mathbb{F}\} \subseteq V$$

and we say that $\mathbf{u}_1, \ldots, \mathbf{u}_m$ is a *spanning set* when $\mathbb{F}(\mathbf{u}_1, \ldots, \mathbf{u}_m) = V$. We say that $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ is an *independent set* if for all $b_1, \ldots, b_n \in \mathbb{F}$ we have

$$(b_1\mathbf{v}_1 + \cdots + b_n\mathbf{v}_n = \mathbf{0}) \Rightarrow (b_1 = \cdots = b_n = 0).$$

If $\mathbf{u}_1, \ldots, \mathbf{u}_m$ are spanning and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are independent, prove that $n \leq m$. [Hint: Assume for contradiction that $m < n$. Since the $\mathbf{u}_i$ are spanning we have $\mathbf{v}_1 = \sum_i a_i\mathbf{u}_i$ and since the $\mathbf{v}_j$ are independent, not all of the coefficients are zero. Without loss suppose that $a_1 \neq 0$ and use this to show that $\mathbf{v}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ is spanning. Now show by induction that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a spanning set and use this to obtain a contradiction.]
(c) An independent spanning set is called a *basis* of V. If V has a finite spanning set, prove that V has a finite basis.
(d) Continuing from (b) and (c), prove that any two finite bases have the same size. This size is called the *dimension* of the vector space V.

3. Conjugacy Classes. Let G be a group and for all $a, b \in G$ define the following relation:

$$a \sim b \iff a = gbg^{-1} \text{ for some } g \in G.$$

(a) Prove that this is an equivalence relation, called *conjugacy*.
(b) Compute the conjugacy classes for the group of symmetries of an equilateral triangle:

$$D_6 = \langle R, F \rangle = \{I, R, R^2, F, RF, R^2F\}.$$

Observe that conjugate elements "do the same thing" to the triangle.

(c) Explicitly describe the conjugacy classes of the symmetric group S_n. [Hint: Let $f, g \in S_n$. Show that g sends i to j if and only if fgf^{-1} sends $f(i)$ to $f(j)$. What does this say about the cycle structure?]

4. Multiplication of Subgroups, Part II. Let $(G, *, \varepsilon)$ be a group and let $H, K \subseteq G$ be any two subgroups.

(a) If at least one of H or K is normal, prove that $HK \subseteq G$ is a subgroup and hence that HK equals the join $H \vee K$. The converse is not true.

(b) Prove that the multiplication function $\mu : H \times K \to G$ is a group isomorphism if and only if (1) H and K are both normal, (2) $H \wedge K = \{\varepsilon\}$ and (3) $H \vee K = G$. In this case we write
$$G = H \times K$$
and we say that G is the *internal direct product* of the subgroups H and K.

5. Euler's Rotation Theorem. Recall the definition of the special orthogonal group:
$$SO(3) = \{A \in \text{Mat}_3(A) : A^T A = I \text{ and } \det(A) = 1\}.$$
We have seen that every element of this group is an isometry of $\mathbb{R}^3$. Now you will show that every element of this group is a **rotation**.

(a) Recall that there exists a nonzero vector $\mathbf{0} \neq \mathbf{u} \in \mathbb{R}^3$ satisfying $A\mathbf{u} = \lambda\mathbf{u}$ if and only if $\det(A - \lambda I) = 0$. Prove that there exists a unit vector $\mathbf{u} \in \mathbb{R}^3$ satisfying $A\mathbf{u} = \mathbf{u}$.

(b) For all $\mathbf{v}$ perpendicular to $\mathbf{u}$, prove that $A\mathbf{v}$ is perpendicular to $\mathbf{u}$.

(c) Prove that there exists a matrix $B \in SO(3)$ and a real number $\theta \in \mathbb{R}$ such that
$$B^{-1}AB = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{array}\right).$$
[Hint: Choose unit vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^3$ so that $\mathbf{u}, \mathbf{v}, \mathbf{w}$ are mutually perpendicular. These are the columns of B.] It follows from this that $\mathbf{x} \mapsto A\mathbf{x}$ is a rotation around the vector $\mathbf{u}$ by angle θ.