Math 55a

September 29, 2025

§1 Midterm 1 Review

Part 1: Groups

A *group* $(G, \cdot)$ is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying the following axioms:

1. There exists an identity element $e \in G$ such that $eg = ge = g$ for all $g \in G$.
2. For each $g \in G$, there exists an inverse $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.
3. The operation is associative: $(ab)c = a(bc)$ for all $a, b, c \in G$.

A group is said to be *abelian* if its operation is commutative, that is, if $ab = ba$ for all $a, b \in G$.

Examples.

- $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{C}^\times, \cdot)$.
- Symmetric groups S_n.
- Dihedral groups D_n.
- Cyclic groups $C_n \cong \mathbb{Z}/n\mathbb{Z}$
- Direct products of groups, such as $(a, b)(a', b') = (aa', bb')$ in $A \times B$.

Just as sets can be finite, countable, or uncountable, groups can also take these forms. For example, $\mathbb{Z}_n$ and S_n are finite groups, $\mathbb{Z}$, $\mathbb{Z}^n$, and $\mathbb{Q}$ are countable groups, while $\mathbb{R}$ is an uncountable group.

A subgroup $H \subseteq G$ is a nonempty subset of G that is itself a group under the operation of G. Explicitly, H is a subgroup if $a, b \in H$ implies $ab \in H$ and $a^{-1} \in H$. A key example is that all subgroups of $(\mathbb{Z}, +)$ are of the form $n\mathbb{Z}$ for some $n \geq 0$.

A *homomorphism* $\varphi : G \to H$ between two groups is a map such that

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{for all } a, b \in G.$$

If φ is bijective, it is called an *isomorphism*. An automorphism is an isomorphism from a group to itself. The set of all automorphisms of a group G forms a group under composition, denoted $\mathrm{Aut}(G)$.

The *kernel* of a homomorphism $\varphi : G \to H$ is

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e_H\},$$

which is always a normal subgroup of G. The homomorphism φ is injective if and only if $\ker \varphi = \{e_G\}$.

> **Remark 1.1.** This injectivity criteria only applies to homomorphisms. *Functions* (which are not necessarily homomorphisms) can have trivial kernels without being injective.

The *image* of φ is

$$\mathrm{Im}(\varphi) = \{\varphi(g) \mid g \in G\},$$

which is a subgroup of H.

Given $a \in G$, the map $n \mapsto a^n$ defines a homomorphism $\mathbb{Z} \to G$, whose image is the cyclic subgroup $\langle a \rangle$ generated by a. The kernel of this map is $n\mathbb{Z}$, where n is the order of a. Thus, if a has order n, then $\langle a \rangle \cong \mathbb{Z}_n$. In particular, G is said to be *cyclic* if it can be generated by a single element.

> **Problem** (Artin M.3) — Classify all groups of order 6

A subgroup $H \subseteq G$ is *normal* if $aH = Ha$ for all $a \in G$, equivalently if $aHa^{-1} = H$ for all $a \in G$. For a normal subgroup H, one can form the quotient group G/H, whose elements are the left cosets aH, with multiplication given by $(aH)(bH) = (ab)H$. The size of the quotient group satisfies $|G/H| = |G|/|H|$ whenever G is finite.

> **Problem** (Artin 12.1) — Show that if a subgroup H of a group G is not normal, then there exist left cosets aH and bH whose product is not a coset.

The *First Isomorphism Theorem* states that if $\varphi : G \to H$ is a group homomorphism, then

$$G/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

A group is called *simple* if it has no nontrivial normal subgroups. For example, $\mathbb{Z}/p\mathbb{Z}$ is simple whenever p is prime.

Finally, the *center* of a group G is defined as

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\},$$

which is always a normal subgroup of G. In fact, $Z(G)$ is abelian by definition.

Problem (Artin 12.4) — Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicity. Is G/H isomorphic to G?

Remark 1.2. When we know that the order of a group is finite and "small", we can guess at which group it is isomorphic to (cyclic, dihedral, etc.). There is only a limited number of unique groups up to isomorphism when the order is low.

Part 2: Linear Algebra

A *field* $(k, +, \cdot)$ is a set k with two operations: addition and multiplication. The axioms are as follows:

- $(k, +)$ is an abelian group with identity 0.
- $(k^\times, \cdot) = (k \setminus \{0\}, \cdot)$ is an abelian group with identity 1.
- Multiplication distributes over addition: $a(b + c) = ab + ac$ for all $a, b, c \in k$.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is prime.

The *characteristic* of a field is the smallest $n \geq 1$ such that $1+1+\cdots+1 = 0$ (n times), if such an n exists. Otherwise, the characteristic is 0. For example, the characteristic of $\mathbb{R}$ is 0.

A *vector space* V over a field k is a set with:

- an addition $+ : V \times V \to V$ making $(V, +)$ into an abelian group, and

- scalar multiplication $k \times V \to V$ which is associative and distributive, with $1 \cdot v = v$ for all $v \in V$.

Examples. k^n, polynomial rings $k[x]$, continuous functions on $\mathbb{R}$.

A *subspace* $W \subseteq V$ is a subset closed under addition and scalar multiplication.

Given vectors $v_1, \ldots, v_n \in V$, the *span* is

$$\operatorname{span}(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} a_i v_i \;\middle|\; a_i \in k \right\}.$$

We say the vectors $v_1, \ldots, v_n$ are linearly independent if

$$a_1 v_1 + \cdots + a_n v_n = 0 \quad \implies \quad a_1 = \cdots = a_n = 0.$$

A *basis* of V is a set of linearly independent vectors which span V. All bases of V have the same cardinality, called the *dimension* of V, written $\dim V$.

A *linear map* $\varphi : V \to W$ between vector spaces over k is a function satisfying

$$\varphi(u + v) = \varphi(u) + \varphi(v), \qquad \varphi(\lambda u) = \lambda \varphi(u).$$

The collection of all linear maps $V \to W$ is denoted $\operatorname{Hom}(V, W)$, and forms a vector space.

If V is finite-dimensional with basis $\{v_1, \ldots, v_n\}$ and W is finite-dimensional with basis $\{w_1, \ldots, w_m\}$, then each $\varphi \in \operatorname{Hom}(V, W)$ can be represented by an $m \times n$ matrix A such that

$$\varphi(v_j) = \sum_{i=1}^{m} A_{ij} w_i.$$

Direct sum decomposition. Suppose $V = W_1 \oplus \cdots \oplus W_r$, meaning every $v \in V$ can be uniquely written as $v = w_1 + \cdots + w_r$ with $w_i \in W_i$, and $\dim V = \dim W_1 + \cdots + \dim W_r$. Then we say V decomposes as a direct sum of subspaces.

Rank-nullity formula. For a linear map $\varphi \in \operatorname{Hom}(V, W)$, with V finite-dimensional, we have

$$\dim V = \dim \ker(\varphi) + \dim \operatorname{Im}(\varphi).$$

Dual space. The dual vector space of V is

$$V^* = \operatorname{Hom}(V, k).$$

If $\{v_1, \ldots, v_n\}$ is a basis of V, then the *dual basis* is defined by linear maps $v_i^* \in V^*$ with $v_i^*(v_j) = \delta_{ij}$.

For any subspace $U \subseteq V$, the *annihilator* of U is

$$\mathrm{Ann}(U) = \{f \in V^* \mid f(u) = 0 \ \forall u \in U\},$$

which is a subspace of V^*.

Given $\varphi \in \mathrm{Hom}(V, W)$, its *transpose* is the map

$$\varphi^t : W^* \to V^*, \qquad \varphi^t(f) = f \circ \varphi.$$

If $U \subseteq V$ is a subspace, then the *quotient*

$$V/U = \{v + U \mid v \in V\}$$

is also a vector space, with natural projection map $V \to V/U$. This projection is surjective with kernel U. A map $\varphi : V \to W$ factors through V/U if and only if $U \subseteq \ker(\varphi)$.

Remark 1.1. As you might notice, this is very similar to what we know about quotients of groups. In fact, an easy way to remember the rank-nullity formula is to think of it as the vector-analogue of the first isomorphism theorem.

Problem (Axler 2B.8) — Prove or give a counterexample to the following statement:

Suppose $\{v_1, v_2, v_3, v_4\}$ is a basis of a vector space V, and let U be a subspace of V such that $v_1, v_2 \in U$, while $v_3 \notin U$ and $v_4 \notin U$. Then $\{v_1, v_2\}$ is a basis of U.

Problem (Axler 3B.5, 3B.6) —

1. Give an example of a linear operator $T \in \mathrm{End}(\mathbb{R}^4)$ such that
$$\mathrm{im}(T) = \ker(T).$$
2. Prove that there does not exist a linear operator $T \in \mathrm{End}(\mathbb{R}^5)$ such that
$$\mathrm{im}(T) = \ker(T).$$

We call an element $\varphi \in \mathrm{Hom}(V, V)$ a *linear operator* on V; $W \subset V$ is an *invariant subspace* of φ if $\varphi(W) \subset W$.

Examples. $\ker(\varphi)$, $\mathrm{im}(\varphi)$, *eigenspaces* $\ker(\varphi - \lambda I)$.

If V is a direct sum of invariant subspaces V_i, there exists a basis of V where the matrix M of φ in this basis is block diagonal:

$$\begin{pmatrix} \varphi_{|V_1} & 0 \\ 0 & \varphi_{|V_2} \end{pmatrix}$$

If V has a basis composed of *eigenvectors* $v_i \in V$, $v_i \neq 0$, $\varphi(v_i) = \lambda_i v_i$, then φ is *diagonalizable*, i.e. there exists a basis where the matrix representing φ is a diagonal matrix. Eigenvectors of φ with distinct eigenvalues are linearly independent.

If k is algebraically closed (i.e. $\mathbb{C}$), any linear operator φ has an eigenvalue; there exists a basis where the matrix of φ is upper triangular. These three statements are all equivalent:

1. $\lambda \in k$ is an eigenvalue of φ
2. $\varphi - \lambda$ is not invertible
3. λ appears on the diagonal in a triangular matrix representing φ

Problem (Axler 5A.13) — Suppose $T \in \mathrm{Hom}(V, V)$. Suppose $S \in \mathrm{Hom}(V, V)$ is invertible.

a) Prove that T and $S^{-1}TS$ have the same eigenvalues.

b) What is the relationship between the eigenvectors of T and the eigenvectors of $S^{-1}TS$?