MATH COMPREHENSIVE EXAM NOTES

ALEXANDER LEE

Linear Algebra

Vector Spaces and Subspaces

Definition. A (real) *vector space* is a set V (whose elements are called *vectors*) together with

(1) an operation called *vector addition*, which for each pair of vector $\vec{x}, \vec{y} \in V$ produces another vector in V denoted $\vec{x} + \vec{y}$, and
(2) an operation called *multiplication by a scalar* (a real number), which for each vector $\vec{x} \in V$, and each scalar $c \in \mathbb{R}$ produces another vector in V denoted $c\vec{x}$.

Furthermore, the two operations must satisfy the follow *axioms*:

(1) For all vectors $\vec{x}, \vec{y}$, and $\vec{z} \in V$, $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$.
(2) For all vectors $\vec{x}$ and $\vec{y} \in V$, $\vec{x} + \vec{y} = \vec{y} + \vec{x}$.
(3) There exists a vector $\vec{0} \in V$ with the property that $\vec{x} + \vec{0} = \vec{x}$ for all vectors $\vec{x} \in V$.
(4) For each vector $\vec{x} \in V$, there exists a vector denoted $-\vec{x}$ with the property that $\vec{x} + -\vec{x} = \vec{0}$.
(5) For all vectors $\vec{x}$ and $\vec{y} \in V$ and all scalars $c \in \mathbb{R}$, $c(\vec{x} + \vec{y}) = c\vec{x} + c\vec{y}$.
(6) For all vectors $\vec{x} \in V$, and all scalars c and $d \in \mathbb{R}$, $(c + d)\vec{x} = c\vec{x} + d\vec{x}$.
(7) For all vectors $\vec{x} \in V$, and all scalars c and $d \in \mathbb{R}$, $(cd)\vec{x} = c(d\vec{x})$.
(8) For all vectors $\vec{x} \in V$, $1\vec{x} = \vec{x}$.

Examples. Some simple vector spaces:

- $\mathbb{R}^n$ is the vector space of ordered n-tuples of real numbers. Note: $\dim(\mathbb{R}^n) = n$.
- $P_n(\mathbb{R})$ is the vector space of polynomials of degree *less than or equal to* n. Note: $\dim(P_n(\mathbb{R})) = n + 1$.
- $M_{m\times n}(\mathbb{R})$ is the vector space of $m \times n$ matrices with real entries. Note: $\dim(M_{m\times n}(\mathbb{R})) = mn$.

Definition. Let V be a vector space and let $W \subseteq V$ be a subset. Then W is a (vector) *subspace* of V if W is a vector space itself under the operations of vector sum and scalar multiplication from V.

Notes. The empty set $\emptyset$ is not a vector space. Instead the smallest vector space is the trivial space, $\{\vec{0}\}$. Every vector space V has two obvious subspaces: the trivial subspace $\{\vec{0}\} \subseteq V$, and the improper subspace $V \subseteq V$.

Theorem (Subspace Theorem)**.** Let V be a vector space. A subset $W \subseteq V$ is a subspace if it satisfies the following properties:

(1) $W \neq \emptyset$
(2) For all $\vec{x}, \vec{y} \in W$ and all $c \in \mathbb{R}$, we have $c\vec{x} + \vec{y} \in W$.

Definition. Let V be a vector space, and let $S = \{\vec{v}_1, \ldots, \vec{v}_n\} \subseteq V$ be a finite set of vectors in V.

- A *linear combination* of elements of S is an expression $a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$ for some scalars $a_1, \ldots, a_n \in \mathbb{R}$.
- The *span* of S, denoted $\mathrm{Span}(S)$, is the set of all linear combinations of elements of S. That is,
$$\mathrm{Span}(S) = \{a_1\vec{v}_1 + \cdots a_n\vec{v}_n \mid a_1, \ldots, a_n \in \mathbb{R}\}.$$
- We define $\mathrm{Span}(\emptyset) = \{\vec{0}\}$.
- If $\mathrm{Span}(S) = W$, we say that S spans W.

Theorem. Let V be a vector space and let S be any subset of V. Then $\mathrm{Span}(S)$ is a subspace of V.

Theorem. If W is a subspace and $S \subseteq W$, then $\mathrm{Span}(S) \subseteq W$.

Definition. The set S is *linearly dependent* if there exists scalars $a_1, \ldots, a_n \in \mathbb{R}$ that are not all zero such that $a_1\vec{v}_1 + \cdots + a_n\vec{v}_n = \vec{0}$. S is *linearly independent* if it is not linearly dependent. Equivalently, for any scalars $a_1, \ldots, a_n \in \mathbb{R}$ such that $a_1\vec{v}_1 + \cdots a_n\vec{v}_n = \vec{0}$, we must have $a_1 = \cdots = a_n = 0$.

Definition. The set $S \subseteq V$ is a basis for V if S is linearly independent and $\mathrm{Span}(S) = V$.

Definition. The *dimension* of V is the number $\dim(V)$ of elements in a basis for V. If V has no finite basis, we say $\dim(V) = \infty$.

Theorem. Any two bases of V have the same number of elements.

Fact. The three kinds of row reduction steps are

(1) Switching two rows.
(2) Multiplying a row by a nonzero scalar.
(3) Adding a multiple of one row to another.

Definition. A matrix is in *echelon form* if it satisfies all of the following conditions:

(1) If a row is not a zero row (i.e., all entries of that row are zeros), then the first nonzero entry is a 1 (and called the *pivot*).
(2) If a column contains a pivot, then all other entries in that column are 0.
(3) If a row contains a pivot, then each row above contains a pivot further to the left. This also implies that zero rows, if any, appear at the bottom.

Variables corresponding to the pivots are called *pivot variables*. All other variables are called *free variables*.

Definition. A *homogeneous* system of linear equations is when all the linear combinations equal 0. A system is *inhomogeneous* otherwise.

Definition. The *nullspace* of a matrix A is the solution set of its corresponding homogeneous system of equations. The basis of the nullspace of A is the set of vectors that the free variables end up multiplied by in the solution.

Definition. The *column space* of a matrix A is the span of its columns. If B is the echelon form of A, then the columns of A corresponding to the columns of B with pivots form a basis of the column space.

Abstract Algebra

Groups

Definition. Suppose that:

(1) G is a set and $*$ is a binary operation on G,
(2) $*$ is associative,
(3) there exists an element e of G such that $\forall x \in G$
$$x * e = e * x = x \text{ (identity element)}$$
(4) for each $x \in G$, there exists an element $y \in G$ such that
$$x * y = y * x = e$$

Then G, together with the binary operation $*$, is called a *group* and denoted $(G, *)$.

Theorem. If $(G, *)$ is a group, then there is only one identity element in G.

Theorem. If $(G, *)$ is a group and $x \in G$, then x has only one inverse.

Definition. We say a group G is *abelian* if the group operation is commutative, i.e., if $xy = yx$ for all $x, y \in G$.

Notation. For $g \in G$ and $n \in \mathbb{Z}$, $g^n = g \cdot g \cdots g$ (n-times).

Notation. If the operation of G is called $+$, then we write ng instead of g^n.

Notation. When G is finite, its order $|G|$ is the number of elements in the group.

Notation. When $g \in G$ has finite order, its order $o(g)$ is the smallest integer $m > 0$ with $g^m = e$.

Notation. If $g^m = e$ for some $m \in \mathbb{Z}$, then $o(g) \mid m$.

Subgroups

Definition. Let $(G, *)$ be a group and $H \subseteq G$. H is a *subgroup* of G if the elements of H from a group under $*$. I.e. $(H, *)$ is a group.

Theorem. Let H be a nonempty subset of group G. Then, H is a subgroup of G if and only if

(1) $\forall a, b \in H$, $ab \in H$ and
(2) $\forall a \in H$, $a^{-1} \in H$.

Terminology: If H has property 1 we say it is closed under multiplication. If H has property 2 we say it is closed under inverses.

Definition. An element $g \in G$ generates the *cyclic* subgroup $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$.

Theorem. An element $g \in G$ has finite order if and only if $\langle g \rangle$ is finite, in which case $o(g) = |\langle g \rangle|$.

Theorem (Lagrange's Theorem)**.** If H is a subgroup of a finite group G, then $|H| \mid |G|$.

Corollary. If $|G|$ is prime, the G is cyclic.

Corollary. For all $g \in G$, we have $o(g) \mid |G|$.

Corollary. For all $g \in G$, we have $g^{|G|} = e$.

Cosets

Definition. If H is a subgroup of G, then by *right coset of H in G* we mean a subset of the form Hg, where $g \in G$ and

$$Hg = \{hg \mid h \in H\}.$$

Definition. If H is a subgroup of G, then by *left coset of H in G* we mean a subset of the form gH, where $g \in G$ and

$$gH = \{gh \mid h \in H\}.$$

Theorem. Two right cosets Hx and Hy are either the same set or disjoint sets. (That is, if they share even one element, they are exactly the same set.) The same holds for left cosets. (On the other hand, a right coset and a left coset can intersect each other without being the same set.)

Corollary (Right coset relation)**.** $Hx = Hy \iff xy^{-1} \in H \iff x \in Hy$.

Corollary (Left coset relation)**.** $xH = yH \iff y^{-1}x \in H \iff x \in yH$.

Corollary. $Hx = H \iff x \in H \iff xH = H$.

Notation. If G is abelian and the group operation is written as addition, then the left and right cosets of $H \subseteq G$ coincide and are written

$$H + a = \{h + a \mid h \in H\}.$$

Here, the coset relation becomes

$$H + a = H + b \iff a - b \in H \iff a \in H + b.$$

Definition. When a group G is a union of finitely many left cosets of a subgroup H, we say that *H has finite index in G* and the *index of H in G* is defined to be

$$[G : H] = \text{number of distinct left cosets of } H \text{ in } G.$$

The same holds for right cosets. When G is finite, $[G : H] = |G|/|H|$, since all cosets of H have the same number of elements.

Normal Subgroups

Theorem. Given a subgroup $H \subseteq G$, H being normal in G is equivalent to any of the following conditions:

- $gH = Hg$ for all $g \in G$.
- $gHg^{-1} = H$ for all $g \in G$.
- $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Corollary. When $N \subseteq G$ is a normal subgroup, every left coset is a right coset, and vice versa.

Theorem. The set of all cosets of N in G forms a group and is denoted G/N. The group operation is defined by $Na \cdot Nb = Nab$, which is well-defined since N is normal. When G is finite, G/N is also finite and $|G/N| = [G : N] = |G|/|N|$.

Group Homomorphisms

Definition. Let G and H be groups and let $\phi : G \to H$ be a function. We say that ϕ is a *homomorphism* if for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b).$$

Theorem. If $\phi : G \to H$ is a homomorphism, then

- $\phi(e_G) = e_H$.
- $\phi(g^n) = \phi(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$.