Linear Algebra
Lecture Notes in progress

László Babai

Version: November 11, 2007

These notes are based on the "apprentice course" and the "discrete mathematics" course given by the author at the Summer 2007 REU of the Department of Mathematics, University of Chicago. The author is grateful to the scribes Sundeep Balaji and Shawn Drenning (other scribes will be acknowledged as their parts get incorporated in the text).

1 Basic structures

1.1 Groups

A group is a set G endowed with a binary operation, usually called addition or multiplication, satisfying the following axioms (written in multiplicative notation):

(a) $(\forall a, b \in G)(\exists! ab \in G)$ (operation uniquely defined)

(b) $(\forall a, b, c \in G)((ab)c = a(bc))$ (associativity)

(c) $(\exists e \in G)(\forall a \in G)(ea = ae = a)$ (identity element)

(d) $(\forall a \in G)(\exists b \in G)(ab = ba = e)$ (inverses)

In additive notation, we postulate

(a) $(\forall a, b \in G)(\exists! a + b \in G)$ (operation uniquely defined)

(b) $(\forall a, b, c \in G)((a + b) + c = a + (b + c))$ (associativity)

(c) $(\exists e \in G)(\forall a \in G)(e + a = a + e = a)$ (identity element)

(d) $(\forall a \in G)(\exists b \in G)(a + b = b + a = e)$ (inverses)

The multiplicative identity is usually denoted by "1," the additive identity by "0." The multiplicative inverse of a is denoted by a^{-1}; the additive inverse by $(-a)$.

The group is *commutative* or *abelian* if it satisfies $(\forall a, b \in G)(ab = ba)$ (or $(\forall a, b \in G)(a + b = b + a)$ in the additive notation). The additive notation is customarily reserved for abelian groups.

Example 1.1.1. $(\mathbb{Z}, +)$ (the additive group of integers), $(\mathbb{Z}_n, +)$ (the additive group of modulo n residue classes), the general linear group $\mathrm{GL}_2(p)$ (2×2 matrices over $\mathbb{Z}_p$ with nonzero determinant (nonzero mod p where p is prime)) under matrix multiplication, the special linear group $\mathrm{SL}_2(p)$ (the subgroup of $\mathrm{GL}_2(p)$ consisting of those matrices with determinant $= 1 \pmod p$)

Exercise 1.1.2. If p is a prime $(\mathbb{Z}_p^\times, \cdot)$ is a group. Here $\mathbb{Z}_p^\times$ is the set of non-zero residue classes modulo p.

The *order* of a group is the number of elements of the group. For instance, the order of $(\mathbb{Z}_n, +)$ is n; the order of $(\mathbb{Z}_p^\times, \cdot)$ is $p - 1$; the order of $(\mathbb{Z}, +)$ is infinite. Note that the order of a group is at least 1 since it has an identity element. The idenity element alone is a group.

Exercise 1.1.3. Calculate the order of the special linear group $\mathrm{SL}_2(p)$. (Give a very simple exact formula.)

1.2 Fields

Informally, a *field* is a set $\mathbb{F}$ together with two binary operations, addition and multiplication, so that all the usual identities and rules of inversion hold (all nonzero elements have a multiplicative inverse). Here is the formal definition.

$(\mathbb{F}, +, \cdot)$ is a field if

(a) $(\mathbb{F}, +)$ is an abelian group (the additive group of the field);

(b) $(\mathbb{F}^\times, \cdot)$ is an abelian group (the multiplicative group of the field) (where $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$);

(c) $(\forall a, b, c \in \mathbb{F})(a(b + c) = ab + ac)$ (distributivity)

Examples: the real numbers ($\mathbb{R}$), the complex numbers ($\mathbb{C}$), the rational numbers ($\mathbb{Q}$), the modulo p residue classes ($\mathbb{F}_p$) (where p is a prime). (This latter is the same as $\mathbb{Z}_p$; we write $\mathbb{F}_p$ to emphasize that it is a field.) There are many other examples but only these will matter for us so you do not need to know the formal definition of a field, just think of these examples.

Note that every field has order ≥ 2 since it has a 0 (additive identity) and among the nonzero elements it has a 1 (multiplicative identity). $\mathbb{F}_2$ has order 2. The fields $\mathbb{F}_p$ are finite; they are not the only finite fields. There exists a unique finite field of order q for every prime power q (Galois).

Exercise 1.2.1. Prove: in a field, $ab = 0$ if and only if $a = 0$ or $b = 0$.

Exercise 1.2.2. Prove: multiplication in a field is associative. (Observe that this statement is NOT an axiom as given above. What is missing?)

Exercise 1.2.3. Prove: if $(\mathbb{Z}_n, +, \cdot)$ is a field then n is a prime.

Exercise 1.2.4. Prove: the numbers of the form $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ form a field. (This field is denoted $\mathbb{Q}[\sqrt{2}]$.)

Exercise* 1.2.5. Prove: the "complex numbers over $\mathbb{F}_p$" form a field if and only if $p \equiv -1 \pmod 4$. (The "complex numbers over $\mathbb{F}_p$" are the formal expressions $a + bi$ where $a, b \in \mathbb{F}_p$ and multiplication is performed using the rule $i^2 = -1$.)

2 Basic Concepts of Group Theory

2.1 Generators, subgroups

Definition 2.1.1. If H is a non-empty subset of G which is a group under the same operation as G, we say H is a subgroup of G and write $H \leq G$.

Exercise 2.1.2. A nonempty subset H of G is a subgroup if and only if for all $a, b \in H$ we have $ab^{-1} \in H$.

Observe: the "subgroup" relation is transitive: if $K \leq H$ and $H \leq G$, then $K \leq G$.

Definition 2.1.3. If $A, B \subseteq G$, then $A \cdot B = \{ab \mid a \in A, b \in B\}$.

Exercise 2.1.4. (a) $|AB| \leq |A||B|$; (b) $\emptyset \cdot B = \emptyset$; (c) if $A \neq \emptyset$ then $AG = G$.

Exercise 2.1.5. $H \subseteq G$ is a subgroup if and only if $H \neq \emptyset$ and $HH^{-1} \subseteq H$.

Exercise 2.1.6. The intersection of a family of subgroups of a group is a subgroup.

Definition 2.1.7. Let $S \subseteq G$ and let H be the intersection of all subgroups of G containing S. We say that H is the subgroup of G **generated by** S and write $\langle S \rangle = H$.

Exercise 2.1.8. Let S be a non-empty subset of G. We define

$$S^{-1} = \{s^{-1} \mid s \in S\}$$

and

$$(S \cup S^{-1})^n = \{a_1 a_2 \dots a_n \mid a_i \in S \cup S^{-1}\}.$$

Prove that

$$\langle S \rangle = \bigcup_{n=0}^{\infty} (S \cup S^{-1})^n.$$

2.2 Permutations, the symmetric group

The set of all bijections of a set Ω is a group under composition. We call this group the *symmetric group on* Ω and denote it $\mathrm{Sym}(\Omega)$. We call Ω the *permutation domain* and the elements of $\mathrm{Sym}(\Omega)$ *permutations* of Ω. If $|\Omega| = n$ we often denote $\mathrm{Sym}(\Omega)$ by S_n. We often will write elements of S_n using cycle notation. The symbol $(a_1, \ldots, a_k)$ denotes the "k-cycle" which moves a_i to a_{i+1} $(i = 1, \ldots, k-1)$ and a_k to a_1 (here the a_i are distinct elements of Ω); all other elements of Ω are fixed.

Composition of permutations is performed left to right. For example, $(123) = (13)(23)$ (verify!)

Exercise 2.2.1. Every permutation can be written as a product of disjoint cycles. This is referred to as the *cycle decomposition* of the permutation. This decomposition is unique apart from the order of the cycles and the possible omission of cycles of length 1.

Definition 2.2.2. Let the cycle-decomposition of a permutation σ consist of a cycle of length n_1, a cycle of length n_2, ..., and a cycle of length n_m, where $n_1 \geq n_2 \geq \cdots \geq n_m$. In this representation, we include all fixed points as cycles of length one. We say that σ has *cycle-type* $(n_1, n_2, \ldots, n_m)$.

Exercise 2.2.3. The order of S_n is $n!$.

Definition 2.2.4. A transposition is a 2-cycle.

Exercise 2.2.5. S_n is generated by the $n-1$ transpositions of the form $(i, i+1)$.

Exercise 2.2.6. (a) Let T be a set of transpositions. View T as the set of edges of a graph. Give a graph theoretic characterization of those T which generate S_n. (b) S_n cannot be generated by fewer than $n-1$ transpositions.

Exercise 2.2.7. The number of $(n-1)$-tuples of transpositions that generate S_n is n^{n-2}. (Hint: Cayley's Formula in Graph Theory.)

Definition 2.2.8. $\sigma \in S_n$ is **even** if it is a product of an even number of transpositions and **odd** if it is a product of an odd number of transpositions.

Exercise 2.2.9. If σ is even, then σ is not odd. (What you need to prove is that the identity permutation is not odd.)

Exercise 2.2.10. Prove: a k-cycle is an even permutation if and only if k is odd.

2.3 Lagrange's Theorem

Theorem 2.3.1 (Lagrange's Theorem). *If $H \leq G$, then $|H| \Big| |G|$.*

Proof. Define a relation by $a \sim b$ if $ab^{-1} \in H$.

Exercise 2.3.2. Verify that this is an equivalence relation.

We call the sets of the form aH (this is shorthand for $\{a\}H$) and Ha the left and right **cosets** of H, respectively. We have $ab^{-1} \in H$ if and only if $a \in Hb$. It follows that (a) the equivalence classes of the equivalence relation defined above are exactly the right cosets of H; and (b) all cosets are of the same size. We call the number of right cosets of H in G the **index** of H and G. This is denoted by $|G : H|$. Since all the cosets have the same number of elements, we must have $|G| = |H||G : H|$. □

Exercise 2.3.3. Prove: if $H \leq G$ then the number of right cosets and the number of left cosets is equal. (Your proof should work for infinite as well as for finite groups.)

Exercise 2.3.4. The only subgroups of $\mathbb{Z}$ are of the form $d\mathbb{Z}$ for $d \in \mathbb{N}$. What is $|\mathbb{Z} : d\mathbb{Z}|$? Show that two cosets of $a + d\mathbb{Z}$ and $b + d\mathbb{Z}$ are equal if and only if $a \equiv b \mod d$. Cosets of $d\mathbb{Z}$ in $\mathbb{Z}$ are called modulo d residue classes.

2.4 The alternating group

Definition 2.4.1. The set of all even permutations of S_n is a subgroup of S_n called the **alternating group of degree** n and denoted A_n.

Exercise 2.4.2. The 3-cycles generate A_n.

Exercise 2.4.3. If $n \geq 2$ then $|S_n : A_n| = 2$.

Exercise 2.4.4. For $n \geq 2$, A_n is the only subgroup of index 2 in S_n.

2.5 Two famous puzzles

Now we would like to study the number of possible configurations of **Rubik's cube** obtainable by pulling the cube apart and then reassembling it, without changing the colors on the faces of the "cubies." We think of the 6 face centers as fixed to the center. There are 8! ways to arrange the "corner cubies" and 12! ways to arrange the "edge cubies." Once the location of a corner cubie is fixed, there are 3 ways to place it; once the location of an edge cubie is fixed, there are 2 ways to place it. In all, this gives $8!12!3^8 2^{12}$ configurations. These configurations form a group which we call the "total group" T of Rubik's cube and call the subgroup of configurations obtained through legal moves G.

Exercise 2.5.1. $|T : G| = 12$.

Exercise 2.5.2. We will now describe what is known as **Sam Lloyd's 15 puzzle**. Suppose the numbers $1, 2, \ldots, 15$ and "blank" are arranged in a 4×4 grid. A legal move is to swap the empty cell ("blank") with an adjacent cell. Prove that it is not possible through legal moves to go from

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

to

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(so the first configuration is not "feasible" – the goal being to reach the second configuration). In fact, exactly half of the 16! configurations are feasible.

2.6 Generation, diameter, Cayley graphs

Exercise 2.6.1. $S_n = \langle (12\ldots n), (12) \rangle$

Definition 2.6.2. Let G be a group and S a subset of G. We define the **Cayley Graph** of G with respect to S to be the graph whose vertices are the elements of G with an edge between g_1 and g_2 if $g_1 = g_2 s$ for some $s \in S \cup S^{-1}$.

Definition 2.6.3. The **diameter** of group G with respect to a set S of generators is defined to be the diameter of the Cayley graph of G with respect to S and is denoted $\mathrm{diam}(G, S)$.

Exercise 2.6.4. Let $\sigma = (12\ldots n)$ and $\tau = (12)$. Then $\mathrm{diam}(S_n, \{\sigma, \tau\}) = \Theta(n^2)$.

2.7 Conjugacy

Definition 2.7.1. We say $a, b \in G$ are **conjugates** if $(\exists g \in G)(a = g^{-1}bg)$. **Conjugation** by g is the map $G \to G$ given by $a \mapsto g^{-1}ag$.

Definition 2.7.2. If G and H are groups, a map $\varphi : G \to H$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. A homomorphism that is also a bijection is called an **isomorphism**. An isomorphism from a group to itself is called an **automorphism**. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$ and is a group under composition.

Exercise 2.7.3. Conjugation by g is a group automorphism. Such automorphisms are called *inner automorphisms*. The group of all inner automorphisms of G is denoted $\mathrm{Inn}(G)$.

Observe that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$.

Exercise 2.7.4. Conjugacy (the relation of being conjugates) is an equivalence relation on G. We call the classes **conjugacy classes**.

Exercise 2.7.5. In S_n, two permutations are conjugate if and only if they have the same cycle structure.

2.8 Congruences of the plane

Definition 2.8.1. A map $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ is an *isometry* if it preserves distance. More generally, if $A, B \subset \mathbb{R}^n$, $\varphi : A \to B$ is an isometry if it is a distance preserving bijection. The set of all isometries of $\mathbb{R}^2$ is a group under composition. If there is an isometry between two subsets of $\mathbb{R}^n$, we say they are *congruent*.

Exercise 2.8.2. Every isometry of the plane is either

1. a translation, or
2. a rotation, or
3. a reflection (in an axis), or
4. a "glide reflection," that is, a reflection followed by a translation parallel to the axis of reflection.

The conjugates of an isometry are of the same type. In fact, a conjugate of a rotation by angle α is a rotation by $\pm\alpha$ (when is it $-\alpha$?), a conjugate of a translation is a the translation by a vector of the same length, and the same holds for the translation involved in a glide reflection.

2.9 Partitions

Definition 2.9.1. A **partition of a number** n is a sequence of natural numbers $a_1, \dots a_k$ satisfying $a_1 \geq a_2 \geq \ldots \geq a_k \geq 1$ such that $n = a_1 + \ldots + a_k$. The number of partitions of n is denoted $p(n)$.

Note that $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$.

Exercise 2.9.2. The number of conjugacy classes of S_n is $p(n)$.

A most amazing asymptotic formula for $p(n)$ was found Hardy and Ramanujan.

Theorem 2.9.3 (Hardy-Ramanujan). $p(n) \sim \frac{c_1}{n} \mathrm{e}^{c_2\sqrt{n}}$ *where* $c_1 = \frac{1}{4\sqrt{3}}$ *and* $c_2 = \frac{2\pi}{\sqrt{6}}$.

For an elementary proof of the weaker but still surprisingly tight inequality $\ln p(n) < \frac{2\pi}{\sqrt{6}}\sqrt{n}$, see Matoušek and Nešetřil's "Invitation to Discrete Mathematics," Chapter 10.7.

Exercise 2.9.4. Prove from first principles: $\log p(n) = \Theta(\sqrt{n})$.

2.10 Homormorphisms, normal subgroups

Definition 2.10.1. $N \leq G$ is a **normal subgroup**, denoted $N \lhd G$, if N is invariant under conjugation, i. e., $(\forall g \in G)(g^{-1}Ng \subseteq N)$.

Exercise 2.10.2. $N \leq G$ is a normal subgroup if and only if $(\forall g \in G)(g^{-1}Ng = N)$.

Note that every subgroup of an abelian group is normal.

Exercise 2.10.3. Let $\varphi : G \to H$ be a homomorphism and $N = \varphi^{-1}(1_H)$. Prove that N is a normal subgroup and the partition by φ is cosets of N.

Definition 2.10.4. If $\varphi : G \to H$ is a homomorphism, we define

$$\mathrm{Im}(\varphi) = \{\varphi(a) \,:\, a \in G\}$$

and

$$\ker(\varphi) = \{g \in G \,:\, \varphi(g) = 1\}.$$

Exercise 2.10.5. $\mathrm{Im}(\varphi) \leq H$ and $\ker(\varphi) \lhd G$.

Theorem 2.10.6. *For normal subgroups $N \lhd G$, the cosets Na form a group under the operation of set multiplication defined in 2.1.3.*

Proof. Using the fact that $aN = Na$, we see that $(Na)(Nb) = N(aN)b = Nab$. □

The group of cosets of N is denoted G/N and called a *quotient group*.

Example 2.10.7. *$d\mathbb{Z} \lhd \mathbb{Z}$ and $\mathbb{Z}/d\mathbb{Z} = \mathbb{Z}_d$.*

Exercise 2.10.8. If $\varphi : G \to H$ is a homomorphism then $\mathrm{Im}(\varphi) \cong G/\ker\varphi$.

2.11 The sign of a permutation

The sign of a permutation

$$\mathrm{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

is a homomorphism from S_n onto the multiplicative group $\{-1, 1\}$:

Exercise 2.11.1. For any $\sigma, \tau \in S_n$ we have $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$.

The kernel of sgn is A_n, so $S_n/A_n \cong \mathbb{Z}_2$.

2.12 Symmetries of Platonic solids

We would like to figure out the group of isometries of the Platonic solids. First we consider the tetrahedron T. We denote the group of isometries of T by $O(T)$. Any isometry of T is determined by what it does to the four vertices of T. This gives an injection φ of $O(T)$ into S_4. By looking at reflections across a plane intersecting two of the vertices and bisecting the edge connecting the other two vertices, we see that all transpositions are in the image of φ. We conclude that $\mathrm{Im}(\varphi) = S_4$; therefore $O(T) \cong S_4$.

Exercise 2.12.1. Give a simple explicit description of a spatial congruence that maps under φ to (1234).

We say an isometry of the space is **orientation preserving** if it turns a right hand into a right hand; and it is **orientation reversing** if it turns a right hand into a left hand.

Definition 2.12.2. The group of those congruences of $\mathbb{R}^3$ which fix the origin is called the 3-dimensional **orthogonal group** and is denoted $O(\mathbb{R}^3)$ or $O_3(\mathbb{R})$. Its index-2 subgroup consisting of the orientation preserving congruences that fix the origin is $SO(\mathbb{R}^3)$ or $SO_3(\mathbb{R})$, the **special orthogonal group.**

We have, as usual, a homomorphism $\varphi : O(\mathbb{R}^3) \to \{1, -1\}$ given by $\varphi(x) = 1$ if and only if x is orientation preserving; $\ker(\varphi) = SO(\mathbb{R}^3)$. So, $SO(\mathbb{R}^3) \lhd O(\mathbb{R}^3)$.

Since the only subgroup of index 2 in S_4 is A_4, we must have that $SO(T) = A_4$.

Now let us find the $O(\text{cube})$. Any vertex v of a cube can be mapped to one of 8 vertices. Once we decide where v is mapped, there are 3 possibilities for where a vertex adjacent to v can be mapped. Once we fix this, we can do one additional reflection. We conclude that $|O(\text{Cube})| = 48$. A cube has four main diagonals. Any member of $O(\text{Cube})$ permutes these diagonals. This gives us a homomorphism φ from $O(\text{Cube})$ into S_4. If we restrict to $SO(\text{Cube})$, φ is injective. As with the tetrahedron, we can verify that all transpositions are in the image of φ. It follows that φ is onto and $SO(\text{Cube}) \cong S_4$. From this we see that $O(\text{Cube}) \cong S_4 \times \mathbb{Z}_2$.

The octahedron can be embedded in the cube so that its six vertices correspond to the centers of the six faces of the cube. It follows that the isometry group of the octahedron is isomorphic to the isometry group of the cube.

Finally, we consider isometries of the dodecahedron. A similar argument to the one we used to count the isometries of the cube shows us that the dodecahedron has 120 isometries.

Definition 2.12.3. The center of G is

$$Z(G) = \{g \in G : g \text{ commutes with all elements of } G\}$$

Exercise 2.12.4. (a) $Z(G) \lhd G$; (b) $G/Z(G) \cong \mathrm{Inn}(G)$.

Exercise 2.12.5. If $n \geq 3$, $Z(S_n) = \{1\}$.

Since the isometry group of the dodecahedron has non-trivial center, it cannot be S_5.

Exercise 2.12.6. Show that

$$O(\text{dodecahedron}) = SO(\text{dodecahedron}) \times \mathbb{Z}_2$$

and

$$SO(\text{dodecahedron}) \cong A_5.$$

Definition 2.12.7. An **automorphism** of a graph G is a permutation of the set of vertices V that preserves adjacency. The set $\mathrm{Aut}(G)$ of all automorphisms of G is a group under composition. Note that $\mathrm{Aut}(G) \leq \mathrm{Sym}(V)$.

Exercise 2.12.8. The group of automorphisms of the Petersen graph is isomorphic to S_5.

Definition 2.12.9. If V is a vector space over a field $\mathbb{F}$, we define $\mathrm{GL}(V)$ to be the group of automorphisms of V. We define $\mathrm{GL}_n(\mathbb{F})$ to be the set of $n \times n$ invertible matrices with coefficients in $\mathbb{F}$.

2.13 Representations of groups

Definition 2.13.1. A **representation** of G is a group homomorphism $G \to \mathrm{GL}(V)$. If V is of finite dimension n over the field $\mathbb{F}$ then this is equivalent to giving a homomorphism into $\mathrm{GL}_n(\mathbb{F})$.

Recall we found two representations of S_4 in $O(\mathbb{R}^3)$, namely the $SO(\text{Cube})$ and $O(\text{tetrahedron})$.

Definition 2.13.2. $G \to \mathrm{GL}(V)$ is *irreducible* if no subspace of V is mapped into itself by each element of G.

Exercise 2.13.3. Find an irreducible representation $S_4 \to O(\mathbb{R}^2)$.

We have the following irreducible representations of S_4:

1. $S_4 \to \{1\}$
2. $\mathrm{sgn} : S_4 \to \{\pm 1\}$
3. $S_4 \to O(\mathbb{R}^2)$ (Ex. 2.13)
4. $S_4 \to O(\text{tetrahedron})$
5. $S_4 \to O(\text{Cube})$

Theorem 2.13.4. (Frobenius) *If G is a finite group, the number of irreducible representations over $\mathbb{C}$ of G is equal to the number of conjugacy classes of G.*

Exercise 2.13.5. (Cayley) If $|G| = n$, then $G \leq S_n$.

Exercise 2.13.6. (Frucht) $(\forall G)(\exists \text{ graph } X)(\mathrm{Aut}(X) \cong G)$.

Definition 2.13.7. G is *cyclic* if $G = \langle g \rangle$.

Exercise 2.13.8. If G is cyclic and $|G| = n$, then G is isomorphic to $\mathbb{Z}_n$. If G is cyclic and infinite, then $G \cong \mathbb{Z}$.

Definition 2.13.9. The group of symmetries of a regular n-gon is called a **dihedral group** and denoted D_n.

Observe that $|D_n| = 2n$ and $SO(\text{regular } n\text{-gon}) \cong \mathbb{Z}_n$.

Exercise 2.13.10. The center of D_n is $\{1\}$ if n is odd and $\{1, -1\}$ if n is even.

Exercise 2.13.11. $Z(\mathrm{GL}_n(\mathbb{F})) = \{\lambda I : \lambda \in \mathbb{F}^\times\}$ ("scalar matrices").

Exercise 2.13.12. If A is an $n \times n$ matrix over the integers then A^{-1} is an integer matrix if and only if the determinant of A is ± 1.

Definition 2.13.13. $\mathrm{GL}_n(\mathbb{Z})$ is the group of all $n \times n$ matrices with determinant ± 1.

Exercise 2.13.14. If $\mathbb{F}$ is a field, the determinant map is a homomorphism $\mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^\times$. The kernel of the determinant map is $\mathrm{SL}_n(\mathbb{F})$.

3 Linear Algebra: basic concepts

3.1 Vector space, linear independence, rank

Throughout, $\mathbb{F}$ will be a field (think of $\mathbb{F}$ being $\mathbb{R}$, the set of real numbers).

Definition 3.1.1. A **vector space** V over a field $\mathbb{F}$ of scalars is an abelian group where we can multiply by scalars such that $(\forall \alpha, \beta \in \mathbb{F}, v, w \in V)$

(a) $(\alpha\beta)v = \alpha(\beta v)$,

(b) $(\alpha + \beta)v = \alpha v + \beta v$,

(c) $\alpha(v + w) = \alpha v + \alpha w$,

(d) $1 \cdot v = v$.

Example 3.1.2. $C[0, 1]$ = continuous real-valued functions on $[0, 1]$ form a vector space over $\mathbb{R}$; the set $\mathbb{F}^n = n \times 1$ column vectors with entries from $\mathbb{F}$ form a vector space over $\mathbb{F}$.

Exercise 3.1.3. Prove: if $\alpha \in \mathbb{F}$ and $v \in V$ then $\alpha v = 0$ if and only if $\alpha = 0$ or $v = 0$. (Note that we are talking about two different zeros here.)

Definition 3.1.4. A **linear combination** of the vectors $v_1, \ldots, v_k$ is an expression of the form $\sum_{i=1}^{k} \alpha_i v_i$.

Definition 3.1.5. $v_1, \ldots, v_k$ are said to be **linearly independent over** $\mathbb{F}$ if $(\forall \alpha_1, \ldots, \alpha_k \in \mathbb{F})(\sum_{i=1}^{k} \alpha_i v_i = 0 \ \Rightarrow \ \alpha_1 = \ldots = \alpha_k = 0)$.

Note that if any of the v_i is zero or if $v_i = v_j$ for some $i \neq j$ then the system is not linearly independent. Note also that every subset of a linearly independent set of vectors is linearly independent.

Definition 3.1.6. An infinite set of vectors is said to be linearly independent if every finite subset is linearly independent.

Definition 3.1.7. If $S \subseteq V$, the **rank** of S (denoted $\mathrm{rk}(S)$) is the maximal number of linearly independent vectors in S.

Exercise* 3.1.8. Find a curve in $\mathbb{R}^n$ such that any n points are linearly independent (give a simple explicit formula). (Hint: Vandermonde determinant)

Exercise 3.1.9. $\mathbb{R}$ is a vector space over $\mathbb{Q}$. Prove that $1, \sqrt{2}, \sqrt{3}$ are linearly independent over $\mathbb{Q}$.

Exercise* 3.1.10. The square roots of all square-free positive integers (integers not divisible by the square of any prime) are linearly independent over $\mathbb{Q}$.

Definition 3.1.11. A subset $\mathbb{F}$ of a field $\mathbb{G}$ is a *subfield* if $\mathbb{F}$ is a field under the same operations.

Warning: $\mathbb{F}_2$ is NOT a subfield of $\mathbb{Q}$, even though $\mathbb{F}_2 = \{0, 1\}$ can be viewed as a subset of $\mathbb{Q}$ and both are fields. Why is $\mathbb{F}_2$ not a subfield of $\mathbb{Q}$?

Exercise 3.1.12. If $\mathbb{F}$ is a subfield of the field $\mathbb{G}$ then $\mathbb{G}$ is a vector space over $\mathbb{F}$.

3.2 Subspace, span, dimension, basis

Definition 3.2.1. A subset W of V is a **subspace** of V (denoted $W \leq V$) if it is closed under linear combinations, i. e., all linear combinations of elements of W belong to W.

Remarks. 1. If W is a subspace then $0 \in W$ (take a linear combination of the empty set; note that the empty sum is zero).
2. If $W \leq V$ then W is a vector space over $\mathbb{F}$ (with respect to the same operations). Note that W is a vector space *over the same field* as V.

Since subspaces are vector spaces in their own right, every concept to be defined for vector spaces applies to subspaces as well (e. g, subspaces will have generators and dimension, see below).

Exercise 3.2.2. A subset $W \subseteq V$ is a subspace if and only if (a) $0 \in W$; (b) $(\forall a, b \in W)(a + b \in W)$; (c) $(\forall \lambda \in \mathbb{F})(\forall a \in W)(\lambda a \in W)$.

Definition 3.2.3. The rank of a vector space is called its **dimension**.

Exercise 3.2.4. The intersection of any set of subspaces is a subspace. (Here we permit to take the intersection of infinitely many subspaces; and we may also consider the empty set of subspaces. What is the intersection of the empty set of subspaces?)

Exercise 3.2.5. Prove: if the union of two subspaces is a subspace then one of the two subspaces contains the other.

Exercise 3.2.6. Prove: if a union of fewer than $|\mathbb{F}| + 1$ subspaces of a finite dimensional space is a subspace then one of them contains all the others. (This is true whether $\mathbb{F}$ is finite or infinite. In the infinite case, "fewer than $|\mathbb{F}| + 1$" means *fewer than* $|\mathbb{F}|$, not $\leq |\mathbb{F}|$.)

Definition 3.2.7. The **span** of a set $S \subseteq V$ is the set of all linear combinations of S (i. e., the set of all linear combinations of all finite subsets of S). In particular, for finite families, $\mathrm{Span}(v_1, \ldots, v_k) = \{\sum \alpha_i v_i \mid \alpha_i \in \mathbb{F}\}$.

Definition 3.2.8. We say that a vector space is *finite dimensional* if it has a finite set of generators; otherwise, *infinite dimensional*.

Our focus in these notes are finite dimensional spaces, even though we often consider finite dimensional subspaces of certain infinite dimensional spaces (function spaces, spaces of polynomials, spaces of sequences, etc.).

Exercise 3.2.9. The span of any subset of V is a subspace.

Exercise 3.2.10. $\mathrm{Span}(W) = W$ if and only if $W \leq V$ (W is a subspace).

Exercise 3.2.11. $\mathrm{Span}(\mathrm{Span}(S)) = \mathrm{Span}(S)$.

Exercise 3.2.12. If $S \subseteq T \subseteq V$ then $\mathrm{Span}(S) \leq \mathrm{Span}(T) \leq V$.

Exercise 3.2.13. If $S \subseteq W \leq V$ then $\mathrm{Span}(S) \leq W$. In other words, $\mathrm{Span}(S)$ is the *smallest* subspace containing S.

Definition 3.2.14. A subset $S \subseteq V$ **generates** V if $\mathrm{Span}(S) = V$.

Definition 3.2.15. A **basis** of V is a linearly independent set of generators.

Exercise 3.2.16. $\{v_i : i \in I\}$ is a basis if and only if every vector is a unique linear combination of the v_i.

Example 3.2.17. $\mathbb{F}[x] = \{\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \mid a_i \in \mathbb{F}, n \in \mathbb{N}\}$ = the space of polynomials over $\mathbb{F}$. A basis is $\{1, x, x^2, x^3, \ldots\}$. Indeed, every polynomial is a unique linear combination of powers of the variable.

Exercise 3.2.18. If $f_0, f_1, \ldots \in \mathbb{F}[x]$ and $\deg(f_i) = i$, then $f_0, f_1, \ldots$ form a basis of $\mathbb{F}[x]$.

Exercise 3.2.19. Every linearly independent set can be extended to a basis and every set of generators contains a basis.

It follows in particular that every vector space has a basis. We note that for infinite dimensional spaces, the proof of this result requires Zorn's Lemma from set theory.

Exercise 3.2.20. Every maximal linearly independent set is a basis. ("Maximal" means if we add any element to it, it will no longer be linearly independent.)

3.3 Dimension invariance: the first miracle of linear algebra

Theorem 3.3.1. ***(Miracle #1 of linear algebra)*** *If L is a linearly independent set and G is a set of generators then $|L| \leq |G|$.*

Infer the following corollaries:

Exercise 3.3.2. All bases have equal cardinality (same number of vectors); this common cardinality is the dimension of V.

Exercise 3.3.3. $\mathrm{rk}(S) = \mathrm{rk}(\mathrm{Span}(S)) = \dim(\mathrm{Span}(S))$.

Exercise 3.3.4. $\dim(\mathbb{F}^k) = k$.

Definition 3.3.5. A mapping $f : V \to W$ between two vector spaces over the same field is an **isomorphism** if f is a bijection and f preserves linear combinations: $f(\sum \alpha_i a_i) = \sum \alpha_i f(a_i)$. V and W are **isomorphic** if there exists an isomorphism between them; notation: $V \cong W$.

Exercise 3.3.6. (Dimension invariance) If $\mathbb{F}^k \cong \mathbb{F}^\ell$ then $k = \ell$.

Theorem 3.3.7. *If $\dim V = k$ then $V \cong \mathbb{F}^k$.*

Proof. We start with a definition.

Definition 3.3.8. If $B = (b_1, \ldots, b_k)$ is a basis and $v = \alpha_1 b_1 + \cdots + \alpha_k b_k$ then $\alpha_1, \ldots, \alpha_k$ are the **coordinates** of v with respect to this basis. We arrange the coordinates as a $k \times 1$ column vector, denoted $[v]_B$:

$$[v]_B = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{bmatrix}.$$

Exercise 3.3.9. Prove: given a basis $B = (b_1, \ldots, b_k)$, the mapping $f : w \mapsto [w]_B$ is an isomorphism from V to $\mathbb{F}^k$.

This exercise completes the proof of the theorem.

Hence a vector space is characterized, up to isomorphism, by its dimension and the field of scalars.

Exercise 3.3.10. If $\mathbb{F}$ is a finite field of order q and V is a k-dimensional vector space over $\mathbb{F}$ then $|V| = q^k$.

Exercise 3.3.11. Prove: if $\mathbb{F}$ and $\mathbb{G}$ are finite fields and $\mathbb{F}$ is a subfield of $\mathbb{G}$ then $|\mathbb{G}| = |\mathbb{F}|^k$ for some positive integer k.

Notation: if $S, T \subseteq V$ then $S + T = \{s + t : s \in S, t \in T\}$.

Exercise 3.3.12. Prove: if U, W are subspaces then $U + W$ is also a subspace.

Exercise 3.3.13. (Modular equation) If U, W are subspaces then $\dim(U \cap W) + \dim(U + W) = \dim(U) + \dim(W)$.

(Submodularity of rank)

Exercise 3.3.14. If $S, T \subseteq V$ then $\mathrm{rk}(S \cap T) + \mathrm{rk}(S \cup T) \leq \mathrm{rk}(S) + \mathrm{rk}(T)$.

3.4 Surprising applications to extremal combinatorics

Exercise* 3.4.1. If there are n people, and they can form clubs such that (a) no two clubs have the exact same set of members; (b) every club has an even number of members; and (c) any two clubs have an even number of members in common ("Eventown Rules") then prove that the maximum number of clubs that can be formed in Eventown is $2^{\lfloor n/2 \rfloor}$.

Exercise* 3.4.2. Let us now slightly change the rules. (i) Every club must have an *odd* number of members; and (ii) any two clubs must have an even number of members in common ("Oddtown Rules"). Prove that the maximum number of clubs that can be formed in Oddtown is n.

Exercise* 3.4.3. Prove that in Eventown, every maximal set of clubs is maximum.

Exercise 3.4.4. Prove that this is not the case in Oddtown; in fact, in Oddtown there always exists a maximal set of clubs consisting of at most two clubs.

Exercise* 3.4.5. (Generalized Fisher Inequality) In Blocktown, the rule is that no two clubs have identical membership and every pair of clubs must share the exact same number, say k, members, where $k \geq 1$. Prove: the number of clubs in Blocktown is at most n.

3.5 Matrix rank: the second miracle

Definition 3.5.1. We denote by $\mathbb{F}^{n \times k}$ the set of all $n \times k$ matrices with coefficients in $\mathbb{F}$. If $A \in \mathbb{F}^{n \times k}$, the **column rank** of A is the rank of the set of columns of A and the **row rank** is the rank of the set of rows of A.

Theorem 3.5.2. *(***Miracle #2 of linear algebra***) The row rank and column rank of a matrix are equal and this number is called the* **rank** *of the matrix.*

Definition 3.5.3. The **column space** of A is the span of its columns; the **row space** of A is the span of its rows.

Accroding to the Second Miracle, these two, seemingly unrelated, spaces have equal dimension.

Definition 3.5.4. If A is an $m \times n$ matrix with i, j entry $a_{i,j}$, then the transpose of A (denoted A^T) is the $n \times m$ matrix with i, j entry $a_{j,i}$.

So another way of stating Miracle #2 is that

$$\mathrm{rk}(A) = \mathrm{rk}(A^T). \tag{3.5.1}$$

In the following exercises, A and B are matrices of the right dimensions so that the operations indicated can be performed.

Exercise 3.5.5. $(A + B)^T = A^T + B^T$.

Exercise 3.5.6. $(AB)^T = B^T A^T$.

Exercise 3.5.7. $\mathrm{rk}(A+B) \leq \mathrm{rk}(A) + \mathrm{rk}(B)$.

Exercise 3.5.8. $\mathrm{rk}(AB) \leq \min\{\mathrm{rk}(A), \mathrm{rk}(B)\}$.

Exercise 3.5.9. If A and B are $n \times n$ matrices then $\mathrm{rk}(AB) \geq \mathrm{rk}(A) + \mathrm{rk}(B) - n$.

Exercise* 3.5.10. Over the real numbers, $\mathrm{rk}(A^T A) = \mathrm{rk}(A)$.

The following two exercises show that over fields other than the real numbers (and its subfields), this conclusion is false.

Exercise 3.5.11. Find a matrix A over $\mathbb{F}_p$ (p a prime) such that $A = A^T \neq 0$ and $A^2 = 0$.

Exercise 3.5.12. Find a 2×2 matrix $A \neq 0$ over $\mathbb{C}$ such that $A^T A = 0$.

3.6 Function spaces, spaces of sequences

Definition 3.6.1. If A, B are sets, then $A^B = \{f : B \to A\}$. Note that $\left|A^B\right| = |A|^{|B|}$.

If Ω is a set, $\mathbb{F}^\Omega$ is a vector space. If Ω is finite, then $\dim(\mathbb{F}^\Omega) = |\Omega|$.

Exercise 3.6.2. Let $S = \{\sin(x+\alpha); \alpha \in \mathbb{R}\}$. This is a subset of the space $\mathbb{R}^\mathbb{R}$ of real functions. Prove: $\mathrm{rk}(S) = 2$. Find a very simple basis of $\mathrm{Span}(S)$.

The seqences $(a_0, a_1, a_2, \ldots)$ of elements of $\mathbb{F}$ form the vector space $\mathbb{F}^\mathbb{N}$.

Definition 3.6.3. A sequence $(a_1, a_2, \ldots)$ is of **Fibonacci type** if for all $n \geq 2$ we have $a_n = a_{n-1} + a_{n-2}$. We let $\mathcal{F}$ be the set of all Fibonacci type sequences.

Exercise 3.6.4. Prove: (a) $\mathcal{F} \leq \mathbb{F}^\mathbb{N}$. (b) Prove: $\dim(\mathcal{F}) = 2$.

Exercise 3.6.5. Let $A = (a_{ij})$ be the $n \times n$ matrix defined by $a_{ij} = i + j$. Determine the rank of A (over $\mathbb{R}$).