A Little Beyond: Linear Algebra

Akshay Tiwary

March 6, 2016

Any suggestions, questions and remarks are welcome!

1 A little extra Linear Algebra

1. Show that any set of non-zero polynomials in $\mathbb{F}[x]$, no two of which have same degree, is linearly independent over $\mathbb{F}$.

2. Suppose that V is a vector space with dimension ≥ 2. Show that V has more than one basis.

3. Suppose that K, L, M article subspaces of a vector spaces V. Show that $K \cap (L + (K \cap M) = (K \cap L) + (K \cap M)$.

4. Suppose M and N are subspaces of a vector space V. Show that $(M + N)/N \cong M/(M \cap N)$.

5. Let V be a vector space over an infinite field $\mathbb{F}$. Show that V cannot be the union of finitely many proper subspaces of V.

6. Suppose that V is a finite dimensional vector space over $\mathbb{F}$. Suppose $TS = ST$ for every endomorphism S on V. Show that $T = xI_V$ for some scalar x.

7. Suppose that T is a linear functional on V. Show that $(\operatorname{Im} T^*)^\perp = \ker T$ and that $\ker T^* = \operatorname{Im} T^\perp$. Hence show that if V and W are finite dimensional vector spaces over $\mathbb{F}$, and $T : V \to W$ is a linear transformation, then rank T = rank T^*.

8. Suppose that V is a vector space and that $S = \{f_1, \ldots, f_n\} \subseteq V^*$, Show $S^\perp = \bigcap_{i=1}^n \ker f_i$.

9. Suppose that $\mathbb{F}$ is a finite field. Let V be a vector space over $\mathbb{F}$ of dimension n. Show that for every $m < n$, the number of subspaces of V of dimension m is exactly the same as the number of subspaces of V of dimension $n - m$.

10. Suppose that $v_1, \ldots, v_n$ are distinct non-zero vectors in a vector space V. Show that there is $T \in V^*$ such that $T(v_i) \neq \mathbf{0}$ for any i.

11. Suppose $V = M \oplus N$, where M and N are subspaces of the vector space V. Show that $V^* = N^\perp \oplus M^\perp$.

12. (Oddtown) There are n inhabitants of Oddtown numbered $1, \ldots, n$. They are allowed to form clubs according to the following rules:

    (a) Each club has an odd number of members.

    (b) Each pair of clubs share an even number of members.

    Show that the number of clubs formed cannot exceed n. *Hint: Associate each club with a vector in* $\mathbb{Z}_2^n$.

13. (From A Walk Through Combinatorics - Bona) The set A consists of $n+1$ positive integers, none of which has a prime divisor that is larger than the nth smallest prime number. Prove that there exists a non-empty subset $B \subseteq A$ so that the product of the elements of B is a perfect square.

Definition (Eigenvector)**.** A non-zero vector $v \in V$ is said to be an *eigenvector* for $T : V \to V$ if span v is $T-$invariant.

Definition (Eigenvalue)**.** If $T(v) = \lambda v$, we say λ is the *eigenvalue* for T corresponding to v.

Definition (Eigenspace)**.** For a given map $T : V \to V$ and a scalar $\lambda \in \mathbb{F}$, we define the *eigenspace* V_λ to be

$$V_\lambda = \{v \in V : Tv = \lambda v\}.$$

That is, V_λ is the set of eigenvectors for T corresponding to λ.

Exercise 1.1. Show that V_λ is a subspace of V.

Definition (Geometric Multiplicity)**.** For a given $\lambda \in \mathbb{F}$ and V_λ as above, dim V_λ is called the *geometric multiplicity* of λ.

Exercise 1.2. Think of rotation by 90° as linear map on $\mathbb{R}^2$. What are the eigenvectors?

Exercise 1.3. Suppose v is an eigenvector for T with eigenvalue λ and suppose f is an automorphism on V. Can you find an eigenvector for $f \circ T \circ f^{-1}$?

Exercise 1.4. Suppose $B = \{v_1, \ldots, v_n\}$ is a basis for V and that each v_i is an eigenvector for a linear transformation $T : V \to V$ such that v_i corresponds to the eigenvalue λ_i. What will the matrix representation of T with respect to B look like?

Exercise 1.5. Show that 0 is an eigenvalue for a linear transformation T on V iff T is not injective.

Exercise 1.6. Suppose ϕ, ψ are linear transformations on V. Show that $\phi \circ \psi$ and $\psi \circ \phi$ have exactly the same eigenvalues.

Exercise 1.7. Suppose $v_1, \ldots, v_n$ are different non-zero vectors for some linear transformation T on V corresponding to distinct eigenvalues $\lambda_1, \ldots, \lambda_n$. Show that the $v_1, \ldots, v_n$ are linearly independent.

2 Groups

Definition (Group)**.** A nonempty set G is said to form a *group* if there is an associated binary operation (which we will denote by $\circ$) such that

1. (Closure) If $a, b \in G$, then $a \circ b \in G$.
2. (Associativity) If $a, b, c \in G$, then $(a \circ b) \circ c \in G$.
3. (Existence of Identity) There is an element $e \in G$ such that $a \circ e = e \circ a = a$ for every $a \in G$.
4. (Existence of Inverses) For every $a \in G$ there is an element $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

If, in addition, the group satisfies the condition that for every $a, b \in G$, $a \circ b = b \circ a$, then we call the group an abelian group.

Exercise 2.1. Show that the identity in a group is unique. Show also that each $g \in G$ has a unique inverse and so we can talk about "the" identity and "the" inverse of g.

Exercise 2.2. Show that for each pair $a, b \in G$, there is a unique element $x \in G$ such that $a \circ x = b$ and a unique $y \in G$ such that $y \circ a = b$. This means that the "equations" $a \circ x = b$ and $y \circ a = b$ have unique solutions.

Exercise 2.3. Suppose that H is a nonempty set with an associative operation (which we will denote by $*$) and an identity element e. Suppose that every element $h \in H$ has a left inverse h' such that $h' * h = e$. Show that $(H, *)$ is a group.

By showing this, you are showing that the axioms for a group are stronger than necessary.

Exercise 2.4. For an arbitrary element in a group, show that $h^{-1} \circ g^{-1} = (g \circ h)^{-1}$.

Example 2.5. Let X be a nonempty set and let $L(X)$ be the set of all bijections from X to itself. Then $L(X)$ is a group under the operation of composition of functions. If X is finite, what is $|L(X)|$?

Definition. Suppose that $(G, \circ)$ is a group. Suppose that H and K are subsets of G. Then define HK to be the set $\{h \circ k : h \in H, k \in K\}$.

Similarly, we can define gH and Kg for $g \in G$ to be $\{gh : h \in H\}$ and $\{kg : k \in K\}$ respectively.

Definition. Suppose $G = (G, \circ)$ is a group. Suppose H is a nonempty subset of G which is closed under $\circ$. Suppose that the following also hold.

1. $H \circ H \subseteq H$.
2. If $h \in H$, then $h^{-1} \in H$.

Then we say H is a *subgroup* of G.

Exercise 2.6. Suppose that for every $i \in I$, H_i is a subgroup of a group G. Show that

$$\bigcap_{i \in I} H_i$$

is a subgroup of G.

Do you remember an analogous theorem for subspaces? You will see many similarities with subspaces and subgroups because a Vector space is really an abelian group with respect to addition.

Exercise 2.7. Note that $(\mathbb{Z}, +)$ is a group. Show that every subgroup of $\mathbb{Z}$ under $+$ is of the form $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ where $n \in \mathbb{Z}$.

Definition (Cosets)**.** Suppose that H is a subgroup of G and $g \in G$. Then gH as defined above is called the *left coset* of g with respect to H. We can analogously define Hg, the right coset of g with respect to H.

Exercise 2.8. Suppose that G is a group and that N is a subgroup of G. Let $\sim$ be a relation on a group G such that $g \sim h$ iff $h \in gN$. Show that this is an equivalence relation on G.

We denote $G/\!\sim\, = \{gN : g \in G\}$ by G/N.

Exercise 2.9. Consider the group $(\mathbb{Z}, +)$. Suppose $n \in \mathbb{Z}^+$. What is $\mathbb{Z}/n\mathbb{Z}$?

Definition (Normal Subgroup)**.** A subgroup N of a group G is called a *normal subgroup* of G if $gN = Ng$ for every $g \in G$. We call gN the coset of g modulo N.

That is, the left and right cosets are the same. Every subgroup in an abelian group is clearly normal, but normal subgroups are possible in non-abelian groups as well.

Exercise 2.10. Suppose that N is a normal subgroup of a group G and $g, h \in G$. Show that $(gN)(hN) = (g \circ h)N$ where $(gN)(hN)$ denotes the product of the sets gN and hN as defined above.

This shows that normal subgroups respect products, and this allows for a lot of interesting properties.

Exercise 2.11. Suppose that G is a group and N is a normal subgroup of N. Let $[g]$ denote gN, the coset of g modulo N. Let $* : G/N \to G/N$ be defined by $[g] * [h] = [g \circ h]$. Show that $(G/N, *)$ is a group. What is the identity? What is the inverse of $[g]$?

Definition (Group Homomorphism)**.** Suppose $(G, \circ)$ and $(G', \circ')$ are groups. A function $\phi : G \to G'$ is called a *group homomorphism* if for every $g, h \in G$ we have

$$\phi(g \circ h) = \phi(g) \circ' \phi(h).$$

A homomorphism from G to itself is called an *endomorphism*.

Definition. Suppose $\phi : G \to G'$ is a group homomorphism. The kernel of ϕ, denoted by ker ϕ, is the set $\{g \in G : \phi(g) = e'\} = \phi^{-1}(e')$.

Exercise 2.12. Suppose e and e' are the identity elements of G and G' respectively. Show that $\phi(e) = e'$. Suppose $g \in G$. What is $\phi(g^{-1})$?

Exercise 2.13. Suppose $\phi : G \to G'$ is a group homomorphism. Show that ker ϕ is a normal subgroup of G.

Exercise 2.14. Suppose N is a normal subgroup of a group G. Show that there is some group homomorphism for which N is the kernel.

Exercise 2.15. Suppose $\phi : G \to G'$ is a group homomorphism. Let $N = \ker \phi$. Then, for $g \in G$, show that $gN = Ng = \phi^{-1}(\phi(g))$.

Exercise 2.16. Show that a homomorphism $\phi : G \to G'$ is injective iff ker $\phi = \{e\}$.

Exercise 2.17. Suppose N is a normal subgroup of G. Show that the quotient function $\psi : G \to G/N$ is a surjective homomorphism. What is ker ψ?

Definition. A bijective homomorphism $\phi : G \to G'$ is called an *isomorphism*. In this case we say that G and G' are isomorphic and write $G \cong G'$. An isomorphism from a group to itself is called an *automorphism*.

Isomorphic groups are essentially identical. In fact, the relation $\cong$ on a set of groups is an equivalence relation.

Exercise 2.18. Suppose that $\phi : G \to G'$ is an isomorphism. Show that ϕ^{-1} is an isomorphism as well.

Exercise 2.19. Suppose that G is a group and that $g \in G$. Then the map $\phi : G \to G$ defined by $\phi(x) = gxg^{-1}$ is an automorphism.

Exercise 2.20. Let $\phi : G \to G'$ be a homomorphism. Is Im ϕ a normal subgroup of G'?

Exercise 2.21. Show that the image of a normal subgroup N of a group G under a surjective homomorphism $\phi : G \to G'$ is a normal subgroup of G'. What happens if ϕ is not surjective?

Exercise 2.22 (First Isomorphism Theorem). Let $\phi : G \to G'$ be a homomorphism and that ψ is the quotient function $\psi : G \to G/\ker \phi$. Then there is a unique isomorphism $\widetilde{\phi} : G/\ker \phi \to \operatorname{Im} \phi$ such that $\phi = \widetilde{\phi} \circ \psi$. Hence $G/\ker \phi \cong \operatorname{Im} \phi$.

Definition. The *order* of a group $(G, \circ)$ is $|G|$ and is denoted by $o(G)$. This is only relevant when G is finite.

Exercise 2.23. Show that there is a bijection between the (left) right cosets formed by a subgroup H of a group G.

Exercise 2.24. (Lagrange's Theorem) Suppose that G is a group having finite order and that H is a subgroup of G. Show that H also has finite order and that $o(H) \mid o(G)$.

3 Algebras over a Field

Definition (Algebra over a Field)**.** An *algebra* over a field $\mathbb{F}$ (sometimes called an $\mathbb{F}$-algebra) is a vector space V over $\mathbb{F}$ which also has a binary operation $*$ (which we call "multiplication" or a bilinear product) such that for all $\vec{u},\vec{v},\vec{w} \in V$ we have

1. $\vec{u}\cdot(\vec{v}+\vec{w}) = \vec{u}\cdot\vec{v}+\vec{u}\cdot\vec{w}$,
2. $(\vec{v}+\vec{w})\cdot\vec{u} = \vec{v}\cdot\vec{u}+\vec{w}\cdot\vec{u}$,
3. and, $\vec{v}\cdot(a\vec{w}) = a(\vec{v}\cdot\vec{w}) = (a\vec{v})\cdot\vec{w}$ for any scalar a.

We say that an algebra has a *unit element* if there is a $\vec{1} \in V$ such that $\vec{1}\vec{v} = \vec{v}\vec{1} = \vec{v}$.

Note that any field is an algebra over itself, but every algebra need not be a field because there may be non-invertible non-zero elements in the algebra.

Definition. Suppose that V is a vector space over a field $\mathbb{F}$. Let $End(V)$ denote the set of endomorphisms on V. Remember that $End(V)$ is a vector space over $\mathbb{F}$.

Let's make $End(V)$ into an algebra. For $f,g \in End(V)$ define fg to be $h \in End(V)$ where $h(v) = f(g(v))$. That is $fg = f\circ g$, where $\circ$ represents the usual operation of composition.

Exercise 3.1. Show that $End(V)$ is really an algebra with the multiplication defined above. Is there a unit element?

Definition (Units)**.** Suppose that A is an algebra with a unit element 1. Then define an element $a \in A$ to be a *unit* if there is a $b \in A$ such that $ab = ba = 1$. That is, a unit is an invertible element in A.

Exercise 3.2. Suppose A is an algebra over a field $\mathbb{F}$. Suppose the multiplication on A is associative (we call it an associative algebra). Show that U, the set of all the units in A, is a group under multiplication.

In the case of $End(V)$, this group is denoted by $GL(V)$ and called the general linear group over V. $GL(n,\mathbb{R})$ (or $GL_n(\mathbb{F})$ in general) is the set of invertible $n\times n$ matrices with elements in $\mathbb{R}$. Do you see why $GL(n,\mathbb{R})$ is a group?

Exercise 3.3. What is the order of $GL_2(\mathbb{Z}/p\mathbb{Z})$ when p is prime?

Exercise 3.4. Show that the units in $End(V)$ are precisely the automorphisms on V.

Exercise 3.5. Suppose A is an algebra over $\mathbb{F}$ and $v \in A$. Define $\phi_a : A \to A$ by $\phi_a(v) = a\circ v$ for any $v \in A$. Show that ϕ_a is an endomorphism on A. Similarly show that $\psi_a : A \to A$ by $\psi_a(v) = v\circ a$ is an endomorphism as well.

Thus the multiplication in an algebra is a special type of an operation called a *bilinear map*. Can you guess why it is called that?

Exercise 3.6. Suppose V and W are vector spaces and $\phi : End(V) \to End(V')$ is an isomorphism.

(a) Suppose that V and V' are finite dimensional. Show that $V \cong V'$.

(b) Now remove the assumption that V or V' is finite dimensional. Show that $V \cong V'$.

Definition (Division Algebra)**.** An algebra A with a unit 1 is called a division algebra if $A\setminus\{\mathbf{0}\}$ is a group under multiplication. That is, in a division algebra every non-zero element is a unit.

Exercise 3.7. Show that a finite dimensional algebra A with unity is a division algebra iff it has no zero divisors.

Let's talk about quaternions. They came about as William Rowan Hamilton's failed efforts to form a three dimensional number system (the real numbers are a one dimensional number system and the complex numbers are a two dimensional number system). He instead discovered the *Quaternions*, which is a almost a four dimensional number system because it lacks commutativity.

Definition. Consider $\mathbb{H}$, a four dimensional vector space over $\mathbb{R}$ with a basis $\{1, i, j, k\}$. That is, every element $h \in \mathbb{H}$ can be written uniquely in the form $h = a1 + bi + cj + dk$ for reals a, b, c, d. Lets make it into an algebra with the following rules of multiplication:

1. $1 \circ h = h$ for every $h \in \mathbb{H}$;
2. $i^2 = j^2 = k^2 = -1$;
3. $i \circ j = k$, $j \circ j = i$, $k \circ i = j$;
4. $j \circ i = -k$, $k \circ j = -i$, $i \circ k = -j$.

We call this the *Quaternion Algebra over* $\mathbb{R}$.

Exercise 3.8. Consider the map $C : \mathbb{H} \to \mathbb{H}$ defined by $C(a + bi + cj + dk = a - bi - cj - dk$. We call this the "complex conjugation map" and write $C(z) = \bar{z}$ for $z \in \mathbb{H}$. SHow that $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$ for every $z_1, z_2 \in \mathbb{H}$.

Note that we expect this to be true because the quaternions are really meant to be an extension of the complex numbers.

Exercise 3.9. Suppose $z = a + bi + cj + dk \in \mathbb{H}$. Show $z \cdot \overline{z} = a^2 + b^2 + c^2 + d^2$.

Exercise 3.10. Show that every non-zero element in $\mathbb{H}$ is invertible. Hence conclude that $\mathbb{H}$ is a division algebra.