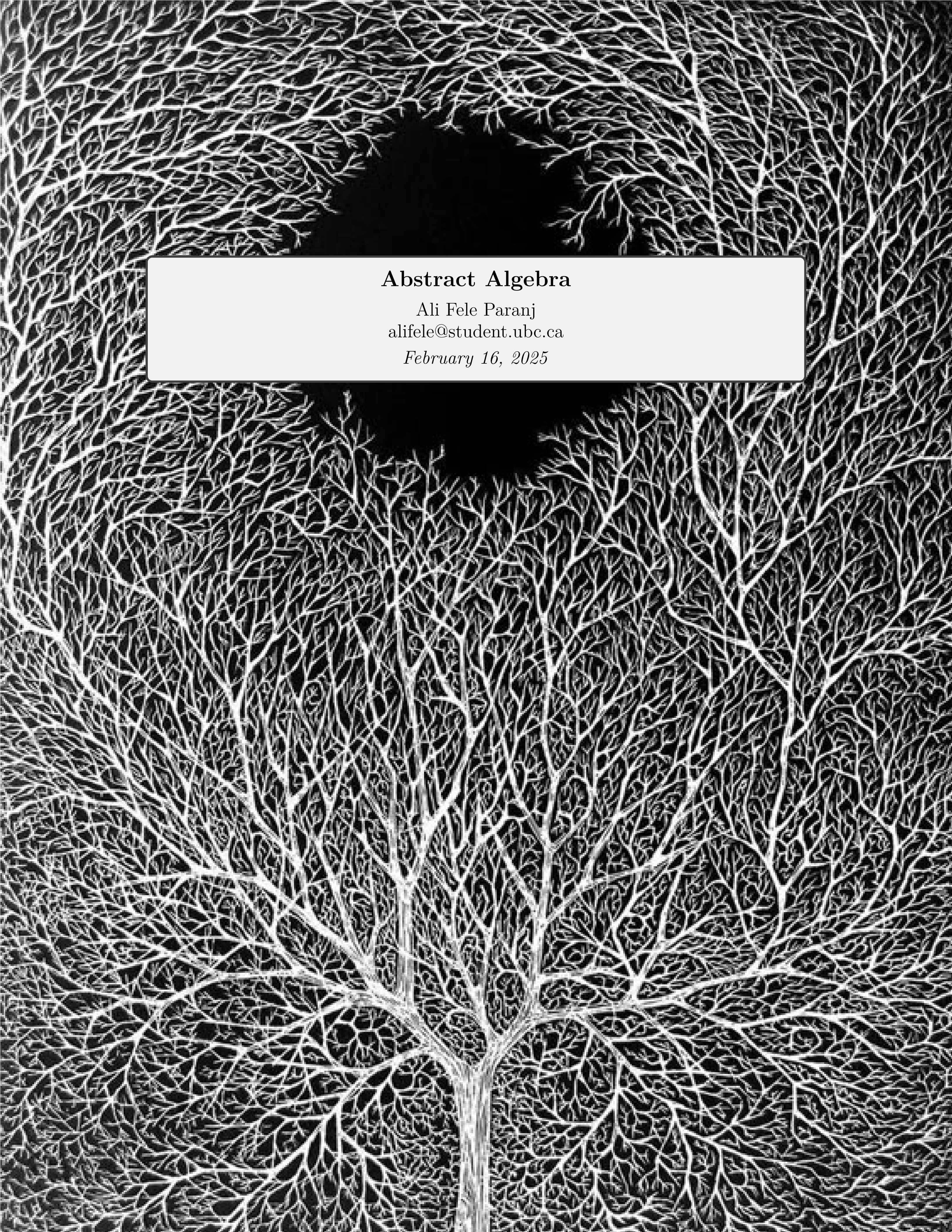
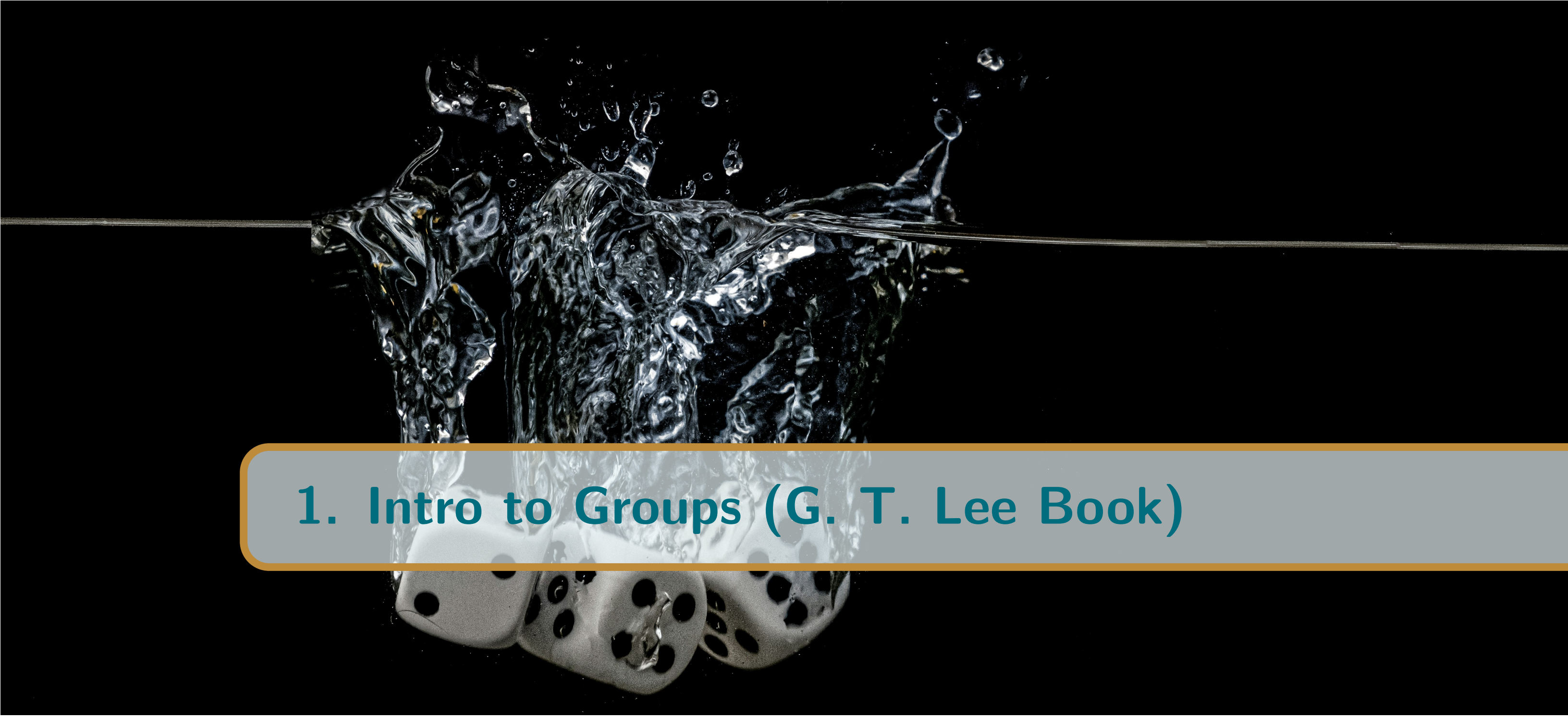
Abstract Algebra

Ali Fele Paranj
alifele@student.ubc.ca

February 16, 2025



0. Contents



1. Intro to Groups (G. T. Lee Book)

Theorem 1.1 Let G be a group and let $a \in G$. Suppose $i, j \in \mathbb{Z}$. Then

(i) If a has infinite order, then $a^i = a^j$ if and only if $i = j$.

(ii) If $|a| = n < \infty$, then $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.

Proof. Proof for (i) and (ii) is as follows.

(i) $\boxed{\Rightarrow}$: Assume $a^i = a^j$ for some $i, j \in \mathbb{Z}$. Thus $a^{i-j} = e$. However, since a has infinite order, it implies that $i - j = 0$, hence $i = j$.

$\boxed{\Leftarrow}$: The converse direction follows immediately from the definition of group.

(ii) $\boxed{\Rightarrow}$: Assume $a^i = a^j$ for some $i, j \in \mathbb{Z}$. We can write $a^{i-j} = e$. Using division algorithm we can write $i - j = nq + r$ where $q, r \in \mathbb{Z}$ and $0 \le r < n$. So

$$a^{i-j} = (a^n)^q a^r = e.$$

Since n is the order of a, it implies that $a^n = e$. Thus the equality above implies that $a^r = e$. By definition n was the smallest number with this property, and by division algorithm we have $0 \le r < n$. This implies that $r = 0$. So $i - j = nq$ or equivalently $i \equiv j \pmod{n}$.

$\boxed{\Leftarrow}$: Assume $i \equiv j \pmod{n}$. This implies $i - j = qn$ for some $q \in \mathbb{Z}$. Thus $a^{i-j} = (a^n)^q = e$. This implies $a^i = a^j$.

□

1.1 Solved Problems

The following problems are from Gregory T. Lee abstract algebra book in SUMS.

■ **Problem 1.1** In S_4 let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. Calculate the followings.

(a) $\sigma\tau$

(b) $\tau\sigma$

(c) the inverse of σ

Solution (a)

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$

(b)

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

(c)

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

■ **Problem 1.2** In S_5, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$. Calculate the following.

(a) $\sigma\tau\sigma$

(b) $\sigma\sigma\tau$

(c) the inverse of σ

Solution (a)

$$\sigma\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

(b)

$$\sigma\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

(c)

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}.$$

■ **Problem 1.3** How many permutations are there in S_n? How many of those permutation satisfy $\alpha(2) = 2$?

Solution There are n choices for $\alpha(1)$, $n-1$ choices for $\alpha(2)$, and so on. So there are in total $n!$ elements in S_n. Fixing the value of $\alpha(2) = 2$ will leave 4 possible values for $\alpha(1)$, 3 possible values for $\alpha(3)$, and so on. Thus there will be $4! = 24$ permutations satisfying $\alpha(2) = 2$.

■ **Problem 1.4** Let H be the set of all permutations $\alpha \in S_5$ satisfying $\alpha(2) = 2$. Which of the properties, closure, associativity, identity, and inverse does H enjoy under composition of functions?

Solution Closure is satisfied: Let $\alpha, \beta \in H$. Then $\alpha(\beta(2)) = \alpha(2) = 2$ and also $\beta(\alpha(2)) = \beta(2) = 2$. Associativity is satisfied which follows from the axioms of the group. The identity of the group is in H, which is given by

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Every element in H also has an inverse. Let $\alpha \in H$. Let $\tau \in S_5$ be its inverse. We have

$$\tau(2) = \tau(\alpha(2)) = e(2) = 2.$$

Thus $\tau \in H$.

■ **Problem 1.5** Consider the set of all functions from $\{1, 2, 3, 4, 5\}$ to $\{1, 2, 3, 4, 5\}$. Which of the properties, i.e. closure, associativity, identity, and inverse does this set enjoy under the composition of functions.

Solution The composition of any two functions is a function, thus the set is closed under composition. The associativity follows from the properties of the function composition. The identity function is the function that maps every element to itself hence is in the set. But not every function necessarily has an inverse (injectivity, and surjectivity is needed to guarantee the inverse).

■ **Problem 1.6** Give group tables for the following additive groups

(a) $U(12)$,

(b) S_3.

Solution (a)

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(b)

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$
$(2,0)$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(2,1)$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$

■ **Problem 1.7** Give group tables from the following groups.

(a) $U(12)$.

(b) S_3.

Solution (a) First observe that $U(12) = \{1, 5, 7, 11\}$. So

$*$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(b) Call the following permutations as $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$, and σ_6 respectively

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$*$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_4	σ_1	σ_2	σ_6	σ_5
σ_4	σ_4	σ_3	σ_6	σ_5	σ_1	σ_2
σ_5	σ_5	σ_6	σ_2	σ_1	σ_4	σ_3

2. Advanced Linear Algebra - Roman

2.1 Tensor Product

We start with the following proposition

Proposition 2.1 Let U, V be vector spaces. Then exists a unique linear map

$$\theta : U^* \otimes V^* \to (U \otimes V)^*,$$

defined by $f \otimes v = f \odot g$ where

$$(f \odot g)(u \otimes v) = f(u)g(v).$$

Moreover, θ is an embedding and is an isomorphism if U and V are finite dimensional. Thus the tensor product of linear functionals, i.e. $f \otimes g$ is a linear functions, i.e. $f \odot g$ on the tensor product.

Proof. Fix some $f \in U^*$ and $g \in V^*$. Consider the bilinear map

$$G : U^* \times V^* \to (U \otimes V)^*$$

given by $G(f, g) = f \odot g$ where $(f \odot g)(u \otimes v) = f(u)g(v)$. This map $f \odot g$ exists, since the map $F_{f,g}(u, v) : U \times V \to F$ given by $F_{f,g}(u, v) = f(u)g(v)$ is bilinear, and by the universal property of the tensor product, there exist some linear map from $U \otimes V$ to F whose values matches $f(u)g(v)$, and we call this map $f \odot g$. The bilinear map G induces a linear map $\theta : U^* \otimes V^* \to (U \otimes V)^*$ given by

$$\theta(f \otimes g) = f \odot g.$$

For the rest of proof see Roman 14.7. $\square$

3. Random Notes

3.1 Interesting Observations from Roman

Observation 3.1.1 — Geometric Interpretation of Dual Vectors. The notion of the dual space of a vector space is somewhat abstract and one usually struggles to have a geometric realization of the functionals and dual spaces. Here, I provide a very interesting point of view. Let V be a finite dimensional vectors space. Then every $f \in V^*$ is characterized by a hyperplane H such that $H = \ker f$.
With this point of view, $f(x) = 0$ corresponds to the fact that $x \in H$. Also, it is very straight forward to see the following properties of functionals with this geometric point of view.

Proposition 3.1 (a) If $f(x) \neq 0$ then

$$V = \langle x \rangle \oplus \ker f.$$

(b) For every $x \in V$ there exists $f \in V^*$ such that $f(x) \neq 0$.

(c) For $x \in V$, $f(x) = 0$ for all $f \in V^*$ implies $x = 0$.

(d)

Proof. (Geometric interpretation)

(a) If $x \notin H$ for some hyperplane H, then

$$V = \langle x \rangle \oplus H.$$

(b) Given any point of the space, there is some hyperplane that misses that particular point.s

(c) The only point that belongs to all hyperplanes is the origin.

□

Observation 3.1.2 — More Geometric Interpretation of Dual Vectors. The characterization above, i.e. identifying the linear functionals with their kernel, i.e. hyperplanes, work surprisingly well in characterizing very interesting facts. For instance, we can have the following definition of the annihilators of a set.

Definition 3.1 — Annihilators. Let $M \subset V$ (no necessarily a linear subspace). Then the annihilators of M, denoted by M^0 is the set of all linear functionals that kills M. I.e.

$$M^0 = \{f \in V^* | f(M) = 0\}.$$

With the geometric point of view above, the annihilators of M is the set of all hyperplanes that contain M.

For instance, let L be a one dimensional linear subspace of $\mathbb{R}^3$. Then L^0 will be the set of all hyperplanes containing L. Each such hyperplane can be represented by a normal vectors. So the set of all hyperplanes containing L is isomorphic to a plane perpendicular to L and going through the origin (more generally, any 2-dimensional linear subspace of $\mathbb{R}^3$ that does not contain L). It is now very straightforward to see the result of Theorem 3.14 part (2). The set M^{00} is the set of all hyperplanes containing M^0. There is just one such hyperplane, and since it can be parameterized using one normal vector (along L), we have

$$M^{00} \simeq \operatorname{span} L.$$

Observation 3.1.3 — Double Dual Map. We start with the following definition.

Definition 3.2 Let $\tau \in \mathcal{L}(U, V)$. The dual map $\tau^\times \in \mathcal{L}(V^*, U^*)$ and, the double dual map $\tau^{\times\times} = \mathcal{L}(U^{**}, V^{**})$ is defined as

$$(\tau^\times f)(u) = f(\tau u), \qquad \text{for } u \in U,\ f \in V^*,$$

and

$$(\tau^{\times\times} E)(f) = E(\tau^\times f), \qquad \text{for } E \in V^{**},\ f \in W^*.$$

In finite dimension, the following is a very useful characterization of $\tau^{\times\times}$. Let $u \in U$ and using the canonical map $u \mapsto E_u \in V^{**}$, where E_u is the evaluation map at u.Also let $f \in V^*$. Then we can write

$$\begin{aligned}(\tau^{\times\times} E_u)(f) &= E_u(\tau^\times f)\\ &= (\tau^\times f)(u)\\ &= f(\tau u)\\ &= E_{\tau u}(f).\end{aligned}$$

Thus we have

$$\tau^{\times\times} E_u = E_{\tau u}.$$

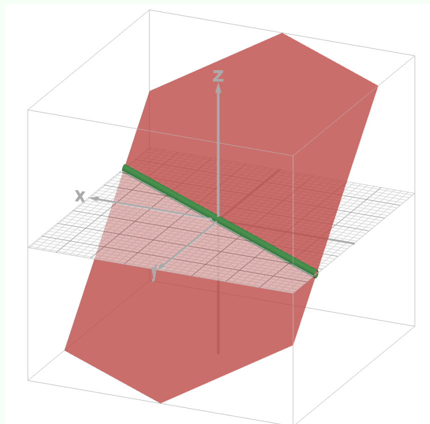
Observation 3.1.4 — Geometric Interpretation of Dual Map. For $\tau \in \mathcal{L}(V, W)$, the dual map $\tau^\times \in \mathcal{L}(W^*, V^*)$ is given by

$$(\tau^\times f)(v) = f(\tau v),$$

where $f \in W^*$ and $v \in V$. Using out geometric point of view of the functionals (as hyperplanes) we can have a geometric interpretation of what is the dual of a map. The following is a high level summary:

> Let $f \in W^*$ be a functional, i.e. a hyperplane. Then $\tau^\times$ returns a hyperplane in V that is the pre-image of restriction of f to $\operatorname{im}(\tau)$.

For instance, if $\tau : \mathbb{R}^2 \to \mathbb{R}^3$ the inclusion map that sends $\mathbb{R}^2$ to the xy plane in $\mathbb{R}^3$, the $\tau^\times$ map maps the following red hyperplane (as a functional in $\mathbb{R}^3$) to the green hyperplane (as a functional in $\mathbb{R}^2$).



Using the interpretation above we can have the following "geometric" proof of the following facts in Roman (presented in Theorem 3.19).

Proposition 3.2 Let $\tau \in \mathcal{L}(V, W)$. Then

(a) $\ker(\tau^\times) = \operatorname{im}(\tau)^0$.

(b) $\operatorname{im}(\tau^\times) = \ker(\tau)^0$.

Geometric proof. (a) We want to show $\ker(\tau^\times) \subset \operatorname{im}(\tau)^0$. Let $f \in \ker(\tau^\times)$ be a hyperplane (i.e. functional). This means that if we restrict f to $\operatorname{im}(\tau)$ and then consider its pre-image, it should be the whole space (i.e. the zero functional). Thus f should contain $\operatorname{im}(\tau)$. So $f \in \operatorname{im}(\tau)^0$ (remember that $\operatorname{im}(\tau)^0$) is the set of all hyperplanes containing $\operatorname{im}(\tau)$. For the converse, we want to show $\operatorname{im}(\tau)^0 \subset \ker(\tau^\times)$. Let $f \in \operatorname{im}(\tau)^0$. I.e. f is a hyperplane that contains $\operatorname{im}(\tau)$. So restricting f to $\operatorname{im}(\tau)$ will be whole $\operatorname{im}(\tau)$. So the pre-image of the restriction of f to $\operatorname{im}(\tau)$ will be the whole space V (thus the zero functional). So $f \in \ker(\tau^\times)$. *Note: We have used the fact that for any linear map τ we have $\operatorname{im}(\tau) \simeq \operatorname{dom}(\tau)$.*

(b)

$\square$

Observation 3.1.5 — Coordinate maps. Let (V, F) be a vector space (defined on the field F) with finite dimension n. Once we choose an ordered basis for V, like $\mathcal{B} = (v_1, \cdots, v_n)$, we can define the coordinate map

$$\phi_{\mathcal{B}} : V \to F^n,$$

that

$$v = \sum_i \alpha_i v_n \mapsto \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

In particular, for the basis vectors we have $\phi(v_i) = e_i$, where e_i is a column vector whose entries are all zero, but the i^{th} row. This coordinate map ϕ justifies the name "vector space" for this algebraic structure. The elements of any finite dimensional vector space defined on F can be "coordinated" by the elements of F^n.

Observation 3.1.6 As a continuiation of the note above, lets now focus on the linear maps $\mathcal{L}(F^n, F^m)$. We know that every matrix in $A \in \mathcal{M}_{n,m}$ induces a linear map $\tau_A \in \mathcal{L}(F^n, F^m)$, given by

$$\tau_A(v) = Av.$$

The converse is also true. Every linear map $\tau \in \mathcal{L}(F^n, F^m)$ has a matrix representation $A \in \mathcal{M}_{n,m}$ given by

$$A = (\tau e_1 | \cdots | \tau e_n),$$

i.e. apply τ on the basis vectors, write the coordinates of the resulting vector in the columns of a matrix to get the matrix representation of the linear transformation.

Observation 3.1.7 I have started to notice a very interesting interaction between the following objects, and each pair of these notions induces a similar feeling. I have not yet been able to quantify this feeling. But I am sure there is some connection there.

surjective	ker	spanning	exists
injective	img	linearly independent	for all

3.2 On going thoughts