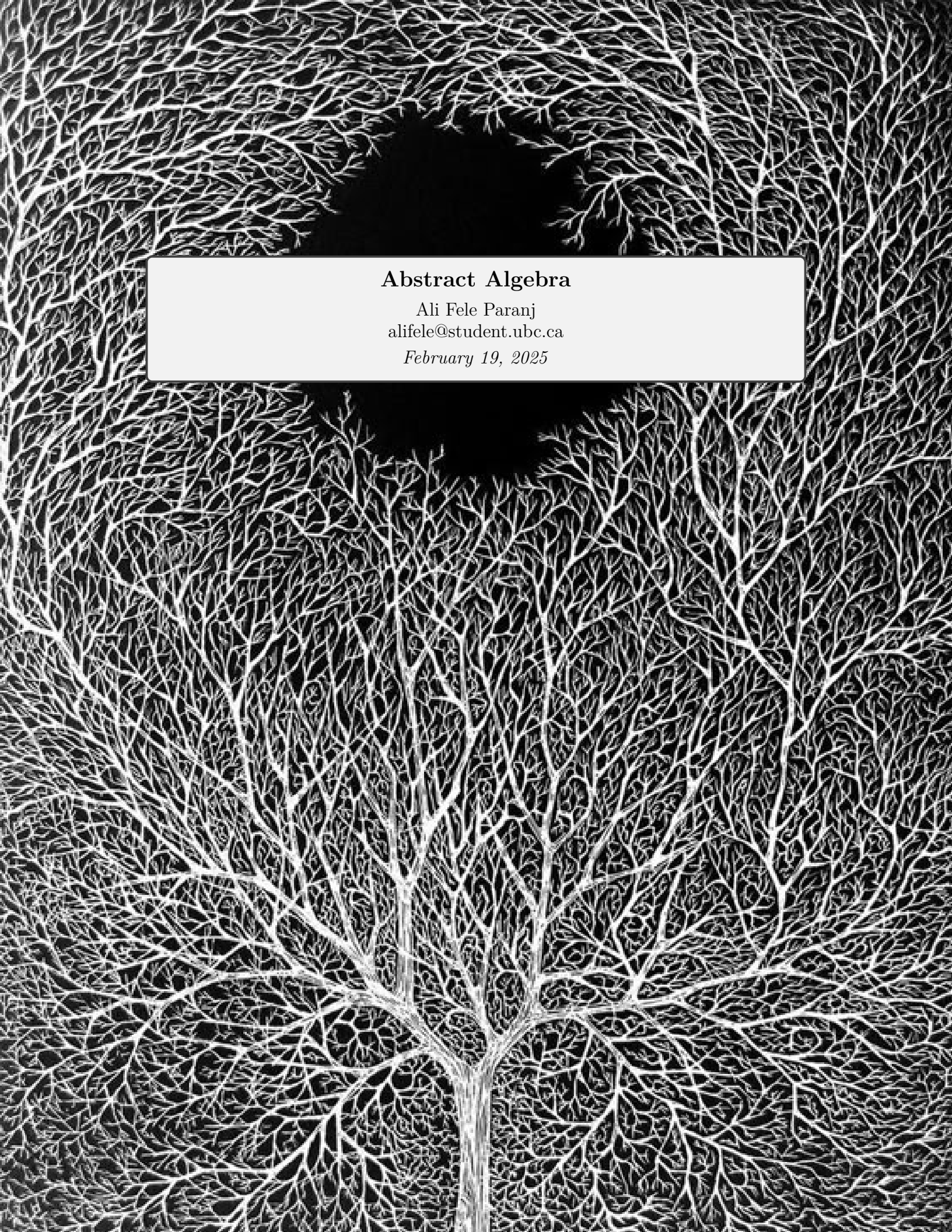


Abstract Algebra

Ali Fele Paranj
alifele@student.ubc.ca

February 19, 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 $0 \leq r < n$. 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 $0 \leq r < n$. 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. □

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

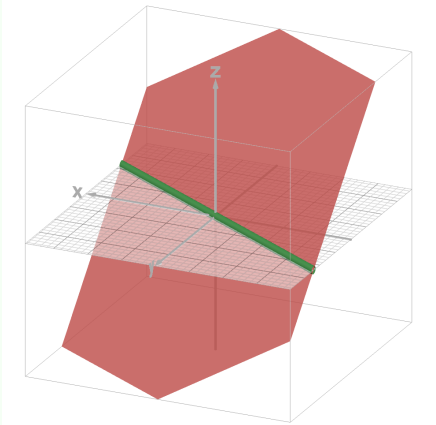
$$(\tau^\times f)(v) = f(\tau v),$$

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 $\text{im}(\tau)$.

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

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

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

(b)

□

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

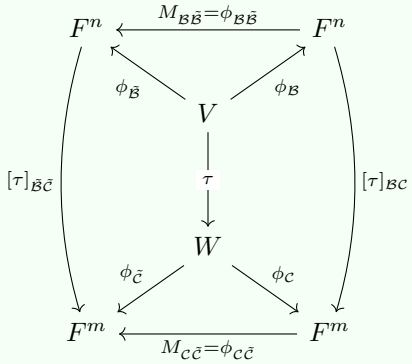
$$A = (\tau e_1 | \cdots | \tau e_n),$$

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

Observation 3.1.8 — Change of basis. Consider the following diagram.



where V, W are vector spaces with dimension n and m respectively. Furthermore, $\mathcal{B}$ and $\tilde{\mathcal{B}}$ are two ordered basis for V with the coordinate maps $\phi_{\mathcal{B}}$ and $\phi_{\tilde{\mathcal{B}}}$ respectively. Similarly $\mathcal{C}$ and $\tilde{\mathcal{C}}$ are two ordered basis for W with $\phi_{\mathcal{C}}$ and $\phi_{\tilde{\mathcal{C}}}$ as the corresponding coordinate maps. The change of basis matrices are given in Theorem 2.12 Roman. This diagram summarizes the relation between the vectors in the abstract vector spaces V and W with their representation

with we change the basis in either of the spaces. Also it capture the transformation that happens for the representation of linear maps when we change basis. For instance it is very easy to see

$$[\tau]_{\tilde{\mathcal{B}}\tilde{\mathcal{C}}} = M_{\mathcal{C}\tilde{\mathcal{C}}}[\tau]_{BC}M^{-1}_{\mathcal{B}\tilde{\mathcal{B}}}.$$

It is also easier to memorize the following relation instead

$$[\tau]_{\tilde{\mathcal{B}}\tilde{\mathcal{C}}}M_{\mathcal{B}\tilde{\mathcal{B}}} = M_{\mathcal{C}\tilde{\mathcal{C}}}[\tau]_{\mathcal{B}\mathcal{C}}.$$

Observation 3.1.9 — Characteristic of a filed and the alternating, v.s. skew-symmetric forms. It is only when $\mathrm{Char}(F) \neq 2$ we have the equivalence between the alternating forms and the skew-symmetric forms

$$\text{alternating} \qquad \Longleftrightarrow \qquad \text{skew-symmetric.}$$

For the forward direction we don't need any restriction on the characteristic of the field. To see this let f be an alternating bi-linear form.

$$f(u+v, u+v) = f(u,u) + f(v,v) + f(u,v) + f(v,u).$$

Since f is alternating, we have $f(u+v, u+v) = 0$ as well as $f(u,u) = f(v,v) = 0$. So we can conclude that

$$f(u,v) = -f(v,u).$$

However, for the converse, we need $\mathrm{Char}(F)$ $neq2$. Because if f is skew-symmetric, then $f(u,u) = -f(u,u)$, which implies $2f(u,u) = 0$. We can only conclude $f(u,u) = 0$ when $\mathrm{Char}(F) \neq 2$, i.e. when 2 is invertible in the field.

Observation 3.1.10 — Symmetric and Antisymmetric tensor products with Roman's notation. In Roman text book, he introduces the notion of the symmetric and anti-symmetric tensor products with a notation that is not easy to understand, unless there is a running example. Here in this box, I will give an explicit example. Let V has dimension $n = 3$ and let $\{e_1, e_2, e_3\}$ be a basis for V. We want to explicitly construct the basis vectors for the $\mathrm{ST}^p(V)$ and $\mathrm{AT}^p(V)$. We will have the following cases

(i) $p = 2$. Then the basis elements of $\mathrm{ST}^2(V)$ will be

M	$\sum_{t\in G_M}$ t	equiv in $F_2[e_1, e_2, e_3]$
$\{1,1\}$	$e_1 \otimes e_1$	$e_1 \vee e_1$
$\{2,2\}$	$e_2 \otimes e_2$	$e_2 \vee e_2$
$\{3,3\}$	$e_3 \otimes e_3$	$e_3 \vee e_3$
$\{1,2\}$	$e_1 \otimes e_2 + e_2 \otimes e_1$	$e_1 \vee e_2$
$\{1,3\}$	$e_1 \otimes e_3 + e_3 \otimes e_1$	$e_1 \vee e_3$
$\{2,3\}$	$e_1 \otimes e_2 + e_2 \otimes e_1$	$e_1 \vee e_2$

And the basis elements of $\mathrm{AT}^2(V)$ will be

M	$\sum_{t\in G_M} \mathrm{t}$	equiv in $F_2[e_1,e_2,e_3]$
$\{1,2\}$	$e_1\otimes e_2 - e_2\otimes e_1$	$e_1\wedge e_2$
$\{1,3\}$	$e_1\otimes e_3 - e_3\otimes e_1$	$e_1\wedge e_3$
$\{2,3\}$	$e_2\otimes e_3 - e_3\otimes e_2$	$e_2\wedge e_3$

(ii) $p=3$. Then the basis elements of $\mathrm{ST}^3(V)$ will be

M	$\sum_{t\in G_M} \mathrm{t}$	equiv in $F_2[e_1,e_2,e_3]$
$\{1,1,1\}$	$e_1\otimes e_1\otimes e_1$	$e_1\vee e_1\vee e_1$
$\{2,2,2\}$	$e_2\otimes e_2\otimes e_2$	$e_2\vee e_2\vee e_2$
$\{3,3,3\}$	$e_3\otimes e_3\otimes e_3$	$e_3\vee e_3\vee e_3$
$\{1,2,2\}$	$e_1\otimes e_2\otimes e_2 + e_2\otimes e_1\otimes e_2 + e_2\otimes e_2\otimes e_1$	$e_1\vee e_2\vee e_2$
$\{1,3,3\}$	$e_1\otimes e_3\otimes e_3 + e_3\otimes e_1\otimes e_3 + e_3\otimes e_3\otimes e_1$	$e_1\vee e_3\vee e_3$
$\{2,1,1\}$	$e_2\otimes e_1\otimes e_1 + e_1\otimes e_2\otimes e_1 + e_2\otimes e_2\otimes e_1$	$e_1\vee e_1\vee e_2$
$\{2,3,3\}$	$e_2\otimes e_3\otimes e_3 + e_3\otimes e_2\otimes e_3 + e_3\otimes e_3\otimes e_2$	$e_2\vee e_3\vee e_3$
$\{3,1,1\}$	$e_3\otimes e_1\otimes e_1 + e_1\otimes e_3\otimes e_1 + e_1\otimes e_1\otimes e_3$	$e_1\vee e_1\vee e_3$
$\{3,2,2\}$	$e_3\otimes e_2\otimes e_2 + e_2\otimes e_3\otimes e_2 + e_2\otimes e_2\otimes e_3$	$e_2\vee e_2\vee e_3$
$\{1,2,3\}$	$e_1\otimes e_2\otimes e_3 + e_1\otimes e_3\otimes e_2 + e_2\otimes e_1\otimes e_3$ $+e_2\otimes e_3\otimes e_1 + e_3\otimes e_1\otimes e_2 + e_3\otimes e_2\otimes e_1$	$e_1\vee e_2\vee e_3$

And for $\mathrm{AT}^3(V)$ we have

M	$\sum_{t\in G_M} \mathrm{t}$	equiv in $F_2[e_1,e_2,e_3]$
$\{1,2,3\}$	$e_1\otimes e_2\otimes e_3 - e_1\otimes e_3\otimes e_2 + e_2\otimes e_1\otimes e_3$ $-e_2\otimes e_3\otimes e_1 + e_3\otimes e_1\otimes e_2 - e_3\otimes e_2\otimes e_1$	$e_1\wedge e_2\wedge e_3$

This we have following two theorems.

Theorem 3.1 Let V be a finite dimensional vector space, and let $\mathcal{B}=\{e_1,\cdots,e_n\}$ be a basis. Then

$$\mathrm{ST}^p(V)\simeq F_p[e_1,\cdots,e_n],$$

and

$$\mathrm{AT}^p(V)\simeq F_p^-[e_1,\cdots,e_n].$$

In words,

> The symmetric tensor space $\mathrm{ST}^p(V)$ is isomorphic to the algebra $F_p[e_1,\cdots,e_n]$ of homogeneous polynomials of degree p.

And similarly

> The anti-symmetric tensor space $\mathrm{AT}^p(V)$ is isomorphic to the algebra $F_p^-[e_1,\cdots,e_n]$ of anti-commutative homogeneous polynomials of degree p.

It is easy to see (Roman Theorem 14.18) that

$$\dim(\mathrm{AT}^p(V))=\binom{n}{p},\qquad \dim(\mathrm{ST}^p(V))=\binom{n+p-1}{p}.$$

The formula for the dimension of $\mathrm{ST}^p(V)$ resembles the formula for all possible distribution of p units on energy in n containers (see Schroeder, Equation 2.9).

3.2 Ongoing thoughts

Observation 3.2.1 — Ongoing thought on the relation of the space of linear operators and the tensor product. In many instances, I have noticed a similar structure between $\mathcal{L}(V, W)$ and $V \otimes W$. For instance, we know that while $u \otimes v$ is a tensor (a pure tensor), but not every tensor can be written like this, but rather it is a linear combination of pure tensors. This is very similar to the idea that for $A : V \to W$ and $B : U \to W$, we can construct a linear map $C : U \oplus V \to W$, that has a block diagonal representation. But, we can not write every matrix in a block diagonal representation.

Also, another hint is that $\dim(\mathcal{L}(V, W)) = n \times m$, and similarly, $\dim(U \otimes V) = n \times m$. Yet another hint is that every elements of $U \otimes V$ has a matrix coordinate. I need to make this connection more clear and easy to see / understand.

4. Halmos Solution Manual

4.1 Fields

Observation 4.1.1 In a group we can only add one element an integer number of times with itself. For instance we can only have $\alpha + \alpha + \cdot + \alpha = m\alpha$ for some $m \in \mathbb{N}$. However, field is a generalization of group in the sense that we can have more general many times addition with itself for every element. For instance we can have $q\alpha$ where q is not necessarily an integer. The same is true in vector spaces. The fact that we can multiply a vector by some element of the underlying field (i.e. the scalar) shows this.

■ **Problem 4.1**

Solution (a) Holds because $(F, 0, +)$ is an abelean group.

(b) Since $(\mathcal{F}, 0, +)$ is an abelian group, then α has an inverse (i.e. $-\alpha$). Add this to both sides of the equation.

(c) We can write

$$\begin{aligned} \alpha + (\beta - \alpha) &= \alpha + (\beta + (-\alpha)) \\ &= \alpha + \beta + (-\alpha) && \text{(distributivity of multiplication)} \\ &= \alpha + (-\alpha) + \beta = \beta && ((F, 0, +) \text{ is abelian group}) \end{aligned}$$

(d) We can write

$$\alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0 + \alpha \cdot 0 = 2\alpha \cdot 0.$$

Adding the inverse of $\alpha \cdot 0$ to both sides we will get

$$\alpha \cdot 0 = 0.$$

(e) We can use the distributivity of multiplication and write

$$(-1)\alpha + \alpha = (-1 + 1)\alpha = 0 \cdot \alpha = 0.$$

Adding the inverse of α to both sides we will get

$$(-1)\alpha = -\alpha.$$

(f) We can write

$$\begin{aligned}(-\alpha)(-\beta) &= (-1(\alpha))(-\beta) && \text{(property proved above)}\\ &= ((-1)(\alpha))((-1)(\beta)) && \text{(property proved above)}\\ &= (-1)(-1)\alpha\beta && \text{(associativity of product)}\\ &= -(-1)\alpha\beta = \alpha\beta\end{aligned}$$

(g) If both α and β are zero, then it follows that $\alpha\beta = 0$. If one of them is not zero, WLOG we can assume $\beta \neq 0$, then β^{-1} exists, and multiplying it on the both sides we will get

$$\alpha = 0.$$

In a second run, I observed that my proof above might be wrong. I am somehow using the conclusion to prove the hypothesis.

■ **Problem 4.2**

Solution (a) No. $(F, 0, +)$ is not a group. $(F\backslash\{0\}, 1, \cdot)$ is not a group.

(b) No. $(F\backslash\{0\}, 1, \cdot)$ is not a group. The set of all integers is a Ring with identity.

(c) Yes. For instance, consider the set of all integers $\mathbb{Z}$. Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be a bijection. Define the addition and multiplication as

$$m \oplus n = \phi^{-1}(\phi(m) + \phi(n)), \qquad m \odot n = \phi^{-1}(\phi(m) \cdot \phi(n)).$$

Let $z_1 = \phi^{-1}(1)$ and $z_0 = \phi^{-1}(0)$. Then we claim that $(\mathbb{Z}, z_0, z_1, \oplus, \odot)$ is a field. It is straightforward to check that $(\mathbb{Z}, z_0, \oplus)$, and $(\mathbb{Z}\backslash\{z_0\}, z_1, \odot)$ are groups, and the distributitivty law holds. For instance, to check for the associativity of addition let $m, n, l \in \mathbb{Z}$. Then we have

$$\begin{aligned}(m \oplus n) \oplus l &= \phi^{-1}(\phi(m \oplus n) + \phi(l))\\ &= \phi^{-1}(\phi(m) + \phi(n) + \phi(l))\\ &= \phi^{-1}(\phi(m) + \phi(n \oplus l))\\ &= m \oplus (n \oplus l),\end{aligned}$$

where we have used the fact that $\phi(m \oplus n) = \phi(m) + \phi(n)$.

■ **Problem 4.3**

Solution (a) We can solve this part with different levels of abstraction. But we want to use the fact that the multiplicative group $U(n)$ (i.e. the set of numbers in $\mathbb{Z}_n$ that are prime relative to n) is a group under multiplication (see example 3.3 Lee Abstract Algebra). When n is prime, then $U(n)$ contains all numbers $1, \cdots, n-1$. Thus when n is prime, $(\mathbb{Z}_n\backslash\{0\}, \cdot)$ and $(\mathbb{Z}_n, +)$ are both groups, and since the distribution law holds, it follows that $\mathbb{Z}_n$ is a field if and only if n is a prime number.

(b) $-1 = 4$ in $\mathbb{Z}_5$.

(c) $\frac{1}{3} = 5$ in $\mathbb{Z}_7$.

Observation 4.1.2 The field $\mathbb{Z}_p$ has characteristic p.

■ **Problem 4.4**

Solution First, observe that if the cardinality of the underlying set of the field is infinite, then we have $\underbrace{1+\cdots+1}_{m} = m \cdot 1 \neq 0$ for all $m \in \mathbb{N}$. However, when F is finite, then

$$F \text{ is finite } \implies m \cdot 1 = 0 \text{ for some } m \in \mathbb{N}.$$

We can see this by contrapositive. If $m \cdot 1 \neq 0$ for all $m \in \mathbb{N}$ then F has at least $\mathbb{N}$ many elements. We want to show that the smallest such m is prime. Assume otherwise. Then $m = pq$ for some $p, q \neq 0$. Then

$$0 = m \cdot 1 = pq \cdot 1 = pq.$$

Since every field is an integral domain (has no zero divisors) (see Theorem 8.9 Lee Abstract Algebra), then it implies that $p = 0$ or $q = 0$, this is a contradiction.

■ **Problem 4.5**

Solution (a) Yes. It is easy to check that $(\mathbb{Q}(\sqrt{2}), 0, +)$ and $(\mathbb{Q}(\sqrt{2})\backslash\{0\}, 1, \cdot)$ are groups. The associativity and closedness of the operators can be shown directly. For instance

$$(\alpha + \beta\sqrt{2})(\eta + \gamma\sqrt{2}) = (\alpha\eta + 2\beta\gamma) + \sqrt{2}(\alpha\gamma + \beta\eta),$$

hence the multiplication is closed. Also, $0, 1 \in \mathbb{Q}$ are the same as $0, 1 \in \mathbb{Q}(\sqrt{2})$. Also, it is easy to check that the additive inverse of $\alpha + \sqrt{2}\beta$ is $-\alpha - \sqrt{2}\beta$. And the multiplicative inverse is easy to calculate and follows from the observation that

$$(\alpha + \beta\sqrt{2}) \cdot (\frac{\alpha - \beta\sqrt{2}}{\alpha^2 - 2\beta^2}) = 1.$$

So the multiplicative inverse of $\alpha + \beta\sqrt{2}$ is

$$\frac{\alpha - \beta\sqrt{2}}{\alpha^2 - 2\beta^2}.$$

(b) No. Because $1 + \sqrt{2}$ has no inverse of the form $\alpha + \beta\sqrt{2}$ where $\alpha, \beta \in \mathbb{Z}$.

■ **Problem 4.6**

Solution (a) No. Not every polynomial has an inverse with integer coefficients. For instance, $p = 2x^2 - 1$ should be multiplied by

$$-1 + 2x^2 - 4x^4 + 8x^6 - \cdots$$

to get the 1 polynomial. But the expression above is not a polynomial.

(b) No. The same problem above. The set of all polynomials with integer or real coefficients forms a commutative Ring.

■ **Problem 4.7**

Solution (a) The addition part of OK! I.e. $(F, (0,0), +)$ forms an abelian group. However, $(F\backslash\{(0,0)\}, \mathbb{1}, \cdot)$ does not form a group as defined above. Because by the provided definition of multiplication we need to have $(\alpha, \beta)\mathbb{1} = (\alpha, \beta)$ that implies that the only choice for $\mathbb{1}$ is

$$\mathbb{1} = (1, 1).$$

But then the elements $(0, 1)$ and $(1, 0)$ have no multiplicative inverses. This is not the only obstacle though.

(b) Yes. This multiplication resolves the obstacles above and $(F\backslash\{(0,0)\}, \mathbb{1}, \cdot)$ is an abelian group. It is easy to check that the multiplicative identity should be

$$\mathbb{1} = (1, 0).$$

I.e. this is the only choice that satisfies $(\alpha, \beta) \cdot \mathbb{1} = (\alpha, \beta)$. It is also easy to check that the inverse for a non-zero element (α, β) is

$$(\frac{\alpha}{\alpha^2 + \beta^2}, \frac{-\beta}{\alpha^2 + \beta^2}).$$

(c) It will lead to the same kind of structure.

4.2 Vector Spaces

Problem 4.8

Solution (a) This follows from $(V, 0, +)$ being an abelian group.

(b) The additive inverse of the zero element in an additive group is itself. So this follows from $(V, 0, +)$ being an abelian group.

(c) We can write

$$\alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0 + \alpha \cdot 0$$

Since the set of vectors is an additive abelian group, we can add the inverse of $\alpha \cdot 0$ to both sides and get

$$\alpha \cdot 0 = 0.$$

(d) We can write

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x.$$

Since the set of vectors is an additive abelian group, then adding the inverse of $0 \cdot x$ to both sides we will get

$$0 \cdot x = 0.$$

Remark Note that in the expression above, the zero on the LHS is the zero element of the field, and the zero on the RHS is the zero element of the vector field.

(e) Still thinking. I was trying to do a similar proof as for problem 1 part (g), but I realized that my proof for that part is also not correct.

(f) We can add $x = 1 \cdot x$ to $(-1)x$. Then using the distributivity law we can write

$$x + (-1)x = 0.$$

Adding the additive inverse of x to both sides we will get

$$(-1)x = -x.$$

(g) We can write

$$y + (x - y) = 1 \cdot y + 1 \cdot (x - y) = 1 \cdot (y + x + (-y)) = 1 \cdot x = x.$$

■ **Problem 4.9** The elements of $\mathbb{Z}_p^n$ are the n-tuples, or equivalently the set of all functions $f : [p] \to \mathbb{Z}_p$ where $[n] = \{1, 2, \cdots, n\}$. There are p^n such functions.

■ **Problem 4.10**

Solution No. One of the immediate problems that I can see is that the scalar 1 does not interact nicely with the vectors. I.e. in the vector space axioms we have $1 \cdot x = x$ for all $x \in V$. However, in the definition above we have $1 \cdot (\xi_1, \xi_2) = (1\xi_1, 0) = (\xi_1, 0) \neq (\xi_1, \xi_2)$.

■ **Problem 4.11**

Solution We assume that the vector space $\mathbb{C}^3$ is defined on $\mathbb{C}$ rather than $\mathbb{R}$.

(a) No. While the vector space $(V, 0, +)$ forms a group, but the scalars does not behave nicely. For instance $i \cdot (r_1, \xi_2, \xi_3) = (ir_1, \xi_2, \xi_3)$ and the first argument is not longer a real number.

(b) Yes.

(c) No. because $(\xi_1, 0, \xi_2) + (0, \tilde{\xi}_2, \tilde{\xi}_3) = (\xi_1, \tilde{\xi}_2, \xi_2 + \tilde{\xi}_3)$ and neither its first or second argument is zero.

(d) The vector space $(V, 0, +)$ forms a group. The addition is closed: Let (ξ_1, ξ_2, ξ_3) and $(\tilde{\xi}_1, \tilde{\xi}_2, \tilde{\xi}_3)$ be in the subspace. Then

$$\alpha(\xi_1, \xi_2, \xi_3) + \beta(\tilde{\xi}_1, \tilde{\xi}_2, \tilde{\xi}_3) = (\alpha\xi_1 + \beta\tilde{\xi}_1, \alpha\xi_2 + \beta\tilde{\xi}_2, \xi_3 + \tilde{\xi}_3).$$

Since

$$\alpha(\xi_1 + \xi_2) + \beta(\tilde{\xi}_1 + \tilde{\xi}_2) = 0,$$

then the sum is also in the subspace, and the addition is closed. Also, in additive inverse of (ξ_1, ξ_2, ξ_3) is

$$(-\xi_1, -\xi_2, -\xi_3)$$

where since $-(\xi_1 + \xi_2) = 0$ it implies that the inverse is also in the subspace. It is also easy to check that the scalars behave nicely with the vector space.

(e) No. This subspace does not contain the origin $(0, 0, 0)$.