Chapter 1 Proofs

Item	Summary
Definition 1.1	Complex numbers
Theorem 1.1	Properties of complex arithmetic
Definition 1.2	$-\alpha$, subtraction, $1/\alpha$, division
Notation 1.1	$\mathbf{F}$
Corollary 1.1	Power operations
Definition 1.3	List, length
Definition 1.4	$\mathbf{F}^n$
Definition 1.5	Addition in $\mathbf{F}^n$
Theorem 1.2	Commutativity of addition in $\mathbf{F}^n$
Definition 1.6	0
Definition 1.7	Additive inverse in $\mathbf{F}^n$
Definition 1.8	Scalar multiplication in $\mathbf{F}^n$
Definition 1.9	Addition, scalar multiplication
Definition 1.10	Vector space
Definition 1.11	Vector, point
Definition 1.12	Real vector space, complex vector space
Notation 1.2	$\mathbf{F}^S$
Theorem 1.3	Unique additive identity
Theorem 1.4	Unique additive inverse
Notation 1.3	$-v, w-v$
Notation 1.4	V
Theorem 1.5	The number 0 times a vector
Theorem 1.6	A number times the vector 0
Theorem 1.7	The number -1 times a vector
Definition 1.13	Subspace
Theorem 1.8	Conditions for a subspace
Theorem 1.9	Sum of subspaces is the smallest containing subspace
Definition 1.14	Direct sum

Theorem 1.10	Condition for a direct sum
Theorem 1.11	Direct sum of two subspaces

Theorem 1.1 (Properties of complex arithmetic)

- **Commutativity**

  $\alpha + \beta = \beta + \alpha$ and $\alpha\beta = \beta\alpha$ for all $\alpha, \beta \in \mathbf{C}$.

- **Associativity**

  $(\alpha + \beta) + \lambda = \alpha + (\beta + \lambda)$ and $(\alpha\beta)\lambda = \alpha(\beta\lambda)$ for all $\alpha, \beta, \lambda \in \mathbf{C}$.

- **Identities**

  $\lambda + 0 = \lambda$ and $\lambda \cdot 1 = \lambda$ for all $\lambda \in \mathbf{C}$.

- **Additive inverse**

  For every $\alpha \in \mathbf{C}$, there exists a unique $\beta \in \mathbf{C}$ such that $\alpha + \beta = 0$.

- **Multiplicative inverse**

  For every $\alpha \in \mathbf{C}$ with $\alpha \neq 0$, there exists a unique $\beta \in \mathbf{C}$ such that $\alpha\beta = 1$.

- **Distributive property**

  $\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta$ for all $\lambda, \alpha, \beta \in \mathbf{C}$.

Proof. For all $\alpha, \beta, \lambda \in \mathbf{C}$, let $\alpha = a + bi, \beta = c + di, \lambda = e + fi$, where $a, b, c, d, e, f \in \mathbf{R}$.

- **Commutativity**

$$\begin{aligned}
\alpha + \beta &= (a + bi) + (c + di) \\
&= (a + c) + (b + d)i \\
&= (c + a) + (d + b)i \\
&= (c + di) + (a + bi) \\
&= \beta + \alpha. \\
\alpha\beta &= (a + bi)(c + di) \\
&= (ac - bd) + (ad + bc)i \\
&= (ac - bd) + (da + cb)i \\
&= (ca - db) + (cb + da)i \\
&= (c + di)(a + bi) \\
&= \beta\alpha.
\end{aligned}$$

- **Associativity**

$$\begin{aligned}(\alpha+\beta)+\lambda &= [(a+bi)+(c+di)]+(e+fi)\\ &= [(a+c)+(b+d)i]+(e+fi)\\ &= (a+c+e)+(b+d+f)i\\ &= (a+bi)+[(c+e)+(d+f)i]\\ &= (a+bi)+[(c+di)+(e+fi)]\\ &= \alpha+(\beta+\lambda).\\ (\alpha\beta)\lambda &= [(a+bi)(c+di)](e+fi)\\ &= [(ac-bd)+(ad+bc)i](e+fi)\\ &= (ace-bde-adf-bcf)+(acf-bdf+ade+bce)i\\ &= (a+bi)[(ce-df)+(cf+de)i]\\ &= (a+bi)[(c+di)(e+fi)]\\ &= \alpha(\beta\lambda).\end{aligned}$$

- **Identities**

$$\lambda+0=(e+fi)+(0+0i)=(e+0)+(f+0)i=e+fi=\lambda.$$
$$\lambda\cdot 1=(e+fi)(1+0i)=(e\cdot 1-f\cdot 0)+(e\cdot 0+f\cdot 1)i=e+fi=\lambda.$$

- **Additive inverse**

  Let $c=-a$ and $d=-b$, then

  $$\alpha+\beta=(a+bi)+(c+di)=(a+c)+(b+d)i=(a-a)+(b-b)i=0+0i=0.$$

- **Multiplicative inverse**

  Because $\alpha\neq 0$, $a^2+b^2\neq 0$. Let $c=a/(a^2+b^2)$ and $d=-b/(a^2+b^2)$, then

  $$\alpha\beta=(a+bi)\left(\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i\right)=\left(\frac{a^2+b^2}{a^2+b^2}+\frac{-ab+ab}{a^2+b^2}i\right)=(1+0i)=1.$$

- **Distributive property**

$$\begin{aligned}\lambda(\alpha+\beta) &= (e+fi)[(a+bi)+(c+di)]\\ &= (e+fi)[(a+c)+(b+d)i]\end{aligned}$$

$$
\begin{aligned}
&= (ea + ec - fb - fd) + (eb + ed + fa + fc)i \\
&= [(ea - fb) + (eb + fa)i] + [(ec - fd) + (ed + fc)i] \\
&= (e + fi)(a + bi) + (e + fi)(c + di) \\
&= \lambda\alpha + \lambda\beta.
\end{aligned}
$$

■

Corollary 1.1 For all $\alpha, \beta \in \mathbf{F}$ and all positive integers m, n, there is $(\alpha^m)^n = \alpha^{mn}$ and $(\alpha\beta)^m = \alpha^m\beta^m$.

Proof. For all $\alpha, \beta \in \mathbf{F}$ and all positive integers m, n, there is

$$
(\alpha^m)^n = \underbrace{\alpha^m\alpha^m \cdots \alpha^m}_{n} = \alpha^{mn}.
$$

$$
(\alpha\beta)^m = \underbrace{(\alpha\beta)(\alpha\beta)\cdots(\alpha\beta)}_{m} = (\underbrace{\alpha\alpha\cdots\alpha}_{m})(\underbrace{\beta\beta\cdots\beta}_{m}) = \alpha^m\beta^m.
$$

■

Theorem 1.2 (Commutativity of addition in $\mathbf{F}^n$) If $x, y \in \mathbf{F}^n$, then $x + y = y + x$.

Proof. For $x, y \in \mathbf{F}^n$, let $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$, then

$$
\begin{aligned}
x + y &= (x_1, \cdots, x_n) + (y_1, \cdots, y_n) \\
&= (x_1 + y_1, \cdots, x_n + y_n) \\
&= (y_1 + x_1, \cdots, y_n + x_n) \\
&= (y_1, \cdots, y_n) + (x_1, \cdots, x_n) \\
&= y + x.
\end{aligned}
$$

■

Theorem 1.3 (Unique additive identity) A vector space has a unique additive indentity.

Proof. Suppose that a vector space V has another additive indentity $0'$, so $v + 0 = v + 0' = v$ for all $v \in V$. Then

$$
\left.
\begin{aligned}
&0 + 0' = 0' + 0 \\
&0 + 0' = 0' \\
&0' + 0 = 0
\end{aligned}
\right\}
\quad \Rightarrow \quad 0 = 0'.
$$

Thus, a vector space has a unique additive indentity.

■

Theorem 1.4 (Unique additive inverse) Every element in a vector space has a unique additive inverse.

Proof. Suppose that every element in a vector space V has another additive inverse, so for every $v \in V$, there exists $w, w' \in V$ such that $v + w = v + w' = 0$. Then

$$w = w + 0 = w + (v + w') = (w + v) + w' = 0 + w' = w'.$$

Thus, every element in a vector space has a unique additive inverse.

■

Theorem 1.5 (The number 0 times a vector) $0 \cdot v = 0$ for every $v \in V$.

Proof. For every $v \in V$, we have

$$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v \quad \Rightarrow \quad 0 \cdot v = 0.$$

Thus, $0 \cdot v = 0$ for every $v \in V$.

■

Theorem 1.6 (A number times the vector 0) $a \cdot 0 = 0$ for every $a \in \mathbf{F}$.

Proof. For every $a \in \mathbf{F}$, we have

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \quad \Rightarrow \quad a \cdot 0 = 0.$$

Thus, $a \cdot 0 = 0$ for every $a \in \mathbf{F}$.

■

Theorem 1.7 (The number −1 times a vector) $(-1) \cdot v = -v$ for every $v \in V$.

Proof. For every $v \in V$, we have

$$v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = [1 + (-1)] \cdot v = 0 \cdot v = 0.$$

Thus, $(-1) \cdot v = -v$ for every $v \in V$.

■

Theorem 1.8 (Conditions for a subspace) A subset U of V is a subspace of V if and only if U satisfies the following three conditions:

- **Additive identity**

$$0 \in U.$$

- **Closed under addition**

$$u, w \in U \text{ implies } u + w \in U.$$

- **Closed under scalar multiplication**

$$a \in \mathbf{F} \text{ and } u \in U \text{ implies } au \in U.$$

Proof.

1. A subset U of V is a subspace of V $\Rightarrow$ U satisfies those three conditions.

   Because U is a subspace of V, U is a vector space. With the additive identity, there exists an element $0 \in U$ such that $u + 0 = U$ for all $u \in U$; with the addition, $u + w \in U$ for each pair of elements $u, w \in U$; with the scalar multiplication, $au \in U$ for each $a \in \mathbf{F}$ and each $u \in U$.

2. A subset U of V is a subspace of V $\Leftarrow$ U satisfies those three conditions.

   - Commutativity

     Because $U \in V$ and for all $u, v \in U$, there are $u, v \in V$. Because $u + v = v + u$ for all $u, v \in V$, there are $u + v = v + u$ for all $u, v \in U$.

   - Associativity

     Because $U \in V$ and for all $u, v, w \in U$, there are $u, v, w \in V$. Because $(u + v) + w = u + (v + u)$ and $(ab)v = a(bv)$ for all $u, v, w \in V$ and all $a, b \in \mathbf{F}$. There are $(u + v) + w = u + (v + u)$ and $(ab)v = a(bv)$ for all $u, v, w \in U$ and all $a, b \in \mathbf{F}$.

   - Additive identity

     Because $U \in V$ and for all $u \in U$, there is $u \in V$. Because there exists an element $0 \in V$ such that $v + 0 = v$ for all $v \in V$, there is $u + 0 = u$ for all $u \in U$.

- Additive inverse

  If $u \in U$, because $-1 \in \mathbf{F}$, there is $-1 \cdot u = -u \in U$. For every $u \in U$, there exists $-u \in U$ such that $u + (-u) = 0$.

- Multiplicative identity

  Because $U \in V$ and for all $u \in U$, there is $u \in V$. Because $1 \cdot v = v$ for all $v \in V$, there is $1 \cdot u = u$ for all $u \in U$.

- Distributive identity

  Because $U \in V$ and for all $u, v \in U$, there is $u, v \in V$. Because $a(u + v) = au + av$ and $(a + b)v = av + bv$ for all $a, b \in \mathbf{F}$ and all $u, v \in V$, there is $a(u + v) = au + av$ and $(a + b)v = av + bv$ for all $a, b \in \mathbf{F}$ and all $u, v \in U$.

To sum up, U is a vector space. With U is a subset of V, U is a subspace of V.

$\blacksquare$

Theorem 1.9 (Sum of subspaces is the smallest containing subspace) Suppose $U_1, \cdots, U_m$ are subspaces of V. Then $U_1 + \cdots + U_m$ is the smallest subspace of V containing $U_1, \cdots, U_m$.

Proof.

1. We will prove that $U_1 + \cdots + U_m$ is a subspace of V.

   - Because $0 \in U_1, \cdots, 0 \in U_m$, then $0 + \cdots + 0 = 0 \cdot m = 0 \in U_1 + \cdots + U_m$.
   - For every $u_1, w_1 \in U_1, \cdots, u_m, w_m \in U_m$, we have $u_1 + w_1 \in U_1, \cdots, u_m + w_m \in U_m$ and $u_1 + \cdots + u_m, w_1 + \cdots + w_m \in U_1 + \cdots + U_m$. In addition,

     $$(u_1 + w_1) + \cdots + (u_m + w_m) \in U_1 + \cdots + U_m.$$

     Because

     $$(u_1 + w_1) + \cdots + (u_m + w_m) = (u_1 + \cdots + u_m) + (w_1 + \cdots + w_m),$$

     $U_1 + \cdots + U_m$ is closed under addition.

- For every $a \in \mathbf{F}$ and $u_1 \in U_1, \cdots, u_m \in U_m$, we have $au_1 \in U_1, \cdots, au_m \in U_m$ and $u_1 + \cdots + u_m \in U_1 + \cdots + U_m$. In addition,

$$au_1 + \cdots + au_m \in U_1 + \cdots + U_m.$$

Because

$$au_1 + \cdots + au_m = a(u_1 + \cdots + u_m),$$

$U_1 + \cdots + U_m$ is closed under scalar multiplication.

To sum up, $U_1 + \cdots + U_m$ is a subspace of V.

2. We will prove that $U_1 + \cdots + U_m$ is the smallest subspace of V containing $U_1, \cdots, U_m$.

- For $j = 1, \cdots, m$ and for every $u_1 \in U_1, \cdots, u_m \in U_m$, we have

$$\underbrace{0 + \cdots + 0 + u_j + 0 + \cdots + 0}_{m} = u_j \in U_1 + \cdots + U_m.$$

Therefore, $U_1, \cdots, U_m$ are all contained in $U_1 + \cdots + U_m$.

- Because every element $u \in U_1 + \cdots + U_m$ can be written in the form

$$u = u_1 + \cdots + u_m,$$

where $u_1 \in U_1, \cdots, u_m \in U_m$. Every subspace of V must contain all the elements of $U_1 + \cdots + U_m$, so it contains $U_1 + \cdots + U_m$.

To sum up, $U_1 + \cdots + U_m$ is the smallest subspace of V containing $U_1, \cdots, U_m$.

■

Theorem 1.10 (Condition for a direct sum) Suppose $U_1, \cdots, U_m$ are subspaces of V. Then $U_1 + \cdots + U_m$ is a direct sum if and only if the only way to write 0 as a sum $u_1 + \cdots + u_m$, where each u_j is in U_j, is by taking each u_j equal to 0.

Proof.

1. $U_1 + \cdots + U_m$ is a direct sum $\Rightarrow$ the only way to write 0 as a sum $u_1 + \cdots + u_m$, where each u_j is in U_j, is by taking each u_j equal to 0.

   Because $U_1 + \cdots + U_m$ is a direct sum and $0 \in U_1 + \cdots + U_m$, there is only one way to write 0 as a sum $u_1 + \cdots + u_m$. If we take each u_j which is in U_j equal to 0, we can get 0. Therefore, it is the only way to write 0 as a sum $u_1 + \cdots + u_m$, where each u_j is in U_j.

2. $U_1+\cdots+U_m$ is a direct sum $\Leftarrow$ the only way to write 0 as a sum $u_1+\cdots+u_m$, where each u_j is in U_j, is by taking each u_j equal to 0.

   Let $v \in U_1+\cdots+U_m$. We can write

$$v = u_1+\cdots+u_m$$

   for some $u_1 \in U_1, \cdots, u_m \in U_m$. To show that this representation is unique, suppose we also have

$$v = v_1+\cdots+v_m$$

   where $v_1 \in U_1, \cdots, v_m \in U_m$. Subtracting these two equations, we have

$$0 = (u_1-v_1)+\cdots+(u_m-v_m).$$

   Because $u_1-v_1 \in U_1, \cdots, u_m-v_m \in U_m$, the equation above implies that each u_j-v_j equals 0. Thus, $u_1=v_1, \cdots, u_m=v_m$.

■

Theorem 1.11 (Direct sum of two subspaces) Suppose U and W are subspaces of V. Then $U+W$ is a direct sum if and only if $U \cap W = \{0\}$.

Proof.

1. $U+W$ is a direct sum $\Rightarrow U \cap W = \{0\}$.

   Because $0 \in U$ and $0 \in W$, we have $0 \in U \cap W$. Suppose that there exists another element $v \in U \cap W$ and $v \neq 0$, then there are two ways to write v as a sum $u+w$, where $u \in U, w \in W$.

$$\left.\begin{aligned} u=v, w=0 \quad &\Rightarrow \quad v+0=v \\ u=0, w=v \quad &\Rightarrow \quad 0+v=v \end{aligned}\right\} \quad \Rightarrow \quad v=v+0=0+v.$$

   This contradicts with the statement that $U+W$ is a direct sum, so $U \cap W = \{0\}$.

   If $v \in U \cap W$, then $0 = v+(-v)$, where $v \in U$ and $-v \in W$. By the unique representation of 0 as the sum of a vector in U and a vector in W, we have $v=0$. Thus $U \cap W = \{0\}$.

2. $U + W$ is a direct sum $\Leftarrow U \cap W = \{0\}$.

   Because there is one way to write v as a sum $u + w$, where $u \in U, w \in W$. Let $u = w = 0$, then $u + w = 0 + 0 = 0$. Suppose that there is another way to write v as a sum $u + w$, where $u \in U, w \in W$. Let $u \neq 0$, then

   $$u + w = 0 \quad \Rightarrow \quad w = -u.$$

   However, because $w = -u \in W$ and $-1 \in \mathbf{F}$, we have $-1 \cdot (-u) = -(-u) - u \in W$. Therefore, $u \in U \cap W$ and $u \neq 0$, which contradicts with the statement that $U \cap W = \{0\}$. Thus, the only way to write 0 as a sum $u + w$, where each $u \in U$ and $w \in W$, is by taking each u and w equal to 0. With Theorem 1.10, we can conclude that $U + W$ is a direct sum.

   Suppose $u \in U, w \in W$, and

   $$0 = u + w.$$

   The equation above implies that $u = -w \in W$. Thus, $u \in U \cap W$. Hence, $u = 0$, which by the equation above implies that $w = 0$.

■