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 1.1 (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.

$\blacksquare$

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.

$\blacksquare$

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 $v \in V$.

$\blacksquare$

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 $a \in \mathbf{F}$.

$\blacksquare$

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 $v \in V$.

$\blacksquare$