F.2. Proofs: Vector Spaces

Proposition F.2.1. — *Let V be an $\mathbb{F}$-vector space and let W be a subgroup of V. Then the cosets of W in V partition V.*

Proof. —
To show: (a) If $v \in V$ then there exists $v' \in V$ such that $v \in v' + W$.
(b) If $(v_1 + W) \cap (v_2 + W) \neq \emptyset$ then $v_1 + W = v_2 + W$.

(a) Let $v \in V$.
Since $0 \in W$ then $v = v + 0 \in v + W$.
So $v \in v + W$.

(b) Assume $(v_1 + W) \cap (v_2 + W) \neq \emptyset$.
To show: (ba) $v_1 + W \subseteq v_2 + W$.
(bb) $v_2 + W \subseteq v_1 + W$.
Let $a \in (v_1 + W) \cap (v_2 + W)$.
Suppose $a = v_1 + w_1$ and $a = v_2 + w_2$ where $w_1, w_2 \in W$.
Then

$$v_1 = v_1 + w_1 - w_1 = a - w_1 = v_2 + w_2 - w_1 \quad \text{and}$$
$$v_2 = v_2 + w_2 - w_2 = a - w_2 = v_1 + w_1 - w_2.$$

(ba) Let $v \in v_1 + W$.
Then there exists $w \in W$ such that $v = v_1 + w$.
Since $w_2 - w_1 + w \in W$.

$$v = v_1 + w = v_2 + w_2 - w_1 + w \in v_2 + W.$$

So $v_1 + W \subseteq v_2 + W$.

(bb) Let $v \in v_2 + W$.
Then there exists $w \in W$ such that $v = v_2 + w$.
Since $w_1 - w_2 + w \in W$ then

$$v = v_2 + w = v_1 + w_1 - w_2 + w \in v_1 + W.$$

So $v_2 + W \subseteq v_1 + W$.

So $v_1 + W = v_2 + W$.

So the cosets of W in V partition V. □

Theorem F.2.2. — *Let W be a subgroup of an $\mathbb{F}$-vector space V. Then W is a subspace of V if and only if V/W with operations given by*

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W \quad \textit{and} \qquad c(v + W) = cv + W,$$

is an $\mathbb{F}$-vector space.

Proof. —
$\Longrightarrow$: Assume W is a subspace of V.
To show: (a) $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$ is a well defined operation on V/W.
(b) The operation given by $c(v + W) = cv + W$ is well defined.
(c) If $v_1 + W, v_2 + W, v_3 + W \in V/W$ then
$\big((v_1 + W) + (v_2 + W)\big) + (v_3 + W) = (v_1 + W) + \big((v_2 + W) + (v_3 + W)\big)$.
(d) If $v_1 + W, v_2 + W \in V/W$ then $(v_1 + W) + (v_2 + W) = (v_2 + W) + (v_1 + W)$.
(e) $0 + W = W$ is the zero in V/W.

Notes of Arun Ram aram@unimelb.edu.au, Version: 7 April 2020

(f) $-v+W$ is the additive inverse of $v+W$.
(g) If $c_1, c_2 \in F$ and $v+W \in V/W$, then $c_1\big(c_2(v+W)\big) = (c_1c_2)(v+W)$.
(h) If $v+W \in V/W$ then $1(v+W) = v+W$.
(i) If $c \in \mathbb{F}$ and $v_1+W, v_2+W \in V/W$ then
$c\big((v_1+W)+(v_2+W)\big) = c(v_1+W)+c(v_2+W)$.
(j) If $c_1, c_2 \in \mathbb{F}$ and $v+W \in V/W$ then $(c_1+c_2)(v+W) = c_1(v+W)+c_2(v+W)$.

(a) To show:

$$\begin{array}{ccc} V/W \times V/W & \to & V/W \\ (v_1+W, v_2+W) & \mapsto & (v_1+v_2)+W \end{array} \quad \text{is a function.}$$

Let $(v_1+W, v_2+W), (v_3+W, v_4+W) \in V/W \times V/W$ such that $(v_1+W, v_2+W) = (v_3+W, v_4+W)$.
Then $v_1+W = v_3+W$ and $v_2+W = v_4+W$.
To show: $(v_1+v_2)+W = (v_3+v_4)+W$.
To show: (aa) $(v_1+v_2)+W \subseteq (v_3+v_4)+W$.
(ab) $(v_3+v_4)+W \subseteq (v_1+v_2)+W$.

(aa) Since $v_1+W = v_3+W$ then $v_1 = v_1+0 \in v_3+W$.
So there exists $w_1 \in W$ such that $v_1 = v_3+w_1$.
Similarly there exists $w_2 \in W$ such that $v_2 = v_4+w_2$.
Let $t \in (v_1+v_2)+W$.
Then there exists $w \in W$ such that $t = v_1+v_2+w$.
Since addition is commutative then

$$\begin{aligned} t &= v_1+v_2+w \\ &= v_3+w_1+v_4+w_2+w \\ &= v_3+v_4+w_1+w_2+w, \end{aligned}$$

So $t = (v_3+v_4)+(w_1+w_2+w) \in v_3+v_4+W$.
So $(v_1+v_2)+W \subseteq (v_3+v_4)+W$.

(ab) Since $v_1+W = v_3+W$ then there exists $w_1 \in W$ such that $v_1+w_1 = v_3$.
Since $v_2+W = v_4+W$ there exists $w_2 \in W$ such that $v_2+w_2 = v_4$.
Let $t \in (v_3+v_4)+W$.
Then there exists $w \in W$ such that $t = v_3+v_4+w$.
Since addition is commutative then

$$\begin{aligned} t &= v_3+v_4+w \\ &= v_1+w_1+v_2+w_2+w \\ &= v_1+v_2+w_1+w_2+w, \end{aligned}$$

So $t = (v_1+v_2)+(w_1+w_2+w) \in (v_1+v_2)+W$.
So $(v_3+v_4)+W \subseteq (v_1+v_2)+W$.

So $(v_1+v_2)+W = (v_3+v_4)+W$.
So the operation given by $(v_1+W)+(v_3+W) = (v_1+v_3)+W$ is a well defined operation on V/W.

(b) To show:

$$\begin{array}{ccc} \mathbb{F} \times V/W & \to & V/W \\ (c, v+W) & \mapsto & cv+W \end{array} \quad \text{is a function.}$$

Let $(c_1, v_1+W), (c_2, v_2+W) \in (\mathbb{F} \times V/W)$ such that $(c_1, v_1+W) = (c_2, v_2+W)$.

Then $c_1 = c_2$ and $v_1 + W = v_2 + W$.
To show: $c_1v_1 + W = c_2v_2 + W$.
To show: (ba) $c_1v_1 + W \subseteq c_2v_2 + W$.
(bb) $c_2v_2 + W \subseteq c_1v_1 + W$.

(ba) Since $v_1 + W = v_2 + W$ then there exists $w_1 \in W$ such that $v_1 = v_2 + w_1$.
Let $t \in c_1v_1 + W$.
Then there exists $w \in W$ such that $t = c_1v_1 + w$.
Since $c_1 = c_2$ then

$$\begin{aligned} t &= c_1v_1 + w \\ &= c_2(v_2 + w_1) + w \\ &= c_2v_2 + c_2w_1 + w, \end{aligned}$$

Since W is a subspace then $c_2w_1 \in W$ and $c_2w_1 + w \in W$.
So $t = c_2v_2 + c_2w_1 + w \in c_2v_2 + W$.
So $c_1v_1 + W \subseteq c_2v_2 + W$.

(bb) Since $v_1 + W = v_2 + W$ then there exists $w_2 \in W$ such that $v_2 = v_1 + w_2$.
Let $t \in c_2v_2 + W$.
Then there exists $w \in W$ such that $t = c_2v_2 + w$.
Since $c_2 = c_1$ then

$$\begin{aligned} t &= c_2v_2 + w \\ &= c_1(v_1 + w_2) + w \\ &= c_1v_1 + c_1w_2 + w, \end{aligned}$$

Since W is a subspace then $c_1w_2 \in W$ and $c_1w_2 + w \in W$.
So $t = c_1v_1 + c_1w_2 + w \in c_1v_1 + W$.
So $c_2v_2 + W \subseteq c_1v_1 + W$.
So $c_1v_1 + W = c_2v_2 + W$.
So the operation is well defined.

(c) By the associativity of addition in V and the definition of the operation in V/W, if $v_1 + W, v_2 + W, v_3 + W \in V/W$ then

$$\begin{aligned} \big((v_1 + W) + (v_2 + W)\big) + (v_3 + W) &= \big((v_1 + v_2) + W\big) + (v_3 + W) \\ &= \big((v_1 + v_2) + v_3\big) + W \\ &= \big(v_1 + (v_2 + v_3)\big) + W \\ &= (v_1 + W) + \big((v_2 + v_3) + W\big) \\ &= (v_1 + W) + \big((v_2 + W) + (v_3 + W)\big) \end{aligned}$$

(d) By the commutativity of addition in V and the definition of the operation in V/W, if $v_1 + W, v_2 + W \in V/W$ then

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W = (v_2 + v_1) + W = (v_2 + W) + (v_1 + W).$$

(e) If $v + W \in V/W$ then

$$\begin{aligned} W + (v + W) &= (0 + v) + W \\ &= v + W \\ &= (v + 0) + W \\ &= (v + W) + W. \end{aligned}$$

So the coset $W = 0 + W$ is the zero in V/W.

(f) Let $v + W \in V/W$. Then

$$\begin{aligned} (v + W) + (-v + W) &= v + (-v) + W \\ &= 0 + W \\ &= W \\ &= (-v + v) + W \\ &= (-v + W) + v + W \end{aligned}$$

Thus $(-v) + W$ is the additive inverse of $v + W$.

(g) Assume $c_1, c_2 \in \mathbb{F}$ and $v + W \in V/W$.
Then, by definition of the operation,

$$\begin{aligned} c_1\big(c_2(v + W)\big) &= c_1(c_2 v + W) \\ &= c_1(c_2 v) + W \\ &= (c_1 c_2)v + W \\ &= (c_1 c_2)(v + W). \end{aligned}$$

(h) Assume $v + W \in V/W$.
Then, by definition of the operation,

$$\begin{aligned} 1(v + W) &= (1v) + W \\ &= v + W. \end{aligned}$$

(i) Assume $c \in \mathbb{F}$ and $v_1 + W, v_2 + W \in V/W$.
Then

$$\begin{aligned} c\big((v_1 + W) + (v_2 + W)\big) &= c\big((v_1 + v_2) + W\big) \\ &= c(v_1 + v_2) + W \\ &= (cv_1 + cv_2) + W \\ &= (cv_1 + W) + (cv_2 + W) \\ &= c(v_1 + W) + c(v_2 + W). \end{aligned}$$

(j) Assume $c_1, c_2 \in F$ and $v + W \in V/W$.
Then

$$\begin{aligned} (c_1 + c_2)(v + W) &= \big((c_1 + c_2)v\big) + W \\ &= (c_1 v + c_2 v) + W \\ &= (c_1 v + W) + (c_2 v + W) \\ &= c_1(v + W) + c_2(v + W). \end{aligned}$$

So V/W is a vector space over $\mathbb{F}$.

$\Longleftarrow$: Assume W is a subgroup of V and V/W is a vector space over $\mathbb{F}$ with action given by $c(v+W) = cv + W$.
To show: W is a subspace of V.
To show: If $c \in \mathbb{F}$ and $w \in W$ then $cw \in W$.
First we show: If $w \in W$ then $w + W = W$.
To show: (a) $w + W \subseteq W$.
(b) $W \subseteq w + W$.

(a) Let $k \in w + W$.
Then there exists w_1 $\in W$ such that $k = w + w_1$.
Since W is a subgroup then $w + w_1 \in W$.
So $w + W \subseteq W$.

(b) Let $k \in W$.
Since $k - w \in W$ then $k = w + (k - w) \in w + W$.
So $W \subseteq w + W$.

Now assume $c \in \mathbb{F}$ and $w \in W$.
Then, by definition of the operation on V/W,

$$\begin{aligned} cw + W &= c(w + W) \\ &= c(0 + W) \\ &= c \cdot 0 + W \\ &= 0 + W \\ &= W. \end{aligned}$$

So $cw = cw + 0 \in W$.
So W is a subspace of V. □

Proposition F.2.3. — *Let $T\colon V \to W$ be a linear transformation. Let 0_V and 0_W be the zeros for V and W respectively. Then*

(a) $T(0_V) = 0_W$.
(b) For any $v \in V$, $T(-v) = -T(v)$.

Proof. —

(a) Add $-T(0_V)$ to both sides of the following equation,

$$T(0_V) = T(0_V + 0_V) = T(0_V) + T(0_V).$$

(b) Since $T(v) + T(-v) = T\big(v + (-v)\big) = T(0_V) = 0_W$ and

$$T(-v) + T(v) = T\big((-v) + v\big) + T(0_V) = 0_W$$

then $-T(v) = T(-v)$.

□

Proposition F.2.4. — *Let $T\colon V \to W$ be a linear transformation. Then*

(a) $\ker T$ is a subspace of V.
(b) $\mathrm{im} T$ is a subspace of W.

Proof. — Let 0_V and 0_W be the zeros in V and W, respectively.

(a) By condition (a) in the definition of linear transformation, T is a group homomorphism.
To show: (aa) If $k_1, k_2 \in \ker T$ then $k_1 + k_2 \in \ker T$.
(ab) $0_V \in \ker T$.
(ac) If $k \in \ker T$ then $-k \in \ker T$.
(ad) If $c \in \mathbb{F}$ and $k \in \ker T$ then $ck \in \ker T$.

(aa) Assume $k_1, k_2 \in \ker T$.
Then $T(k_1) = 0_W$ and $T(k_2) = 0_W$.
By condition (a) in the definition of a linear transformation,

$$T(k_1 + k_2) = T(k_1) + T(k_2) = 0 + 0 = 0.$$

So $k_1 + k_2 \in \ker T$.

(ab) By Proposition F.2.1(a), $T(0_V) = 0_W$.
So $0_V \in \ker T$.

(ac) Assume $k \in \ker T$.
By Proposition F.2.1(b), $T(-k) = -T(k)$.
So $T(-k) = -T(k) = -0_W = 0_W$, and $-0_W = 0_W$ since $0_W + 0_W = 0_W$.
So $-k \in \ker T$.

(ad) Assume $c \in \mathbb{F}$ and $k \in \ker T$.
Then, by the definition of linear transformation,

$$T(ck) = cT(k) = c\,0_W = 0_W, \qquad \text{and} \quad c\,0_W = 0_W,$$

by adding $-c\,0_W$ to each side of $c\,0_W + c\,0_W = c(0_W + 0_W) = c\,0_W$.
So $T(ck) = 0_W$ and $ck \in \ker T$.

So $\ker T$ is a subspace of V.

(b) By condition (a) in the definition of linear transformation, T is a group homomorphism.
To show: (ba) If $w_1, w_2 \in \operatorname{im} T$ then $w_1 + w_2 \in \operatorname{im} T$.
(bb) $0_W \in \operatorname{im} T$.
(bc) If $w \in \operatorname{im} T$ then $-w \in \operatorname{im} T$.
(bd) If $c \in \mathbb{F}$ and $w \in \operatorname{im} T$ then $ck \in \operatorname{im} T$.

(ba) Assume $w_1, w_2 \in \operatorname{im} T$.
Then there exist $v_1, v_2 \in V$ such that $T(v_1) = w_1$ and $T(v_2) = w_2$.
By condition (a) in the definition of linear transformation,

$$T(v_1 + v_2) = T(v_1) + T(v_2) = w_1 + w_2.$$

So $w_1 + w_2 \in \operatorname{im} T$.

(bb) By Proposition F.2.1(a), $T(0_V) = 0_W$.
So $0_W \in \operatorname{im} T$.

(bc) Assume $w \in \operatorname{im} T$.
The there exists $v \in V$ such that $T(v) = w$.
By Proposition F.2.1(b), $T(-v) = -T(v) = -w$.
So $-w \in \operatorname{im}\ T$.

(bd) To show: If $c \in \mathbb{F}$ and $a \in \operatorname{im} T$ then $ca \in \operatorname{im} T$.
Assume $c \in \mathbb{F}$ and $c \in \operatorname{im} T$.
Then there exists $v \in V$ such that $a = T(v)$.
By the definition of linear transformation,

$$ca = cT(v) = T(cv).$$

So $ca \in \operatorname{im} T$.
So $\operatorname{im} T$ is a subspace of W.

□

Proposition F.2.5. — *Let $T\colon V \to W$ be a linear transformation. Let 0_V be the zero in V. Then*

(a) $\ker T = (0_V)$ *if and only if* T *is injective.*
(b) $\operatorname{im} T = W$ *if and only if* T *is surjective.*

Proof. — Let 0_V and 0_W be the zeros in V and W respectively.

(a) $\Longrightarrow$: Assume $\ker T = (0_V)$.
To show: If $T(v_1) = T(v_2)$ then $v_1 = v_2$.
Assume $T(v_1) = T(v_2)$.
Since T is a linear transformation then

$$0_W = T(v_1) - T(v_2) = T(v_1 - v_2).$$

So $v_1 - v_2 \in \ker T$.
Since $\ker T = (0_V)$ then $v_1 - v_2 = 0_V$.
So $v_1 = v_2$.
So T is injective.

$\Longleftarrow$: Assume T is injective
To show: (aa) $(0_V) \subseteq \ker T$.
(ab) $\ker T \subseteq (0_V)$.
(aa) Since $T(0_V) = 0_W$ then $0_V \in \ker T$.
So $(0_V) \subseteq \ker T$.
(ab) Let $k \in \ker T$.
Then $T(k) = 0_W$.
So $T(k) = T(0_V)$.
Thus, since T is injective then $k = 0_V$.
So $\ker T \subseteq (0_V)$.
So $\ker T = (0_V)$.

(b) $\Longrightarrow$: Assume $\operatorname{im} T = W$.
To show: If $w \in W$ then there exists $v \in V$ such that $T(v) = w$.
Assume $w \in W$.
Then $w \in \operatorname{im} T$.
So there exists $v \in V$ such that $T(v) = w$.
So T is surjective.

$\Longleftarrow$: Assume T is surjective.
To show: (ba) $\operatorname{im} T \subseteq W$.
(bb) $W \subseteq \operatorname{im} T$.
(ba) Let $x \in \operatorname{im} T$.
Then there exists $v \in V$ such that $x = T(v)$.
By the definition of T, $T(v) \in W$.
So $x \in W$.

So $\mathrm{im}\, T \subseteq W$.

(bb) Assume $x \in W$.
Since T is surjective there exists $v \in V$ such that $T(v) = x$.
So $x \in \mathrm{im}\, T$.
So $W \subseteq \mathrm{im}\, T$.
So $\mathrm{im}\, T = W$.

□

Theorem F.2.6. —
(a) Let $T\colon V \to W$ be a linear transformation and let $K = \ker T$. Define

$$\begin{array}{cccc} \hat{T}\colon & V/\ker T & \to & W \\ & v + K & \mapsto & T(v). \end{array}$$

Then $\hat{T}$ is a well defined injective linear transformation.

(b) Let $T\colon V \to W$ be a linear transformation and define

$$\begin{array}{cccc} T'\colon & V & \to & \mathrm{im} T \\ & v & \mapsto & T(v). \end{array}$$

Then T' is a well defined surjective linear transformation.

(c) If $T\colon V \to W$ is a linear transformation, then

$$V/\ker T \simeq \mathrm{im} T$$

where the isomorphism is a vector space isomorphism.

Proof. —
(a) To show: (aa) $\hat{T}$ is a function.
(ab) $\hat{T}$ is injective.
(ac) $\hat{T}$ is a linear transformation.

(aa) To show: (aaa) If $v \in V$ then $\hat{T}(v + K) \in W$.
(aab) If $v_1 + K = v_2 + K \in V/K$ then $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$.

(aaa) Assume $v \in V$.
Then $\hat{T}(v + K) = T(v)$ and $T(v) \in W$, by the definition of $\hat{T}$ and T.

(aab) Assume $v_1 + K = v_2 + K$.
Then there exists $k \in K$ such that $v_1 = v_2 + k$.
To show: $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$, i.e.
To show: $T(v_1) = T(v_2)$.
Since $k \in \ker T$ then $T(k) = 0$ and so

$$T(v_1) = T(v_2 + k) = T(v_2) + T(k) = T(v_2).$$

So $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$.
So $\hat{T}$ is well defined.

(ab) To show: If $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$ then $v_1 + K = v_2 + K$.
Assume $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$. Then $T(v_1) = T(v_2)$.
So $T(v_1) - T(v_2) = 0$.
So $T(v_1 - v_2) = 0$.
So $v_1 - v_2 \in \ker T$.

So there exists $k \in \ker T$ such that $v_1 - v_2 = k$.
So there exists $k \in \ker T$ such that $v_1 = v_2 + k$.
To show: (aba) $v_1 + K \subseteq v_2 + K$.
(abb) $v_2 + K \subseteq v_1 + K$.

(aba) Let $v \in v_1 + K$.
Then there exists $k_1 \in K$ such that $v = v_1 + k_1$.
Since $k + k_1 \in K$ then $v = v_2 + k + k_1 \in v_2 + K$.
So $v_1 + K \subseteq v_2 + K$.

(abb) Let $v \in v_2 + K$.
Then there exists $k_2 \in K$ such that $v = v_2 + k_2$.
Since $-k + k_2 \in K$ then $v = v_1 - k + k_2 \in v_1 + K$.
So $v_2 + K \subseteq v_1 + K$.
So $v_1 + K = v_2 + K$.

So $\hat{T}$ is injective.

(ac) To show: (aca) If $v_1 + K, v_2 + K \in V/K$ then $\hat{T}(v_1 + K) + \hat{T}(v_2 + K) = \hat{T}\big((v_1 + K) + (v_2 + K)\big)$.
(acb) If $c \in \mathbb{F}$ and $v + K \in V/K$ then $\hat{T}\big(c(v + K)\big) = c\hat{T}(v + K)$.

(aca) Let $v_1 + K, v_2 + K \in V/K$.
Since T is a homomorphism,

$$\begin{aligned}
\hat{T}(v_1 + K) + \hat{T}(v_2 + K) &= T(v_1) + T(v_2) \\
&= T(v_1 + v_2) \\
&= \hat{T}\big((v_1 + v_2) + K\big) \\
&= \hat{T}\big((v_1 + K) + (v_2 + K)\big).
\end{aligned}$$

(acb) Let $c \in \mathbb{F}$ and $v + K \in V/K$.
Since T is a homomorphism,

$$\begin{aligned}
\hat{T}\big(c(v + K)\big) &= \hat{T}(cv + K) \\
&= T(cv) \\
&= cT(v) \\
&= c\hat{T}(v + K).
\end{aligned}$$

So $\hat{T}$ is a linear transformation.

So $\hat{T}$ is a well defined injective linear transformation.

(b) To show: (ba) T' is a function.
(bb) T' is surjective.
(bc) T' is a linear transformation.

(ba) By the definition of $\operatorname{im} T$, if $v \in V$ then $T(v) \in \operatorname{im} T$.
Thus, since T is a function then T' is a function.

(bb) Since $\operatorname{im} T = \{T(v) \mid v \in V\}$ then if $w \in \operatorname{im} T$ then there exists $v \in V$ such that $T(v) = w$.
Since $T'(v) = T(v) = w$ then T' is surjective.

(bc) To show: (bca) If $v_1, v_2 \in V$ then $T'(v_1 + v_2) = T'(v_1) + T'(v_2)$.
(bcb) If $c \in F$ and $v \in V$ then $T'(cv) = cT'(v)$.

(bca) Let $v_1, v_2 \in V$.

Then, since T is a linear transformation,

$$T'(v_1 + v_2) = T(v_1 + v_2) = T(v_1) + T(v_2) = T'(v_1) + T'(v_2).$$

(bcb) Let $v_1, v_2 \in V$.
Then, since T is a linear transformation,

$$T'(cv) = T(cv) = cT(v) = cT'(v).$$

So T' is a linear transformation.

So T' is a well defined surjective linear transformation.

(c) Let $K = \ker T$.
By (a), the function

$$\begin{array}{rccc} \hat{T}\colon & V/K & \to & W \\ & v+K & \mapsto & T(v) \end{array}$$

is a well defined injective linear transformation.
By (b), the function

$$\begin{array}{rcccl} \hat{T}'\colon & V/K & \to & \mathrm{im}\hat{T} & \\ & v+K & \mapsto & \hat{T}(v+K) & = T(v) \end{array}$$

is a well defined surjective linear transformation.
To show: (ca) $\mathrm{im}\,\hat{T} = \mathrm{im}\,T$.
(cb) $\hat{T}'$ is injective.

(ca) To show: (caa) $\mathrm{im}\,\hat{T} \subseteq \mathrm{im}\,T$.
(cab) $\mathrm{im}\,T \subseteq \mathrm{im}\hat{T}$.

(caa) Let $w \in \mathrm{im}\hat{T}$.
Then there is some $v + K \in V/K$ such that $\hat{T}(v + K) = w$.
Let $v' \in v + K$.
Then there exists $k \in K$ such that $v' = v + k$.
Then, since T is a linear transformation and $T(k) = 0$,

$$\begin{aligned} T(v') &= T(v + k) \\ &= T(v) + T(k) \\ &= T(v) \\ &= \hat{T}(v + K) \\ &= w. \end{aligned}$$

So $w \in \mathrm{im}\,T$.
So $\mathrm{im}\,\hat{T} \subseteq \mathrm{im}\,T$.

(cab) Let $w \in \mathrm{im}T$.
Then there is some $v \in V$ such that $T(v) = w$.
So $\hat{T}(v + K) = T(v) = w$.
So $w \in \mathrm{im}\,\hat{T}$.
So $\mathrm{im}T \subseteq \mathrm{im}\,\hat{T}$.
So $\mathrm{im}T = \mathrm{im}\,\hat{T}$.

(cb) To show: If $\hat{T}'(v_1 + K) = \hat{T}'(v_2 + K)$ then $v_1 + K = v_2 + K$.
Assume $\hat{T}'(v_1 + K) = \hat{T}'(v_2 + K)$.
Then $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$.
Since $\hat{T}$ is injective then $v_1 + K = v_2 + K$.
So $\hat{T}'$ is injective.

Thus,

$$\begin{array}{rccc} \hat{T}': & V/K & \to & \mathrm{im}\hat{T} \\ & v+K & \mapsto & T(v) \end{array}$$

is a well defined bijective linear transformation.

□

Proposition F.2.7. — *Let V be an $\mathbb{F}$-vector space and let B be a subset of V. The following are equivalent:*

(a) B is a basis of V.
(b) B is a minimal element of $\{S \subseteq V \mid span_{\mathbb{F}}(S) = V\}$.
(c) B is a maximal element of $\{L \subseteq V \mid L \text{ is linearly independent}\}$.

(In (b) and (c) the ordering is by inclusion.)

Proof. —
(b) $\Rightarrow$ (a): Let $S \subseteq V$ such that $\mathrm{span}_{\mathbb{F}}(S) = V$.

To show: If S is minimal such that $\mathrm{span}_{\mathbb{F}}(V)$ then S is a basis.
To show: If S is minimal such that $\mathrm{span}_{\mathbb{F}}(V)$ then S is linearly independent.
Proof by contrapositive.
To show: If S is not linearly independent then S is not minimal such that $\mathrm{span}_{\mathbb{F}}(S) = V$.
Assume S is not linearly independent.
To show: There exists $s \in S$ such that $\mathrm{span}_{\mathbb{F}}(S - \{s\}) = V$.
Since S is linearly independent then there exist $k \in \mathbb{Z}_{>0}$ and $s_1, \ldots, s_k \in S$ and $c_1, \ldots, c_k \in \mathbb{F}$ and $i \in \{1, \ldots, k\}$ such that $c_1 s_1 + \cdots + c_k s_k = 0$ and $c_i \neq 0$.
Let $s = s_i$.
Using that $\mathbb{F}$ is a field and $c_i \neq 0$ then

$$\begin{aligned} s = s_i &= c_i^{-1}(c_1 s_1 + \ldots + c_{i-1}s_{i-1} + c_{i+1}s_{i+1} + \cdots + s_k c_k) \\ &= c_i^{-1}c_1 s_1 + \cdots + c_i^{-1}c_{i-1}s_{i-1} + c_i^{-1}c_{i+1}s_{i+1} + \cdots + c_i^{-1}c_k s_k. \end{aligned}$$

So $V = \mathrm{span}_{\mathbb{F}}(S) = \mathrm{span}_{\mathbb{F}}(S - \{s\})$.
So S is not minimal such that $\mathrm{span}_{\mathbb{F}}(S) = V$.

(a) $\Rightarrow$ (b): Proof by contrapositive.

To show: If B is not minimal element of $\{S \subseteq V \mid \mathrm{span}_{\mathbb{F}}(S) = V\}$ then B is not a basis of V.
Assume B is not minimal element of $\{S \subseteq V \mid \mathrm{span}_{\mathbb{F}}(S) = V\}$.
So there exists $b \in B$ such that $\mathrm{span}_{\mathbb{F}}(B - \{b\}) \neq V$.
To show: (aa) $B \in \{S \subseteq V \mid \mathrm{span}_{\mathbb{F}}(S) = V\}$.
(ab) If $b \in B$ then $B - \{b\} \notin \{S \subseteq V \mid \mathrm{span}_{\mathbb{F}}(S) = V\}$.

(aa) Since $\mathrm{span}_{\mathbb{F}}(B) = V$ then $B \in \{S \subseteq V \mid \mathrm{span}_{\mathbb{F}}(S) = V\}$.
(ab) Assume $b \in B$.
To show: $B - \{b\} \notin \{S \subseteq V \mid \mathrm{span}_{\mathbb{F}}(S) = V\}$.
To show: $\mathrm{span}_{\mathbb{F}}(B - \{b\}) \neq V$.
Since $\mathrm{span}_{\mathbb{F}}(B) = V$ then there exist $k \in \mathbb{Z}_{>0}$, $b_1, \ldots, b_k \in B$ and $c_1, \ldots, c_k \in \mathbb{F}$ such that $b = c_1 b_1 + \cdots c_k b_k$.
So $0 = c_1 b_1 + \cdots + c_k b_k + (-1)b$.

(a) $\Rightarrow$ (c): Assume B is a basis of V.

Since B is linearly independent then $B \in \{L \subseteq V \mid L \text{ is linearly independent}\}$.
To show: If $v \in V$ and $v \notin B$ then $B \cup \{v\}$ is not linearly independent.

Assume $v \in V$ and $v \notin B$.
Since $\mathrm{span}_{\mathbb{F}}(B) = V$ then there exists $k \in \mathbb{Z}_{>0}$ and $b_1, \ldots, b_k \in B$ and $c_1, \ldots, c_k \in \mathbb{F}$ such that $v = c_1 b_1 + \ldots + c_k b_k$.
So $0 = c_1 b_1 + \cdots + c_k b_k + (-1)v$.
So $B \cup \{v\}$ is not linearly independent.

(c) $\Rightarrow$ (a): Assume S is a maximal element of $\{L \subseteq V \mid L \text{ is linearly independent}\}$.
To show: $\mathrm{span}_{\mathbb{F}}(S) = V$.
To show: $V \subseteq \mathrm{span}_{\mathbb{F}}(S)$.
Let $v \in V$.
To show: $v \in \mathrm{span}_{\mathbb{F}}(S)$.
Case 1: $v \in S$. Then $v \in \mathrm{span}_{\mathbb{F}}(S)$.
Case 2: $v \notin S$.
Then $S \cup \{v\}$ is not linearly independent and S is linearly independent.
So there exist $k \in \mathbb{Z}_{>0}$ and $s_1, \ldots, s_k \in S$ and $c_0, c_1, \ldots, c_k \in \mathbb{F}$ such that

$$c_0 \neq 0 \qquad \text{and} \qquad c_0 v + c_1 s_1 + \cdots + c_k s_k = 0.$$

Since $\mathbb{F}$ is a field and $c_0 \neq 0$ then

$$v = (-c_0^{-1} c_1) s_1 + \cdots + (-c_0^{-1} c_k) s_k.$$

So $v \in \mathrm{span}_{\mathbb{F}}(S)$.
So $V \subseteq \mathrm{span}_{\mathbb{F}}(S)$ and $V = \mathrm{span}_{\mathbb{F}}(S)$.
So S is linearly independent and $\mathrm{span}_{\mathbb{F}}(S) = V$.
So S is a basis of V.

□

Theorem F.2.8. — *Let V be an $\mathbb{F}$-vector space. Then*
(a) V has a basis, and
(b) Any two bases of V have the same number of elements.

Proof. —
(a) The idea is to use Zorn's lemma on the set $\{L \subseteq V \mid L \text{ is linearly independent}\}$, ordered by inclusion. We will not prove Zorn's lemma, we will assume it. Zorn's lemma is equivalent to the axiom of choice. For a proof see Isaacs book [**Isa**, §11D].

> **Zorn's Lemma.** *If S is a nonempty poset such that every chain in S has an upper bound then S has a maximal element.*

Let $v \in V$ such that $v \neq 0$.
Then $L = \{v\}$ is linearly independent.
So $\{L \subseteq V \mid L \text{ is linearly independent}\}$ is not empty.
To show: If $\cdots \subseteq S_{k-1} \subseteq S_k \subseteq S_{k+1} \subseteq \cdots$ chain of linearly independent subsets of V then there exists a linearly independent set S that contains all the S_k.
Assume $\cdots \subseteq S_{k-1} \subseteq S_k \subseteq S_{k+1} \subseteq \cdots$ is a chain of linearly independent subsets of V.
Let $L = \bigcup_k S_k$.
To show L is linearly independent.
Assume $\ell \in \mathbb{Z}_{>0}$ and $s_1, \ldots, s_\ell \in L$.
Then there exists k such that $s_1, \ldots, s_\ell \in S_k$.
Since S_k is linearly independent then if $c_1, \ldots, c_\ell \in \mathbb{F}$ and $c_1 s_1 + \cdots + c_\ell s_\ell = 0$ then $c_1 = 0$, $c_2 = 0, \ldots, c_\ell = 0$.

So L is linearly independent.
So, if $\cdots \subseteq S_{k-1} \subseteq S_k \subseteq S_{k+1} \subseteq \cdots$ chain of linearly independent subsets of V then there exists a linearly independent set B that contains all the S_k.
Thus, by Zorn's lemma, $\{L \subseteq V \mid L \text{ is linearly independent}\}$ has a maximal element B.
By Proposition F.2.7, B is a basis of V.

(b) Let B and C be bases of V.

Case 1: V has a basis B with $\mathrm{Card}(B) < \infty$.
Let $b \in B$.
Then there exists $c \in C$ such that $c \notin \mathrm{span}_{\mathbb{F}}(B - \{b\})$.
Then $B_1 = (B - \{b\}) \cup \{c\}$ is a basis with the same cardinality as B.
Since B is finite then, by repeating this process, we can, after a finite number of steps, create a basis B' of V such that $B' \subseteq C$ and $\mathrm{Card}(B') = \mathrm{Card}(B)$.
Thus $\mathrm{Card}(B) = \mathrm{Card}(B') \leqslant \mathrm{Card}(C)$.
A similar argument with C in place of B gives that $\mathrm{Card}(B) \geqslant \mathrm{Card}(C)$.
So $\mathrm{Card}(B) = \mathrm{Card}(C)$.

Case 2: V has an infinite basis B.
Let C be a basis of V.
Define $P_{cb} \in \mathbb{F}$ for $c \in C$ and $b \in B$ by

$$b = \sum_{c \in C} P_{cb} c, \quad \text{and let} \qquad S_b = \{c \in C \mid P_{cb} \neq 0\} \quad \text{for } b \in B.$$

If $b \in B$ then S_b is a finite subset of C and

$$C = \bigcup_{b \in B} S_b, \qquad \text{since } C \text{ is a minimal spanning set.}$$

So $\mathrm{Card}(C) \leqslant \max\{\mathrm{Card}(S_b) \mid b \in B\} \leqslant \aleph_0 \mathrm{Card}(B)$.
A similar argument with B and C switched shows that $\mathrm{Card}(B) \leqslant \aleph_0 \mathrm{Card}(C)$.
So $\mathrm{Card}(C) \leqslant \aleph_0 \mathrm{Card}(B) = \mathrm{Card}(B) \leqslant \aleph_0 \mathrm{Card}(C) = \mathrm{Card}(C)$.
Since $\mathrm{Card}(C) \leqslant \mathrm{Card}(B) \leqslant \mathrm{Card}(C)$ then $\mathrm{Card}(C) = \mathrm{Card}(B)$.

$\square$