

Chapter 3. FIELDS AND VECTOR SPACES

§1P. Fields

(3.1.3) Proposition. *If $f: K \rightarrow F$ is a field homomorphism then f is injective.*

Proof.

To show: $f: K \rightarrow F$ is injective.

Assume $f: K \rightarrow F$ is a field homomorphism.

To show: If $x_1, x_2 \in K$ and $f(x_1) = f(x_2)$ then $x_1 = x_2$.

Assume $x_1, x_2 \in K$ and $f(x_1) = f(x_2)$.

To show: $x_1 = x_2$.

Proof by contradiction: Assume $x_1 \neq x_2$.

Let 0_K and 0_F be the additive identities in K and F respectively.

Let 1_K and 1_F be the multiplicative identities in K and F respectively.

Then $f(x_1) - f(x_2) = 0_F$ and $x_1 - x_2 \neq 0_K$.

Let $y = (x_1 - x_2)^{-1}$, which exists by property h) in the definition of a field.

Then, since $f: K \rightarrow F$ is a homomorphism and $f(x_1) - f(x_2) = 0_F$,

$$\begin{aligned} 1_F &= f(1_K) = f((x_1 - x_2)y) \\ &= f(x_1 - x_2)f(y) \\ &= (f(x_1) - f(x_2))f(y) \\ &= 0_F \cdot f(y) \\ &= 0_F. \end{aligned}$$

This is a contradiction to property g) in the definition of a field.

So $x_1 = x_2$.

So $f: K \rightarrow F$ is injective. \square

§2P. Vector Spaces

(3.2.4) Proposition. *Let V be a vector space over a field F 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 $v \in v' + W$ for some $v' \in V$.
 b) If $(v_1 + W) \cap (v_2 + W) \neq \emptyset$ then $v_1 + W = v_2 + W$.

a) Let $v \in V$.

Then, since $0 \in W$, $v = v + 0 \in v + W$.
 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

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

ba) Let $v \in v_1 + W$.

Then $v = v_1 + w$ for some $w \in W$.
 Then

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

since $w_2 - w_1 + w \in W$.
 So $v_1 + W \subseteq v_2 + W$.

bb) Let $v \in v_2 + W$.

Then $v = v_2 + w$ for some $w \in W$.
 Then

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

since $w_1 - w_2 + w \in W$.
 So $v_2 + W \subseteq v_1 + W$.

So $v_1 + W = v_2 + W$.

So the cosets of W in V partition V . \square

(3.2.5) Theorem. *Let W be a subgroup of a vector space V over a field F . Then W is a subspace of V if and only if V/W with operations given by*

$$\begin{aligned} (v_1 + W) + (v_2 + W) &= (v_1 + v_2) + W, \quad \text{and} \\ c(v + W) &= cv + W, \end{aligned}$$

is a vector space over F .

Proof.

\implies : 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) $((v_1 + W) + (v_2 + W)) + (v_3 + W) = (v_1 + W) + ((v_2 + W) + (v_3 + W))$
 for all $v_1 + W, v_2 + W, v_3 + W \in V/W$.

d) $(v_1 + W) + (v_2 + W) = (v_2 + W) + (v_1 + W)$ for all $v_1 + W, v_2 + W \in V/W$.

- e) $0 + W = W$ is the zero in V/W .
- 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 $c_1(c_2(v + W)) = (c_1c_2)(v + W)$.
- h) If $v + W \in V/W$ then $1(v + W) = v + W$.
- i) If $c \in F$ and $v_1 + W, v_2 + W \in V/W$,
then $c((v_1 + W) + (v_2 + W)) = c(v_1 + W) + c(v_2 + W)$.
- j) If $c_1, c_2 \in F$ and $v + W \in V/W$,
then $(c_1 + c_2)(v + W) = c_1(v + W) + c_2(v + W)$.

a) We want the operation on V/W given by

$$\begin{aligned} V/W \times V/W &\rightarrow V/W \\ (v_1 + W, v_2 + W) &\mapsto (v_1 + v_2) + W \end{aligned}$$

to be well defined.

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: $(v_1 + v_2) + W = (v_3 + v_4) + W$.

So we must 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) We know $v_1 = v_3 + 0 \in v_3 + W$ since $v_1 + W = v_3 + W$.

So $v_1 = v_3 + w_1$ for some $w_1 \in W$.

Similarly $v_2 = v_4 + w_2$ for some $w_2 \in W$.

Let $t \in (v_1 + v_2) + W$.

Then $t = v_1 + v_2 + w$ for some $w \in W$.

So

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

since addition is commutative.

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 $v_1 + W = v_3 + W$, we know $v_1 + w_1 = v_3$ for some $w_1 \in W$.

Since $v_2 + W = v_4 + W$, we know $v_2 + w_2 = v_4$ for some $w_2 \in W$.

Let $t \in (v_3 + v_4) + W$.

Then $t = v_3 + v_4 + w$ for some $w \in W$.

So

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

since addition is commutative.

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) We want the operation given by

$$\begin{aligned} F \times V/W &\rightarrow V/W \\ (c, v + W) &\mapsto cv + W \end{aligned}$$

to be well defined.

Let $(c_1, v_1 + W), (c_2, v_2 + W) \in (F \times V/W)$ 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 $v_1 + W = v_2 + W$, we know $v_1 = v_2 + w_1$ for some $w_1 \in W$.

Let $t \in c_1v_1 + W$.

Then $t = c_1v_1 + w$ for some $w \in W$. So

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

since $c_1 = c_2$.

Since W is a subspace, $c_2w_1 \in W$, 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 $v_1 + W = v_2 + W$, we know $v_2 = v_1 + w_2$ for some $w_2 \in W$.

Let $t \in c_2v_2 + W$.

Then $t = c_2v_2 + w$ for some $w \in W$. So

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

since $c_2 = c_1$.

Since W is a subspace, $c_1w_2 \in W$, 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 ,

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

for all $v_1 + W, v_2 + W, v_3 + W \in V/W$.

d) By the commutativity of addition in V and the definition of the operation in V/W ,

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

for all $v_1 + W, v_2 + W \in V/W$.

e) The coset $W = 0 + W$ is the zero in V/W since

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

for all $v + W \in V/W$.

f) Given any coset $v + W$, its additive inverse is $(-v) + W$ since

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

for all $v + W \in V/W$.

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

$$\begin{aligned}
c_1(c_2(v + W)) &= c_1(c_2v + W) \\
&= c_1(c_2v) + W \\
&= (c_1c_2)v + W \\
&= (c_1c_2)(v + W).
\end{aligned}$$

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 $c \in F$ and $v_1 + W, v_2 + W \in V/W$.
Then

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

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

$$\begin{aligned}
(c_1 + c_2)(v + W) &= ((c_1 + c_2)v) + W \\
&= (c_1v + c_2v) + W \\
&= (c_1v + W) + (c_2v + W) \\
&= c_1(v + W) + c_2(v + W).
\end{aligned}$$

So V/W is a vector space over F .

\Leftarrow : Assume W is a subgroup of V and V/W is a vector space over F with action given by

$$c(v + W) = cv + W.$$

To show: W is a subspace of V .

To show: If $c \in F$ 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 $k \in w + W$.

So $k = w + w_1$ for some $w_1 \in W$.

Since W is a subgroup, $w + w_1 \in W$.

So $w + W \subseteq W$.

b) Let $k \in W$.

Since $k - w \in W$, $k = w + (k - w) \in w + W$.

So $W \subseteq w + W$.

Now assume $c \in F$ 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 . \square

(3.2.8) Proposition. Let $T: V \rightarrow W$ 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 $T(v) + T(-v) = T(v + (-v)) = T(0_V) = 0_W$ and

$T(-v) + T(v) = T((-v) + v) = T(0_V) = 0_W$, then

$$-T(v) = T(-v). \quad \square$$

(3.2.10) Proposition. Let $T: V \rightarrow W$ be a linear transformation. Then

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

b) $\text{im } T$ is a subspace of W .

Proof.

a) By condition a) in the definition of linear transformation, T is a group homomorphism.

By Proposition 1.1.13 a), $\ker T$ is a subgroup of V .

To show: If $c \in F$ and $k \in \ker T$ then $ck \in \ker T$.

Assume $c \in F$ and $k \in \ker T$.

Then, by the definition of linear transformation,

$$T(ck) = cT(k) = c \cdot 0 = 0.$$

So $ck \in \ker T$.

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

b) By condition a) in the definition of linear transformation, T is a group homomorphism.

By Proposition 1.1.13 b), $\text{im } T$ is a subgroup of W .

To show: If $c \in F$ and $a \in \text{im } T$ then $ca \in \text{im } T$.

Assume $c \in F$ and $a \in \text{im } T$.

Then $a = T(v)$ for some $v \in V$.

By the definition of linear transformation,

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

So $ca \in \text{im } T$.

So $\text{im } T$ is a subspace of W . \square

(3.2.11) Proposition. Let $T: V \rightarrow W$ 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) $\text{im } T = W$ if and only if T is surjective.

Proof.

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

a) \implies : Assume $\ker T = (0_V)$.

To show: If $T(v_1) = T(v_2)$ then $v_1 = v_2$.

Assume $T(v_1) = T(v_2)$.

Then, by the fact that T is a homomorphism,

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

So $v_1 - v_2 \in \ker T$.

But $\ker T = (0_V)$.

So $v_1 - v_2 = 0_V$.

So $v_1 = v_2$.

So T is injective.

\Leftarrow : Assume T is injective.

To show: aa) $(0_V) \subseteq \ker T$.

ab) $\ker T \subseteq (0_V)$.

aa) Since $T(0_V) = 0_W$, $0_V \in \ker T$.

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, $k = 0_V$.

So $\ker T \subseteq (0_V)$.

So $\ker T = (0_V)$.

b) \implies : Assume $\text{im } T = W$.

To show: If $w \in W$ then there exists $v \in V$ such that $T(v) = w$.

Assume $w \in W$.

Then $w \in \text{im } T$.

So there is some $v \in V$ such that $T(v) = w$.

So T is surjective.

\Leftarrow : Assume T is surjective.

To show: ba) $\text{im } T \subseteq W$.

bb) $W \subseteq \text{im } T$.

ba) Let $x \in \text{im } T$.

Then $x = T(v)$ for some $v \in V$.

By the definition of T , $T(v) \in W$.

So $x \in W$.

So $\text{im } T \subseteq W$.

bb) Assume $x \in W$.

Since T is surjective there is a v such that $T(v) = x$.

So $x \in \text{im } T$.

So $W \subseteq \text{im } T$.

So $\text{im } T = W$. \square

(3.2.12) Theorem.

a) Let $T: V \rightarrow W$ be a linear transformation and let $K = \ker T$. Define

$$\begin{aligned} \hat{T}: V/\ker T &\rightarrow W \\ v + K &\mapsto T(v). \end{aligned}$$

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

b) Let $T: V \rightarrow W$ be a linear transformation and define

$$\begin{aligned} T': V &\rightarrow \text{im } T \\ v &\mapsto T(v). \end{aligned}$$

Then T' is a well defined surjective linear transformation.

c) If $T: V \rightarrow W$ is a linear transformation, then

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

where the isomorphism is a vector space isomorphism.

Proof.

a) To show: aa) \hat{T} is well defined.

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 $v_1 = v_2 + k$, for some $k \in K$.

To show: $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$, i.e.,

To show: $T(v_1) = T(v_2)$.

Since $K \in \ker T$, we have $T(k) = 0$ and so

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

$$\text{So } \hat{T}(v_1 + K) = \hat{T}(v_2 + K).$$

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 $v_1 - v_2 = k$, for some $k \in \ker T$.

So $v_1 = v_2 + k$, for some $k \in \ker T$.

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 $v = v_1 + k_1$, for some $k_1 \in K$.

So $v = v_2 + k + k_1 \in v_2 + K$, since $k + k_1 \in K$.

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

abb) Let $v \in v_2 + K$. Then $v = v_2 + k_2$, for some $k_2 \in K$.

So $v = v_1 - k + k_2 \in v_1 + K$ since $-k + k_2 \in K$.

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

$$\hat{T}(v_1 + K) + \hat{T}(v_2 + K) = \hat{T}((v_1 + K) + (v_2 + K)).$$

acb) If $c \in F$ and $v + K \in V/K$ then $\hat{T}(c(v + K)) = c\hat{T}(v + K)$.

aca) Let $v_1 + K, v_2 + K \in V/K$.

Since T is a homomorphism,

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

acb) Let $c \in F$ and $v + K \in V/K$.

Since T is a homomorphism,

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

So \hat{T} is a linear transformation.

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

b) To show: ba) T' is well defined.

bb) T' is surjective.

bc) T' is a linear transformation.

ba) and bb) are proved in Ex. 2.2.3 b), Part I.

bc) To show: bca) If $v_1, v_2 \in V$ then $T'(v_1 + v_2) = T'(v_1) + T'(v_2)$.

bc) 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,

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

bc) 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

$$\begin{aligned}\hat{T}: V/K &\rightarrow W \\ v + K &\mapsto T(v)\end{aligned}$$

is a well defined injective linear transformation.

By b), the function

$$\begin{aligned}\hat{T}': V/K &\rightarrow \text{im } \hat{T} \\ v + K &\mapsto \hat{T}(v + K) = T(v)\end{aligned}$$

is a well defined surjective linear transformation.

To show: ca) $\text{im } \hat{T} = \text{im } T$.

cb) \hat{T}' is injective.

ca) To show: caa) $\text{im } \hat{T} \subseteq \text{im } T$.

cab) $\text{im } T \subseteq \text{im } \hat{T}$.

caa) Let $w \in \text{im } \hat{T}$.

Then there is some $v + K \in V/K$ such that $\hat{T}(v + K) = w$.

Let $v' \in v + K$.

Then $v' = v + k$ for some $k \in K$.

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 $w \in \text{im } T$.

So $\text{im } \hat{T} \subseteq \text{im } T$.

cab) Let $w \in \text{im } T$.

Then there is some $v \in V$ such that $T(v) = w$.

So $\hat{T}(v + K) = T(v) = w$.

So $w \in \text{im } \hat{T}$.

So $\text{im } T \subseteq \text{im } \hat{T}$.

So $\text{im } T = \text{im } \hat{T}$.

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 $\hat{T}(v_1 + K) = \hat{T}(v_2 + K)$.

Then, since \hat{T} is injective, $v_1 + K = v_2 + K$.

So \hat{T}' is injective.

Thus we have

$$\begin{aligned}\hat{T}': V/K &\rightarrow \text{im } \hat{T} \\ v + K &\mapsto T(v)\end{aligned}$$

is a well defined bijective linear transformation. \square