Some Named Theorems

♡

31. lokakuuta 2018

Theorem 1 (Subspace Theorem)
Let V be a vector space over F and WV a subset, $W \neq \varnothing$. Then, the following are equivalent:

1. W is a subspace of V.
2. W is closed under the $+$ and $\cdot$ of V.
3. If $w_1, w_2 \in W$ and $\alpha \in F$, then $\alpha w_1 + w_2 \in W$.

Todistus. $(1 \implies 2)$: True from definition.

$(2 \implies 1)$: Since all the axioms for V hold for W, the only real thing we need to show is that $0_W = 0_V$. To do that, let $w \in W$. By (2), $(-1)w \in W$. Hence, by (2), $(-1)w + w \in W$. Thus, $0_V \in W$, since $w \in V$. As $v + 0_V = v = 0_V + v$ $\forall v \in V$, it is rue for any $w \in W$. So, $0_V = 0_W$.

$(2 \implies 3)$: If $\alpha \in F$ and $w_1, w_2 \in W$, then by (2), $\alpha w_1 \in W$ (and $w_2 \in W$) so, by (2), $\alpha w_1 + w_2 \in W$ as well.

$(3 \implies 2)$: Let $\alpha \in F$, $w_1, w_2 \in W$. We want to show that $\alpha w_1, w_1 + w_2 \in W$.

$0_V = w_1 + (-1)w_1 \in V$, hence W by assumption. It follows that $0_V = 0_W \in W$. Therefore,

$$w_1 + w_2 = 1w_1 + w_2 \in W \qquad \text{(by (3))}$$

$$\alpha w_1 = \alpha w_1 + 0_W \in W \qquad \text{(by (3))}$$

Thus, (2) holds. □

Theorem 2 (Toss-In)
Let V be a vector space over F, and $\varnothing \neq S \subset V$ with S linearly independent.

Suppose $v \in V$ is not in the span of S. Then $S \cup \{v\}$ is linearly independent.

Todistus. Suppose $S \cup \{v\}$ is linearly dependent. Then $\exists v_1, \ldots, v_n \in S$ and $\alpha, \alpha_1, \ldots, \alpha_n \in F$ not all zero such that

$$0 = \alpha_1 v_1 + \ldots + \alpha_n v_n + \alpha v \tag{1}$$

Case I ($\alpha = 0$): In this case, $0 = \alpha_1 v_1 + \ldots + \alpha_n v_n$ with some $\alpha_i \neq 0$, contradicting the linear independence of S.

Case II ($\alpha \neq 0$): So, $\alpha^{-1} \in F$. Then, by rearranging (1) and dividing by the inverse, we get

$$\begin{aligned} \alpha v &= -\alpha_1 v_1 - \ldots - \alpha_n v_n \\ v &= -\alpha^{-1}\alpha_1 v_1 - \ldots - \alpha^{-1}\alpha_n v_n \in \mathrm{Span}(v_1, \ldots, v_n) \end{aligned}$$

which is a contradiction. got 'em! □

Theorem 3 (Replacement Theorem)

Let V be a finite-dimensional vector space over F with basis $\mathscr{B} = \{v_1, \ldots, v_n\}$. Let $v \in V$, with $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$, $\alpha_i \in F$ where some α_i is nonzero. Then $\{v_1, \ldots, v_{i-1}, v, v_{i+1}, \ldots, v_n\}$ is a basis for V.

Todistus. By change of notation, we may assume that $\alpha_1 \neq 0$[1]. Thus, α_1^{-1} exists[2]. Thus,

$$\begin{aligned} v &= \alpha_1 v_1 + \ldots + \alpha_n v_n \implies \\ v_1 &= \alpha_1^{-1} v - \alpha_1^{-1}\alpha_2 v_2 - \ldots - \alpha_1^{-1}\alpha_n v_n \in \mathrm{Span}(v, v_2, \ldots, v_n) \end{aligned}$$

By the **Important Exercise**, we have $\mathrm{Span}(v_1, \ldots, v_n) = \mathrm{Span}(v, v_1, \ldots, v_n) = \mathrm{Span}(v, v_2, \ldots, v_n)$, i.e., $\{v, v_2, \ldots, v_n\}$ spans V.

Suffices to show that $\{v, v_2, \ldots, v_n\}$ is linearly independent[3]. For the sake of contradiction, assume the set isn't linearly independent. Then, $\exists \beta_1, \ldots, \beta_n$ not all zero such that

$$\beta v + \beta_2 v_2 + \ldots + \beta_n v_n = 0$$

[1] All this means is that since some a_i is nonzero, we can, without loss of generality, assume it's the first one.

[2] Because it's a nonzero element of a field F.

[3] We've already shown that it spans, so this is the only remaining condition for it to be a basis.

Case I ($\beta = 0$): Then $0 = \beta_2 v_2 + \ldots + \beta_n v_n$ with not all $\beta_i = 0$, i.e., $\{v_2, \ldots, v_n\}$ is linearly dependent, hence $\mathscr{B}$ is linearly dependent. This is a contradiction!

Case II ($\beta \neq 0$): Since $\beta \neq 0$, β^{-1} is alive and kicking. So,

$$\begin{aligned} v &= -\beta^{-1}\beta_2 v_2 - \ldots - \beta^{-1}\beta_n v_n \\ &= 0 \cdot v_1 - \beta^{-1}\beta_2 v_2 - \ldots - \beta^{-1}\beta_n v_n \end{aligned}$$

Recall from above that

$$v = \alpha_1 v_1 + \ldots + \alpha_n v_n$$

Setting these two things equal to each other, we get

$$\alpha_1 v_1 + \ldots + \alpha_n v_n = 0 = 0 \cdot v_1 - \beta^{-1}\beta_2 v_2 - \ldots - \beta^{-1}\beta_n v_n$$

However, by the **Coördinate Theorem**, in a basis, coördinates are unique! But we said at the beginning that $\alpha_1 \neq 0$, so this is a contradiction[4]. got 'em!

□

Note 4

On an intuitive level, the reason we split the proof into two cases is because we always want β to have an inverse. For that to happen, we quickly show that the case where it doesn't have an inverse (i.e., equals zero) doesn't work.

More concisely,

Note 5

If it's non-zero, then it has an inverse, so divide by it.

Theorem 6 (Main Theorem)

Suppose V is a finite-dimensional vector space over F, and $V = \text{Span}(v_1, \ldots, v_n)$. Then any linearly independent subset in V has at most n elements; i.e., if S is a linearly independent subset, $|S| \leq n$.

[4]Right? cause $\alpha_1 v_1 = 0 \cdot v_1$ by the Coordinate theorem, but we said that $\alpha_1 \neq 0$.

Todistus. By the **Toss-Out Theorem**, $\{v_1, \ldots, v_n\}$ is a basis. In particular, we may assume $\{v_1, \ldots, v_n\}$ is a basis to show $|S| \leq n$.

Suffices to show that if $S = \{w_1, \ldots, w_m\}$ is linearly independent in V, then $m \leq n$. Assume $m < n$.

Claim 6.1. After changes of notation (on the v_i's) if necessary, then for each $k < n$, $\{w_1, \ldots, w_k, v_{k+1}, \ldots, v_n\}$ is linearly independent.

Clearly, the claim implies the proof of the theorem. To see why, apply the claim to $n = k$. Then, $\{w_1, \ldots, w_n\}$ is a basis. Then, $w_{n+1} \in \mathrm{Span}(w_1, \ldots, w_n) = V$, so $\{w_1, \ldots, w_{n+1}\}$ is linearly dependent. Thus, proving the claim will show the theorem.

Proof of claim. We prove this by induction ok k.

Let $k = 1$. Then $0 \neq w_1 \in \mathrm{Span}(v_1, v_2, \ldots, v_n)$.

$0 \neq w_1 = \alpha_1 v_1 + \ldots + \alpha_n v_n$, not all $\alpha_i = 0$. After changing notation, we can assume that $\alpha_1 \neq 0$, so $\{w_1, v_2, \ldots, v_n\}$ is a basis by the **Replacement Theorem** (3).

Inductive step: Assume that for some k, $k < n$, $\{w_1, \ldots, w_k, v_{k+1}, \ldots, v_n\}$ is a basis. We want to show that $\{w_1, \ldots, w_{k+1}, v_{k+2}, \ldots, v_n\}$ is a basis (up to changing notation). We have that $0 \neq w_{k+1} = \alpha_1 w_1 + \ldots + \alpha_k w_k + \beta_{k+1} v_{k+1} + \ldots + \beta n v_n$, where $\alpha_i, \beta_i \in F$ are not all zero.

Case I ($\beta_i = 0\ \forall i$): Then $w_{k+1} \in \mathrm{Span}(w_1, \ldots, w_k)$, contradicting the linear independence of the set $\{w_1, \ldots, w_m\}$.

Case II ($\exists \beta_j \neq 0$): Changing notation, we may assume that $\beta_{k+1} \neq 0$. Hence, $\{w_1, \ldots, w_{k+1}, v_{k+2}, \ldots, v_n\}$ is a basis by the **Replacement Theorem** (3). □

□

Corollary 7

Let V be a finite-dimensional vector space over F with bases $\mathscr{B}_1$, $\mathscr{B}_2$. Then $|\mathscr{B}_1| = |\mathscr{B}_2|$. We call $|\mathscr{B}_1|$ the **dimension** of V and write $\dim_F V$ or $\dim V$.

Todistus. By definition, there exists a basis $\mathscr{C}$ for V such that $|\mathscr{C}| < \infty$. If $\mathscr{B}$ is another basis, then $|\mathscr{B}| \leq |\mathscr{C}|$ by the **Main Theorem** (6). Also, $|\mathscr{C}| \leq |\mathscr{B}|$. Thus, $|\mathscr{B}| = |\mathscr{C}|$. □

Corollary 8

Let V be a finite-dimensional vector space over F of dimension $n > 0$, and $0 \neq S \subset V$ a subset. Then

a) If $|S| > n$, then S is linearly dependent.

b) If $|S| < n$, then S does not span V.

Todistus. The theorem tells us that the maximal linearly independent set in V is a basis. By the **Toss-Out Theorem**, a minimal spanning set of V is a basis. $\square$

Theorem 9 (Extension Theorem)

Let V be a finite-dimensional vector space over F, and suppose $W \subset V$ is a subspace. Suppose $S \subset W$ is a linearly independent subset. Then S is finite, and part of a basis for W.

Todistus. We have $|S| \leq \dim V < \infty$ by the **Main Theorem**. If $W = \mathrm{Span}(S)$, W is a basis by definition, so we're done. If not, $\exists w_1 \in W \setminus \mathrm{Span}(S)$. By the **Toss-In Theorem**, $\exists w_1 \in W$ such that $S \cup \{w_1\}$ is linearly independent. Call this set $S_1 := S \cup \{w_1\}$.

Clearly, $|S_1| = |S| + 1$ since we just added another vector, and $\mathrm{Span}(S) < \mathrm{Span}(S_1)$.

If $\mathrm{Span}(S_1) < W$, then $\exists w_2 \in W \ni S_2 = S_1 \cup \{w_2\}$is linearly independent, by the **Toss-In Theorem**. $|S_2| = |S| + 2$.

Continue tossing in linearly independent vectors and, since W is finite, eventually $\mathrm{Span}(S_n) = W$. $\square$

Corollary 10

Let V be a finite-dimensional vector space over F, and $S \subset V$ a linearly independent set. Then S can be extended to a basis of V.

Corollary 11

Let V be a finite-dimensional vector space over F and $W \subset V$ a subspace, then W is a finite dimensional vector space over F and $\dim W \leq \dim V$, with equality holding if and only if $V = W$.

Theorem 12 (Counting Theorem)
Let V be a vector space over F, $W_1, W_2 \subset V$ be finite-dimensional subspaces. Then,

1. $W_1 \cap W_2$ is a finite-dimensional vector space.
2. $W_1 + W_2$ is a finite-dimensional vector space.
3. $\dim W_1 + \dim W_2 = \dim (W_1 + W_2) + \dim (W_1 \cap W_2)$.

Todistus. (1, 2): Let $\mathscr{B}_i$ be a basis for W_i, $i \in \{1, 2\}$. Then $|\mathscr{B}_1 \cup \mathscr{B}_2| \leq |\mathscr{B}_1| + |\mathscr{B}_2| < \infty$.

Hence, $\text{Span}(\mathscr{B}_1 \cup \mathscr{B}_2)$ is a finite-dimensional vector space by the **Toss-Out Theorem**. Also, $\text{Span}(\mathscr{B}_1 \cup \mathscr{B}_2) = W_1 + W_2$, so $W_1 + W_2$ is a finite-dimensional vector space.

(3): Let $\mathscr{B} = \{v_1, \ldots, v_n\}$ be a basis for $W_1 \cap W_2$. By the **Extension Theorem**, this extends to bases

$$\mathscr{C}_1 = \{v_1, \ldots, v_n, y_1, \ldots, y_m\}$$

for W_1 and

$$\mathscr{C}_2 = \{v_1, \ldots, v_n, z_1, \ldots, z_m\}$$

for W_2.

Claim 12.1. $\mathscr{C} = \{v_1, \ldots, v_n, y_1, \ldots, y_m, z_1, \ldots, z_r\}$ is a basis for $W_1 + W_2$.

Remark 13. If we show this claim, we're done.

Proof of claim. ($\mathscr{C}$ spans $W_1 + W_2$): This is true, since $W_1 + W_2 = \text{Span}(\mathscr{C}_1 \cup \mathscr{C}_2) = \text{Span}(\mathscr{C})$.

($\mathscr{C}$ linearly independent): For the sake of contradiction, assume it isn't. Then there exist $\alpha_i, \beta_i, \gamma_i \in F$, not all zero, such that

$$\alpha_1 v_1 + \ldots + \alpha_n v_n + \beta_1 y_1 + \ldots + \beta_m y_m + \gamma_1 z_1 + \ldots + \gamma_r z_r = 0$$

Case I ($\gamma_i = 0\ \forall i$). This can't be true, since it would contradict the linear independence of C_1.

Case II ($\exists i \ni \gamma_i \neq 0$): Without loss of generality, we can say that $\gamma_1 \neq 0$. Note that

$$0 \neq z = \gamma_1 z_1 + \ldots + \gamma_r z_r \in \operatorname{Span}(\mathscr{C}_2) = W_2 \tag{2}$$

but also

$$z = -\alpha_1 v_1 - \ldots - \alpha_n v_n - \beta_1 y_1 - \ldots - \beta_m y_m \tag{3}$$

Setting (2) and (3) equal to each other, we get

$$\gamma_1 z_1 + \ldots + \gamma_r z_r = z = -\alpha_1 v_1 - \ldots - \alpha_n v_n - \beta_1 y_1 - \ldots - \beta_m y_m$$

Hence $\exists \delta_1, \ldots, \delta_n \ni (0 \neq)\ z = \delta_1 v_1 + \ldots + \delta_n v_n$.
Thus, we get that

$$\delta_1 v_1 + \ldots + \delta_n v_n + 0 \cdot z_1 + \ldots + 0 \cdot z_r = \gamma_1 z_1 + \ldots + \gamma_r z_r \neq 0$$

But $\gamma_1 \neq 0$, so by the **Coördinate Theorem** we get a contradiction, because $\mathscr{C}_2$ is a basis! □

□

Corollary 14

If V is a finite-dimensional vector space over F, $W_1, W_2 \subset V$ finite-dimensional subspaces such that $W_1 \cap W_2 = 0$, then $\dim(W_1 + W_2) = \dim W_1 + \dim W_2$.

Theorem 15 (Dimension Theorem)

Let $T : V \longrightarrow W$ be linear with V a finite-dimensional vector space over F. Then

1. $\ker T \subset V$ and $\operatorname{im} T \subset W$ are finite-dimensional subspaces.
2. $\dim V = \dim \ker T + \dim \operatorname{im} T$.

Todistus. Let $n = \dim V$.

We have $\ker T \subset V$ and $\operatorname{im} T \subset W$ are subspaces. In particular, $\ker T \subset V$ is a finite-dimensional subspace. Let $\mathscr{B}_0 = \{v_1, \ldots, v_m\}$ be a basis for $\ker T$.

Extend $\mathscr{B}_0$ to $\mathscr{B} = \{v_1, \ldots, v_n\}$, a basis for V, using the **Extension Theorem**. It suffices to show that $\mathscr{C} = \{Tv_{m+1}, \ldots, Tv_n\}$ is a basis for $\operatorname{im} T$[5]. So, let's show it!

($\mathscr{C}$ spans $\operatorname{im} T$): Let $w \in \operatorname{im} T$, and $v \in V$ satisfy $Tv = w$. As $\mathscr{B}$ is a basis for V, $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$ for some $\alpha_i \in F$. Thus,

[5] Why? Make sure you understand this.

$$\begin{aligned} w &= Tv \\ &= \alpha_1 Tv_1 + \ldots + \alpha_m Tv_m + \alpha_{m+1} Tv_{m+1} + \ldots + \alpha_n Tv_n \\ &= \alpha_1 \cdot 0 + \ldots + \alpha_m \cdot 0 + \alpha_{m+1} Tv_{m+1} + \ldots + \alpha_n Tv_n \in \operatorname{Span}(\mathscr{C}) \end{aligned}$$

($\mathscr{C}$ is linearly independent): Observe that

$$\alpha_{m+1} Tv_{m+1} + \ldots + \alpha_n Tv_n = 0$$

for $\alpha_i \in F$, $i > m+1$.

By linearity,

$$T(0_V) = T(\alpha_{m+1} Tv_{m+1} + \ldots + \alpha_n Tv_n) = 0_W$$

so $\alpha_{m+1} Tv_{m+1} + \ldots + \alpha_n Tv_n \in \ker T$. As $\mathscr{B}_0$ is a basis for $\ker_T$, we know that

$$\alpha_{m+1} v_{m+1} + \ldots + \alpha_n v_n = \beta_1 v_1 + \ldots + \beta_m v_m$$

for some $\beta_i \in F$. Thus,

$$-\beta_1 v_1 - \ldots - \beta_m v_m + \alpha_{m+1} v_{m+1} + \ldots + \alpha_n v_n = 0$$

Since $\mathscr{B}$ is linearly independent, $\beta_j = \alpha_i = 0 \; \forall i, j$. □

Theorem 16 (Monomorphism Theorem)

Let $T : V \longrightarrow W$ be linear. Then the following are equivalent:

1. T is a monomorphism (i.e., T is one-to-one),
2. T takes linearly independent sets to linearly independent sets,
3. $\ker T = 0$,
4. $\dim \ker T = 0$.

Todistus. ($1 \implies 2$): To show 2, it suffices to show T takes finitely many distinct linearly independent elements to linearly independent elements. Let $v_1, \ldots, v_n$ in V be linearly independent, $\alpha_1, \ldots, \alpha_n \in F$. Since T is one-to-one and linear, $0_W = T(0_V) \implies 0 = \alpha_1 v_1 + \ldots + \alpha_n v_n$. By linearity, it follows that $\alpha_1 Tv_1 + \ldots + \alpha_n Tv_n = 0_W$, so $\alpha_i = 0 \; \forall i$, since $\{v_1, \ldots, v_n\}$ are linearly independent.

($2 \implies 3$): Let $v \in V$, with $v \in \ker T$, so $T(v) = 0_W = T(0_V)$.

If $v \neq 0$, $\{v\}$ is linearly independent, as $\alpha v = 0 \implies \alpha = 0$when $v \neq 0$. So $T(v) \neq 0$ by (2). Thus, $\ker T$ must equal 0.

$(3 \iff 4)$: By definition.

$(3 \implies 1): Suppose T(v_1) = T(v_2)$, for some $v_1, v_2 \in V$. So $0 = T(v_1 - T(v_2) = T(v_1 - v_2) \implies v_1 - v_2 \in \ker T \implies v_1 = v_2$. □

Note 17

This theorem states that $\ker T$ is the **obstruction** of T being a monomorphism.

Note 18

Recall that $W \cong W$ means only that $\exists T : V \longrightarrow W$ an isomorphism, **not** that all linear $S : V \longrightarrow W$ are isomorphisms.

Theorem 19 (Isomorphism Theorem)

Suppose $T : V \longrightarrow W$ with V, W finite-dimensional vector spaces of the same dimension over F; i.e., $\dim V = \dim W < \infty$.

Then, the following are equivalent:

1. T is an isomorphism,
2. T is a monomorphism,
3. T is an epimorphism,
4. If $\mathscr{B} = \{v_1, \ldots, v_n\}$ is a basis for V, then $\{Tv_1, \ldots, Tv_n\}$ is a basis for W; i.e., T takes bases of V to bases of W,
5. $\exists$ a basis for V such that T takes it to a basis for W.

Note 20

$\dim V = \dim W < \infty$ is a very, very, very, very, very strong condition!

Todistus. $(1 \implies 2)$: ✓

$(2 \iff 3)$: By the **Dimension Theorem**, $\dim W = \dim V = \dim \ker T + \dim \operatorname{im} T < \infty$.

T is onto means that $W = \operatorname{im} T \iff \dim \operatorname{im} T = \dim W \iff \ker T = 0 \iff T$ is one-to-one[6].

[6]We used the corollary to the **Extension Theorem** in the second if and only if.

(2 and 3 $\implies$ 1): ✓

(2 $\implies$ 4): By the **Monomorphism Theorem**, $\{Tv_1, \ldots, Tv_n\}$ is linearly independent where $n = \dim W$, so it is a basis since it spans (by the Extension Theorem, or the Main Theorem, or whatever you want, really.)

(4 $\implies$ 5): ✓

(5 $\implies$ 3): If $\mathscr{B} = \{v_1, \ldots, v_n\}$ is a basis, $\{Tv_1, \ldots, Tv_n\}$ is a basis. Hence, it spans. Thus, T is onto and therefore an epimorphism. □

Theorem 21 (Universal Property of Vector Spaces)

Let V be a finite-dimensional vector space over F, $\mathscr{B} = \{v_1, \ldots, v_n\}$ a basis for V, W a vector space over F. Suppose $w_1, \ldots, w_n \in W$, not necessarily distinct. Then $\exists!\, T : V \longrightarrow W$ linear such that $Tv_i = w_i$, $i - \{1, \ldots, n\}$.

In other words, let $\mathscr{B}$ a basis, $B \overset{\text{inc}}{\hookrightarrow} V$. Then given a diagram

$$\begin{array}{ccc} \mathscr{B} & \overset{\text{inc}}{\hookrightarrow} & V \\ & {\scriptstyle f}\searrow & \\ & & W \end{array}$$

then $\exists!\, T : V \longrightarrow W$ linear such that

$$\begin{array}{ccc} \mathscr{B} & \overset{\text{inc}}{\hookrightarrow} & V \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle T} \\ & & W \end{array}$$

commutes.

Todistus. Here ♡ □