

MATH 110 Lecture Notes 7

GSI Carter

July 2, 2008

1 Invertibility

Let $T : V \rightarrow W$ be a linear transformation. Then a function $U : W \rightarrow V$ is said to be an inverse of T if UT is the identity function on V and TU is the identity function on W . If such an inverse exists, it is unique and is denoted T^{-1} .

If T and U are invertible, then:

- $(UT)^{-1} = T^{-1}U^{-1}$
- $(T^{-1})^{-1} = T$

Theorem. Let $T : V \rightarrow W$ be an invertible linear transformation. Then $T^{-1} : W \rightarrow V$ is linear.

Similarly, a matrix A is invertible if and only if there exists another matrix B such that $AB = BA = I$. In this case, we say $B = A^{-1}$.

Only square matrices can possibly be invertible, and the $n \times n$ matrix A is invertible if and only if the linear transformation $L_A : F^n \rightarrow F^n$ defined by $L_A(v) = Av$ is an invertible linear transformation.

2 Isomorphisms

An invertible linear transformation is also called an *isomorphism of vector spaces*. We say that the vector spaces V and W are isomorphic if there is an isomorphism between them.

Example. Let $T : F^2 \rightarrow P_1(F)$ be defined by $T(a, b) = a + bx$. Then T is one-to-one and onto, so it is an isomorphism. Therefore F^2 and $P_1(F)$ are isomorphic vector spaces.

Theorem. Let V and W be vector spaces over a field F . Then V and W are isomorphic if and only if $\dim V = \dim W$.

Proof. In order for the statement to generalize to infinite-dimensional vector spaces, we will interpret the statement “ $\dim V = \dim W$ ” as meaning that there exist bases for V and W which can be put in one-to-one correspondence with one another. That is, there exist a basis α of V , a basis β of W , and a function $\phi : \alpha \rightarrow \beta$ which is both one-to-one and onto, and hence invertible.

First, suppose there exists such an α , β , and ϕ . Then we can define a linear transformation $T : V \rightarrow W$ by deciding where T should send each element of α . For each $v \in \alpha$, we will let $T(v) = \phi(v)$. Since ϕ is onto, $T(\alpha) = \beta$. Therefore

$$R(T) = \text{span}(\beta) = W.$$

Suppose there exist $v_1, \dots, v_n \in \alpha$ and $a_1, \dots, a_n \in F$ such that

$$T(a_1v_1 + \dots + a_nv_n) = 0.$$

By linearity,

$$0 = a_1T(v_1) + \dots + a_nT(v_n) = a_1\phi(v_1) + \dots + a_n\phi(v_n).$$

Since ϕ is one-to-one, the vectors $\phi(v_1), \dots, \phi(v_n)$ are all distinct elements of β . Then since β is linearly independent, $a_i = 0$ for all i . Therefore T is one-to-one.

Conversely, suppose $T : V \rightarrow W$ is an isomorphism. Let α be a basis for V , let $\beta = T(\alpha)$, and let $\phi = T|_{\alpha}$. We must show that β is a basis for W and that ϕ is one-to-one (ϕ is onto by construction). First, since α generates V , $\beta = T(\alpha)$ generates $R(T)$, which is W since T is onto. Given $v, w \in \alpha$, if $\phi(v) = \phi(w)$, then $T(v - w) = 0$. Since T is one-to-one, this implies $v = w$. Therefore ϕ is one-to-one. To show that β is linearly independent, suppose there exist $T(v_1), T(v_2), \dots, T(v_n) \in \beta$ and $a_1, a_2, \dots, a_n \in F$ such that

$$a_1T(v_1) + a_2T(v_2) + \dots + a_nT(v_n) = 0.$$

Then

$$T(a_1v_1 + a_2v_2 + \dots + a_nv_n) = 0.$$

Since T is one-to-one,

$$a_1v_1 + a_2v_2 + \dots + a_nv_n = 0.$$

Since α is linearly independent, this implies $a_1 = a_2 = \dots = a_n = 0$, which completes the proof.

Exercise 2.4.2. Determine whether the following linear transformations are invertible.

Division Algorithm for Polynomials. Let F be a field, and let $a, b \in P(F)$ with $b \neq 0$. Then there exist $q, r \in P(F)$ such that $\deg r < \deg b$ (if b is a constant, this means $r = 0$) and $a(x) = q(x)b(x) + r(x)$.

Proof. It is clear that if we remove the condition that $\deg r < \deg b$, then we can choose such a q and r (for example, $q = 0$ and $r = a$). We must show that among the choices for q and r satisfying $a = qb + r$, there is at least one with $\deg r < \deg b$.

Suppose all such choices of q and r have $\deg r \geq \deg b$. Then let q and r be polynomials satisfying $a = qb + r$ with r of smallest possible degree. Then

$$r(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_0$$

for some n , where $\alpha_0, \dots, \alpha_n \in F$ and $\alpha_n \neq 0$, and

$$b(x) = \beta_m x^m + \beta_{m-1} x^{m-1} + \dots + \beta_0$$

for some $m \leq n$, where $\beta_0, \dots, \beta_m \in F$ and $\beta_0 \neq 0$. Then

$$a(x) = q(x)b(x) + r(x) = \left[q(x) + \frac{\alpha_n}{\beta_m} x^{n-m} \right] b(x) + \left[r(x) - \frac{\alpha_n}{\beta_m} b(x)x^{n-m} \right].$$

Since $q(x) + \frac{\alpha_n}{\beta_m} x^{n-m} \in P(F)$ and $\deg \left(r(x) - \frac{\alpha_n}{\beta_m} b(x)x^{n-m} \right) < n$, this is a contradiction, which completes the proof.

Corollary. Let $f(x)$ be a polynomial with a root $\alpha \in F$. Then $(x - \alpha)$ is a factor of $f(x)$.

Proof. We can write $f(x) = q(x)(x - \alpha) + r(x)$, where $q(x) \in P(F)$ and $\deg r(x) < 1$. Therefore $r(x)$ is a constant $r \in F$. Then evaluating both sides at α , we get

$$r = q(\alpha)(\alpha - \alpha) + r = f(\alpha) = 0.$$

Therefore $f(x) = q(x)(x - \alpha)$.

Exercise 2.4.22. Let c_0, c_1, \dots, c_n be distinct scalars from an infinite field F . Define $T : P_n(F) \rightarrow F^{n+1}$ by $T(f) = (f(c_0), f(c_1), \dots, f(c_n))$. Prove that T is an isomorphism. Hint: Check that T is one-to-one using the above corollary, and compare dimensions.