Dimension of a span of matrix powers

Let $A \in M^C_{n\times n}$ be a square matrix with a minimal polynomial of degree k. What would be $\dim(\text{Span}\{I, A, A^2, A^3, \dots\})$? I think it's k but I'm not sure exactly how to prove it.

(linear-algebra)

edited Nov 5 '11 at 18:33
Bill Cook
8,405 6 23

asked Nov 5 '11 at 18:17
dan
36 4

Wouldn't it be nice if the span you are interested in were isomorphic to $\mathbb{C}[X]/(minimal\ polynomial)$? Hmmm, let me see, how would we prove that... – Georges Elencwajg Nov 5 '11 at 18:27

feedback

2 Answers

Suppose that $c_0 I_n + c_1 A + c_2 A^2 + \cdots + c_{k-1} A^{k-1} = 0$. Then if $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{k-1} x^{k-1}$, we have $f(A) = 0$. But the minimal polynomial has degree $k > k-1$. Therefore, $f(x) = 0$ and so $c_0 = \cdots = c_{k-1} = 0$. This shows that the set $\{I_n, A, A^2, \cdots, A^{k-1}\}$ is linearly independent.

Now suppose A has minimal polynomial $g(x) = a_0 + a_1 x + \cdots + a_k x^k$. This means $A^k = a_k^{-1}(a_0 I_n + \cdots + a_{k-1} A^{k-1})$ and in general $A^m = a_k^{-1}(a_0 I_n + \cdots + a_{k-1} A^{k-1})A^{m-k}$ for all $m \geq k$. Thus powers of A bigger than A^{k-1} can always be replaced with lower powers. Thus $\{I_n, A, A^2, \cdots, A^{k-1}\}$ spans as well.

Therefore, the dimension of the span of powers of A is exactly the degree of its minimal polynomial.

Edit: To elaborate on the spanning arugment.

Suppose that $A^n = c_0 I_n + c_1 A + \cdots + c_\ell A^\ell$ with $c_\ell \neq 0$ and ℓ as small as possible. Then if $\ell \geq k$, we can write $A^\ell = a_k^{-1}(a_0 I_n + \cdots + a_{k-1} A^{k-1})A^{\ell-k}$ and so $A^n = c_0 I_n + c_1 A + \cdots + c_{\ell-1} A^{\ell-1} + c_\ell a_k^{-1}(a_0 I_n + \cdots + a_{k-1} A^{k-1})A^{\ell-k}$. We have expressed A^n using $I_n, A, \dots, A^{\ell-1}$ so ℓ was not minimal (contradiction). Thus $\ell < k$.

edited Nov 5 '11 at 18:39

answered Nov 5 '11 at 18:32
Bill Cook
8,405 6 23

feedback

It cannot be *more than k*, because the minimal polynomial allows us to write every A^n with

$n \geq k$ as a linear combination of lower powers. On the other hand, it cannot be *less* than k because then there would be a non-trivial linear relation among $I, A, A^2, \ldots, A^{k-1}$, which would be a polynomial with $p(A) = 0$ of degree $< k$, contradicting the minimality of the minimal polynomial.

answered Nov 5 '11 at 18:28


Henning Makholm
47.6k 3 59 123

feedback