EXAMPLES OF PROOFS BY INDUCTION

KEITH CONRAD

1. Introduction

Mathematical induction is a method that allows us to prove infinitely many similar statements in a systematic way, by organizing them all in a definite order and showing

- the first statement is correct ("base case")
- if a particular but unspecified statement in the list is correct ("inductive hypothesis"), then the statement after it in the list is correct ("inductive step").

This implies all statements in the list are correct. It is *not* circular reasoning, but "spiraling reasoning". An analogy to falling dominos is common, but dominos are not infinitely long.

The most basic results that are proved by induction are summation identities, such as

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{1.1}$$

for all integers $n \geq 1$. View this identity as a separate statement for each n: $S(1), S(2), S(3)$, and so on, where $S(n)$ is the (as yet unproved) statement in (1.1). At $n = 1$, each side of (1.1) is 1, so $S(1)$ is true. Next, *if* $S(n)$ is true for some $n \geq 1$, then to show $S(n+1)$ is true we write $1 + 2 + \cdots + n + (n+1)$ in terms of $1 + 2 + \cdots + n$ and use the truth of $S(n)$:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= (1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \qquad \text{since } S(n) \text{ is assumed to be true} \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Equality of the first and last expressions here is exactly what it means for $S(n+1)$ to be true. We proved $S(1)$ is true and proved for each $n \geq 1$ that **if** $S(n)$ is true, then $S(n+1)$ is true. Thus all of $S(1), S(2), S(3), \ldots$ are true, which proves (1.1) for all $n \geq 1$. Understand that we really did something. It's not just "simplifying a formula" or voodoo magic!

Another way to prove the inductive step (for $n \geq 1$, if $S(n)$ is true then $S(n+1)$ is true) is to add $n+1$ to both sides of (1.1):

$$\begin{aligned} 1 + 2 + \cdots + n = \frac{n(n+1)}{2} &\Longrightarrow 1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) \\ &\Longrightarrow 1 + 2 + \cdots + n + (n+1) = \frac{n(n+1) + 2(n+1)}{2} \\ &\Longrightarrow 1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Advice. Proofs by induction may not be about algebraic identities, but they are *always* about proving infinitely many statements recursively. Know what those statements are each time! In the inductive step, earlier cases must help us derive the next case, but we don't always turn each case into the next case or start with the inductive hypothesis. There is no single path through inductive proofs: the "next step" may need creativity.

We will meet proofs by induction involving linear algebra, polynomial algebra, calculus, and exponents. In each proof, find the statement depending on a positive integer. Check how, in the inductive step, the inductive hypothesis is used. Some results below are about all integers (positive, negative, and 0) so that you can see induction in that type of setting.

2. Linear Algebra

Theorem 2.1. *For $n \times n$ matrices A and M, where M is invertible, $(MAM^{-1})^k = MA^kM^{-1}$ for all integers $k \geq 0$. If A is invertible, then that equation is true for all integers k.*

Proof. We argue by induction on the exponent k (not on n, the size of the matrix).

The equation $(MAM^{-1})^k = MA^kM^{-1}$ is clear for $k = 0$: both sides are the $n \times n$ identity matrix I. For $k = 1$, the equation $(MAM^{-1})^k = MA^kM^{-1}$ says $MAM^{-1} = MAM^{-1}$, which is true. Here is a proof of $k = 2$:

$$\begin{aligned}(MAM^{-1})^2 &= (MAM^{-1})(MAM^{-1}) \\ &= MA(M^{-1}M)AM^{-1} \\ &= MAIAM^{-1} \\ &= MAAM^{-1} \\ &= MA^2M^{-1}.\end{aligned}$$

Now assume $(MAM^{-1})^k = MA^kM^{-1}$ for some exponent $k \geq 1$. Then

$$\begin{aligned}(MAM^{-1})^{k+1} &= (MAM^{-1})^k(MAM^{-1}) \\ &= (MA^kM^{-1})(MAM^{-1}) \quad \text{by the inductive hypothesis} \\ &= MA^k(M^{-1}M)AM^{-1} \\ &= MA^kIAM^{-1} \\ &= MA^kAM^{-1} \\ &= MA^{k+1}M^{-1},\end{aligned}$$

which proves the inductive step. So the base case $k = 1$ is true for all A and M, and if the k-th case is true for all A and M, then the $(k+1)$-th case is true for all A and M. Thus $(MAM^{-1})^k = MA^kM^{-1}$ for all integers $k \geq 0$ and all A and M.

When A is invertible, let's prove $(MAM^{-1})^k = MA^kM^{-1}$ for all $k < 0$. Set $k = -K$, so $K \geq 1$. We won't use induction again with negative k, but simply calculate both sides to see they're equal by reducing ourselves to the case of positive exponents, which has already been proved (by induction). **Note**: for all invertible B, $B^{-K} = (B^{-1})^K$ for all $K \geq 1$.

The matrices $MA^{-1}M$ and MAM^{-1} are inverses:

$$(MAM^{-1})(MA^{-1}M^{-1}) = MA(M^{-1}M)A^{-1}M^{-1} = MAA^{-1}M^{-1} = MM^{-1} = I.$$

So $(MAM^{-1})^{-1} = MA^{-1}M^{-1}$. That tells us

$$(MAM^{-1})^k = (MAM^{-1})^{-K} = ((MAM^{-1})^{-1})^K = (MA^{-1}M^{-1})^K. \tag{2.1}$$

The proved case of positive exponents tells us $(MA^{-1}M^{-1})^K = M(A^{-1})^K M^{-1}$ by replacing A with A^{-1}. Feeding that into (2.1),

$$(MAM^{-1})^k = M(A^{-1})^K M^{-1} \tag{2.2}$$

Since $A^k = A^{-K} = (A^{-1})^K$, (2.2) becomes $(MAM^{-1})^k = MA^kM^{-1}$, which is what we wanted, so we're done. □

Theorem 2.2. *Let A be a square matrix. Eigenvectors for A having distinct eigenvalues are linearly independent: if $\mathbf{v}_1, \dots, \mathbf{v}_r$ are eigenvectors for A, with $A\mathbf{v}_i = \lambda_i \mathbf{v}_i$ for distinct scalars $\lambda_1, \dots, \lambda_r$, then $\mathbf{v}_1, \dots, \mathbf{v}_r$ are linearly independent.*

Proof. We induct on r, the number of eigenvectors. The result is true if $r = 1$: eigenvectors are not $\mathbf{0}$ and a single nonzero vector is linearly independent. Suppose $r > 1$ and the result has been verified for all sets of fewer than r eigenvectors of A (with distinct eigenvalues).

Given r eigenvectors $\mathbf{v}_i$ of A with distinct eigenvalues λ_i, suppose

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r = \mathbf{0} \tag{2.3}$$

for some scalars c_i. We want to prove each c_i is 0.

Applying A to both sides of (2.3), we get

$$c_1\lambda_1\mathbf{v}_1 + c_2\lambda_2\mathbf{v}_2 + \cdots + c_r\lambda_r\mathbf{v}_r = \mathbf{0}. \tag{2.4}$$

Now multiply through (2.3) by λ_1:

$$c_1\lambda_1\mathbf{v}_1 + c_2\lambda_1\mathbf{v}_2 + \cdots + c_r\lambda_1\mathbf{v}_r = \mathbf{0}. \tag{2.5}$$

Subtracting (2.5) from (2.4) eliminates the first term:

$$c_2(\lambda_2 - \lambda_1)\mathbf{v}_2 + \cdots + c_r(\lambda_r - \lambda_1)\mathbf{v}_r = \mathbf{0}. \tag{2.6}$$

By the inductive hypothesis, the $r-1$ eigenvectors $\mathbf{v}_2, \dots, \mathbf{v}_r$ are linearly independent. Therefore (2.6) tells us that $c_i(\lambda_i - \lambda_1) = 0$ for $i = 2, 3, \dots, r$. Since the eigenvalues are distinct, $\lambda_i - \lambda_1 \neq 0$, so $c_i = 0$ for $i = 2, 3, \dots, r$. Feeding this into (2.3) gives us $c_1\mathbf{v}_1 = \mathbf{0}$, so $c_1 = 0$ as well since $\mathbf{v}_1 \neq \mathbf{0}$. Thus every c_i is 0. □

3. Polynomial algebra

Theorem 3.1. *Let $f(x)$ be a nonconstant polynomial with real coefficients and degree d. Then $f(x)$ has at most d real roots.*

We can't replace "at most d real roots" with "exactly d real roots" since there are nonconstant real polynomials like $x^2 + 1$ that have no real roots.

Proof. We induct on the degree d of $f(x)$. Each step in the induction is about infinitely many polynomials: the theorem in degree 1, then in degree 2, then in degree 3, and so on.

The base case has $d = 1$. A polynomial of degree 1 with real coefficients is of the form $f(x) = ax + b$, where a and b are real and $a \neq 0$. This has exactly one root, namely $-b/a$, and thus *at most* one real root. That settles the theorem for $d = 1$.

Now assume the theorem is true for all polynomials of degree d with real coefficients. We will prove the theorem is true for all polynomials of degree $d+1$ with real coefficients.

A typical polynomial of degree $d+1$ with real coefficients is

$$f(x) = c_{d+1}x^{d+1} + c_dx^d + \cdots + c_1x + c_0, \tag{3.1}$$

where $c_j \in \mathbf{R}$ and $c_{d+1} \neq 0$. If $f(x)$ has no real roots, then we're done, since $0 \leq d+1$. If $f(x)$ has a real root, say r, then

$$0 = c_{d+1}r^{d+1} + c_d r^d + \cdots + c_1 r + c_0. \tag{3.2}$$

Subtracting (3.2) from (3.1), the constant terms c_0 cancel and we get

$$f(x) = c_{d+1}(x^{d+1} - r^{d+1}) + c_d(x^d - r^d) + \cdots + c_1(x - r). \tag{3.3}$$

Each difference $x^j - r^j$ for $j = 1, 2, \ldots, d+1$ has $x - r$ as a factor:

$$x^j - r^j = (x - r)(x^{j-1} + rx^{j-2} + \cdots + r^i x^{j-1-i} + \cdots + r^{j-2}x + r^{j-1}).$$

Write the more complicated second factor, a polynomial of degree $j - 1$, as $Q_{j,r}(x)$. So

$$x^j - r^j = (x - r)Q_{j,r}(x), \tag{3.4}$$

and substituting (3.4) into (3.3) gives

$$\begin{aligned} f(x) &= \sum_{j=1}^{d+1} c_j(x - r)Q_{j,r}(x) \\ &= (x - r)\sum_{j=1}^{d+1} c_j Q_{j,r}(x) \\ &= (x - r)(\underbrace{c_{d+1}}_{\neq 0}\overbrace{Q_{d+1,r}(x)}^{\text{degree } d} + \underbrace{\cdots + c_1 Q_{1,r}(x)}_{\text{lower degree}}). \qquad (3.5) \end{aligned}$$

Since $c_{d+1}Q_{d+1,r}(x)$ is a polynomial of degree d, and each lower degree polynomial does not decrease the degree when added to $c_{d+1}Q_{d+1,r}(x)$, the second factor in (3.5) has degree d.

Each root of $f(x)$ is either r or a root of the second factor in (3.5). Each $Q_{j,r}(x)$ has real coefficients and all c_j are real, so the second factor in (3.5) has real coefficients. We can therefore apply the inductive hypothesis to the second factor and conclude that the second factor in (3.5) has at most d real roots, so $f(x)$ has at most $d+1$ real roots. As $f(x)$ was an arbitrary polynomial of degree $d+1$ with real coefficients, we have shown that the d-th case of the theorem being true implies the $(d+1)$-th case is true. By induction on the degree, the theorem is true for all nonconstant polynomials. □

Our next two theorems use the truth of some earlier case to prove the next case, but not necessarily the truth of the immediately previous case to prove the next case. This approach is called the "strong" form of induction.

Theorem 3.2. *Every nonconstant polynomial has an irreducible factor.*

Recall that a nonconstant polynomial is called irreducible when its only factors are constants and constant multiples of itself. For example, x is irreducible. It has factorizations like $2(x/2)$ and $5(x/5)$, but those are trivial since one of the factors is constant. **Warning**: a polynomial with no roots doesn't have to be irreducible! Consider $(x^2 + 1)(x^2 + 2)$.

Proof. We induct on the degree d of the nonconstant polynomial.

When $d = 1$, the polynomial is linear. Linear polynomials are irreducible, so the case $d = 1$ is settled.

Assuming every nonconstant polynomial with degree $\leq d$ has an irreducible factor, consider a polynomial $f(x)$ with degree $d+1$. If $f(x)$ is irreducible, then $f(x)$ has an irreducible factor (namely itself). If $f(x)$ is not irreducible, then we can factor $f(x)$ into nonconstant parts, say $f(x) = g(x)h(x)$ where $1 \leq \deg g(x),\ \deg h(x) < d+1$. By our (strong) inductive assumption, $g(x)$ has an irreducible factor, and this irreducible polynomial will also be a factor of $f(x)$ since $g(x)$ is a factor of $f(x)$. Thus $f(x)$ has an irreducible factor and we are done. □

Theorem 3.3. *Every nonconstant polynomial is a product of irreducible polynomials.*

We include here the convention that an irreducible polynomial is considered to be a 1-term product of irreducible polynomials. For example, x^2+1 is irreducible and it is a 1-term product of irreducibles.

Proof. We induct on the degree d of the nonconstant polynomial.

When $d = 1$, the polynomial is linear. Linear polynomials are irreducible, so the case $d = 1$ is settled.

Assume every nonconstant polynomial with degree $\leq d$ is a product of irreducible polynomials. We want to prove every polynomial with degree $d + 1$ is a product of irreducible polynomials. Let $f(x)$ be a polynomial with degree $d + 1$. Either $f(x)$ is irreducible or it is not. If $f(x)$ is irreducible, then it is a 1-term product of irreducible polynomials. (namely itself). If $f(x)$ is not irreducible, then we can factor $f(x)$ into nonconstant parts, say $f(x) = g(x)h(x)$ where $1 \leq \deg g(x),\ \deg h(x) < d + 1$. By our (strong) inductive assumption, $g(x)$ and $h(x)$ are each products of irreducible polynomials:

$$g(x) = p_1(x)\cdots p_r(x), \qquad h(x) = q_1(x)\cdots q_s(x),$$

where $p_i(x)$ and $q_j(x)$ are irreducible polynomials. Then

$$f(x) = g(x)h(x) = p_1(x)\cdots p_r(x)q_1(x)\cdots q_s(x),$$

so $f(x)$ is a product of irreducible polynomials. □

While this last proof by induction shows every nonconstant polynomial has an irreducible factorization, it does *not* tell us how to find it! For example, it is not obvious how to write

$$x^5 + 2x^4 - 2x^2 - x + 1$$

as an explicit product of irreducible polynomials.

4. Calculus

A calculus analogue of proving summation identities by induction is proving derivative identities by induction. Here is an example.

Theorem 4.1. *For* $n \geq 1$, $\dfrac{\mathrm{d}^n}{\mathrm{d}x^n}(e^{x^2}) = P_n(x)e^{x^2}$, *where* $P_n(x)$ *is a polynomial of degree* n.

Before working out the proof, let's see how we could *guess* such a result by doing calculations for small n:

1. The first derivative of e^{x^2} is $2xe^{x^2}$.
2. The second derivative of e^{x^2} is $(2xe^{x^2})'$, which is $(4x^2 + 2)e^{x^2}$ by the product rule.
3. The third derivative of e^{x^2} is $((4x^2+2)e^{x^2})'$, which is $(8x^3+12x)e^{x^2}$ by the product rule again.

Each time we are getting a polynomial times e^{x^2}, and the degree of the polynomial matches the order of the derivative. So the formulation of Theorem 4.1 is not a surprise based on the initial examples. (They also suggest proving that $P_n(x)$ has leading coefficient 2^n.)

Proof. We argue by induction on n.

Our base case is $n = 0$. The zeroth derivative of a function is the function itself, so we want to know e^{x^2} is $P_0(x)e^{x^2}$ for a polynomial $P_0(x)$ of degree 0. This is true using $P_0(x) = 1$. Let's check $n = 1$. The first derivative $(e^{x^2})'$ is $2xe^{x^2}$, so this is $P_1(x)e^{x^2}$ for the polynomial $P_1(x) = 2x$, which has degree 1.

Now we do the inductive step. For $n \geq 1$, assume

$$(e^{x^2})^{(n)} = P_n(x)e^{x^2} \tag{4.1}$$

for some polynomial $P_n(x)$ of degree n. To compute $(e^{x^2})^{(n+1)}$, we differentiate both sides of (4.1) and obtain

$$\begin{aligned} (e^{x^2})^{(n+1)} &= (P_n(x)e^{x^2})' && \text{by the inductive hypothesis} \\ &= P_n(x)(e^{x^2})' + e^{x^2}P_n'(x) && \text{by the product rule} \\ &= P_n(x)(2xe^{x^2}) + P_n'(x)e^{x^2} \\ &= (2xP_n(x) + P_n'(x))e^{x^2}. \end{aligned}$$

The first factor here is $2xP_n(x) + P_n'(x)$. Since $P_n(x)$ has degree n, $2xP_n(x)$ has degree $n+1$ while $P_n'(x)$ has degree $n-1$. When you add polynomials with different degrees, the degree of the sum is the larger of the two degrees (in fact, the whole leading term of the sum is the leading term of the larger degree polynomial). Therefore, setting $P_{n+1}(x) := 2xP_n(x) + P_n'(x)$, we have $(e^{x^2})^{(n+1)} = P_{n+1}(x)e^{x^2}$, where $P_{n+1}(x)$ is a polynomial of degree $n+1$. That settles the inductive step and completes the proof. □

This is not an interesting illustration of induction because the proof of the inductive step is too routine ("differentiate both sides," which is analogous to "adding something to both sides" in the proof of a summation identity). Most uses of induction in calculus proofs are not a matter of differentiating both sides of an identity. Here is an example.

Theorem 4.2. *For all sets of differentiable functions $f_1(x), \ldots, f_n(x)$ where $n \geq 2$,*

$$\frac{(f_1(x)\cdots f_n(x))'}{f_1(x)\cdots f_n(x)} = \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)}.$$

Proof. We induct on n, the number of functions.

The base case is $n = 2$ and it follows from the product rule

$$(f_1(x)f_2(x))' = f_1'(x)f_2(x) + f_1(x)f_2'(x)$$

by dividing both sides by $f_1(x)f_2(x)$:

$$\frac{(f_1(x)f_2(x))'}{f_1(x)f_2(x)} = \frac{f_1'(x)f_2(x) + f_1(x)f_2'(x)}{f_1(x)f_2(x)} = \frac{f_1'(x)}{f_1(x)} + \frac{f_2'(x)}{f_2(x)}.$$

Now assume the result is true for all sets of n differentiable functions for some $n \geq 2$. To prove the result for all sets of $n+1$ differentiable functions $f_1(x), \ldots, f_{n+1}(x)$, write their product either as a product of two functions or as a product of n functions by collecting some factors into a single function:

$$f_1(x)f_2(x)\cdots f_{n+1}(x) = (f_1(x)f_2(x)\cdots f_n(x)) \cdot f_{n+1}(x) \tag{4.2}$$

is a product of the two functions $f_1(x)f_2(x)\cdots f_n(x)$ and $f_{n+1}(x)$, while

$$f_1(x)f_2(x)\cdots f_{n+1}(x) = (f_1(x)f_2(x))f_3(x)\cdots f_{n+1}(x) \tag{4.3}$$

is a product of the n functions $f_1(x)f_2(x), f_3(x), \ldots, f_{n+1}(x)$.

Both (4.2) and (4.3) lead to separate approaches to the inductive step: use the base case (all sets of 2 differentiable functions) and then the inductive hypothesis (all sets of n differentiable functions) or use the inductive hypothesis and then the base case. For the first method, write

$$\begin{aligned}\frac{(f_1(x)\cdots f_{n+1}(x))'}{f_1(x)\cdots f_{n+1}(x)} &= \frac{((f_1(x)\cdots f_n(x))\cdot f_{n+1}(x))'}{(f_1(x)\cdots f_n(x))\cdot f_{n+1}(x)} \\ &= \frac{(f_1(x)\cdots f_n(x))'}{f_1(x)\cdots f_n(x)} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{by the base case} \\ &= \frac{f_1'(x)}{f_1(x)} + \cdots + \frac{f_n'(x)}{f_n(x)} + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{by the inductive hypothesis}\end{aligned}$$

and this is what we needed to show for $n+1$ functions. For the second method, write

$$\begin{aligned}\frac{(f_1(x)\cdots f_{n+1}(x))'}{f_1(x)\cdots f_{n+1}(x)} &= \frac{((f_1(x)f_2(x))f_3(x)\cdots f_{n+1}(x))'}{(f_1(x)f_2(x))f_3(x)\cdots f_{n+1}(x)} \\ &= \frac{(f_1(x)f_2(x))'}{f_1(x)f_2(x)} + \frac{f_3'(x)}{f_3(x)} + \cdots + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{by the ind. hypothesis} \\ &= \frac{f_1'(x)}{f_1(x)} + \frac{f_2'(x)}{f_2(x)} + \frac{f_3'(x)}{f_3(x)} + \cdots + \frac{f_{n+1}'(x)}{f_{n+1}(x)} && \text{by the base case.}\end{aligned}$$

□

Remark 4.3. In the appendix we prove a second theorem by induction on the number of terms.

Theorem 4.4. *For $x > 0$ and integers $n \geq 0$, $e^x > 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$.*

This inequality is clear without induction, using the power series expansion for e^x: $e^x = \sum_{k\geq 0} x^k/k!$ for all real x, and when $x > 0$ the terms in the sum are all positive so we can drop all the terms of the series past the nth term and the inequality of Theorem 4.4 drops out. So why prove Theorem 4.4 by induction if we can prove the theorem quickly using power series? Just to illustrate techniques!

Proof. We will prove the inequality by induction on n.

The base case $n = 0$ says: $e^x > 1$ for $x > 0$. This is true since e^x is an increasing function, so $e^x > e^0 = 1$ when x is positive.

Now we make our inductive hypothesis:

$$e^x > 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} \tag{4.4}$$

for all $x > 0$. We will derive the same inequality with $n+1$ in place of n (for all $x > 0$).

We will actually give two different approaches to the inductive step: the first will use integrals and the second will use derivatives. These approaches are logically independent of each other and can be read in either order.

The Integral Approach: When $f(x) > g(x)$ on an interval $[a, b]$, their integrals over the interval have the same inequality: $\int_a^b f(x)\,\mathrm{d}x > \int_a^b g(x)\,\mathrm{d}x$. This is also true if the functions are equal at an endpoint but otherwise satisfy $f(x) > g(x)$. (We have in mind here only continuous functions.)

We are going to apply this idea to the inequality (4.4). Our inductive hypothesis is that (4.4) holds for every $x > 0$, but at $x = 0$ we get equality in (4.4) since both sides become 1. Therefore we can integrate both sides of (4.4) over *every* interval $[0, t]$ where $t > 0$:

$$\int_0^t e^x \, \mathrm{d}x > \int_0^t \left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}\right) \mathrm{d}x.$$

Evaluating both sides,

$$e^t - 1 > t + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots + \frac{t^{n+1}}{(n+1)!}.$$

Now add 1 to both sides and we have

$$e^t > 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots + \frac{t^{n+1}}{(n+1)!}.$$

This has been derived for every $t > 0$, so we can now simply rename t as x and we have completed the inductive step.

The Derivative Approach: The key idea we will use with derivatives is that a function having a positive derivative on an interval is increasing on this interval. In particular, if $g(x)$ is differentiable for $x \geq 0$ and $g'(x) > 0$ for $x > 0$ then $g(x) > g(0)$ for $x > 0$. Make sure you understand this idea before reading further.

We are assuming (4.4) holds for some n and all $x > 0$, and we want to use this to derive the analogue of (4.4) for the next exponent $n + 1$: for all $x > 0$,

$$e^x \overset{?}{>} 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n+1}}{(n+1)!}. \tag{4.5}$$

Well, let $F(x)$ be the difference of the two sides of (4.5):

$$F(x) = e^x - \left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \frac{x^{n+1}}{(n+1)!}\right).$$

Our goal is to show $F(x) > 0$ if $x > 0$. Consider the derivative

$$F'(x) = e^x - \left(0 + 1 + x + \cdots + \frac{x^{n-1}}{(n-1)!} + \frac{x^n}{n!}\right).$$

Our induction hypothesis (4.4) is *exactly* the statement that $F'(x)$ is positive for $x > 0$. Therefore by our induction hypothesis $F(x)$ is an increasing function for $x \geq 0$, so $F(x) > F(0)$ when $x > 0$. Since $F(0) = 0$, we obtain $F(x) > 0$ for all $x > 0$, which completes the inductive step using this second approach. □

Notice how the inductive hypothesis was used in the two approaches to the inductive step. In the integral approach, we integrated the inequality in the inductive hypothesis to derive the inequality for the next exponent. In the derivative approach, on the other hand, we did not start with the inductive hypothesis and "do something to both sides." Instead, we set up a convenient function $F(x)$ related to what we wanted to show and used the inductive hypothesis to tell us something relevant about the derivative of that function.

The following corollary of Theorem 4.4 is important: it says e^x grows *faster* than every fixed integral power of x.

Corollary 4.5. *For every integer $n \geq 0$, $\dfrac{e^x}{x^n} \to \infty$ and $\dfrac{x^n}{e^x} \to 0$ as $x \to \infty$.*

Proof. Since $e^x/x^n > 0$ when $x > 0$, saying $e^x/x^n \to \infty$ and $x^n/e^x \to 0$ are the same thing. We will prove the first version, that $e^x/x^n \to \infty$ as $x \to \infty$. By Theorem 4.4,

$$e^x > 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \frac{x^{n+1}}{(n+1)!}$$

when $x > 0$. (Why did we use the inequality out to degree $n+1$ instead of degree n? Read on and you'll see.) In particular, since all lower degree terms on the right side are positive when $x > 0$,

$$e^x > \frac{x^{n+1}}{(n+1)!}$$

when $x > 0$. Divide both sides of this inequality by x^n:

$$\frac{e^x}{x^n} > \frac{x}{(n+1)!}.$$

Here n is fixed and x is an arbitrary positive real number. In this inequality, the right side tends to ∞ as $x \to \infty$. Therefore $e^x/x^n \to \infty$ as $x \to \infty$. (We did not use induction in this proof.) □

From Corollary 4.5 we draw two further conclusions.

Corollary 4.6. *For every polynomial $p(x)$, $\dfrac{p(x)}{e^x} \to 0$ as $x \to \infty$.*

Proof. By Corollary 4.5, $x^n/e^x \to 0$ as $x \to \infty$. Every polynomial is a sum of multiples of such ratios: writing $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, we have

$$\frac{p(x)}{e^x} = a_d \frac{x^d}{e^x} + a_{d-1}\frac{x^{d-1}}{e^x} + \cdots + a_1 \frac{x}{e^x} + a_0 \frac{1}{e^x}.$$

Each x^n/e^x appearing here tends to 0 as $x \to \infty$, so $p(x)/e^x$ tends to 0 as $x \to \infty$. □

Corollary 4.7. *For every integer $n \geq 0$, $\dfrac{(\log x)^n}{x} \to 0$ as $x \to \infty$,*

Proof. Set $y = \log x$, so $x = e^y$ and $(\log x)^n/x = y^n/e^y$. We want to show $y^n/e^y \to 0$ as $x \to \infty$. As $x \to \infty$, also $y \to \infty$. Therefore by Corollary 4.5, $e^y/y^n \to \infty$ as $x \to \infty$, so $y^n/e^y \to 0$ as $x \to \infty$. □

Theorem 4.8. *For $n \geq 0$, $\displaystyle\int_0^\infty x^n e^{-x}\, dx = n!$.*

Proof. We argue by induction on n. For $n = 0$,

$$\int_0^\infty e^{-x}\, dx = -\, e^{-x}\Big|_0^\infty = \lim_{b\to\infty} -\, e^{-x}\Big|_0^b = \lim_{b\to\infty} -e^{-b} + 1 = 0 + 1 = 1.$$

For $n \geq 1$, we express $\int_0^\infty x^n e^{-x}\,\mathrm{d}x$ in terms of $\int_0^\infty x^{n-1}e^{-x}\,\mathrm{d}x$ using integration by parts:

$$\begin{aligned}
\int_0^\infty x^n e^{-x}\,\mathrm{d}x &= \int_0^\infty u\,\mathrm{d}v && (u = x^n, \mathrm{d}v = e^{-x}\,\mathrm{d}x)\\
&= uv\Big|_0^\infty - \int_0^\infty v\mathrm{d}u && (\mathrm{d}u = nx^{n-1}, v = -e^{-x})\\
&= n\frac{x^{n-1}}{e^x}\Big|_0^\infty + n\int_0^\infty x^{n-1}e^{-x}\,\mathrm{d}x\\
&= (0-0) + n\cdot(n-1)! && \text{by Corollary 4.5 and the ind. hypothesis}\\
&= n!.
\end{aligned}$$

□

Theorem 4.9. *The function e^x is not "algebraic": for no $n \geq 1$ and polynomials $c_0(x)$, $c_1(x)$, …, $c_n(x)$ that are not all identically zero can we have*

$$c_n(x)e^{nx} + c_{n-1}(x)e^{(n-1)x} + \cdots + c_1(x)e^x + c_0(x) = 0 \tag{4.6}$$

for all $x \in \mathbf{R}$. In other words, if such a functional identity does hold then all the polynomial coefficients $c_k(x)$ are the zero polynomial.

The left side of (4.6) is a "polynomial in e^x with polynomial coefficients," which can be thought of as

$$c_n(x)y^n + c_{n-1}(x)y^{n-1} + \cdots + c_1(x)y + c_0(x) \tag{4.7}$$

where we have substituted e^x for y. Since the $c_k(x)$'s are polynomials in x, (4.7) is a two-variable polynomial in x and y. The theorem is saying no two-variable polynomial $P(x,y)$ can have e^x as a "root" in y. By comparison, the function $x^{1/3}$ is a "root" of the two-variable polynomial $Q(x,y) = y^3 - x$: when we substitute $x^{1/3}$ in for y, the result $Q(x, x^{1/3})$ is the zero function.

Proof. We argue by induction on n. Corollary 4.6 will play a role!

The base case is $n = 1$. Suppose

$$c_1(x)e^x + c_0(x) = 0 \tag{4.8}$$

for all x and some polynomials $c_0(x)$ and $c_1(x)$. We want to show $c_0(x)$ and $c_1(x)$ are both the zero polynomial. Dividing by e^x and re-arranging, we have

$$c_1(x) = -\frac{c_0(x)}{e^x}$$

for all x. We now think about what this tells us as $x \to \infty$. The right side tends to 0 by Corollary 4.6. This forces $c_1(x)$ to be the zero polynomial, since a non-zero polynomial does not tend to 0 as $x \to \infty$: a non-zero constant polynomial keeps its constant value while a non-constant polynomial tends to $\pm\infty$ (depending on the sign of the leading coefficient). Now that we know $c_1(x)$ is identically zero, our original equation (4.8) becomes $c_0(x) = 0$ for all x. This concludes the base case.

For the inductive step, assume for some $n \geq 1$ that the only way to satisfy (4.6) for all x is to have all coefficients $c_k(x)$ equal to the zero polynomial. Then suppose there are $n+1$ polynomials $a_0(x), \ldots, a_{n+1}(x)$ such that

$$a_{n+1}(x)e^{(n+1)x} + a_n(x)e^{nx} + \cdots + a_1(x)e^x + a_0(x) = 0 \tag{4.9}$$

for all x. We want to show every $a_k(x)$ is the zero polynomial.

As in the base case, we divide this equation by an exponential, but now take it to be $e^{(n+1)x}$ instead of e^x:

$$a_{n+1}(x) + \frac{a_n(x)}{e^x} + \cdots + \frac{a_1(x)}{e^{nx}} + \frac{a_0(x)}{e^{(n+1)x}} = 0.$$

Moving all but the first term to the other side,

$$a_{n+1}(x) = -\frac{a_n(x)}{e^x} - \cdots - \frac{a_1(x)}{e^{nx}} - \frac{a_0(x)}{e^{(n+1)x}} \tag{4.10}$$

for all x.

What happens in (4.10) when $x \to \infty$? On the right, $-a_n(x)/e^x \to 0$ by Corollary 4.6. Other terms have the form $-a_k(x)/e^{(n+1-k)x}$ for $k = 0, 1, \ldots, n-1$. Writing this as $-(a_k(x)/e^x)(1/e^{(n-k)x})$, it tends to $0 \cdot 0 = 0$ by Corollary 4.6 (since $n - k > 0$). Therefore the right side of (4.10) tends to 0 as $x \to \infty$, so the polynomial $a_{n+1}(x)$ must be the zero polynomial (same argument as in the base case). This means the left-most term in (4.9) disappears, so (4.9) becomes

$$a_n(x)e^{nx} + \cdots + a_1(x)e^x + a_0(x) = 0$$

for all x. This is a relation of degree n in e^x, so by the inductive hypothesis (at last!) all of its polynomial coefficients are the zero polynomial. Therefore all the coefficients of (4.9) are the zero polynomial, which completes the inductive step. □

Remark 4.10. Since the values of x that mattered in the limits are large values (we took $x \to \infty$), we could have incorporated this into the statement of the theorem and obtained a (slightly) stronger result: if there are polynomials $c_0(x), \ldots, c_n(x)$ such that

$$c_n(x)e^{nx} + c_{n-1}(x)e^{(n-1)x} + \cdots + c_1(x)e^x + c_0(x) = 0$$

just for sufficiently large x, then every $c_k(x)$ is the zero polynomial. The argument proceeds exactly as before except we replace "for all x" by "for all sufficiently large x" in each occurrence. The logical structure of the argument is otherwise unchanged.

5. Integral exponents

Every nonzero real number a has a reciprocal $1/a = a^{-1}$. The integral powers a^n for $n \in \mathbf{Z}$ are defined as follows:

- Recursively, $a^1 = a$ and $a^n = a^{n-1}a$ for $n \geq 2$ (or concretely, $a^n = \underbrace{a \cdots a}_{n \text{ times}}$ if $n \geq 1$),
- $a^0 = 1$,
- $a^n = (a^{-1})^{|n|}$ for $n \leq -1$ (*e.g.*, $a^{-3} = a^{-1}a^{-1}a^{-1}$).

In words, the specific powers $a^1 = a$ and $a^{-1} = 1/a$ are defined first, the remaining nonzero powers of a are repeated products of a^1 or a^{-1}, and $a^0 = 1$.

To illustrate the use of induction on formulas with two parameters, we will prove the following equations for all $a \neq 0$ and arbitrary m and n in $\mathbf{Z}$:

$$a^m a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}.$$

Theorem 5.1. *For all $a \neq 0$ and all integers m and n, $a^m a^n = a^{m+n}$.*

Proof. We will first prove this for *arbitrary* $m \in \mathbf{Z}$ *and all* $n \geq 1$, and then handle the remaining cases (arbitrary m and $n \leq 0$) by often reducing to the case where $n \geq 1$.

First we will prove $a^m a^n = a^{m+n}$ for $n \geq 1$ by induction on n. Since a and m also appear in that equation, let's clarify the statement $S(n)$ that we'll be proving for each $n \geq 1$: $S(n)$

says *for all* $a \neq 0$ *and all* $m \in \mathbf{Z}$, $a^m a^n = a^{m+n}$. We will prove $S(n)$ is true for all $n \geq 1$ by induction on n.

Base case $n = 1$. Since $a^n = a^1 = a$ by definition, the desired equation $a^m a^n \overset{?}{=} a^{m+n}$ for all $m \in \mathbf{Z}$ says when $n = 1$ that $a^m a \overset{?}{=} a^{m+1}$ for all $m \in \mathbf{Z}$. Let's break this into separate parts depending on the sign of m.

- If $m \geq 1$, then the recursive definition of powers of a says $a^{m+1} = a^{m+1-1}a = a^m a$.
- If $m = 0$, then $a^m a = a^0 a = 1 \cdot a = a$ and $a^{m+1} = a^1 = a$.
- If $m = -1$, then $a^m a = a^{-1} a = 1$ and $a^{m+1} = a^0 = 1$.
- If $m \leq -2$, then set $m = -M$ with $M \geq 2$, so $a^m a = a^{-M} a = (a^{-1})^M a = (a^{-1})^{M-1} a^{-1} a = (a^{-1})^{M-1} = a^{-(M-1)} = a^{-M+1} = a^{m+1}$.

Inductive step. Assume for all $a \neq 0$ and all $m \in \mathbf{Z}$ that $a^m a^n = a^{m+n}$ for some $n \geq 1$. We want to show for all $a \neq 0$ and all $m \in \mathbf{Z}$ that $a^m a^{n+1} = a^{m+n+1}$. The term a^{n+1} is $a^n a$ by the recursive definition of positive powers of a, so

$$a^m a^{n+1} = a^m (a^n a) = (a^m a^n) a = a^{m+n} a,$$

where the last equation comes from the inductive hypothesis, and $a^{m+n} a = a^{m+n+1}$ by the base case above using exponent $m + n$ *in the role of* m (an arbitrary integer).

We have proved $a^m a^n = a^{m+n}$ for all nonzero a, all $m \in \mathbf{Z}$, and all n in $\mathbf{Z}^+$ by using induction on n. It remains to prove $a^m a^n = a^{m+n}$ for all $m \in \mathbf{Z}$ and all $n \leq 0$ in $\mathbf{Z}$.

$n = 0$. Both sides of $a^m a^n \overset{?}{=} a^{m+n}$ when $n = 0$ become a^m since $a^0 = 1$, so the equation is true in this case.

$n < 0$. Write $n = -N$, so $N \in \mathbf{Z}^+$ and we want to show $a^m a^{-N} \overset{?}{=} a^{m-N}$ for all $m \in \mathbf{Z}$, which is equivalent to $a^m (a^N)^{-1} \overset{?}{=} a^{m-N}$ for all $m \in \mathbf{Z}$. The validity of this equation would be unaffected by multiplying both sides by a^N, and doing that lets us simplify the right side thanks to what we already proved:

$$a^m (a^{-1})^N \overset{?}{=} a^{m-N} \iff a^m (a^{-1})^N a^N \overset{?}{=} a^{m-N} a^N, \tag{5.1}$$

and on the right side $a^{m-N} a^N = a^{(m-N)+N} = a^m$ by what we proved earlier ($m - N$ is some integer and $N \geq 1$), so now we want to check that $a^m (a^{-1})^N a^N \overset{?}{=} a^m$. This looks obvious since the product $(a^{-1})^N a^N$ ought to be 1. Let's check $(a^{-1})^N a^N = 1$ for all nonzero a and all $N \in \mathbf{Z}^+$ by using induction on N.

For the base case $N = 1$, $(a^{-1})^N a^N = (a^{-1}) a = 1$. For the inductive step, if $(a^{-1})^N a^N = 1$ for an $N \geq 1$, then to obtain the same equation with $N + 1$ in the exponents,

$$(a^{-1})^{N+1} a^{N+1} = (a^{-1})^N a^{-1} a^{N+1} \tag{5.2}$$

by the recursive definition of positive powers of a^{-1}. Write a^{N+1} as a^{1+N}. We already proved $a^{m+n} = a^m a^n$ for all $m \in \mathbf{Z}$ and all $n \geq 1$, so $a^{1+N} = a a^N$. That turns (5.2) into

$$(a^{-1})^{N+1} a^{N+1} = (a^{-1})^N a^{-1} a a^N = (a^{-1})^N a^N$$

because $a^{-1} a = 1$. We have $(a^{-1})^N a^N = 1$ by the inductive hypothesis. This completes the inductive step, so we have shown $(a^{-1})^N a^N = 1$ for all $N \in \mathbf{Z}^+$. Returning to (5.1), we already saw $a^{m-N} a^N = a^m$, and now we know $a^m (a^{-1})^N a^N$ is $a^m \cdot 1 = a^m$, so we have proved $a^m a^n = a^{m+n}$ for all nonzero a, all $m \in \mathbf{Z}$, and all negative integers n. □

Theorem 5.2. *For all* $a \neq 0$ *and all integers* m *and* n, $(a^m)^n = a^{mn}$.

Proof. First we will treat the case $n \geq 1$. Let $S(n)$ be the statement *for all* $a \neq 0$ *and all* $m \in \mathbf{Z}$, $(a^m)^n = a^{mn}$. We will prove $S(n)$ is true for all $n \geq 1$ by induction on n and then treat the case $n \leq 0$.

Base case $n = 1$. Since everything to the power 1 is itself by definition, the desired equation $(a^m)^n \overset{?}{=} a^{mn}$ when $n = 1$ says $a^m \overset{?}{=} a^m$, which is true.

Inductive step. Assume for all $a \neq 0$ and all $m \in \mathbf{Z}$ that $(a^m)^n = a^{mn}$ for some $n \geq 1$. We want to show for all $a \neq 0$ and all $m \in \mathbf{Z}$ that $(a^m)^{n+1} \overset{?}{=} a^{m(n+1)}$. By the recursive definition of positive powers of a^m,

$$(a^m)^{n+1} = (a^m)^n a^m. \tag{5.3}$$

From the inductive hypothesis, $(a^m)^n = a^{mn}$, and plugging that into (5.3) tells us

$$(a^m)^{n+1} = a^{mn}a^m = a^{mn+m},$$

where the last equation is a special case of Theorem 5.1 with exponents mn and m. Since $mn+m = m(n+1)$, we finally obtain $(a^m)^{n+1} = a^{m(n+1)}$, which finishes the inductive step.

Now we turn to the case that $n \leq 0$.

$n = 0$. Since the 0 power is 1 by definition, the desired equation $(a^m)^n \overset{?}{=} a^{mn}$ when $n = 0$ says $(a^m)^0 \overset{?}{=} a^0$, which says $1 \overset{?}{=} 1$, and that's true.

$n < 0$. Write $n = -N$, so $N \in \mathbf{Z}^+$ and we want to show $(a^m)^{-N} \overset{?}{=} a^{m(-N)}$. The left side is $((a^m)^N)^{-1}$ by the definition of negative powers of a^m, and the right side is a^{-mN}, From what we already proved when the outer exponent is a positive integer and the inner exponent is an arbitrary integer,

$$(a^m)^N = a^{mN}.$$

Therefore we want to show

$$(a^{mN})^{-1} \overset{?}{=} a^{-mN}$$

for arbitrary $m \in \mathbf{Z}$. The left side denotes the (multiplicative) inverse of a^{mN}, and that is a^{-mN} thanks to Theorem 5.1 since that theorem tells us that $a^{mN}a^{-mN} = a^0 = 1$. □

Appendix A. Another proof by induction on the number of terms

In Theorem 4.2 we proved an identity about derivatives by induction on the number of functions in the identity. Here is another example of a theorem proved by induction on the number of terms.

Theorem A.1. *For all odd numbers* $a_1, \ldots, a_n$ *where* $n \geq 2$, *the product* $a_1 \cdots a_n$ *is odd.*

Proof. We induct on n, the number of odd numbers.

For the base case $n = 2$ we want to every product of two odd numbers a_1 and a_2 is odd. Since these numbers are odd, $a_1 = 2k_1 + 1$ and $a_2 = 2k_2 + 1$ for some integers k_1 and k_2. Then

$$a_1a_2 = (2k_1 + 1)(2k_2 + 1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2(2k_1k_2 + k_1 + k_2) + 1,$$

which is an odd number since $2k_1k_2 + k_1 + k_2$ is an integer. That settles the base case.

Now assume for an $n \geq 2$ that the result is true for all sets of n odd numbers. To prove the result for $n + 1$, we want to show every set of $n + 1$ odd numbers $a_1, \ldots, a_{n+1}$ has a product $a_1 \cdots a_{n+1}$ that is odd.

A product of $n+1$ numbers can be written either as a product of 2 numbers or as a product of n numbers by collecting some factors into a single number:

$$a_1a_2\cdots a_{n+1} = (a_1a_2\cdots a_n)a_{n+1} \tag{A.1}$$

is a product of the two numbers $a_1a_2\cdots a_n$ and a_{n+1}, while

$$a_1a_2\cdots a_{n+1} = a_1a_2\cdots a_{n-1}(a_na_{n+1}) \tag{A.2}$$

is a product of the n numbers a_1, $a_2, \ldots, a_{n-1}$, and a_na_{n+1}.

Each of (A.1) and (A.2) leads to a proof of the inductive step: using (A.1) involves the inductive hypothesis (all sets of n odd numbers) and then the base case (all sets of 2 odd numbers) while (A.2) involves the base case (all sets of 2 odd numbers) and then the inductive hypothesis (all sets of n odd numbers).

First method. Write

$$a_1a_2\cdots a_na_{n+1} = (a_1a_2\cdots a_n)a_{n+1}$$

and the product $a_1a_2\cdots a_n$ is odd by the inductive hypothesis (for n odd numbers). Then $(a_1a_2\cdots a_n)a_{n+1}$ is a product of *two* odd numbers, $a_1a_2\cdots a_n$ and a_{n+1}, so their product is odd by the base case. Thus $a_1a_2\cdots a_na_{n+1}$ is an odd number.

Second method. Write

$$a_1a_2\cdots a_na_{n+1} = a_1a_2\cdots a_{n-1}(a_na_{n+1}).$$

The product a_na_{n+1} is an odd number by the base case, so $a_1a_2\cdots a_{n-1}(a_na_{n+1})$ is a product of n odd numbers: a_1, $a_2, \ldots, a_{n-1}$, and a_na_{n+1}. Therefore their product is odd by the inductive hypothesis, which says $a_1a_2\cdots a_{n-1}(a_na_{n+1})$ is odd, so $a_1a_2\cdots a_na_{n+1}$ is odd. □