Proof by Induction

This note is intended to do three things: (a) remind you of what proof by induction means, how it works; (b) use induction to prove Corollary 1.1 from our textbook, i.e. work out exercise 44 on page 53, and (c) consider what a proof is, and how much one needs to say to constitute a proof.

(I am going to assume we know that any product of matrices, assuming the sizes are such that the product is defined, can be "reassociated", i.e. we can put in parentheses in any way and get the same result. The case of three matrices is part (a) in Theorem 1.2 on page 35. To prove carefully that it is true for any number of matrices would itself be done by induction. But it is confusingly difficult even to write out what that means, since there are so many different ways to put in the parentheses. For four matrices there are five ways to put in the parentheses, and for five there are fourteen. You might find the paper at **http://www.math.hmc.edu/∼su/pcmi/projects/pcmi-Catalan.pdf** interesting!)

First of all, "proof by induction" is used in the following situation: (There are actually several forms of proof by induction, but they are equivalent and I won't worry about the difference for now.) We have some statement that is either true or false, depending on a number. The number will typically be a positive whole number, $1,\ 2,\ 3, \cdots$: There is no reason it could not start at 0 or some other value, but we definitely want there to be a "first" value such as 1. (So in its basic form we would not use induction to prove some statement was true for <u>all</u> whole numbers including $0,\ -1,\ -2,\ -3 \cdots$ as well the positive ones, since there would be nowhere to get started.) For any particular number (among those that we care about, e,g, the positive ones) the statement must be either true or false, depending perhaps on the number but not undecideable. So a statement like "this number is even" would be OK, true for some but not for others, but "this number is even and it is presently raining in Paris" would not. Corollary 1.1 says that the product of any n nonsingular matrices in some prescribed order is itself nonsingular, and tells us what the inverse of that product should be. That does not make much sense for $n = 1$: What is the product of 1 matrix. But it does make sense (and for the moment might be either true or false) for $n = 2$, in which case the corollary becomes just a restatement of Theorem 1.6, or forsubject to approval of the circuit $n = 3,\ 4,\ 5, \cdots$.

Side issue: What does it mean to say something is a Corollary, as in this case Corollary 1.1? In general a corollary is apt to follow soon after some theorem. We use the word theorem to apply to something that can be shown to be true, where the proof may well require some creative thought and/or be complicated. A corollary is generally itself really a theorem, in the sense that it is a statement to be proved true, but one whose proof is based on a (perhaps itself creative) use of the theorem it follows. This is exactly the situation we have here, Corollary 1.1 will be proved by using Theorem 1.6. It would have been possible to state a different theorem, that said the product of at least two nonsingular matrices is nonsingular and the inverse was such and such, rather than do the case of 2 matrices first and separately, but it is convenient to arrange things this way.

Back to what proof by induction means: This is frequently described by analogy. Suppose you have some small blocks of wood. (Frequently it is suggested these might be dominoes, if you know what they are,) Suppose they are set up on a table so that they can be knocked over, and suppose two things more: (a) They are arranged so that if the first block falls over, it knocks over the second, and if the second falls over, it brings down the third, and in general if the k^{th} block falls over, it knocks down the $(k+1)^{th}$ block. (b) The first block gets pushed over. Then what will happen? I claim that any given block will get pushed over, which we might formalize as "Block n falls over for any n." There are several details to consider: What does "for any n" mean? That only makes sense for $n = 1$, $n = 2$, etc., not for 0 or -7 or 4.6. And is it equivalent to say "all the blocks fall over"? This latter point is sticky: If we did this physically, it might be a long time before the $1,000,000,000^{th}$ block fell over! There is a subtle difference between "all the blocks fall over" and "for any given block, ultimately it falls over". If you go a lot further in mathematics you will encounter situations where that difference matters, but for our purposes here we will consider them the same.

Now switching to a very formal notation, we could describe proving something by induction this way: There is some statement $P(n)$ which for numbers n (in some set, e.g. the positive whole numbers that are at least 2) is either true or false. Suppose there is some number n_0 for which $P(n_0)$ is true. Suppose also that whenever $k \geq n_0$, if $P(k)$ is true then $P(k+1)$ has to be true also. Then we can claim that $P(n)$ is true for every $n \geq n_0$. Establishing that $P(n_0)$ is true is called "the basis" of the induction, and

establishing that $P(k)$ being true imples that $P(k+1)$ has to be true is called "the inductive step". You can see how that resembles the falling blocks. The basis pushes over the first block, and the inductive step guarantees that each block pushes over the next one.

(If you are interested in where mathematical truth comes from, you might wonder what right I have to say "Then we can claim ...". We can't really go into that here: We would have to dig into what numbers really are! Fundamentally this comes down to a property of the whole numbers called "well ordering".)

So enough of this generality, let's use induction to prove Corollary 1.1. The actual statement is

Corollary 1.1
If A_1, $A_2, \ldots,$ A_r are nonsingular matrices, then $A_1A_2\cdots A_r$ is nonsingular and $(A_1A_2\cdots A_r)^{-1} = A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}$.

That is really a statement about a number r. It might be true for some values of r and false for others. In fact it does not even make sense unless (a) r is a whole number (What would it mean to multiply $3\frac{1}{2}$ matrices?) and (b) r is at least 2 (Again, what would the product of fewer than 2 matrices mean? I suppose you could define the product of 1 matrix to be just that matrix, and occasionally that is actually useful, but we don't need it here.) So, although the authors did not write it out, there is an implied "for whole numbers r that are at least 2" built into the statement. But that is good: Remember that proof by induction works for statements about whole numbers with some starting point.

(There is actually another statement lurking here that was not spelled out: "nonsingular" was only defined for square matrices, so we need to know $A_1A_2\cdots A_r$ is square before the rest of the statement even makes sense! So one thing we could do, to be very careful, would be to introduce another claim, called a lemma because it would be used to help prove this result, that the product of r matrices, each one $n \times n$, is also $n \times n$! I won't be that careful, but the case $r = 2$, the product of <u>two</u> square matrices, is built into the definition of matrix multiplication on page 22, and then a proof by induction could be used to get from that to any greater number of matrices. But I won't belabor this, we will assume we know that the product $A_1A_2\cdots A_r$ is $n \times n$.)

Now what do we really have to show? The second claim in the statement of the corollary is really the heart of it: $(A_1A_2\cdots A_r)^{-1} = A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}$. To be nonsingular, a matrix just has to <u>have</u> an inverse. If we can show that $A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}$ does the right thing to be the inverse of $A_1A_2\cdots A_r$, then $A_1A_2\cdots A_r$ will have $A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}$ as its inverse, the second claim, and so will be nonsingular, the first claim. So what we have to show is that $\left(A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}\right)(A_1A_2\cdots A_r) = I_n$ and $(A_1A_2\cdots A_r)\left(A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}\right) = I_n$.

Now a question that is fundamental to proving things: Can't we get away by just saying that is obvious? I mean come on! We can see that in the middle of the first product we have A_1 right next to A_1^{-1}, so those cancel out, and then we can cancel the A_2 and A_2^{-1} that will then be next to each other, etc. And in the second product we can cancel A_r^{-1} and A_r, and again work our way out. It is <u>obvious</u>! But "obvious" is a very nasty word. What is obvious to one person may not be to another: That does not make the second person stupid, it may mean he/she just has a higher standard of checking things. And what is obvious to you today may be very puzzling when you look back at it tomorrow. For many purposes I would say that we could indeed call this obvious. I expect that may well have been all the authors expected as an answer to problem 44, that you go this far to show you know what is required and then say that the results are evident. But that is exactly why this is a good proof to use in demonstrating induction, we can concentrate on the mechanics and not on something puzzling about why the statement is really true. So I will use induction to show those two equations are true, for any particular $r \geq 2$.

In fact I will just do half of that. What I propose to write out fairly carefully is the inductive proof that for any whole number $r \geq 2$, $\left(A_r^{-1}A_{r-1}^{-1}\cdots A_1^{-1}\right)(A_1A_2\cdots A_r) = I_n$.

For the basis of the induction we show the statement is true for $r = 2$: But that is exactly Theorem 1.6, except that in the theorem the matrices were called A and B rather than A_1 and A_2. So (typical for a corollary) the theorem establishes that case.

Now suppose we know $\left(A_k^{-1}A_{k-1}^{-1}\cdots A_1^{-1}\right)(A_1A_2\cdots A_k) = I_n$ is true for some particular k (at least 2), which means that the product of the inverses (of <u>any</u> k matrices) in the opposite order is the inverse of the product of the k matrices. For the inductive <u>step</u> we want to show that it must follow that the corresponding statement is true for any $k+1$ matrices. I.e. we must show that for any $k+1$ nonsingular

$n \times n$ matrices $A_1,\ A_2, \ldots, A_k, A_{k+1}$, $\left(A_{k+1}^{-1} A_k^{-1} \cdots A_1^{-1}\right)(A_1 A_2 \cdots A_{k+1}) = I_n$.

We are assuming associativity, so I can rewrite the product $\left(A_{k+1}^{-1} A_k^{-1} \cdots A_1^{-1}\right)(A_1 A_2 \cdots A_{k+1})$ with parentheses arranged as $A_{k+1}^{-1}\left(\left(A_k^{-1} \cdots A_1^{-1}\right)(A_1 A_2 \cdots A_k)\right) A_{k+1}$.

Now the product inside the outermost parentheses is exactly what we had above in the assumption that it all worked for k matrices, $\left(A_k^{-1} A_{k-1}^{-1} \cdots A_1^{-1}\right)(A_1 A_2 \cdots A_k) = I_n$. So we have the product of just three matrices, A_{k+1}^{-1}, I_n, and A_{k+1}. We can write that with parentheses wherever we need them (the associativity assumption again), e.g. $\left(A_{k+1}^{-1} I_n\right) A_{k+1}$. But I_n multiplied on the right of any matrix (of a size such that the product exists, in this case $n \times n$) gives just that matrix as the result, so this is the same as $A_{k+1}^{-1} A_{k+1}$ which (by the definition of the inverse of a matrix) gives I_n, and we have established the induction step. Hence the claim about the one product is proved by mathematical induction. The other product is proved similarly.

That was a lot of work to prove something that we thought was pretty obvious. So a key question that you need to think about is this: For homework/quizzes/exams in this course, how much detail do you need to put into a proof? There is no crisp answer. Someone said that "a proof is whatever it takes to convince whomever you have to convince" that something is true. For homework, etc., you really don't generally have to convince the grader that the result is true, he/she already knows that! What you do have to convince the grader of is that you know why it is true, that you understand the definitions involved, etc. And what you have to say to make that clear is itself not so clear. It is surely always safer to err on the side of being too careful, too detailed. But it is not the case that just piling on lots of words or symbols is good, that (in addition to irritating the grader, who has finite time!) may lead the grader to believe you don't really know what you are doing. So one thing you should be picking up from homework, from examples done in class, from questions and answers in discussion, etc., is a calibration on what you need to say to be convincing. (If you find that unsettling, if you have always believed that in math everything has a nice crisp answer, welcome to reality! This is no worse than writing a paper in some other course, where the amount of detail and the kind of logic you must use in arguing are not well defined. At least in math we do have pretty well defined what the logic is. And if you ever expect to use math in "the real world", let me assure you on the basis of my own experience that most problems won't have just one right answer, let alone just one way to do them!)