

Math 331 Fall 2026, Lecture 5: Powers

website: <https://www.cip.ifi.lmu.de/~grinberg/t/26fa/>

(GPT-6 was used to polish the writing that follows, and to draw pictures.)

1.7. Powers

1.7.1. Definition of the n -th power

We have defined the product of n elements of a semigroup. If these n elements are all equal to a single element a , this product is called a power, just as for numbers. Again, just as for numbers, we can extend this definition to $n = 0$ when there is a neutral element, and to negative n when a is invertible:

Definition 1.7.1. Let S be a semigroup (written multiplicatively), and let $a \in S$ be arbitrary.

(a) For any positive integer n , we define

$$a^n := \underbrace{aa \cdots a}_{n \text{ times}}.$$

(Thus, $a^1 = a$ and $a^2 = aa$ and $a^3 = aaa$ and so on.)

(b) If S is a monoid, then we define

$$a^0 := 1 \quad (\text{the neutral element of } S).$$

Thus, in this case, a^n is defined for all $n \in \mathbb{N}$ (where $\mathbb{N} = \mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}$ is the set of all nonnegative integers).

(c) If S is a monoid and a has an inverse, then we define

$$a^n := (a^{-1})^{-n} \quad \text{for all negative integers } n.$$

Thus, in this case, a^n is defined for all $n \in \mathbb{Z}$.

We refer to a^n as the n -th power of a .

(The attentive reader will have noticed that we have previously defined a^{-1} to mean the inverse of a , whereas now a^{-1} acquires a new meaning thanks to Definition 1.7.1 (c). Have we given the same name to two different things? No, because the new meaning of a^{-1} agrees precisely with its old meaning. Indeed, Definition 1.7.1 (c) (applied to $n = -1$) yields $a^{-1} := (a^{-1})^{-(-1)}$, where the a^{-1} on the left-hand side is the new meaning while the a^{-1} on the right-hand side is the old one. Since $(a^{-1})^{-(-1)} = (a^{-1})^1 = a^{-1}$, this is saying that the new a^{-1} equals the old a^{-1} , and everything is good.)

1.7.2. Laws of exponents: nonnegative powers

What rules do you expect the powers to satisfy? For powers of numbers, we know the laws of exponents:

- We have $a^n a^m = a^{n+m}$.
- We have $(a^n)^m = a^{nm}$.
- We have $a^{-n} = (a^{-1})^n$ (when a has an inverse).
- We have $(ab)^n = a^n b^n$.

We will soon see which of these laws still hold for elements of a semigroup (potentially assuming that an inverse exists). Not all of them do! Can you tell which ones don't?

Let us prove them one by one (the ones that do hold). We start with the ones that don't involve inverses or negative powers, as they are the easiest.

Convention 1.7.2. All semigroups (and thus all monoids and groups) in this section will be written multiplicatively. In particular, their neutral elements, when they exist, will be denoted by 1. The inverse a^{-1} of an element a (when it exists) thus satisfies $aa^{-1} = a^{-1}a = 1$.

Theorem 1.7.3. Let S be a semigroup. Let $a \in S$. Then:

- (a) For any positive integers n and m , we have $a^n a^m = a^{n+m}$.
- (b) Assume that S is a monoid. Then, $a^n a^m = a^{n+m}$ holds for all nonnegative integers n and m .

Proof.

- (a) Let n and m be two positive integers. Generalized associativity (Theorem 1.4.2 (a) from Lecture 4, applied to $n + m$ and n instead of n and k) yields

$$\underbrace{a * a * \cdots * a}_{n+m \text{ times}} = \underbrace{(a * a * \cdots * a)}_{n \text{ times}} * \underbrace{(a * a * \cdots * a)}_{m \text{ times}}.$$

Since we are writing S multiplicatively, this equality takes the form

$$\underbrace{aa \cdots a}_{n+m \text{ times}} = \underbrace{(aa \cdots a)}_{n \text{ times}} \underbrace{(aa \cdots a)}_{m \text{ times}}.$$

But this is saying precisely that $a^{n+m} = a^n a^m$ (since we defined the positive powers a^k to be $\underbrace{aa \cdots a}_{k \text{ times}}$). This proves part (a) of the theorem.

- (b) Let n and m be two nonnegative integers. We must prove that $a^n a^m \stackrel{?}{=} a^{n+m}$. If both n and m are positive, then this follows from part (a). It remains to handle the cases when $n = 0$ and when $m = 0$. If $n = 0$, then the claim $a^n a^m \stackrel{?}{=} a^{n+m}$ becomes $a^0 a^m \stackrel{?}{=} a^{0+m}$, that is, $1a^m \stackrel{?}{=} a^m$, which is true because 1 is neutral. The case $m = 0$ can be handled similarly. $\square$

Theorem 1.7.4. Let S be a semigroup. Let $a \in S$. Then:

- (a) For any positive integers n and m , we have $(a^n)^m = a^{nm}$.
 (b) Assume that S is a monoid. Then, $(a^n)^m = a^{nm}$ holds for all nonnegative integers n and m .

Proof.

- (a) Fix a positive integer n . We induct on m . The *base case* (the case $m = 1$) says that $(a^n)^1 = a^{n \cdot 1}$, which is clearly true (both sides are a^n). For the *induction step* (from m to $m + 1$), we fix a positive integer m and assume that $(a^n)^m = a^{nm}$; and we set out to prove that $(a^n)^{m+1} \stackrel{?}{=} a^{n(m+1)}$. We note that Theorem 1.7.3 (a) (applied to a^n , m and 1 instead of a , n and m) yields $(a^n)^m (a^n)^1 = (a^n)^{m+1}$. Hence,¹

$$\begin{aligned} (a^n)^{m+1} &= \underbrace{(a^n)^m}_{\substack{= a^{nm} \\ \text{(by the IH)}}} \underbrace{(a^n)^1}_{= a^n} \\ &= a^{nm} a^n = a^{nm+n} \quad (\text{by Theorem 1.7.3 (a)}) \\ &= a^{n(m+1)} \quad (\text{since } nm + n = n(m+1)), \end{aligned}$$

which is precisely what we wanted to prove. Thus, the induction is complete, and part (a) is proved.

- (b) This is analogous to part (a), with just two changes: Instead of using Theorem 1.7.3 (a), we must now use Theorem 1.7.3 (b) (since n and m can be 0). Moreover, the base case is now the case $m = 0$ (not $m = 1$), but is equally easy because it boils down to $1 = 1$ (since the 0-th power of any element of S is defined to be 1). $\square$

Next, we could try to prove the rule $(ab)^n = a^n b^n$ for all $a, b \in S$ and $n > 0$; but we would soon hit a hurdle: even for $n = 2$, we cannot transform $(ab)^2 = abab$ into $a^2 b^2 = aabb$ without swapping factors, which is not allowed by our axioms. And in fact, $(ab)^n = a^n b^n$ is not generally true in a semigroup, or even in a group. Here is a counterexample:

¹The shorthand “IH” means “induction hypothesis”.

Example 1.7.5. Let S_3 be the group of all bijective maps from $\{1, 2, 3\}$ to $\{1, 2, 3\}$ with respect to composition (that is, fg means $f \circ g$). These bijective maps are called the *permutations* of $\{1, 2, 3\}$, and we will learn more about them soon. Consider the two specific permutations $s_1 \in S_3$ and $s_2 \in S_3$ given by

$$\begin{array}{lll} s_1(1) = 2, & s_1(2) = 1, & s_1(3) = 3, \\ s_2(1) = 1, & s_2(2) = 3, & s_2(3) = 2. \end{array}$$

Then, $s_1^2 = s_1 s_1 = s_1 \circ s_1 = \text{id} = 1$ and similarly $s_2^2 = 1$. But $s_1 s_2$ is the 3-cycle that sends 1, 2, 3 to 2, 3, 1, respectively; its square $(s_1 s_2)^2$ is the other 3-cycle that sends 1, 2, 3 to 3, 1, 2, respectively. So $(s_1 s_2)^2 \neq 1$ but $s_1^2 s_2^2 = 1 \cdot 1 = 1$. Thus, $(ab)^2 = a^2 b^2$ does not hold for $a = s_1$ and $b = s_2$.

So we cannot expect $(ab)^n = a^n b^n$ as a general rule. However, it does hold when a and b commute, i.e., when $ab = ba$. That is:

Theorem 1.7.6. Let S be a semigroup. Let $a, b \in S$ be such that $ab = ba$. Then,

$$(ab)^n = a^n b^n \quad \text{for each } n \in \mathbb{Z}_{>0}. \quad (1)$$

This also holds for $n = 0$ if S is a monoid.

We defer the proof of this theorem until later.

Also, there is a problem on homework set #1 that claims that (1) holds when ab is central, i.e., when ab commutes with all elements of S .

1.7.3. Laws of exponents: negative powers

Now we come to the rules of exponents that contain inverses. We begin with the most basic one:

Theorem 1.7.7. Let S be a monoid. Let $a \in S$ have an inverse. Then,

$$a^{-n} = (a^{-1})^n \quad \text{for each } n \in \mathbb{Z}.$$

Proof. Let $n \in \mathbb{Z}$. We must prove that $a^{-n} \stackrel{?}{=} (a^{-1})^n$. We distinguish between three cases, depending on the sign of the integer n :

Case 1: We have $n > 0$. In this case, $-n$ is negative, so the definition of a^{-n} (see Definition 1.7.1 (c)) yields $a^{-n} = (a^{-1})^{-(-n)} = (a^{-1})^n$, which is precisely our claim.

Case 2: We have $n = 0$. In this case, our claim just says $a^{-0} \stackrel{?}{=} (a^{-1})^0$, which is simply saying that $1 = 1$.

Case 3: We have $n < 0$. The element a^{-1} is itself invertible, with inverse a , by Theorem 1.3.5 (a) from Lecture 2–3. Thus, negative powers of a^{-1} are defined, and we can apply Definition 1.7.1 (c) to a^{-1} instead of a . This gives

$$\left(a^{-1}\right)^n = \left(\underbrace{\left(a^{-1}\right)^{-1}}_{=a}\right)^{-n} = a^{-n},$$

so that $a^{-n} = \left(a^{-1}\right)^n$. But this is precisely our claim.

Thus, we have proved Theorem 1.7.7 in all three cases. $\square$

The following lemma will be used in the proof of Theorem 1.7.9 below:

Lemma 1.7.8. Let S be a monoid. Let $a \in S$ have an inverse. Then:

- (a) We have $a^n a = a^{n+1}$ for all $n \in \mathbb{Z}$.
- (b) We have $aa^n = a^{n+1}$ for all $n \in \mathbb{Z}$.

Proof.

- (a) Let $n \in \mathbb{Z}$. We must prove that $a^n a \stackrel{?}{=} a^{n+1}$. We again distinguish between three cases: $n > -1$ and $n = -1$ and $n < -1$.

Case 1: We have $n > -1$. Thus, $n \geq 0$ (since n is an integer). Therefore, we can apply Theorem 1.7.3 (b) to $m = 1$. This yields $a^n a^1 = a^{n+1}$; in other words, $a^n a = a^{n+1}$ (since $a^1 = a$). Thus, we are done in Case 1.

Case 2: We have $n = -1$. Thus, $n + 1 = 0$, so that our claim $a^n a \stackrel{?}{=} a^{n+1}$ rewrites as $a^{-1} a \stackrel{?}{=} a^0$. But this is true because both sides of this equality are 1.

Case 3: We have $n < -1$. In this case, both n and $n + 1$ are negative, so that the respective powers a^n and a^{n+1} are defined by $a^n = (a^{-1})^{-n}$ and $a^{n+1} = (a^{-1})^{-(n+1)}$ (see Definition 1.7.1 (c)). Therefore, the desired claim $a^n a \stackrel{?}{=} a^{n+1}$ rewrites as

$$\left(a^{-1}\right)^{-n} a \stackrel{?}{=} \left(a^{-1}\right)^{-(n+1)}.$$

Moving the a onto the right-hand side (using Theorem 1.6.1 (b) from Lecture 4, applied to $b = (a^{-1})^{-n}$ and $c = (a^{-1})^{-(n+1)}$), we see that this claim is equivalent to

$$\left(a^{-1}\right)^{-n} \stackrel{?}{=} \left(a^{-1}\right)^{-(n+1)} a^{-1}.$$

If we set $b := a^{-1}$ and $k := -(n+1)$ (this is a nonnegative integer because $n < -1$), then we can rewrite this as

$$b^{k+1} \stackrel{?}{=} b^k b$$

(since $k = -(n+1)$ entails $k+1 = -(n+1)+1 = -n$). But this follows easily from Theorem 1.7.3 **(b)**: Indeed, k is nonnegative, so that Theorem 1.7.3 **(b)** (applied to b, k and 1 instead of a, n and m) yields $b^{k+1} = b^k b^1 = b^k b$.

(b) This follows by reading all products in the proof of part **(a)** right-to-left. (For example, instead of “ $(a^{-1})^{-(n+1)} a^{-1}$ ”, read “ $a^{-1} (a^{-1})^{-(n+1)}$ ”). $\square$

We can now extend Theorem 1.7.3 to negative powers of a , provided that a has an inverse:

Theorem 1.7.9. Let S be a monoid. Let $a \in S$ have an inverse. Then,

$$a^n a^m = a^{n+m} \quad \text{for all integers } n \text{ and } m.$$

Proof. Fix $n \in \mathbb{Z}$. We must prove that $a^n a^m = a^{n+m}$ for all integers m .

We do this by two-sided induction on m . Recall that **two-sided induction** is an analogue of the usual method of induction that can be used to prove a statement for **all** integers (not just for the nonnegative ones, or the ones that are $\geq g$ for a given lower bound g). It proceeds as follows: If we want to prove a certain statement $\mathcal{A}(m)$ for all integers m , then we must show that

1. it holds for **some** integer m (we often take $m = 0$, but we can just as well take any other integer), and that
2. for each integer m , the **equivalence** $\mathcal{A}(m) \iff \mathcal{A}(m+1)$ holds (i.e., that $\mathcal{A}(m)$ implies $\mathcal{A}(m+1)$ but also the other way round).

The first of these two steps is called the *base case*; the second is called the (*two-sided*) *induction step*. Unlike in regular induction, the induction step requires proving the equivalence $\mathcal{A}(m) \iff \mathcal{A}(m+1)$ rather than merely the implication $\mathcal{A}(m) \implies \mathcal{A}(m+1)$. As a consequence, if we have shown $\mathcal{A}(0)$ as our base case, then we obtain both chains of implications

$$\begin{aligned} \mathcal{A}(0) &\implies \mathcal{A}(1) \implies \mathcal{A}(2) \implies \dots, \\ \mathcal{A}(0) &\implies \mathcal{A}(-1) \implies \mathcal{A}(-2) \implies \dots. \end{aligned}$$

These two chains together entail that $\mathcal{A}(m)$ holds for all integers m .

So let us apply this to our situation, in which the statement $\mathcal{A}(m)$ that we must prove is saying that $a^n a^m = a^{n+m}$. We prove this by two-sided induction. As the *base case*, we pick the case $m = 0$; that is, we show that $\mathcal{A}(0)$ holds.

This boils down to the identity $a^n a^0 = a^{n+0}$, which is indeed true because $a^n \underbrace{a^0}_{=1} = a^n 1 = a^n$ and $a^{n+0} = a^n$. For the *induction step*, we fix an integer m ; we must then prove the equivalence $\mathcal{A}(m) \iff \mathcal{A}(m+1)$. However, the statement $\mathcal{A}(m+1)$ says that $a^n a^{m+1} = a^{n+m+1}$. Meanwhile, Lemma 1.7.8 tells us that $a^m a = a^{m+1}$ and $a^{n+m} a = a^{n+m+1}$. Now, we have the following chain of equivalences:

$$\begin{aligned} \mathcal{A}(m+1) &\iff \left(a^n \underbrace{a^{m+1}}_{=a^m a} = \underbrace{a^{n+m+1}}_{=a^{n+m} a} \right) \\ &\iff (a^n a^m a = a^{n+m} a) \\ &\iff (a^n a^m = a^{n+m}) \quad (\text{see below}) \\ &\iff \mathcal{A}(m). \end{aligned}$$

(The third equivalence here is obtained by right cancellation of a , which is legitimate because a has an inverse. More precisely, it is Theorem 1.6.1 (d) from Lecture 4, applied to $b = a^n a^m$ and $c = a^{n+m}$.) In other words, we have $\mathcal{A}(m) \iff \mathcal{A}(m+1)$. But this is precisely what we had to prove in order to complete our induction step. Thus, we are done with the induction and thus with the proof of the theorem. $\square$

In order to extend the $(a^n)^m = a^{nm}$ rule (Theorem 1.7.4) to negative n 's and m 's, we must first show that the existence of an inverse is inherited by the powers of an element. That is:

Lemma 1.7.10. Let S be a monoid. Let $a \in S$ have an inverse. Let $n \in \mathbb{Z}$. Then, a^n has an inverse, and this inverse is $(a^n)^{-1} = a^{-n}$.

Proof. Theorem 1.7.9 gives

$$a^n a^{-n} = a^{n+(-n)} = a^0 = 1 \quad \text{and} \quad a^{-n} a^n = a^{(-n)+n} = a^0 = 1.$$

These two equalities show that a^{-n} is an inverse of a^n . This proves Lemma 1.7.10. $\square$

Now we can state our negative version of Theorem 1.7.4:

Theorem 1.7.11. Let S be a monoid. Let $a \in S$ have an inverse. Then,

$$(a^n)^m = a^{nm} \quad \text{for all integers } n \text{ and } m.$$

Proof. This will be on homework set #2. $\square$

We can extend Theorem 1.7.6 as well:

Theorem 1.7.12. Let S be a monoid. Let $a, b \in S$ be two elements that have inverses and satisfy $ab = ba$. Then,

$$(ab)^n = a^n b^n \quad \text{for each } n \in \mathbb{Z}.$$

Proof. This will be on homework set #2. □

All the above results about semigroups and monoids can, of course, be applied to groups. In this setting, they become even easier to state, because we no longer need to require our elements to have inverses; after all, every element in a group has an inverse by definition. We will mostly use these results in the setting of a group.

1.7.4. Powers in finite semigroups

For **finite** semigroups, the powers of a given element form an eventually periodic sequence (not necessarily periodic from the start):

Theorem 1.7.13. Let S be a **finite** semigroup. Let $a \in S$. Then:

- (a) There exist positive integers $n > m$ such that $a^n = a^m$.
- (b) The sequence $(a^1, a^2, a^3, \dots)$ is periodic from some point on. That is, there exist positive integers m and p such that all $k \geq m$ satisfy $a^k = a^{k+p}$.

Proof.

- (a) Set $N := |S|$, the number of elements of S . (This is an actual integer, since S is finite.) The $N + 1$ elements

$$a^1, a^2, \dots, a^{N+1}$$

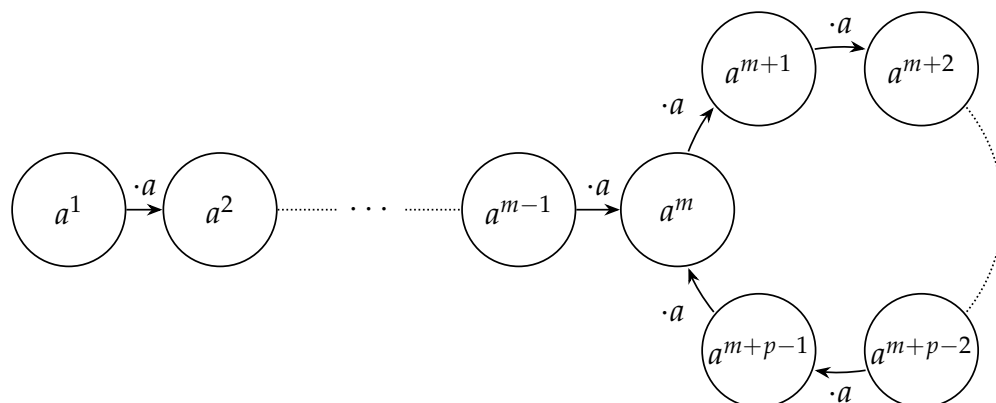
all belong to the N -element set S . Thus, two of them must be equal (since the pigeonhole principle says that $N + 1$ elements in an N -element set cannot all be distinct). In other words, there are integers $1 \leq m < n \leq N + 1$ such that $a^n = a^m$. This proves part (a).

- (b) Part (a) tells us that there exist positive integers $n > m$ such that $a^n = a^m$. Consider them, and set $p := n - m$. Then, $n = m + p$, so that $a^n = a^{m+p}$ and therefore $a^{m+p} = a^n = a^m$. So the equality $a^k = a^{k+p}$ holds at least for $k = m$. However, if this equality holds for a given integer $k \geq m$, then it holds for $k + 1$ as well, because Theorem 1.7.3 (a) yields

$$\begin{aligned} a^{k+1} &= \underbrace{a^k}_{=a^{k+p}} a^1 = a^{k+p} a^1 = a^{k+p+1} && \text{(again by Theorem 1.7.3 (a))} \\ &= a^{k+1+p}. \end{aligned}$$

Thus, by induction, it holds for all $k \geq m$. This proves part (b). □

Remark 1.7.14. The following picture visualizes the powers of an arbitrary element a in a finite semigroup:



Here, the nodes are the (positive) powers of a ; each solid arrow means right multiplication by a . Repeated multiplication by a eventually leads us into a cycle, as Theorem 1.7.13 (a) predicts. Note that it can happen that a^1 is already part of that cycle; in this case, the “tail” (the part of the chain from a^1 to a^m) is reduced to a single node. Also, it is possible that the cycle consists of just a single node (i.e., that $a^m = a^{m+1}$) with an arc looping directly back into it.

For an element with an inverse (in a monoid), Theorem 1.7.13 can be improved, yielding a **purely** periodic sequence:

Theorem 1.7.15. Let S be a **finite** monoid. Let $a \in S$ have an inverse. Then:

- (a) There exists a positive integer n such that $a^n = 1$.
- (b) The sequence $(a^0, a^1, a^2, \dots)$ is purely periodic (i.e., the period starts right away). That is, there exists some positive integer n such that all $k \geq 0$ satisfy $a^k = a^{k+n}$.

Proof.

- (a) Theorem 1.7.13 (a) tells us that there exist positive integers $n > m$ such that $a^n = a^m$. Consider these n and m , and set $p := n - m > 0$. Then, $n = m + p$, so that $a^n = a^{m+p} = a^m a^p$ (by Theorem 1.7.3 (a)). Comparing this with $a^n = a^m = a^m 1$, we obtain

$$a^m a^p = a^m 1. \quad (2)$$

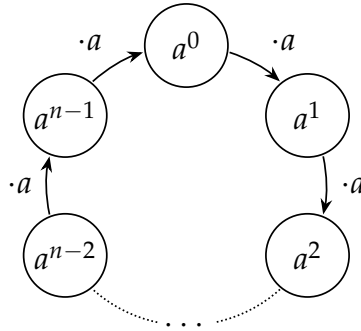
But a has an inverse, so a^m also has an inverse (by Lemma 1.7.10, applied to m instead of n). Hence, we can cancel a^m in the equality (2) (i.e., apply Theorem 1.6.1 (c) in Lecture 4 to a^m , a^p and 1 instead of a , b and c). Thus, we obtain $a^p = 1$. So we have found a positive integer n such that $a^n = 1$ (but it's our p , not our n). Hence, such an n exists. This proves part (a) of the theorem.

- (b) Part (a) shows that there exists a positive integer n such that $a^n = 1$. Consider this n . Then, Theorem 1.7.3 (b) shows that every $k \geq 0$ satisfies

$$a^{k+n} = a^k \underbrace{a^n}_{=1} = a^k 1 = a^k,$$

and therefore $a^k = a^{k+n}$. This proves part (b). $\square$

Remark 1.7.16. Similarly to Remark 1.7.14, we can visualize the powers of an arbitrary element a in a finite monoid that has an inverse:



Here, we only have a cycle, no tail leading into it, since Theorem 1.7.15 (a) tells us that the powers eventually loop back into $1 = a^0$.