**Theorem:** Let $(A, *)$ be a monoid, and let $a \in A$ be invertible. Then $a^m * a^n = a^{m+n}$ $\forall m, n \in \mathbb{Z}$.

**Proof:** When $m \geq 0$ and $n \geq 0$, we have already proven this result. The rest of the proof splits into cases.

**Case 1:** $m = 0$ or $n = 0$

If $m = 0$, $n \in \mathbb{Z}$, $a^m * a^n = a^0 * a^n = e * a^n = a^n = a^{0+n}$ as needed.

If $m \in \mathbb{Z}$, $n = 0$, $a^m * a^n = a^m * a^0 = a^m * e = a^m = a^{m+0}$ as needed.

**Case 2:** $m < 0$ and $n < 0$

$m < 0 \Rightarrow \exists p \in \mathbb{N}\ s.t.\ p = -m$. $n < 0 \Rightarrow \exists q \in \mathbb{N}\ s.t.\ q = -n$.

$a^m = a^{-p} = (a^p)^{-1}$ and $a^n = a^{-q} = (a^q)^{-1}$

$a^m * a^n = (a^p)^{-1} * (a^q)^{-1} = (a^q * a^p)^{-1} = (a^{p+q})^{-1} = a^{-(p+q)} = a^{-q-p} = a^{m+n}$

**Case 3:** $m$ and $n$ have opposite signs.

Without loss of generality, assume $m < 0$ and $n > 0$ (the case $m > 0$ and $n < 0$ is handled by the same argument). Since $m < 0, \exists p \in \mathbb{N}\ s.t.\ p = -m$. This case splits into two subcases:

**Case 3.1:** $m + n \geq 0$

Set $q = m + n$. Then $a^{m+n} = a^q = e * a^q = (a^p)^{-1} * a^p * a^q = (a^p)^{-1} * a^{p+q} = a^{-p} * a^{p+q} = a^m * a^{-m+m+n} = a^m * a^n$

**Case 3.2:** $m + n < 0$

Set $q = -(m+n) = -m-n \in \mathbb{N}^*$. Then $a^{m+n} = a^{-q} = (a^q)^{-1} * e = (a^q)^{-1} * (a^{-n} * a^n) = (a^q)^{-1} * (a^n)^{-1} * a^n = (a^n * a^q)^{-1} * a^n = (a^{n+q})^{-1} * a^n = (a^{n-m-n})^{-1} * a^n = (a^{-m})^{-1} * a^n = (a^p)^{-1} * a^n = a^m * a^n$

**Theorem:** Let $(A, *)$ be a monoid, and let $a$ be an invertible element of $A$. $\forall m, n \in \mathbb{Z}, (a^m)^n = a^{mn}$.

**Proof:** We consider 3 cases:

**Case 1:** $n > 0$, **i.e.** $n \in \mathbb{N}^*$. $m \in \mathbb{Z}$ with no additional restrictions we proceed by induction on $m$.

**Base Case:** $n = 1$ $\quad (a^m)^1 = a^m = a^{m\times 1}$

**Inductive Step:** We assume $(a^m)^n = a^{mn}$ and seek to prove $(a^m)^{n+1} = a^{m(n+1)}$. Start with $(a^m)^{n+1} = (a^m)^n * (a^m)^1 = a^{mn} * a^m = a^{mn+m} = a^{m(n+1)}$

**Case 2:** $n = 0$; no restriction on $m \in \mathbb{Z}$

$(a^m)^n = (a^m)^0 = e = a^0 = a^{m\times 0} = a^{mn}$

**Case 3:** $n < 0$; no restriction on $m \in \mathbb{Z}$.

Since $n < 0, \exists p \in \mathbb{N}\, s.t.\, p = -n$. By case 1, $(a^m)^p = a^{mp}$

$(a^m)^n = (a^m)^{-p} = ((a^m)^p)^{-1} = (a^{mp})^{-1} = a^{-mp} =^{m(-p)}= a^{mn}$

## 7.6 Groups

A notion formally defined in the 1870's even though theorems about groups were proven as early as a century before that.

**Definition:** A group is a monoid in which every element is invertible. In other words, a group is a set $A$ endowed with a binary operation $*$ satisfying the following properties:

1. $*$ is associative, **i.e.** $\forall x, y, z \in A, (x * y) * z = x * (y * z)$
2. There exists an identity element $e \in A$, **i.e.** $\exists e \in A\, s.t. \forall a \in A, a * e = e * a = a$
3. Every element of $A$ in invertible, **i.e.** $\forall a \in A\ \exists a^{-1} \in A\, s.t.\, a * a^{-1} = a^{-1} * a = e$

**Notation for Groups:** $(A, *)$ or $(\underbrace{A}_{set}, \underbrace{*}_{operation}, \underbrace{e}_{identity})$

**Remark:** Closure under the operation $*$ is <u>implicit</u> in the definition **i.e.** $\forall a, b \in A, a * b \in A$

**Definition:** A group $(A, *, e)$ is called <u>commutative</u> or <u>Abelian</u> if its operation $*$ is commutative.

**Examples:**

1. $(\mathbb{R}, +, 0)$ is an Abelian group.

   $-x$ is the inverse of $x, \forall x \in \mathbb{R}$

2. $(\mathbb{Q}^*, \times, 1)$ $\qquad$ $\mathbb{Q}^* = \mathbb{Q}^* \backslash \{0\}$ $\qquad$ $(\mathbb{Q}^*, \times, 1)$ is Abelian

   $\forall q \in \mathbb{Q}^*, q^{-1} = \frac{1}{q}$ is the inverse.