Theorem: Let$(A, *)$ be a semigroup. $\forall a \in A, (a^m)^n = a^{mn}, \forall m, n \in \mathbb{N}^*$

Proof: By induction on n.

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

Inductive Step: Assume the result if true for $n = p$, **i.e.** $(a^m)^p = a^{mp}$ and seek to prove that $(a^m)^{p+1} = a^{m(p+1)}$

$(a^m)^{p+1} = (a^m)^p * a^m = a^{mp} * a^m = a^{mp+m} = a^{m(p+1)}$ by the previous theorem.

7.2.1 General Associative Law

Let $(A, *)$ be a semigroup. $\forall a_1, ..., a_s \in A, a_1 * a_2 * ... * a_s$ has the same value regardless of how the product is bracketed.

Proof Use associativity of $*$.

qed

NB: Unless $(A, *)$ has a commutative binary operation, $a_1 * a_2 * ... * a_s$ does depend on the ORDER in which the $a_j's$ appear in $a_1 * a_2 * ... * a_s$

7.3 Identity Elements

Definition: Let $(A, *)$ be a semigroup. An element $e \in A$ is called an identity element for the binary operation $*$ if $e * x = x * e = x, \forall x \in A$.

Examples:

1. $(\mathbb{R}, +)$ has 0 as the identity element.
2. $(\mathbb{R}, \times)$ has 1 as the identity element.

3. Given a set A, $(P(A), \cup)$ has $\emptyset$ (the empty set) as its identity element, whereas $(P(A), \cap)$ has A as its identity element.
4. $(M_n, *)$ has I_n, the identity matrix, as its identity element.

Theorem A binary operation on a set cannot have more than one identity element, **i.e.** if an identity element exists, then it is unique.

Proof: Assume not (proof by contradiction). Let e and e' both be identity elements for a binary operation on a set A. $e = e * e' = e'$

qed

7.4 Monoids

Definition: A monoid is a set A endowed with an associative binary operation $*$ that has an identity element e. In other words, a monoid is a semigroup $(A, *)$, where $*$ has an identity element e.

Definition: A monoid $(A, *)$ is called commutative (or Abelian) if the binary operation $*$ is commutative.

Example:

1. $(\mathbb{R}, +)$ is a commutative monoid with $e = 0$.
2. $(\mathbb{R}, \times)$ is a commutative monoid with $e = 1$.
3. Given a set A, $(P(A), \cup)$ is a commutative monoid with $e = \emptyset$.
4. $(M_n, *)$ is a monoid since $e = I_n$, but it is not commutative since matrix multiplication is not commutative.
5. $(\mathbb{N}, +)$ is a commutative monoid with $e = 0$, whereas $(\mathbb{N}^*, +)$ is merely a semigroup (recall $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$)

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

Remark: Recall that we proved this theorem for semigroups if $m, n \in \mathbb{N}^*$. We now need to extend that result.

Proof: A monoid is a semigroup $\implies \forall a \in A, a^m * a^n = a^{m+n}$ whenever $m, n \in \mathbb{N}^*$, **i.e.** $m > 0$ and $n > 0$. Now let $m = 0$. $a^m * a^n = a^0 * a^n = e * a^n = a^n = a^{0+n}$
If $n = 0, a^m * a^n = a^m * a^0 = a^m * e = a^m = a^{m+0}$.

qed

Theorem: Let $(A, *)$ be a monoid, $\forall a \in A\ \forall m, n \in \mathbb{N}$, $(a^m)^n = a^{mn}$.

Remark: Once again, we had this result for semigroups when $m > 0$ and $n > 0$.

Proof: By the remark, we only need to prove the result when $m = 0$ or $n = 0$. If $m = 0, (a^0)^n = (e)^n = e = a^0 = a^{0\times n}$. If $n = 0$, then $(a^m)^0 = e = a^0 = a^{0\times m}$.

qed