7.5 Inverses

Task: Understand what an inverse is and what formal properties it satisfies.

Definition: Let $(A, *)$ be a monoid with identity element e and let $a \in A$. An element y of A is called the inverse of x if $x * y = y * x = e$. If an element $a \in A$ has an inverse, then a is called invertible.

Examples:

1. $(\mathbb{R}, +)$ has identity element 0. $\forall x \in \mathbb{R}, (-x)$ is the inverse of x since $x + (-x) = (-x) = x = 0$.
2. $(\mathbb{R}, \times)$ has identity element 1. $x \in \mathbb{R}$ is invertible only if $x \neq 0$. If $x \neq 0$, the inverse of x is $\frac{1}{x}$ since $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$.
3. $(M_n, *)$ the identity element is I_n. $A \in M_n$ is invertible if $\det(A) \neq 0$. A^{-1} the inverse is exactly the one you computed in linear algebra. If $\det(A) = 0, A$ is NOT invertible.
4. Given a set $A, (P(A), \cup)$ has $\emptyset$ as its identity element. Of all the elements of $P(A)$, only $\emptyset$ is invertible and has itself as its inverse: $\emptyset \cup \emptyset = \emptyset \cup \emptyset = \emptyset$.

Theorem: Let $(A, *)$ be a monoid. If $a \in A$ has an inverse, then that inverse is unique.

Proof: By contradiction: Assume not, then $\exists a \in A$ s.t. both b and c in A are its inverses, **i.e.** $a * b = b * a = e$, the identity element of $(A, *)$, and $a * c = c * a = e$, where $b \neq c$. Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. $\Rightarrow\Leftarrow$

qed

Since every invertible element a of a monoid $(A, *)$ has a unique inverse, we can denote the inverse by the more standard notation a^{-1}.

Next, we need to understand inverses of elements obtained via the binary operation:

Theorem: Let $(A, *)$ be a monoid, and let a, b be invertible elements of A. Then $a * b$ is also invertible, and $(a * b)^{-1} = b^{-1} * a^{-1}$.

Remark: You might remember this formula from linear algebra when you looked at the inverse of a product of matrices AB.

Proof: Let e be the identity element of $(A, *)$. $a * a^{-1} = a^{-1} * a = e$, and $b * b^{-1} = b^{-1} * b = e$. We would like to show $b^{-1} * a^{-1}$ is the inverse of $a * b$ by computing $(a * b) * (b^{-1} * a^{-1})$ and $(b^{-1} * a^{-1}) * (a * b)$ and showing both are e.

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$$

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = (b^{-1} * e) * b = b^{-1} * b = e$$

Thus $b^{-1} * a^{-1}$ satisfies the conditions needed for it to be the inverse of $a * b$. Since an inverse is unique, $a * b$ is invertible and $b^{-1} * a^{-1}$ is its inverse.

qed

Theorem: Let $(A, *)$ be a monoid, and let $a, b \in A$. Let $x \in A$ be invertible. $a = b * x \Leftrightarrow b = a * x^{-1}$. Similarly, $a = x * b \Leftrightarrow b = x^{-1} * a$

Proof: Let e be the identity element of $(A, *)$.

First $a = b * x \Leftrightarrow b = a * x^{-1}$:

"$\Rightarrow$" Assume $a = b*x$. Then $a*x^{-1} = (b*x)*x^{-1} = b*x*x^{-1} = b*e = b$ as needed.

"$\Leftarrow$" Assume $b = a*x^{-1}$. Then $b*x = (a*x^{-1})*x = a*(x^{-1}*x) = a*e = a$ as needed.

Apply the same type of argument to show $a = x * b \Leftrightarrow b = x^{-1} * a$.

qed

Let $(A, *)$ be a monoid. We can now make sense of a^n for $n \in \mathbb{Z}, n < 0$ for every $a \in A$ invertible. Since n is a negative integer, $\exists p \in \mathbb{N}$ s.t. $n = -p$. Set $a^n = a^{-p} = (a^p)^{-1}$.

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.