DEF Let $X \& Y$ be sets. The cartesian product $X \times Y$ is the set of all ordered pairs $(x,y)$ with $x \in X, y \in Y$. Ordered here means $x$ first, $y$ second. Thus e.g. in $X \times X$ $(x_1,x_2) = (x_2,x_1)$ unless $x_1 = x_2$. The corresponding (unordered) set is $\{x_1,x_2\} = \{x_2,x_1\}$.

EXAMPLE $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the set of all points in the $xy$ plane.

DEF A monoid is a set $M$, together with a map $\cdot : M \times M \to M$ called multiplication, whose value at $(a,b)$ is denoted by $ab$ or $a \cdot b$, called the product of $a \& b$; this multiplication is required to satisfy:

1. $ab, c = a \cdot (bc)$ for all $a, b, c \in M$;
2. $\exists 1 \in M$ so that $1a = a1 = a, \forall a \in M$.

Condition (1) is called associativity; an element $1$ satisfying (2) is an identity element for $M$. Thus, a monoid is a set $M$, together with an associative multiplication for which there is an identity element.

DEF Let $a \& b$ be elements of a monoid $M$. If $ab = ba$, then $a \& b$ commute. This doesn't always happen, e.g. in $(V)$ below.

EXAMPLES of monoids:

1. $\mathbb{N}^*$ with its usual multiplication, and $1 = \text{the number } 1$, is a monoid.
2. $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ similarly.
3. $\mathbb{Z}^+$ with $+$ instead of $\cdot$ and $0$ instead of $1$ is an "additive monoid.
   Here (1) & (2) are $(x+y)+z = x+(y+z)$ & $0+x = x+0 = x, \forall x,y,z \in \mathbb{Z}$.
4. For each set $X$, the set $\mathcal{P}(X)$ of all subsets of $X$, with $\cup$ (or $\cap$) as multiplication and $\emptyset$ (or $X$) as identity element is a monoid. This gives two examples (if $X \neq \emptyset$).

*) $a \cdot b \cdot c$ means "first multiply $a \& b$, then $ab \& c"; a \cdot b \cdot c$ means "first multiply $b \& c$, then $a \& bc."
(v) For each set $X$, the set $M(X) = \{ \text{all maps } f: X \to X \}$, with composition of maps as multiplication, and $1_X \circ f = f$ is a monoid, since composition, which is always defined for $f, g \in M(X)$, is associative, and $1_X \circ f = f$ for each $f \in M(X)$.

**NON-EXAMPLES** of monoids:

(i) $\mathbb{N}$ with + instead of $\circ$; no identity element.

(ii) $\mathbb{R}^2$ with dot product $\circ$ of vectors; the products are scalars, not vectors.

(iii) $\mathbb{R}^3$ with cross product $\circ$ of vectors; associativity fails, and no identity element.

**NOTATION.** Let $a, b, c$ be elements of a monoid $M$. Because of associativity, we may write simply $abc$ for $ab \circ c$ or $a \circ b \circ c$. Using associativity several times, we obtain:

\[
\begin{align*}
    a(bcd) &= a((bc)d) = (ab)(cd) = (a \circ b) \circ (c \circ d) = (abc) \circ d \\
    &\quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \ quarterly

**THM A.** For each monoid $M$ and $n \geq 2$, we define inductively

\[
    a_1, a_2, \ldots, a_n = (a_1, a_2, \ldots, a_{n-1}) \cdot a_n \quad \text{for } a_1, a_2, \ldots, a_n \in M.
\]

Then for $n \geq 2$,

\[
    a_1(a_2 \cdots a_n) = (a_1 a_2)(a_3 \cdots a_n) = \cdots = (a_1 a_2 \cdots a_{n-1}) a_n = (a_1 \cdots a_n).
\]

**Proof.** \(\Box_2\) is clear, \(\Box_3\) is the associativity law, and \(\Box_4\) is contained in the big display above. Suppose \(n > 1\), and \(\Box_n\) has been proved for \(2 \leq n < \ell\). Then for \(1 \leq m \leq \ell - 2\),

\[
    (a_1 \cdots a_m)(a_{m+1} \cdots a_\ell) = (a_1 \cdots a_m)(a_{m+1} \cdots a_{\ell-1}) a_\ell = (a_1 \cdots a_m)(a_{m+1} \cdots a_{\ell-1}) a_\ell,
\]

the second by associativity, and the first and third by \(\Box_{m+1}\) and \(\Box_{\ell-1}\). Then \(\Box_\ell\) is true.\[\square\]

\(\Box\) For vectors $u, v, w$ in $\mathbb{R}^3$, $(u \times v) \times w = u \times (v \times w) \iff u \parallel w \lor v \perp u \land w$. We end the proof.
Theorem B. Let $M$ be a monoid. Then $M$ has only one identity element.

Proof. If $\tilde{i}$ and $I$ are identity elements for $M$, then

$$\tilde{i} = \tilde{i}, \quad I = I$$

Since $I$ is an identity element, since $\tilde{i}$ is an identity element.

Definition. Let $M$ be a monoid, and let $a \in M$. An inverse for $a$ is any $a' \in M$ satisfying

$$aa' = I \text{ and } a'a = I$$

Theorem C. Let $M$ be a monoid. Then each $a \in M$ has at most one inverse.

Proof. If $a$ and $a'$ are inverses for $a$, then

$$\tilde{a} = \tilde{a} \cdot \tilde{I} = \tilde{a} \cdot a \cdot a' = \tilde{a} \cdot a' = I \cdot a' = a'$$

Property of $I$, definition of inverse, associativity, definition of inverse, property of $I$.

Notation. The inverse of $a$, if there is any, is denoted by $a^{-1}$ (not $a'$ or $\tilde{a}$).

Theorem D. Let $M$ be a monoid, let $I$ be its identity element, and let $a, b \in M$. Then:

1. $I$ has an inverse, and $I^{-1} = I$.
2. If $a$ has an inverse, so does $\tilde{a}$, and $(a^{-1})^{-1} = a$.
3. If $a$ and $b$ have inverses, so does $ab$, and $(ab)^{-1} = b^{-1}a^{-1}$.

Proof (1) The equation $I \cdot I = I$ says $I = I^{-1}$.

(2) The equations $a \cdot a^{-1} = I$ and $a^{-1} \cdot a = I$ say not only that $a^{-1}$ is the inverse of $a$, but also that $a$ is the inverse of $a^{-1}$.

(3) By associativity and properties of inverses and identity elements,

$$ab(a^{-1}b^{-1}) = a(ab^{-1})a^{-1} = a \cdot a^{-1} = a = a^{-1} = I$$

Similarly, $(a^{-1}b^{-1})(ab) = I$. Therefore $a^{-1}b^{-1}$ is an (the?) inverse for $ab$. 

DEF A group is a monoid \( G \) in which each element has an inverse.

DEF An abelian group is a group \( G \) in which \( ab = ba \) for all \( a, b \in G \).

EXAMPLES of groups.

(i) \( \mathbb{Z}_+^+ \) with +, and 0 for identity element, and -n for the inverse of \( n \), is an abelian group.

(ii) Similarly for \( \mathbb{Q}_+^+ \), \( \mathbb{R}_+^+ \), \( \mathbb{C}_+^+ \).

THM E For each monoid \( M \), the set \( M^* \) of \( M \) which have inverses, i.e., the set of invertible elements, or more briefly the units of \( M \), is a group with the same multiplication and the same identity element. \( M^* \) is the unit group of the monoid \( M \).

Proof By THM D, if \( a \cdot b \in M^* \), then \( a \cdot b \in M^* \). Clearly \( a \cdot b \cdot c = a \cdot (b \cdot c) \) for all \( a, b, c \in M^* \), \( 1 \in M^* \) and clearly \( 1 \cdot a = a \cdot 1 = a \) for all \( a \in M^+ \), so \( M^* \) is a monoid. Each \( a \in M^* \) has an inverse \( a^{-1} \) in \( M \). Since \( a^{-1} \) also has an inverse \( (a^{-1})^{-1} \) in \( M \), we have \( a^{-1} \in M^* \), and \( a \cdot a^{-1} = a^{-1} \cdot a = 1 \) shows that \( a^{-1} \) is the inverse for \( a \) in \( M^* \). Since \( M^* \) is a monoid on which each element has an inverse, \( M^* \) is a group.

EXAMPLES of unit groups of monoids.

(i) \( \mathbb{Q}^* = \mathbb{Q} \) except for 0, with \( \cdot \) and 1 and \( \frac{a}{b} \) for \( (\frac{a}{b}) \) for integer \( a, b \in \mathbb{Z} \).

(ii) \( \mathbb{R}^* \) & \( \mathbb{C}^* \) (the nonzero elements of \( \mathbb{R} \) and \( \mathbb{C} \) are the unit groups of the monoids \( \mathbb{R} \) & \( \mathbb{C} \)).

(iii) For each set \( X \), \( \mathcal{M}(X)^* \) consists of the bijective maps \( f : X \to X \).

EXERCISE 1: Prove statement (iii), and show that for \( f \in \mathcal{M}(X)^* \), the inverse \( f^{-1} \) is the inverse map.

NON-EXAMPLES of groups.

(i) \( \mathbb{N}^* \) with \( \cdot \), because, e.g., 2 has no inverse \( (\frac{1}{2} \in \mathbb{Q} \) but \( \frac{1}{2} \notin \mathbb{N} \)).

(ii) \( \mathcal{A}(X) \) with \( \cup \) (or \( \cap \)) with \( X \neq \emptyset \), because \( X \cup A = X \) (or \( \phi \cap A = \emptyset \)) for no \( A \subset X \).
NOTATION The bijections \( f : X \to X \) are also called permutations of \( X \), and \( M(X)^* \) is also called the symmetric group on \( X \), and denoted by \( S_X \).

**Thm F.** If \( |X| = n \in \mathbb{N} \), then \( |S_X| = n! \).

**Proof.** It is more convenient to prove by induction that if \( |X| = |Y| = n \), there are exactly \( n! \) bijections from \( X \) to \( Y \). The case \( n = 1 \) is clear, so let \( n > 1 \) and assume this is true for \( n-1 \). Pick any \( x \in X \). Each bijection \( f : X \to Y \) sends \( x \) to some \( y \in Y \), and is determined by this \( y \), together with the bijection, gotten from \( f \), from \( X - \{x\} \) to \( Y - \{y\} \). Since there are \( n \) choices for \( y \), and, by induction, \((n-1)! \) bijections from \( X - \{x\} \) to \( Y - \{y\} \), there are \( n \cdot (n-1)! = n! \) bijections from \( X \) to \( Y \).

**Exercise 2.** Let \( G \) be a group, and let \( a, b, c \in G \) with \( ac = bc \). Prove \( a = b \).

**Exercise 3.** Let \( M \) be a monoid, let \( n \in \mathbb{N} \), and suppose \( a_1, \ldots, a_n \in M^* \). Prove that \((a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1} \).

**Exercise 4.** There are 5 ways (boxed in the big display on 7.2) of writing abcd, using multiplication \( \times \) factors "two at a time." More generally, Catalan in 1838 proved that the analogous number \( c_n \) for \( a \ldots a_n \) is given by

\[
\begin{align*}
\star & \\
\star & \mathcal{C}_n = \frac{(2n-2)!}{(n-1)! \cdot n!}.
\end{align*}
\]

Verify that \( \star \) is correct for \( n = 4 \), and show that, in agreement with \( \star \), \( \mathcal{C}_5 = 14 \) by making a complete list of all 14 ways of writing abcd analogous to the 5 ways of writing abcd. Setting \( c_1 = 1 \) and \( c_2 = 2 \) prove that for all \( n \geq 2 \),

\[
\star \star \mathcal{C}_n = c_1 \mathcal{C}_{n-1} + c_2 \mathcal{C}_{n-2} + \cdots + c_{n-1} \mathcal{C}_1.
\]

Optional (not to be graded): By considering \( C(x) = \sum_{n=1}^{\infty} \mathcal{C}_n x^n \), use \( \star \star \) to express \( C(x) \) as an elementary function, then use Taylor's coefficient formula to get \( \star \).