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 eg. in $X \times X$ $(x_1, x_2) \neq (x_2, x_1)$ 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 from $M \times M$ to M called multiplication, whose value at (a, b) is denoted by ab or $a.b$, called the product of a & b; this multiplication is required to satisfy

(1)* $ab.c = a.bc$ for all $a, b, c \in M$;

(2) $\exists\, 1 \in M$ so that $1.a = a.1 = a$, $\forall a \in M$.

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, eg. in (v) below

EXAMPLES of monoids:

(i) $\mathbb{N}^\times$ with its usual multiplication, and 1 = the number 1, is a monoid.

(ii) $\mathbb{Z}^\times$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ similarly.

(iii) $\mathbb{Z}^+$ with $+$ instead of $\cdot$ and 0 instead of 1 is an "additive" monoid. Here (1) & (2) are $(x+y)+z = x+(y+z)$ & $0+x = x+0 = x$, $\forall x, y, z \in \mathbb{Z}$.

(iv) For each set X, the set $\mathcal{S}(X)$ of all subsets of X, with $\cup$ (or $\cap$) as multiplication and ϕ (or X) as identity element is a monoid. This gives two examples (if $X \neq \phi$).

*) $ab.c$ means "first multiply a & b, then ab & c"; $a.bc$ means "first multiply b&c, then a & bc."

(v) For each set X, the set $\mathcal{M}(X) = \{\text{all maps } f : X \to X\}$, with composition of maps as multiplication, and 1_X as 1, is a monoid, since composition, which is always defined for $f, g \in \mathcal{M}(X)$, is associative, and $1_X f = f 1_X$ for each $f \in \mathcal{M}(X)$.

NON-EXAMPLES of monoids.

(i) $\mathbb{N}$ with $+$ instead of $\cdot$: no identity element

(ii) $\mathbb{R}^3$ with dot product of vectors : the products are scalars, not vectors.

(iii) $\mathbb{R}^3$ with cross product 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 $ab.c$ or $a.bc$. Using associativity several times,

big display
$$a(bcd) = \boxed{\begin{matrix} a(b.cd) = (ab)(cd) = (a.bc).d \\ \| \qquad\qquad\qquad\qquad \| \\ a(bc.d) \qquad\qquad\qquad (ab.c)d \end{matrix}} = (abc)d,$$

so we may write simply $abcd$ for each of these 7 products. Similarly for $a_1 \dots a_n$:

THM A. For each monoid M and $n \geq 2$ we define inductively $a_1 \dots a_n = (a_1 \dots a_{n-1}) a_n$ for $a_1, \dots, a_n \in M$. Then for $n \geq 2$,

$$\boxed{a_1(a_2 \dots a_n) = (a_1 a_2)(a_3 \dots a_n) = \dots = (a_1 a_2 \dots a_{n-1}) a_n}_{\,n} \quad (= a_1 \dots a_n).$$

Proof. $\square_2$ is clear, $\square_3$ is the associative law, and $\square_4$ is contained in the big display above. Supposing $l > 4$ and $\square_n$ has been proved for $2 \leq n < l$, then for $1 \leq m \leq l-2$,

$$(a_1 \dots a_m)(a_{m+1} \dots a_l) = (a_1 \dots a_m)((a_{m+1} \dots a_{l-1}) a_l) = ((a_1 \dots a_m)(a_{m+1} \dots a_{l-1})) a_l = (a_1 \dots a_{l-1}) a_l.$$

the second = by associativity, and the first and third by $\square_{l-m}$ and $\square_{l-1}$. Thus $\square_l$ is true.

*) For vectors u, v, w in $\mathbb{R}^3$, $(u \times v) \times w = u \times (v \times w) \Leftrightarrow u \parallel w$ or $v \perp u \,\&\, w$. We omit the proof.

THM B Let M be a monoid. Then M has only one identity element.

Proof. If $\tilde{1}$ and 1 are identity elements for M, then

$$\tilde{1} = \tilde{1} . 1 = 1$$

since 1 is an identity element   since $\tilde{1}$ is an identity element.

DEF Let M be a monoid, and let $a \in M$. An <u>inverse</u> for a is any $a' \in M$ satisfying

$$a a' = 1 \text{ and } a' a = 1.$$

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

Proof. If $\tilde{a}$ and a' are inverses for a, then

$$\tilde{a} = \tilde{a} . 1 = \tilde{a} . a a' = \tilde{a} a . a' = 1 . a' = a'$$

property of 1   def. of inverse   associativity   def. of inverse   property of 1.

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

THM D Let M be a monoid, let 1 be its identity element, and let $a, b \in M$. Then:

(1) 1 has an inverse, and $1^{-1} = 1$.

(2) If a has an inverse, so does a^{-1}, and $(a^{-1})^{-1} = a$.

(3) If a & b have inverses, so does ab, and $(ab)^{-1} = b^{-1} a^{-1}$.

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

(2) The equations $a a^{-1} = 1$ and $a^{-1} a = 1$ 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 element,

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

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

DEF A <u>group</u> is a monoid G in which each element has an inverse.

DEF An <u>abelian group</u> 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 <u>invertible</u> elements, or more briefly the <u>units</u> of M, is a group with the same multiplication and the same identity element. M^* is the <u>unit group</u> of the monoid M.

Proof By THM D, if $a \& b \in M^*$, then $ab \in M^*$. Clearly $a.bc = ab.c$ for all $a, b, c \in M^*$; $1 \in M^*$ and clearly $1.a = a.1 = a$ 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) in M, we have $a^{-1} \in M^*$, and $aa^{-1} = a^{-1}a = 1$ shows that a^{-1} is the inverse for a in M^*. Since M^* is a monoid in 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 $\frac{n}{m}$ for $\left(\frac{m}{n}\right)^{-1}$ for nonzero $m, n \in \mathbb{Z}$.

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

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

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

NON-EXAMPLES of groups.

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

(ii) $\mathcal{S}(X)$ with $\cup$ (or $\cap$) with $X \neq \emptyset$, because $X \cup A = \emptyset$ (or $\emptyset \cap A = X$) for no $A \subset X$.

NOTATION The bijections $f: X \to X$ are also called <u>permutations</u> of X, and $\mathcal{M}(X)^*$ is also called the <u>symmetric group</u> 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 $x_1 \in X$. Each bijection $f: X \to Y$ sends x_1 to some $y_1 \in Y$, and is determined by this y_1, together with the bijection, gotten from f, from $X - \{x_1\}$ to $Y - \{y_1\}$. Since there are n choices for y_1 and, by induction, $(n-1)!$ bijections from $X - \{x_1\}$ to $Y - \{y_1\}$, there are $n.(n-1)! = n!$ 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 $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

EXERCISE 4. There are 5 ways (boxed in the big display on 7.2) of writing $abcd$, using multiplication of factors "two at a time." More generally, Catalan in 1838 proved that the analogous number c_n for $a_1 \cdots a_n$ is given by

$$* \qquad c_n = \frac{(2n-2)!}{(n-1)!\, n!}.$$

Verify that $*$ is correct for $n=4$, and show that, in agreement with $*$, $c_5 = 14$, by making a complete list of all 14 ways of writing $abcde$ analogous to the 5 ways of writing $abcd$. Putting $c_1 = 1$ and $c_2 = 2$ prove that for all $n \geq 2$,

$$** \qquad c_n = c_1 c_{n-1} + c_2 c_{n-2} + \cdots + c_{n-1} c_1 .$$

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