In a group one has the associative rule 
\[(xy)z = x(yz)\].
When we multiply e.g. numbers, we drop all parentheses, since we know that the result doesn't depend on order of operations at all (provided we've only multiplying).

Prop: Suppose an associative operation 
\[S \times S \rightarrow S\]
is given on a set \(S\). Then there is a unique way to define operations 
\[S^n \rightarrow S, \quad n \geq 1,\]
written temporarily as 
\[(a_1, \ldots, a_n) \mapsto [a_1 \ldots a_n] \]
so that
(i) \([a_1] = a_1\)
(ii) \([a_1 a_2] = a_1 \cdot a_2\)
(iii) For any \(1 \leq i \leq n-1\) we have 
\([a_1, \ldots, a_n] = [a_1, \ldots, a_i][a_{i+1}, \ldots, a_n].\]
Proof. We use induction on \( n \). The operation is already given for \( n=1 \) and \( n=2 \), and it certainly satisfies (iii) for \( n=2 \).

Suppose the operations \( S \to S \) are defined for \( r \leq n-1 \) and that these are uniquely determined by (i) – (iii).

Define
\[
[a_1 \ldots a_n] = [a_1 \ldots a_{n-1} \cdot a_n]
\]
for all \( a_1, \ldots, a_n \in S \). If an operation \( S^n \to S \) exists with property (iii), it must be given by this formula. To check that (iii) holds for this operation, observe:
\[
[a_1 \ldots a_n] = [a_1 \ldots a_{n-1} \cdot a_n] \quad \text{(definition)}
\]
\[
= ([a_1 \ldots a_i] \cdot [a_{i+1} \ldots a_{n-1}] \cdot a_n] \quad \text{by inductive hypothesis}
\]
\[
= [a_1 \ldots a_i] \cdot ([a_{i+1} \ldots a_{n-1}] \cdot a_n] \quad \text{by associativity of } \cdot
\]
\[
= [a_1 \ldots a_i] \cdot [a_{i+1} \ldots a_n] \quad \text{by inductive hypothesis}
\]
for all \( 1 \leq i \leq n-2 \).

This completes the proof of (iii) at
This completes the proof of (iii) at the inductive step. Hence our proof is complete.

In general, then, in a group we'll omit parentheses whenever we like.
Def. A group $G$ is abelian if for every $x, y \in G$ one has $xy = yx$.

A group $G$ is nonabelian if there exist $x, y \in G$ such that $xy \neq yx$.

Example. Consider $G = \text{Aut} (\{1, 2, 3\})$, and let

\[
\begin{array}{cccc}
  \times & 0 & 1 & 2 & 3 \\
  0 & 0 & 1 & 2 & 3 \\
  1 & 1 & 0 & * & 2 \\
  2 & 2 & * & 3 & 1 \\
  3 & 3 & * & 1 & 2 \\
\end{array}
\]

Then

\((x \circ y)(3) = x(2) = 1, \quad \text{but} \quad (y \circ x)(3) = y(3) = 2\).

So $x \circ y \neq y \circ x$. 
Examples of Groups

\[(\mathbb{Z}, +)\]
\[(\mathbb{Q}, +)\]
\[(\mathbb{R}, +)\]
\[(\mathbb{C}, +)\]

\[(\mathbb{Q}^\times, \cdot)\]
\[(\mathbb{R}^\times, \cdot)\]
\[(\mathbb{C}^\times, \cdot)\]

\underline{Not} \ (\mathbb{Z}^\times, \cdot) \ !! \text{Unless}

\[\mathbb{Z}^\times\] means "multiplicative units"
\[(a \text{ unit} \ is \ an \ element \ that \ has \ a \ multiplicative \ inverse).\]
Let 
\[ \mu_n = \{ z \in \mathbb{C} \mid z^n = 1 \} \subseteq \mathbb{C}^x. \]

Prop \((\mu_n, \cdot)\) is a group.

Proof. If \( z^n = 1 \) and \( w^n = 1 \) then
\[(zw)^n = z^n w^n = 1 \cdot 1 = 1. \]
So \(\mu_n\) is closed under multiplication.

Multiplication is certainly associative.
\(1^n = 1\) so \(1 \in \mu_n\).

Finally, if \( z^n = 1 \), then
\[(z^n)^{-1} = (z^{-1})^n = 1^{-1} = 1, \]
so \(z^{-1} \in \mu_n\).
Thus \(\mu_n\) has inverses.

We call \((\mu_n, \cdot)\) the group of \textit{nth roots of unity}. 
Lemma \(M_n\) has \(n\) elements.

Proof. The polynomial \(z^n - 1\) has at most \(n\) roots (do you know this?), so \(M_n\) has at most \(n\) elements.

But \(e^{2\pi i k/n}\), \(k = 0, 1, 2, \ldots, n-1\), gives \(n\) distinct elements of \(M_n\).

\[
\text{Note } e^{2\pi i k/n} = \cos(2\pi k/n) + i\sin(2\pi k/n).
\]

[Do you know this? Use Taylor expansions]

\[
e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!},
\]

\[
\sin z = \sum_{n=0}^{\infty} \frac{z^{2n+1}}{(2n+1)!}(-1)^n, \quad \cos z = \sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!}(-1)^n.
\]
Example

\[ \text{GL}(n, \mathbb{C}) = \{ \text{nxn matrices } M \text{ w/ C-coefficients } \mid \text{det} M \neq 0 \} \]

This is a group under matrix mult.

Example

\[ \text{GL}(n, \mathbb{C}) \supseteq W = \{ \text{matrices } M \text{ w/ a single 1 in each row and each column, zeroes elsewhere} \} \]

Let

\[ E = \{ e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C}^n \} \]

With entry

That is, \( E \subseteq \mathbb{C}^n \) is the subset of standard basis vectors.

Prop An element \( M \in \text{GL}(n, \mathbb{C}) \) lies in \( W \) if and only if \( M \cdot E = E \).
Note M·E means
\[ \{ M \cdot e_i \in \mathbb{C}^n \mid i = 1, 2, \ldots, n \} \]
= \{ M e_1, M e_2, \ldots, M e_n \}.

Proof of Prop. Note that M·e_i is exactly the i-th column of M. So, M·e_i \in E for all i iff M has a single 1 in each column and all other entries 0. If M E W then M has a single 1 in each row, so it can't be the case for distinct i and j that M e_i = M e_j. Since the function M : E \rightarrow E is thus one-to-one and E is a finite set, M is surjective as well, i.e. M·E = E. Conversely, if M·E = E then M : E \rightarrow E is
injective, and it follows that no
two columns of $M$ are the same.
Consequently, since each column of $M$
is determined by the row in which it
has a 1, $M$ has only one 1 per row. $\square$

Corollary $W$ is a group under matrix
multiplication.
Def. A nonempty subset $H$ of a group $G$ is a subgroup of $G$ if, under the product of $G$, $H$ is itself a group.

So, e.g., $W \subseteq \text{GL}(n, \mathbb{C})$ is a subgroup.

Lemma. A nonempty subset $H$ of $G$ is a subgroup of $G$ if and only if

1. $a, b \in H$ implies that $ab \in H$.
2. $a \in H$ implies that $a^{-1} \in H$.

Proof. ($\Rightarrow$) is clear.

($\Leftarrow$) Suppose $H \subseteq G$ is a subset for which (1) and (2) hold.

Associativity of the product is clear, so we need only prove that $e \in H$.

But, choosing some $a \in H$, we have $a^{-1} \in H$.
by (2), so \( a \cdot a^{-1} \in H \) by (1). \( \square \)

**Example**

Let \( S \) be a set, \( T \subseteq S \) a subset, set

\[
\text{Aut}(S) 
\implies H = \{ f \in \text{Aut}(S) \mid f(T) = T \}
\]

Then \( H \) is a subgroup of \( \text{Aut}(S) \).

**Example**

\((\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)\)

is a chain of subgroups.

**Example**

For any group, \( g \in G \). The set

\[
\langle g \rangle = \{e, g, g^{-2}, g^{-1}, g^2, g^3, \ldots \}
\]

is a subgroup of \( G \), e.g., \( \mathbb{Z} \subseteq (\mathbb{R}, +) \), \( \mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle \). Also,
$\{e^{2\pi i \cdot 2/10}\} = \mu_5$

is a subgroup. [In particular, it does not need to be the case that $\langle g \rangle$ is infinite!]

$\langle g \rangle$ is the subgroup generated by $g$.

More generally, if $S \subseteq G$ is any subset, $\langle S \rangle$ is the intersection of all subgroups of $G$ that contain $S$; it is called the subgroup of $G$ generated by $S$.

**Lemma** $\langle S \rangle$ is a subgroup of $G$.

You're (essentially) proving this for homework.
Def Let $G$ and $H$ be groups. A function $\bar{\phi} : G \to H$ is a homomorphism if $\bar{\phi}(ab) = \bar{\phi}(a) \overline{\phi}(b)$ for all $a, b \in G$.

$H$ is said to be an isomorphism if there is a homomorphism $\overline{\psi} : H \to G$ with $\overline{\psi} \circ \bar{\phi} = \overline{\text{id}}_G$ and $\bar{\phi} \circ \overline{\psi} = \overline{\text{id}}_H$.

Lemma Suppose $\bar{\phi} : G \to H$ is a homomorphism. Then $G$ is an isomorphism if $\bar{\phi}$ is one-to-one and onto.

Pf. If $G$ is an isomorphism then $\overline{\psi}$ is an inverse function for $\bar{\phi}$, so $\bar{\phi}$ is one-to-one and onto. Conversely, if $\bar{\phi}$ is one-to-one and onto then
an inverse function $\overline{\phi}^{-1}$ exists, and we only need to check that

$$
\overline{\phi}^{-1}(uv) = \overline{\phi}^{-1}(u) \overline{\phi}^{-1}(v) \text{ for all } u, v \in H.
$$

But

$$
\overline{\phi}(\overline{\phi}^{-1}(uv)) = uv \quad \text{and}
$$

$$
\overline{\phi}(\overline{\phi}^{-1}(u) \overline{\phi}^{-1}(v)) = \overline{\phi}(\overline{\phi}^{-1}(u)) \overline{\phi}(\overline{\phi}^{-1}(v)) = uv,
$$

so $\overline{\phi}$ one-to-one implies

$$
\overline{\phi}^{-1}(uv) = \overline{\phi}^{-1}(u) \overline{\phi}^{-1}(v), \text{ as desired.}\]

Example. Recall our procedure for giving a function from $S_n$ to $W \subseteq GL(n, C)$ : $f \in S_n$ goes to the matrix $p(f)$ whose entries are given by $$(p(f))_{ij} = \begin{cases} 1 & \text{if } f(j) = i \\ 0 & \text{otherwise} \end{cases}.$$
I claim that the function

\[ p : S_n \rightarrow \mathbb{W} \]

so defined is an isomorphism. First, it is a homomorphism: \( p(f)_{ij} \) may be written

\[ p(f)_{ij} = \delta_{f(j), i} \]

where \( \delta_{uv} \) is the Kronecker delta function,

\[ \delta_{uv} = \begin{cases} 1 & \text{if } u=v, \\ 0 & \text{otherwise}. \end{cases} \]

Then

\[ (p(g)p(f))_{ik} = \sum_j p(g)_{ij} p(f)_{jk} \]

\[ = \sum_j \delta_{g(j), i} \delta_{f(k), j} = \sum_j \delta_{g(j), i} \delta_{g(f(k)), j} \]

\[ = \delta_{g(f(k)), i} = p(g \circ f)_{ik}. \]

So \( p(g)p(f) = p(g \circ f) \).
It remains to check that $P$ is a bijection. Note that you may count that $S_n$ has $n!$ elements and so does $W$, so it remains only to check, for example, that $P$ is one-to-one. Note, though, that $P(f)(e_i) = e_{f(i)}$, so if $P(f) = P(g)$ then $f(i) = g(i)$ for all $1 \leq i \leq n$, implying $f = g$. \[\square\]

Example The determinant function

\[\det : \text{GL}(n, \mathbb{C}) \to \mathbb{C}^*\]

\[M \mapsto \det(M)\]

is a homomorphism.
Lemma 1. If $H \leq G$ is a subgroup and $G \xrightarrow{\pi} G'$ is a homomorphism then $\pi: H \to G'$ is a homomorphism.

Lemma 2. If $\Phi: G \to H$, $\Psi: H \to L$ are homomorphisms, so is $\Phi \circ \Psi: G \to L$.

Example. The composite

$$S_n \xrightarrow{\pi} W \to \text{GL}(n, \mathbb{C}) \xrightarrow{\text{det}} \mathbb{C}^*$$

is known as the signature homomorphism.

Lemma 3. If $f \in S_n$ then $\text{sgn}(f) \in \{1, -1\} \subset \mathbb{C}^*$.

Proof. It suffices to check for $\text{det}(w)$, $w \in \text{GL}(n, \mathbb{C})$. We do this by
induction on $n$. The case $n = 1$

is clear. If $w \in GL(n, \mathbb{C})$ then

$w$ has the form

\[
\begin{pmatrix}
0 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & 1 \\
0 & \cdots & 0 & 1
\end{pmatrix}
\]  

$i$th row

If we remove the $1$st column and
$i$th row of $w$, the remaining matrix
$w'$ has a single $1$ in each row
(we've removed a $0$ from each) and
a single $1$ in each column (we've removed
a $0$ from each). The usual expansion
by minors in the first column shows
that $\det(w) = \det(w')$. This completes
the inductive step. \qed
Example: Let $T \subseteq \{1, 2, \ldots, n\}$ be a nonempty subset, $S_n \supseteq H = \{ f \in S_n \mid f(T) = T \}$. Then we get a homomorphism $H \to \text{Aut}(T)$ by $f \mapsto f|_T$.

Direct Product: Suppose $G$ and $H$ are groups. Let $G \times H$ denote the Cartesian product of the sets $G$ and $H$ with operation $(G \times H) \times (G \times H) \to G \times H$  

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2).$$
Lemma. This makes $G \times H$ a group.

Proof. Exercise: use $(e_G, e_H)$ as the identity (where $e_G$ denotes the identity element of $G$ and $e_H$ denotes the identity element of $H$) and

$$(g, h)^{-1} = (g^{-1}, h^{-1}) \quad \Box.$$