Recall we were constructing the sign homomorphism \( \eta : S_n \to \mathbb{Z}_2 \), we defined the function \( \eta \) as such: let \( \alpha = \alpha_1, \ldots, \alpha_n \) be a complete factorization and

\[
\eta(\alpha) = (-1)^{n-r}
\]

If \( \gamma = (a, b) \) is a transposition, we saw that \( \eta(\gamma) = -1 \)

Now, if \( \alpha = (a_1, \ldots, a_r) \) then

\[
\alpha = (a_1, a_r)(a_1, a_{r-1}) \ldots (a_1, a_2)(a_1, a_1)
\]

Hence any cycle (and thus any permutation) can be written as a product of transpositions.
This holds if \( \beta \in S_n \). Then \( \text{sgn}(\alpha \cdot \beta) \)
\[
= \text{sgn}(\alpha) \cdot \text{sgn}(\beta)
\]

pf

As any permutation can be written as a product of transpositions, it suffices to consider the case \( \alpha \cdot \beta \) is a transposition (\( \alpha \) then \( \text{sgn}(T_1 \cdots T_m \cdot \beta) \))
\[
= \text{sgn}(T_1) \cdot \text{sgn}(T_1 \cdots T_m) \cdot \text{sgn}(\beta)
\]
\[
= \text{sgn}(T_1) \cdots \text{sgn}(T_m) \cdot \text{sgn}(\beta)
\]
\[
= \text{sgn}(T_1 \cdots T_m) \cdot \text{sgn}(\beta)
\]
\[
= \text{sgn}(\alpha) \cdot \text{sgn}(\beta)
\]

So suppose \( \alpha = (a \ b) \) and let
\( \beta = B_1 \cdots B_r \) be a complete factorization
Then \( a, b \) appear in precisely one cycle
Case 1: $a$ and $b$ appear in the same cycle $B_i$.
Writing $B_i = (a \ c_i \ \cdots \ c_e \ b \ c_{e+1} \ \cdots \ c_m)$ we compute

$$AB_i = (a \ b) (a \ c_i \ \cdots \ c_e \ b \ c_{e+1} \ \cdots \ c_m)
$$

$$= (a \ c_i \ \cdots \ c_e \ b \ c_{e+1} \ \cdots \ c_m)$$

Thus, the complete factorization of $AB_i$ is a product of $(n+1)$ disjoint cycles and $\text{sgn}(AB_i) = -\text{sgn}(B) = \text{sgn}(A) \text{sgn}(B)$

Case 2: $a$ and $b$ appear in distinct cycles $B_i$ and $B_j$.

$$B_i = (a c_i \ \cdots c_e) \ B_j = (b c_{e+1} \ \cdots c_m)$$

$$\ (a \ b) (a c_i \ \cdots c_e) (b c_{e+1} \ \cdots c_m)
$$

$$= (a c_i \ \cdots c_e b c_{e+1} \ \cdots c_m)$$
To each fact, \( \det AB \) is a product of 
\( n-1 \) disjoint cycles and \( \text{sgn}(AB) = -\text{sgn}(B) \) if 

Let \( k = \mathbb{Q} \) or \( \mathbb{R} \). 
Let \( GL_n(k) \) be the set of all 
n\times n \text{ matrices with non-zero determinant} 
is a group with product given by 
matrix multiplication. 
The function \( \det: GL_n(k) \rightarrow k^* \) 
\( \det(A \cdot B) = \det(A) \cdot \det(B) \) 

and hence is a homomorphism.

Subgroups

Let \( H \) be a subset of a group \( G, \cdot \) 
we say \( H \) is a subgroup if the 
following hold: (i) \( H, \cdot \) is a 
"
(i) \( H \times \mathbb{C}H, \ x^{-1} \in H \)

Notice that if \( H \) is a subgroup, then \( H \) is itself a group with respect to the operation \( * \). If \( H \) is a subgroup in \( G \), we write \( H \leq G \).

Examples / Nonexamples

(i) The set \( \mathbb{Z} \) of even integers is a subgp of \( \mathbb{Z} \) (how about odd integers?)

(ii) \( \mathbb{Q} \) is not a subgp of \( \mathbb{Q} \)

(iii) Let \( SL_n(\mathbb{F}) \) be the subset of \( GL_n(\mathbb{F}) \) consisting of matrices \( A \) with \( \det A = 1 \). Then \( SL_n(\mathbb{F}) \leq GL_n(\mathbb{F}) \).

(iv) The set of even permutations \( \Sigma \in S_n | \text{sgn}(\Sigma) = 1 \) is a subgp of \( S_n \).
Prop (The Subgroup Criterion)
A subset \( H \) of a group \( G \) is a subgroup if and only if \( \forall x \in H \) and \( \forall y \in H \),
\( xy \in H \) and \( y^{-1} \in H \).

Proof: If \( H \leq G \), then \( H \) is a group if
\( \forall x \in H \) and \( \forall y \in H \),
\( xy^{-1} \in H \) and \( x^{-1} \in H \).

Suppose \( \forall x \in H \), \( \forall y \in H \), \( xy^{-1} \in H \).
Then, setting \( x = 1 \), we see that \( \forall y \in H \), \( y^{-1} \in H \)
(assump. (iii) of subgp.). Now if \( xy \in H \)
then \( x, y^{-1} \in H \) and \( (xy)^{-1} = x(y^{-1})^{-1} \)
so \( xy \in H \) which is assump. (iii).

If \( n \) is an integer and \( x \in G \),
then we define \( x^n = x \cdot x \cdots x \quad (n \text{ copies}) \),
\( x^0 = 1 \), \( n \in \mathbb{Z} \),
\( x^{-n} = (x^n)^{-1} \quad (n < 0) \).
The cyclic subgroup \( \langle x \rangle \) generated by \( x \) is the subgroup 
\[ \{ x^n \mid n \in \mathbb{Z} \} \]

Clearly \( \langle x \rangle \) is a subgroup of \( G \).

Let \( x \in G \) (\( G \) a gp). The order \( |x| \) of \( x \) is defined to be the least positive integer \( n \) s.t. \( x^n = 1 \). If \( |x| \) is not a positive integer, we say that the order is infinity.

**Prop.**
Let \( x \in G \). Then \( |x| = \) the number of elements in \( \langle x \rangle \).

**Pf.** If \( |x| = 1 \) then \( |x| = 1 = \# \langle x \rangle \).
So suppose \( |x| > 1 \), let \( m \) be non-negative integers and suppose \( 0 \leq l \leq m \in \langle x \rangle \).
Then \( x^e + x^m \). Indeed, if \( x^e = x^m \)
then \( x^{m-e} = 1 \) contradicting that \( m-e < |x| \).

Then the set \( \{ x^1, x^2, \ldots, x^{|x|-1} \} \) consists of \(|x|\) distinct elements. It suffices to show \( \exists (x_1 x_2 \cdots x_r) \Rightarrow \exists (x) \)

So let \( x^n \in \langle x \rangle \). Write
\[
h = m \mid x \mid + r, \quad 0 \leq r < |x|
\]

using the division algorithm.

Then \( x^n = x^{m\mid x \mid + r} = x^m \cdot x^r \).

\[
\begin{align*}
\Rightarrow x^r & \in \langle x \rangle \\
\Rightarrow x^r & \in \{ x^1, x^2, \ldots, x^{|x|-1} \}
\end{align*}
\]

Prop: Let \( H_i : \forall i \geq 1 \) be any family of subgroups of \( G \) then the intersection \( \cap H_i \)
is a subgp of $G$.

**Proof.** Let $x, y \in \bigcap H_i$. Then $x y^{-1} \in H_i$ for all $i$. Thus $x y^{-1} \in \bigcap H_i$.

But then $x y^{-1} \in \bigcap H_i$.

So $\bigcap H_i \leq G$. \[\text{i.f.} \quad G.\]

Now let $X$ be any subset of $G$.

The subgroup generated by $X$, written $\langle X \rangle$, is defined to be the intersection of all subgroups $H \leq G$ containing the set $X$.

$$\langle X \rangle = \bigcap \{ H \leq G \mid X \subseteq H \}.$$  

Notice that if $H$ is a subgroup of $G$ containing $X$, we have
\langle x \rangle \leq H

Hence \langle x \rangle \text{ is the smallest subgroup of } G \text{ containing } x.