Some definitions -

Finite Sequence - an English word like "excellent" can be viewed as the finite sequence e, x, c, e, l, l, e, n, t

Strings - Sequence of letters or other symbols written without commas are also called strings. ex. ab/cx.

An infinite string like ababab.... may be regarded as the infinite sequence a, b, a, b, ...

Note: Strings are also called words in certain context.

Semigroups - It is a mathematical structure consisting of a set S together with a binary operation * which is Associative defined on S. Semigroup is denoted by (S, *) or simply S. We also refer to a*b as the product of a & b. Semigroup (S, *)

is said to be **Commutative** if Semigp (2)
$*$ is Commutative.

ex. $(Z, +)$ is a Commutative Semigp
$\because$ in Z (set of integers), + is Associative
& also Commutative.

$$a + (b+c) = (a+b)+c \text{ — Asso.}$$
$$\text{\& also } a+b = b+a \quad \forall a,b,c \in S.$$
— Comm.

ex. $(Z, -)$ is NOT a Semigrp. $\because$
$-$ is NOT Asso.

Counter example:
$$(2-5)-1 = -3-1 = 4$$
$$2-(5-1) = 2-4 = -2$$
$$4 \neq -2$$

A typical example —
Let $A = \{a_1, a_2, \ldots, a_n\}$ be a non empty set.
A^* is the set of all finite sequences of elements of A ie., A^* consists of all words that can be formed from the alphabet A. For ex,
if $A = \{a, b, c\}$ then $A^* = \{ab, bc, abc, acc \ldots\}$
Note that a Catenation or concatenation is

a binary operation '$\cdot$' on A^*. If $\alpha, \beta \in A^*$ and $\alpha = a_1 a_2 \cdots a_n$ & $\beta = b_1 b_2 \cdots b_k$

then $\alpha \cdot \beta = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_k$.

It is clear that if $\alpha, \beta, \gamma \in A^*$ then

$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ But '$\cdot$' is

NOT Commutative $\because \beta \cdot \alpha = b_1 b_2 \cdots b_k a_1 a_2 \cdots a_n$

$\therefore$ '$\cdot$' is Asso. & $\therefore$ $(A^*, \cdot)$ is a Semigroup Called the Free Semigrp Generated by A.

Monoid - A monoid is a Semigrp $(S, *)$ which has an identity e.

$$e * a = a * e = a \quad \forall a \in S.$$

ex. 0 is an identity in Semigp$(Z, +)$

$$\because 0 + 2 = 2 + 0 = 2$$

ex $P(S)$: PowerSet - set of all subsets of set S.

$S = \{a, b, c\}$, $P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

union

$\phi * A = \phi \cup A = A = A \cup \phi = A * \phi$; A is any element ~~subset~~ of $P(S)$ (a subset of S)

$\therefore$ empty set ϕ is identity. $\therefore (P(S), \cup)$: Monoid.

Thm Let $(S, *)$ & $(T, *')$ be monoids with identities e & e', respectively. Let $f: S \to T$ be an isomorphism. Then $f(e) = e'$.

Pf. Let b be any element of T. Since f is onto, there is an element a in S s.t. $f(a) = b$

Then $a = a * e$

$b = f(a) = f(a * e) = f(a) *' f(e)$ ($\because f$ is Iso.)

$= b *' f(e)$ —— (1)

Similarly, since $a = e * a$, $b = f(e) *' b$

similar to (1)

Thus for any $b \in T$,

$b = b *' f(e)$

$= f(e) *' b$ —— (2)

(1) & (2) $\Rightarrow f(e)$ is an identity for T.

Since identity is unique

$\Rightarrow f(e) = e'$.

HB

Congruence Relation — An Equivalence Relation (Reflexive, Symmetric & Transitive) R on the semigp $(S, *)$ is called a Congruence Relation if aRa' and $bRb' \Rightarrow (a*b) R (a'*b')$

Ex. Prove: $a \equiv b \bmod 2$ is a congruence relation.
(a is congruent to b mod 2)

Sol. $a \equiv b \bmod 2 \Leftrightarrow 2 \mid (a-b)$

Consider the semigp $(\mathbb{Z}, +)$ & the equivalence rel. on $\mathbb{Z}$ defined by $aRb \Leftrightarrow a \equiv b \bmod 2$.

We show: R is a Congruence Rel.

If $a \equiv b \bmod 2$ & $c \equiv d \bmod 2$

then $2 \mid (a-b)$ & $2 \mid (c-d)$

Note: $\mid \Rightarrow$ divides with 0 remainder

$\therefore a-b = 2m$ & $c-d = 2n$; $m, n \in \mathbb{Z}$

Adding, $(a-b) + (c-d) = 2m + 2n$

$+$ from $(\mathbb{Z}, +)$

Or $(a+c)-(b+d) = 2(m+n)$

$\therefore a+c \equiv (b+d) (\bmod 2)$ (defn)

$\therefore R$ is a Congruence Rel.

HP