iii) $\{g_0 \to g_0\}$

E20) Find a grammar that generates {b, aba, aabaa, aaabaaa, …}.

E21) Find a grammar with the alphabet set A that generates A^*, i.e., the universal language.

Now, let us look at what kind of grammars make up the classes L_1 to L_4 in Chomsky's hierarchy, mentioned earlier.

Definitions: 1) A language $L \subseteq A^*$ is **regular** if it can be generated by a grammar with rewriting rules of the form $x \to ay$, $x \to a$ for $a \in A^*$ and $x, y \in G$. (For those of you familiar with deterministic finite accepters (dfa), a language L is regular iff $L = L(M)$ for some dfa M.)

2) A grammar $\mathcal{G}$ is called **context-free** if all its rewriting rules are of the form $x \to y$, where $x \in G$ and $y \in A^*$.
A language L is called **context-free** if $L = L(\mathcal{G})$ for some context-free grammar $\mathcal{G}$.

3) A grammar $\mathcal{G}$ is called **context-sensitive** if for every rewriting rule $x \to y$ in $\mathcal{G}$, we have $l(x) \le l(y)$, where $l(x)$ is the length of the string $x \in A^*$. A language L is called **context-sensitive** if $L = L(\mathcal{G})$ for some context sensitive grammar $\mathcal{G}$.

4) A language L is called a **computable language** if $L = L(\mathcal{G})$ for some grammar $\mathcal{G}$.

Here is a remark about this.

Remark 3: As you can see, every regular language is context-free, every context-free language is context-sensitive, and all these types of languages are computable languages.

Let us look at some examples.

Example 11: Show that every finite language is regular and context-free.

Solution: Let $L = \{x_1, x_2, \ldots, x_n\} \subseteq A^*$ for some A. Each of these elements can be obtained from a finite set of elements S of A by applying the rules of the form $g_0 \to g_0 a$, and $g_0 \to \Lambda$, where $g_0 \in G$, $a \in S$. For instance, if $x_i = s_1 \ldots s_n$, then $g_0 \to g_0 s_n \to g_0 s_{n-1} s_n \to \ldots \to g_0 x_i \to x_i$, applying $g_0 \to g_0 a$ first, and finally $g_0 \to \Lambda$. Therefore, L is regular.

Note that, over here the rewriting rules have only g_0 in the LHS. Hence L is context-free.

***

Example 12: Show that $L = \{xy^n \mid n \ge 0\}$ is a regular language, and context-free.

Solution: Here $A = \{x, y\}$, $G = \{g_0\}$, $g_0 \notin A$, and the rules are

$g_0 \to x$, $g_0 \to g_0 y$.

Then $L = L(\mathcal{G})$, and hence L is regular.

Here too, the rewriting rules only have g_0 in the LHS. Hence L is context-free.

***

We will now state, without proof, a result here to help us get an example of a language which is not regular.

Theorem 7: Let $A = \{a\}$ and $L \subseteq A^*$. L is regular if and only if $L = \{a^n \mid n \in P\}$, where P is a periodic subset of $\mathbb{N} \cup \{0\}$. ■

A set $\{p_n \mid n \in \mathbb{N}\}$ is called **periodic** if $\exists k, n_0 \in \mathbb{N}$ such that $p_{n+k} - p_n$ is constant $\forall n \geq n_0$.

Using this result, we can immediately say that $\{a^{n^2} \mid n \in \mathbb{N} \cup \{0\}\}$ is not regular since $\{n^2 \mid n \in \mathbb{N} \cup \{0\}\}$ is not a periodic set.

Try some exercises now.

E22) Show that $L(\mathcal{G}_1) = L(\mathcal{G}_2)$, where
$\mathcal{G}_1 = (\{a, b\}, \{g_0\}, \{g_0 \to g_0 g_0, g_0 \to aa\}, g_0)$ and
$\mathcal{G}_2 = (\{a, b\}, \{g_0\}, \{g_0 \to a g_0 a, g_0 \to aa\}, g_0)$.

Different grammars can generate the same language.

E23) Check whether or not $\{a^n \mid n \equiv 3 (\mathrm{mod}\, 4)\}$ is regular.

E24) Give an example, with justification, of a computable language.

With this we come to the end of our discussion on semigroups, monoids and their applications. Let us now take a look at the points covered by us in this unit.

7.5 SUMMARY

In this unit we have discussed the following points.

1) The definition, and some examples, of a semigroup/monoid.

2) What the unit group of a monoid is.

3) The definition of a subsemigroup and of a semigroup homomorphism/isomorphism.

4) Any non-empty intersection of subsemigroups of a semigroup S is a subsemigroup of S. This is not true if 'intersection' is replaced by 'union'.

5) The subsemigroup of S generated by $T \subseteq S$ is the smallest subsemigroup of S containing T, which is $\bigcap_i \{S_i \mid S_i \leq S, T \subseteq S_i\}$. This is denoted by $< T >$.

6) The definition, and examples, of a free semigroup.

7) A free semigroup is infinite, even if its basis is finite.

8) For any set $A \neq \emptyset$, there exists a semigroup F_A which is free on A. In fact, $F_A = \{a_1 a_2 \ldots a_n \mid a_i \in A\}$, the set of all finite formal products of elements of A.

9) Let a semigroup F be free on a finite set A and on a set A′. Then A′ is finite, and $|A| = |A'|$.

10) If F and F′ are both free semigroups on A, then $F \simeq F'$.

11) The definition, and examples, of (semi)automata.

12) Any semigroup/monoid gives rise to a (semi)automaton.

13) Given a (semi)automaton, there is a monoid corresponding to it.

14) For $A \neq \emptyset$, $A^* = F_A \cup \{\Lambda\}$ is a monoid with respect to concatenation, where Λ is the empty word. A formal language L over the set A is a subset of A^*.

15) A grammar is a 4-tuple $(A, G, \rightarrow, g_0)$ where A is its alphabet, G is the set of grammar symbols, $\rightarrow$ is the set of rewriting rules, and $g_0 \in G$ is the initial symbol. Here $A \cap G = \emptyset$, and $V = A \cup G$ is called the complete vocabulary.

7.6 SOLUTIONS/ANSWERS

E1) All three sets are non-empty, and closed w.r.t. the operations given. However, the first two are semigroups, and $(\mathbb{Z}, -)$ is not, since '–' is not an associative operation.

E2) Since $S \neq \emptyset$, $S \times S = \emptyset$. Therefore, $\text{Rel}(S) \neq \emptyset$.
For $R_1, R_2 \subseteq S \times S$, $R_1 * R_2 \subseteq S \times S$.
Therefore, $*$ is a binary operation.
Now, let $R_1, R_2, R_3 \in \text{Rel}(S)$.
Then $(\alpha, \beta) \in (R_1 * R_2) * R_3$
$\Leftrightarrow$ $\exists s \in S$ s.t. $(\alpha, s) \in R_1 * R_2$ and $(s, \beta) \in R_3$
$\Leftrightarrow$ $\exists s \in S, t \in S$ s.t. $(\alpha, t) \in R_1$, $(t, s) \in R_2$ and $(s, \beta) \in R_3$
$\Leftrightarrow$ $\exists t \in S$ s.t. $(\alpha, t) \in R_1$ and $(t, \beta) \in R_2 * R_3$
$\Leftrightarrow$ $(\alpha, \beta) \in R_1 * (R_2 * R_3)$
Therefore, $*$ is associative.
Thus, $(\text{Rel}(S), *)$ is a semigroup.

E3) $\wp(X) \neq \emptyset$ since $X \neq \emptyset$.

Next, $\otimes$ is a binary operation on $\wp(X)$.

Finally, $(A \otimes B) \otimes C = A \otimes (B \otimes C) \forall A, B, C \in \wp(X)$ since $*$ is associative on S.

E4) Since $n_1 \cdot n_2 \in \mathbb{N} \forall n_1, n_2 \in \mathbb{N}$ it follows that $(\mathbb{N}, \cdot) \leq (\mathbb{Z}, \cdot)$.

E5) i) As noted earlier, the unit group for this is $\{0\}$.

ii) In this case the identity is 1. Hence the unit group is $\{\pm 1\}$.

iii) Here the identity is S. Therefore, the only subset of S which has an inverse is S.

iv) $Id : S \to S$ is the identity map.
Thus, Bij(S, S), the set of all bijective mappings from S onto S, is the unit group of Map(S, S).

E6) $f(x.y) = 0 = 0 + 0 = f(x) + f(y) \forall x, y \in \mathbb{Z}$.
$\therefore$ f is a homomorphism.

E7) Define
$\phi : \wp(\{1, 2, 3\}) \to \wp(\{a, b, c\}) : \phi(\emptyset) = \emptyset, \phi(\{1\}) = \{a\}, \phi(\{2\}) = \{b\}, \phi(\{3\}) = \{c\},$
and extend ϕ elementwise.
This means that we consider the subsets of $\{1, 2, 3\}$, namely,
$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$.
Then, under ϕ, the images of these are
$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$, respectively.
You can check that $\phi(S_1 \cap S_2) = \phi(S_1) \cap \phi(S_2) \forall$ subsets S_1, S_2 of $\{1, 2, 3\}$.
Also, from the definition of ϕ, it is clear that ϕ is a monomorphism and an epimorphism. Hence, ϕ is an isomorphism.

E8) Consider $T = \bigcap_{i \in I} S_i$, where $S_i \leq S \ \forall \ i \in I$, the indexing set. (Note that I may be finite or infinite.)
For $x, y \in T$, $x, y \in S_i \ \forall i \in I$.
$\Rightarrow \quad x * y \in S_i \ \forall i \in I$
$\Rightarrow \quad x * y \in T$
$\therefore \quad T \leq S$.

E9) Consider $S = (\mathbb{Z}, +)$, and take $S_1 = (\mathbb{N}, +)$, $S_2 = (\mathbb{Z}^-, +)$, where $\mathbb{Z}^-$ is the set of negative integers.
Then $S_1 \cup S_2 = \mathbb{Z} \setminus \{0\}$, which is not a semigroup w.r.t. addition (e.g., $1 + (-1) \notin \mathbb{Z} \setminus \{0\}$).

E10) Let $(S = \{s_1, \ldots, s_n\}, \cdot)$ be a subsemigroup of $(G, \cdot)$.
Consider $s \in S$, and take $S' = \{ss_1, ss_2, \ldots, ss_n\}$. Then $S' \subseteq S$.
Also, $ss_i = ss_j \Rightarrow s_i = s_j$, since $ss_i, ss_j \in G$. So, $|S'| = |S|$.
$\therefore \quad S' = S$.
$\therefore \quad \exists$ i s.t. $ss_i = s$ in S, and in G.
$\therefore \quad s_i = e$.

Thus, $e \in S$.
Using a similar argument, you can show that $s^{-1} \in S \ \forall \ s \in S$.
Thus, S is a subgroup of G.
However, if G is infinite, this need not hold. E.g., $(\mathbb{N}, \cdot)$ is a subsemigroup of the group $(\mathbb{R}^*, \cdot)$, but $(\mathbb{N}, \cdot)$ is not a group.

E11) In general, $\wp(S)$ is generated by itself. Thus, if $\wp(S)$ is finite, i.e., if S is finite, then $\wp(S)$ will be finitely generated.

Now, take the case when S is infinite. Then $\wp(S)$ is infinite. Suppose it is finitely generated, say, by $S_1, \ldots, S_r$. Then
$\langle S_1, \ldots, S_r \rangle = \left\{ S_{i_1} \cap \ldots \cap S_{i_n} \middle| 1 \le i_1 < i_2 < \ldots < i_n \le r \right\}$ is also a finite collection of subsets of S, and hence this is not infinite. Therefore, it cannot be $\wp(S)$. Thus, $\wp(S)$ is f.g. iff S is finite.

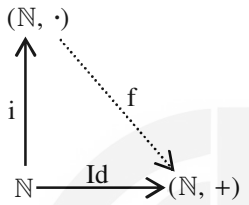

Fig. 6: Why $(\mathbb{N}, \cdot)$ is not a free semigroup.

E12) $(\mathbb{N}, \cdot)$ is not free. To prove this, suppose $(\mathbb{N}, \cdot)$ is free. Then we have the commutative diagram in Fig. 6, where $i(n) = Id(n) = n \ \forall \ n \in \mathbb{N}$. So f will be an isomorphism. But $(\mathbb{N}, +)$ has no identity element, while $(\mathbb{N}, \cdot)$ does. So, we reach a contradiction. Hence $(\mathbb{N}, \cdot)$ is not free.

On the same lines you can show that $(\mathbb{N} \cup \{0\}, +)$ and $(\mathbb{R}, +)$ are not free semigroups.

E13) i) A non-empty subset A, of a monoid $(M, *)$, is called a **submonoid**
- if A contains the identity of M, and
- A is closed w.r.t. $*$.

ii) A monoid $(M, *)$ is called **free** (on a non-empty set B) if
- $M \supseteq B$; and
- any mapping f from B into a monoid $(M', *')$ can be extended to a unique monoid homomorphism from M to M'.

E14) Let $s \in S$. If S is free, then $\{s^n | n \in \mathbb{N}\} \subseteq S$, where $s^n \neq s^m$ for $n = m$.
$\therefore$ S can't be finite.

E15) Let $\{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r\}$ generate $(\mathbb{Z}_n, \cdot)$, where $a_i \in \mathbb{N}$. Take F to be the free semigroup on $\{a_1, a_2, \ldots, a_r\} \subseteq \mathbb{Z}$. Define
$\psi : F \to \mathbb{Z}_n : \psi(x_1 x_2 \ldots x_k) = (x_1 \cdot x_2 \cdot \ldots \cdot x_k) (\mathrm{mod}\, n)$, where $x_1 x_2 \ldots x_k$ is a string in F.
Then ψ is surjective, and $\psi(xy) = \psi(x) \cdot \psi(y) \ \forall \ x, y \in F$.

E16) Since $\psi(x + y) = \psi(x) + \psi(y)$, ψ is a homomorphism. It is not $1-1$, since, e.g., $\psi(0) = \psi(n)$ and $0 \neq n$ in $\mathbb{Z}$.

E17) i) $S = \{s_0, s_1, s_2, \ldots, s_{10}\}$, $A = \{a_1, a_2, a_3\}$, where
a_1 : No coin is inserted

a_2 : A correct coin is inserted

a_3 : A wrong coin is inserted

$\delta : S \times A \to S$ is defined by the following table.

δ	a_1	a_2	a_3
s_0	s_0	s_0	s_0
s_1	s_1	s_0	s_1
s_2	s_2	s_1	s_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
s_{10}	s_{10}	s_9	s_{10}

ii) Let $A_2 = \{b_1, b_2, b_3\}$, where

b_1 : No output

b_2 : A stamp

b_3 : A coin

Then $\lambda : S \times A_1 \to A_2$ is defined by the following table:

λ	a_1	a_2	a_3
s_0	b_1	b_3	b_3
s_1	b_1	b_2	b_3
s_2	b_1	b_2	b_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$
s_{10}	b_1	b_2	b_3

E18) Here $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$.

δ	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$

λ	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{2}$	$\overline{2}$	$\overline{2}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{4}$	$\overline{4}$	$\overline{4}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{6}$	$\overline{6}$	$\overline{6}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{8}$	$\overline{8}$	$\overline{8}$	$\overline{8}$

The monoid corresponding to (S, A_1, δ) is $(\{f_x \mid x \in F_{A_1}\}, \circ)$, where F_{A_1} is the free monoid on 5 symbols.

E19) i) Starting with g_0, any derivation will lead to a or b and to no other string. So, $L(\mathcal{G}) = \{a, b\}$.

ii) Here, any string can be Λ, a, aba.
So, $L(\mathcal{G}) = \{\Lambda, a, aba\}$.

iii) Here, there is no string in A^* derived from g_0. So, $L(\mathcal{G}) = \emptyset$.

E20) Take $\mathcal{G} = (\{a, b\}, \{g_0\}, \{g_0 \to b, g_0 \to ag_0a\}, g_0)$, where $g_0 \notin \{a, b\}$.
Then the strings would be b, aba, aabaa, ….

E21) $\mathcal{G} = (A, \{g_0\}, \{g_0 \to \Lambda, g_0 \to g_0a \mid a \in A\}, g_0)$, where $g_0 \notin A$.
Then $L(\mathcal{G}) = A^*$.

E22) In both cases $L = \{(aa)^n \mid n \in \mathbb{N}\}$.

E23) Since $\{n \mid n \equiv 3(\text{mod } 4)\}$ is a periodic set, $\{a^n \mid n \equiv 3(\text{mod } 4)\}$ is regular.

E24) For instance, L in E22 is computable since it is $L(\mathcal{G}_1)$.