Revision

Theorem 1.6 Let (S, o) be a semigroup and for any two elements $a, b \in S$, each of the equation $a o x = b$ and $y o a = b$ has a solution in S for x and y. Then (S, o) is a group.

Theorem 1.7 Let (S, o) be a finite semigroup in which both the cancellation laws hold, i.e., $a o b = a o c \Rightarrow b = c$, for $a, b, c \in S$ and $b o a = c o a \Rightarrow b = c$, for $a, b, c \in S$

Then (S, o) is a group.

Note If S be infinite, Theorem 1.7 may not be true. For example, $(\mathbb{N}, \cdot)$ is a semigroup and both the Cancellation Laws hold. But $(\mathbb{N}, \cdot)$ is not a group ($\mathbb{N}$ = the set of all natural numbers)

Definition Power of an element. Let $a \in G$, and (G, o) be a group Then we define $a^0 = e$ (e_G is the identity element in G)

For $n > 0$ and $n \in \mathbb{Z}$, we define a^n by induction as follows:

$a^1 = a$

$a^n = a o a^{n-1}$.

and for $n < 0$ and $n \in \mathbb{Z}$

$a^n = (a^{-1})^{-n}$

Definition: Subgroup of a group: Let (G, o) be a group and H be a non-empty subset of G. Then o restricted to H is a mapping from $H \times H$ to G. We say H is closed under o if the mapping o restricted to H be from $H \times H$ to H. H is said to be a subgroup of G if (H, o) is a group.

Example: $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$. A_3 is a subgroup of S_3

Theorem 1.8 Let (H,o) be a subgroup of (G,o). Then
(i) the identity element of (H,o) is the identity element of (G,o).
(ii) if $a \in H$ then the inverse of a in (H,o) is same as the inverse of a in (G,o).

Proof: (i) Let e_H be the identity in (H,o) and e_G be the identity in (G,o)
Let $h \in H \subset G$. Then $e_H o h = h$ and $e_G o h = h$ (considering h as element of G also). So, $e_H o h = e_G o h$
So, by left cancellation Law $e_H = e_G = e$ (say)

(ii) Let a' be the inverse of a in (H,o) and a'' be the inverse of a in (G,o)
Let $a \in H \subset G$. Then $a' o a = e$ and $a'' o a = e$ (considering a as an element of G. So, $a' o a = a'' o a$. So, by right-cancellation Law, $a' = a''$

Note: So, every subgroup of (G,o) contains the identity element of G. Therefore there can not be two disjoint subgroups of (G,o)

Definition: Order of an element: Let (G,o) be a group and $a \in G$.
a is said to be of finite order if $\exists$ a positive integer n such that $a^n = e$, e is the identity element in G. Otherwise, it is said be of infinite order.
When the order of an element $a \in G$ is finite, the order of a is the least positive integer n such that $a^n = e$ and is denoted by $o(a)$.
a is said to be of infinite order if the order of a is not finite and we write $o(a)$ is infinite.

Example In group S_3, $o(\rho_1) = 3$, $o(\rho_2) = 3$, $o(\rho_0) = 1$, $o(\rho_3) = o(\rho_4) = o(\rho_5) = 2$

Note: Identity element is the only element of order 1 in a group.

Theorem 1.9. Let a be an element of a group G. Then

(i) $o(a) = o(a^{-1})$

(ii) if $o(a) = n$ and $a^m = e$, then n is a divisor of m.

(iii) if $o(a) = n$ then $a, a^2, \ldots, a^n (= e)$ are distinct elements in G.

(iv) if $o(a) = n$, then for a positive integer m, $o(a^m) = \dfrac{n}{\gcd(m,n)}$

(v) if $o(a)$ is infinite and p is a positive integer, then $o(a^p)$ is infinite

(vi) if $o(a) = n$ then $o(a^p) = n$ if and only if p is prime to n.

Theorem 1.10 Let a be an element of a group G. Then for integers m, n

(i) $a^m \circ a^n = a^{m+n}$ (ii) $(a^m)^n = a^{mn}$ (iii) $(a^n)^{-1} = a^{-n}$

Theorem 1.11 Let G be a group. A non-empty subset H of G is a subgroup of G if and only if

(i) $a, b \in H \Rightarrow ab \in H$ (ii) $a \in H \Rightarrow a^{-1} \in H$

Theorem 1.12 Let G be a group. A non-empty subset H of G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$

Theorem 1.13 Let G be a group. A non-empty finite subset H of H is a subgroup of G if and only if $a, b \in H \Rightarrow ab \in H$.

Note: Theorem 1.13 does not hold if H be an infinite subset of G. For example, let $G = (\mathbb{Z}, +)$ and $H = \mathbb{N}$. $(\mathbb{Z}, +)$ is a group. $\mathbb{N}$ is an infinite subset of $\mathbb{Z}$ and $\mathbb{N}$ is closed under addition but $(\mathbb{N}, +)$ is not a group.

Theorem 1.14 Let G be a group and $\{H_\alpha : \alpha \in I\}$ be an arbitrary collection of subgroups of G. Then $\bigcap_{\alpha \in I} H_\alpha$ is a subgroup of G.

Note: Union of two subgroups may not be a subgroup.
Consider the group $(\mathbb{Z},+)$ and the subgroups $(2\mathbb{Z},+)$ and $(3\mathbb{Z},+)$
but $(2\mathbb{Z}\cup 3\mathbb{Z},+)$ is not a subgroup as $2\in 2\mathbb{Z}$, $3\in 3\mathbb{Z}$
but $2+3=5\notin 2\mathbb{Z}\cup 3\mathbb{Z}$

Theorem 1.15 Let G be a group and H and K are subgroups of G. Then $H\cup K$ forms a subgroup of G if and only if $H\subset K$ or $K\subset H$.

Note: A group can not be the union of two proper subgroups.

Note: $\{e\}$ is said to be the trivial subgroup of G and G is said to be the improper subgroup of G.

Theorem 1.16 Let H and K be subgroups of a group G. Then $HK=\{hk: h\in H, k\in K\}$ is a subgroup of G if and only if $HK=KH$

Theorem 1.17 Let H and K be finite subgroups of a group G such that HK is a subgroup of G. Then $o(HK)=\frac{o(H)\,o(K)}{o(H\cap K)}$

Theorem 1.18 Every element of a finite group is of finite order.

Some Exercises: 1.(a) Define a binary operation $\circ$ on $\mathbb{Q}$ by $a\circ b=2a+b$, $a,b\in\mathbb{Q}$. Show that $(\mathbb{Q},\circ)$ is a quasigroup but not a semigroup.
(A groupoid $(G,\circ)$ is said to be a quasi-group if for any two elements $a,b\in G$ each of the equation $a\circ x=b$ and $y\circ a=b$ has a unique solution in G.)

Solution: Here $(\mathbb{Q},\circ)$ is a groupoid. Now Consider the equation
$a\circ x=b$, $a,b\in\mathbb{Q}$
or, $2a+x=b \Rightarrow x=b-2a\in\mathbb{Q}$. So $b-2a$ is a solution of $a\circ x=b$. Let $x_1,x_2\in\mathbb{Q}$ be two solutions of $a\circ x=b$.
Then $a\circ x_1=b$, $a\circ x_2=b$. So $a\circ x_1=a\circ x_2$
$\Rightarrow 2a+x_1=2a+x_2 \Rightarrow x_1=x_2$. So $b-2a$ is the unique solution of $a\circ x=b$ in $\mathbb{Q}$.