Given a group G and a subgroup H, generally, it is not possible for a group homomorphism to exist which preserves the group operations. Passing the structure through a homomorphism is possible only when the equivalence relation $\sim$ generating the quotient set satisfies a certain condition.

It turns out that for well definedness (i.e, ϕ to be well defined) the equivalence relation must also be congruent. That is if $x \sim x'$, $y \sim y' \Rightarrow xy \sim x'y'$.

For the group G and subgroup H, $\sim_H$ is an equivalence relation defined as $a \sim_H b$ if $b^{-1}a \in H$.
The set of equivalence classes (quotient set) is denoted as G/H. Show that $\sim_H$ is a congruence relation if and only if H is normal.

$\sim_H$ is congruent $\iff$ H is a normal subgroup.

Example: $(\mathbb{Z}, +) \xrightarrow{\pi} \mathbb{Z}_n$, $\sim \equiv \bmod n$.
Show that the homomorphism π, is also a ring homomorphism.

$x \xmapsto{\pi} [x]$,

Given a ring R, and a ideal A of R, is it possible to construct a ring R', and a ring homomorphism ϕ such that $\ker \phi = A$, (i.e $\phi: R \longrightarrow R'$, $\ker \phi = A$).

Define a equivalence relation $\sim_A$; $x \sim_A y$ if $(x-y) \in A$.
Verify the following:
(i) $\sim_A$ is congruent.
(ii) The quotient generated by $\sim_A$ ($R/\sim_A$) has the well defined operations; (a) $[x]+[y] = [x+y]$,
(b) $[x] \cdot [y] = [x \cdot y]$, where $[x], [y] \in R/\sim_A$.

(iii) $R' = R/\sim_A$ is a ring with the above operations of '+' and '.'. The identity element for '+' operation is $A = [0]$. (equivalence class for the element 0).

(iv) Consider the map $\phi: R \longrightarrow R'$, $x \longmapsto [x]$. Show that ϕ is a ring homomorphism

(v) $\ker \phi = A$.

Cyclic groups: A group G is called cyclic if $G = H(x)$ for some $x \in G$.
Note that $H(x)$ could be finite or countably infinite.

G is called finitely generated if $G = H(x_1, x_2 \ldots x_r)$ where $H(x_1, x_2, \ldots x_r)$ is the smallest subgroup which contains $(x_1, x_2 \ldots x_r)$. The smallest subgroup can also be defined as follows: let H_i $(i \in I)$ be a family of subgroups which contain $(x_1, x_2 \ldots x_r)$. The smallest subgroup is $\bigcap_{i \in I} H_i$.

Show that $\bigcap_{i \in I} H_i$ is a subgroup.

15.1 Proposition: $(\mathbb{Q}, +)$ is not finitely generated.
Proof: (Based on fundamental theorem of arithmetic)
Suppose $(x_1, x_2, \ldots x_r)$ is a generating set for $(\mathbb{Q}, +)$. Since $x_i \in \mathbb{Q}$, each x_i should be of the form $x_i = \frac{a_i}{b_i}$, $a_i, b_i \in \mathbb{Z}$.

Therefore, the generating set $(x_1, x_2 \ldots x_r)$ can be replaced by $\left(\frac{1}{b_1}, \frac{1}{b_2}, \frac{1}{b_3} \ldots \frac{1}{b_r}\right)$.

In other words every element $x \in \mathbb{Q}$, can be expressed in the form

$$x = \frac{n_1}{b_1} + \frac{n_2}{b_2} \cdots \frac{n_r}{b_r}, \quad n_1, n_2, \ldots n_r \in \mathbb{Z}$$

$$\Rightarrow x = \frac{m}{\text{lcm}(b_1, b_2 \ldots b_r)} \quad \text{i.e} \quad \frac{1}{b} = \frac{1}{\text{lcm}(b_1, b_2 \ldots b_r)}$$

is also a generating set. Note that b is an integer, and therefore has a ~~pri~~ prime number decomposition. Choose a prime number q which does not divide b. Since $\frac{1}{b}$ is a generating number of $\mathbb{Q}$

$$\frac{1}{q} = \frac{c}{b} \Rightarrow b = cq$$ which is a contradiction

Therefore, $(\mathbb{Q}, +)$ is not finitely generated.

Given a ring R, consider the Abelian subgroup generated by 1_R. $m \cdot 1_R = \underbrace{1_R + 1_R \ldots 1_R}_{m \text{ times}} \quad m \in \mathbb{Z}, \; m > 0$

$$-m \cdot 1_R = \underbrace{-1_R - 1_R \cdots -1_R}_{m \text{ times}} \quad A$$

It is clear that $(m \cdot 1_R) \cdot (n \cdot 1_R) = (m \cdot n) \cdot 1_R \quad m, n \in \mathbb{Z}$

Show that the above set is a ring with the same operations. ~~Consider a sub-ring~~ The order of this ring is called the characteristic of R. Consider a subring R' of R. It contains the element 1_R. From the properties of a ring one can show that the subring generated by 1_R is contained in R'. Therefore, $m 1_R$ is the smallest subring containing the element 1_R. Moreover, $\text{char}(R') = \text{char}(R)$. Consider the ring homomorphism from $\mathbb{Z} \xrightarrow{\phi} R$, $\phi(1) \longrightarrow 1_R$, $\phi(n) \longrightarrow n \cdot 1_R$.

The image of ϕ is $m 1_R$.