Ideals and Quotient rings

An integral domain R is called Principal ~~dom~~ ideal domain (PID) if every ideal in R is a principal idea, i.e, $A = Rx$ for some $x \in R$.

Example: $\mathbb{Z}$ is a principal ideal domain because every ideal in $\mathbb{Z}$ is a principal ideal.

In any ring R, for every element $x \in R$, $Rx = \{ax \mid a \in R\}$ are principal ideals in R.

For a field K, what are the ideals?

$\{0\}$ is always a ideal. Kx is a ideal.

It is obvious $Kx \subseteq K$. $x \neq 0$

However, ~~consider~~ $x^{-1} \in K \Rightarrow x^{-1} \cdot x = 1 \in Kx$.

Any element $a \in K \Rightarrow (a \cdot x^{-1})x \in K. \Rightarrow K \subseteq Kx$

Therefore $Kx = K$.

14.1 Lemma: In any ring R, $x \neq 0$ in R, ~~Rx~~

$$Rx = R \iff x \in R^{\times}$$

Proof: (1) If $x \in R^{\times} \Rightarrow \exists y \in R^{*}$ such that $y \cdot x = 1$
$\Rightarrow y \cdot x = 1 \in Rx$. Consider any element $a \in R$. $a \cdot y \cdot x = a \in Rx \Rightarrow R \subseteq Rx$.
It is obvious that $Rx \subseteq R$.
Therefore $Rx = R$.

(2) Let $Rx = R. \Rightarrow \exists\, y \in R$ such that $y \cdot x = 1$
$\Rightarrow x \in R^{\times}$.

14.2 Proposition: Any ring R is a field iff 0, R are the only ~~fields~~ ideals in R.

Proof: Consider any ~~elem~~ ideal A of a field R.
If $x \in A$, then $x^{-1} \in R$, $\Rightarrow x \cdot x^{-1} = 1 \in A$.
Therefore any element $a \in R$, $\Rightarrow a \cdot x \cdot x^{-1} \in A$.

Since $A \subseteq R$, & $R \subseteq A \Rightarrow R = A$. (This proof is true only if $A \neq \{0\}$. Therefore, any ideal of a field is either R or 0.

For the converse, it is enough to show that $R^* \subseteq R^\times$. (Note $R^\times \subseteq R^*$). Let $x \in R^*$ ($x \neq 0$).
Rx is a ideal. Since the only ideals are $\{0\}$ and R, $Rx = R$. From lemma 14.1, $x \in R^\times$.
Therefore $(R^*, \cdot)$ is a group. $\Rightarrow$ R is a field.

If $R \xrightarrow{\phi} R'$ is a ring homomorphism, then

$$\operatorname{Ker} \phi = \{x \in R \mid \phi(x) = 0\} \subseteq R \text{ is an ideal in } R$$

$x \in \operatorname{Ker}\phi$ $a \in R \Rightarrow \phi(ax) = \phi(a)\phi(x) = 0$

$0 \in \operatorname{Ker}\phi$, $x, y \in \operatorname{Ker}\phi \Rightarrow (x-y) \in \operatorname{Ker}\phi$.

Therefore $\operatorname{Ker}\phi$ is an ideal.

> Given a ideal A, is it possible to construct an homomorphism ϕ such that
>
> $$R \xrightarrow{\phi} R', \quad \operatorname{Ker}\phi = A.$$

X is any set, $\sim$ is an equivalence relation on X.
The quotient set

$$X/\sim \; = \{[x] \mid [x] \text{ is the equivalence class of } x \text{ under } \sim\}$$

$$[x] = \{y \in X \mid x \sim y\}$$

There exists a surjective map $X \longrightarrow X/\sim$

$$x \longmapsto [x]$$

Example: In a commutative monoid M, $x \sim y \Leftrightarrow x, y$ are associates
Then, the quotient set $M/\sim$ is also a monoid.
Verify that $[x] \cdot [y] = [x \cdot y]$.

Another example: $M = (P(X), \cup)$ Let $\sim$ be the relation $A \sim B \iff |A| = |B|$ (1·1 → Cardinality)
Show that the above relation is an equivalence relation. However, the quotient set generated by this ~~mon~~ is not a monoid because the operation

$$[A][B] = [A \cup B] \text{ is not well defined.}$$

Check for ~~$[A] = \{a\}$~~ $A = \{a\}$, $B = \{b\}$.

Example: On $\mathbb{Z}$ the relation $\sim$ $\equiv (\text{mod } n)$

$$\mathbb{Z} \longrightarrow \mathbb{Z}_n$$
$$x \longmapsto r(x) \bmod n$$

This relation preserves the monoid operation.

Definition: Let M be a monoid and $\sim$ be an equivalence relation on M. We say that $\sim$ is an ~~equivalent~~ congruent relation (or $\sim$ is compatible with the binary operation on M) if whenever ~~$x \sim y$~~, $x \sim x'$, $y \sim y'$ then $xy \sim x'y'$.
In other words,

$$[x] = [x'],\ [y] = [y'] \Rightarrow [xy] = [x'y'].$$

Consider a group G, and a subgroup H of G.
Define $a \sim b$ if $b^{-1}a \in H$. i.e., $a \in bH$.
Show that $\sim$ is an equivalence relation
The equivalence class $[b] = bH$ are called the left cosets of H by b.
Define a map

$$G \xrightarrow{\pi} G/H$$
$$b \longmapsto bH.$$

Show that ~ is an congruent relation on G iff H is normal, i.e, $[a] \cdot [b] = [a \cdot b]$

Also, show that π ~~is~~ has as its kernel H.

i.e, $\ker \pi = H$.

Verify that G is abelian $\Longleftrightarrow$ every subgroup is normal.

There exists a bijective map $H \longrightarrow bH$. Therefore $|bH|$ is the same as $|H|$.

$\# G/H = [G:H] =$ index of H in G.

Since the equivalence classes are either equal or disjoint

$$G = \biguplus_{[x] \in G/H} [x]$$

$$\Rightarrow |G| = \sum_{[x] \in G/H} \# [x] = \# [x] \, \# G/H$$

$$= (\# H)(\# G/H)$$

Lagrange's theorem: If G is finite, and H is a subgroup, then $|H| \,/\, |G|$.

Corollary: Let $x \in G$, G is finite, $H(x)$ is the subgroup generated by x. Then $\operatorname{ord}(x) \mid |G|$.

In particular,

$$x^{|G|} = \left| x^{\operatorname{ord} x} \right|^{\frac{|G|}{\operatorname{ord}(x)}} = e.$$

The above statement is Fermat's little theorem.

Corollary: G is a finite group, $|G| = p$ prime No. $x \in G$, $x \neq e$, then

$$H(x) = \begin{cases} \{e\} & \text{if } x = e \\ G & \text{if } x \neq e. \end{cases}$$