Quotients and isomorphism theorems

Given $I \subseteq R$ an ideal, $R/I := \{$ cosets of I in R under $+\}$.

and $a+I = \{a+x \mid x \in I\}$ are the equivalence classes.

Since $(R,+)$ is abelian, $(I,+)$ is a normal subgroup $\Rightarrow$

$(R/I, +)$ is a group via $(a+I) + (b+I) = (a+b)+I$.

There's a natural binary operation, $\times$ on R/I given by,

$$(a+I) \times (b+I) = ab + I$$

Lemma $\times$ is well defined.

Pf Let $a_1, a_2, b_1, b_2 \in R$ s.t. $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$.

Then $a_1 - a_2 \in I$ and $b_1 - b_2 \in I$.

Thus, $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2$

$= a_1 \underbrace{(b_1 - b_2)}_{\in I} + \underbrace{(a_1 - a_2)}_{\in I} b_2$

Thus, $a_1 b_1 - a_2 b_2 \in I \Rightarrow a_1 b_1 + I = a_2 b_2 + I$ ∎

Lemma/Defn $(R/I, +, \times)$ is a ring, called the quotient ring. Note that $0_{R/I} = 0_R + I$ and $1_{R/I} = 1_R + I$.

Ex. $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ is the quotient of $m\mathbb{Z} \subseteq \mathbb{Z}$ as rings.

- There's a natural ring homomorphism,

$$\phi : R \to R/I, \quad x \mapsto x + I$$

Moreover, $I = \ker \phi$.

· [First isomorphism theorem for rings] Let $\phi: R \to S$ be a ring homomorphism. Then the map,

$$\bar{\phi}: R/\ker\phi \longrightarrow \operatorname{im}\phi \quad , \quad x+\ker\phi \longmapsto \phi(x)$$

is a ring homomorphism.

Pf By ~~first~~ isomorphism theorem for groups, we know $\bar{\phi}$ is well defined a group homomorphism.

Note $\bar{\phi}\left((x+\ker\phi)(y+\ker\phi)\right) = \bar{\phi}(xy+\ker\phi)$

$$= \phi(xy) = \phi(x)\phi(y)$$
$$= \bar{\phi}(x+\ker\phi)\,\bar{\phi}(y+\ker\phi).$$

Lastly, $\bar{\phi}(1_R+\ker\phi) = \phi(1_R) = 1_S$ ∎

· [Second isomorphism theorem for rings] Let R be a ring and $S \subseteq R$ a subring and I an ideal. Then,

① $S+I = \{s+x \mid x \in I, s \in S\}$ is a subring of R

② $S \cap I$ is an ideal of S and

$$S+I/I \cong S/S\cap I.$$

· [Third isomorphism theorem] Let $I \subseteq R$ be an ideal. There are a bijection of ~~sets~~ sets:

① $\{$subrings of R containing $I\} \longleftrightarrow \{$subrings of $R/I\}$

$S \longmapsto S/I$

② $\{$ideals of R containing $I\} \longleftrightarrow \{$ideals of $R/I\}$

$J \longmapsto J/I$

③ If $J \subseteq R$ an ideal and $I \subseteq J$ an ideal, then

$$(R/I)/(J/I) \cong R/J.$$

ALL RINGS are now assumed to be COMMUTATIVE

Defn Let R be a ring. An element $x \in R$ is said to be invertible, or a unit, if it has a multiplicative inverse i.e. $\exists\, y \in R$ s.t. $xy = yx = 1$.

Let $R^* = \{a \in R : a \text{ is a unit}\}$. This is called the group of units.

(Note if $x, y \in R^*$, then $xy \in R^*$. Indeed, if we write x^{-1}, y^{-1} for the respective inverses, we have $(xy)^{-1} = y^{-1} \cdot x^{-1}$.)

Defn A non trivial ring R in which every non-zero element is invertible is called a field i.e. $R - \{0\} = R^*$.

(We are assuming R is commutative)

Ex
- $\mathbb{Z}/p\mathbb{Z}$ is a field (see next page and note $[a] \in \mathbb{Z}/p\mathbb{Z}$ is a unit $\forall\, a \not\equiv p \pmod{p}$ as $\gcd(a,p) = 1$).
- $\mathbb{Z}^* = \{\pm 1\}$
- (non-commutative example) $M_n(\mathbb{C})^* = GL_n(\mathbb{C})$.
- $(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} : a \text{ coprime to } n\}$ (next page)

The group $(\mathbb{Z}/m\mathbb{Z})^*$

Let $m \geq 1$. Notice that $\times : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$,

$$[a] \times [b] := [a \cdot b]$$

(integer multiplication)

is a binary relation.

It satisfies the associativity and inverse axioms of a group.

But it fails the inverse axiom as $[0] \times y \neq [1] \quad \forall\, y \in \mathbb{Z}/m\mathbb{Z}$.

We can ask which elements have inverses?

[Euclidean Algorithm] Given $a, b \in \mathbb{Z} - \{0\}$, $\exists\, u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a,b)$. Moreover, if $au + bv = s$ then $\gcd(a,b) \mid s$.

Ex • $\gcd(4,6) = 2 \longrightarrow 6 \cdot 1 + 4(-1) = 2$

and $6u + 4v$ is always divisible

- $\gcd(a,b) = 1 \iff \exists\, u, v$ s.t. $au + bv = 1$
- $\gcd(5,7) = 1 \longrightarrow 5 \cdot 3 + 7 \cdot (-2) = 1$

Going back to $\mathbb{Z}/m\mathbb{Z}$ we have,

$$\begin{aligned}
[a] \cdot [b] = [1] &\iff [ab] = [1] \\
&\iff [ab - 1] = [0] \\
&\iff ab - 1 = m \cdot k \quad \text{for some } k \in \mathbb{Z} \\
&\iff a \cdot b + m(-k) = 1 \\
&\iff \gcd(a, m) = 1.
\end{aligned}$$

Thus $[a] \in \mathbb{Z}/m\mathbb{Z}$ has an inverse w.r.t. $\times$ iff a, m are coprime.