Ring Theory

Defn A (unital) ring R is a set with two binary operations $+$ and $\times$ such that

(1) $(R, +)$ is an abelian group

(2) $(R, \times)$ is a monoid (satisfies axiom (1) and (2) of a group: $r\times(s\times t) = (r\times s)\times t$ and $\exists\ 1_R \in R$ s.t. $1_R \times r = r \times 1_R = r\ \forall\ r, s, t$)

(3) [Distributive Law] $(x+y)\times z = (x\times z) + (y\times z)$
$x\times(y+z) = (x\times y) + (x\times z)$
$\forall\ x, y, z \in R$.

Ex
- $(\mathbb{Z}, +, \times)$ with 1 the "multiplicative identity"
- $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ with $[1]$ the " " "
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $(M_n(\mathbb{R}), +, \times)$
- $(C(\mathbb{R}), +, \times)$ ← continuous functions from $\mathbb{R} \to \mathbb{R}$
- $(\mathbb{C}[x], +, \times)$ where $\mathbb{C}[x] = \{$polynomials in x with coefficients in $\mathbb{C}\}$

Notation:
- 0_R is the additive identity (usually written 0)
- 1_R is the multiplicative identity (usually written 1)
- We will write xy instead of $x\times y$
- $$nx = \begin{cases} \underbrace{x + \dots + x}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{(-x) + \dots + (-x)}_{n \text{ times}} & \text{if } n < 0 \\ 0_R & \text{if } n = 0 \end{cases} \qquad x^n = \begin{cases} \underbrace{x \cdots x}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{x^{-1} \cdots x^{-1}}_{n \text{ times}} & \text{if } n < 0 \\ 1_R & \text{if } n = 0 \end{cases}$$
- Note by distributivity $(\sum x_i)(\sum y_i) = \sum x_i y_i$

Defn Let R, S be two rings. A homomorphism ϕ from R to S is a map of sets $\phi: R \to S$ such that $\forall x, y \in R$,

① $\phi(x+y) = \phi(x) + \phi(y)$ (so it's a group homomorphism under $+$)

② $\phi(xy) = \phi(x)\phi(y)$

③ $\phi(1_R) = 1_S$

- $id_R : R \to R$ is a homomorphism
- $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto [a]$ is a ring homomorphism.

Defn A homomorphism $\phi : R \to S$ is an isomorphism if it's bijective. We write $R \cong S$ to mean, $\exists\ \phi : R \to S$ an isomorphism.

- $\phi : R \to S$ an isomorphism $\iff$ $\exists\ \psi : S \to R$ an isomorphism
  $\iff$ $\exists\ \psi : S \to R$ homomorphism satisfying $\psi \circ \phi = id_R$ and $\phi \circ \psi = id_S$.
- An isomorphism $\phi : R \to R$ is called an automorphism.

Ex $\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is a homomorphism.

$[a]_{nm} \longmapsto ([a]_n, [a]_m)$

We have seen that this is an isomorphism $\iff n, m$ are coprime.

Defn R a ring and $S \subseteq R$ a subset. We say S is a subring of R if

① $(S, +)$ is a subgroup of $(R, +)$

② $\forall x, y \in S \Rightarrow xy \in S$

③ $1_R \in S$

Of course $(S, +, \times)$ inherits the operations of R.

Ex • $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$

• $M_n(\mathbb{R}) \subseteq M_n(\mathbb{C})$.

Lemma $0_R \cdot x = 0_R = x \cdot 0_R \quad \forall x \in R$

Defn The trivial ring is the ring containing 1 element

Lemma R is trivial $\iff 0_R = 1_R$

Pf If $0_R = 1_R$, then $x = x \cdot 1_R = x \cdot 0_R = 0_R \ \forall x \in R \Rightarrow |R| = 1$ ∎

Other constructions

• Given $R_1, \dots, R_n$ rings we have a direct product of rings, $R_1 \times \cdots \times R_n$ with $1_{R_1 \times \cdots \times R_n} = (1_{R_1}, \dots, 1_{R_n})$ and $+, \times$ defined coordinate wise.

• If $\{S_i\}$ is a collection of subrings of R, $\bigcap_i S_i$ is a subring of R.

Defn If $\phi : R \to S$ is a homomorphism define,
$\ker \phi = \{x \in R \mid \phi(x) = 0_R\}$ and $\operatorname{im} \phi = \{\phi(x) \in S \mid x \in R\}$.

• We know that $\ker \phi$ and $\operatorname{im} \phi$ are subgroups, since $\phi : (R,+) \to (S,+)$ is a group homomorphism.

Prop $\operatorname{Im}(\phi) \subseteq S$ is a subring of S.

Pf • $\operatorname{Im}(\phi) \subseteq S$ is a subgroup

• $\phi(x), \phi(y) \in \operatorname{Im}(\phi) \Rightarrow \phi(x)\phi(y) = \phi(xy) \in \operatorname{Im} \phi$ (homomorphism)

• $\phi(1_R) = 1_S \in S$ ∎

Unfortunately (?), $\ker \phi$ is <u>NOT</u> a subring of R:

Lemma $\ker\phi \subseteq R$ is a subring $\iff$ S is trivial $\iff$ $\ker\phi = R$.

Pf $\ker\phi$ subring $\iff$ $1_R \in \ker\phi$ $\iff$ $\phi(1_R) = 0_S$. But $\phi(1_R) = 1_S$. Thus $1_S = 0_S \iff S$ is trivial $\iff \ker\phi = R$ ∎

(↑ other requirements are satisfied)

Although $\ker\phi$ is not a subring, its an "ideal":

Defn Let R be a ring. An ideal $I \subseteq R$ is a subset satisfying,

1. I is a subgroup under $+$
2. $\forall x \in I$, $r \in R \Rightarrow x\cdot r, r\cdot x \in I$.

Ex • $\ker\phi$ is an ideal:

1. $\ker\phi$ is a subgroup under $+$
2. $\forall x \in \ker\phi$ and $r \in R$ we have,

$\phi(rx) = \phi(r)\phi(x) = \phi(r)\cdot 0_S = 0_S \Rightarrow rx \in \ker\phi$. Similarly $xr \in \ker\phi$.

- $\{0_R\}$ and R are ideals of R
- $m\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal of $\mathbb{Z}$, not a subring.
- Generalizing the above lemma, I an ideal is a subring $\iff I = R \iff 1_R \in I$.