Commutative Algebra: Rings

Dr. Zvi Rosen

Department of Mathematical Sciences,
Florida Atlantic University

Definition: Ring

Let A be a set with two binary operations, addition & multiplication

s.t. 1) $(A, +)$ is an abelian gp.

0_A, additive inverses, + comm

2) $\times$ associative, distributes over the addition on Left and Right. $a(bc) = (ab)c$.

Definition: Ring

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc.$$

3) $\times$ comm. (comm. ring)

$$xy = yx.$$

4) 1_A multiplicative identity.

Is the Abelian group axiom necessary?

Use 1_A as multipl. identity.

$$(1_A+x)(1_A+y) = 1_A(1_A+y)+x(1_A+y)$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$(1_A+x)1_A+(1_A+x)y \qquad \cancel{1_A}+y+x+\cancel{xy}.$$

$$\cancel{1_A}+x+y+\cancel{xy}.$$

$$x+y=y+x.$$

What if we drop properties?

- No additive inverses. (i.e. semigroup under +)

semi-ring. Ex Tropical semi-ring.

- No 1_A (multiplicative identity).

rng (missing i) Ex Any 2-sided ideal in a ring.

- Distributive on one side only, and $(A, +)$ not abelian.

near-ring. Ex Functions on a group.

Some Commutative Rings you Probably Know

$\mathbb{Z}$ integers.

$\mathbb{Q}$ rationals

$\mathbb{R}$ reals.

$\mathbb{C}$ complex numbers.

$\mathbb{Z}/n\mathbb{Z}$ integers mod n.

$C(X)$ continuous fns on topological sp X.

$R[x]$ ring of polynomials in x with coeffs in R.

$R[[x]]$ power series in x with coeffs in R.

Some Noncommutative Rings you Might Know

$\mathbb{H}$ = ring of Hamilton Quaternions

$$\{a + bi + cj + dk \mid i^2 = j^2 = k^2 = -1,\ ijk = 1\}.$$

$M_n(R)$ = $n \times n$ matrices with entries in R.

$$RG = \left\{\sum_{i \in I} a_i g_i : a_i \in R,\ g_i \in G\right\}.$$

$$(ag)(bh) = (ab)(gh)$$

× ring group operation.

Definition: Ring Homomorphism

Map $f: A \to B$ satisfying

1) $f(x+y) = f(x) + f(y)$

2) $f(xy) = f(x)f(y)$.

3) $f(1_A) = 1_B$.

Examples of Ring Homomorphisms

$$\mathbb{Z} \longrightarrow \mathbb{Q}$$
$$n \longmapsto n$$

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$a \longmapsto a \bmod n$$

$$\mathbb{Q}[x] \longrightarrow \mathbb{Q}$$
$$p(x) \longmapsto p(1).$$

$f(0)$ and $f(1)$

We were told $f(1_A) = 1_B$.

What about $f(0)$?

$$f(a+b) = f(a) + f(b)$$

$$\cancel{f(a)} = f(a+0_A) = \cancel{f(a)} + f(0_A)$$

$$\Rightarrow f(0_A) = 0_B.$$

Definition: Subring

$S \subseteq A$ ring.

$1_A \in S$.

S closed under add., mult.

$\Rightarrow S$ subring of A.

$$\begin{tikzcd}
& \mathbb{Q}[x] \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q} \arrow[dr, dash] & & \mathbb{Z}[x] \arrow[dl, dash] \\
& \mathbb{Z} &
\end{tikzcd}$$

Definition: Ideal & Quotient

- An ideal of A is an additive subgroup $\mathfrak{a} \subset A$ closed under mult. by A

  i.e. $\forall x \in A, \forall a \in \mathfrak{a}, \quad xa \in \mathfrak{a}$.

- Quotient $A/\mathfrak{a} \ \{(r+\mathfrak{a}) : r \in A\}$

  $(r+\mathfrak{a}) + (s+\mathfrak{a}) = (r+s)+\mathfrak{a}$

  $(r+\mathfrak{a})(s+\mathfrak{a}) = rs+\mathfrak{a}$

Why must ideals be closed under multiplication by A?

$$(r+\mathfrak{a})(s+\mathfrak{a}) = rs + \mathfrak{a}$$

$$(r+a)(s+b) \qquad a, b \in \mathfrak{a}$$

$$\| $$

$$rs + as + rb + ab \overset{\text{WANT}}{\equiv} rs \mod \mathfrak{a}$$

$$as + rb + ab \in \mathfrak{a}$$

Set $a = 0$, $\quad rb \in \mathfrak{a}. \Rightarrow \mathfrak{a}A \subseteq \mathfrak{a}.$

Bijection between sets of ideals

Proposition 1.1 (Atiyah-MacDonald)

There is a one-to-one order-preserving correspondence between ideals $\mathfrak{b} \subset A$ containing $\mathfrak{a}$ and ideals $\tilde{\mathfrak{b}} \subset A/\mathfrak{a}$.

$A = \mathbb{Z}$ $\quad \mathfrak{a} = 20\mathbb{Z}$

ideals containing $\mathfrak{a}$: $\mathbb{Z}, 2\mathbb{Z}, 4\mathbb{Z}, 5\mathbb{Z}, 10\mathbb{Z}$.

...

in $\mathbb{Z}/20\mathbb{Z}$: $\mathbb{Z}/20\mathbb{Z}, 2\mathbb{Z}/20\mathbb{Z}, 4\mathbb{Z}/20\mathbb{Z},$

$5\mathbb{Z}/20\mathbb{Z}, 10\mathbb{Z}/20\mathbb{Z}$.

Kernel and Image

Let $f: A \to B$ be ring homomorphism.

$\ker(f) = \{ x \in A : f(x) = 0 \}$

$\mathrm{im}(f) = \{ x \in B : \exists y \in A, f(y) = x \}$.

- kernel is an ideal.

$$f(x) = 0 \Rightarrow f(ax) = f(a)\underbrace{f(x)}_{0} = 0.$$

- image is a subring.

$f(1_A) = 1_B$. $f(x) + f(y) = f(x+y) \ldots$

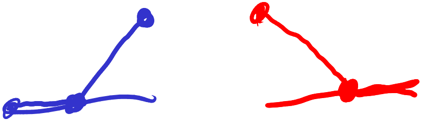
Definition: Zero-divisor

A ring. $x \in A$ is zero-divisor

if $\exists y \in A$, $y \neq 0$, s.t. $xy = 0$.

<u>ex</u> $\mathbb{Z}/6\mathbb{Z}$: $2, 3 \neq 0$, $2 \cdot 3 = 0$.

$C([0,1])$:



zero-divisors

Ring with no zero-divisors is an integral domain.

Definition: Nilpotent

Let A be ring.

$x \in A$ is nilpotent if $\exists n \in \mathbb{N}$

s.t. $x^n = 0$.

Ex

$\mathbb{Z}/8\mathbb{Z}$: 2 nilpotent.

$M_2(\mathbb{R})$: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ nilpotent (not comm ring)

Definition: Principal Ideal

Ideal given by all multiples of $x \in A$. Written as (x) or Ax.

Ex $12\mathbb{Z}$ principal ideal.

$\{12, 24, -12, \ldots\}$

$(x^2-1) \subset \mathbb{Q}[x]$

$\{x^2-1, x^3-x, 2x^2-2, x^3+x^2-x-1, \ldots\}$

Non-ex $(2, x) \subset \mathbb{Z}[x]$.

Definition: Unit, Field

A ring. $x \in A$ unit if $\exists y \in A$ s.t. $xy = 1_A$.

If all elements of A are units then A is a field.

Fields, ideals, and homomorphisms

Proposition 1.2 (Atiyah-MacDonald)

Let A be a nonzero ring. TFAE:

1. A is a field.
2. The only ideals of A are 0 and (1).
3. Every homomorphism of A to a non-zero ring B is injective.

$1 \Rightarrow 2$ $\quad (x)$ includes $xy = 1 \Rightarrow (x) = (1)$ unless $x = 0$.

$2 \Rightarrow 3$ $\quad \ker f : A \to B$ not (1).

$\Rightarrow \ker f = (0) \Rightarrow f$ inj.