NOTES ON RINGS

ARTHUR RYMAN

ABSTRACT. This article contains formal definitions for mathematical concepts related to rings. It uses Z Notation and has been type checked by *f*UZZ.

CONTENTS

INTRODUCTION

This article contains notes from the course *Computational Commutative Algebra and Algebraic Geometry* taught by Professor Michael Stillman in Winter 2025 as part of the Fields Academy Shared Graduate Courses program. It contains formal definitions for mathematical concepts related to rings. It uses Z Notation[3] and has been type checked by *f*UZZ[4].

0.1. **Source Material.** The course is concerned with Computational Commutative Algebra and Algebraic Geometry. The course uses `Macaulay2` for computation. I'll use [1] as the source for Commutative Algebra and [2] as the source for Algebraic Geometry.

0.2. **Type Checking.** I'll start by pulling in the set of real numbers $\mathbb{R}$, and its zero element 0. So far, these are just LaTeX commands.

Next, I'll say something formal about them.

Remark. *Zero is a real number.*

$0 \in \mathbb{R}$

Date: February 2, 2025.

0.3. **TODO List.** Define enough terms so that I can express the problem sets. Also try to write formal specifications for the data types and functions in `Macaulay2`.

Define the following terms:

- ring
- homomorphism
- ideal
- field
- quotient of ring modulo an ideal
- ideal quotient, colon ideal
- Hilbert series, function
- monomial order
- Gröbner basis
- elimination as in `Macaulay2`

1. Rings and Ideals

Refer to [1, Chapter 1] for definitions.

1.1. Rings and Ring Homomorphisms.

A *ring* A is a set with addition and multiplication operations such that:

(1) The set A is an abelian group with respect to addition. The zero element is denoted by 0 and the additive inverse of $x \in A$ is denoted by $-x$.

(2) Multiplication is associative ($(xy)z = x(yz)$) and distributive over addition ($x(y + z) = xy + xz, (y + z)x = yx + zx$).

(3) The ring is said to be *commutative* if the multiplication is commutative.

(4) The ring is said to have an *identity element* if it has an element that is a left and right multiplicative identity

1.1.1. *Rings.*

The first two axioms define a general ring. As a structure, we define a ring $\mathbf{A}$ to be a triple $(A, (\_+\_), (\_*\_))$ consisting of a set, an addition operation, and a multiplication operation.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Ring\_Core}[\mathsf{t}]} \\
A : \mathbb{P}\,\mathsf{t} \\
\_+\_, \_*\_ : \textit{PBinOp}[\mathsf{t}] \\
\mathbf{A} : \mathbb{P}\,\mathsf{t} \times \textit{PBinOp}[\mathsf{t}] \times \textit{PBinOp}[\mathsf{t}] \\
\hline
(A, (\_+\_)) \in \textit{abgroup}[A] \\
(A, (\_*\_)) \in \textit{semigroup}[A] \\
\forall\, x, y, z : A \bullet x * (y + z) = (x * y) + (x * z) \\
\forall\, x, y, z : A \bullet (y + z) * x = (y * x) + (z * x) \\
\mathbf{A} = (A, (\_+\_), (\_*\_)) \\
\hline
\end{array}
$$

- addition is an abelian group
- multiplication is a semigroup
- left multiplication distributes over addition
- right multiplication distributes over addition
- the structure is a triple consisting of the carrier and two operations

The additive identity element is denoted 0, the additive inverse of x is denoted $\text{-}\,x$, and the sum of x and $\text{-}\,y$ is denoted $x - y$.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Ring}[\mathsf{t}]} \\
\textit{Ring\_Core}[\mathsf{t}] \\
0 : \mathsf{t} \\
\text{-} : \mathsf{t} \rightarrow\!\!\!\!\!\!+\;\; \mathsf{t} \\
\_-\_ : \textit{PBinOp}[\mathsf{t}] \\
\hline
0 = \textit{identity\_element}(A, (\_+\_)) \\
(\lambda\, x : A \bullet \text{-}\,x) = \textit{inverse\_operation}(A, (\_+\_)) \\
(\_-\_) = (\lambda\, x, y : A \bullet x + (\text{-}\,y)) \\
\hline
\end{array}
$$

- 0 is the additive identity element
- $\text{-}\,x$ is the additive inverse of x
- subtraction is defined in terms of addition and negation

Define $\textit{rng}[\mathsf{t}]$ to be the set of all rings in t. Here we omit the letter i from the word *ring* to remind us that a ring might not have a multiplicative identity element.

$\textit{rng}[\mathsf{t}] == \{\, \textit{Ring}[\mathsf{t}] \bullet \mathbf{A} \,\}$

Example. *The integers with addition and multiplication is a ring.*

$(\mathbb{Z}, (\_+\_), (\_*\_)) \in \textit{rng}[\mathbb{Z}]$

1.1.2. *Ring Homomorphisms.* Let $\mathbf{A}$ and $\mathbf{A}'$ be rings. A *ring homomorphism* from $\mathbf{A}$ to $\mathbf{A}'$ is a function f from A to A' that preserves the addition and multiplication operations. As a structure, we represent a ring homomorphism F as the pair $(\mathbf{A}, \mathbf{A}') \mapsto f$.

$$
\begin{array}{|l}
\hline
\textit{Ring\_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Ring}[\mathsf{t}] \\
\textit{Ring}'[\mathsf{u}] \\
f : \mathsf{t} \pfun \mathsf{u} \\
F : (\textit{rng}[\mathsf{t}] \times \textit{rng}[\mathsf{u}]) \times (\mathsf{t} \pfun \mathsf{u}) \\
\hline
f \in A \longrightarrow A' \\
\forall x, y : A \bullet f(x + y) = f(x) +' f(y) \\
\forall x, y : A \bullet f(x * y) = f(x) *' f(y) \\
F = (\mathbf{A}, \mathbf{A}') \mapsto f \\
\hline
\end{array}
$$

- f maps A to A'
- f preserves addition
- f preserves multiplication
- the homomorphism as a structure consists of the pair of rings and the map between them

Define $\textit{rng\_Hom}[\mathsf{t}, \mathsf{u}]$ to be the set of all ring homomorphisms from rings in t to rings in u.

$$\textit{rng\_Hom}[\mathsf{t}, \mathsf{u}] == \{ \textit{Ring\_Hom}[\mathsf{t}, \mathsf{u}] \bullet F \}$$

Define $\textit{rng\_hom}(\mathbf{A}, \mathbf{A}')$ to be the set of all ring homomorphism from $\mathbf{A}$ to $\mathbf{A}'$.

$$
\begin{array}{l}
\textit{rng\_hom}[\mathsf{t}, \mathsf{u}] == \\
\quad (\lambda\, \mathbf{A} : \textit{rng}[\mathsf{t}]; \mathbf{A}' : \textit{rng}[\mathsf{u}] \bullet \\
\qquad \{ (\mathbf{A}, \mathbf{A}') \} \lhd \textit{rng\_Hom}[\mathsf{t}, \mathsf{u}])
\end{array}
$$

1.1.3. *Identity Maps.* Define $\textit{rng\_id}[\mathsf{t}]$ to be the set of all identity maps from rings in t to themselves.

$$\textit{rng\_id}[\mathsf{t}] == \{ \textit{Ring}[\mathsf{t}] \bullet (\mathbf{A}, \mathbf{A}) \mapsto \mathrm{id}\, A \}$$

Remark. *The identity map on any ring is a homomorphism.*

$$\textit{rng\_id}[\mathsf{T}] \subseteq \textit{rng\_Hom}[\mathsf{T}, \mathsf{T}]$$

1.1.4. *Composition.* Given ring homomorphisms f from A to A' and f' from A' to A'', we can define their *composition* $g = f' \circ f$ from A to A''.

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{Ring\_Composition}[\mathsf{t},\mathsf{u},\mathsf{v}]} \\
\mathit{Ring\_Hom}[\mathsf{t},\mathsf{u}] \\
\mathit{Ring\_Hom}'[\mathsf{u},\mathsf{v}] \\
g : \mathsf{t} \pfun \mathsf{v} \\
G : (\mathit{rng}[\mathsf{t}] \times \mathit{rng}[\mathsf{v}]) \times (\mathsf{t} \pfun \mathsf{v}) \\
\hline
g = f' \circ f \\
G = (\mathbf{A}, \mathbf{A}'') \mapsto g \\
\hline
\end{array}
$$

Remark. *The composition of ring homomorphisms is a ring homomorphism.*

$\forall\, \mathit{Ring\_Composition}[\mathsf{T},\mathsf{U},\mathsf{V}] \bullet G \in \mathit{rng\_hom}(\mathbf{A}, \mathbf{A}'')$

Let $G = F' \circ F$ denote the composition of ring homomorphisms.

$(\_ \circ \_)[\mathsf{t},\mathsf{u},\mathsf{v}] == \{\, \mathit{Ring\_Composition}[\mathsf{t},\mathsf{u},\mathsf{v}] \bullet (F', F) \mapsto G \,\}$

TODO: remark that the identity map is a left and right identity element under composition

1.1.5. *Commutative Rings.* A ring is said to be *commutative* if its multiplication is commutative.

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{CommRing}[\mathsf{t}]} \\
\mathit{Ring}[\mathsf{t}] \\
\hline
\forall\, x, y : A \bullet x * y = y * x \\
\hline
\end{array}
$$

- multiplication is commutative

Define $\mathit{commrng}[\mathsf{t}]$ to be the set of all commutative rings in t.

$\mathit{commrng}[\mathsf{t}] == \{\, \mathit{CommRing}[\mathsf{t}] \bullet A \,\}$

TODO: define homomorphisms, identity maps, composition, and composition with identity maps

1.1.6. *Unital Rings.* A ring is said to have an *identity element* if it has a left and right multiplicative identity element. In other words, the multiplication operation is a monoid. A ring with an identity element is also said to be a *unital* ring. The multiplicative identity element of a unital ring is denoted 1.

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{UnitalRing}[\mathsf{t}]} \\
\mathit{Ring}[\mathsf{t}] \\
1 : \mathsf{t} \\
\hline
(A, (\_ * \_)) \in \mathit{monoid}[A] \\
1 = \mathit{identity\_element}(A, (\_ * \_)) \\
\hline
\end{array}
$$

- the multiplication operation is a monoid
- the multiplicative identity element is denoted 1

Define $ring[\mathsf{t}]$ to be the set of all unital rings in t.

$ring[\mathsf{t}] == \{ \, UnitalRing[\mathsf{t}] \bullet \mathbf{A} \, \}$

TODO: define homomorphisms, identity maps, composition, and composition with identity maps

1.1.7. *Commutative Unital Rings.* Commutative algebra is primarily concerned with commutative, unital rings.

$$\begin{array}{|l}
\hline
CURing[\mathsf{t}] \\
CommRing[\mathsf{t}] \\
UnitalRing[\mathsf{t}] \\
\hline
\end{array}$$

Define $commring[\mathsf{t}]$ to be the set of commutative unital rings in t.

$commring[\mathsf{t}] == \{ \, CURing[\mathsf{t}] \bullet \mathbf{A} \, \}$

TODO: define homomorphisms, identity maps, composition, and composition with identity maps

For the remainder of this article the term *ring* will denote a commutative ring with an identity element. However, the formal notation will always be explicit.

1.1.8. *Zero Rings.* If the additive and multiplicative identity elements are the same then the ring is said to be a *zero ring*.

$$\begin{array}{|l}
\hline
ZeroRing[\mathsf{t}] \\
CURing[\mathsf{t}] \\
\hline
1 = 0 \\
\hline
\end{array}$$

- the additive and multiplicative identity elements are the same

Remark. *A zero ring contains exactly one element, namely the zero element.*

$\forall \, ZeroRing[\mathsf{T}] \bullet A = \{0\}$

Proof.

$x : A$ [assumption-intro]

x

$= x * 1$ [1 is the identity element]

$= x * 0$ [$1 = 0$ by *ZeroRing*]

$= 0$ [0 is the zero element]

$x : A \Rightarrow x = 0$ [assumption-elim]

$A = \{0\}$ [set extensionality]

□

TODO: remark on the universal properties of the zero ring in each of the four categories of rings

1.1.9. *Ring Homomorphisms.* A ring homomorphism is a mapping f from ring A into ring A' that preserves addition, multiplication, and identity elements.

$$
\begin{array}{|l}
\hline
\textit{CURing\_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Ring\_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{CURing}[\mathsf{t}] \\
\textit{CURing}'[\mathsf{u}] \\
f : \mathsf{t} \nrightarrow \mathsf{u} \\
\hline
f \in A \longrightarrow A' \\
\forall\, x, y : A \bullet f(x + y) = f(x) +' f(y) \\
\forall\, x, y : A \bullet f(x * y) = f(x) *' f(y) \\
f(1) = 1' \\
\hline
\end{array}
$$

TODO: merge this in with the general discussion of homomorphisms

1.1.10. *Subrings.* A subring A of A' is a subset of elements that contains the identity element and is closed under addition and multiplication.

TODO: use S and A to match textbook

$$
\begin{array}{|l}
\hline
\textit{CURing\_Subring}[\mathsf{t}] \\
\textit{CURing}'[\mathsf{t}] \\
A : \mathbb{P}\,\mathsf{t} \\
\hline
A \subseteq A' \\
1' \in A \\
\forall\, x, y : A \bullet x +' y \in A \\
\forall\, x, y : A \bullet x *' y \in A \\
\hline
\end{array}
$$

A subring itself becomes a ring by restriction of the enclosing ring operations.

$$
\begin{array}{|l}
\hline
\textit{CURing\_Restriction}[\mathsf{t}] \\
\textit{CURing\_Subring}[\mathsf{t}] \\
\textit{CURing}[\mathsf{t}] \\
\hline
(\_ + \_) = (\lambda\, x, y : A \bullet x +' y) \\
(\_ * \_) = (\lambda\, x, y : A \bullet x *' y) \\
\hline
\end{array}
$$

Set inclusion defines a map f from the subring to the ring.

$$
\begin{array}{|l}
\hline
\textit{CURing\_Inclusion}[\mathsf{t}] \\
\textit{CURing\_Restriction}[\mathsf{t}] \\
f : \mathsf{t} \nrightarrow \mathsf{t} \\
F : (\textit{commring}[\mathsf{t}] \times \textit{commring}[\mathsf{t}]) \times (\mathsf{t} \nrightarrow \mathsf{t}) \\
\hline
f = (\lambda\, x : A \bullet x) \\
F = (\mathbf{A}, \mathbf{A}') \mapsto f \\
\hline
\end{array}
$$

Remark. *Subring inclusion is a ring homomorphism.*

$\forall \, CURing\_Inclusion[\mathsf{T}] \bullet CURing\_Hom[\mathsf{T}, \mathsf{T}]$

1.1.11. *Composition.* Given homomorphisms $f : A \longrightarrow A'$ and $f' : A' \longrightarrow A''$ their composition $f' \circ f$ is a mapping $g : A \longrightarrow A''$.

$CURing\_Composition[\mathsf{t}, \mathsf{u}, \mathsf{v}]$

$CURing\_Hom[\mathsf{t}, \mathsf{u}]$
$CURing\_Hom'[\mathsf{u}, \mathsf{v}]$
$g : \mathsf{t} \twoheadrightarrow \mathsf{v}$

$g = f' \circ f$

Remark. *The composition of homomorphisms is a homomorphism.*

TODO: merge with general discussion

NOTE: the preceding sections should be completed and made consistent with eachother, however, I will continue on with formalizing the content of Atiyah-MacDonald so I can determine if anything is actually hard to formalize, and also so that I can be more effective with Macaulay 2.

1.2. **Ideals. Quotient rings.** An *ideal* $\mathfrak{a}$ of a ring A is a subset of A that is an additive subgroup and is such that $A\mathfrak{a} \subseteq \mathfrak{a}$.

$Ideal[\mathsf{t}]$

$CURing[\mathsf{t}]$
$\mathfrak{a} : \mathbb{P}\, \mathsf{t}$

$\mathfrak{a} \subseteq A$

$\forall \, x, y : \mathfrak{a} \bullet x + y \in \mathfrak{a} \wedge x - y \in \mathfrak{a}$

$\forall \, x : A; \, y : \mathfrak{a} \bullet x * y \in \mathfrak{a}$

- the ideal is a subset of the ring
- the ideal is closed under addition and subtraction, making it a subgroup
- the ideal is closed under multiplication by elements of the ring

The quotient group $A/\mathfrak{a}$ inherits a well-defined multiplication from A making a a ring called the *quotient ring* (or *residue class ring* $A/\mathfrak{a}$.

$QuotientRing[\mathsf{t}]$

$CURing\_Hom[\mathsf{t}, \mathbb{P}\, \mathsf{t}]$
$Ideal[\mathsf{t}]$

$f = (\lambda \, x : A \bullet \{ \, y : \mathfrak{a} \bullet x + y \, \})$

$A' = \operatorname{ran} f$

TODO: first define the quotient group and the projection and cosets, showing that the projection is a homomorphism. we need to show that the cosets from an additive group. Then show that the cosets form a monoid. The moral of the story is that I can't skip any steps. Otherwise the definitions get big and repetitive.

1.3. **Zero-divisors. Nilpotent elements. Units.**

1.4. **Prime ideals and maximal ideals.**

1.5. **Nilradical and Jacobson radical.**

1.6. **Operations on ideals.**

1.7. **Extension and contraction.**

1.8. **Exercises.**

References

[1] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Addison-Wesley, 1969.
[2] Robin Hartshorne. *Algebraic Geometry*. 1st. Graduate Texts in Mathematics 52. Springer, 1977.
[3] J. M. Spivey. *The Z Notation*. Second Edition. Prentice Hall International, 1992. URL: `https://spivey.oriel.ox.ac.uk/wiki/files/zrm/zrm.pdf`.
[4] Mike Spivey. *The fUZZ Manual*. Second Edition. The Spivey Partnership, 2000. URL: `https://github.com/Spivoxity/fuzz/blob/59313f201af2d536f5381e65741ee6d98db54a70/doc/fuzzman-pub.pdf`.

Email address, Arthur Ryman: `arthur.ryman@gmail.com`