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

1. 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].

1.1. 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.

1.2. 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: January 31, 2025.

1.3. **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`

2. Rings and Ideals

Refer to [1, Chapter 1] for definitions.

2.1. **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

2.1.1. *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.

Ring_Core[t]

$A : \mathbb{P}\,\mathsf{t}$

$\_ + \_, \_ * \_ : PBinOp[\mathsf{t}]$

$\mathbf{A} : \mathbb{P}\,\mathsf{t} \times PBinOp[\mathsf{t}] \times PBinOp[\mathsf{t}]$

$(A, (\_ + \_)) \in abgroup[A]$

$(A, (\_ * \_)) \in semigroup[A]$

$\forall\, x, y, z : A \bullet x * (y + z) = (x * y) + (x * z)$

$\forall\, x, y, z : A \bullet (y + z) * x = (y * x) + (z * x)$

$\mathbf{A} = (A, (\_ + \_), (\_ * \_))$

- 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 $x - y$.

Ring[t]

Ring_Core[t]

$0 : \mathsf{t}$

$\text{-} : \mathsf{t} \rightarrowtail\!\!\!\!\!+ \; \mathsf{t}$

$\_ - \_ : PBinOp[\mathsf{t}]$

$0 = identity\_element(A, (\_ + \_))$

$(\lambda\, x : A \bullet \text{-}\,x) = inverse\_operation(A, (\_ + \_))$

$(\_ - \_) = (\lambda\, x, y : A \bullet x + (\text{-}\,y))$

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

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

CommutativeRing[t]

Ring[t]

$\forall\, x, y : A \bullet x * y = y * x$

- multiplication is commutative

2.1.3. *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.

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

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

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{CURing}[\mathsf{t}]} \\
\hline
\mathit{CommutativeRing}[\mathsf{t}] \\
\mathit{UnitalRing}[\mathsf{t}] \\
\hline
\end{array}
$$

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.

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

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

- the additive and multiplicative identity elements are the same

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

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

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]

□

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

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

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

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

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

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

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

$$
\begin{array}{|l}
\hline
\mathit{CURing\_Inclusion}[\mathsf{t}] \\
\mathit{CURing\_Restriction}[\mathsf{t}] \\
f : \mathsf{t} \leftrightarrow \mathsf{t} \\
\hline
f = (\lambda\, x : A \bullet x) \\
\hline
\end{array}
$$

Remark. *Subring inclusion is a ring homomorphism.*

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

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

$$
\begin{array}{|l}
\hline
\textit{CURing\_Composition}[\mathsf{t}, \mathsf{u}, \mathsf{v}] \\
\hline
\textit{CURing\_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{CURing\_Hom}'[\mathsf{u}, \mathsf{v}] \\
g : \mathsf{t} \rightarrow\!\!\!\!\!\rightarrow \mathsf{v} \\
\hline
g = f' \circ f \\
\hline
\end{array}
$$

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

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`