

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	1
2. Rings and Ideals	2
References	8

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. Typechecking. I'll start by pulling in the set of real numbers \mathbb{R} , and its zero element 0. So far, these are just *L*^AT_EX commands.

Next, I'll say something formal about them.

Remark. *Zero is a real number.*

$0 \in \mathbb{R}$

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. *Elements.* A ring has a set of elements.

$\begin{array}{l} \text{Ring_Elements}[\mathbf{t}] \\ A : \mathbb{P} \mathbf{t} \end{array}$

2.1.2. *Addition.* A ring has a binary operation of addition on its element.

$\begin{array}{l} \text{Ring_Add}[\mathbf{t}] \\ \text{Ring_Elements}[\mathbf{t}] \\ _ + _ : \mathbf{t} \times \mathbf{t} \leftrightarrow \mathbf{t} \end{array}$
$(_ + _) \in A \times A \longrightarrow A$

- addition is a binary operation on A

Addition is associative.

$Ring_Add_Associative[t]$	_____
$Ring_Add[t]$	
$\forall x, y, z : A \bullet (x + y) + z = x + (y + z)$	

- addition is associative

A ring has a zero element that is the identity element under addition.

$Ring_Zero[t]$	_____
$Ring_Add[t]$	
$0 : t$	
$0 \in A$	
$\forall x : A \bullet 0 + x = x = x + 0$	

- A has an element 0
- 0 is an additive identity element

A ring has a unary operation of negation that maps each element to its additive inverse.

$Ring_Neg[t]$	_____
$Ring_Zero[t]$	
$- : t \rightarrow t$	
$- \in A \rightarrow A$	
$\forall x : A \bullet x + (-x) = 0 = (-x) + x$	

- negation is a unary operation on A
- $-x$ is the additive inverse of x

It is convenient to define the binary operation of subtraction in terms of addition and negation.

$Ring_Sub[t]$	_____
$Ring_Neg[t]$	
$- - : t \times t \rightarrow t$	
$(- -) \in A \times A \rightarrow A$	
$\forall x, y : A \bullet x - y = x + (-y)$	

- subtraction is a binary operation on A
- subtraction is defined in terms of addition and negation

A ring is a group under addition.

$\text{Ring_Add_Group}[\mathbf{t}]$
$\text{Ring_Add_Associative}[\mathbf{t}]$
$\text{Ring_Zero}[\mathbf{t}]$
$\text{Ring_Neg}[\mathbf{t}]$

Addition is commutative.

$\text{Ring_Add_Commutative}[\mathbf{t}]$
$\text{Ring_Add}[\mathbf{t}]$
$\forall x, y : A \bullet x + y = y + x$

- addition is commutative

A ring is an abelian group under addition.

$\text{Ring_Add_AbelianGroup}[\mathbf{t}]$
$\text{Ring_Add_Group}[\mathbf{t}]$
$\text{Ring_Add_Commutative}[\mathbf{t}]$

2.1.3. *Multiplication.* A ring has a binary operation of multiplication on its elements.

$\text{Ring_Mul}[\mathbf{t}]$
$\text{Ring_Elements}[\mathbf{t}]$
$_ * _ : \mathbf{t} \times \mathbf{t} \mapsto \mathbf{t}$
$(_ * _) \in A \times A \rightarrow A$

- multiplication is a binary operation on A

Multiplication is associative.

$\text{Ring_Mul_Associative}[\mathbf{t}]$
$\text{Ring_Mul}[\mathbf{t}]$
$\forall x, y, z : A \bullet (x * y) * z = x * (y * z)$

- multiplication is associative

Multiplication distributes over addition.

$\text{Ring_Mul_Distributive}[\mathbf{t}]$
$\text{Ring_Add}[\mathbf{t}]$
$\text{Ring_Mul}[\mathbf{t}]$
$\forall x, y, z : A \bullet x * (y + z) = (x * y) + (x * z)$
$\forall x, y, z : A \bullet (y + z) * x = (y * x) + (z * x)$

- left multiplication distributes over addition
- right multiplication distributes over addition

2.1.4. *Ring*. A ring is a set of elements with associative binary operations of addition and multiplication such that the elements are an abelian group under addition and multiplication distributes over addition.

$Ring[t]$	_____
$Ring_Add_AbelianGroup[t]$	
$Ring_Mul_Distributive[t]$	

2.1.5. *Commutative Ring*. The multiplication operation may be commutative.

$Ring_Mul_Commutative[t]$	_____
$Ring_Mul[t]$	
$\forall x, y : A \bullet x * y = y * x$	

- multiplication is commutative

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

$CommutativeRing[t]$	_____
$Ring[t]$	
$Ring_Mul_Commutative[t]$	

2.2. **Unital Ring**. A ring is said to have an *identity element* if it has a left and right multiplicative identity element.

$Ring_One[t]$	_____
$Ring_Mul[t]$	
$1 : t$	
$1 \in A$	
$\forall x : A \bullet 1 * x = x = x * 1$	

- the ring contains an element 1
- 1 is a left and right multiplicative identity element

Suppose a ring has a second identity element, say $1'$.

$Ring_Ones[t]$	_____
$Ring_One[t]$	
$1' : t$	
$1' \in A$	
$\forall x : A \bullet 1' * x = x = x * 1'$	

- the ring contains an element $1'$
- $1'$ is a left and right multiplicative identity element

Remark. If a ring has an identity element then it is uniquely determined.

$$\forall Ring_Ones[T] \bullet 1' = 1$$

Proof.

$$\begin{array}{ll}
 1' & \\
 = 1' * 1 & [1 \text{ is an identity element}] \\
 = 1 & [1' \text{ is an identity element}]
 \end{array}$$

□

A ring with an identity element is also said to be a *unital* ring.

$$\begin{array}{l}
 \text{UnitalRing}[\mathbf{t}] \\
 \hline
 \text{Ring}[\mathbf{t}] \\
 \text{Ring_One}[\mathbf{t}]
 \end{array}$$

2.3. Commutative Algebra. Commutative algebra is primarily concerned with commutative, unital rings.

$$\begin{array}{l}
 \text{CURing}[\mathbf{t}] \\
 \hline
 \text{CommutativeRing}[\mathbf{t}] \\
 \text{UnitalRing}[\mathbf{t}]
 \end{array}$$

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.

2.3.1. Zero Ring. If the zero element and the one element are the same then the ring is said to be a *zero* ring.

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

- the zero and one elements are the same

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

$$\forall \text{ZeroRing}[\mathbf{T}] \bullet A = \{0\}$$

Proof.

$$\begin{array}{ll}
 x : A & [\text{assumption-intro}] \\
 x & \\
 = x * 1 & [1 \text{ is the identity element}] \\
 = x * 0 & [1 = 0 \text{ by } \text{ZeroRing}] \\
 = 0 & [0 \text{ is the zero element}] \\
 x : A \Rightarrow x = 0 & [\text{assumption-elim}] \\
 A = \{0\} & [\text{set extensionality}]
 \end{array}$$

□

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

$CURing_Hom[t, u]$
$CURing[t]$ $CURing'[u]$ $f : t \rightarrow u$
$f \in A \rightarrow A'$ $\forall x, y : A \bullet f(x + y) = f(x) +' f(y)$ $\forall x, y : A \bullet f(x * y) = f(x) *' f(y)$ $f(1) = 1'$

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

$CURing_Subring[t]$
$CURing'[t]$ $A : \mathbb{P} t$
$A \subseteq A'$ $1' \in A$ $\forall x, y : A \bullet x +' y \in A$ $\forall x, y : A \bullet x *' y \in A$

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

$CURing_Restriction[t]$
$CURing_Subring[t]$ $CURing[t]$
$(- + -) = (\lambda x, y : A \bullet x +' y)$ $(- * -) = (\lambda x, y : A \bullet x *' y)$

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

$CURing_Inclusion[t]$
$CURing_Restriction[t]$ $f : t \rightarrow t$
$f = (\lambda x : A \bullet x)$

Remark. *Subring inclusion is a ring homomorphism.*

$$\forall CURing_Inclusion[T] \bullet CURing_Hom[T, T]$$

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

$CURing_Composition[t, u, v]$	_____
$CURing_Hom[t, u]$	
$CURing_Hom'[u, v]$	
$g : t \rightarrow v$	
$g = f' \circ f$	

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.orient.ox.ac.uk/wiki/files/zrm/zrm.pdf>.
- [4] Mike Spivey. *The fuzz Manual*. Second Edition. The Spivey Partnership, 2000. URL: <https://github.com/Spivosity/fuzz/blob/59313f201af2d536f5381e65741ee6d98db54a70/doc/fuzzman-pub.pdf>.

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