Algebra II

Evan Halloran

Abstract

[1] These notes will prove

[1]The content of these notes is largely based on *Algebra* by Michael Artin.

Contents

Chapter 1

Rings

1.1 Definition of a Ring

A **ring** is a set with two operations, called addition ($+$) and multiplication ($\cdot$), subject to certain requirements.

Example. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all rings. Likewise, the sets $\mathbb{Z}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$ (the set of all polynomials with coefficients in $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, respectively) are rings as well.

Definition. A **(commutative) ring** is a set R with two operations (or laws of composition) called addition and multiplication satisfying

1. $(R, +)$ is an abelian group; its identity element is denoted by 0,
2. $(R, \cdot)$ is commutative, associative, and has an identity element denoted by 1,
3. for all $a, b, c \in R$, $(a + b) \cdot c = ac + bc$ (distributive law).

Let's unpack the definition:

1. $(R, +)$ is a group means:
   - associative $\quad (a + b) + c = a + (b + c)$,
   - identity $\quad \exists 0 : a + 0 = 0 + a = a \quad \forall a$,
   - inverse $\quad \forall a,\ \exists$ "$-a$" such that $a + (-a) = (-a) + a = 0$,
   - abelian $\quad a + b = b + a$.
2. $(R, \cdot)$ satisfies:

- commutative $ab = ba$,
- associative $a(bc) = (ab)c$,
- identity $\exists 1 : a1 = 1a = a \quad \forall a$,
- no inverse requirement!

Example. The **zero ring** is the trivial ring containing but one element, namely $R = \{0\}$. In this ring, both identities are equal ($1 = 0$).

Example. The following sets are rings.

1. $\mathbb{Z}/n\mathbb{Z}$,
2. $R = \{\text{all functions } f : \mathbb{R} \to \mathbb{R}\}$ with the usual addition and multiplication of functions: $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$. The additive identity 0 is the constant function zero, and the multiplicative identity 1 is the constant function one,
3. $R_1 = \{\text{all continuous functions } f : \mathbb{R} \to \mathbb{R}\}$,
4. $R_2 = \{\text{all differentiable functions } f : \mathbb{R} \to \mathbb{R}\}$,
5. $R_1 = \{\text{all polynomial functions } f : \mathbb{R} \to \mathbb{R}\}$, where a polynomial is a function of the form $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, for some coefficients $a_0, ..., a_n \in R$.

Recall the set of complex numbers $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$. Addition and multiplication in $\mathbb{C}$ are defined by

$$\begin{aligned}(a + ib) + (c + id) &= (a + c) + i(c + d),\\ (a + ib) \cdot (c + id) &= ac + iad + ibc + i^2bc\\ &= (ac - bd) + i(ad + bc).\end{aligned}$$

The ring of **Gaussian integers** is the set $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ which consists of all complex numbers whose real and imaginary parts are integers.

Example. The following sets are not rings.

1. The set $R = \{n \times n \text{ matrices (with real or complex entries) }\}$ is not a ring because the multiplication is <u>not</u> commutative,

2. The set of quaternions $H = \{a + ib + jc + kd : a, b, c, d \in \mathbb{R}\}$ is not a ring because of the following multiplications:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= -ji = k, \\ jk &= -kj = i, \\ ki &= -ik = j. \end{aligned}$$

These are non-commutative rings; they must satisfy the additional axiom $c \cdot (a+b) = ca + cb$.

Let R be a ring. We have the following observations:

1. The identity element for $(R, \cdot)$ is unique: $1 = 1 \cdot 1' = 1'$,

2. If $x \in R$, $x \neq 0$, $n = 0, 1, 2, 3, ...$, then

$$\begin{aligned} x^n &= \underbrace{x \cdot x \cdot ... \cdot x}_{n \text{ times}}, \\ x^0 &= 1, \\ x^{m+n} &= x^m \cdot x^n, \\ (x^m)^n &= x^{mn} \quad (m, n \geq 0). \end{aligned}$$

3. For all $x \in R$, we have $0x = x0 = 0$ (because $0x = (0 + 0)x = 0x + 0x$),

4.

Proposition 0.1. *If $1 = 0$, then R is the zero ring ($R = \{0\}$).*

Proof. If $1 = 0$, then $\forall x \in R$, $x = 1x = 0x = 0$. □

Proposition 0.2. *If $x \in R$ has a multiplicative inverse, then it is unique.*

Proof. Let y, y' be such that $xy = 1$ and $y'x = 1$. Then

$$y = 1y = (y'x)y = y'(xy) = y'1 = y'.$$

□

Exercises

1. Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing the rational numbers $\mathbb{Q}$ and the elements $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$?

2. Decide whether or not S is a subring of R, when

   (a) S is the set of rational numbers a/b, where b is not divisible by 3, and $R = \mathbb{Q}$.

   (b) S is the set of functions which are linear combinations with integer coefficients of the functions $\{1, \cos nt, \sin nt\}$, $n \in \mathbb{Z}$, and R is the set of all real valued functions of t.
   Hint for (b): $\int_0^{2\pi} \sin(mt)\sin(nt)dt \neq 0$ only if $m = \pm n$, $\int_0^{2\pi} \cos(mt)\cos(nt)dt \neq 0$ only if $m = \pm n$.

3. Decide whether the given structure forms a ring. If it is not a ring, decide which of the ring axioms hold and which fail:

   (b) R is the set of continuous functions $\mathbb{R} \to \mathbb{R}$. Addition and multiplication are defined by the rules $[f + g](x) = f(x) + g(x)$ and $[f \circ g](x) = f(g(x))$.

4. Determine the units in:

   (a) $\mathbb{Z}/12\mathbb{Z}$,

   (b) $\mathbb{Z}/8\mathbb{Z}$,

   (c) $\mathbb{Z}/n\mathbb{Z}$.

5. Let R be a set with two laws of composition satisfying all ring axioms except the commutative law for addition. Use the distributive law to prove that the commutative law for addition holds, so that R is a ring.
   Hint: Consider $(1 + a)(1 + b) = (1 + b)(1 + a)$.

6. Let R be a ring, and let x, y be elements in R such that $xy = 0$, but $x \neq 0$, $y \neq 0$. Then x and y are called *zero divisors*. Prove that a zero divisor cannot be a unit. (In particular, a field cannot have zero divisors).

1.2 Fields

Exercises

1. Recall that the textbook defines fields as rings in which $0 \neq 1$ and the set of non-zero elements is an abelian group under multiplication (pages 80-81).
   Let R be a ring such that $0 \neq 1$ and every non-zero element is a unit. Prove that R is a field. (The part that requires some work is showing that $R \setminus \{0\}$ is closed under multiplication.)

2. Let F be a field of characteristic $p > 0$. Prove that

$$(a + y)^p = x^p + y^p \quad \text{for all } x \text{ and } y \text{ in } F.$$

3. (a) Prove *Fermat's Theorem*: For every integer a, $a^p \equiv a$ modulo p.

   (b) Prove *Wilson's Theorem*: $(p-1)! \equiv -1$ (modulo p).

1.3 Polynomial Rings

Exercises

1. For which positive integers n does x^2+x+1 divide $x^4+3x^3+x^2+7x+5$ in $[\mathbb{Z}/(n)][x]$?

1.4 Homomorphisms and Ideals

Exercises

1. Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.

2. An *automorphism* of a ring R is an isomorphism from R to itself. Let R be a ring, and let $f(y)$ be a polynomial in one variable with coefficients in R. Prove that the map $R[x, y] \to R[x, y]$ defined by $x \mapsto x + f(y)$, $y \mapsto y$ is an automorphism of $R[x, y]$.

3. Determine the automorphisms of the polynomial ring $\mathbb{Z}[x]$.

4. Let R be a ring of prime characteristic p. Prove that the map $R \to R$ defined by $x \mapsto x^p$ is a ring homomorphism. (It is called the *Frobenius map.*)

5. (a) An element x of a ring R is called *nilpotent* if some power if 0. Prove that if x is nilpotent, then $1 + x$ is a unit.

   (b) Suppose that R has prime characteristic $p \neq 0$. Prove that if a is nilpotent then $1 + a$ is *unipotent*, that is, some power of $1 + a$ is equal to 1.

6. Let I and J be ideals of a ring R. Prove that the set $I + J$ of elements of the form $x + y$, with x in I and y in J, is an ideal. This ideal is called the *sum* of the ideals I and J.

1.5 Quotient Rings

Exercises

Let R be a ring, $R[x]$ the ring of polynomials with coefficients in R, and let $f(x)$ be a monic polynomial in $R[x]$ of degree $n \geq 1$. Use the bar notation to denote passage to the quotient ring $R[x]/(f(x))$.

(a) Show that every element of $R[x]/(f(x))$ is of the form $p(\bar{x})$

1.6 Adjoining Elements

1.7 Product Rings

1.8 Fractions

1.9 Maximal Ideals

Chapter 2

Factoring

2.1 Factoring Integers

2.2 Unique Factorization Domains

2.3 Gauss's Lemma

2.4 Factoring Integer Polynomials

2.5 Gauss Primes

Chapter 3

Linear Algebra in a Ring

Chapter 4

Fields

4.1 Examples of Fields

4.2 Algebraic and Transcendental Elements

4.3 The Degree of a Field Extension

4.4 Finding the Irreducible Polynomial

4.5 Ruler and Compass Constructions