Chapter 1. Basics

1.1. The Definitions

Note. In this section we review the definitions of ring, field, division ring, ring homomorphism and isomorphism, ideal, principal ideal, quotient ring, and generating set for a ring. These definitions are covered in Introduction to Modern Algebra 1 and 2 (MATH 4127/5127 and 4137/5137); see my online notes for Intro to Modern Algebra 1 (see in particular Section IV.18. Rings and Fields) and Intro to Modern Algebra 2 (see Section V.26. Homomorphisms and Factor Rings and Section V.27. Prime and Maximal Ideals). We also give some definitions that are likely new to you, such as embedding, anti-isomorphism, anti-automorphism, and involution.

Definition. A *ring* is a system R with two binary operations, associating with each pair of elements, a and b, a *sum* $a+b$ and a *product* $a.b$ (more commonly just denoted ab), again lying in R and satisfying the following axioms:

R.1. $a+b=b+a$ (commutative law of addition);

R.2. $(a+b)+c=a+(b+c)$ (associative law of addition);

R.3. there exists $0 \in R$ such that $a+0=a$ (neutral element of addition);

R.4. for each $a \in R$ there exists $-a \in R$ such that $a+(-a)=0$ (additive inverse);

R.5. $a(bc)=(ab)c$ (associative law of multiplication);

R.6. $(a+b)c=ac+bc$, $(c(a+b)=ca+cb$ (distributive laws);

R.7. there exists $1 \in R$ such that $1a=a1=a$ (neutral element for multiplication)

Note. Notice that R-1–R.4 imply that R is an abelian group under addition. A *semigroup* is a system with one binary operation which is associative (semigroups are studied in graduate-level Modern Algebra 1 [MATH 5410] in Section I.1. Semigroups, Monoids, and Groups). By R.5, R is a semigroup under multiplication. Also in Modern Algebra 1, a *monoid* is defined as a semigroup with an element (denoted "1") which is neutral for the binary operation. By R.7, R is a monoid under multiplication. The neutral element for multiplication is called *one* (or "the multiplicative identity) and the neutral element for addition (denoted "0") is called *zero* (or "the additive identity").

Definition. A ring R that satisfies the axiom

R.8. $ab = ba$ for all $a, b \in R$ (commutative law of mulitplication)

is a *commutative ring*. If R.8 does not hold every a and b in R, then R is a *non-commutative ring*.

Note. An example of a ring is the integers, $\mathbb{Z}$, under the usual addition and multiplication. In fact, $\mathbb{Z}$ is a commutative ring. Notice that in Cohn's book, the natural numbers $\mathbb{N}$ includes 0: $\mathbb{N} = \{0, 1, 2, \ldots\}$. Therefore $\mathbb{N}$ is not a ring (it violates R.4), but it is a semigroup and a monoid under both addition and multiplication. The set of all 2×2 matrices with real entries form a non-commutative ring under the usual matrix addition and multiplication. Next, we give a number of the examples of rings from Cohn's book.

Example 1.1.1. The rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ each form a ring under the usual definition of addition and multiplication.

Example 1.1.2. The set $\mathbb{Q}[x]$ of all polynomials in x with rational coefficients is a ring. In fact, for any ring R the set $R[x]$ of all polynomials with coefficients from ring R is itself a ring; for more details, see the Introduction to Modern Algebra 1 (MATH 4127/5127) notes on Section IV.22. Rings of Polynomials.

Revised: 7/10/2023