Part IV. Rings and Fields

Section IV.18. Rings and Fields

Note. Roughly put, modern algebra deals with three types of structures: groups, rings, and fields. In this section we introduce rings and fields. In this last part of the course, we look at some properties of these algebraic structures. We will finally see the "basic goal" of the text in Section IV.22 when mention is made of solving polynomial equations in a field (see page 206).

Note. In Introduction to Modern Algebra 2 (MATH 4137/5137) you will explore rings some more (Parts V and IX) and you will explore fields a lot more (in Parts VI and X). There are still some important results from group theory yet to be presented and these can be found in Part VII. Applications of group theory to topology can be found in the optional Part VIII.

Note. Rings and fields have *two* binary operations. We denote these operations as $+$ and $\cdot$. In group theory, we used both $+$ and $\cdot$ as *the* binary operation of a group. The choice of $+$ or $\cdot$ was irrelevant in the group setting; it was usually motivated by the types of example under consideration ($\mathbb{Z}_n$ is additive and $GL(n, \mathbb{R})$ is multiplicative), but in group theory the difference between $+$ and $\cdot$ is purely notational. This is not the case in ring theory or field theory. We require, by definition, different properties for one binary operation $(+)$ than for the other $(\cdot)$.

Definition 18.1. A *ring* $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, called *addition* and *multiplication*, respectively, defined on R such that:

$\mathcal{R}_1$**:** $\langle R, + \rangle$ is an abelian group.

$\mathcal{R}_2$**:** Multiplication $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

$\mathcal{R}_3$**:** For all $a, b, c \in R$, the *left distribution law* $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the *right distribution law* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Note. We adopt the usual order of operations and so we can denote $(a \cdot c) + (b \cdot c)$ as $ac + bc$ without the parentheses (and often without writing the "$\cdot$").

Example 18.2. Some of our most familiar mathematical structures are rings: $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$ $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$.

Note. Since $\langle R, + \rangle$ is an abelian group, then we know that any $a \in R$ has an additive inverse in R, denoted $-a$. However, elements of R may not have multiplicative inverses. Notice that $\langle \mathbb{Z}, +, \cdot \rangle$ is an example of a ring for which most elements do not have multiplicative inverses (in fact, 1 and -1 are the only elements of $\mathbb{Z}$ with multiplicative inverses).

Example 18.3. Let R be any ring and let $M_n(R)$ be the collection of all $n \times n$ matrices of elements R. Then $\langle M_n(R), + \rangle$ is "'clearly" an abelian group. If we define the product of two matrices in $M_n(R)$ in the usual "row times column" way, then matrix multiplication is associative and the left and right distribution laws hold (not "clear," but true). So $M_n(R)$ is itself a ring. Notice that $GL(n, R)$ is a "subring" of $M_n(R)$.

Example 18.6. We can use $\langle \mathbb{Z}_n, + \rangle$ to define a ring. We only need to define $\cdot$ on $\mathbb{Z}_n$. For $a, b \in \mathbb{Z}_n$, define $a \cdot b = ab \pmod{n}$. Then $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a ring (more details about this claim appears in Section V.26). Notice that sometimes elements of $\mathbb{Z}_n$ have multiplicative inverses and sometimes they do not.

Example 18.7. Let $R_1, R_2, \ldots, R_n$ be rings. Define $R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R_i \text{ for } 1 \leq i \leq n\}$. Define addition and multiplication on $R_1 \times R_2 \times \cdots \times R_n$ component-wise. Then $R_1 \times R_2 \times \cdots \times R_n$ is itself a ring called the *direct product* of $R_1, R_2, \ldots, R_n$.

Note. We adopt some standard notation in a ring. If $a \in R$ is added to itself n times, we denote the sum as na. If $a \in R$ is multiplied by itself n times, we denote the product as a^n. We denote the additive inverse of $a \in R$ as $-a$. The additive identity is denoted 0. If ring R has a multiplicative identity, we denote it as 1 (as in Theorem 3.13, we can show that a multiplicative identity is unique). In the event that $a \in R$ has a multiplicative inverse, we denote it as a^{-1}.

Note. The following result establishes the usual properties of the interactions of products of "positives," "negatives," and zero. Be careful, though, in your interpretation of these results. Remember that "negative a" may not make sense, but the "additive inverse of a" does make sense in the ring setting (and the field setting and even the additive group setting).

Theorem 18.8. If R is a ring with additive identity 0, then for all $a, b \in R$ we have

1. $0a = a0 = 0$,

2. $a(-b) = (-a)b = -(ab)$, and

3. $(-a)(-b) = ab$.

Exercise 18.12. Consider $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication. Is this a ring?

Solution. Yes! Pay particular attention to closure under $\cdot$.

Definition 18.9. For rings R and R', a map $\phi : R \to R'$ is a *homomorphism* if for all $a, b \in R$ we have:

1. $\phi(a + b) = \phi(a) + \phi(b)$, and

2. $\phi(ab) = \phi(a)\phi(b)$.

Note. As usual, a homomorphism preserves the "structure"—that is, it preserves the binary operations.

Note. A ring homomorphism between $\langle R, +, \cdot \rangle$ and $\langle R', +, \cdot \rangle$ is also a group homomorphism between $\langle R, + \rangle$ and $\langle R', + \rangle$. Recall that ϕ is one to one if and only if $\text{Ker}(\phi) = \{a \in R \mid \phi(a) = 0'\} = \{0\} \subset R$. This holds as well for ring homomorphisms. In Section III.14 we used group homomorphisms and kernels to define factor groups. A similar approach will be used in Section V.26 to define factor rings.

Definition 18.12. A *isomorphism* $\phi : R \to R'$ from ring R to ring R' is a homomorphism which is one to one and onto R'.

Definition 18.14. A ring in which multiplication is commutative (i.e., $ab = ba$ for all $a, b \in R$) is a *commutative ring*. A ring with a multiplicative identity element is a *ring with unity*.

Note. As commented above, Theorem 3.13 implies that the multiplicative identity is unique. We denote it as "1" and it is called *unity*.

Example 18.15. $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic rings when $\gcd(r, s) = 1$. Since $\mathbb{Z}_{rs}$ is cyclic, we need $\gcd(r, s) = 1$ so that $\mathbb{Z}_r \times \mathbb{Z}_s$ is cyclic (it is generated by $(1, 1)$, for example).

Definition 18.16. Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is a *unit* of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a *division ring* (or *skew field*). A *field* is a commutative division ring. A noncommutative division ring is called a *strictly skew field*.

Example. $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$ are all examples of fields. An example of a strictly skew field (a noncommutative division ring) is the quaternions (we encountered the quaternions as a group of order 8, Q_8, in Section I.7; strictly speaking the quaternions are an infinite group generated by the elements of Q_8 using real "scalars"—see page 224 of Section IV.24 for details).

Example. Find the units of $\mathbb{Z}_8$.

Solution. The units are: 1 since $1 \cdot 1 = 1$, 3 since $3 \cdot 3 = 9 \equiv 1 \pmod 8$, 5 since $5 \cdot 5 = 25 \equiv 1 \pmod 8$, and 7 since $7 \times 7 = 49 \equiv 1 \pmod 8$.

Revised: 12/14/2013