1

Rings and Subrings

The Notion of a Ring

In 1888 — when he was only 26 years old — David Hilbert stunned the mathematical world by solving the main outstanding problem in what was then called invariant theory. The question that Hilbert settled had become known as *Gordan's Problem*, for it was Paul Gordan who, 20 years earlier, had shown that *binary* forms have a finite basis. Gordan's proof was long and laboriously computational; there seemed little hope of extending it to ternary forms, and even less of going beyond. We will not take the time here to explore any of the details of Gordan's problem or even the nature of invariant theory (and you shouldn't be at all concerned if you don't have the foggiest idea what binary or ternary forms are or what a basis is), but Hilbert — in a single brilliant stroke — proved that there is in fact a *finite* basis for all invariants, *no matter how high the degree*.

The structure of Hilbert's proof is really quite simple and is worth looking at (again we will not worry at all about most of the details). First, Hilbert showed that if a ring R has a certain property P, then the ring of polynomials in a single variable x with coefficients from the ring R also has that same property P. (Today we would say that P is the property that any ideal is finitely generated, but that is getting well ahead of our story.) We will use the convenient notation $R[x]$ to represent this ring of polynomials in x with coefficients from R, and so we can summarize Hilbert's first step as

$$\text{if a ring } R \text{ has property } P, \text{ then so does the ring } R[x].$$

Next, Hilbert wanted to show that the ring of polynomials in *two* variables x and y with coefficients from the ring R also has property P. We represent this ring of polynomials in two variables by $R[x, y]$. These polynomials are just like ordinary polynomials we are used to such as $x^2 + 4$ and $2y^2 - y + 3$, except that now we can have the two variables x and y mixed together in a single polynomial. An example of such a polynomial is

$$3x^2 + 4xy + 2y^2 + 7x - 5y + 12,$$

where in this case the coefficients are all integers. Hilbert saw that this ring of polynomials $R[x, y]$ in *two* variables x and y with coefficients from the ring R can be thought of as the ring of polynomials in a *single* variable y with coefficients from the ring of polynomials in x. For example, we can write the above polynomial in two ways, depending on how we choose to group the terms:

$$3x^2 + 4xy + 2y^2 + 7x - 5y + 12 \;=\; 2y^2 + (4x - 5)y + (3x^2 + 7x + 12).$$

On the left the polynomial is written as a polynomial in the ring $R[x, y]$, whereas on the right it is written as a polynomial in one variable y where the coefficients are themselves polynomials in x. Our notation for this latter ring is $\big(R[x]\big)[y]$ — or more simply $R[x][y]$ — emphasizing the fact that the coefficients are now polynomials in the ring $R[x]$.

Using this simple idea, Hilbert concluded that the ring of polynomials $R[x, y]$ also has property P. His argument went like this: since the ring R has property P, so does the ring $R[x]$; but then since the ring $R[x]$ has property P, so does the ring $R[x][y]$; and, as we have just seen, this latter ring is really the same as the ring $R[x, y]$.

In this way, by adding one variable at a time, Hilbert showed that the polynomial ring in any finite number of variables has property P. For example, we could now conclude that the ring $R[x, y, z]$ has property P since this ring is the same as the ring $R[x, y][z]$ and we have just argued that $R[x, y]$ has property P. The key to Hilbert's argument, then, is to verify his very first step — namely, that if a ring R has property P, then so does the polynomial ring with coefficients from R.

Now Hilbert did this not by explicitly constructing a basis (as Gordan had done for the binary case), but rather — and this is the brilliant part of his proof — by showing that if there were no finite basis, then a contradiction arises. Therefore, there *must* be a finite basis after all! Nowadays, we are very comfortable with such a *proof by contradiction*, but Hilbert had used this technique in a new way: he had proved the *existence* of something without actually constructing it. This existence proof did not meet with universal favor in the mathematical climate of his day. In fact, Gordan — hardly an impartial observer — chose this time to issue one of the most memorable lines in all of mathematics: "Das is nicht Mathematik. Das ist Theologie." It was not until four years later, when Hilbert was able to use the existence of a finite basis to show how such a basis could actually be constructed, that Gordan conceded: "I have convinced myself that theology also has its advantages."

At the heart of Hilbert's proof — and the attendant controversy — lies the abstract notion of a ring, though it would be several years until

Hilbert would actually provide us with the term *ring* (or *Zahlring* — literally, number ring) which we now use today. The idea is that, for instance, although polynomials certainly differ in many obvious ways from integers, there are ways in which polynomials and integers are similar: for example, you can add or multiply integers and you can also add or multiply polynomials. It is the differences between integers and polynomials that most of us notice first, but Hilbert focused instead on their similarities. So, the idea behind the notion of a ring is that integers, rationals, reals, complex numbers, polynomials with complex coefficients, and continuous functions, as different as all of these systems may appear to us, all share certain characteristics. It is these shared underlying characteristics which provide the basis for the following unifying axioms and our definition of a ring, for it is the abstract notion of a ring that so elegantly captures the essence of what these familiar mathematical systems share in their behavior.

The Definition of a Ring

Before we actually define a ring, let us talk a bit about what a ring is. Quite simply it is a set of elements (typically a set of numbers of some kind, or perhaps a set consisting of a particular type of function) together with two operations on those elements called addition and multiplication. It is very important to think of a ring as a single object consisting of *both* the underlying set and the two operations, and *not* just as a set by itself. Furthermore, these operations will need to behave the way we expect them to behave. For example, if a and b are two elements in a ring, we expect $a + b$ and $b + a$ to be equal, or we expect $a + 0$ to equal a, or we expect $a(a + b)$ to equal $a^2 + ab$. We have these expectations no matter whether a and b are numbers, or polynomials, or matrices.

Let us look at some specific examples of rings. In each case, note that we present both a set and two operations on that set in order to describe the ring.

Example 1

Certainly the single most fundamental example of a ring is the ring based on the numbers $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$. We will call this ring the *ring of integers* or, more simply, *the integers*, and we will denote this ring by $\mathbf{Z}$. This letter for the integers may seem peculiar to you at first, but it comes from *Zahl*, the German word for number, and serves as a nice reminder to us of the history of the notion of a ring. The ring $\mathbf{Z}$ then consists of the set of integers together with the ordinary operations of addition and multiplication.

Example 2
The most natural ring to consider next is the ring based on the numbers that are fractions of integers, such as $\frac{1}{3}$ and $\frac{22}{7}$. Thus, we will consider the *rational numbers* or, more simply, *the rationals* as a ring with the ordinary operations of addition and multiplication of fractions. This ring is denoted by $\mathbf{Q}$. (By the way, why do you suppose mathematicians long ago decided on this particular letter to represent the rationals?)

Example 3
Similarly the *real numbers* or, more simply, *the reals* together with the ordinary operations of addition and multiplication form a ring which we denote by $\mathbf{R}$.

Example 4
The *complex numbers* with their ordinary operations of addition and multiplication form a ring which we denote by $\mathbf{C}$. A complex number is a number of the form $a + b\,i$, where a and b are real numbers and $i^2 = -1$. The two operations of addition and multiplication in this ring are completely natural — for example,

$$(1 + 7\,i) + (2 - 3\,i) = 3 + 4\,i$$

and

$$(1 + 7\,i) \cdot (2 - 3\,i) = 2 - 21\,i^2 - 3\,i + 14\,i = 23 + 11\,i,$$

since $i^2 = -1$.

Somewhat more formally, the two operations of addition and multiplication of complex numbers can be defined as follows, where $a, b, c, d \in \mathbf{R}$:

$$(a + b\,i) + (c + d\,i) = (a + c) + (b + d)\,i$$

and

$$(a + b\,i) \cdot (c + d\,i) = (ac - bd) + (ad + bc)\,i.$$

Example 5
The *set of polynomials with integer coefficients* together with the ordinary operations of addition and multiplication of polynomials — that is, you

add and multiply polynomials just as you did in high school — also form a ring. We denote this ring by $\mathbf{Z}[x]$. So, for example,

$$(1 + x + x^2) + (-2 + 3x - x^3) = -1 + 4x + x^2 - x^3$$

and

$$(1 + x + x^2) \cdot (-2 + 3x - x^3) = -2 + x + x^2 + 2x^3 - x^4 - x^5.$$

Example 6

The set of 2 *by* 2 *matrices* whose entries are real numbers together with the ordinary operations of matrix addition and multiplication form a ring. We denote this ring by $\mathbf{M}_2$. Formally, the two operations for $\mathbf{M}_2$ are defined as follows, where $a, b, c, d, e, f, g, h \in \mathbf{R}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$

This might be a good time to point out that often we are quite casual about making distinctions in either notation or language between operations on sets that are in fact not at all the same operation. For instance, in Example 6 we use the same symbol, a plus sign (+), to denote both the operation of matrix addition and the operation of addition of real numbers; moreover, we normally refer to each of these operations simply as "addition" as we do in this example and in Example 3.

With these six examples of rings well in hand, we are now ready for the formal definition of a ring. Our definition will lay down the list of axioms that any set with two operations must satisfy in order to attain the status of being called a ring. As you read this list of axioms, you might want to pause in turn and think about what each axiom says in the context of each of our six examples.

Definition 1.1. *A* **ring** *is a set R together with two operations on R (addition and multiplication) such that:*

1. *addition is associative — that is, for all* $a, b, c \in R$

$$a + (b + c) = (a + b) + c;$$

2. *addition is commutative — that is, for all* $a, b \in R$

$$a + b = b + a;$$

3. *R has a zero element — that is, there is an element* 0 *in R such that, for all* $a \in R$

$$a + 0 = a;$$

4. *for every* $a \in R$*, there is an element* $-a$ *in R such that*

$$a + (-a) = 0;$$

5. *multiplication is associative — that is, for all* $a, b, c \in R$

$$a(bc) = (ab)c;$$

6. *multiplication is distributive over addition — that is, for all* $a, b, c \in R$

$$(a + b)c = ac + bc \quad \textit{and} \quad a(b + c) = ab + ac.$$

The previous six axioms define a ring*, but we will want to concern ourselves in this book only with rings that satisfy two additional axioms. Thus, a* **commutative ring with identity** *is a ring R such that:*

7. *multiplication is commutative — that is, for all* $a, b \in R$

$$ab = ba;$$

8. *R has a multiplicative identity — that is, there is an element* 1 *in R such that for all* $a \in R$

$$a \cdot 1 = a.$$

It will be extremely important to remember that throughout the rest of this book the word *ring* will always mean *commutative ring with an identity element*. This should cause no confusion, but should always be kept firmly in mind, since the theory of noncommutative rings has quite a different character from commutative ring theory. Note that we have already seen one example of a noncommutative ring, the ring of 2 *by* 2 *matrices*, $\mathbf{M}_2$, defined in Example 6, and that the set of even integers, $2\mathbf{Z}$, forms a commutative ring without an identity element.

Verifying that a given set together with two operations of addition and multiplication is in fact a ring — that is, that it satisfies all eight axioms — can be a long and tedious process (see Problem 1.7). Note also that the zero element mentioned in Axiom (3) can take different forms depending on the ring in question. For the rings $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$ the zero element is just the number 0. For the ring $\mathbf{C}$ it is the complex number $0 + 0\,i$ which we also usually denote more simply by 0. Similarly, for the ring of polynomials, $\mathbf{Z}[x]$, the zero element is the constant polynomial 0. For $\mathbf{M}_2$ it is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. You should make sure that, for each of these examples of rings, you can identify the additive inverse mentioned in Axiom (4), as well as the multiplicative identity of Axiom (8).

Given that the eight ring axioms stated above were motivated by our desire to have rings behave algebraically just as we expect, it is not at all surprising that the following three familiar rules of algebra still hold in an arbitrary ring R:

1. $0a = 0$, for all $a \in R$;
2. $(-a)b = -(ab)$, for all $a, b \in R$;
3. $a(b - c) = ab - ac$, for all $a, b, c \in R$.

The verification of these rules from the axioms is left to you (see Problem 1.2).

The Definition of a Subring

It is frequently the case that we wish to focus our attention on a particular subset of a ring. For example, within the ring $\mathbf{R}$ of all real numbers we may wish to deal with the integers. The point here is that the integers themselves form a ring, and this ring shares with the larger ring $\mathbf{R}$ the operations of addition and multiplication, as well as having the same identity. In such a situation, we say that the subset in question is a *subring* of the larger ring.

As mentioned above, it is would be tedious always to have to check in complete detail that a given subset of a ring is itself a ring in order to know it is a subring. Fortunately, in the context we are discussing, there is a shortcut which we will adopt as our definition of a subring. Then I will leave to you in Problem 1.13 the one-time-only details of showing that this shortcut is in fact equivalent to the notion of a subring given in the preceding paragraph.

Using this shortcut, then, in order to verify that a given subset of a ring is indeed a subring, all that needs to be done is to check that the subset contains the identity of the larger ring, that the subset is *closed*

under addition and multiplication — that is, if you add or multiply two elements of the subset then you get an element of the subset — and, finally, that the subset contains additive inverses — that is, for each element in the subset, its additive inverse is also in the subset.

Definition 1.2. *A subset S of a ring R is a* **subring** *of R if S is closed under the addition and multiplication operations of R, contains additive inverses, and contains the (multiplicative) identity of R.*

Problems

1.1 Show that in a ring the zero element, the multiplicative identity, and additive inverses are each unique — that is, there is only one element that behaves like 0, only one element that behaves like 1, and for each element a only one element that behaves like $-a$.

1.2 Use the eight ring axioms to prove the three familiar rules of algebra (1)–(3) listed on page 7. (Of course, $b - c$ is simply a convenient shorthand for $b + (-c)$.)

1.3 Let R be a ring, and let $a, b \in R$. Prove that $(-a)(-b) = ab$.

1.4 In this problem we see that the ordinary rules for exponents we are familiar with still work perfectly in a ring. Let R be a ring and let $a \in R$. We can inductively define powers of a as follows:

$$a^0 = 1 \quad \text{and} \quad a^n = a^{n-1}a \quad \text{for } n > 0\,.$$

Use induction on n (fixing m as necessary) to prove that:

$$\text{(i) } (ab)^n = a^n b^n\,; \quad \text{(ii) } a^m a^n = a^{m+n}\,; \quad \text{(iii) } (a^m)^n = a^{mn},$$

for any non-negative integers m and n.

Note that we have not defined a^{-1} since in an arbitrary ring a given element a may or may not have a multiplicative inverse. For example, the element 2 does not have a multiplicative inverse in the ring $\mathbf{Z}$. Therefore, the symbol a^{-1} should only be written when you are sure that the element a does in fact have a multiplicative inverse in the ring.

1.5 Let R be a ring such that $1 = 0$, where 0 is the zero element and 1 is the multiplicative identity in the ring. Show that R consists of just a single element. (By the way, you should convince yourself that, conversely, the *set* $R = \{0\}$ where the operations of addition and multiplication are defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$ is actually a ring by verifying all the axioms.) This rather trivial, yet not altogether uninteresting, example of a ring is called the *zero ring*.

1.6 We define the set $\mathbf{Z} \times \mathbf{Z}$ to be the set of all ordered pairs of integers — that is, $\mathbf{Z} \times \mathbf{Z} = \{\,(a, b) \mid a, b \in \mathbf{Z}\,\}$. Show how to make $\mathbf{Z} \times \mathbf{Z}$ into a ring by suitably defining the operations of addition and multiplication. What is the zero element of this ring? What is the multiplicative identity?

1.7 You may want to skip this exercise. It is long and tedious, but you should probably do it anyway, just so that you know you can go through the details of verifying the ring axioms when necessary. Assuming that the set of real numbers $\mathbf{R}$ is a ring, show that the complex numbers form a ring with operations as defined in Example 4.

1.8 We quite naturally denote the set of even integers by $2\mathbf{Z}$. Is $2\mathbf{Z}$ a subring of $\mathbf{Z}$?

1.9 Do the rationals form a subring of the reals?

1.10 Does the set of all numbers of the form $a + b\sqrt{3}$ where a and b are rational numbers form a subring of the reals?

1.11 Do the reals form a subring of the complex numbers?

1.12 Does the set of all numbers of the form $a + b\,i$ where a and b are integers form a subring of the complex numbers?

1.13 Let S be a subset of a ring R. Show that if S is a subring by the definition on page 7, then S is itself a ring.