CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information

# Chapter 1

# Commutative rings and subrings

This book is designed for students who have followed an elementary undergraduate course on commutative ring theory, such as that covered in D. W. Sharpe's little book [20], and who wish to learn more about the subject. The aim of the book is to assist the reader to attain a level of competence in the introductory aspects of commutative algebra sufficient to enable him or her to begin with confidence the study of a more advanced book on the subject, such as H. Matsumura's [13].

We begin by introducing some of the notation that will be used throughout this book.

**1.1** NOTATION. The symbol $\mathbb{Z}$ will always denote the set of integers; in addition, $\mathbb{N}$ (respectively $\mathbb{N}_0$) will always denote the set of positive (respectively non-negative) integers. The set of rational (respectively real, complex) numbers will be denoted by the symbol $\mathbb{Q}$ (respectively $\mathbb{R}$, $\mathbb{C}$).

The symbol $\subseteq$ will stand for 'is a subset of'; the symbol $\subset$ will be reserved to denote strict inclusion. Thus, for sets $A, B$, the expression $A \subset B$ means that $A \subseteq B$ and $A \neq B$.

The symbol '$\square$' will be used to denote the end, or absence, of a proof.

We shall reserve the symbols

$$X, Y, X_1, \ldots, X_n$$

to denote indeterminates.

We shall denote the number of elements in a finite set $\Omega$ by $|\Omega|$.

A comment should perhaps be made about the distinction between a family and a set. We shall often use round parentheses ( ), as in $(a_i)_{i \in I}$,



© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



to denote a family indexed by the set $I$; here $a_i$ should be thought of as situated in the 'position' labelled by $i$; and the family $(a_i)_{i\in I}$ is considered to be equal to $(b_i)_{i\in I}$ if and only if $a_i = b_i$ for all $i \in I$. One can think of a family $(a_i)_{i\in I}$, where $a_i$ lies in the set $A$ for all $i \in I$, as a function from $I$ to $A$: in this interpretation, the image of $i$ under the function is $a_i$.

On the other hand, curly braces { }, as in

$$\{d_1, \ldots, d_n\} \qquad \text{or} \qquad \{d \in D : \text{statement } P(d) \text{ is true}\},$$

will often be used to indicate sets. A set is completely determined by its members, and no concept of 'position' is involved when the members of the set are displayed within braces. The distinction between a family and a set parallels that between a function and its image. To illustrate the distinction, let $d_1 = d_2 = 1$ and $d_3 = 3$. Then the family $(d_i)_{i=1}^3$ can be thought of as the ordered triple $(1, 1, 3)$, whereas the set $\{d_1, d_2, d_3\}$ is just the 2-element set $\{1, 1, 3\} = \{1, 3\}$.

As we are going to regard the contents of [20] as typical preparation for the study of this book, we shall in the main follow the terminology of [20]. In particular, all the rings we study will have multiplicative identity elements. To be precise, by a *ring* we shall mean a set, $R$ say, furnished with two laws of composition, addition and multiplication, such that $R$ is an Abelian group with respect to addition, multiplication is associative and both right and left distributive over addition, and $R$ contains a multiplicative identity element $1_R$ (or simply 1) such that

$$1_R r = r = r 1_R \qquad \text{for all } r \in R.$$

If, in addition, the multiplication in $R$ is commutative, then we shall say that $R$ is a *commutative ring*. Virtually all the rings we shall study in this book will be commutative, although occasionally we shall focus attention on certain commutative subrings of rings which might not be commutative, such as endomorphism rings of modules. Thus we shall occasionally have to refer to non-commutative rings, and for this reason the word 'commutative' will always be inserted at appropriate places in hypotheses.

The reader should have a substantial fund of examples of commutative rings at his or her disposal, and we review some familiar examples now. We use this opportunity to introduce some more of the notation that will be employed in this book.

**1.2** EXAMPLES. (i) The ring of integers $\mathbb{Z}$ is an example of a commutative ring.

(ii) The ring of Gaussian integers will be denoted by $\mathbb{Z}[i]$. See [20, p. 18]. The ring $\mathbb{Z}[i]$ consists of all complex numbers of the form $a + ib$ where

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



$a, b \in \mathbb{Z}$, and the ring operations are ordinary addition and multiplication of complex numbers. This is, of course, an example of a commutative ring.

(iii) Let $n$ be an integer with $n > 1$. The ring of residue classes of integers modulo $n$ will (sometimes) be denoted by $\mathbb{Z}_n$. See [20, 1.7]. This ring has exactly $n$ elements, and so is an example of a finite commutative ring.

(iv) Another example of a commutative ring is given by the set $C[0,1]$ of all continuous real-valued functions defined on the closed interval $[0,1]$. See [20, p. 8]. In this ring, the operations of addition and multiplication are defined 'pointwise': thus, for $f, g \in C[0,1]$ we define $f+g$ and $fg$ by the rules

$$(f+g)(x) = f(x) + g(x) \qquad \text{for all } x \in [0,1]$$

and

$$(fg)(x) = f(x)g(x) \qquad \text{for all } x \in [0,1].$$

**1.3** REMARK. Let $R$ be a commutative ring. In our definition, there is no requirement that the multiplicative identity element $1_R$ of $R$ should be different from its zero element $0_R$ (or 0). (This is one way in which our approach differs from that of [20].) A ring $R$ in which $1_R = 0_R$ is called a *trivial* ring; such a ring consists of just one, necessarily zero, element.

Let $R$ be a commutative ring. Two new commutative rings which can be constructed from $R$ are the ring $R[X]$ of polynomials in the indeterminate $X$ with coefficients in $R$, and the ring $R[[X]]$ of formal power series in $X$ with coefficients in $R$. As both these methods of constructing new commutative rings from old are absolutely fundamental to the subject matter of this book, it is appropriate for us to review the ideas involved here. It is expected that the review will be revision (both $R[X]$ and $R[[X]]$ are discussed in [20]); this means that it is reasonable to take the neat approach of discussion of $R[[X]]$ before $R[X]$.

A typical element of $R[[X]]$ is a 'formal power series'

$$a_0 + a_1 X + \cdots + a_n X^n + \cdots,$$

where the coefficients $a_0, a_1, \ldots, a_n, \ldots \in R$. (For each non-negative integer $n$, we refer to $a_n$ as the *$n$-th coefficient* of the above formal power series.) Even though the symbol '+' is used, the reader should not think that, at this elementary stage, an addition is involved: the above expression is really just a convenient notation for the infinite sequence

$$(a_0, a_1, \ldots, a_n, \ldots),$$

and the alternative notation $\sum_{i=0}^{\infty} a_i X^i$ is preferable from some points of view.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



Two formal power series $\sum_{i=0}^{\infty} a_i X^i$ and $\sum_{i=0}^{\infty} b_i X^i$ in $R[[X]]$ are considered equal precisely when $a_i = b_i$ for all integers $i \geq 0$. Addition and multiplication in $R[[X]]$ are defined as follows: for all $\sum_{i=0}^{\infty} a_i X^i$, $\sum_{i=0}^{\infty} b_i X^i \in R[[X]]$,

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i,$$

and

$$\left(\sum_{i=0}^{\infty} a_i X^i\right)\left(\sum_{j=0}^{\infty} b_j X^j\right) = \sum_{k=0}^{\infty} c_k X^k,$$

where, for each integer $k \geq 0$,

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0.$$

With these definitions, it turns out that $R[[X]]$ is a commutative ring, with zero element $\sum_{i=0}^{\infty} 0X^i$ (abbreviated to 0, of course) and identity element

$$1 + 0X + \cdots + 0X^n + \cdots.$$

The subset of $R[[X]]$ consisting of all formal power series $\sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ in which only finitely many of the coefficients $a_i$ are non-zero is also a commutative ring with respect to the above operations, having the same identity element as $R[[X]]$. It is called the *ring of polynomials in $X$ with coefficients in $R$* and is denoted by $R[X]$. It is customary to omit a 'term' $a_n X^n$ from the formal expression

$$a_0 + a_1 X + \cdots + a_i X^i + \cdots$$

for a formal power series or polynomial when the coefficient $a_n$ is zero. Thus, with this convention, a typical polynomial in $R[X]$ has the form

$$a_0 + a_1 X + \cdots + a_d X^d$$

for some non-negative integer $d$, where $a_0, \ldots, a_d \in R$, and furthermore the '+' signs in the above expression really can now be interpreted as standing for addition. If we have $a_d \neq 0$ here, then we say that $d$ is the *degree* of the above polynomial. We define the degree of the zero polynomial to be $-\infty$.

With the convention just introduced, $R$ itself is regarded as a subset of $R[X]$ and of $R[[X]]$. It is time we had the concept of subring at our disposal.

**1.4** DEFINITION. A subset $S$ of a ring $R$ is said to be a *subring* of $R$ precisely when $S$ is itself a ring with respect to the operations in $R$ and $1_S = 1_R$, that is, the multiplicative identity of $S$ is equal to that of $R$.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



It should be clear to the reader that, if $R$ is a commutative ring, and $X$ is an indeterminate, then $R$ is a subring of $R[X]$ and also a subring of $R[[X]]$, and $R[X]$ is a subring of $R[[X]]$.

There is a simple criterion for a subset of a ring $R$ to be a subring of $R$.

**1.5** THE SUBRING CRITERION. (See [20, Theorem 1.4.4].) *Let $R$ be a ring and let $S$ be a subset of $R$. Then $S$ is a subring of $R$ if and only if the following conditions hold:*

(i) $1_R \in S$;
(ii) *whenever* $a, b \in S$, *then* $a + b \in S$;
(iii) *whenever* $a \in S$, *then* $-a \in S$;
(iv) *whenever* $a, b \in S$, *then* $ab \in S$. □

The notion of subring leads naturally to the concept of ring homomorphism.

**1.6** DEFINITION. Let $f : R \to S$ be a mapping from the ring $R$ to the ring $S$. Then $f$ is said to be a *homomorphism* (or *ring homomorphism*) precisely when

(i) $f(a + b) = f(a) + f(b)$ for all $a, b \in R$,
(ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$, and
(iii) $f(1_R) = 1_S$.

A bijective ring homomorphism is called an *isomorphism* (or *ring isomorphism*).

For example, if $R'$ is a subring of the ring $R$, then the inclusion mapping $i : R' \to R$ is an injective ring homomorphism. In fact, there are many situations where we use an injective ring homomorphism $f : T \to R$ from a ring $T$ to a ring $R$ to identify elements of $T$ as elements of $R$.

**1.7** ♯EXERCISE. Let $R, S$ be rings, and let $f : R \to S$ be an isomorphism of rings. Prove that the inverse mapping

$$f^{-1} : S \to R$$

is also a ring isomorphism.

In view of this result, we say, if there is a ring isomorphism from $R$ to $S$, that $R$ and $S$ are *isomorphic* rings, and we write $R \cong S$.

**1.8** LEMMA. (See [20, Theorem 1.4.5].) *Let $f : R \to S$ be a homomorphism of rings. Then* $\operatorname{Im} f$, *the image of $f$, is a subring of $S$.* □

**1.9** DEFINITION. Let $R$ be a commutative ring. By an *$R$-algebra* we shall mean a ring $S$ endowed with a ring homomorphism $f : R \to S$. Thus the homomorphism $f$ is to be regarded as part of the structure of the $R$-algebra $S$. When we have this situation, it is automatic that $S$ is an algebra over its subring $\operatorname{Im} f$ by virtue of the inclusion homomorphism.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



We should point out at once that the concept of $R$-algebra introduced in 1.9 above occurs very frequently in ring theory, simply because every ring is automatically a $\mathbb{Z}$-algebra. We explain in 1.10 why this is the case.

**1.10** REMARK. Let $R$ be a ring. Then the mapping $f : \mathbb{Z} \to R$ defined by $f(n) = n(1_R)$ for all $n \in \mathbb{Z}$ is a ring homomorphism, and, in fact, is the only ring homomorphism from $\mathbb{Z}$ to $R$.

Here,

$$n(1_R) = \begin{cases} 1_R + \cdots + 1_R \quad (n \text{ terms}) & \text{for } n > 0, \\ 0_R & \text{for } n = 0, \\ (-1_R) + \cdots + (-1_R) \quad (-n \text{ terms}) & \text{for } n < 0. \end{cases}$$

It should be clear from 1.5 that the intersection of the members of any non-empty family of subrings of a ring $R$ is again a subring of $R$. This observation leads to the following lemma. Before we state it, it is appropriate to point out the convention whereby, for $a \in R$, the symbol $a^0$ is interpreted as $1_R$.

**1.11** LEMMA. *Let $S$ be a subring of the ring $R$, and let $\Gamma$ be a subset of $R$. Then $S[\Gamma]$ is defined to be the intersection of all subrings of $R$ which contain both $S$ and $\Gamma$. (There certainly is one such subring, namely $R$ itself.) Thus $S[\Gamma]$ is a subring of $R$ which contains both $S$ and $\Gamma$, and it is the smallest such subring of $R$ in the sense that it is contained in every other subring of $R$ that contains both $S$ and $\Gamma$.*

*In the special case in which $\Gamma$ is a finite set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, we write $S[\Gamma]$ as $S[\alpha_1, \alpha_2, \ldots, \alpha_n]$.*

*In the special case in which $S$ is commutative, and $\alpha \in R$ is such that $\alpha s = s\alpha$ for all $s \in S$, we have*

$$S[\alpha] = \left\{ \sum_{i=0}^{t} s_i \alpha^i : t \in \mathbb{N}_0,\ s_0, \ldots, s_t \in S \right\}.$$

*Proof.* Only the claim in the last paragraph still requires proof. For this, let

$$H = \left\{ \sum_{i=0}^{t} s_i \alpha^i : t \in \mathbb{N}_0,\ s_0, \ldots, s_t \in S \right\}.$$

Since $S$ is commutative and $\alpha s = s\alpha$ for all $s \in S$, it is clear from the Subring Criterion 1.5 that $H$ is a subring of $R$; it also contains $S$ and $\alpha = (1_S)\alpha$. Hence

$$S[\alpha] \subseteq H.$$

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



On the other hand, it is clear that $H$ must be contained in every subring of $R$ which contains both $S$ and $\alpha$. Hence $S[\alpha] = H$. □

Note that, when $R$ is a commutative ring and $X$ is an indeterminate, then it follows from 1.11 that our earlier use of $R[X]$ to denote the polynomial ring is consistent with this new use of $R[X]$ to denote 'ring adjunction'. A similar comment applies to our earlier notation $\mathbb{Z}[i]$ (of 1.2(ii)) for the ring of Gaussian integers: of course, the set $\mathbb{C}$ of all complex numbers is a ring with respect to ordinary addition and multiplication of complex numbers, and, since $i^2 = -1$, the ring of Gaussian integers is the smallest subring of $\mathbb{C}$ which contains both $\mathbb{Z}$ and $i$.

**1.12** ♯EXERCISE. Let $S$ be a subring of the commutative ring $R$, and let $\Gamma$, $\Delta$ be subsets of $R$. Show that $S[\Gamma \cup \Delta] = S[\Gamma][\Delta]$, and

$$S[\Gamma] = \bigcup_{\Omega \subseteq \Gamma,\ |\Omega| < \infty} S[\Omega].$$

(Here is a hint: show that the right-hand side in the above display is a subring of $R$ which contains both $S$ and $\Gamma$.)

The polynomial ring $R[X]$, where $R$ is a commutative ring, has the 'universal property' described in the following lemma.

**1.13** LEMMA. *Let $R$ be a commutative ring, and let $X$ be an indeterminate; let $T$ be a commutative $R$-algebra with structural ring homomorphism $f : R \to T$; and let $\alpha \in T$. Then there is a unique ring homomorphism $f_1 : R[X] \to T$ which extends $f$ (that is, is such that $f_1|_R = f$) and satisfies $f_1(X) = \alpha$.*

*Proof.* If $f_1 : R[X] \to T$ were a ring homomorphism which extends $f$ and satisfies $f_1(X) = \alpha$, then it would have to satisfy $f_1(rX^i) = f(r)\alpha^i$ for $r \in R$ and $i \in \mathbb{N}_0$, and it follows that the only possible candidate for $f_1$ is the mapping defined by

$$f_1\left(\sum_{i=0}^{n} r_i X^i\right) = \sum_{i=0}^{n} f(r_i)\alpha^i$$

for all $n \in \mathbb{N}_0$, $r_0, \ldots, r_n \in R$. It is completely straightforward to check that this mapping does indeed have all the desired properties. □

Consider again the ring of polynomials $R[X]$ in the indeterminate $X$ with coefficients in the commutative ring $R$ (we sometimes say 'ring of

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



polynomials over $R$'). What happens if we form the ring of polynomials over $R[X]$ in another indeterminate $Y$? The new ring can be denoted by $R[X][Y]$, and, in view of 1.12, also by $R[X,Y]$; but what can we say about its elements?

A typical element of $R[X][Y]$ has the form

$$f_0 + f_1 Y + \cdots + f_n Y^n$$

for some $n \in \mathbb{N}_0$ and $f_0, \ldots, f_n \in R[X]$, and so can be expressed as a finite sum of expressions of the form

$$r_{ij} X^i Y^j,$$

where $i, j \in \mathbb{N}_0$, $r_{ij} \in R$. Moreover, it is easy to see that an expression of the form

$$\sum_{i=0}^{n} \sum_{j=0}^{m} s_{ij} X^i Y^j$$

in $R[X][Y]$, where $n, m \in \mathbb{N}_0$ and $s_{ij} \in R$ for $i = 0, \ldots, n$, $j = 0, \ldots, m$, is zero if and only if $s_{ij} = 0$ for all $i = 0, \ldots, n$ and $j = 0, \ldots, m$. We describe this property of $X$ and $Y$ by saying that they are 'algebraically independent' over $R$.

The above ideas can easily be extended from 2 to any finite number of indeterminates.

**1.14** DEFINITION. Let $R$ be a commutative ring, and let $\alpha_1, \ldots, \alpha_n \in R$; let $R_0$ be a subring of $R$. Then $\alpha_1, \ldots, \alpha_n$ are said to be *algebraically independent over* $R_0$ (strictly speaking, we should say *the family* $(\alpha_i)_{i=1}^n$ *is algebraically independent over* $R_0$) precisely when the following condition is satisfied: whenever $\Lambda$ is a finite subset of ${\mathbb{N}_0}^n$ and elements

$$r_{i_1,\ldots,i_n} \in R_0 \qquad ((i_1, \ldots, i_n) \in \Lambda)$$

are such that

$$\sum_{(i_1,\ldots,i_n)\in\Lambda} r_{i_1,\ldots,i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n} = 0,$$

then $r_i = 0$ for all $i \in \Lambda$.

**1.15** REMARK. Let $R$ be a commutative ring and let $n$ be a positive integer. Form polynomial rings successively by defining $R_0 = R$, $R_i = R_{i-1}[X_i]$ for $i = 1, \ldots, n$, where $X_1, \ldots, X_n$ are indeterminates. Then

(i) $R_n = R[X_1, \ldots, X_n]$;

(ii) $X_1, \ldots, X_n$ are algebraically independent over $R$;

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



(iii) a typical element of $R_n$ has the form

$$\sum_{(i_1,\ldots,i_n)\in\Lambda} r_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

for some finite subset $\Lambda$ of ${\mathbb{N}_0}^n$ and some

$$r_{i_1,\ldots,i_n} \in R \qquad ((i_1,\ldots,i_n) \in \Lambda),$$

and, if it is non-zero, then its *(total) degree* is defined to be the greatest $d \in \mathbb{N}_0$ for which there exists $(i_1,\ldots,i_n) \in \Lambda$ such that $i_1 + \cdots + i_n = d$ and $r_{i_1,\ldots,i_n} \neq 0$; and

(iv) as in the case of one variable, the *(total) degree* of the zero element of $R_n$ is defined to be $-\infty$.

We shall refer to $R_n$ as the *ring of polynomials with coefficients in $R$ (or over $R$) in the $n$ indeterminates $X_1,\ldots,X_n$*.

The next exercise shows that the above polynomial ring $R[X_1,\ldots,X_n]$ has a universal property analogous to that described for $R[X]$ in 1.13.

**1.16** ♯EXERCISE. Let $R'$ be a commutative ring, and let $\xi_1,\ldots,\xi_n \in R'$ be algebraically independent over the subring $R$ of $R'$. Let $T$ be a commutative $R$-algebra with structural ring homomorphism $f : R \to T$ and let $\alpha_1,\ldots,\alpha_n \in T$. Show that there is exactly one ring homomorphism

$$g : R[\xi_1,\ldots,\xi_n] \to T$$

which extends $f$ (that is, is such that $g|_R = f$) and is such that $g(\xi_i) = \alpha_i$ for all $i = 1,\ldots,n$.

Deduce that there is a (unique) ring isomorphism

$$h : R[\xi_1,\ldots,\xi_n] \longrightarrow R[X_1,\ldots,X_n],$$

where $R[X_1,\ldots,X_n]$ denotes the polynomial ring constructed in 1.15, such that $h(\xi_i) = X_i$ for all $i = 1,\ldots,n$ and $h|_R : R \to R$ is the identity map.

This exercise shows that, whenever $\xi_1,\ldots,\xi_n$ are elements of a commutative ring $R'$ and $\xi_1,\ldots,\xi_n$ are algebraically independent over the subring $R$ of $R'$, then $R[\xi_1,\ldots,\xi_n]$ is 'essentially' the ring of polynomials $R[X_1,\ldots,X_n]$ discussed in 1.15. Indeed, whenever we discuss such a ring of polynomials in the rest of the book, it will, of course, be (tacitly) understood that the family $(X_i)_{i=1}^n$ is algebraically independent over $R$. The reader is reminded (see 1.1) that the symbols $X, Y, X_1,\ldots,X_n$ always denote indeterminates in this book.

The above exercise leads to the idea of 'evaluation' of a polynomial.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521646235 - Steps in Commutative Algebra, Second Edition
R. Y. Sharp
Excerpt
More information



**1.17** DEFINITION. Let $R$ be a subring of the commutative ring $S$, and consider the polynomial ring $R[X_1, \ldots, X_n]$ over $R$ in $n$ indeterminates $X_1, \ldots, X_n$. Let $\alpha_1, \ldots, \alpha_n \in S$. By 1.16, there is exactly one ring homomorphism $g : R[X_1, \ldots, X_n] \to S$ with the properties that

$$g(r) = r \qquad \text{for all } r \in R$$

and

$$g(X_i) = \alpha_i \qquad \text{for all } i = 1, \ldots, n.$$

This homomorphism $g$ is called *the evaluation homomorphism*, or just *evaluation*, at $\alpha_1, \ldots, \alpha_n$.

It is clear that, in the situation of 1.17, the effect of $g$ on an element $p \in R[X_1, \ldots, X_n]$ is worked out simply by replacing, for each $i = 1, \ldots, n$, each occurrence of $X_i$ by $\alpha_i$. For this reason, $g$ is sometimes referred to as 'the result of putting $X_i = \alpha_i$ for $i = 1, \ldots, n$'. This is perhaps unfortunate, because, although we shall certainly write the image of $p$ under the evaluation homomorphism $g$ as

$$p(\alpha_1, \ldots, \alpha_n)$$

on occasion, one should certainly not confuse the concept of polynomial with that of function. The following exercise illustrates the point.

**1.18** EXERCISE. Let $p = X^7 - X \in \mathbb{Z}_7[X]$. Show that $p(\alpha) = 0$ for all $\alpha \in \mathbb{Z}_7$.

**1.19** EXERCISE. Let $K$ be an infinite field, let $\Lambda$ be a finite subset of $K$, and let $f \in K[X_1, \ldots, X_n]$, the ring of polynomials over $K$ in the indeterminates $X_1, \ldots, X_n$. Suppose that $f \neq 0$. Show that there exist infinitely many choices of

$$(\alpha_1, \ldots, \alpha_n) \in (K \setminus \Lambda)^n$$

for which $f(\alpha_1, \ldots, \alpha_n) \neq 0$.

Again, let $R$ be a commutative ring, and let $X_1, \ldots, X_n$ be indeterminates. We can successively form power series rings by the following inductive procedure: set $R_0 = R$, and, for each $i \in \mathbb{N}$ with $0 < i \leq n$, let

$$R_i = R_{i-1}[[X_i]].$$

Such power series rings are very important in commutative algebra, and it is desirable that we have available a convenient description of them. To this

© Cambridge University Press www.cambridge.org