IDEAL THEORY

PRELIMINARIES

The starting point of the theory which is developed in the following pages, is the definition of the algebraic system which is known as a ring. Roughly speaking, a ring is a set of objects which can be *added* and *multiplied*, and which may be manipulated, in so far as these two operations are concerned, more or less in the natural manner. We shall now define precisely what it is that the algebraists call a ring, and then we shall deduce those elementary consequences of the definition, which are used constantly in the handling of formulae.

Suppose that we have a set R of objects, which we shall refer to as the *elements* of R, and which we shall denote by the letters a, b, c, and so on. Suppose, further, that with each ordered pair a, b of elements of R, there are associated two elements of R, which are called the *sum* and the *product* of a and b, and which are denoted by $a+b$ and by ab respectively. The set R (together with the operations of addition and multiplication) is said to form a *ring*, whenever the following six conditions are satisfied:

(1) $a+b=b+a$ *for all* a *and* b.

(2) $(a+b)+c=a+(b+c)$ *for all* a, b, *and* c.

(3) *There is an element* Θ *such that* $a+\Theta=a$ *for all* a.

(4) *For each element* a *there exists at least one element* x *such that* $a+x=\Theta$.

(5) $a(bc)=(ab)c$ *for all* a, b, *and* c.

(6) $a(b+c)=ab+ac$ *and* $(b+c)a=ba+ca$ *for all* a, b, *and* c.

In (1), the expression 'for all a and b' means, of course, 'for all pairs of elements a and b belonging to R', and similar interpretations are intended in (2), (3), (5) and (6). For brevity, instead of writing 'a belongs to R' we shall often write $a \in R$, and, more generally, if S is a subset of R we shall write $a \in S$ if we wish

to indicate that a belongs to S. We shall now deduce those elementary consequences of the definition of a ring, to which a reference has already been made.

(7) *There is only one element* Θ *with the property that* $a+\Theta=a$ *for all* a.

For assume that $a+\Theta=a+\Theta'=a$ for all a. Then, on the one hand, $\Theta'+\Theta=\Theta'$; and, on the other hand, using (1), we have $\Theta'+\Theta=\Theta+\Theta'$ which is equal to Θ by hypothesis. Thus $\Theta'=\Theta'+\Theta=\Theta$. The element Θ is called the *zero element* of the ring.

(8) *If* a *and* b *are given the equation* $a+x=b$ *has one and only one solution.*

For by (4) there exists $y\in R$ such that $a+y=\Theta$, and then, since

$$a+(y+b)=(a+y)+b=\Theta+b=b+\Theta=b,$$

it follows that $y+b$ is one solution. Again, supposing $a+x=b$, we have

$$y+b=y+(a+x)=(y+a)+x=(a+y)+x=\Theta+x=x+\Theta=x,$$

which shows that $y+b$ is the only solution.

As a particular case we notice that the equation $a+x=\Theta$ has a unique solution. This solution will be denoted by $-a$. From $\Theta+\Theta=\Theta$ we see that $-\Theta=\Theta$, and from $(-a)+a=a+(-a)=\Theta$ we see that $-(-a)=a$. Again, by (1), (2) and (3), we have $(a+b)+(-a)=b$, and if we now add $-b$ to both sides of this equation we find that $-(a+b)=(-a)+(-b)$.

(9) $\Theta a=a\Theta=\Theta$ *for all* a.

In fact, $\Theta a=(\Theta+\Theta)a=\Theta a+\Theta a$ and since we also have $\Theta a+\Theta=\Theta a$ it follows, by (8), that $\Theta a=\Theta$. We can prove that $a\Theta=\Theta$ in a similar way.

(10) $-(ab)=(-a)b=a(-b)$, *and* $(-a)(-b)=ab$.

To see this we note that

$$\Theta=\Theta b=(a+(-a))b=ab+(-a)b$$

which shows that $-(ab)=(-a)b$, and the proof that

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

is similar. If we now take the negatives of both sides of the equation $-(ab) = (-a)\,b$ we obtain

$$ab = -(-a)\,b = (-a)(-b).$$

It is usually convenient to write $a-b$ in place of $a+(-b)$. It follows immediately that $-(a-b) = b-a$; that $c(a-b) = ca-cb$; and that $(a-b)\,c = ac-bc$.

To the above observations, we add the remark that from (2) and (5) it follows, in the usual way, that we can use symbols such as $a_1+a_2+\ldots+a_n$ and $a_1a_2\ldots a_n$, that is, sums and products of more than two terms, without ambiguity.

Commutative rings. The ring R is called *commutative* if $ab = ba$ for all a and b. In such a ring, permuting the terms of a product $a_1a_2\ldots a_n$ does not change its value. Roughly speaking, in a commutative ring all the usual algebraic manipulations are permissible, except those which involve cancellation or division. The rings, which will concern us, are such that, usually, we cannot conclude from $ab = ac$ and $a \neq \Theta$ that $b = c$; and it will hardly ever be true that $a \neq \Theta$ implies that the equation $ax = b$ has a solution.

Rings with a unit element. A ring R, commutative or not, is said to have an element e as a *unit element* if $e \neq \Theta$, and if $ea = ae = a$ for all a. A ring has at most one unit element, for if

$$ea = ae = e'a = ae' = a$$

for all a, then ee' is equal both to e and to e', hence e and e' are the same.

It is extremely easy to give a large number of different examples of a ring, but we shall not stop to try and indicate the scope of this concept. However, it is a good idea for the reader to keep a definite example in mind, and for this the polynomials in n variables, with complex numbers as coefficients, will serve excellently. Such polynomials are easily seen to form a ring, and it was the study of this ring (in connexion with algebraic geometry) which gave rise to a large part of contemporary ideal theory.

CHAPTER I

THE PRIMARY DECOMPOSITION

1·1. A convention. Now that we have given a formal definition of a ring, we can begin the systematic development of our subject. The rings that we shall consider will all be commutative, and they will all have a unit element. It is therefore convenient to use the word 'ring' in a more restricted sense than is customary in modern algebra, and for this reason we lay down the following convention: *From now on 'ring' will always mean a commutative ring with a unit element.* The zero element and the unit element of a ring R will be denoted by 0 and 1 respectively, or, if we are concerned with several rings at the same time, by 0_R and 1_R.

1·2. Ideals and their calculus. Let R be a ring (commutative and with a unit element), and let $\mathfrak{a}$ be a non-empty subset of R, then $\mathfrak{a}$ is called an *ideal* of R in all cases where the following two conditions are satisfied:

(1) *Whenever* a_1 *and* a_2 *belong to* $\mathfrak{a}$, *then* $a_1 \pm a_2$ *both belong to* $\mathfrak{a}$.

(2) *If* $a \in \mathfrak{a}$, *then* $ra \in \mathfrak{a}$ *for all* $r \in R$.

A trivial example of an ideal is obtained by taking $\mathfrak{a}$ to be the whole ring. We shall call an ideal which is not the whole ring a *proper ideal*; for example, the set consisting only of the zero element is not only an ideal (this follows immediately from the definition), but it is also a proper ideal, for by the very definition of the unit element, 1 and 0 are different. Let us note that every ideal $\mathfrak{a}$ contains the zero element, for we can choose $a \in \mathfrak{a}$ (since $\mathfrak{a}$ is not empty) and then $0a = 0$ will belong to $\mathfrak{a}$ by (2); further, since $-a = 0 - a$, it follows from (1) that if $a \in \mathfrak{a}$ then $-a \in \mathfrak{a}$.

As far as is convenient we shall use small German letters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc., to denote ideals, and we shall employ small Latin and Greek letters to denote elements.

The four basic ways of combining ideals are known as *addition*, *multiplication*, *intersection*, and *residual division*.

Addition. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two given ideals, and that $\mathfrak{c}$ is the set of all elements which can be written in the form $a+b$, where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Then $\mathfrak{c}$ is an ideal. To see this suppose that $x_1 \in \mathfrak{c}$, that $x_2 \in \mathfrak{c}$, and that $r \in R$, then $x_1 = a_1 + b_1$, $x_2 = a_2 + b_2$ where a_1, a_2 belong to $\mathfrak{a}$ and where b_1, b_2 belong to $\mathfrak{b}$, and we also have

$$x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2), \quad x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2),$$
$$rx_1 = (ra_1) + (rb_1).$$

But $\mathfrak{a}$ and $\mathfrak{b}$ are ideals so $a_1 + a_2$, $a_1 - a_2$, ra_1 are all in $\mathfrak{a}$, and $b_1 + b_2$, $b_1 - b_2$, rb_1 are all in $\mathfrak{b}$. This shows that $x_1 + x_2$, $x_1 - x_2$, and rx_1 are all in $\mathfrak{c}$, and thereby establishes that $\mathfrak{c}$ is an ideal. This ideal is called the *sum* of $\mathfrak{a}$ and $\mathfrak{b}$ and is denoted by $\mathfrak{a} + \mathfrak{b}$. It is clear that $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$. Further, if $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ are any three ideals then $\mathfrak{a}_1 + (\mathfrak{a}_2 + \mathfrak{a}_3) = (\mathfrak{a}_1 + \mathfrak{a}_2) + \mathfrak{a}_3$, for both $\mathfrak{a}_1 + (\mathfrak{a}_2 + \mathfrak{a}_3)$ and $(\mathfrak{a}_1 + \mathfrak{a}_2) + \mathfrak{a}_3$ consist of all elements of the form $a_1 + a_2 + a_3$, where $a_i \in \mathfrak{a}_i$ for $i = 1, 2, 3$. Now every element of $\mathfrak{a}$ can be written in the form $a + 0$ where $a \in \mathfrak{a}$, which (since $0 \in \mathfrak{b}$) shows that $\mathfrak{a}$ is contained in $\mathfrak{a} + \mathfrak{b}$. Quite generally, if A and B are two subsets of R, we write $A \subseteq B$ or $B \supseteq A$ whenever every element of A is an element of B (i.e. whenever A is contained in B), and we write $A \subset B$ or $B \supset A$ if $A \subseteq B$ and there is at least one element of B not contained in A (i.e. whenever the inclusion is strict). We have therefore proved that $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$, and since $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$, it follows also that $\mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{b}$.

Multiplication. This time, supposing that $\mathfrak{a}$ and $\mathfrak{b}$ are given ideals, we let $\mathfrak{c}$ consist of all elements which can be written as a finite sum of products ab, where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. $\mathfrak{c}$ is an ideal. For suppose that $x_1, x_2 \in \mathfrak{c}$ and that $r \in R$, then

$$x_1 = a_1 b_1 + a_2 b_2 + \ldots + a_p b_p, \quad x_2 = a'_1 b'_1 + a'_2 b'_2 + \ldots + a'_q b'_q,$$

where the a_i and the a'_j are in $\mathfrak{a}$, and the b_i and b'_j are in $\mathfrak{b}$. From this we obtain

$$x_1 + x_2 = a_1 b_1 + \ldots + a'_q b'_q,$$

$$x_1 - x_2 = a_1 b_1 + \ldots + a_p b_p + (-a'_1) b'_1 + \ldots + (-a'_q) b'_q,$$

and

$$rx_1 = (ra_1) b_1 + \ldots + (ra_p) b_p.$$

Now $-a'_j \in \mathfrak{a}$ and $ra_i \in \mathfrak{a}$, which establishes that $x_1 + x_2$, $x_1 - x_2$, and rx_1 are all in $\mathfrak{c}$, and, consequently, that $\mathfrak{c}$ is an ideal. The ideal

that we have just constructed is called the *product* of $\mathfrak{a}$ and $\mathfrak{b}$, and is denoted by $\mathfrak{ab}$. We see at once that $\mathfrak{ab} = \mathfrak{ba}$, and, if $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ are any three ideals, that $\mathfrak{a}_1(\mathfrak{a}_2\mathfrak{a}_3) = (\mathfrak{a}_1\mathfrak{a}_2)\mathfrak{a}_3$, for both sides of the latter equation consist of all elements which can be written as a finite sum of products $a_1a_2a_3$, where $a_i \in \mathfrak{a}_i$ for $i = 1, 2, 3$. Further,

$$\mathfrak{ab} \subseteq \mathfrak{a}, \quad \mathfrak{ab} \subseteq \mathfrak{b} \quad \text{and} \quad \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2) = \mathfrak{ab}_1 + \mathfrak{ab}_2.$$

Here the first two assertions are quite obvious; let us prove the third. Since $\mathfrak{b}_1 \subseteq \mathfrak{b}_1 + \mathfrak{b}_2$ we have $\mathfrak{ab}_1 \subseteq \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$ and similarly $\mathfrak{ab}_2 \subseteq \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$; consequently

$$\mathfrak{ab}_1 + \mathfrak{ab}_2 \subseteq \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2) + \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2) = \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2),$$

for a moment's reflexion shows that an ideal is unaltered by adding it to itself. Again, if $a \in \mathfrak{a}$, $b_1 \in \mathfrak{b}_1$, and $b_2 \in \mathfrak{b}_2$, then

$$a(b_1 + b_2) = ab_1 + ab_2 \in (\mathfrak{ab}_1 + \mathfrak{ab}_2),$$

and therefore any sum of terms such as $a(b_1 + b_2)$ will also belong to $\mathfrak{ab}_1 + \mathfrak{ab}_2$. In other words, every element of $\mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$ belongs to $\mathfrak{ab}_1 + \mathfrak{ab}_2$, i.e. $\mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2) \subseteq \mathfrak{ab}_1 + \mathfrak{ab}_2$. Combining this with $\mathfrak{ab}_1 + \mathfrak{ab}_2 \subseteq \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$ we obtain $\mathfrak{ab}_1 + \mathfrak{ab}_2 = \mathfrak{a}(\mathfrak{b}_1 + \mathfrak{b}_2)$.

Intersection. Let $\mathfrak{a}_i$ $(i \in I)$ be a finite or infinite set of ideals, the range I of the suffix i being quite arbitrary. The elements which belong to all the $\mathfrak{a}_i$ form a set which is called their *intersection*, and which is denoted by $\bigcap_{i \in I} \mathfrak{a}_i$, or, more casually, by $\bigcap \mathfrak{a}_i$. This intersection is not empty, for all the $\mathfrak{a}_i$ contain the element 0, and a trivial verification shows that it is in fact an ideal. The intersection of a finite set of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ we write either as $\bigcap_{i=1}^{n} \mathfrak{a}_i$, or as $\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n$. We proved earlier that $\mathfrak{ab} \subseteq \mathfrak{a}$ and $\mathfrak{ab} \subseteq \mathfrak{b}$. This can now be written more conveniently as $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Residual division. Once again suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals, and let us denote by $\mathfrak{c}$ the set of all elements x such that $xb \in \mathfrak{a}$ for all $b \in \mathfrak{b}$. $\mathfrak{c}$ is an ideal. For suppose that $x_1, x_2 \in \mathfrak{c}$ and that $r \in R$, then for any $b \in \mathfrak{b}$ we have

$$(x_1 + x_2)b = x_1b + x_2b,$$

$$(x_1 - x_2)b = x_1b - x_2b \quad \text{and} \quad (rx_1)b = r(x_1b).$$

Now x_1b and x_2b belong to $\mathfrak{a}$ by the definition of $\mathfrak{c}$, so $x_1b + x_2b$ and $x_1b - x_2b$ belong to $\mathfrak{a}$; also as $x_1b \in \mathfrak{a}$ we have $r(x_1b) \in \mathfrak{a}$. This

proves that $x_1 \pm x_2$ and rx_1 are all in $\mathfrak{c}$, which shows that $\mathfrak{c}$ is an ideal. $\mathfrak{c}$ is known as the *residual quotient* of $\mathfrak{a}$ and $\mathfrak{b}$, and is denoted by $\mathfrak{a} : \mathfrak{b}$. Since from $x \in (\mathfrak{a} : \mathfrak{b})$ and $b \in \mathfrak{b}$ follows $xb \in \mathfrak{a}$, we see that $(\mathfrak{a} : \mathfrak{b})\,\mathfrak{b} \subseteq \mathfrak{a}$; in fact $\mathfrak{a} : \mathfrak{b}$ is the largest ideal which when multiplied by $\mathfrak{b}$ yields an ideal contained in $\mathfrak{a}$. We note too that if $a \in \mathfrak{a}$ then certainly $ab \in \mathfrak{a}$ for all $b \in \mathfrak{b}$, which gives us the relation $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

For convenience we collect together the basic formulae of our calculus, which have now been established, and add to them some new ones of a more advanced character.

PROPOSITION 1.

(1) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$; $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$.

(2) $\mathfrak{ab} = \mathfrak{ba}$; $\mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\,\mathfrak{c}$; $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$.

(3) $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$; $\mathfrak{ab} \subseteq (\mathfrak{a} \cap \mathfrak{b})$.

(4) $(\mathfrak{a} : \mathfrak{b})\,\mathfrak{b} \subseteq \mathfrak{a}$; $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

(5) $(\bigcap \mathfrak{a}_i) : \mathfrak{b} = \bigcap (\mathfrak{a}_i : \mathfrak{b})$.

(6) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : (\mathfrak{bc})$.

(7) $\mathfrak{a} : (\mathfrak{b}_1 + \mathfrak{b}_2 + \ldots + \mathfrak{b}_n) = (\mathfrak{a} : \mathfrak{b}_1) \cap (\mathfrak{a} : \mathfrak{b}_2) \cap \ldots \cap (\mathfrak{a} : \mathfrak{b}_n)$.

(8) $\mathfrak{a} : \mathfrak{b} = \mathfrak{a} : (\mathfrak{a} + \mathfrak{b})$.

Proof. (1), (2), (3) and (4) have already been established.

(5) Let $x \in (\bigcap \mathfrak{a}_i) : \mathfrak{b}$ and let $b \in \mathfrak{b}$, then $xb \in \bigcap \mathfrak{a}_i$ so that $xb \in \mathfrak{a}_i$ for all i. Keep i fixed, then $xb \in \mathfrak{a}_i$ for all $b \in \mathfrak{b}$; i.e. $x \in (\mathfrak{a}_i : \mathfrak{b})$. We have now shown that $x \in (\mathfrak{a}_i : \mathfrak{b})$ for all i, consequently $x \in \bigcap (\mathfrak{a}_i : \mathfrak{b})$. Since x was any element of $(\bigcap \mathfrak{a}_i) : \mathfrak{b}$, we have proved that $(\bigcap \mathfrak{a}_i) : \mathfrak{b} \subseteq \bigcap (\mathfrak{a}_i : \mathfrak{b})$. Now suppose that $y \in \bigcap (\mathfrak{a}_i : \mathfrak{b})$ and let $b \in \mathfrak{b}$. For each i we have $y \in (\mathfrak{a}_i : \mathfrak{b})$, hence $yb \in \mathfrak{a}_i$, and therefore $yb \in \bigcap \mathfrak{a}_i$. But as b was any element of $\mathfrak{b}$, it follows from $yb \in \bigcap \mathfrak{a}_i$ that $y \in (\bigcap \mathfrak{a}_i) : \mathfrak{b}$. Since y was an arbitrary element of $\bigcap (\mathfrak{a}_i : \mathfrak{b})$ this proves that $\bigcap (\mathfrak{a}_i : \mathfrak{b}) \subseteq (\bigcap \mathfrak{a}_i) : \mathfrak{b}$. Combining this last relation with $(\bigcap \mathfrak{a}_i) : \mathfrak{b} \subseteq \bigcap (\mathfrak{a}_i : \mathfrak{b})$ we obtain the required result.

(6) Let $x \in (\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}$ and let b_i, c_i belong to $\mathfrak{b}$ and $\mathfrak{c}$ respectively for $1 \leqslant i \leqslant s$. Then $xc_i \in (\mathfrak{a} : \mathfrak{b})$ so that $xb_ic_i \in \mathfrak{a}$. If we now sum over i we obtain $x(b_1c_1 + b_2c_2 + \ldots + b_sc_s) \in \mathfrak{a}$. But $b_1c_1 + b_2c_2 + \ldots + b_sc_s$ can be any element of $\mathfrak{bc}$, hence we have proved that $x \in \mathfrak{a} : (\mathfrak{bc})$. Now let $y \in \mathfrak{a} : (\mathfrak{bc})$, let $b \in \mathfrak{b}$ and let $c \in \mathfrak{c}$. Then $ybc \in \mathfrak{a}$. Since this

holds for all $b \in \mathfrak{b}$, we must have $yc \in (\mathfrak{a} : \mathfrak{b})$, and as $yc \in (\mathfrak{a} : \mathfrak{b})$ for all $c \in \mathfrak{c}$, this proves that $y \in (\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}$. Our combined results tell us that $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} \subseteq \mathfrak{a} : (\mathfrak{bc})$, and also that $\mathfrak{a} : (\mathfrak{bc}) \subseteq (\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}$. This is equivalent to what we had to prove.

(7) Suppose first that $n = 2$. Let $x \in \mathfrak{a} : (\mathfrak{b}_1 + \mathfrak{b}_2)$, let $b_1 \in \mathfrak{b}_1$, and let $b_2 \in \mathfrak{b}_2$. Then $b_1 + 0 \in (\mathfrak{b}_1 + \mathfrak{b}_2)$ so that $xb_1 = x(b_1 + 0) \in \mathfrak{a}$. This holds for all $b_1 \in \mathfrak{b}_1$, consequently $x \in \mathfrak{a} : \mathfrak{b}_1$. Similarly, $x \in \mathfrak{a} : \mathfrak{b}_2$, and therefore $x \in (\mathfrak{a} : \mathfrak{b}_1) \cap (\mathfrak{a} : \mathfrak{b}_2)$. Now assume that $y \in (\mathfrak{a} : \mathfrak{b}_1) \cap (\mathfrak{a} : \mathfrak{b}_2)$, let $b_1 \in \mathfrak{b}_1$, and let $b_2 \in \mathfrak{b}_2$. Since $y \in (\mathfrak{a} : \mathfrak{b}_1)$ we have $yb_1 \in \mathfrak{a}$, and since $y \in (\mathfrak{a} : \mathfrak{b}_2)$ we have $yb_2 \in \mathfrak{a}$. By addition we obtain $y(b_1 + b_2) \in \mathfrak{a}$, but as $b_1 + b_2$ can be any element of $\mathfrak{b}_1 + \mathfrak{b}_2$ it follows that $y \in \mathfrak{a} : (\mathfrak{b}_1 + \mathfrak{b}_2)$. We have now established

$$\mathfrak{a} : (\mathfrak{b}_1 + \mathfrak{b}_2) \subseteq (\mathfrak{a} : \mathfrak{b}_1) \cap (\mathfrak{a} : \mathfrak{b}_2) \quad \text{and} \quad (\mathfrak{a} : \mathfrak{b}_1) \cap (\mathfrak{a} : \mathfrak{b}_2) \subseteq \mathfrak{a} : (\mathfrak{b}_1 + \mathfrak{b}_2),$$

which is equivalent to (7) when $n = 2$. The extension to a general n is now obtained by a simple induction. It should be noted that in writing $\mathfrak{b}_1 + \mathfrak{b}_2 + \ldots + \mathfrak{b}_n$ we are already making use of the associative law of addition, namely, $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$.

(8) By (7) $\mathfrak{a} : (\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} : \mathfrak{a}) \cap (\mathfrak{a} : \mathfrak{b})$. It is clear that $\mathfrak{a} : \mathfrak{a}$ is the whole ring R, accordingly $\mathfrak{a} : (\mathfrak{a} + \mathfrak{b}) = R \cap (\mathfrak{a} : \mathfrak{b}) = \mathfrak{a} : \mathfrak{b}$.

Remarks. The relation (5) is particularly important, for it says that an arbitrary intersection may be divided term by term.

We have already had occasion to note that an expression such as $\mathfrak{b}_1 + \mathfrak{b}_2 + \ldots + \mathfrak{b}_n$ is effectively unambiguous on account of the associative law of addition. A similar observation applies to a product $\mathfrak{b}_1 \mathfrak{b}_2 \ldots \mathfrak{b}_n$.

1·3. The ideal generated by a set. Let A be an arbitrary non-empty set of elements of our ring R. The aggregate of all elements which can be written in the form $\Sigma r_i a_i$, where $r_i \in R$, where $a_i \in A$, and where the number of terms in the sum is finite, is an ideal. The verification is extremely simple and will be left to the reader. This ideal, which is known as the *ideal generated by* A, contains every element of A, for if $a \in A$ then $1a = a$ belongs to the ideal in question. Further, every ideal which contains A will also contain the ideal generated by A, so that the ideal generated by A may be characterized as the smallest ideal containing A. As examples we note that the sum of two ideals

$\mathfrak{a}$ and $\mathfrak{b}$ is generated by the union of $\mathfrak{a}$ and $\mathfrak{b}$, that is, by the set obtained by taking all the elements of $\mathfrak{a}$ and all the elements of $\mathfrak{b}$; while $\mathfrak{ab}$ is generated by the set of all products ab where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

If A consists of a finite number of elements, say $a_1, a_2, \ldots, a_n$, then the ideal which they generate is denoted by $(a_1, a_2, \ldots, a_n)$ and it consists of all elements which can be written in the form $r_1a_1 + r_2a_2 + \ldots + r_na_n$, where the r_i may be any elements of R. Such an ideal is said to be *finitely generated*, and the elements a_i are called a *base* or *basis* of the ideal. We note that

$$(a_1, a_2, \ldots, a_m) + (b_1, b_2, \ldots, b_n) = (a_1, \ldots, a_m, b_1, \ldots, b_n),$$

and that $$(a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_n) = (\ldots, a_ib_j, \ldots)$$

where the base on the right-hand side consists of all products a_ib_j.

An ideal (a) generated by a single element is known as a *principal ideal*.

1·4. Prime ideals. An ideal $\mathfrak{p}$ is called a *prime ideal* if whenever $ab \in \mathfrak{p}$ at least one of a and b belongs to $\mathfrak{p}$. Expressed in another way, our definition states that $\mathfrak{p}$ is prime if, and only if, from $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$ always follows $b \in \mathfrak{p}$. Here we have made use of the symbol $\notin$ (cancelled epsilon) for the first time. It stands for the phrase 'does not belong to'.

PROPOSITION 2. *Let $\mathfrak{p}$ be a prime ideal, and suppose that $a_1a_2 \ldots a_n \in \mathfrak{p}$, then for at least one value of i we have $a_i \in \mathfrak{p}$. Further, if $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ are ideals and $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n \subseteq \mathfrak{p}$, then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for at least one value of i.*

Proof. Suppose that $a_1a_2 \ldots a_n \in \mathfrak{p}$ and that no a_i belongs to $\mathfrak{p}$. We shall obtain a contradiction. We have $a_1(a_2a_3 \ldots a_n) \in \mathfrak{p}$ and $a_1 \notin \mathfrak{p}$, hence, by the definition of a prime ideal, $a_2a_3 \ldots a_n \in \mathfrak{p}$. We now repeat the argument and obtain in succession, $a_3 \ldots a_n \in \mathfrak{p}$, $a_4 \ldots a_n \in \mathfrak{p}$, and finally, $a_n \in \mathfrak{p}$. This is the required contradiction. Next assume that $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n \subseteq \mathfrak{p}$, but that no $\mathfrak{a}_i$ is contained in $\mathfrak{p}$. For each i we can choose $a_i \in \mathfrak{a}_i$ so that $a_i \notin \mathfrak{p}$, and then, by the first part, $a_1a_2 \ldots a_n \notin \mathfrak{p}$. However, $a_1a_2 \ldots a_n \in \mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n$ and therefore *a fortiori* $a_1a_2 \ldots a_n \in \mathfrak{p}$, which is again a contradiction.

1·5. Primary ideals. An ideal $\mathfrak{q}$ is called a *primary ideal* if the conditions $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$ always imply that some positive power of b is in $\mathfrak{q}$. Let us note that prime ideals are always primary.

We can now indicate the lines on which the remainder of this chapter will be developed. The prime and primary ideals play roles which are (very roughly) similar to those played by prime numbers and by prime-power numbers in elementary arithmetic. They are ideals of a particularly simple type, and enjoy many special properties. Our first object will be to derive these properties, and then later we shall consider when and how a general ideal may be decomposed into primary components.

The proposition which follows shows that with every primary ideal there is associated a definite prime ideal.

PROPOSITION 3. *Let $\mathfrak{q}$ be a given primary ideal, and let $\mathfrak{p}$ denote the set of all elements x such that $x^n \in \mathfrak{q}$ for at least one positive integral value of n. Then $\mathfrak{p}$ is a prime ideal which contains $\mathfrak{q}$, and which is contained in every other prime ideal which contains $\mathfrak{q}$.*

Proof. First we show that $\mathfrak{p}$ is an ideal. Let $x, y \in \mathfrak{p}$ and let $r \in R$. Then there exist integers m and n, such that $x^m \in \mathfrak{q}$ and $y^n \in \mathfrak{q}$. Now $(x+y)^{m+n}$ can be written as a sum of terms $x^\mu y^\nu$, where $0 \leqslant \mu$, $0 \leqslant \nu$, and where $\mu + \nu = m + n$. Accordingly, we have either $\mu \geqslant m$ or $\nu \geqslant n$. In the first case $x^\mu \in \mathfrak{q}$, and in the second case $y^\nu \in \mathfrak{q}$, so that in either case $x^\mu y^\nu \in \mathfrak{q}$. This shows that $(x+y)^{m+n} \in \mathfrak{q}$, consequently, by the definition of $\mathfrak{p}$, $x+y \in \mathfrak{p}$. A similar argument shows that $x-y \in \mathfrak{p}$. Again, $(rx)^m = r^m x^m \in \mathfrak{q}$ and therefore $rx \in \mathfrak{p}$. Since $x+y$, $x-y$, and rx are all in $\mathfrak{p}$, $\mathfrak{p}$ is an ideal.

We shall now prove that $\mathfrak{p}$ is prime. Assume that $ab \in \mathfrak{p}$ and that $a \notin \mathfrak{p}$. It will be enough to show that $b \in \mathfrak{p}$. Since $ab \in \mathfrak{p}$ there is a positive integer s such that $a^s b^s \in \mathfrak{q}$. But $a^s \notin \mathfrak{q}$, for otherwise a would belong to $\mathfrak{p}$, consequently (since $\mathfrak{q}$ is primary) some power of b^s is in $\mathfrak{q}$. This is the same as saying that some power of b is in $\mathfrak{q}$, or that $b \in \mathfrak{p}$.

It is obvious from the definition that $\mathfrak{p} \supseteq \mathfrak{q}$. Let $\mathfrak{p}'$ be any prime ideal containing $\mathfrak{q}$ and let $x \in \mathfrak{p}$. Then, with a suitable integer m, $x^m \in \mathfrak{q} \subseteq \mathfrak{p}'$. Since $\mathfrak{p}'$ is prime it follows from Proposition 2 that $x \in \mathfrak{p}'$. Thus $\mathfrak{p} \subseteq \mathfrak{p}'$ and the proof is complete.