and is contained in every ideal containing S. We call (S) *the ideal generated by* S. If S is a finite set, $\{a_1, a_2, \ldots, a_n\}$, then we write $(a_1, a_2, \ldots, a_n)$ for (S). It is not easy to write down all the elements of this ideal. It is clear first that it contains all finite sums of products of the form xa_iy where $x, y \in R$ and there is no way of combining $xa_iy + x'a_iy'$ into a single term. Thus we see that to indicate explicitly all the elements of the ideal $(a_1, a_2, \ldots, a_n)$ we must consider all elements of the form

$$\sum_{i_1} x_{1i_1} a_1 y_{1i_1} + \sum_{i_2} x_{2i_2} a_2 y_{2i_2} + \cdots + \sum_{i_n} x_{ni_n} a_n y_{ni_n}. \tag{18}$$

Now it is clear that the set I of elements of the form (18) is an ideal. It is clear also that I contains every $a_i = 1a_i1$. Hence

$$I = (a_1, a_2, \ldots, a_n).$$

If I and J are ideals we denote the ideal generated by $I \cup J$ as $I + J$. We claim that this is the set K of elements of the form $a + b$, $a \in I$, $b \in J$. This is clear since K is an ideal containing I and J and is contained in every ideal containing I and J. Another important ideal associated with I and J is the product IJ, defined to be the ideal generated by all the products ab, $a \in I$, $b \in J$. It is easily seen that IJ coincides with the set of elements of the form $a_1b_1 + a_2b_2 + \cdots + a_mb_m$ where $a_i \in I$, $b_i \in J$.

Sometimes we need to consider a sequence of ideals $I_1, I_2, \ldots$ such that $I_1 \subset I_2 \subset \cdots$. We call this an *ascending chain of ideals*. It is useful to observe that for such a chain, $\bigcup I_j$ is an ideal. It suffices to show that $\bigcup I_j$ is closed under subtraction and under left and right multiplication by arbitrary elements of R. To see the first, let $a, b \in \bigcup I_j$. Then $a \in I_j$ for some j and $b \in I_k$ for some k. If l is the greater of j and k then both a and b are in I_l. Hence $a - b \in I_l$ since I_l is an ideal. Also xa and $ax \in I_j$ for any $x \in R$. Thus $a - b \in \bigcup I_j$ and $xa, ax \in \bigcup I_j$ for any a and b in $\bigcup I_j$ and any $x \in R$. Then $\bigcup I_j$ is an ideal.

If R is commutative, our description of the elements of $(a_1, a_2, \ldots, a_n)$ simplifies considerably: namely, this ideal is the set of elements of the form $\sum_1^n x_i a_i$ $(= \sum_1^n a_i x_i)$, $x_i \in R$. This is clear from (18). In particular, the ideal (a) generated by a is the set of elements xa, $x \in R$. This is called the *principal ideal generated* by a.

We can give a neat characterization of fields in terms of ideals: namely, we have

THEOREM 2.2. *Let R be a commutative ring $\neq 0$. Then R is a field if and only if the only ideals in R are R $(=(1))$ and 0 $(=(0))$.*

Proof. Suppose R is a division ring and I is a non-zero ideal in R. If $a \neq 0$ is in I then so is $1 = aa^{-1}$. It is clear that the only ideal of a ring containing 1 is R (since I will then contain every $x = x1$). Hence $I = R$. This proves that the only ideals in a division ring are 0 and R. In particular this holds for fields. Conversely, suppose that R is a commutative ring $\neq 0$ whose only ideals are 0 and R. If $a \neq 0$ is in R then $(a) \neq 0$, so $(a) = R$. It follows that $1 \in (a)$ and hence there is an $x \in R$ such that $ax = 1$. Thus every non-zero element of R is invertible and R is a field. □

EXERCISES

1. Let Γ be the ring of real-valued continuous functions on $[0, 1]$ (example 8, p. 87). Let S be a subset of $[0, 1]$ and let $Z_S = \{f \mid f(x) = 0, x \in S\}$. Verify that Z_S is an ideal. Let $S_1 = [0, \frac{1}{2}]$, $S_2 = [\frac{1}{2}, 1]$, $I_1 = Z_{S_1}$, $I_2 = Z_{S_2}$. Show that $I_1I_2 = I_1 \cap I_2 = 0$.
2. Show that the associative law holds for products of ideals: $(IJ)K = I(JK)$ if I, J, and K are ideals.
3. Does the distributive law, $I(J + K) = IJ + IK$ hold?
4. If R is a ring we define a *right* (*left*) *ideal* in R to be a subgroup of the additive group of R such that $ba \in I$ $(ab \in I)$ for every $a \in R$, $b \in I$. Verify that the subset of matrices of the form $\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$ is a right ideal and the subset of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal in $M_2(R)$ for any R. Are either of these sets ideals?
5. Prove the following extension of Theorem 2.2. A ring $R \neq 0$ is a division ring if and only if 0 and R are the only left (right) ideals in R.
6. Let R be a commutative ring and let N denote the set of nilpotent elements of R. Show that N is an ideal and R/N contains no non-zero nilpotent elements.
7. Let I be an ideal in R, U the group of units of R. Let U_1 be the subset of elements $a \in U$ such that $a \equiv 1 \pmod{I}$. Show that U_1 is a normal subgroup of U.
8. Let I be an ideal in R and let $M_n(I)$ denote the set of $n \times n$ matrices with entries in I. Show that $M_n(I)$ is an ideal in $M_n(R)$. Prove that every ideal in $M_n(R)$ has the form $M_n(I)$ for some ideal I of R, and that $I \to M_n(I)$ is a bijective map of the set of ideals of R onto the set of ideals of $M_n(R)$.

2.6 IDEALS AND QUOTIENT RINGS FOR ℤ

After the generalities of the last section we now consider the ideals of $\mathbb{Z}$ and their corresponding quotient rings $\mathbb{Z}/I$. This will lead us to some interesting number theoretic results.

As we have seen in section 1.5 and again in section 1.10, the subgroups of the additive group $(\mathbb{Z}, +, 0)$ are the cyclic groups $\langle k\rangle$ where k is a non-negative integer. Since $\langle k\rangle = \{xk | x \in \mathbb{Z}\}$ it is clear that $\langle k\rangle$ is the same thing as the principal ideal (k) of multiples of k. Since any ideal is a subgroup it follows that every ideal in $\mathbb{Z}$ is a principal ideal. Now it is clear that $(l) \supset (k)$ if and only if $k \in (l)$, hence, if and only if $k = lm$, $m \in \mathbb{Z}$. Thus the inclusion relation $(l) \supset (k)$ for the principal ideals (l), (k) is equivalent to the divisibility condition $l|k$. A consequence of this is that if $m, n \in \mathbb{Z}$ and (m, n) denotes the ideal generated by m and n, then $(m, n) = (d)$ where d is a g.c.d. of m and n. Since $(m, n) \supset (m)$ and (n), we have $d|m$ and $d|n$. On the other hand, if $e|m$ and $e|n$ then $(e) \supset (m)$ and $(e) \supset (n)$. Then $(e) \supset (m, n) = (d)$ so $e|d$. Similarly, we see that $(m) \cap (n) = ([m, n])$ where $[m, n]$ is a least common multiple of m and n.

We look next at the quotient ring $\mathbb{Z}/(k)$, which is called the *ring of residues modulo k*. Since $(k) = (-k)$ we may assume $k \geq 0$. If $k = 0$, then $\mathbb{Z}/(k)$ can be identified with $\mathbb{Z}$, and if $k > 0$, the elements of $\mathbb{Z}/(k)$ are the k cosets

$$\bar{0} = (k), \bar{1} = 1 + (k), \bar{2} = 2 + (k), \ldots, \overline{k-1} = k - 1 + (k).$$

Suppose first that k is composite: $k = lm$, $l > 1$, $m > 1$. Then $\bar{l} \neq \bar{0}$ and $\bar{m} \neq \bar{0}$ in $\mathbb{Z}/(k)$ but $\overline{lm} = \bar{k} = \bar{0}$. Thus $\mathbb{Z}/(k)$ has non-zero zero divisors if k is composite. Next let $k = p$ be a prime. In this case every $\bar{a} \neq \bar{0}$ in $\mathbb{Z}/(p)$ is invertible. Since $\mathbb{Z}/(k)$ is commutative ($\bar{a}\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\bar{a}$), it follows that $\mathbb{Z}/(p)$ is a field. Given $\bar{a} \neq \bar{0}$, then $p \nmid a$ and 1 is a g.c.d. of p and a. Hence we have integers x and y such that $ax + py = 1$. Then $\bar{1} = \overline{ax + py} = \overline{ax} + \overline{py} = \bar{a}\bar{x}$. Hence $\bar{a}$ is invertible with $\bar{x}$ as inverse.

These simple results are important enough to state as a theorem.

THEOREM 2.3. *The ring $\mathbb{Z}/(k)$ for k composite is not a domain. On the other hand, $\mathbb{Z}/(p)$ for p prime is a field.*

We shall now determine the group $U(\mathbb{Z}/(k))$ of units of $\mathbb{Z}/(k)$. If $k = 0$ then these are 1 and -1. If $k > 0$ we have

THEOREM 2.4. *The group $U(\mathbb{Z}/(k))$, $k > 0$, consists of the classes $\bar{a} = a + (k)$ such that a and k are relatively prime (that is, have 1 as g.c.d.).*

Proof. If $(a, k) = 1$ (equivalently: the ideal $(a, k) = (1)$), then we have integers x and y such that $ax + ky = 1$. Then $\bar{a}\bar{x} = \bar{1}$, so $\bar{a}$ is invertible. Conversely, if $\bar{a}\bar{b} = \bar{1}$, then $\overline{ab} = \bar{1}$, so $ab = 1 + mk$, $m \in \mathbb{Z}$. Clearly this equation shows that any common divisor of a and k divides 1. Hence a and k are relatively prime. □

The foregoing result shows that $|U(\mathbb{Z}/(k))|$ is the number $\varphi(k)$ of positive integers less than k and relatively prime to k. The function φ of positive integers thus defined is called the *Euler φ-function* (see exercises 4, p. 47). For example, if $k = 12$, the units of $\mathbb{Z}/(k)$ are $\bar{1}$, $\bar{5}$, $\bar{7}$, $\overline{11}$, and thus $\varphi(12) = 4$. In the next section we shall indicate in an exercise a formula for computing $\varphi(k)$ from the factorization of k into primes. At this point we note that if p is a prime, then it is clear from the definition that $\varphi(p) = p - 1$. Also it is easy to see that $\varphi(p^e) = p^e - p^{e-1} = p^e(1 - 1/p)$.

We recall that is G is a finite group, then $a^{|G|} = 1$ for every $a \in G$. A consequence of this result and Theorem 2.4 is that if $(a, k) = 1$, then $\bar{a}^{\varphi(k)} = \bar{1}$. The usual way of stating this result is

THEOREM 2.5. (Euler.) *If a is an integer prime to the positive integer k, then $a^{\varphi(k)} \equiv 1 \pmod{k}$.*

For $k = p$ a prime this reduces to an earlier result due to Fermat.

COROLLARY. *If p is a prime and a is an integer not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$.*

This result can also be stated in a slightly different form, namely, that $a^p \equiv a \pmod{p}$. This holds for all a since it is trivial if a is divisible by p. On the other hand, if $a^p \equiv a \pmod{p}$ and $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$ by cancellation. Hence the two statements are equivalent.

EXERCISES

1. Write down addition and multiplication tables for $\mathbb{Z}/(5)$ and for $\mathbb{Z}/(6)$.
2. Show that $\mathbb{Z}/(k)$ contains non-zero nilpotent elements ($z^n = 0$, $z \neq 0$) if and only if k is divisible by the square of a prime. Determine the nilpotent elements of $\mathbb{Z}/(180)$.
3. Prove that if D is a finite division ring then $a^{|D|} = a$ for every $a \in D$.
4. Let $A \in GL_2(\mathbb{Z}/(p))$ (that is, A is an invertible 2×2 matrix with entries in $\mathbb{Z}/(p)$). Show that $A^q = 1$ if $q = (p^2 - 1)(p^2 - p)$. Show also that $A^{q+2} = A^2$ for every $A \in M_2(\mathbb{Z}/(p))$.