$$\begin{aligned}\tan P &= -\tan(\beta+\gamma)\\ &= \left(\frac{e}{1+f}+\frac{e}{1-f}\right)\bigg/\left(\frac{e^2}{1-f^2}-1\right)\\ &= \frac{2e}{e^2+f^2-1}\\ &= \frac{2(\sin B+\sin C)}{1-2\cos(B+C)}=\frac{\sin B+\sin C}{\cos A+\frac{1}{2}}.\end{aligned}$$

It is interesting to note the corollary that, if $\angle A = 120°$, then $\angle P = 90°$, whatever the values of $\angle B$ and $\angle C$.

C. F. PARRY

7 Auclum Close, Burghfield Common, Reading RG7 3DY

Groups in modular arithmetic

K. ROBIN McLEAN

It has often been noted that modular arithmetic provides a rich source of supply of groups. Indeed, a remarkable theorem† asserts that any finite commutative group can be found by a sufficiently diligent search through the multiplicative groups and subgroups of modular arithmetic! During the last few years two articles in this area have appeared in *Mathematics Teaching*. In the first [1], Tim Brand drew attention to the fact that such a multiplicative group can have an identity element other than 1. (For example, 8 is the identity of the group {2,4,8} under multiplication mod 14.) More recently [2] Geoff Saltmarsh described an ingenious way of finding the identity and put forward an interesting conjecture about these groups.

Here I shall look at things from a slightly different standpoint, being concerned not only with the groups themselves but also with the ring of integers mod n in which each group in embedded. In particular I would like to examine the way in which the group structure influences the ring structure and vice versa, for the interaction between different types of structure is often a fruitful avenue to explore. I have not found it easy to decide how far to go with proofs. Both the articles referred to [1, 2] were written in the spirit of open-ended investigation, and in such situations there is a danger that an over-zealously supplied proof may spoil someone else's fun. On the other hand it is often interesting to see what sort of ideas are used in a proof and how the ideas are combined in the overall strategy. In the end I decided to prove a modified version of Saltmarsh's conjecture (his

† The theorem is stated without proof on p. 280 of F. J. Budden's *The fascination of groups* (Cambridge, 1972). My own proof depends on Dirichlet's theorem about prime numbers in arithmetic progressions.

original version is very nearly true!), because this seems an appropriate response to what he wrote, but for the rest I shall proceed mainly by examples which indicate how things go, whilst still (I hope) leaving enough unsignposted territory for other people to explore if they wish.

Before looking at groups or rings I shall simply state the following lemma which will be useful later for finding both identity elements and inverses:

If x and y are coprime integers, then there are integers a and b such that

$$1 = ax - by.$$

For example, if $x = 8$ and $y = 15$, we can take $a = 2$ and $b = 1$ giving

$$1 = 2 \times 8 - 1 \times 15.$$

Another way of expressing 1 in terms of 8s and 15s is given by adding $8 \times 15 - 15 \times 8$ to both sides. We then get

$$1 = 7 \times 15 - 13 \times 8.$$

In practice, possible values for a and b can often be spotted. They can always be found by using Euclid's algorithm (see, for example, [3] pp. 26–31) to calculate the h.c.f. (=1) of x and y and then working backwards.

Now let us start with a ring (e.g. $\mathbb{Z}_{12}$, the ring of integers mod 12) and look for multiplicative groups inside it. What are the possibilities for the identity element, e, of such a group? Clearly we need to have

$$e^2 = e.$$

Any solution of this equation is called an *idempotent*, because all its powers must be the same, viz.

$$e = e^2 = e^3 = e^4 = \ldots.$$

Conversely, each idempotent is the identity of a multiplicative group, for the set $\{e\}$ itself is such a group.

In a ring as small as $\mathbb{Z}_{12}$ it is possible to spot the idempotents using trial and error, but it is instructive to see how they can be found systematically. Suppose that e is an integer whose residue mod 12 is an idempotent. Then

$$e^2 \equiv e \pmod{12}. \qquad (1)$$

Hence

$$e(e-1) \equiv 0 \pmod{12}. \qquad (2)$$

It follows that e and $e - 1$ must be coprime (because they are consecutive) integers whose product is a multiple of 12. Disregarding the obvious idempotent residues 0 and 1 (mod 12) which arise when one of the integers e and $e - 1$ is itself a multiple of 12, we are left with the case when one of these integers is a multiple of 4 and the other is a multiple of 3. The next step is to apply our preliminary lemma to express the difference, 1, between e and $e-1$ as the difference between a multiple of 4 and a multiple of 3. The obvious way of doing this is to write

$$1 = 4 - 3, \tag{3}$$

which corresponds to $e = 4$ and $e - 1 = 3$. Our method ensures that these values satisfy equation (2), and we get the idempotent $e \equiv 4 \pmod{12}$ as a solution to equation (1). Alternatively we can add $4 \times 3 - 3 \times 4$ to (3) to get

$$1 = 3 \times 3 - 2 \times 4 = 9 - 8.$$

This yields the idempotent $e \equiv 9 \pmod{12}$. We might expect that further variations of this theme such as

$$1 = 7 \times 4 - 9 \times 3 = 28 - 27$$

or

$$1 = 7 \times 3 - 5 \times 4 = 21 - 20$$

would produce more and more idempotents, but in each case we return to one of the members of our original pair 4 and 9 (mod 12), because

$$28 \equiv 4 \quad \text{and} \quad 21 \equiv 9 \pmod{12}.$$

The pair of idempotents which we have found have the interesting property that their sum is 1 and their product is 0 (mod 12):

$$4 + 9 \equiv 1 \pmod{12}, \quad 4 \times 9 \equiv 0 \pmod{12}.$$

It is a general feature of life that idempotents go about in pairs of this type, the best known pair being 0 and 1. To see this, let e be an idempotent in any ring with identity 1; then

$$(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e,$$

so that $f = 1 - e$ is also an idempotent. Clearly

$$e + f = 1$$

and

$$ef = e(1-e) = e - e^2 = 0.$$

This result can be useful for finding the second idempotent of a pair. For example, having found $e \equiv 4 \pmod{12}$, we could have worked out

$$f \equiv 1 - e \equiv 1 - 4 \equiv -3 \equiv 9 \pmod{12}.$$

Tim Brand wrote about surprising identity elements. Indeed they are—and you can arrange for the favourite number of your choice to be one! Writing in Silver Jubilee year I shall assume that your favourite number is $e = 25$. If you insist on choosing 1977, you will be pleased to know that this is the identity of the group $\{1977, 5931\}$ under multiplication mod 7908. But to see what is going on we shall work with $e=25$. We require this to be an idempotent in arithmetic mod n:

$$\begin{aligned} & e^2 \equiv e \pmod{n} \\ \Leftrightarrow\ & e(e-1) \equiv 0 \pmod{n} \\ \Leftrightarrow\ & n \text{ is a factor of } e(e-1) = 25 \times 24 = 600. \end{aligned}$$

For example, taking the factor $n=40$, we get

$$25^2 \equiv 25 \pmod{40}.$$

But, you may ask, where is the group which has 25 for its identity? Now if you were only offered a group with a single element $\{25\}$, you might well feel a sense of anticlimax; so let us see if we can find any larger group with identity 25 within the ring $\mathbb{Z}_{40}$ of residues mod 40.

Any group element, g, must be a multiple, ge, of the group identity $e=25$. Hence the only possible group elements are in the set

$$R = \{0, e, 2e, \ldots, 7e\}$$

of multiples of the idempotent $e \equiv 25 \pmod{40}$. The set R has only 8 elements because $8e \equiv 0 \pmod{40}$. It is no accident that R looks remarkably like $\mathbb{Z}_8$, the ring of integers mod 8. For R and $\mathbb{Z}_8$ turn out to be isomorphic rings with e taking the place of the residue 1 (mod 8) and with (e.g.) the element $3e$ corresponding to the residue 3 (mod 8). (Note how the fact that $e^2 \equiv e$ forces the set R to be closed under multiplication and shows that e is the multiplicative identity of R.)

At this stage we have shown that any group G with identity 25 inside $\mathbb{Z}_{40}$ must be contained in the ring R, i.e. we must have $G \subseteq R$. It does not follow that every element of R necessarily lies in G. Indeed it is clear that the only elements of R which have any chance of lying in G must have multiplicative inverses with respect to the common identity element e of G and R. A pleasant result (which applies to any ring R with identity e) is that we can form a group by taking *all* the elements of R which have inverses. This group,

$$G(R) = \{r \in R : \exists r^{-1} \in R \quad \text{such that} \quad rr^{-1} = r^{-1}r = e\},$$

is called the group of invertible elements of R. It is not hard to verify that $G(R)$ is a group. Readers may care to attempt this as an exercise. In our own particular case,

$$R = \{0, 25, 50, \ldots, 175\} \quad (\text{mod } 40).$$

Picking out the invertible elements, we get

$$G(R) = \{25, 75, 125, 175\} \quad (\text{mod } 40).$$

Reducing mod 40 and rearranging gives

$$G(R) = \{5, 15, 25, 35\} \quad (\text{mod } 40).$$

Since $G(R)$ was formed by taking all the elements of $\mathbb{Z}_{40}$ which have inverses with respect to $e = 25$, any group with this identity inside $\mathbb{Z}_{40}$ must be a subgroup of $G(R)$.

Every group discussed by Brand and Saltmarsh is in fact the group of invertible elements of some ring. For all such groups Saltmarsh's conjecture is true. He claimed that if

$$G = \{e, a, b, \dots\} \pmod{n}$$

is a multiplicative group and k is an integer coprime to n, then

$$H = \{ke, ka, kb, \dots\} \pmod{kn}$$

is a multiplicative group isomorphic to G. We have just met an example of this, for, since the rings $\mathbb{Z}_8$ and R are isomorphic, their groups of invertible elements

$$G(\mathbb{Z}_8) = \{1, 3, 5, 7\} \pmod{8}$$

and

$$G(R) = \{5, 15, 25, 35\} \pmod{40}$$

must also be isomorphic. However, if we take subgroups of these groups, things are not so straightforward. For example, if we take the subgroups

$$G_1 = \{1, 5\} \quad \text{and} \quad G_2 = \{1, 3\} \pmod{8}$$

and put $k = 5$, then the corresponding sets are

$$H_1 = \{5, 25\} \quad \text{and} \quad H_2 = \{5, 15\} \pmod{40}.$$

A quick check shows that H_1 is a group, but H_2 is not. What has gone wrong? Can we repair the damage?

Ideally we would like to have some way of telling in advance whether the set H which Saltmarsh constructed will be a group. Fortunately there is a simple criterion for deciding this, as I have found. In order to describe it and to prove a modified version of Saltmarsh's conjecture, I shall use a notation which distinguishes clearly between an integer such as r and its corresponding residue $\mathbf{r}$ modulo n.

If H is a multiplicative group, then (unlike H_2) it must possess an identity, in particular an idempotent element. Thus there must be an integer m whose residue $\mathbf{m}$ belongs to G such that

$$(km)^2 \equiv km \pmod{kn}.$$

It follows that $(km)^2 - km$ is divisible by kn. Hence $km^2 - m$ is divisible by n, i.e.

$$\mathbf{km}^2 = \mathbf{m}. \tag{4}$$

Since $\mathbf{m} \in G$, there exists a residue $\mathbf{m}^{-1} \in G$ such that

$$\mathbf{mm}^{-1} = \mathbf{e}.$$

Multiplying (4) by $\mathbf{m}^{-2}$ gives

$$\mathbf{ke} = \mathbf{m}^{-1}, \tag{5}$$

which shows that the residue **ke** belongs to G.

Conversely, if $\mathbf{ke} \in G$, then there is a residue $\mathbf{m} \in G$ such that (5) holds. Let $\mathbf{g} \in G$. Multiplying (5) by **mg** gives

$$\mathbf{kmg} = \mathbf{g}. \tag{6}$$

With the natural interpretation of $k\mathbf{mg}$ as an element of H, it is easy to verify that the map $\theta: G \to H$ given by $\mathbf{g} \to k\mathbf{mg}$ is a 1-1 mapping of G onto H and that $\theta(\mathbf{g}_1)\theta(\mathbf{g}_2) = \theta(\mathbf{g}_1\mathbf{g}_2)$ for all $\mathbf{g}_1,\mathbf{g}_2 \in G$. It follows that H is a group isomorphic to G. Further, from (6), the inverse map $\theta^{-1}: H \to G$ is simply reduction mod n, as Saltmarsh stated.

Looking back to the groups G_1 and G_2 with their common identity element $e \equiv 1 \pmod 8$, we have $n = 8$ and $k = 5$ so that $ke \equiv 5 \pmod 8$. This residue belongs to H_1 but not to H_2, which explains why H_1 is a group but H_2 is not a group.

We have seen that if G is a group, then H is a group if and only if $\mathbf{ke} \in G$. But what has happened to Saltmarsh's condition that k should be coprime to n? It seems to have disappeared entirely. However, it turns out that a somewhat less restrictive condition on k can be recovered as Saltmarsh suspected. I shall not provide any further proof but simply assert that if $\mathbf{ke} \in G$, then k is coprime to a certain factor q of n, where q is defined as the least positive integer such that $qe \equiv 0 \pmod n$. A further example will illustrate this point.

Let

$$G = \{6, 12, 18, 24\} \pmod{30}$$

and

$$H = \{18, 36, 54, 72\} \pmod{90}.$$

Then G is a multiplicative group with $e \equiv 6 \pmod{30}$. The modulus $n = 30$, so that $q = 5$. We have $k = 3$, which is coprime to q. Despite the fact that k is not coprime to n, it is easy to check (either directly or because $\mathbf{ke} \in G$) that H is a group isomorphic to G.

Our exploration of groups in modular arithmetic has revealed a fascinating interplay between groups and rings. Group identities led us to idempotents and we saw how to find these elements in a given ring (in our case in $\mathbb{Z}_{12}$). Conversely it is possible to start with a given integer (e.g. $e = 25$) and then to find a ring (e.g. $\mathbb{Z}_{40}$) in which the residue of e is an idempotent. Multiples of this idempotent make up a ring R, whose group of invertible elements we examined. This led to Saltmarsh's conjecture about groups. To conclude this article I would like to return to $\mathbb{Z}_{12}$ to illustrate the strong influence which the idempotents exert on the overall structure of a (commutative) ring. The results are simple to describe, have links with vectors and geometry and offer scope for further investigations in other rings.

We saw earlier that in $\mathbb{Z}_{12}$ there are exactly two pairs of idempotents, viz. the obvious pair 0 and 1 and the potentially more interesting pair $e = 4$ and $f = 9$. We also noted that

$$4+9 \equiv 1 \quad \text{and} \quad 4 \times 9 \equiv 0 \pmod{12}.$$

Another striking property of this latter pair of idempotents is that each element of the ring $\mathbb{Z}_{12}$ can be expressed as a linear combination of e and f. To show the patterns clearly it is worth writing out a full list of elements in this form. (In this list, equality means equality of residues modulo 12.)

$$\begin{array}{lll}
0 = 0e + 0f & 4 = 1e + 0f & 8 = 2e + 0f \\
1 = 1e + 1f & 5 = 2e + 1f & 9 = 0e + 1f \\
2 = 2e + 2f & 6 = 0e + 2f & 10 = 1e + 2f \\
3 = 0e + 3f & 7 = 1e + 3f & 11 = 2e + 3f
\end{array}$$

Moreover, in each of these expressions the coefficients of e and f are unique, provided that we interpret the coefficient of e as an element of $\mathbb{Z}_3$ and the coefficient of f as an element of $\mathbb{Z}_4$. Another feature of the expressions is that if we choose an element such as 11, the coefficients are given by

$$11 \equiv 2 \pmod 3 \quad \text{and} \quad 11 \equiv 3 \pmod 4.$$

It is hard to avoid thinking of the idempotents $e = 4$ and $f = 9$ as unit vectors and the coefficients as coordinates. Who can refrain from trying to sketch the "position" of each element in the ring? Suppose we draw an "e-axis" and an "f-axis" ... (Fig. 1).

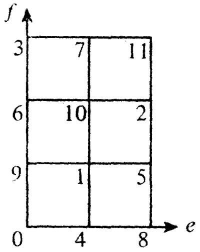

FIGURE 1.

We can even interpret $4 + 9 \equiv 1 \pmod{12}$ vectorially! It is clear that each of the twelve elements of $\mathbb{Z}_{12}$ corresponds to one of the twelve lattice points, and because we have only a finite number of points the picture appears somewhat restricted. If we are prepared to accept a certain amount of ambiguity in the position of each element we can, of course, extend the picture by indefinite repetition to cover the whole plane (Fig. 2).

0	4	8	0	4	8	0	4	8	0	4	8	0
3	7	11	3	7	11	3	7	11	3	7	11	3
6	10	2	6	10	2	6	10	2	6	10	2	6
9	1	5	9	1	5	9	1	5	9	1	5	9
0	4	8	0	4	8	0	4	8	0	4	8	0
3	7	11	3	7	11	3	7	11	3	7	11	3
6	10	2	6	10	2	6	10	2	6	10	2	6
9	1	5	9	1	5	9	1	5	9	1	5	9
0	4	8	0	4	8	0	4	8	0	4	8	0
3	7	11	3	7	11	3	7	11	3	7	11	3
6	10	2	6	10	2	6	10	2	6	10	2	6
9	1	5	9	1	5	9	1	5	9	1	5	9
0	4	8	0	4	8	0	4	8	0	4	8	0

FIGURE 2.

This diagram has several advantages over the previous one. For instance, we can follow right through the sequence 0, 1, 2, 3, 4, ... of elements by moving smoothly along a diagonal instead of jumping around. Additions such as $10+5 \equiv 3 \pmod{12}$ which have no easy vectorial interpretation in the first diagram can now be illustrated in a wide variety of mutually consistent ways. The second diagram also shows that a pattern which repeats itself in cycles of 3 units horizontally and 4 units vertically will repeat in cycles of 12 units along suitably chosen diagonals. This aspect of the diagram illustrates the fact that C_{12}, the cyclic group of order 12, is isomorphic to the direct product $C_3 \times C_4$ of cyclic groups of orders 3 and 4.

Readers who enjoy geometry may prefer a third diagram which appears to combine the advantages of both earlier ones. The great merit of the first diagram is that it shows a 1-1 correspondence between points and ring elements, a feature which is entirely lost in the second figure. Suppose that we try to preserve this 1-1 correspondence. We shall need to glue together all the points labelled 0 in the second diagram, all those labelled 1 and so on. The natural way to do this is first to roll the diagram over and over into a cylinder so that all the copies of the "f-axis" coincide. Then bend the cylinder into a torus and keep pushing it through itself until all the copies of the "e-axis" coincide. (If you think of the cylinder as a snake with a head at one end and a tail at the other, the snake must swallow its tail to form the torus. The tail then slips right down the body of the snake until it reaches the tail position when it is swallowed again . . . and so on.) In the end we get our third diagram, in which a ring is shown as a ring† (Fig. 3)!

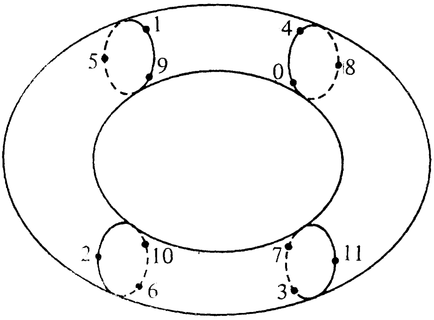

FIGURE 3.

At this stage it seems reasonable to introduce coordinates into the ring $\mathbb{Z}_{12}$ based on coefficients of e and f. For example, since $11 = 2e + 3f$, we shall identify the element 11 with the point (2, 3), where the e-coordinate is taken mod 3 and the f-coordinate is taken mod 4. (Both the second diagram and the torus show how natural it is to regard the first coordinate as an element of $\mathbb{Z}_3$ and the second as an element of $\mathbb{Z}_4$.)

All calculations in $\mathbb{Z}_{12}$ can be done by working with the separate e- and f-coordinates in $\mathbb{Z}_3$ and $\mathbb{Z}_4$ respectively. As we might expect, addition looks very like ordinary vector addition. For example,

$$11 = 2e + 3f = (2, 3),$$
$$5 = 2e + f = (2, 1);$$
$$(2, 3) + (2, 1) = (2 + 2, 3 + 1) = (1, 0)$$

and

$$11 \ + \ 5 \qquad\qquad \equiv \ 4 \quad (\text{mod } 12).$$

More surprisingly, multiplication goes through in the same way. For example,

$$(2, 3) \times (2, 1) = (2 \times 2, 3 \times 1) = (1, 3)$$

and

$$11 \ \times \ 5 \qquad\qquad \equiv \ 7 \quad (\text{mod } 12).$$

† I would be interested to know the origin of the word "ring" in abstract algebra.

A direct evaluation of $(2e+3f)(2e+f)$ shows that the basic facts $e^2=e$, $f^2=f$ and $ef=0$ are responsible for this pleasant behaviour of multiplication.

Just as a large group can be formed from two given smaller ones by constructing their direct product, so it is possible in a similar way to construct what is called the direct sum of two rings. In this direct sum both addition and multiplication are done componentwise. Here we have exhibited the ring $\mathbb{Z}_{12}$ as the direct sum of $\mathbb{Z}_3$ and $\mathbb{Z}_4$. Let us look briefly at the effect which this split in the ring structure has on the corresponding groups of invertible elements.

It is not often realised that our opening lemma can give a quick way of finding inverses. For example, to find the inverse of 7 in $\mathbb{Z}_{12}$ we express 1 as the difference between a multiple of 7 and a multiple of 12:

$$1=7\times 7-4\times 12.$$

Thus

$$1\equiv 7\times 7 \pmod{12},$$

which shows that 7 is its own inverse in $\mathbb{Z}_{12}$. The same answer can be reached by inverting the coordinates (=residues) of 7 in $\mathbb{Z}_3$ and $\mathbb{Z}_4$:

$$7^{-1}=(1,3)^{-1}=(1^{-1},3^{-1})=(1,3)=7.$$

Now let G_n be the group of invertible elements of $\mathbb{Z}_n$. Then

$$G_3=\{1,2\},\quad G_4=\{1,3\},$$

and

$$G_{12}=\{1,5,7,11\}=\{(1,1),(2,1),(1,3),(2,3)\}.$$

This shows that the split in the ring structure of $\mathbb{Z}_{12}$ caused by the idempotents e and f has forced the group G_{12} to decompose into a direct product $G_3\times G_4$.

We have come a long way in our exploration of the interaction between groups and rings. Readers who wish to explore further might care to try the exercises which follow—and, if you are still keen on having 1977 as an identity, there is a group of order 864 in arithmetic modulo 3 906 552 all waiting for you to discover.

Exercises

1. Show that in a field the only idempotents are 0 and 1.
2. In $\mathbb{Z}_{30}$, the ring of integers mod 30, find idempotents e_1, e_2 and e_3 such that $2e_1=3e_2=5e_3=0$ and $e_1+e_2+e_3=1$. If $f_1=e_2+e_3$, $f_2=e_3+e_1$ and $f_3=e_1+e_2$, check that f_1, f_2 and f_3 are also idempotents.
3. Let $R=\{0,m,2m,\ldots,(n-1)m\} \pmod{mn}$. Find conditions which m and n must satisfy in each of the following cases:
   (i) R contains a non-zero idempotent.
   (ii) R contains a (multiplicative) identity element.

(iii) The only idempotents of R are the residues 0 and 1 (mod mn).
(iv) R is a field.

In each case, try to find conditions on m and n which are exactly equivalent to the numbered statement.

4. Let R be the set of all matrices of the form

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix},$$

where a and b are real numbers. Find all the idempotents of R and interpret the equations $e+f=1$ and $ef=0$ in matrix form.

References

1. T. E. Brand, Some surprising identity elements, *Maths Teaching* **64**, 50–52 (September 1973).
2. G. S. Saltmarsh, Identity elements, *Maths Teaching* **79**, 33 (June 1977).
3. H. Davenport, *The higher arithmetic*. Hutchinson (1952).

K. ROBIN MCLEAN

School of Education, 19–23 Abercromby Square, P.O. Box 147,
Liverpool L69 3BX

Constructing a ring without unique factorisation

COLIN R. FLETCHER AND M. LIDSTER

1. Unique factorisation

The study of unique factorisation is almost as old as mathematics itself. The so-called Fundamental Theorem of Arithmetic, which states that every integer greater than 1 can be factorised into a product of primes in only one way, was probably the first major theorem proved. It is interesting to note that Euclid (c. 300 B.C.) did not give the result in this form. He proved (IX 14) that "if a number be the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it" (see [1]).

However, it was not until the advent of abstract algebra, and in particular ring theory, that the subject took up the form in which we know it today. The fundamental concept is that of an *irreducible element*. This by convention is not zero nor a unit (i.e. a divisor of the identity) and is defined by the property that any factorisation of an irreducible can be further factorised to make the irreducible appear among the factors. So in $\mathbb{Z}$, the ring of integers, the units are +1 and −1, and all positive and negative prime numbers are irreducible. Uniqueness is defined up to order and up to multiplication by units. For example, 6 has only the factorisations