and the fibers of φ are the additive cosets $r + I$ of the kernel I (more precisely, if r is any element of R mapping to $a \in S$, $\varphi(r) = a$, then the fiber of φ over a is the coset $r + I$ of the kernel I). These fibers have the structure of a ring naturally isomorphic to the image of φ: if X is the fiber over $a \in S$ and Y is the fiber over $b \in S$, then $X + Y$ is the fiber over $a + b$ and XY is the fiber over ab. In terms of cosets of the kernel I this addition and multiplication is

$$(r + I) + (s + I) = (r + s) + I \tag{7.1}$$

$$(r + I) \times (s + I) = (rs) + I. \tag{7.2}$$

As in the case for groups, the verification that these operations define a ring structure on the collection of cosets of the kernel I ultimately rests on the corresponding ring properties of S. This ring of cosets is called the *quotient ring* of R by $I = \ker \varphi$ and is denoted R/I. Note that the additive structure of the ring R/I is just the additive quotient group of the additive abelian group R by the (necessarily normal) subgroup I. When I is the kernel of some homomorphism φ this additive abelian quotient group also has a multiplicative structure, defined by (7.2), which makes R/I into a ring.

As in the case for groups, we can also consider whether (1) and (2) can be used to define a ring structure on the collection of cosets of an *arbitrary* subgroup I of R. Note that since R is an abelian additive group, the subgroup I is necessarily normal so that the quotient R/I of cosets of I is automatically an additive abelian group. The question then is whether this quotient group also has a *multiplicative* structure induced from the multiplication in R, defined by (2). The answer is no in general (just as the answer is no in trying to form the quotient by an arbitrary subgroup of a group), which leads to the notion of an *ideal* in R (the analogue for rings of a normal subgroup of a group). We shall then see that the ideals of R are exactly the kernels of the ring homomorphisms of R (the analogue for rings of the characterization of normal subgroups as the kernels of group homomorphisms).

Let I be an arbitrary subgroup of the additive group R. We consider when the multiplication of cosets in (2) is well defined and makes the additive abelian group R/I into a ring. The statement that the multiplication in (2) is well defined is the statement that the multiplication is independent of the particular representatives r and s chosen, i.e., that we obtain the same coset on the right if instead we use the representatives $r + \alpha$ and $s + \beta$ for any $\alpha, \beta \in I$. In other words, we must have

$$(r + \alpha)(s + \beta) + I = rs + I \tag{$*$}$$

for all $r, s \in R$ and all $\alpha, \beta \in I$.

Letting $r = s = 0$, we see that I must be closed under multiplication, i.e., I must be a *subring* of R.

Next, by letting $s = 0$ and letting r be arbitrary, we see that we must have $r\beta \in I$ for every $r \in R$ and every $\beta \in I$, i.e., that I must be closed under multiplication on the left by elements from R. Letting $r = 0$ and letting s be arbitrary, we see similarly that I must be closed under multiplication on the right by elements from R.

Conversely, if I is closed under multiplication on the left and on the right by elements from R then the relation $(*)$ is satisfied for all $\alpha, \beta \in I$. Hence this is a necessary and sufficient condition for the multiplication in (2) to be well defined.

Finally, if the multiplication of cosets defined by (2) is well defined, then this multiplication makes the additive quotient group R/I into a ring. Each ring axiom in the quotient follows directly from the corresponding axiom in R. For example, one of the distributive laws is verified as follows:

$$\begin{aligned}(r+I)[(s+I)+(t+I)] &= (r+I)[(s+t)+I]\\ &= r(s+t)+I = (rs+rt)+I\\ &= (rs+I)+(rt+I)\\ &= [(r+I)(s+I)]+[(r+I)(t+I)].\end{aligned}$$

This shows that the quotient R/I of the ring R by a subgroup I has a natural ring structure if and only if I is also closed under multiplication on the left and on the right by elements from R (so in particular must be a subring of R since it is closed under multiplication). As mentioned, such subrings I are called the *ideals* of R:

Definition. Let R be a ring, let I be a subset of R and let $r \in R$.

(1) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

(2) A subset I of R is a *left ideal* of R if

- **(i)** I is a subring of R, and
- **(ii)** I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.

Similarly I is a *right ideal* if (i) holds and in place of (ii) one has

- **(ii)′** I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$ for all $r \in R$.

(3) A subset I that is both a left ideal and a right ideal is called an *ideal* (or, for added emphasis, a *two-sided ideal*) of R.

For commutative rings the notions of left, right and two-sided ideal coincide. We emphasize that to prove a subset I of a ring R is an ideal it is necessary to prove that I is nonempty, closed under subtraction and closed under multiplication by all the elements of R (and not just by elements of I). If R has a 1 then $(-1)a = -a$ so in this case I is an ideal if it is nonempty, closed under addition and closed under multiplication by all the elements of R.

Note also that the last part of Proposition 5 proves that the kernel of any ring homomorphism is an ideal.

We summarize the preceding discussion in the following proposition.

Proposition 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I) = (r+s)+I \qquad \text{and} \qquad (r+I)\times(s+I) = (rs)+I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition. When I is an ideal of R the ring R/I with the operations in the previous proposition is called the *quotient ring* of R by I.

Theorem 7.

(1) *(The First Isomorphism Theorem for Rings)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map

$$R \to R/I \qquad \text{defined by} \qquad r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this homomorphism is called the *natural projection* of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

Proof: This is just a matter of collecting previous calculations. If I is the kernel of φ, then the cosets (under addition) of I are precisely the fibers of φ. In particular, the cosets $r+I$, $s+I$ and $rs+I$ are the fibers of φ over $\varphi(r)$, $\varphi(s)$ and $\varphi(rs)$, respectively. Since φ is a ring homomorphism $\varphi(r)\varphi(s) = \varphi(rs)$, hence $(r + I)(s + I) = rs + I$. Multiplication of cosets is well defined and so I is an ideal and R/I is a ring. The correspondence $r + I \mapsto \varphi(r)$ is a bijection between the rings R/I and $\varphi(R)$ which respects addition and multiplication, hence is a ring isomorphism.

If I is any ideal, then R/I is a ring (in particular is an abelian group) and the map $\pi : r \mapsto r + I$ is a group homomorphism with kernel I. It remains to check that π is a ring homomorphism. This is immediate from the definition of multiplication in R/I:

$$\pi : rs \mapsto rs + I = (r + I)(s + I) = \pi(r)\pi(s).$$

As with groups we shall often use the bar notation for reduction mod I: $\overline{r} = r + I$. With this notation the addition and multiplication in the quotient ring R/I become simply $\overline{r} + \overline{s} = \overline{r + s}$ and $\overline{r}\,\overline{s} = \overline{rs}$.

Examples

Let R be a ring.

(1) The subrings R and $\{0\}$ are ideals. An ideal I is *proper* if $I \neq R$. The ideal $\{0\}$ is called the *trivial ideal* and is denoted by 0.

(2) It is immediate that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any $n \in \mathbb{Z}$ and these are the only ideals of $\mathbb{Z}$ since in particular these are the only subgroups of $\mathbb{Z}$. The associated quotient ring is $\mathbb{Z}/n\mathbb{Z}$ (which explains the choice of notation and which we have now proved is a ring), introduced in Chapter 0. For example, if $n = 15$ then the elements of $\mathbb{Z}/15\mathbb{Z}$ are the cosets $\overline{0}, \overline{1}, \dots, \overline{13}, \overline{14}$. To add (or multiply) in the quotient, simply choose any representatives for the two cosets, add (multiply, respectively) these representatives in the integers $\mathbb{Z}$, and take the corresponding coset containing this sum (product, respectively). For example, $\overline{7} + \overline{11} = \overline{18}$ and $\overline{18} = \overline{3}$, so $\overline{7} + \overline{11} = \overline{3}$ in $\mathbb{Z}/15\mathbb{Z}$. Similarly, $\overline{7}\,\overline{11} = \overline{77} = \overline{2}$ in $\mathbb{Z}/15\mathbb{Z}$. We could also express this by writing $7 + 11 \equiv 3 \bmod 15$, $7(11) \equiv 2 \bmod 15$.

The natural projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is called *reduction mod n* and will be discussed further at the end of these examples.