Looking at the second line of the above computation, we can see that what was needed to verify $a'b' \in ab + n\mathbb{Z}$ is that $n(kb + knr) + anr \in n\mathbb{Z}$. The key to make this computation work is that when an element of $\mathbb{Z}$ is multiplied by an element of $n\mathbb{Z}$, the product is in $n\mathbb{Z}$. This observation is the reason for the following definition.

30.2 Definition An additive subgroup N of the ring R is an **ideal** if

$$aN = \{an \mid n \in N\} \subseteq N \quad \text{and} \quad Na = \{na \mid n \in N\} \subseteq N \quad \text{for all } a \in R. \qquad ■$$

30.3 Example We see that $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$ since we know it is a subring, and $s(nm) = (nm)s = n(ms) \in n\mathbb{Z}$ for all $s \in \mathbb{Z}$. ▲

30.4 Example Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let C be the subring of F consisting of all the constant functions in F. Is C an ideal in F? Why?

Solution It is not true that the product of a constant function with every function is again a constant function. For example, the product of $\sin x$ and 2 is the function $2 \sin x$. Thus C is not an ideal of F. ▲

■ Historical Note

It was Ernst Eduard Kummer (1810–1893) who introduced the concept of an "ideal complex number" in 1847 in order to preserve the notion of unique factorization in certain rings of algebraic integers. In particular, Kummer wanted to be able to factor into primes numbers of the form $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1}$, where α is a complex root of $x^p = 1$ (p prime) and the a_i are ordinary integers. Kummer had noticed that the naive definition of primes as "unfactorable numbers" does not lead to the expected results; the product of two such "unfactorable" numbers may well be divisible by other "unfactorable" numbers. Kummer defined "ideal prime factors" and "ideal numbers" in terms of certain congruence relationships; these "ideal factors" were then used as the divisors necessary to preserve unique factorization. By use of these, Kummer was in fact able to prove certain cases of Fermat's Last Theorem, which states that $x^n + y^n = z^n$ has no solutions $x, y, z \in \mathbb{Z}^+$ if $n > 2$.

It turned out that an "ideal number," which was in general not a "number" at all, was uniquely determined by the set of integers it "divided." Richard Dedekind took advantage of this fact to identify the ideal factor with this set; he therefore called the set itself an ideal, and proceeded to show that it satisfied the definition given in the text. Dedekind was then able to define the notions of prime ideal and product of two ideals and show that any ideal in the ring of integers of any algebraic number field could be written uniquely as a product of prime ideals.

30.5 Example Let F be as in the preceding example, and let N be the subring of all functions f such that $f(2) = 0$. Is N an ideal in F? Why or why not?

Solution Let $f \in N$ and let $g \in F$. Then $(fg)(2) = f(2)g(2) = 0g(2) = 0$, so $fg \in N$. Similarly, we find that $gf \in N$. Therefore N is an ideal of F. ▲

30.6 Theorem **(Analogue of Theorem 12.7)** Let H be an additive subgroup of the ring R. Multiplication of additive cosets of H is well defined by the equation

$$(a + H)(b + H) = ab + H$$

if and only if H is an ideal in R.

Proof Suppose first that H is an ideal in R. Let $a, b \in R$, $a' \in a + H$, and $b' \in b + H$. There are elements $h_1, h_2 \in H$ with $a' = a + h_1$ and $b' = b + h_2$. We have

$$\begin{aligned} a'b' &= (a + h_1)(b + h_2) \\ &= ab + ah_2 + h_1 b + h_1 h_2 \\ &\in ab + H \qquad \text{since } H \text{ is an ideal.} \end{aligned}$$

We now suppose that $(a + H)(b + H) = ab + H$ defines a binary operation on cosets of H in R. We let $a \in R$ and $h \in H$ with the goal of showing that $aH \subseteq H$ and $Ha \subseteq H$. Since $h + H = 0 + H$,

$$H = 0a + H = (0 + H)(a + H) = (h + H)(a + H) = ha + H.$$

This shows $ha \in H$, which implies $Ha \subseteq H$. Similarly,

$$H = a0 + H = (a + H)(0 + H) = (a + H)(h + H) = ah + H.$$

This shows $ah \in H$ and therefore $aH \subseteq H$. Thus H is an ideal in R. ◆

Once we know that multiplication by choosing representatives is well defined on additive cosets of a subring N of R, the associative law for multiplication and the distributive laws for these cosets follow immediately from the same properties in R. We have at once this corollary of Theorem 30.6.

30.7 Corollary **(Analogue of Corollary 12.8)** Let N be an ideal of a ring R. Then the additive cosets of N form a ring R/N with the binary operations defined by

$$(a + N) + (b + N) = (a + b) + N$$

and

$$(a + N)(b + N) = ab + N.$$

♦

30.8 Definition The ring R/N in the preceding corollary is the **factor ring** (or **quotient ring**) **of** R **by** N. ■

If we use the term *quotient ring*, be sure not to confuse it with the notion of the *field of quotients* of an integral domain, discussed in Section 26.

Homomorphisms

We defined the concepts of *homomorphism* and *isomorphism* for rings in Section 22, since we wished to talk about evaluation homomorphisms for polynomials and about isomorphic rings. We repeat some definitions here for easy reference. Recall that a homomorphism is a *structure-relating map*. A homomorphism for rings must relate both their additive structure and their multiplicative structure.

30.9 Definition A map ϕ of a ring R into a ring R' is a **homomorphism** if

$$\phi(a + b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a)\phi(b)$$

for all elements a and b in R. ■

In Example 22.10 we defined evaluation homomorphisms, and Example 22.11 showed that the map $\phi : \mathbb{Z} \to \mathbb{Z}_n$, where $\phi(m)$ is the remainder of m when divided by n, is a homomorphism. We give another simple but very fundamental example of a homomorphism.

30.10 Example **(Projection Homomorphisms)** Let $R_1, R_2, \cdots, R_n$ be rings. For each i, the map $\pi_i : R_1 \times R_2 \times \cdots \times R_n \to R_i$ defined by $\pi_i(r_1, r_2, \cdots, r_n) = r_i$ is a homomorphism, *projection onto the ith component*. The two required properties of a homomorphism hold for π_i since both addition and multiplication in the direct product are computed by addition and multiplication in each individual component. ▲

Properties of Homomorphisms

We continue to parallel our development of ring homomorphisms and factor rings with the analogous material for group homomorphisms and factor groups.

30.11 Theorem Let $\phi : R \to R'$ be a ring homomorphism.

1. If 0 is the additive identity in R, then $\phi(0) = 0'$ is the additive identity in R'.
2. If $a \in R$, then $\phi(-a) = -\phi(a)$.
3. If S is a subring of R, then $\phi[S]$ is a subring of R'.
4. If S' is a subring of R', then $\phi^{-1}[S']$ is a subring of R.
5. If R has unity 1, then $\phi(1)$ is unity for $\phi[R]$.
6. If N is an ideal in R, then $\phi[N]$ is an ideal in $\phi[R]$.
7. If N' is an ideal in either R' or $\phi[R]$, then $\phi^{-1}[N']$ is an ideal in R.

Proof Let ϕ be a homomorphism of a ring R into a ring R'. Since, in particular, ϕ can be viewed as a group homomorphism of $\langle R, +\rangle$ into $\langle R', +'\rangle$, Theorem 8.5 tells us that $\phi(0) = 0'$ is the additive identity element of R' and that $\phi(-a) = -\phi(a)$.

Theorem 8.5 also tells us that if S is a subring of R, then, considering the additive group $\langle S, +\rangle$, the set $\langle \phi[S], +'\rangle$ gives a subgroup of $\langle R', +'\rangle$. If $\phi(s_1)$ and $\phi(s_2)$ are two elements of $\phi[S]$, then

$$\phi(s_1)\phi(s_2) = \phi(s_1 s_2)$$

and $\phi(s_1 s_2) \in \phi[S]$. Thus $\phi(s_1)\phi(s_2) \in \phi[S]$, so $\phi[S]$ is closed under multiplication. Consequently, $\phi[S]$ is a subring of R'.

Going the other way, Theorem 8.5 also shows that if S' is a subring of R', then $\langle \phi^{-1}[S'], +\rangle$ is a subgroup of $\langle R, +\rangle$. Let $a, b \in \phi^{-1}[S']$, so that $\phi(a) \in S'$ and $\phi(b) \in S'$. Then

$$\phi(ab) = \phi(a)\phi(b).$$

Since $\phi(a)\phi(b) \in S'$, we see that $ab \in \phi^{-1}[S']$, so $\phi^{-1}[S']$ is closed under multiplication and thus is a subring of R.

If R has unity 1, then for all $r \in R$,

$$\phi(r) = \phi(1r) = \phi(r1) = \phi(1)\phi(r) = \phi(r)\phi(1),$$

so $\phi(1)$ is unity for $\phi[R]$.

The proof of the remainder of the theorem is Exercise 22. ◆

Note in Theorem 30.11 that $\phi(1)$ is unity for $\phi[R]$, but not necessarily for R' as we ask you to illustrate in Exercise 9. Furthermore, although $\phi[N]$ is an ideal in $\phi[R]$, it may not be an ideal in R' as verified in Exercise 22.