22. Let S be a set, X a subset, and assume neither S nor X is empty. Let R be a ring. Let $F(S, R)$ be the ring of all mappings of S into R, and let

$$\rho: F(S, R) \to F(X, R)$$

be the restriction, i.e. if $f \in F(S, R)$, then $\rho(f)$ is just f viewed as a map of X into R. Show that ρ is surjective. Describe the kernel of ρ.

23. Let K be a field and S a set. Let x_0 be an element of S. Let $F(S, K)$ be the ring of mappings of S into K, and let J be the set of maps $f \in F(S, K)$ such that $f(x_0) = 0$. Show that J is a maximal ideal. Show that $F(S, K)/J$ is isomorphic to K.

24. Let R be a commutative ring. A map $D: R \to R$ is called a **derivation** if $D(x + y) = Dx + Dy$, and $D(xy) = (Dx)y + x(Dy)$ for all $x, y \in R$. If D_1, D_2 are derivations, define the bracket product

$$[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1.$$

Show that $[D_1, D_2]$ is a derivation.

Example. Let R be the ring of infinitely differentiable real-valued functions of, say, two real variables. Any differential operator

$$f(x, y)\frac{\partial}{\partial x} \quad \text{or} \quad g(x, y)\frac{\partial}{\partial y}$$

with coefficients f, g which are infinitely differentiable functions, is a derivation on R.

III, §4. QUOTIENT FIELDS

In the preceding sections, we have assumed that the reader is acquainted with the rational numbers, in order to give examples for more abstract concepts. We shall now study how one can define the rationals from the integers. Furthermore, in the next chapter, we shall study polynomials over a field. One is accustomed to form quotients f/g $(g \neq 0)$ of polynomials, and such quotients are called rational functions. Our discussion will apply to this situation also.

Before giving the abstract discussion, we analyze the case of the rational numbers more closely. In elementary school, what is done (or what should be done), is to give rules for determining when two quotients of rational numbers are equal. This is needed, because, for instance, $\frac{3}{4} = \frac{6}{8}$. The point is that a fraction is determined by a pair of numbers, in this special example $(3, 4)$, but also by other pairs, e.g. $(6, 8)$.

we get our cue how to define the fraction, namely as a certain equivalence class of pairs. Next, one must give rules for adding fractions, and the rules we shall give in general are precisely the same as those which are (or should be) given in elementary school.

Our discussion will apply to an arbitrary integral ring R. (Recall that integral means that $1 \neq 0$, that R is commutative and without divisors of 0.)

Let (a, b) and (c, d) be pairs of elements in R, with $b \neq 0$ and $d \neq 0$. We shall say that these pairs are **equivalent** if $ad = bc$. We contend that this is an equivalence relation. Going back to the definition of Chapter I, §5, we see that **ER 1** and **ER 3** are obvious. As for **ER 2**, suppose that (a, b) is equivalent to (c, d) and (c, d) is equivalent to (e, f). By definition,

$$ad = bc \quad \text{and} \quad cf = de.$$

Multiplying the first equality by f and the second by b, we obtain

$$adf = bcf \quad \text{and} \quad bcf = bde,$$

whence $adf = bde$, and $daf - dbe = 0$. Then $d(af - be) = 0$. Since R has no divisors of 0, it follows that $af - be = 0$, i.e. $af = be$. This means that (a, b) is equivalent to (e, f), and proves **ER 2**.

We denote the equivalence class of (a, b) by a/b. We must now define how to add and multiply such classes.

If a/b and c/d are such classes, we define their sum to be

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

and their product to be

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

We must show of course that in defining the sum and product as above, the result is independent of the choice of pairs (a, b) and (c, d) representing the given classes. We shall do this for the sum. Suppose that

$$a/b = a'/b' \quad \text{and} \quad c/d = c'/d'.$$

We must show that

$$ad + bc \qquad a'd' + b'c'$$

This is true if and only if

$$b'd'(ad + bc) = bd(a'd' + b'c'),$$

or in other words

$$(1) \qquad b'd'ad + b'd'bc = bda'd' + bdb'c'.$$

But $ab' = a'b$ and $cd' = c'd$ by assumption. Using this, we see at once that (1) holds. We leave the analogous statement for the product as an exercise.

We now contend that the set of all quotients a/b with $b \neq 0$ is a ring, the operations of addition and multiplication being defined as above. Note first that there is a unit element, namely 1/1, where 1 is the unit element of R. One must now verify all the other axioms of a ring. This is tedious, but obvious at each step. As an example, we shall prove the associativity of addition. For three quotients a/b, c/d, and e/f we have

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{fad + fbc + bde}{bdf}.$$

On the other hand,

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf}.$$

It is then clear that the expressions on the right-hand sides of these equations are equal, thereby proving associativity of addition. The other axioms are equally easy to prove, and we shall omit this tedious routine. We note that our ring of quotients is commutative.

Let us denote the ring of all quotients a/b by K. We contend that K is a field. To see this, all we need to do is prove that every non-zero element has a multiplicative inverse. But the zero element of K is 0/1, and if $a/b = 0/1$ then $a = 0$. Hence any non-zero element can be written in the form a/b with $b \neq 0$ and $a \neq 0$. Its inverse is then b/a, as one sees directly from the definition of multiplication of quotients.

Finally, observe that we have a natural map of R into K, namely the map

$$a \mapsto a/1.$$

It is again routine to verify that this map is an injective ring-homomorphism. Any injective ring-homomorphism will be called an **embedding.** We see that R is embedded in K in a natural way.

We call K the **quotient field of** R. When $R = \mathbf{Z}$, then K is by definition the field of rational numbers. When R is the ring of polynomials

defined in the next chapter, its quotient field is called the field of **rational functions.**

Suppose that R is a subring of a field F. The set of all elements ab^{-1} with $a, b \in R$ and $b \neq 0$ is easily seen to form a field, which is a subfield of F. We also call this field the quotient field of R in F. There can be no confusion with this terminology, because the quotient field of R as defined previously is isomorphic to this subfield, under the map

$$a/b \mapsto ab^{-1}.$$

The verification is trivial, and in view of this, the element ab^{-1} of F is also denoted by a/b.

Example. Let K be a field and as usual, $\mathbf{Q}$ the rational numbers. There does not necessarily exist an embedding of $\mathbf{Q}$ into K (for instance, K may be finite). However, if an embedding of $\mathbf{Q}$ into K exists, there is only one. This is easily seen, because any homomorphism

$$f: \mathbf{Q} \to K$$

must be such that $f(1) = e$ (unit element of K). Then for any integer $n > 0$ one sees by induction that $f(n) = ne$, and consequently

$$f(-n) = -ne.$$

Furthermore,

$$e = f(1) = f(nn^{-1}) = f(n)f(n^{-1})$$

so that $f(n^{-1}) = f(n)^{-1} = (ne)^{-1}$. Thus for any quotient $m/n = mn^{-1}$ with integers m, n and $n > 0$ we must have

$$f(m/n) = (me)(ne)^{-1}.$$

thus showing that f is uniquely determined. It is then customary to identify $\mathbf{Q}$ inside K and view every rational number as an element of K.

Finally, we make some remarks on the extension of an embedding of a ring into a field.

Let R be an integral ring, and

$$f: R \to E$$

an embedding of R into some field E. Let K be the quotient field of R. Then f admits a unique extension to an embedding of K into E, that is

To see the uniqueness, observe that if f^* is an extension of f, and

$$f^*: K \to E$$

is an embedding, then for all $a, b \in R$ we must have

$$f^*(a/b) = f^*(a)/f^*(b) = f(a)/f(b),$$

so the effect of f^* on K is determined by the effect of f on R. Conversely, one can *define* f^* by the formula

$$f^*(a/b) = f(a)/f(b),$$

and it is seen at once that the value of f^* is independent of the choice of the representation of the quotient a/b, that is if $a/b = c/d$ with

$$a, b, c, d \in R \qquad \text{and} \qquad bd \neq 0,$$

then

$$f(a)/f(b) = f(c)/f(d).$$

One also verifies routinely that f^* so defined is a homomorphism, thereby proving the existence.

III, §4. EXERCISES

1. Put in all details in the proof of the existence of the extension f^* at the end of this section.

2. A (ring-) isomorphism of a ring onto itself is also called an **automorphism**. Let R be an integral ring, and $\sigma: R \to R$ an automorphism of R. Show that σ admits a unique extension to an automorphism of the quotient field.