

§30

Subrings, Ideals and Homomorphisms

As in the case of groups, we give a name to subsets of a ring which are themselves rings.

30.1 Definition: Let R be a ring. A nonempty subset S of R is called a *subring* of R if S itself is a ring with respect to the operations on R .

Thus a nonempty subset S of a ring R is a subring of R if and only if S satisfies all the ring axioms in Definition 29.1. As in the case of groups, we can dispense with some of them.

Let $(R,+,·)$ be a ring and $\emptyset \neq S \subseteq R$. If S is a subring of R , then $(S,+)$ is a commutative group, thus $(S,+)$ is a subgroup of $(R,+)$; and $(S,+)$ is a subgroup of $(R,+)$ if and only if

- (i) $a + b \in S$ for all $a, b \in S$,
- (ii) $-a \in S$ for all $a \in S$,

as we know from Lemma 9.2. Let us now consider multiplication. If $(S,+,·)$ is to be a ring, the restriction of the operation \cdot to S must be a binary operation on S ; and this holds if and only if

- (1) $a \cdot b \in S$ for all $a \in S$.

So, if a nonempty subset S of a ring R is a subring of R , then (i),(ii),(1) hold. Conversely, if S is a nonempty subset of a ring R and (i),(ii),(1) hold, then $(S,+)$ is a subgroup of $(R,+)$, so $(S,+)$ is a commutative group, and \cdot is a binary operation on S , and the associativity of multiplication and the distributivity of multiplication over addition holds in S since they hold in fact in R . Thus $(S,+,·)$ is a subring of $(R,+,·)$. We proved the following lemma.

30.2 Lemma (Subring criterion): Let $(R,+,·)$ be a ring and let S be a nonempty subset of R . Then $(S,+,·)$ is a subring of R if and only if

- (i) $a + b \in S$ for all $a, b \in S$,

- (ii) $-a \in S$ for all $a \in S$,
 (iii) $a \cdot b \in S$ for all $a, b \in S$. □

30.2' Examples: (a) $\{0\}$ and R are subrings of any ring R .

(b) If R is a ring and S_i is an arbitrary collection of subrings of R , then it follows immediately from Lemma 30.2 that $\bigcap_{i \in I} S_i$ is a subring of R .

(c) If R is a ring and X is a subset of R , the intersection of all subrings of R that contain X is a subring of R by Example 30.2'(b). It is called the *subring generated by X* .

Some properties of multiplication are inherited by subrings.

30.3 Lemma: (1) A subring of a commutative ring is a commutative ring.

(2) A subring of a noncommutative ring can be commutative.

(3) A subring of a ring with identity can be a ring without identity.

(4) A subring of a ring without identity can be a ring with identity.

(5) A subring of a ring without zero divisors is a ring without zero divisors.

(6) A subring of a ring with zero divisors can be a ring without zero divisors.

(7) A subring of a division ring is not necessarily a division ring.

(8) A subring of a field is not necessarily a field.

(9) A subring, distinct from $\{0\}$, of an integral domain is an integral domain if and only if it contains the identity.

Proof: Let R be a ring and S a subring of R .

(1) If R is commutative, then $ab = ba$ for all $a, b \in R$ and, a fortiori, $ab = ba$ for all $a, b \in S$. Hence S is commutative.

(2) Assume R is not commutative. Then there are $a, b \in R$ with $ab \neq ba$. The point is that all such pairs a, b may be outside S , and that $st = ts$ may

hold for all $s, t \in S$. For example, $R = \text{Mat}_2(\mathbb{Q})$ is not commutative, but $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q} \right\}$ is a subring of R and S is commutative.

(3) The point is that the identity 1 of R need not belong to S . For example, \mathbb{Z} is a ring with identity, $2\mathbb{Z}$ is a subring of \mathbb{Z} and $2\mathbb{Z}$ has no identity.

(4) The point is that there may be an e in S such that $es = se = s$ for all s in S , but $er = re = r$ need not be true for all $r \in R$, i.e., $er_0 \neq r_0$ or $r_0e \neq r_0$ for a particular r_0 in R . As an example, consider $R = \mathbb{Z} \times \mathbb{Z}$, on which addition and multiplication are defined by declaring

$$\begin{aligned} (a,b) + (c,d) &= (a+c, a+d) \\ (a,b)(c,d) &= (ac, ad) \end{aligned}$$

for all $(a,b) \in R$ and which is easily verified to be a ring with respect to these operations. If $(a,b) \in R$ is a left identity element of R so that $(a,b)(x,y) = (x,y)$ for all $(x,y) \in R$, then $(ax, ay) = (x,y)$ for all $(x,y) \in R$, thus $a = 1$. But $(1,b)$ is not a right identity element of R , because $(x,y)(1,b) = (x,xb) \neq (x,y)$ for any $(x,y) \in R$ with $y \neq xb$. Thus R is a ring without an identity. However, $S = \{(a,0) : a \in \mathbb{Z}\}$ is a subring of R with an identity $(1,0) \in S$, as $(1,0)(a,0) = (a,0) = (a,0)(1,0)$ for any $(a,0) \in S$.

(5) If R has no zero divisors, then

$$\text{for all } a, b \in R, \quad a \neq 0 \neq b \implies ab \neq 0.$$

But this holds for all $a, b \in S$, too. Hence S has no zero divisors.

(6) If R has no zero divisors, it may happen that all zero divisors fall outside S , and in this case S has no zero divisors. For instance, The ring $R = \text{Mat}_2(\mathbb{Q})$ has zero divisors, but its subset $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Q} \right\}$ is a subring of R with no zero divisors. For if $s, t \in S$ and $st = 0$, then $s = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ and $t = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ for some $a, b \in \mathbb{Q}$, and $st = 0$ means $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, which is possible only if $a = 0$ or $b = 0$ (in \mathbb{Q}), that is, only if $s = 0$ or $t = 0$ (in S).

(7) and (8) Consider the division ring \mathbb{Q} , which is a field as well. Its subring \mathbb{Z} is neither a division ring nor a field.

(9) A subring $S \neq \{0\}$ of an integral domain R is commutative by (1) and has no zero divisors by (5). Hence S is an integral domain if and only if S has an identity. We claim S has an identity if and only if the identity of R belongs to S . Indeed, if S contains the identity element 1_R of R , then of course 1_R is an identity element of S . Conversely, if S has an identity element e , then $ee = e = 1_R e$, so $ee - 1_R e = 0$, so $(e - 1_R)e = 0$ and, since $e \neq 0$ (for $S \neq \{0\}$ by assumption) and R has no zero divisors, $e - 1_R = 0$ and hence e must be equal to 1_R . \square

The claim in the proof of Lemma 30.3(9) is not self-evident. If R is a ring with identity and S is a subring of R , then it is possible that S is a ring with identity and the identity of S is *distinct* from the identity of R . Can you give some examples?

Just as in the case of groups, we want to define factor rings by subrings. We take our factor group construction as a model. For a group G and a subgroup H of G , the factor group G/H is the set of all right cosets of H in G , on which the multiplication is defined by the rule $Ha \cdot Hb = Hab$. In order that this multiplication be well defined, it is necessary and sufficient that H be normal in G (Theorem 18.4).

Now let R be a ring and S a subring of R . Then R is an abelian group with respect to addition and S is a subgroup of R . Using our results in group theory, we build the factor group R/S . This is possible because S is a normal subgroup of R (any subgroup of an abelian group is normal in that group). The elements of R/S are the (right or left) cosets $r + S$, where r ranges over R . Of course we must write the cosets as $r + S$ or as $S + r$, not as rS or as Sr , for the group R is an additive group. We now wish to define a multiplication on R/S and make R/S into a ring.

The most natural way to define a multiplication on R/S is to put

$$(r + S)(u + S) = ru + S \quad \text{for all } r, u \in R.$$

Let us see if this multiplication is well defined. Once we show that this multiplication is well defined, it is routine to prove that R/S becomes a ring with this multiplication. This multiplication is well defined if and only if the implication

$$r_1 + S = r_2 + S, \quad t_1 + S = t_2 + S \quad \Rightarrow \quad r_1 t_1 + S = r_2 t_2 + S \quad (\text{for all } r_1, r_2, t_1, t_2 \in R)$$

holds, and it holds if and only if

$$r_1 = r_2 + s_1, t_1 = t_2 + s_2, s_1, s_2 \in S \implies r_1 t_1 - r_2 t_2 \in S \quad (\text{for all } r_1, r_2, t_1, t_2 \in R),$$

i.e., if and only if

$$s_1, s_2 \in S \implies (r_2 + s_1)(t_2 + s_2) - r_2 t_2 \in S \quad (\text{for all } r_2, t_2 \in R),$$

i.e., if and only if

$$s_1, s_2 \in S \implies r_2 s_2 + s_1 t_2 + s_1 s_2 \in S \quad (\text{for all } r_2, t_2 \in R),$$

that is, since $s_1 s_2 \in S$ when $s_1, s_2 \in S$, if and only if

$$s_1, s_2 \in S \implies r s_2 + s_1 t \in S \quad (\text{for all } r, t \in R) \quad (*)$$

is true. We dropped the subscripts of r_2 and t_2 .

Assume (*) holds. Then, choosing $t = 0$, we see $r s_2 \in S$ whenever $r \in R$, $s_2 \in S$; and choosing $r = 0$, we see $s_1 t \in S$ whenever $s_1 \in S$, $t \in R$. Conversely, if $r s_2 \in S$ and $s_1 t \in S$ whenever $r \in R$, $s_2 \in S$ and $s_1 \in S$, $t \in R$, then $r s_2 + s_1 t \in S$ for all $r, t \in R$, $s_2, s_1 \in S$, since S is a subgroup of R with respect to addition. Thus (*) is equivalent to, and the multiplication on R/S is well defined if and only if:

$$\text{for all } s \in S, r \in R, \text{ there hold } r s \in S \text{ and } s r \in S. \quad (**)$$

Subrings with this property have a name.

30.4 Definition: A nonempty subset S of a ring R is called an *ideal of R* if the following two conditions are satisfied.

- (i) S is a subgroup of R under addition.
- (ii) For all $s \in S$, $r \in R$, we have $r s \in S$ and $s r \in S$.

According to this definition, an ideal of a ring R is a subring of R , since it is closed under multiplication by (ii). The condition (ii) tells more than simply that the product of an element in S by an element in S is in S . It tells that the product of any element in R by any element in S , as well as the product of any element in S by an element in R , are both in S . Thus S "swallows" or "absorbs" products by elements in R .

The condition (ii) consists of two subconditions: $r s \in S$ and $s r \in S$. In a commutative ring, these subconditions are identical. But when R is not commutative, neither of them implies the other in general, and one of them is not enough to make S an ideal: both of them ought to hold.

Definition 30.4 and the discussion preceding it give us the following theorem (cf. Theorem 18.4).

30.5 Theorem: Let R be a ring and S a subgroup of R under addition. The multiplication on the set R/S of right (and left) cosets of S , given by

$$(r + S)(u + S) = ru + S \quad \text{for all } r, u \in R.$$

is well defined if and only if S is an ideal of R . □

After giving some examples of ideals, we will prove that the multiplication on R/S makes R/S into a ring.

30.6 Examples: (a) In any ring R , the set $\{0\}$ is an ideal (Lemma 29.6(1) and (2)). The set R itself is also an ideal of R since R is closed under multiplication.

(b) In the ring \mathbb{Z} of integers, $2\mathbb{Z}$ is a subring and in fact an ideal of \mathbb{Z} , since the product of an even integer by an arbitrary integer is always an even integer. In the same way, the set $n\mathbb{Z}$ is an ideal of \mathbb{Z} ($n \in \mathbb{N}$).

(c) Let K be the ring of real-valued functions on $[0,1]$ (Example 29.2(i)). Its subset $\{f \in K: f(1/2) = 0\}$ is an ideal of K . Similarly, when Y is a subset of $[0,1]$, the subset $\{f \in K: f(y) = 0 \text{ for all } y \in Y\}$ is an ideal of K .

(d) Let $T = \{a/b \in \mathbb{Q}: (a,b) = 1, p \nmid b\}$ be the ring in Example 29.2(g). Then its subsets

$A = \{a/b \in \mathbb{Q}: (a,b) = 1, p \nmid b, p \mid a\}$ and $\{a/b \in \mathbb{Q}: (a,b) = 1, p \nmid b, p^2 \mid a\}$ are ideals of T .

(e) \mathbb{Z} is not an ideal of \mathbb{Q} , since for example, $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, but $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.

(f) Consider the subset $S = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Q} \right\}$ of $Mat_2(\mathbb{Q})$. Then S is a subring of $Mat_2(\mathbb{Q})$. Also, one sees easily that $rs \in S$ for all $r \in Mat_2(\mathbb{Q})$, $s \in S$. Nevertheless, S is not an ideal of $Mat_2(\mathbb{Q})$, since it is not true that $sr \in S$ for all $r \in Mat_2(\mathbb{Q})$, $s \in S$: for example $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in S$, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in Mat_2(\mathbb{Q})$, but $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin S$.

Now let $S_1 = \left\{ \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} : c \in \mathbb{Q} \right\}$ and $S_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q} \right\}$. It is easy to see that S_1 and S_2 are subrings of $Mat_2(\mathbb{Q})$ and of course $S_1 \subseteq S_2$. Here S_1 is an ideal of S_2 , because $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix} \in S_1$ for any $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in S_2$ and $\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} \in S_1$. On the other hand, S_1 is not an ideal of $Mat_2(\mathbb{Q})$, because, for example, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S_1$, $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in Mat_2(\mathbb{Q})$ and yet $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin S_1$. Thus S_1 is an ideal of S_2 but not an ideal of $Mat_2(\mathbb{Q})$. This shows that "idealness" is not an intrinsic property of a subring. A subring is not merely an ideal, but an ideal of a ring that has to be clearly specified. Compare this with Example 18.5(i).

(g) Intersection of ideals in a ring is an ideal. More precisely, if R is a ring and S_i are ideals of R ($i \in I$), then $S := \bigcap_{i \in I} S_i$ is an ideal of R : we know that S is an additive subgroup of R (Example 9.4(f)) and whenever $r \in R, s \in S$, we have $s \in S_i$ for all $i \in I$, hence $rs \in S_i$ and $sr \in S_i$ for all $i \in I$, hence $rs \in S$ and $sr \in S$, and S is therefore an ideal of R .

(h) Let R be a ring and X a subset of R . There are ideals of R which contain X , for example R itself. The intersection of all ideals that contain X is an ideal of R by Example 30.6(g). This ideal is called the *ideal generated by X* . Compare this with Definition 24.1. When X consists of a single element only, say when $X = \{a\}$, the ideal generated by X is said to be a *principal ideal*, more exactly the *principal ideal generated by a* . It is easy to verify that the principal ideal generated by a is

$$\{za + ua + at + \sum_{i=1}^n r_i a s_i : z \in \mathbb{Z}, u, t, r_i, s_i \in R, n \in \mathbb{N}\}$$

(cf. Lemma 24.2). If R has an identity, this ideal can be written more simply as

$$\left\{ \sum_{i=1}^n r_i a s_i : r_i, s_i \in R, n \in \mathbb{N} \right\}.$$

If R is commutative, the principal ideal generated by a is

$$\{za + ra : z \in \mathbb{Z}, r \in R\}.$$

If R is a commutative ring with identity, in particular, if R is an integral domain,

$$\{ra : r \in R\} = \{ar : r \in R\}$$

is the principal ideal generated by a . This is usually written as Ra , or as aR , or as (a) .

30.7 Theorem: *Let R be a ring and A an ideal of R . On the set R/A of right cosets of A in R , we define two operations $+$ and \cdot by*

$$(r + A) + (s + A) = (r + s) + A, \quad (r + A) \cdot (s + A) = rs + A$$

for all $r, s \in R$. With respect to these operations, R/A is a ring.

Proof: The addition on R/A is well defined since A is a normal additive subgroup of R and the multiplication on R/A is well defined since A is an ideal of R (Theorem 30.5).

R/A is a commutative group under addition (Theorem 18.7, Lemma 18.9(2)). We must now check the associativity of multiplication and the distributivity laws.

For all $r + A, s + A, t + A \in R/A$, we have

$$\begin{aligned} [(r + A) \cdot (s + A)] \cdot (t + A) &= (rs + A) \cdot (t + A) \\ &= (rs)t + A \\ &= r(st) + A \\ &= (r + A) \cdot (st + A) \\ &= (r + A) \cdot [(s + A) \cdot (t + A)], \end{aligned}$$

so multiplication is associative; and we also have

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

and

$$\begin{aligned} [(s + A) + (t + A)] \cdot (r + A) &= [(s + t) + A] \cdot (r + A) \\ &= (s + t)r + A \\ &= (sr + tr) + A \\ &= (sr + A) + (tr + A) \\ &= (s + A) \cdot (r + A) + (t + A) \cdot (r + A). \end{aligned}$$

Hence R/A is a ring. □

30.8 Definition: Let A be an ideal of a ring R . The ring R/A of Theorem 30.7 is called the *factor ring of R with respect to A* , or the *factor ring R by A* , or the *factor ring $R \bmod(\text{ulo}) A$* . Other names for R/A are: "quotient ring", "difference ring", "residue class ring".

30.9 Examples: (a) In the ring \mathbb{Z} of integers, the multiples $n\mathbb{Z}$ of an integer n form an ideal, the principal ideal generated by n (Example 30.6(b) and (h)). The factor ring $\mathbb{Z}/n\mathbb{Z}$ is exactly the ring \mathbb{Z}_n of integers mod n .

(b) Let T and A be as in Example 30.6(d). Then A is an ideal of T and we can build the factor ring T/A . This factor ring has precisely p elements. What are they?

(c) Let R be a ring and A an ideal of R . If R is commutative, so is R/A , for then $(r + A) \cdot (s + A) = rs + A = sr + A = (s + A) \cdot (r + A)$ for all $(r + A), (s + A)$ in R/A ; and if R is a ring with identity, so is R/A , for if 1 is an identity of R , then $1 + A \in R/A$ is an identity of R/A , because

$$(r + A) \cdot (1 + A) = r1 + A = r + A = r1 + A = (1 + A) \cdot (r + A)$$

for all $r + A \in R/A$.

Ideals are the subrings with respect to which we can build factor rings, just as normal subgroups are the subgroups with respect to which we can build factor groups. We know that normal subgroups are exactly the kernels of homomorphisms. We now show that ideals, too, are the kernels of homomorphisms.

30.10 Definition: Let R and R_1 be rings and let $\varphi: R \rightarrow R_1$ be a mapping from R into R_1 . If

$$(a + b)\varphi = a\varphi + b\varphi \quad \text{and} \quad (ab)\varphi = a\varphi \cdot b\varphi$$

for all $a, b \in R$, then φ is called a (*ring*) *homomorphism*.

The operations on the left hand sides are the operations on R , and those on the right hand side are the operations on R_1 . If the operations on R_1

were denoted by \oplus and \otimes , the equations would read $(a + b)\varphi = a\varphi \oplus b\varphi$ and $(ab)\varphi = a\varphi \otimes b\varphi$.

If $\varphi: R \rightarrow R_1$ is a ring homomorphism and S is a subring of R , then the restriction φ_S of φ to S is also a ring homomorphism.

A ring homomorphism is a homomorphism of additive groups which preserves products as well. This remark enables us to use the properties of group homomorphisms whenever we investigate ring homomorphisms.

30.11 Lemma: *Let $\varphi: R \rightarrow R_1$ be a ring homomorphism.*

(1) $0\varphi = 0$.

(2) $(-a)\varphi = -(a\varphi)$ for all $a \in R$.

(3) $(a_1 + a_2 + \cdots + a_n)\varphi = a_1\varphi + a_2\varphi + \cdots + a_n\varphi$ for all $a_1, a_2, \dots, a_n \in R$, $n \in \mathbb{N}$, $n \geq 2$. (In particular, $(na)\varphi = n(a\varphi)$ for all $a \in R$).

(4) $(a_1 a_2 \cdots a_n)\varphi = a_1\varphi a_2\varphi \cdots a_n\varphi$ for all $a_1, a_2, \dots, a_n \in R$, $n \in \mathbb{N}$, $n \geq 2$. (In particular, $(a^n)\varphi = (a\varphi)^n$ for all $a \in R$).

Proof: (1),(2),(3) follow immediately from Lemma 20.3, since φ is a group homomorphism. (4) is proved by the same argument as in the proof of Lemma 20.3(3). \square

We now establish the ring theoretical analogues of theorems about group homomorphisms.

30.12 Theorem: *Let $\varphi: R \rightarrow R_1$ and $\psi: R_1 \rightarrow R_2$ be a ring homomorphisms.*

Then the composition mapping

$$\varphi\psi: R \rightarrow R_2$$

is a ring homomorphism from R into R_2 .

Proof: We regard φ and ψ as group homomorphisms. We know from Theorem 20.4 that $\varphi\psi$ is an additive group homomorphism. It remains to show that $\varphi\psi$ preserves multiplication. Since

$$\begin{aligned} (rs)\varphi\psi &= ((rs)\varphi)\psi \\ &= (r\varphi \cdot s\varphi)\psi \end{aligned}$$

$$\begin{aligned}
&= (r\varphi)\psi \cdot (s\varphi)\psi \\
&= r(\varphi\psi) \cdot s(\varphi\psi)
\end{aligned}$$

for all $r, s \in R$, $\varphi\psi$ does preserve multiplication and hence $\varphi\psi$ is a ring homomorphism. \square

Since any ring homomorphism $\varphi: R \rightarrow R_1$ is a group homomorphism, we can talk about the image and kernel of φ . Of course

$$Im \varphi = \{r\varphi \in R_1 : r \in R\} \subseteq R_1 \text{ and } Ker \varphi = \{r \in R : r\varphi = 0\} \subseteq R.$$

30.13 Theorem: *Let $\varphi: R \rightarrow R_1$ be a ring homomorphism. Then $Im \varphi$ is a subring of R_1 and $Ker \varphi$ is an ideal of R (cf. Theorem 20.6).*

Proof: $Im \varphi$ is a subgroup of R_1 by Theorem 20.6. We must show that $Im \varphi$ is closed under multiplication (Lemma 30.2). Let $x, y \in Im \varphi$. Then $x = r\varphi$, $y = s\varphi$ for some $r, s \in R$. Then $xy = r\varphi \cdot s\varphi = (rs)\varphi$ is the image, under φ , of an element of R , namely of $rs \in R$. So $xy \in Im \varphi$ and $Im \varphi$ is closed under multiplication. This proves that $Im \varphi$ is a subring of R_1 .

$Ker \varphi$ is a subgroup of R by Theorem 20.6. We must only show that $Ker \varphi$ has the "absorbing" property (Definition 30.4). For any $r \in R$ and $a \in Ker \varphi$, we have $a\varphi = 0$ and so

$$(ra)\varphi = r\varphi \cdot a\varphi = r\varphi \cdot 0 = 0 \text{ and } (ar)\varphi = a\varphi \cdot r\varphi = 0 \cdot r\varphi = 0$$

by Lemma 29.6(1),(2). Thus $ra \in Ker \varphi$ and $ar \in Ker \varphi$. Therefore $Ker \varphi$ is an ideal of R . \square

We prove conversely that every ideal is the kernel of some homomorphism.

30.14 Theorem: *Let R be a ring and let A be an ideal of R . Then*

$$\begin{aligned}
v: R &\rightarrow R/A \\
r &\rightarrow r + A
\end{aligned}$$

is a ring homomorphism from R onto R/A and $Ker v = A$ (v is called the natural or canonical homomorphism).

Proof: The natural mapping $v: R \rightarrow R/A$ is a group homomorphism from R onto R/A and $\text{Ker } v = A$ by Theorem 20.12. So we need only show that v is a ring homomorphism, i.e., that v preserves multiplication. This follows from the very definition of multiplication in R/A : we have

$$(rs)v = rs + A = (r + A)(s + A) = rv \cdot sv$$

for all $r, s \in R$. So v is a ring homomorphism. \square

30.15 Definition: A ring homomorphism $\varphi: R \rightarrow R_1$ is called a (*ring*) *isomorphism* if it is one-to-one and onto. In this case, we say R is *isomorphic* to R_1 and write $R \cong R_1$. If R is not isomorphic to R_1 , we put $R \not\cong R_1$.

So a ring isomorphism is a group isomorphism that preserves multiplication. We use the same sign " \cong " for isomorphic rings as for isomorphic groups. This should not lead to any confusion. When confusion is likely, we state explicitly whether we mean ring isomorphism or group isomorphism.

30.16 Lemma: Let $\varphi: R \rightarrow R_1$ and $\psi: R_1 \rightarrow R_2$ be ring isomorphisms.

- (1) $\varphi\psi: R \rightarrow R_2$ is a ring isomorphism.
- (2) $\varphi^{-1}: R_1 \rightarrow R$ is a ring isomorphism.

Proof: (1) We know that $\varphi\psi$ is a group isomorphism (Lemma 20.11(1)) and a ring homomorphism (Theorem 30.12), so $\varphi\psi$ is a ring isomorphism. This proves (1).

(2) We know that φ^{-1} is a group isomorphism (Lemma 20.11(2)). We must also show that φ^{-1} preserves products. For any $x, y \in R_1$, we must show $(xy)\varphi^{-1} = x\varphi^{-1} \cdot y\varphi^{-1}$. Since φ is onto, there are $a, b \in R$ such that $a\varphi = x$ and $b\varphi = y$. Now a and b are unique with this property, for φ is one-to-one, and $a = x\varphi^{-1}$, $b = y\varphi^{-1}$. This is the definition of the inverse mapping. Since φ is a homomorphism, we have

$$\begin{aligned} (ab)\varphi &= a\varphi \cdot b\varphi \\ (ab)\varphi &= xy \\ ab &= (xy)\varphi^{-1} \end{aligned}$$

$$x\varphi^{-1} \cdot y\varphi^{-1} = (xy)\varphi^{-1}$$

for all $x, y \in R_1$. So $\varphi^{-1}: R_1 \rightarrow R$ is a ring homomorphism and consequently φ^{-1} is a ring isomorphism. \square

30.17 Theorem (Fundamental theorem on homomorphisms): *Let $\varphi: R \rightarrow R_1$ be a ring homomorphism and let $\nu: R \rightarrow R/\text{Ker } \varphi$ be the natural homomorphism.*

$$\begin{array}{ccccc}
 & R/\text{Ker } \varphi & & R/\text{Ker } \varphi & \\
 & \nu & & \nu & \psi \\
 R & \xrightarrow{\varphi} & R_1 & R & \xrightarrow{\varphi} & R_1 \\
 & (a) & & (b) &
 \end{array}$$

Then there is a one-to-one ring homomorphism $\psi: R/\text{Ker } \varphi \rightarrow R_1$ such that $\nu\psi = \varphi$.

Proof: From Theorem 20.15 and its proof, we know that the mapping

$$\begin{aligned}
 \psi: R/\text{Ker } \varphi &\rightarrow R_1 \\
 r + \text{Ker } \varphi &\rightarrow r\varphi
 \end{aligned}$$

is a well defined one-to-one group homomorphism such that $\nu\psi = \varphi$. It only remains to check that ψ preserves multiplication. For all $r, s \in R$, we have

$$\begin{aligned}
 ((r + \text{Ker } \varphi) \cdot (s + \text{Ker } \varphi))\psi &= (rs + \text{Ker } \varphi)\psi \\
 &= (rs)\varphi \\
 &= r\varphi \cdot s\varphi \\
 &= (r + \text{Ker } \varphi)\psi \cdot (s + \text{Ker } \varphi)\psi,
 \end{aligned}$$

so ψ preserves products and ψ is a ring homomorphism. \square

30.18 Theorem: *Let $\varphi: R \rightarrow R_1$ be a ring homomorphism. Then*

$$R/\text{Ker } \varphi \cong \text{Im } \varphi \quad (\text{ring isomorphism}).$$

Proof: The mapping $\psi: R/\text{Ker } \varphi \rightarrow R_1$ is a one-to-one ring homomorphism

$$r + \text{Ker } \varphi \rightarrow r\varphi$$

(Theorem 30.17) and $Im \psi = Im \varphi$ (see the proof of Theorem 20.16). Thus ψ is a one-to-one ring homomorphism onto $Im \varphi$ and therefore

$$R/Ker \varphi \cong Im \varphi. \quad \square$$

30.19 Theorem: Let $\varphi: R \rightarrow R_1$ be a ring homomorphism from R onto R_1 .

(1) Each subring S of R with $Ker \varphi \subseteq S$, is mapped to a subring of R_1 , which will be denoted by S_1 .

(2) If S and T are subrings of R and $Ker \varphi \subseteq S \subseteq T$, then $S_1 \subseteq T_1$.

(3) If S and T are subrings of R containing $Ker \varphi$ and if $S_1 \subseteq T_1$, then $S \subseteq T$.

(4) If S and T are subrings of R containing $Ker \varphi$ and if $S_1 = T_1$, then $S = T$.

(5) For any subring U of R_1 , there is a subring S of R such that $Ker \varphi \subseteq S$ and $S_1 = U$.

(6) Let S be a subring of R containing $Ker \varphi$. Then S is an ideal of R if and only if S_1 is an ideal of R_1 .

(7) If S is an ideal of R containing $Ker \varphi$, then $R/S \cong R_1/S_1$.

$$\begin{array}{ccc|ccc} R & & R_1 & & R & & R_1 & & R_1/S_1 \\ T & & T_1 & & & & & & \\ S & & S_1 & & S & & S_1 & & 1 \\ Ker \varphi & & \{0\} & & Ker \varphi & & \{0\} & & \\ \{0\} & & & & \{0\} & & & & \end{array}$$

Proof: (1) As in Theorem 21.1, we put $S_1 = Im \varphi_S$. By Theorem 30.13, S_1 is a subring of R_1 . (The restriction of a ring homomorphism to a subring is also a ring homomorphism.)

(2),(3),(4) We regard φ merely as a group homomorphism and apply Theorem 21.1(2),(3),(4).

(5) Let U be a subring of R_1 . Consider U as an additive subgroup of R_1 . From Theorem 21.1(5), we know that there is a subgroup S of R , namely

$$S = \{r \in R: r\varphi \in U\}$$

with $\text{Ker } \varphi \subseteq S$ and $S_1 = U$. It remains to show that S is a subring of R . We need only check that S is closed under multiplication, and this is easy: if $r, s \in S$, then $r\varphi, s\varphi \in U$, then $r\varphi \cdot s\varphi \in U$, then $(rs)\varphi \in U$, then $rs \in S$ and S is multiplicatively closed.

(6) Let S be a subring of R , with $\text{Ker } \varphi \subseteq S$. First we assume that S is an ideal of R and prove that S_1 is an ideal of R_1 . We must show that $r_1 s_1 \in S_1$ and $s_1 r_1 \in S_1$ for all $r_1 \in R_1, s_1 \in S_1$. Well, if $r_1 \in R_1, s_1 \in S = \text{Im } \varphi_S$, then there are $r \in R$ with $r\varphi = r_1$ and $s \in S$ with $s\varphi = s_1$, and so

$$\begin{aligned} r_1 s_1 &= r\varphi \cdot s\varphi = (rs)\varphi \in \text{Im } \varphi_S = S_1 \text{ since } rs \in S \text{ as } S \text{ is an ideal of } R, \\ s_1 r_1 &= s\varphi \cdot r\varphi = (sr)\varphi \in \text{Im } \varphi_S = S_1 \text{ since } sr \in S \text{ as } S \text{ is an ideal of } R. \end{aligned}$$

This proves that S_1 is an ideal of R_1 if S is an ideal of R .

Next we suppose S_1 is an ideal of R_1 . By Theorem 30.14, $S_1 = \text{Ker } \nu'$, where $\nu': R_1 \rightarrow R_1/S_1$ is the natural homomorphism. Then $\varphi\nu': R \rightarrow R_1/S_1$ is a ring homomorphism (Theorem 30.12) with

$$\text{Ker } \varphi\nu' = S, \tag{*}$$

as follows from (ii) on page 225. By Theorem 30.13, S is an ideal of R .

(7) Assume that S is an ideal of R and S_1 is an ideal of R_1 . From the ring homomorphism $\varphi\nu': R \rightarrow R_1/S_1$, we get

$$R/\text{Ker } \varphi\nu' \cong \text{Im } \varphi\nu' \quad (\text{ring isomorphism})$$

by Theorem 30.18. Here $\text{Ker } \varphi\nu' = S$ by (*) and $\text{Im } \varphi\nu' = R_1/S_1$, for φ and ν' are both onto. Thus

$$R/S \cong R_1/S_1 \quad (\text{ring homomorphism}). \quad \square$$

30.20 Theorem: *Let A be an ideal of R . The subrings of R/A are given by S/A , where S runs through the subrings of R containing A . In other words, for each subring U of R/A , there is a unique subring S of R such that $A \subseteq U$ and $U = S/A$. When U_1 and U_2 are subrings of R/A , say with $U_1 = S_1/A$ and $U_2 = S_2/A$, where S_1, S_2 are subrings of R containing A , then $U_1 \subseteq U_2$ if and only if $S_1 \subseteq S_2$. Furthermore, S/A is an ideal of R/A if and only if S is an ideal of R . In this case*

$$R/A / S/A \cong R/S \quad (\text{ring isomorphism}).$$

Proof: The natural homomorphism $\nu: R \rightarrow R/A$ is onto by Theorem 30.14. Now we may apply Theorem 30.19, which states that any subring

of R/A is of the form $S_1 = \text{Im } \nu_S = \{sv \in R/A: s \in S\} = \{s + A \in R/A: s \in S\} = S/A$ for some subring S of R containing $\text{Ker } \nu = A$ (notice that S/A is meaningful, for A is an ideal of S when $A \subseteq S$ and S is a subring of R). We know that $U_1 = \text{Im } \nu_{S_1} \subseteq \text{Im } \nu_{S_2} = U_2$ if and only if $S_1 \subseteq S_2$ (Theorem 30.19 (2),(3)). Finally, $S/A = \text{Im } \nu_S$ is an ideal of R/A if and only if S is an ideal of R , in which case $R/A / S/A \cong R/S$ (Theorem 30.19(6),(7)).

□

30.21 Theorem: Let R be a ring, S a subring of R and A an ideal of R .

- (1) $S + A$ is a subring of R (here $S + A$ denotes $\{s + a \in R: s \in S, a \in A\} \subseteq R$ in accordance with Definition 19.1).
- (2) A is an ideal of $S + A$, and $S \cap A$ is an ideal of S .
- (3) $S + A / A \cong S / S \cap A$ (ring isomorphism).

Proof: (1) $S + A$ is an additive subgroup of R (Lemma 19.4), and it is also closed under multiplication since

$$(s + a)(s' + a') = ss' + sa' + as' + aa' \in S + A$$

for all $s, s' \in S, a, a' \in A$, because then $ss' \in S$; and $sa', as', aa' \in A$, consequently $sa' + as' + aa' \in A$. So $S + A$ is a subring of R .

(2) A is an ideal of R and a subset of $S + A$, so, a fortiori, A is an ideal of $S + A$. Also, $S \cap A$ is a subgroup of S and, for all $a \in S \cap A, s \in S$,

$$sa \in S \text{ and } sa \in A, \text{ so } sa \in S \cap A,$$

$$as \in S \text{ and } as \in A, \text{ so } as \in S \cap A$$

since S is closed under multiplication and A is an ideal of R . This shows that $S \cap A$ is an ideal of S .

(3) We have a ring homomorphism $\nu_S: S \rightarrow R/A$, the restriction of the natural homomorphism $\nu: R \rightarrow R/A$. Hence $S/\text{Ker } \nu_S \cong \text{Im } \nu_S$. From the proof of Theorem 21.3, we know $\text{Ker } \nu_S = S \cap A$ and $\text{Im } \nu_S = S + A / A$. So

$$S + A / A \cong S / S \cap A$$

as contended. □

Exercises

1. Let R be a ring. The *center of R* is defined to be the set

$$Z(R) = \{z \in R: za = az \text{ for all } a \in R\}.$$

Is $Z(R)$ a subring or an ideal of R ?

2. Given a ring R , find $Z(\text{Mat}_2(R))$.

3. Prove that, if D is a division ring, then $Z(D)$ is a field.

4. Let R be a ring and $b \in R$. Is the *centralizer*

$$C_R(b) := \{r \in R: rb = br\}$$

of b a subring of R ?

5. Let R be a ring with identity. Prove or disprove that $Z(R^\times) = (Z(R))^\times$.

6. Show that, if K is a field, then $\{0\}$ and K are the only ideals of K .

7. Let D be a division ring. Find all ideals of $\text{Mat}_2(D)$.

8. Let R be a ring and let $\text{End}(R)$ be the set of all ring homomorphisms from R into R . For any $\varphi, \psi \in \text{End}(R)$, we define $\varphi + \psi: R \rightarrow R$ by

$$r(\varphi + \psi) = r\varphi + r\psi.$$

Show that $\varphi + \psi \in \text{End}(R)$ and that $(\text{End}(R), +, \circ)$ is a ring (\circ is the composition of functions).

9. Let R be a ring and A an ideal of R . Prove that

$$\{r \in R: rx \in A \text{ for all } x \in R\}$$

is an ideal of R .

10. Let $(R, +, \cdot)$ be a ring. If A, B are nonempty subsets of R , we define AB to be the nonempty subset

$$\{a_1b_1 + a_2b_2 + \cdots + a_nb_n \in R: n \in \mathbb{N}, a_i \in A, b_i \in B\}$$

of R . A subgroup A of $(R, +)$ is called a *right* (resp. *left*) *ideal of R* provided $ar \in A$ (resp. $ra \in A$) for all $a \in A, r \in R$. Prove that, if A, B, C are arbitrary right (resp. left) ideals of R , then

(a) $A + B, AB, A \cap B$ are right (resp. left) ideals of R ,

(b) $(AB)C = A(BC)$,

(c) $A(B + C) = AB + AC$ and $(B + C)A = BA + CA$.

11. Let R be a ring. An ideal P of R is said to be *prime* if $P \neq R$ and if, for any two ideals A, B of R , the implication

$$AB \subseteq P \implies A \subseteq P \text{ or } B \subseteq P$$

is valid (see Ex. 10). Prove the following statements.

(a) Let P be an ideal of R and $P \neq R$. If, for any $a, b \in R$,

$$ab \in P \implies a \in P \text{ or } b \in P$$

then P is a prime ideal of R .

(b) Let R be commutative. If P is a prime ideal of R , then

$$ab \in P \implies a \in P \text{ or } b \in P$$

for any $a, b \in R$.

(c) $\{0\}$ is a prime ideal of any integral domain.

(d) Let R be a commutative ring with identity and P an ideal of R . Then P is a prime ideal of R if and only if R/P is an integral domain.

12. Let R be a ring. An ideal (resp. right ideal, resp. left ideal) M of R is said to be *maximal ideal* (resp. *right ideal*, resp. *left ideal*) of R if $M \neq R$ and if there is no ideal (resp. right ideal, resp. left ideal) N of R such that $M \subset N \subset R$. Prove the following statements.

(a) If R is a commutative ring with identity, then every maximal ideal of R is prime.

(b) If R is a ring with identity, distinct from the null ring, and if M is an ideal of R such that R/M is a division ring, then M is maximal.

(c) If R is a ring with identity and M a maximal ideal of R , then R/M is a field.

(d) Find a noncommutative ring R with identity and a maximal ideal M of R such that R/M is not a division ring.

13. An element a in a ring R is said to be nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$. Prove that, if a, b are nilpotent elements in a ring, and if $ab = ba$, then $a + b$ is also nilpotent.

14. Let R be a commutative ring. Show that the set N of all nilpotent elements in R is an ideal of R and that the factor ring R/N has no nilpotent elements other than 0.

15. Find rings R, S with identities $1_R, 1_S$ respectively and a ring homomorphism $\varphi: R \rightarrow S$ such that $(1_R)\varphi \neq 1_S$.

16. If R, S are rings with identities $1_R, 1_S$ respectively, and if $\varphi: R \rightarrow S$ is a ring homomorphism onto S , prove that $(1_R)\varphi = 1_S$.

17. The notation being as in §29, Ex. 7, prove that the mapping $r \rightarrow (r, 0)$ is a one-to-one ring homomorphism from R into S .