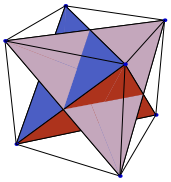


CHAPTER 6

Rings

6.1. A Recollection of Rings

We encountered the definitions of rings and fields in Section 1.11. Let us recall them here for convenience.

Definition 6.1.1. A *ring* is a nonempty set R with two operations: addition, denoted here by $+$, and multiplication, denoted by juxtaposition, satisfying the following requirements:

(a) Under addition, R is an abelian group.
(b) Multiplication is associative.
(c) Multiplication distributes over addition: $a(b+c) = ab+ac$, and $(b+c)a = ba+ca$ for all $a, b, c \in R$.

A ring is called commutative if multiplication is commutative, $ab = ba$ for all elements a, b in the ring. Recall that a multiplicative identity in a ring is an element 1 such that $1a = a1 = a$ for all elements a in the ring. An element a in a ring with multiplicative identity 1 is a *unit* or *invertible* if there exists an element b such that $ab = ba = 1$.

Some authors include the the existence of a multiplicative identity in the definition of a ring, but as this requirement excludes many natural examples, we will not follow this practice.

Let's make a few elementary deductions from the ring axioms: Note that the distributive law $a(b+c) = ab+ac$ says that the map $L_a : b \mapsto ab$ is a group homomorphism of $(R, +)$ to itself. It follows that $L_a(0) = 0$ and $L_a(-b) = -L_a(b)$ for any $b \in R$. This translates to $a\,0 = 0$ and $a(-b) = -ab$. Similarly, $0\,a = 0$, and $(-b)a = -ba$. For $n \in \mathbb{Z}$ and $a \in R$, since nb is the n–th power of b in the abelian group $(R, +)$, we also have $L_a(nb) = nL_a(b)$; that is, $a(nb) = n(ab)$. Similarly, $(na)b = n(ab)$.

In particular, if R has a multiplicative identity element 1, then $(n\,1)b = n(1\,b) = nb$ and $b(n\,1) = n(b\,1) = nb$ for any $n \in \mathbb{Z}$ and $b \in R$.

A field is a special sort of ring:

Definition 6.1.2. A *field* is a commutative ring with multiplicative identity element 1 (different from 0) in which *every nonzero element is a unit.*

We gave a number of examples of rings and fields in Section 1.11, which you should review now. There are (at least) four main sources of ring theory:

1. *Numbers.* The familiar number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings. In fact, all of them but $\mathbb{Z}$ are fields.

2. *Polynomial rings in one or several variables.* We have discussed polynomials in one variable over a field in Section 1.8. Polynomials in several variables, with coefficients in any commutative ring R with identity element, have a similar description: Let $x_1, \ldots, x_n$ be variables, and let $I = (i_1, \ldots, i_n)$ be a so–called *multi-index*, namely, a sequence of nonnegative integers of length n. Let x^I denote the monomial $x^I = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. A polynomial in the variables $x_1, \ldots, x_n$ with coefficients in R is an expression of the form $\sum_I \alpha_I x^I$, where the sum is over multi-indices, the α_I are elements of R, and $\alpha_I = 0$ for all but finitely many multi-indices I.

Example 6.1.3. $7xyz + 3x^2yz^2 + 2yz^3$ is an element of $\mathbb{Q}[x, y, z]$. The three nonzero terms correspond to the multi-indices

$$(1, 1, 1,),\ (2, 1, 2),\ \text{and}\ (0, 1, 3).$$

Polynomials in several variables are added and multiplied according to the following rules:

$$\sum_I \alpha_I x^I + \sum_I \beta_I x^I = \sum_I (\alpha_I + \beta_I) x^I,$$

and

$$(\sum_I \alpha_I x^I)(\sum_J \beta_J x^J) = \sum_I \sum_J \alpha_I \beta_J x^{I+J} = \sum_L \gamma_L x^L,$$

where $\gamma_L = \sum_{\substack{I,J \\ I+J=L}} \alpha_I \beta_J$.

With these operations, the set $R[x_1, \ldots, x_n]$ of polynomials in the variables $\{x_1 \ldots, x_n\}$ with coefficients in R is a commutative ring with multiplicative identity.

Example 6.1.4. Let $p(x,y,z) = 7xyz+3x^2yz^2+2yz^3$ and $q(x,y,z) = 2+3xz+2xyz$. Then

$$p(x,y,z)+q(x,y,z) = 2+3xz+9xyz+3x^2yz^2+2yz^3,$$

and

$$\begin{aligned} p(x,y,z)q(x,y,z) = {} & 14\,x\,y\,z + 27\,x^2\,y\,z^2 + 14\,x^2\,y^2\,z^2 + 4\,y\,z^3 \\ & + 9\,x^3\,y\,z^3 + 6\,x^3\,y^2\,z^3 + 6\,x\,y\,z^4 + 4\,x\,y^2\,z^4. \end{aligned}$$

3. *Rings of functions.* Let X be any set and let R be a field. Then the set of functions defined on X with values in R is a ring, with the operations defined pointwise: $(f+g)(x) = f(x)+g(x)$, and $(fg)(x) = f(x)g(x)$.

If X is a metric space (or a topological space) and R is equal to one of the fields $\mathbb{R}$ or $\mathbb{C}$, then the set of *continuous* R–valued functions on X, with pointwise operations, is a ring. The essential point here is that the sum and product of continuous functions are continuous. (If you are not familiar with metric or topological spaces, just think of X as a subset of $\mathbb{R}$.)

If X is an open subset of $\mathbb{C}$, then the set of *holomorphic* $\mathbb{C}$–valued functions on X is a ring. (If you are not familiar with holomorphic functions, just ignore this example.)

4. *Endomorphism rings and matrix rings.* Let V be a vector space over a field K. The set $\mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)$ of linear maps from V to V has two operations: Addition of linear maps is defined pointwise, $(S+T)(v) = S(v)+T(v)$. Multiplication of linear maps, however, is defined by composition: $ST(v) = S(T(v))$. With these operations, $\mathrm{End}_K(V)$ is a ring.

The set $\mathrm{Mat}_n(K)$ of n-by-n matrices with entries in K is a ring, with the usual operations of addition and multiplication of matrices.

If V is n-dimensional over K, then the rings $\mathrm{End}_K(V)$ and $\mathrm{Mat}_n(K)$ are isomorphic. In fact, for any ordered basis $B = (v_1,\ldots,v_n)$ of V the map that assigns to each linear map $T : V \to V$ its matrix $[T]_{B,B}$ with respect to B is a ring isomorphism from $\mathrm{End}(V)$ to $\mathrm{Mat}_n(K)$.

The notion of subring was introduced informally in Section 1.11; let us give the precise definition.

Definition 6.1.5. A nonempty subset S of a ring R is called a *subring* if S is a ring *with the two ring operations inherited from* R.

For S to be a subring of R, it is necessary and sufficient that

1. For all elements x and y of S, the sum and product $x+y$ and xy are elements of S.

2. For all $x \in S$, the additive opposite $-x$ is an element of S.

We gave a number of examples of subrings in Example 1.11.5. You are asked to verify these examples, and others, in the Exercises.

For any ring R and any subset $\mathcal{S} \subseteq R$ there is a smallest subring of R that contains $\mathcal{S}$, which is called the *subring generated by* $\mathcal{S}$. We say that R *is generated by* $\mathcal{S}$ as a ring if no proper subring of R contains $\mathcal{S}$.

A "constructive" view of the subring generated by $\mathcal{S}$ is that it consists of all possible finite sums of finite products $\pm T_1 T_2 \cdots T_n$, where $T_i \in \mathcal{S}$. In particular, the subring generated by a single element $T \in R$ is the set of all sums $\sum_{i=1}^{n} n_i T^i$. (Note there is no term for $i = 0$.) The subring generated by T and the multiplicative identity 1 (assuming that R has a multiplicative identity) is the set of all sums $n_0 1 + \sum_{i=1}^{n} n_i T^i = \sum_{i=0}^{n} n_i T^i$, where we use the convention $T^0 = 1$.

The subring generated by $\mathcal{S}$ is equal to the intersection of the family of all subrings of R that contain S; this family is nonempty since R itself is such a subring. (As for subgroups, the intersection of an arbitrary nonempty collection of subrings is a subring.)

Example 6.1.6. Let $\mathcal{S}$ be a subset of $\mathrm{End}_K(V)$ for some vector space V. There are two subrings of $\mathrm{End}_K(V)$ associated to $\mathcal{S}$. One is the subring generated by $\mathcal{S}$, which consists of all finite sums of products of elements of $\mathcal{S}$. Another is

$$\mathcal{S}' = \{T \in \mathrm{End}_K(V) : TS = ST \text{ for all } S \in \mathcal{S}\},$$

the so–called *commutant* of $\mathcal{S}$ in $\mathrm{End}(V)$.

Example 6.1.7. Let G be a subgroup of $\mathrm{GL}(V)$, the group of invertible linear transformations of a vector space V over a field K. I claim that the subring of $\mathrm{End}_K(V)$ generated by G is the set of finite sums $\sum_{g \in G} n_g g$, where $n_g \in \mathbb{Z}$. In fact, we can easily check that this set is closed under taking sums, additive opposites, and products.

Example 6.1.8. The previous example inspires the following construction. Let G be any finite group. Consider the set $\mathbb{Z}G$ of formal linear combinations of group elements, with coefficients in $\mathbb{Z}$, $\sum_{g \in G} a_g\, g$. (If you like, you can identify such a sum with the function $g \mapsto a_g$ from G to $\mathbb{Z}$.) Two such expressions are added coefficient-by-coefficient,

$$\sum_{g \in G} a_g\, g + \sum_{g \in G} b_g\, g = \sum_{g \in G} (a_g + b_g)\, g,$$

and multiplied according to the rule

$$\sum_{g\in G} a_g\, g \sum_{h\in G} b_h\, h = \sum_{g\in G}\sum_{h\in G} a_g b_h\, gh = \sum_{\ell\in G}(\sum_{g\in G} a_g b_{g^{-1}\ell})\,\ell.$$

You are asked to verify that $\mathbb{Z}G$ is a ring in the Exercises. $\mathbb{Z}G$ is called the *integer group ring* of G.

Instead of taking coefficients in $\mathbb{Z}$, we can also take coefficients in $\mathbb{C}$, for example; the result is called the *complex group ring* of G.

Example 6.1.9. Let R be a commutative ring with multiplicative identity element. A formal power series in one variable with coefficients in R is a formal infinite sum $\sum_{i=0}^{\infty}\alpha_i x^i$. The set of formal power series is denoted $R[[x]]$. Formal power series are added coefficient-by-coefficient,

$$\sum_{i=0}^{\infty}\alpha_i x^i + \sum_{i=0}^{\infty}\beta_i x^i = \sum_{i=0}^{\infty}(\alpha_i+\beta_i)x^i.$$

The product of formal power series is defined as for polynomials:

$$(\sum_{i=0}^{\infty}\alpha_i x^i)(\sum_{i=0}^{\infty}\beta_i x^i) = \sum_{i=0}^{\infty}\gamma_i x^i,$$

where $\gamma_n = \sum_{j=0}^{n}\alpha_j\beta_{n-j}$. With these operations, the set of formal power series is a commutative ring.

Definition 6.1.10. Two rings R and S are *isomorphic* if there is a bijection between them that preserves both the additive and multiplicative structures. That is, there is a bijection $\varphi : R \to S$ satisfying $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Definition 6.1.11. The *direct sum* of several rings $R_1, R_2, \ldots, R_n$ is the Cartesian product endowed with the operations

$$(r_1, r_2, \ldots, r_n) + (r'_1, r'_2, \ldots, r'_s) = (r_1 + r'_1, r_2 + r'_2, \ldots, r_n + r'_n)$$

and

$$(r_1, r_2, \ldots, r_n)(r'_1, r'_2, \ldots, r'_s) = (r_1 r'_1, r_2 r'_2, \ldots, r_n r'_n).$$

The direct sum of $R_1, R_2, \ldots, R_n$ is denoted $R_1 \oplus R_2 \oplus \cdots \oplus R_n$.

Example 6.1.12. According to the discussion at the end of Section 1.11 and in Exercise 1.11.10, if a and b are relatively prime natural numbers, then $\mathbb{Z}_{ab}$ and $\mathbb{Z}_a \oplus \mathbb{Z}_b$ are isomorphic rings. Consequently, if $a_1, a_2, \ldots, a_n$ are pairwise relatively prime, then $\mathbb{Z}_{a_1 a_2 \cdots a_n} \cong \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}_{a_n}$ as rings.

Exercises 6.1

6.1.1. Show that if a ring R has a multiplicative identity, then the multiplicative identity is unique. Show that if an element $r \in R$ has a left multiplicative inverse r' and a right multiplicative inverse r'', then $r' = r''$.

6.1.2. Verify that $R[x_1, \ldots, x_n]$ is a ring for any commutative ring R with multiplicative identity element.

6.1.3. Consider the set of infinite-by-infinite matrices with real entries that have only finitely many nonzero entries. (Such a matrix has entries a_{ij}, where i and j are natural numbers. For each such matrix, there is a natural number n such that $a_{ij} = 0$ if $i \geq n$ or $j \geq n$.) Show that the set of such matrices is a ring without identity element.

6.1.4. Show that (a) the set of upper triangular matrices and (b) the set of upper triangular matrices with zero entries on the diagonal are both subrings of the ring of all n-by-n matrices with real coefficients. The second example is a ring without multiplicative identity.

6.1.5. Show that the set of matrices with integer entries is a subring of the ring of all n-by-n matrices with real entries. Show that the set of matrices with entries in $\mathbb{N}$ is closed under addition and multiplication but is not a subring.

6.1.6. Show that the set of symmetric polynomials in three variables is a subring of the ring of all polynomials in three variables. A polynomial is symmetric if it remains unchanged when the variables are permuted, $p(x, y, z) = p(y, x, z)$, and so on.

6.1.7. Experiment with variations on the preceding examples and exercises by changing the domain of coefficients of polynomials, values of functions, and entries of matrices: for example, polynomials with coefficients in the natural numbers, complex–valued functions, matrices with complex entries. What is allowed and what is not allowed for producing rings?

6.1.8. Show that $\mathrm{End}_K(V)$ is a ring, for any vector space V over a field K.

6.1.9. Suppose $\varphi : R \to S$ is a ring isomorphism. Show that R has a multiplicative identity if, and only if, S has a multiplicative identity. Show that R is commutative if, and only if, S is commutative.

6.1.10. Show that the intersection of any family of subrings of a ring is a subring. Show that the subring generated by a subset $\mathcal{S}$ of a ring R is the intersection of all subrings R' such that $\mathcal{S} \subseteq R' \subseteq R$.

6.1.11. Show that the set $\mathbb{R}(x)$ of rational functions $p(x)/q(x)$, where $p(x), q(x) \in \mathbb{R}[x]$ and $q(x) \neq 0$, is a field. (Note the use of parentheses to distinguish this ring $\mathbb{R}(x)$ of rational functions from the ring $\mathbb{R}[x]$ of polynomials.)

6.1.12. Let R be a ring and X a set. Show that the set $\mathrm{Fun}(X, R)$ of functions on X with values in R is a ring. Show that R is isomorphic to the subring of constant functions on X. Show that $\mathrm{Fun}(X, R)$ is commutative if, and only if, R is commutative. Suppose that R has an identity; show that $\mathrm{Fun}(X, R)$ has an identity and describe the units of $\mathrm{Fun}(X, R)$.

6.1.13. Let $\mathcal{S} \subseteq \mathrm{End}_K(V)$, where V is a vector space over a field K. Show that

$$\mathcal{S}' = \{T \in \mathrm{End}_K(V) : TS = ST \text{ for all } S \in \mathcal{S}\}$$

is a subring of $\mathrm{End}_K(V)$.

6.1.14. Let V be a vector space over a field K. Let G be a subgroup of $GL(V)$. Show that the subring of $\mathrm{End}_K(V)$ generated by G is the set of all linear combinations $\sum_g n_g g$ of elements of G, with coefficients in $\mathbb{Z}$.

6.1.15. Verify that the "group ring" $\mathbb{Z}G$ of Example 6.1.8 is a ring.

6.1.16. Consider the *group* $\mathbb{Z}_2$ written as $\{e, \xi\}$, where $\xi^2 = e$. The complex group ring $\mathbb{C}\mathbb{Z}_2$ consists of formal sums $ae+b\xi$, with $a, b \in \mathbb{C}$. Show that the map $a+b\xi \mapsto (a+b, a-b)$ is a ring isomorphism from the group ring $\mathbb{C}\mathbb{Z}_2$ to the ring $\mathbb{C} \oplus \mathbb{C}$.

6.1.17. Let R be a commutative ring with identity element. Show that the set of formal power series $R[[x]]$, with coefficients in R is a commutative ring.

6.2. Homomorphisms and Ideals

Certain concepts and constructions that were fundamental to our study of groups are also important for the study of rings. In fact, one could expect analogous concepts and constructions to play a role for any reasonable algebraic structure.

We have already discussed the idea of a subring, which is analogous to the idea of a subgroup. The next concept from group theory

that we might expect to play a fundamental role in ring theory is the notion of a homomorphism.

Definition 6.2.1. A *homomorphism* $\varphi : R \to S$ of rings is a map satisfying $\varphi(x + y) = \varphi(x) + \varphi(y)$, and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in R$.

In particular, a ring homomorphism is a homomorphism for the abelian group structure of R and S, so we know, for example, that $\varphi(-x) = -\varphi(x)$ and $\varphi(0) = 0$. Even if R and S both have an identity element 1, it is not automatic that $\varphi(1) = 1$. If we want to specify that this is so, we will call the homomorphism a *unital* homomorphism.

Example 6.2.2. The map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(a) = [a] = a + n\mathbb{Z}$ is a unital ring homomorphism. In fact, it follows from the definition of the operations in $\mathbb{Z}_n$ that $\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a) + \varphi(b)$, and, similarly, $\varphi(ab) = [ab] = [a][b] = \varphi(a)\varphi(b)$ for integers a and b.

Example 6.2.3. Let R be any ring with multiplicative identity 1. The map $k \mapsto k\,1$ is a ring homomorphism from $\mathbb{Z}$ to R. The map is just the usual *group* homomorphism from $\mathbb{Z}$ to the additive subgroup $\langle 1 \rangle$ generated by 1; see Example 2.4.7. It is necessary to check that $\langle 1 \rangle$ is closed under multiplication and that this map respects multiplication; that is, $(m\,1)(n\,1) = mn\,1$. This follows from two observations:

First, for any $a \in R$ and $n \in \mathbb{Z}$, $(n\,1)a = n\,a$. This was included in the "elementary deductions" on pages 242–243, following the definition of a ring.

Second, $n\,(m\,a) = nm\,a$; this is just the usual law of powers in a cyclic group. (In a group written with multiplicative notation, this law would be written as $(b^m)^n = b^{mn}$.) See Exercise 2.2.8.

Putting these two observations together, we have $(n\,1)(m\,1) = n\,(m\,1) = nm\,1$.

Warning: Such a homomorphism is not always injective. In fact, the ring homomorphism $k \mapsto [k] = k[1]$ from $\mathbb{Z}$ to $\mathbb{Z}_n$ is a homomorphism of this sort that is not injective.

Example 6.2.4. Consider the ring $C(\mathbb{R})$ of continuous real–valued functions on $\mathbb{R}$. Let S be any subset of R, for example, $S = [0, 1]$. The map $f \mapsto f_{|S}$ that associates to each function its restriction to S is a unital ring homomorphism from $C(\mathbb{R})$ to $C(S)$. Likewise, for

any $t \in \mathbb{R}$ the map $f \mapsto f(t)$ is a unital ring homomorphism from $C(\mathbb{R})$ to $\mathbb{R}$.

Further examples of ring homomorphisms are given in the Exercises.

Evaluation of polynomials

We are used to evaluating polynomials (say with real coefficients) by substituting a number for the variable. For example, if $p(x) = x^2 + 2$, then $p(5) = 5^2 + 2 = 27$. When we do this, we are treating polynomials as functions. The following proposition justifies this practice.

Proposition 6.2.5. *(Substitution principle) Suppose that R and R' are rings with multiplicative identity, with R commutative, and $\varphi : R \to R'$ is a unital ring homomorphism. For each $a \in R'$, there is a unique unital ring homomorphism $\varphi_a : R[x] \to R'$ such that $\varphi_a(r) = \varphi(r)$ for $r \in R$, and $\varphi_a(x) = a$. We have*

$$\varphi_a(\sum_i r_i x^i) = \sum_i \varphi(r_i) a^i.$$

Proof. If φ_a is to be a homomorphism, then it must satisfy

$$\varphi_a(\sum_i r_i x^i) = \sum_i \varphi(r_i) a^i.$$

Therefore, we define φ_a by this formula. It is then straightforward to check that φ_a is a ring homomorphism. ■

There is also a multivariable version of the substitution principle, which formalizes evaluation of polynomials of several variables. Suppose that R and R' are rings with multiplicative identity, with R commutative, and $\varphi : R \to R'$ is a unital ring homomorphism. Given an n–tuple $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ of elements in R', we would like to have a homomorphism from $R[x_1, \ldots, x_n]$ to R' extending φ and sending each x_j to a_j. This only makes sense, however, if the elements a_j are mutually commuting, that is, $a_i a_j = a_j a_i$ for every i and j.

Proposition 6.2.6. *(Multivariable subsitution principle) Suppose that R and R' are rings with multiplicative identity, with R commutative, and $\varphi : R \to R'$ is a unital ring homomorphism. Given an n–tuple $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ of mutually commuting elements in R' there is a unique unital ring homomorphism $\varphi_{\boldsymbol{a}} : R[x_1, \ldots, x_n] \longrightarrow R'$ such that $\varphi_{\boldsymbol{a}}(r) = \varphi(r)$ for $r \in R$ and $\varphi_{\boldsymbol{a}}(x_j) = a_j$ for $1 \leq j \leq n$. We have*

$$\varphi_{\boldsymbol{a}}(\sum_I r_I x^I) = \sum_I \varphi(r_I)\boldsymbol{a}^I,$$

where for a multi-index $I = (i_1, i_2, \ldots, i_n)$, $\boldsymbol{a}^I$ denotes $a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}$.

Proof. The proof is essentially the same as that of the one variable substitution principle. ■

Corollary 6.2.7. *(Evaluation of polynomials) Consider the ring $R[x]$ of polynomials over a commutative ring R with multiplicative identity. For any $a \in R$, there is a unique homomorphisms $\mathrm{ev}_a : R[x] \to R$ with the property that $\mathrm{ev}_a(r) = r$ for $r \in R$ and $\mathrm{ev}_a(x) = a$. We have*

$$\mathrm{ev}_a(\sum_i r_i x^i) = \sum_i r_i a^i.$$

We usually denote $\mathrm{ev}_a(p)$ by $p(a)$.

Corollary 6.2.8. *(Extensions of homomorphisms to polynomial rings) If $\psi : R \to R'$ is a unital homomorphism of commutative rings with multiplicative identity, then there is a unique homomorphism $\tilde{\psi} : R[x] \to R'[x]$ that extends ψ.*

Proof. Apply Proposition 6.2.5 with the following data: Take $\varphi : R \to R'[x]$ to be the composition of $\psi : R \to R'$ with the inclusion of R' into $R'[x]$, and let set $a = x$. By the proposition, there is a unique homomorphism from $R[x]$ to $R'[x]$ extending φ, and sending x to x. The extension is given by the formula

$$\tilde{\psi}(\sum_i s_i x^i) = \sum_i \psi(s_i) x^i.$$

■

Example 6.2.9. Let V be a vector space over K and let $T \in \mathrm{End}_K(V)$. Then

$$\varphi_T : \sum_i \lambda_i x^i \mapsto \sum \lambda_i T^i$$

defines a homomorphism from $K[x]$ to $\mathrm{End}_K(V)$.

What does this mean, and how does it follow from Proposition 6.2.5?

$\mathrm{End}_K(V)$ is a vector space over K as well as a ring. The product of a scalar $\lambda \in K$ and a linear map $S \in \mathrm{End}_K(V)$ is defined by $(\lambda S)(v) = \lambda S(v)$ for $v \in V$. Let I denote the identity endomorphism of V defined by $I(v) = v$. Then $\lambda I(v) = \lambda v$ for $v \in V$.

The map $\varphi : K \longrightarrow \mathrm{End}_K(V)$ given by $\lambda \mapsto \lambda I$ is easily seen to be a unital ring homomorphism from K to $\mathrm{End}_K(V)$. By Proposition 6.2.5, there is a unique homomorphism $\varphi_T : K[x] \longrightarrow \mathrm{End}_K(V)$ with $\varphi_T(x) = T$ and $\varphi_T(\lambda) = \lambda I$. Moreover, $\varphi_T(\sum_i \lambda_i x^i) = \sum_i (\lambda_i I) T^i = \sum_i \lambda_i T^i$. We usually write $p(T)$ for $\varphi_T(p)$.

Example 6.2.10. The map $\sum_i k_i x^i \mapsto \sum_i [k_i] x^i$ is a homomorphism of $\mathbb{Z}[x]$ to $\mathbb{Z}_n[x]$.

Example 6.2.11. Let R be a commutative ring with multiplicative identity element. Then $R[x, y] \cong R[x][y]$. To prove this, we use the one– and two–variable substitution principles to produce homomorphisms from $R[x, y]$ to $R[x][y]$ and from $R[x][y]$ to $R[x, y]$.

We have injective homomorphisms $\varphi_1 : R \longrightarrow R[x]$ and $\varphi_2 : R[x] \longrightarrow R[x][y]$. The composition $\varphi = \varphi_2 \circ \varphi_1$ is an injective homomorphism from R into $R[x]]y]$. By the two variable substitution principle, there is a unique homomorphism $\Phi : R[x, y] \longrightarrow R[x][y]$ which extends φ and sends $x \mapsto x$ and $y \mapsto y$.

Now we produce a map in the other direction. We have an injective homomorphism $\psi : R \longrightarrow R[x, y]$. Applying the one variable substitution principle once gives a homomorphism $\psi_1 : R[x] \longrightarrow R[x, y]$ extending ψ and sending $x \mapsto x$. Applying the one variable substitution principle a second time gives a homomorphism $\Psi : R[x][y] \longrightarrow R[x, y]$ extending ψ_1 and mapping $y \mapsto y$.

Now we have maps in both directions, and we have to check that they are inverses of one another. The homomorphism $\Psi \circ \Phi : R[x, y] \longrightarrow R[x, y]$ is the identity on R and sends $x \mapsto x$ and $y \mapsto y$. By the uniqueness assertion in the two variable substitution principle, $\Psi \circ \Phi$ is the identity homomorphism.

Likewise, $\Phi \circ \Psi : R[x][y] \longrightarrow R[x][y]$ is the identity on R and sends $x \mapsto x$ and $y \mapsto y$. By the uniqueness assertion of the one variable substitution principle, the restriction of $\Phi \circ \Psi$ to $R[x]$ is the injection φ_2 of $R[x]$ into $R[x][y]$. Applying the uniqueness assertion one more time gives that $\Phi \circ \Psi$ is the identity homomorphism.

Ideals

The *kernel* of a ring homomorphism $\varphi : R \to S$ is the set of $x \in R$ such that $\varphi(x) = 0$. Observe that a ring homomorphism is injective if, and only if, its kernel is $\{0\}$, because a ring homomorphism is, in particular, a homomorphism of abelian groups, and the assertion is valid for homomorphisms of abelian groups.

Again extrapolating from our experience with group theory, we would expect the kernel of a ring homomorphism to be a special sort of subring. The following definition captures the special properties of the kernel of a homomorphism.

Definition 6.2.12. An *ideal* I in a ring R is a subgroup of $(R, +)$ satisfying $xr, rx \in I$ for all $x \in I$ and $r \in R$. A *left ideal* I of R is a subgroup of $(R, +)$ such that $rx \in I$ whenever $r \in R$ and $x \in I$. A *right ideal* is defined similarly. Note that for commutative rings, all of these notions coincide.

Proposition 6.2.13. *If $\varphi : R \to S$ is a ring homomorphism, then* $\ker(\varphi)$ *is an ideal of of R.*

Proof. Since φ is a homomorphism of abelian groups, its kernel is a subgroup. If $r \in R$ and $x \in \ker(\varphi)$, then $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0$. Hence $rx \in \ker(\varphi)$. Similarly, , $xr \in \ker(\varphi)$. ■

Example 6.2.14. The kernel of the ring homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ given by $k \mapsto [k]$ is $n\mathbb{Z}$.

Example 6.2.15. Let R be any ring with multiplicative identity element. Consider the unital ring homomorphism from $\mathbb{Z}$ to R defined by $k \mapsto k\,1$. Note that if $k\,1 = 0$, then for all $a \in R$, $k\,a = (k\,1)a = 0\,a = 0$, by the "elementary deductions" on pages 242–243. Therefore the kernel coincides with

$$\{k \in \mathbb{Z} : k\,a = 0 \text{ for all } a \in R\}$$

Since the kernel is a subgroup of $\mathbb{Z}$, it is equal to $n\mathbb{Z}$ for a unique $n \geq 0$, according to Proposition 2.2.21. The integer n is called the *characteristic* of R. The characteristic is 0 if the map $k \mapsto k\,1$ is injective. Otherwise, the characteristic is the least positive integer n such that $n\,1 = 0$.

Warning: Suppose R is a commutative ring with multiplicative identity and that R has positive characteristic n. It follows that the polynomial ring $R[x]$ also has characteristic n, because the multiplicative identity of $R[x]$ coincides with that of R. In particular

$nx = 0$ in $R[x]$. Thus the x of $\mathbb{Z}_4[x]$ and the x of $\mathbb{Z}[x]$ are not the same at all; the former satisfies $4x = 0$, and the latter does not.

Example 6.2.16. Consider the situation of Corollary 6.2.8. That is, $\psi : R \to R'$ is a unital homomorphism of commutative rings with multiplicative identity, and $\tilde{\psi} : R[x] \to R'[x]$ is the extension of ψ with $\tilde{\psi}(x) = x$. Then the kernel of $\tilde{\psi}$ is the collection of polynomials with coefficients in $\ker(\psi)$. (Proof: $\sum_i s_i x^i \in \ker(\tilde{\psi}) \iff \sum_i \psi(s_i)x^i = 0 \iff \psi(s_i) = 0$ for all $i \iff s_i \in \ker(\psi)$ for all i.) In particular, $\tilde{\psi}$ is injective if, and only if, ψ is injective.

For example, the kernel of the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}_n[x]$ given by $\sum_i k_i x^i \mapsto \sum_i [k_i]x^i$ is the set of polynomials all of whose coefficients are divisible by n.

Example 6.2.17. The kernel of the ring homomorphism $K[x] \to K$ given by $p \mapsto p(a)$ is the set of all polynomials p having a as a root.

Example 6.2.18. The kernel of the ring homomorphism $C(\mathbb{R}) \to C(S)$ given by $f \mapsto f_{|S}$ is the set of all continuous functions whose restriction to S is zero.

Example 6.2.19. Let K be a field. Define a map φ from $K[x]$ to $\mathrm{Fun}(K, K)$, the ring of K–valued functions on K by $\varphi(p)(a) = p(a)$. (That is, $\varphi(p)$ is the polynomial function on K corresponding to the polynomial p.) Then φ is a ring homomorphism. The homomorphism property of φ follows from the homomorphism property of $p \mapsto p(a)$ for $a \in K$. Thus $\varphi(p + q)(a) = (p + q)(a) = p(a) + q(a) = \varphi(p)(a)+\varphi(q)(a) = (\varphi(p)+\varphi(q))(a)$, and similarly for multiplication.

The kernel of φ is the set of polynomials p such that $p(a) = 0$ for all $a \in K$. If K is infinite, then the kernel is $\{0\}$, since no nonzero polynomial with coefficients in a field has infinitely many roots.

If K is finite, then φ is *never* injective. That is, there always exist nonzero polynomials $p \in K[x]$ such that $p(a) = 0$ for all $a \in K$. Indeed, we need merely take $p(x) = \prod_{a \in K}(x - a)$.

Definition 6.2.20. A ring R with no ideals other than $\{0\}$ and R itself is said to be *simple*.

Any field is a simple ring. You are asked to verify this in Exercise 6.2.10.

In Exercise 6.2.11, you are asked to show that the ring M of n-by-n matrices with real entries is simple. This holds equally well for matrix rings over any field.

Proposition 6.2.21.

(a) *Let $\{I_\alpha\}$ be any collection of ideals in a ring R. Then $\bigcap_\alpha I_\alpha$ is an ideal of R.*

(b) *Let I_n be an increasing sequence of ideals in a ring R. Then $\bigcup_n I_n$ is an ideal of R.*

Proof. Part (a) is an Exercise 6.2.17. For part (b), let $x, y \in I = \bigcup_n I_n$. Then there exist $k, \ell \in \mathbb{N}$ such that $x \in I_k$ and $y \in I_\ell$. If $n = \max\{k, \ell\}$, then $x \in I_k \subseteq I_n$ and $y \in I_\ell \subseteq I_n$. Therefore, $x + y \in I_n \subseteq I$. If $x \in I$ and $r \in R$, then there exists $n \in \mathbb{N}$ such that $x \in I_n$. Then $rx, xr \in I_n \subseteq I$. Thus I is an ideal. ■

The analogues of parts (a) and (b) of the Proposition 6.2.21 hold for left and right ideals as well.

Proposition 6.2.22.

(a) *Let I and J be two ideals in a ring R. Then*

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_sb_s : s \geq 1, a_i \in I, b_i \in J\}$$

is an ideal in R, and $IJ \subseteq I \cap J$.

(b) *Let I and J be two ideals in a ring R. Then $I + J = \{a + b : a \in I \text{ and } b \in J\}$ is an ideal in R.*

Proof. Exercises 6.2.18 and 6.2.19. ■

Ideals generated by subsets

Next we investigate ideals, or one–sided ideals, generated by a subset of a ring.

Proposition 6.2.23. *Let R be a ring and $\mathcal{S}$ a subset of R. Let $\langle \mathcal{S} \rangle$ denote the additive subgroup of R generated by $\mathcal{S}$.*

(a) *Define*

$$R\mathcal{S} = \{r_1s_1 + r_2s_2 + \cdots + r_ns_n : n \in \mathbb{N}, r_i \in R, s_i \in \mathcal{S}\}.$$

Then $R\mathcal{S}$ is a left ideal of R.

(b) *$\langle \mathcal{S} \rangle + R\mathcal{S}$ is the smallest left ideal of R containing $\mathcal{S}$, and is equal to the intersection of all left ideals of R containing $\mathcal{S}$.*

(c) *In case R has an identity element, $R\mathcal{S} = \langle \mathcal{S} \rangle + R\mathcal{S}$.*

Proof. It is straightforward to check that $R\mathcal{S}$ is a left ideal. $\langle\mathcal{S}\rangle + R\mathcal{S}$ is a sum of subgroups R, so it is a subgroup. Moreover, for $r \in R$, we have $r\langle\mathcal{S}\rangle \subseteq R\mathcal{S}$. It follows from this that $\langle\mathcal{S}\rangle + R\mathcal{S}$ is a left ideal. If J is any left ideal of R containing $\mathcal{S}$, then $J \supseteq \langle\mathcal{S}\rangle$, because J is a subgroup of R. Since J is a left ideal, $J \supseteq R\mathcal{S}$ as well. Therefore $J \supseteq \langle\mathcal{S}\rangle + R\mathcal{S}$. This shows that $\langle\mathcal{S}\rangle + R\mathcal{S}$ is the smallest left ideal containing $\mathcal{S}$. The intersection of all left ideals of R containing $\mathcal{S}$ is also the smallest left ideal of R containing $\mathcal{S}$, so (b) follows. Finally, if R has an identity element, then $\mathcal{S} \subseteq R\mathcal{S}$, so $\langle\mathcal{S}\rangle \subseteq R\mathcal{S}$, which implies (c). ■

Definition 6.2.24. The smallest left ideal containing a subset $\mathcal{S}$ is called the *left ideal generated by* $\mathcal{S}$. The smallest left ideal containing a single element $x \in R$ is called the *principal left ideal* generated by x.

When R has an identity element the principal left ideal generated by x is just $Rx = \{rx : r \in R\}$. See Exercise 6.2.8

Proposition 6.2.23 and Definition 6.2.24 have evident analogues for right ideals. The following is the analogue for two-sided ideals:

Proposition 6.2.25. *Let R be a ring and $\mathcal{S}$ a subset of R. Let $\langle\mathcal{S}\rangle$ denote the additive subgroup of R genertated by $\mathcal{S}$.*

(a) *Define*

$$R\mathcal{S}R = \{a_1 s_1 b_1 + a_2 s_2 b_2 + \cdots + a_n s_n b_n : n \in \mathbb{N}, a_n, b_n \in R\}.$$

Then $R\mathcal{S}R$ is a two-sided ideal.

(b) *$\langle\mathcal{S}\rangle + R\mathcal{S}R$ is the smallest ideal of R containing $\mathcal{S}$, and is equal to the interesection of all ideals of R containing $\mathcal{S}$*

(c) *If R has an identity element , then $\langle\mathcal{S}\rangle + R\mathcal{S}R = R\mathcal{S}R$.*

Proof. Essentially the same as the proof of Proposition 6.2.23. ■

Definition 6.2.26. The smallest ideal containing a subset $\mathcal{S}$ is called the *ideal generated by* $\mathcal{S}$, and is denoted by (S). The smallest ideal containing a single element $x \in R$ is called the *principal ideal* generated by x and is denoted by (x).

When R has an identity element, the principal ideal generated by $x \in R$ is

$$(x) = \{a_1 x b_1 + a_2 x b_2 + \cdots + a_n x b_n : n \in \mathbb{N}, a_i, b_i \in R\}.$$

See Exercise 6.2.9. When R is commutative with identity, ideals and left ideals coincide, so

$$(x) = Rx = \{rx : r \in R\}.$$

The ideal generated by $\mathcal{S}$ is, in general, larger than the subring generated by $\mathcal{S}$; for example, the subring generated by the identity element consists of integer multiples of the identity, but the ideal generated by the identity element is all of R.

Ideals in $\mathbb{Z}$ and in $K[x]$

In the ring of integers, and in the ring $K[x]$ of polynomials in one variable over a field, *every ideal is principal*:

Proposition 6.2.27.

(a) *For a subset $S \subseteq \mathbb{Z}$, the following are equivalent:*
  (i) *S is a subgroup of $\mathbb{Z}$.*
  (ii) *S is a subring of $\mathbb{Z}$.*
  (iii) *S is an ideal of $\mathbb{Z}$.*

(b) *Every ideal in the ring of integers is principal.*

(c) *Every ideal in $K[x]$, where K is a field, is principal.*

Proof. Clearly an ideal is always a subring, and a subring is always a subgroup. If S is a nonzero subgroup of $\mathbb{Z}$, then $S = \mathbb{Z}d$, where d is the least positive element of S, according to Proposition 2.2.21. If $S = \{0\}$, then $S = \mathbb{Z}0$. In either case, S is a principal ideal of $\mathbb{Z}$. This proves (a) and (b).

The proof of (c) is similar to that of Proposition 2.2.21. The zero ideal of $K[x]$ is clearly principal. Let J be a nonzero ideal, and let $f \in J$ be a nonzero element of least degree in J. If $g \in J$, write $g = qf + r$, where $q \in K[x]$, and $\deg(r) < \deg(f)$. Then $r = g - qf \in J$. Since $\deg(r) < \deg(f)$ and f was a nonzero element of least degree in J, it follows that $r = 0$. Thus $g = qf \in K[x]f$. Since g was an arbitrary element of J, $J = K[x]f$. ■

Direct Sums

Consider a direct sum of rings $R = R_1 \oplus \cdots \oplus R_n$. For each i, set $\tilde{R}_i = \{0\} \oplus \cdots \oplus \{0\} \oplus R_i \oplus \{0\} \oplus \cdots \oplus \{0\}$. Then $\tilde{R}_i$ is an ideal of R.

How can we recognize that a ring R is isomorphic to the direct sum of several subrings $A_1, A_2, \ldots, A_n$? On the one hand, according to the previous example, the component subrings must actually be ideals. On the other hand, the ring must be isomorphic to the direct

product of the A_i, regarded as abelian groups. These conditions suffice.

Proposition 6.2.28. *Let R be a ring with ideals $A_1, \dots A_s$ such that $R = A_1 + \cdots + A_s$. Then the following conditions are equivalent:*

(a) *$(a_1, \dots, a_s) \mapsto a_1 + \cdots + a_s$ is a group isomorphism of $A_1 \times \cdots \times A_s$ onto R.*

(b) *$(a_1, \dots, a_s) \mapsto a_1 + \cdots + a_s$ is a ring isomorphism of $A_1 \oplus \cdots \oplus A_s$ onto R.*

(c) *Each element $x \in R$ can be expressed as a sum $x = a_1 + \cdots + a_s$, with $a_i \in A_i$ for all i, in exactly one way.*

(d) *If $0 = a_1 + \cdots + a_s$, with $a_i \in A_i$ for all i, then $a_i = 0$ for all i.*

Proof. The equivalence of (a), (c), and (d) is by Proposition 3.3.1. Clearly (b) implies (a). Let us assume (a) and show that the map

$$(a_1, \dots, a_s) \mapsto a_1 + \cdots + a_s$$

is actually a ring isomorphism. We have $A_i A_j \subseteq A_i \cap A_j = \{0\}$ if $i \neq j$ (using condition (d)). Therefore,

$$(a_1 + \cdots + a_s)(b_1 + \cdots + b_s) = a_1 b_1 + \cdots + a_s b_s,$$

whenever $a_i, b_i \in A_i$ for all i. It follows that the map is a ring isomorphism. ■

Exercises 6.2

6.2.1. Show that $A \mapsto \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$ and $A \mapsto \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}$ are homomorphisms of the ring of 2-by-2 matrices into the ring of 4-by-4 matrices. The former is unital, but the latter is not.

6.2.2. Define a map φ from the ring $\mathbb{R}[x]$ of polynomials with real coefficients into the ring M of 3-by-3 matrices by

$$\varphi(\sum a_i x^i) = \begin{bmatrix} a_0 & a_1 & a_2 \\ 0 & a_0 & a_1 \\ 0 & 0 & a_0 \end{bmatrix}.$$

Show that φ is a unital ring homomorphism. What is the kernel of this homomorphism?

6.2.3. If $\varphi : R \to S$ is a ring homomorphism and R has an identity element 1, show that $e = \varphi(1)$ satisfies $e^2 = e$ and $ex = xe = exe$ for all $x \in \varphi(R)$.

6.2.4. Show that if $\varphi : R \to S$ is a ring homomorphism, then $\varphi(R)$ is a subring of S.

6.2.5. Show that if $\varphi : R \to S$ and $\psi : S \to T$ are ring homomorphisms, then the composition $\psi \circ \varphi$ is a ring homomorphism.

6.2.6. Let S be a subset of a set X. Let R be the ring of real–valued functions on X, and let I be the set of real–valued functions on X whose restriction to S is zero. Show that I is an ideal in R.

6.2.7. Let R be the ring of 3-by-3 upper triangular matrices and I be the set of upper triangular matrices that are zero on the diagonal. Show that I is an ideal in R.

6.2.8. Show that if R is a ring with identity element and $x \in R$, then $Rx = \{rx : r \in R\}$ is the principal left ideal generated by x Similarly, $xR = \{xr : r \in R\}$ is the principal right ideal generated by x.

6.2.9. Show that if R is a ring with identity, then the principal ideal generated by $x \in R$ is

$$(x) = \{a_1xb_1 + a_2xb_2 + \cdots + a_nxb_n : n \in \mathbb{N}, a_i, b_i \in R\}.$$

6.2.10. Show that any field is a simple ring.

6.2.11. Show that the ring M of n-by-n matrices over $\mathbb{R}$ has no ideals other than 0 and M. Conclude that any ring homomorphism $\varphi : M \to S$ is either identically zero or is injective. *Hint:* To begin with, work in the 2-by-2 or 3-by-3 case; when you have done these cases, you will understand the general case as well. Let I be a nonzero ideal, and let $x \in I$ be a nonzero element. Introduce the matrix units E_{ij}, which are matrices with a 1 in the (i, j) position and zeros elsewhere. Observe that the set of E_{ij} is a basis for the linear space of matrices. Show that $E_{ij}E_{kl} = \delta_{jk}E_{il}$. Note that the identity E matrix satisfies $E = \sum_{i=1}^{n} E_{ii}$, and write $x = ExE = \sum_{i,j} E_{ii}xE_{jj}$. Conclude that $y = E_{ii}xE_{jj} \neq 0$ for some pair (i, j). Now, since y is a matrix, it is possible to write $y = \sum_{r,s} y_{rs}E_{r,s}$. Conclude that $y = y_{i,j}E_{i,j}$, and $y_{i,j} \neq 0$, and that, therefore, $E_{ij} \in I$. Now use the multiplication rules for the matrix units to conclude that $E_{rs} \in I$ for all (r, s), and hence $I = M$.

6.2.12. An element e of a ring is called an *idempotent* if $e^2 = e$. What are the idempotents in the ring of real–valued functions on a set X? What are the idempotents in the ring of *continuous* real–valued functions on $[0, 1]$?

6.2.13. Find a nontrivial idempotent (i.e., an idempotent different from 0 or 1) in the ring of 2-by-2 matrices with real entries.

6.2.14. Let e be a nontrivial idempotent in a commutative ring R with identity. Show that $R \cong Re \oplus R(1-e)$ as rings.

6.2.15. Find a nontrivial idempotent e in the ring $\mathbb{Z}_{35}$. Show that the decomposition $\mathbb{Z}_{35} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_7$ corresponds to the decomposition $\mathbb{Z}_{35} = \mathbb{Z}_{35}e \oplus \mathbb{Z}_{35}(1-e)$.

6.2.16. Show that a nonzero homomorphism of a simple ring is injective. In particular, a nonzero homomorphism of a field is injective.

6.2.17. Show that the intersection of any family of ideals in a ring is an ideal. Show that the ideal generated by a subset $\mathcal{S}$ of a ring R is the intersection of all ideals J of R such that $\mathcal{S} \subseteq J \subseteq R$.

6.2.18. Let I and J be two ideals in a ring R. Show that

$$I + J = \{a + b : a \in I \text{ and } b \in J\}$$

is an ideal in R.

6.2.19. Let I and J be two ideals in a ring R. Show that

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_sb_s : s \geq 1, a_i \in I, b_i \in J\}$$

is an ideal in R, and $IJ \subseteq I \cap J$.

6.2.20. Let R be a ring without identity and $a \in R$. Show that the ideal generated by a in R is equal to $\mathbb{Z}a + Ra + aR + RaR$, where $\mathbb{Z}a$ is the abelian subgroup generated by a, $Ra = \{ra : r \in R\}$, and so on. Show that if R is commutative, then the ideal generated by a is $\mathbb{Z}a + Ra$.

6.2.21. Let M be an ideal in a ring R with identity, and $a \in R \setminus M$. Show that $M + RaR$ is the ideal generated by M and a. How must this statement be altered if R does not have an identity?

6.2.22. Let R be a ring without identity. This exercise shows how R can be imbedded as an ideal in a ring with identity.

(a) Let $\tilde{R} = \mathbb{Z} \times R$, as an abelian group. Give $\tilde{R}$ the multiplication

$$(n, r)(m, s) = (nm, ns + mr + rs).$$

Show that this makes $\tilde{R}$ into a ring with multiplicative identity $(1, 0)$.

(b) Show that $r \mapsto (0, r)$ is a ring isomorphism of R into $\tilde{R}$ with image $\{0\} \times R$. Show that $\{0\} \times R$ is an ideal in $\tilde{R}$.

(c) Show that if $\varphi : R \longrightarrow S$ is a homomorphism of R into a ring S with multiplicative identity 1, then there is a unique homomorphism $\tilde{\varphi} : \tilde{R} \longrightarrow S$ such that $\tilde{\varphi}((0, r)) = \varphi(r)$ and $\tilde{\varphi}((1, 0)) = 1$.

6.3. Quotient Rings

In Section 2.7, it was shown that given a group G and a normal subgroup N, we can construct a quotient group G/N and a natural homomorphism from G onto G/N. The program of Section 2.7 can be carried out more or less verbatim with rings and ideals in place of groups and normal subgroups:

For a ring R and an ideal I, we can form the quotient *group* R/I, whose elements are cosets $a + I$ of I in R. The additive group operation in R/I is $(a+I)+(b+I) = (a+b)+I$. Now attempt to define a multiplication in R/I in the obvious way: $(a+I)(b+I) = (ab+I)$. We have to check that this this is well defined. But this follows from the closure of I under multiplication by elements of R; namely, if $a + I = a' + I$ and $b + I = b' + I$, then

$$(ab - a'b') = a(b - b') + (a - a')b' \in aI + Ib \subseteq I.$$

Thus, $ab+I = a'b'+I$, and the multiplication in R/I is well defined.

Theorem 6.3.1. *If I is an ideal in a ring R, then R/I has the structure of a ring, and the quotient map $a \mapsto a + I$ is a surjective ring homomorphism from R to R/I with kernel equal to I. If R has a multiplicative identity, then so does R/I, and the quotient map is unital.*

Proof. Once we have checked that the multiplication in R/I is well defined, it is straightforward to check the ring axioms. Let us include one verification for the sake of illustration. Let $a, b, c \in R$. Then

$$\begin{aligned}(a + I)((b + I) + (c + I)) &= (a + I)(b + c + I) = a(b + c) + I \\ &= ab + ac + I = (ab + I) + (ac + I) \\ &= (a + I)(b + I) + (a + I)(c + I).\end{aligned}$$

We know that the quotient map $a \mapsto a + I$ is a surjective homomorphism of abelian groups with kernel I. It follows immediately from the definition of the product in R/I that the map also respects multiplication:

$$ab \mapsto ab + I = (a + I)(b + I)$$

Finally, if 1 is the multiplicative identity in R, then $1 + I$ is the multiplicative identity in R/I. ■

Example 6.3.2. The ring $\mathbb{Z}_n$ is the quotient of the ring $\mathbb{Z}$ by the principal ideal $n\mathbb{Z}$. The homomorphism $a \mapsto [a] = a + n\mathbb{Z}$ is the quotient homomorphism.

Example 6.3.3. For K a field, any ideal in $K[x]$ is of the form $(f) = fK[x]$ for some polynomial f according to Proposition 6.2.27. For any $g(x) \in K[x]$, there exist polynomials q, r such that $g(x) = q(x)f(x) + r(x)$, and $\deg(r) < deg(f)$. Thus $g(x) + (f) = r(x) + (f)$. In other words, $K[x]/(f) = \{r(x) + (f) : \deg(r) < \deg(f)\}$. The multiplication in $K[x]/(f)$ is as follows: Given polynomials $r(x)$ and $s(x)$ each of degree less than the degree of f,the product $(r(x) + (f))(s(x) + (f)) = r(x)s(x) + (f) = a(x) + (f)$, where $a(x)$ is the remainder upon division of $r(x)s(x)$ by $f(x)$.

Let's look at the particular example $K = \mathbb{R}$ and $f(x) = x^2 + 1$. Then $\mathbb{R}[x]/(f)$ consists of cosets $a + bx + (f)$ represented by linear polynomials. Furthermore, we have the computational rule

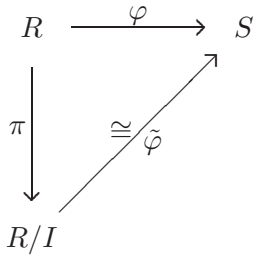
$$x^2 + (f) = x^2 + 1 - 1 + (f) = -1 + (f).$$

Thus

$$(a + bx + (f))(a' + b'x + (f)) = (aa' - bb') + (ab' + a'b)x + (f).$$

All of the homomorphism theorems for groups, which were presented in Section 2.7, have analogues for rings. The basic homomorphism theorem for rings is the following.

Theorem 6.3.4. *(Homomorphism theorem for rings). Let $\varphi : R \longrightarrow S$ be a surjective homomorphism of rings with kernel I. Let $\pi : R \longrightarrow R/I$ be the quotient homomorphism. There is a ring isomorphism $\tilde{\varphi} : R/I \longrightarrow S$ satisfying $\tilde{\varphi} \circ \pi = \varphi$. (See the following diagram.)*



Proof. The homomorphism theorem for groups (Theorem 2.7.6) gives us an isomorphism of abelian groups $\tilde{\varphi} : R/I \to S$ satisfying

$\tilde{\varphi} \circ \pi = \varphi$. We have only to verify that $\tilde{\varphi}$ also respects multiplication. But this follows at once from the definition of the product on R/I:

$$\begin{aligned}\tilde{\varphi}(a+I)(b+I) &= \tilde{\varphi}(ab+I) \\ &= \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(a+I)\tilde{\varphi}(b+I).\end{aligned}$$

■

Example 6.3.5. Define a homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{C}$ by evaluation of polynomials at $i \in \mathbb{C}$, $\varphi(g(x)) = g(i)$. For example, $\varphi(x^3 - 1) = i^3 - 1 = -i - 1$. This homomorphism is surjective because $\varphi(a + bx) = a + bi$. The kernel of φ consists of all polynomials g such that $g(i) = 0$. The kernel contains at least the ideal $(x^2 + 1) = (x^2 + 1)\mathbb{R}[x]$ because $i^2 + 1 = 0$. On the other hand, if $g \in \ker(\varphi)$, write $g(x) = (x^2 + 1)q(x) + (a + bx)$; evaluating at i, we get $0 = a + bi$, which is possible only if $a = b = 0$. Thus g is a multiple of x^2+1. That is $\ker(\varphi) = (x^2+1)$. By the homomorphism theorem for rings, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ as rings. In particular, since $\mathbb{C}$ is a field, $\mathbb{R}[x]/(x^2 + 1)$ is a field. Note that we have already calculated explicitly in Example 6.3.3 that multiplication in $\mathbb{R}[x]/(x^2+1)$ satisfies the same rule as multiplication in $\mathbb{C}$.

Example 6.3.6. Let R be a ring with identity containing ideals B_1, $\ldots, B_s$. Let $B = \cap_i B_i$. Suppose that $B_i + B_j = R$ for all $i \neq j$. Then $R/B \cong R/B_1 \oplus \cdots \oplus R/B_s$. In fact, $\varphi : r \mapsto (r + B_1, \ldots, r + B_s)$ is a homomorphism of R *into* $R/B_1 \oplus \cdots \oplus R/B_s$ with kernel B, so $R/B \cong \varphi(R)$. The problem is to show that φ is surjective. Fix i and for each $j \neq i$ find $r'_j \in B_i$ and $r_j \in B_j$ such that $r'_j + r_j = 1$. Consider the product of all the $(r'_j + r_j)$ (in any order). When the product is expanded, all the summands except for one contain at least one factor r'_j in the ideal B_i, so all of these summands are in B_i. The remaining summand is the product of all of the $r_j \in B_j$, so it lies in $\cap_{j \neq i} B_j$. Thus we get $1 = a_i + b_i$, where $b_i \in B_i$ and $a_i \in \cap_{j \neq i} B_j$. The image of a_i in R/B_j is zero for $j \neq i$, but $a_i + B_i = 1 + B_i$. Now if $(r_1, \ldots, r_s)$ is an arbitrary sequence of elements of R, then $\varphi(r_1 a_1 + r_2 a_2 + \cdots + r_s a_s) = (r_1 + B_1, r_2 + B_2, \ldots, r_s + B_s)$, so φ is surjective.

Proposition 6.3.7. *(Correspondence theorem for rings) Let $\varphi : R \longrightarrow \overline{R}$ be a ring homomorphism of R* onto *$\overline{R}$, and let J denote its kernel. Under the bijection $B \mapsto \varphi^{-1}(B)$ between subgroups of $\overline{R}$ and subgroups of R containing J, subrings correspond to subrings and ideals to ideals.*

Proof. According to Proposition 2.7.12, $\overline{B} \mapsto \varphi^{-1}(\overline{B})$ is a bijection between the subgroups of $\overline{R}$ and the subgroups of R containing J. We leave it as an exercise (Exercise 6.3.3) to show that this bijection carries subrings to subrings and ideals to ideals. ■

Each of the next three results is an analogue for rings of a homomorphism theorem for groups that was presented in Section 2.7. Each can be proved either by using the corresponding result for groups and verifying that the maps respect multiplication, or by adapting the proof of the proposition for groups.

Proposition 6.3.8. *Let $\varphi : R \longrightarrow \overline{R}$ be a surjective ring homomorphism with kernel J. Let $\bar{I}$ be an ideal of $\overline{R}$ and let $I = \varphi^{-1}(\bar{I})$. Then $x + I \mapsto \varphi(x) + \bar{I}$ is a ring isomorphism of R/I onto $\overline{R}/\bar{I}$. Equivalently,*

$$(R/J)/(I/J) \cong R/I$$

as rings.

Proof. By Proposition 2.7.13, the map $x + I \mapsto \varphi(x) + \bar{I}$ is a group isomorphism from $(R/I, +)$ to $(\overline{R}/\overline{I}, +)$. But the map also respects multiplication, as

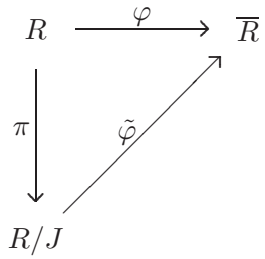
$$(x + I)(y + I) = xy + I \mapsto \varphi(xy) + \bar{I} = (\varphi(x) + \bar{I})(\varphi(y) + \bar{I}).$$

We can identify $\overline{R}$ with R/J by the homomorphism theorem for rings, and this identification carries $\bar{I}$ to the image of I in R/J, namely I/J. Therefore,

$$(R/J)/(I/J) \cong \overline{R}/\bar{I} \cong R/I.$$

■

Proposition 6.3.9. *Let $\varphi : R \to \overline{R}$ be a surjective homomorphism of rings with kernel I. Let $J \subseteq I$ be an ideal of R, and let $\pi : R \to R/J$ denote the quotient map. Then there is a surjective homomorphism $\tilde{\varphi} : R/J \to \overline{R}$ such that $\tilde{\varphi} \circ \pi = \varphi$. (See the following diagram.) The kernel of $\tilde{\varphi}$ is $I/J \subseteq R/J$.*



Proof. By Proposition 2.7.14, $\tilde{\varphi} : x + J \mapsto \varphi(x)$ defines a group homomorphism from R/J to $\overline{R}$ with kernel I/J. We only have to check that the map respects multiplication. This follows from the computation:

$$\begin{aligned}\tilde{\varphi}((x+J)(y+J)) &= \tilde{\varphi}(xy+J) = \varphi(xy)\\ &= \varphi(x)\varphi(y) = \tilde{\varphi}(x+I)\tilde{\varphi}(y+I).\end{aligned}$$

■

Proposition 6.3.10. *Let $\varphi : R \longrightarrow \overline{R}$ be a surjective homomorphism of rings with kernel I. Let A be a subring of R. Then $\varphi^{-1}(\varphi(A)) = A + I = \{a + r : a \in A \text{ and } r \in I\}$. $A + I$ is a subring of R containing I, and*

$$(A + I)/I \cong \varphi(A) \cong A/(A \cap I).$$

Proof. Exercise 6.3.5. ■

An ideal M in a ring R is called *proper* if $M \neq R$ and $M \neq \{0\}$.

Definition 6.3.11. An ideal M in a ring R is called *maximal* if $M \neq R$ there are no ideals strictly between M and R; that is, the only ideals containing M are M and R.

Recall that a ring is called simple if it has no ideals other than the trivial ideal $\{0\}$ and the whole ring; so a nonzero ring is simple precisely when $\{0\}$ is a maximal ideal.

Proposition 6.3.12. *A proper ideal M in R is maximal if, and only if, R/M is simple.*

Proof. Exercise 6.3.6. ■

Proposition 6.3.13. *A (nonzero) commutative ring R with multiplicative identity is a field if, and only if, R is simple.*

Proof. Suppose R is simple and $x \in R$ is a nonzero element. The ideal Rx is nonzero since $x = 1x \in Rx$; because R is simple, $R = Rx$. Hence there is a $y \in R$ such that $1 = yx$. Conversely, suppose R is a field and M is a nonzero ideal. Since M contains a nonzero element x, it also contains $r = rx^{-1}x$ for any $r \in R$; that is, $M = R$. ■

Corollary 6.3.14. *If M is a proper ideal in a commutative ring R with 1, then R/M is a field if, and only if, M is maximal.*

Proof. This follows from Propositions 6.3.12 and 6.3.13. ■

Exercises 6.3

6.3.1. Work out the rule of computation in the ring $\mathbb{R}[x]/(f)$, where $f(x) = x^2 - 1$. Note that the quotient ring consists of elements $a + bx + (f)$. Compare Example 6.3.3.

6.3.2. Work out the rule of computation in the ring $\mathbb{R}[x]/(f)$, where $f(x) = x^3 - 1$. Note that the quotient ring consists of elements $a + bx + cx^2 + (f)$. Compare Example 6.3.3.

6.3.3. Prove Proposition 6.3.7.

6.3.4. Give another proof of Proposition 6.3.8, by adapting the proof of Proposition 2.7.13, rather than appealing to the result of Proposition 2.7.13.

6.3.5. Prove Proposition 6.3.10, following the pattern of the proof of Proposition 2.7.18.

6.3.6. Prove that an ideal M in R is maximal if, and only if, R/M is simple.

6.3.7.

(a) Show that $n\mathbb{Z}$ is maximal ideal in $\mathbb{Z}$ if, and only if, $\pm n$ is a prime.

(b) Show that $(f) = fK[x]$ is a maximal ideal in $K[x]$ if, and only if, f is irreducible.

(c) Conclude that $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is a field if, and only if, $\pm n$ is prime, and that $K[x]/(f)$ is a field if, and only if, f is irreducible.

6.3.8. If J is an ideal of the ring R, show that $J[x]$ is an ideal in $R[x]$ and furthermore $R[x]/J[x] \cong (R/J)[x]$. *Hint:* Find a natural homomorphism from $R[x]$ onto $(R/J)[x]$ with kernel $J[x]$.

6.3.9. For any ring R, and any natural number n, we can define the matrix ring $\mathrm{Mat}_n(R)$ consisting of n-by-n matrices with entries in R. If J is an ideal of R, show that $\mathrm{Mat}_n(J)$ is an ideal in $\mathrm{Mat}_n(R)$ and furthermore $\mathrm{Mat}_n(R)/\mathrm{Mat}_n(J) \cong \mathrm{Mat}_n(R/J)$. *Hint:* Find a natural homomorphism from $\mathrm{Mat}_n(R)$ onto $\mathrm{Mat}_n(R/J)$ with kernel $\mathrm{Mat}_n(J)$.

6.3.10. Let R be a commutative ring. Show that $R[x]/xR[x] \cong R$.

6.3.11. This exercise gives a version of the *Chinese remainder theorem.*

(a) Let R be a ring, P and Q ideals in R, and suppose that $P \cap Q = \{0\}$, and $P + Q = R$. Show that the map $x \mapsto (x + P, x + Q)$ is an isomorphism of R onto $R/P \oplus R/Q$. *Hint:* Injectivity is clear. For surjectivity, show that for each $a, b \in R$, there exist $x \in R$, $p \in P$, and $q \in Q$ such that $x + p = a$, and $x + q = b$.

(b) More generally, if $P + Q = R$, show that $R/(P \cap Q) \cong R/P \oplus R/Q$.

6.3.12.

(a) Show that integers m and n are relatively prime if, and only if, $m\mathbb{Z}+n\mathbb{Z} = \mathbb{Z}$ if, and only if, $m\mathbb{Z}\cap n\mathbb{Z} = mn\mathbb{Z}$. Conclude that if m and n are relatively prime, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ as rings.

(b) State and prove a generalization of this result for the ring of polynomials $K[x]$ over a field K.

6.4. Integral Domains

Definition 6.4.1. An integral domain is a commutative ring with identity element 1 in which the product of any two nonzero elements is nonzero.

You may think at first that the product of nonzero elements in a ring is always nonzero, but you already know of examples where this is not the case! Let R be the ring of real–valued functions on a set X and let A be a proper subset of X. Let f be the characteristic function of A, that is, the function satisfying $f(a) = 1$ if $a \in A$ and $f(x) = 0$ if $x \in X \setminus A$. Then f and $1 - f$ are nonzero elements of R whose product is zero.

For another example, let x be the 2-by-2 matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Compute that $x \neq 0$ but $x^2 = 0$. (An element n in a ring is said to be *nilpotent* if $n^k = 0$ for some k.)

Example 6.4.2.

(a) The ring of integers $\mathbb{Z}$ is an integral domain.

(b) Any field is an integral domain.

(c) If R is an integral domain, then $R[x]$ is an integral domain. In particular, $K[x]$ is an integral domain for any field K.