Module MA3411: Commentary
Rings
Michaelmas Term 2009

D. R. Wilkins

Contents

B Rings

B-1 Finitely Generated Ideals

Lemma 2.5 describes the elements of a finitely-generated ideal of a unital commutative ring.

Note that the proof does not generalize to non-commutative rings. (It is suggested that you review the proof in order to identify the point at which the requirement that the ring be commutative is applied.)

To explore further the case of non-commutative rings, let $M_2(\mathbb{R})$ be the ring of 2×2 matrices with real coefficients, and let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Then the ideal of $M_2(\mathbb{R})$ generated by A contains all four matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

(To verify this, you can check that the second and third of these are obtained from the first by multiplying on the left and on the right respectively by suitably-chosen matrices and therefore belong to the ideal generated by the first. One can then multiply the second and third together in that order to obtain the fourth.) Therefore the ideal of $M_2(\mathbb{R})$ generated by the matrix A is the whole of $M_2(\mathbb{R})$. On the other hand, the set $\{BA : B \in M_2(\mathbb{R})\}$ consists of all 2×2 matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ with $a, b \in \mathbb{R}$.

B-2 Quotient Rings

Let R be a ring, and let I be an ideal of R. Then the ideal I determines a corresponding quotient ring R/I of R. We now discuss the construction of this quotient ring. The basic observations are summarized below.

- Each ideal I of the ring R determines a corresponding relation $\sim_I$ on R, where elements x and y of R satisfy $x \sim_I y$ if and only if $x - y \in I$.
- The definition of ideals ensures that this relation $\sim_I$ is an equivalence relation.
- Because this relation $\sim_I$ is an equivalence relation on R, it partitions R into equivalence classes; these equivalence classes are the cosets of I in R.
- These equivalence classes, or cosets, can be regarded as objects in their own right, and are the elements of a set which we denote by R/I.

- The requirement that the addition operation on R be both commutative and associative ensures that if x, x', y and y' are elements of R, and if $x \sim_I x'$ and $y \sim_I y'$, then $x + y \sim_I x' + y'$. Therefore there is a well-defined operation of addition defined on the set R/I of equivalence classes induced by the operation of addition on the ring R itself.

- The definition of ideals also ensures that if x, x', y and y' are elements of R, and if $x \sim_I x'$ and $y \sim_I y'$, then $xy \sim_I x'y'$. Therefore there is a well-defined operation of multiplication defined on the set R/I equivalence classes induced by the operation of multiplication on the ring R itself.

- The set R/I, with the operations of addition and multiplication induced by the corresponding binary operations on R, satisfies the ring axioms, and is thus itself a ring. The zero element of this quotient ring R/I is the ideal I, where this ideal is regarded as a coset of itself. The negative of the coset $I + x$ containing some element x of R is the coset $I - x$ containing the element $-x$.

- If R is a unital ring, then so is R/I, and the multiplicative identity element of R/I is $I + 1_R$, where 1_R denotes the multiplicative identity element of R.

We now discuss these points in more detail. Let R be a ring with zero element 0_R. A subset I of R is said to be an *ideal* of the ring if $0_R \in I$, $u + v \in I$, $-u \in I$, $ru \in I$ and $ur \in I$ for all $u, v \in I$ and $r \in R$. An ideal I of R determines a binary relation $\sim_I$ on R, where elements x and y of R satisfy $x \sim_I y$ if and only if $x - y \in I$.

Let $\sim_I$ be the relation on the ring R determined by some ideal I of R. Then $x \sim_I x$ for all $x \in R$, because $x - x = 0_R$ and $0_R \in I$. Thus the relation $\sim_I$ is reflexive. Now let x and y be elements of R, where $x \sim_I y$. Then $x - y \in I$. But then $y - x \in I$, because $y - x = -(x - y)$, and the negative of an element of an ideal belongs to that ideal. Thus the relation $\sim_I$ is symmetric. Now let x, y and z be elements of R, where $x \sim_I y$ and $y \sim_I z$. Then $x - y \in I$ and $y - z \in I$. But then $x - z \in I$, because $x - z = (x - y) + (y - z)$, and the sum of two elements of the ideal I must itself belong to I. Thus the relation $\sim_I$ is transitive. The relation $\sim_I$ is thus an equivalence relation, since it is reflexive, symmetric and transitive.

Let us examine what is happening here in a little more generality. Any subset X of the ring R determines a corresponding relation $\sim_X$ on R, where elements x and y of R satisfy $x \sim_X y$ if and only if $x - y$ in R. It is then a straightforward exercise to verify the following results: the relation $\sim_X$ is

reflexive if and only if $0_R \in X$; the relation $\sim_X$ is symmetric if and only if $-u \in I$ for all $u \in I$; the relation $\sim_X$ is transitive if and only if $u + v \in I$ for all $u \in I$ and $v \in I$. It follows from these observations that the relation $\sim_X$ is an equivalence relation on R if and only if X is a subgroup of R with respect to the operation of addition. Now every ideal of R is a subgroup of R with respect to the operation of addition. Therefore the relation $\sim_I$ on R corresponding to an ideal I is an equivalence relation on R.

Now any equivalence relation on a set partitions that set as a disjoint union of equivalence classes. Given any element of the set, there is a unique equivalence class to which the element belongs. In particular, the relation $\sim_I$ determined by some ideal I of R partitions the ring R as a disjoint union of equivalence classes. The equivalence class of an element x of R is the subset $[x]_I$ of R, where

$$[x]_I = \{x' \in R : x' \sim_I x\}.$$

Note that an element x' of R belongs to $[x]_I$ if and only if $x' - x \in I$. It follows that $[x]_I = I + x$, where

$$I + x = \{u + x : u \in I\}.$$

Moreover this subset $I + x$ of R is the unique coset of I in R that contains the element x of R. Thus the equivalence classes under the equivalence relation $\sim_I$ are the cosets of I in R. We denote the set of all cosets of I in R by R/I.

We wish to give this set R/I the structure of a ring. We therefore need to provide it with well-defined operations of addition and multiplication that satisfy all the ring axioms.

Let x, x', y and y' be elements of R, where $x \sim_I x'$ and $y \sim_I y'$. Then $x - x' \in I$ and $y - y' \in I$. Now

$$(x + y) - (x' + y') = (x - x') + (y - y'),$$

because the operation of addition on the ring R is both commutative and associative. But $(x - x') + (y - y')$ is the sum of two elements of the ideal I, and must therefore itself belong to I. It follows that $x + y \sim_I x' + y'$. Also

$$xy - x'y' = x(y - y') + (x - x')y',$$

and $x - x' \in I$ and $y - y' \in I$. The definition of ideals then ensures that $(x - x')y' \in I$ and $x(y - y') \in I$, from which it follows that $xy - x'y' \in I$. Thus $xy \sim_I x'y'$.

Let x and x' be elements of R. Then $I + x = I + x'$ if and only if $x \sim_I x'$. (In other words, $I + x = I + x'$ if and only if $x - x' \in I$.) Let x, x', y and y' be elements of R. Suppose that $I + x = I + x'$ and $I + y = I + y'$. Then $x \sim_I x'$ and $y \sim_I y'$. But then $x + y \sim_I x' + y'$ and $xy \sim_I x'y'$, and therefore $I + x + y = I + x' + y'$ and $I + xy = I + x'y'$. It follows that there are well-defined operations of addition and multiplication defined on the set R/I of cosets of I in R, where

$$(I + x) + (I + y) = I + (x + y) \quad \text{and} \quad (I + x)(I + y) = I + xy$$

for all $x, y \in R$.

Why is the operation of multiplication on R/I *well-defined*? Let A and B be elements of R/I. Then A and B are cosets of I in R. A well-defined multiplication operation on R/I will associate to these cosets A and B some coset C of I that is the product of A and B. Specifically, we let $C = I + xy$, where $x \in A$ and $y \in B$. (Note that $I + x = A$ if and only if $x \in A$, and $I + y = B$ if and only if $y \in B$.) Now, unless I is the zero ideal, there will be more than one possible choice for x and for y. Nevertheless the arbitrariness in the choice of x and y has no effect on the determination of the coset C representing the product of A and B. Indeed, had we chosen x' in place of x, and y' in place of y, where $x' \in A$ and $y' \in B$, then we would have obtained the same product coset C to represent the product of the cosets A and B, because $I + x'y' = I + xy$ whenever $x, x' \in A$ and $y, y' \in B$.

It remains to verify that these operations of addition and multiplication on the set R/I of cosets of I satisfy the ring axioms. The proofs that addition is both commutative and associative, and that multiplication is associative, are trivial. Let us show, for example, that the multiplication operation on R/I is associative. Let $x, y, z \in R$. Then

$$\begin{aligned}((I + x)(I + y))(I + z) &= (I + xy)(I + z) \\ &= I + (xy)z = I + x(yz) \\ &= (I + x)(I + yz) \\ &= (I + x)((I + y)(I + z)).\end{aligned}$$

Every ring has a zero element. The zero element of the ring R/I is the ideal I, where this ideal is considered as a coset of itself. Note that $I = I + 0$. Therefore

$$I + (I + x) = (I + 0) + (I + x) = I + (0 + x) = I + x$$

and $(I + x) + I = I + x$ for all $x \in R$. Also

$$(I + x) + (I + (-x)) = I + (x + (-x)) = I + 0 = I$$

and $(I + (-x)) + (I + x) = I$ for all $x \in R$. Thus the coset $I - x$ is the negative of the coset $I + x$ for all $x \in R$, where $I - x = I + (-x)$. The set R/I of cosets of I and R is thus an Abelian group with respect to the operation of addition of cosets.

We have noted that the operation of multiplication of cosets is an associative binary operation on R/I. Thus, in order to complete the verification that R/I is a ring with respect to the operations of addition and multiplication of cosets, it only remains to verify the distributive laws. Let x, y and z be elements of R. Then

$$\begin{aligned}(I + x)((I + y) + (I + z)) &= (I + x)(I + y + z) \\ &= I + x(y + z) = I + xy + xz \\ &= (I + xy) + (I + xz) \\ &= (I + x)(I + y) + (I + x)(I + z),\end{aligned}$$

and similarly

$$((I + x) + (I + y))(I + z) = (I + x)(I + z) + (I + y)(I + z).$$

Thus $A(B+C) = AB+AC$ and $(A+B)C = AC+BC$ for all $A, B, C \in R/I$. Thus R/I is a ring.

Note that if R is a commutative ring, then so is the quotient ring R/I. Also if R is a unital ring with multiplicative identity element 1_R, then R/I is a unital ring with multiplicative identity element $I + 1_R$.

B-3 Products of Cosets of an Ideal

Let R be a ring, let I be an ideal of R, and let A and B be cosets of I in R. Now it is not difficult to verify that

$$A + B = \{x + y : x \in A \text{ and } y \in B\}.$$

One might wonder whether or not the product coset AB is equal to the set $\{xy : x \in A \text{ and } y \in B\}$. Were this always the case, then one would be able to simplify the definition of multiplication in the quotient ring R/I by *defining* the product of the cosets A and B to be the set of products xy with $x \in A$ and $y \in B$. However the product coset AB is in general not equal to $\{xy : x \in A \text{ and } y \in B\}$, and indeed this latter set may not even be a coset of I in R.

Let us consider an example. We take as our ring R the ring $\mathbb{Z}$ of integers, and we take as our ideal I the ideal $6\mathbb{Z}$ of $\mathbb{Z}$ consisting of the multiples of 6. This ideal determines a corresponding quotient ring $\mathbb{Z}/6\mathbb{Z}$, which is the

ring of congruence classes of integers modulo 6, with the usual operations of addition and multiplication of congruence classes.

Let $A = 6\mathbb{Z} + 2$ and $B = 6\mathbb{Z} + 4$. Now the definitions of addition and multiplication of congruence classes in the ring $\mathbb{Z}/6\mathbb{Z}$ ensure that $A+B = 6\mathbb{Z}$. Also $AB = 6\mathbb{Z} + (2 \times 4) = 6\mathbb{Z} + 8 = 6\mathbb{Z} + 2$. Let P be the subset of $\mathbb{Z}$ defined by $P = \{xy : x \in A \text{ and } y \in B\}$. Now

$$A = \{2 + 6u : u \in \mathbb{Z}\}, \quad B = \{4 + 6v : v \in \mathbb{Z}\},$$

and therefore

$$P = \{8 + 24u + 12v + 36uv : u, v \in \mathbb{Z}\} = \{8 + 12w : w \in \mathbb{Z}\} = 8 + 12\mathbb{Z}.$$

(Note that $24u + 12v + 36uv$ is a multiple of 12 for all $u, v \in \mathbb{Z}$. Moreover any multiple of 12 may be written in the form $24u + 12v + 36uv$, with $u = 0$ and $v \in \mathbb{Z}$.) The subset P of $\mathbb{Z}$ is not a coset of $6\mathbb{Z}$. Therefore it cannot be the product of A and B in the ring $\mathbb{Z}/6\mathbb{Z}$. Note however that $P \subset AB$.

B-4 Quotient Rings and Congruence Classes

Let m be a positive integer. Integers x and y are said to be *congruent* modulo m if $x-y$ is divisible by m. The congruence class of an integer x consists of all integers x' that are congruent to x. Now the set $m\mathbb{Z}$ of integer multiples of m is an ideal of the ring $\mathbb{Z}$ of integers, and the congruence class of an integer x modulo m coincides with the coset $m\mathbb{Z}+x$ of $m\mathbb{Z}$ in $\mathbb{Z}$ that contains x. Thus the congruence classes of integers modulo m correspond to the elements of the quotient ring $\mathbb{Z}/m\mathbb{Z}$.

Congruence classes may be added, subtracted and multiplied. Let x and y be integers. The sum of the congruence classes (modulo m) of x and y is the congruence class of $x + y$, and the product of these congruence classes is the congruence class of xy. These operations of addition and multiplication of congruence classes correspond to the operations of addition and multiplication defined on the quotient ring $\mathbb{Z}/m\mathbb{Z}$.

Or, to put this another way, the theory of quotient rings is a generalization of basic modular arithmetic. Indeed it is sometimes useful to extend the notation of congruences to rings. Given a ring R, and given an ideal I of R, we may define a relation of congruence modulo the ideal I, where elements x and y of R satisfy the congruence $x \equiv y$ (mod. I) if and only if $x - y \in I$.

B-5 A Quotient of a Polynomial Ring

We denote by $\mathbb{R}[x]$ the ring of polynomials with real coefficients. Such a polynomial is of course specified by an expression of the form $\sum_{j=0}^{m} c_j x^j$, where

the coefficients $c_0, c_1, \ldots, c_n$ of the polynomial are real numbers. Such polynomials may be added, subtracted and multiplied in the usual fashion, and the set of all polynomials with real coefficients is a unital commutative ring (with respect to the usual operations of addition and multiplication of polynomials).

The polynomial $x^2 + 1$ generates an ideal I of $\mathbb{R}[x]$, which consists of all polynomials with real coefficients that can be expressed in the form $f(x)(x^2+1)$ for some $f \in \mathbb{R}[x]$. We investigate the structure of the corresponding quotient ring $\mathbb{R}[x]/I$.

Now $(I + x^2) + (I + 1) = I + x^2 + 1 = I$, and therefore $I + x^2 = I - 1$. It follows easily from this that $I + x^{2k} = I + (-1)^k$ for all non-negative integers k. (This follows easily by induction on k, since

$$I + x^{2k+2} = (I + x^{2k})(I + x^2) = (I + x^{2k})(I - 1) = I - x^{2k}$$

for all positive integers k.) Now a polynomial with real coefficients may be written in the form $\sum_{j=0}^{\infty} c_j x^j$, where the coefficients c_j are real numbers. Moreover only finitely many of the coefficients c_j are non-zero. We shall use the notation of sums of infinitely many indices, as above, though all such sums occurring in the following discussion are in fact sums with only finitely many non-zero summands. Now

$$\begin{aligned}
I + \sum_{j=0}^{\infty} c_j x^j &= \sum_{j=0}^{\infty} (I + c_j)(I + x^j) \\
&= \sum_{k=0}^{\infty} (I + c_{2k})(I + x^{2k}) + \sum_{k=0}^{\infty} (I + c_{2k+1})(I + x^{2k+1}) \\
&= \sum_{k=0}^{\infty} (I + c_{2k})(I + (-1)^k) \\
&\qquad + \sum_{k=0}^{\infty} (I + c_{2k+1})(I + x)(I + (-1)^k) \\
&= \sum_{k=0}^{\infty} (I + (-1)^k c_{2k}) + \sum_{k=0}^{\infty} (I + (-1)^k c_{2k+1} x) \\
&= I + a + bx,
\end{aligned}$$

where

$$a = \sum_{k=0}^{\infty} (-1)^k c_{2k}, \quad b = \sum_{k=0}^{\infty} (-1)^k c_{2k+1}.$$

Thus

$$\mathbb{R}[x]/I = \{I + a + bx : a, b \in \mathbb{R}\}.$$

The elements of the quotient $\mathbb{R}[x]/I$ therefore correspond to ordered pairs (a, b) whose coefficients a and b are real numbers.

Now

$$(I + a + bx) + (I + c + dx) = I + (a + c) + (b + d)x,$$

and

$$\begin{aligned}(I + a + bx)(I + c + dx) &= I + (a + bx)(c + dx) \\ &= I + ac + adx + bcx + bdx^2 \\ &= I + ac - bd + (ad + bc)x.\end{aligned}$$

It follows easily from these observations that the function from the quotient ring $\mathbb{R}[x]/I$ to the field $\mathbb{C}$ of complex numbers that sends the coset $I + a + bx$ to the complex number $a + b\sqrt{-1}$ is a bijection of sets that maps sums to sums, and maps products to products. It is therefore an isomorphism of rings. Thus $\mathbb{R}[x]/I \cong \mathbb{C}$.

B-6 Induced Homomorphisms

A *homomorphism* $\varphi\colon R \to S$ from a ring R to a ring S is a function from R to S with the properties that $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in R$.

Let $\varphi\colon R \to S$ be a homomorphism from a ring R to a ring S. Then

$$\varphi(x) = \varphi(x + 0_R) = \varphi(x) + \varphi(0_R)$$

for all $x \in R$, where 0_R denotes the zero element of the ring R. It follows that $\varphi(0_R) = 0_S$, where 0_S denotes the zero element of the ring S. (To verify this, subtract $\varphi(x)$ from both sides of the identity $\varphi(x) = \varphi(x) + \varphi(0_R)$.) Also

$$\varphi(x) + \varphi(-x) = \varphi(x - x) = \varphi(0_R) = 0_S,$$

and therefore $\varphi(-x) = -\varphi(x)$ for all $x \in R$.

The *kernel* $\ker\varphi$ of $\varphi\colon R \to S$ is defined by

$$\ker\varphi = \{x \in R : \varphi(x) = 0_S\},$$

We now show that $\ker\varphi$ is an ideal of R.

Now $0_R \in \ker\varphi$ since $\varphi(0_R) = 0_S$. Let $x, y \in \ker\varphi$ and $r \in R$. Then

$$\varphi(x + y) = \varphi(x) + \varphi(y) = 0_S + 0_S = 0_S, \quad \varphi(-x) = -\varphi(x) = 0_S,$$

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0_S = 0_S, \quad \varphi(xr) = \varphi(x)\varphi(r) = 0_S\varphi(r) = 0_S.$$

It follows that $x + y \in \ker\varphi$, $-x \in \ker\varphi$, $rx \in \ker\varphi$ and $xr \in \ker\varphi$. Thus $\ker\varphi$ is an ideal of R.

Let x and y be elements of the ring R. Then

$$\varphi(x) = \varphi(y) \iff \varphi(x) - \varphi(y) = 0_S \iff \varphi(x-y) = 0_S \iff x - y \in \ker\varphi.$$

It follows that a homomorphism $\varphi\colon R \to S$ is injective if and only if $\ker\varphi = \{0\}$.

We now discuss the proof of Proposition 2.7.

Let $\varphi\colon R \to S$ be a homomorphism from a ring R to a ring S, and let I be an ideal of R satisfying $I \subset \ker\theta$. Let $x, x' \in R$. Suppose that $I + x = I + x'$. Then $x - x' \in I$, and therefore $x - x' \in \ker\varphi$. It follows that

$$\varphi(x) - \varphi(x') = \varphi(x) + \varphi(-x') = \varphi(x - x') = 0_S,$$

and therefore $\varphi(x) = \varphi(x')$. It follows from this that there is a well-defined function $\overline{\varphi}\colon R/I \to S$, where $\overline{\varphi}(I + x) = \varphi(x)$. (Indeed, given any element A of R/I, we define $\overline{\varphi}(A) = \varphi(x)$, where x is any element of R that belongs to the coset A. We can do this because the function φ is constant over the coset A.) Now

$$\overline{\varphi}((I+x)+(I+y)) = \overline{\varphi}(I+x+y) = \varphi(x+y) = \varphi(x)+\varphi(y) = \overline{\varphi}(I+x)+\overline{\varphi}(I+y)$$

and

$$\overline{\varphi}((I + x)(I + y)) = \overline{\varphi}(I + xy) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(I + x)\overline{\varphi}(I + y)$$

for all $x, y \in R$. It follows that $\overline{\varphi}\colon R/I \to S$ is a homomorphism.

The homomorphism $\overline{\varphi}\colon R/I \to S$ is injective if and only if $\ker\overline{\varphi} = \{I\}$. Now $\ker\overline{\varphi} = \{I + x : x \in \ker\varphi\}$. Moreover $I + x = I$ if and only if $x \in I$. It follows that $\ker\overline{\varphi}$ is injective if and only if $\ker\varphi = I$.

B-7 Ideals of Quotient Rings

Let R be a ring, and let I be an ideal of R, and let $\pi\colon R \to R/I$ be the *quotient homomorphism* defined so that $\pi(x) = x + I$ for all $x \in \mathbb{R}$. Note that $\pi(x + y) = \pi(x) + \pi(y)$ and $\pi(xy) = \pi(x)\pi(y)$ for all $x, y \in R$. Also $\ker\pi = I$.

We claim that there is a natural one-to-one correspondence between the ideals of the quotient ring R/I and the ideals J of the ring R that satisfy $I \subset J$.

Let L be an ideal of R/I, and let

$$\pi^{-1}(L) = \{x \in R : \pi(x) \in L\} = \{x \in R : I + x \in L\}.$$

Now $0 \in \pi^{-1}(L)$. Let x and y be elements of $\pi^{-1}(L)$. Then $\pi(x+y) = \pi(x) + \pi(y) \in L$ and $\pi(-x) = -\pi(x) \in L$, and therefore $x + y \in \pi^{-1}(L)$ and $-x \in \pi^{-1}(L)$. Also $\pi(rx) = \pi(r)\pi(x) \in L$ and $\pi(xr) = \pi(x)\pi(r) \in L$ for all $r \in R$, and thus $rx \in \pi^{-1}(L)$ and $xr \in \pi^{-1}(L)$ for all $r \in R$. We conclude that $\pi^{-1}(L)$ is an ideal of R.

Now let J be an ideal of R, and let

$$\pi(J) = \{\pi(x) : x \in J\} = \{I + x : x \in J\}.$$

Now the zero element $I + 0$ of R/I belongs to $\pi(J)$. Let u and v be elements of $\pi(J)$. Then there exist elements x and y of J such that $u = \pi(x) = I + x$ and $v = \pi(y) = I + y$. Then $u + v = \pi(x+y) \in \pi(J)$ and $-u = \pi(-x) \in \pi(J)$. Let s be an element of R/I. Then $s = \pi(r) = I + r$ for some $r \in R$. Then $rx \in J$ and $xr \in J$, and therefore $su = \pi(rx) \in \pi(J)$ and $us = \pi(xr) \in \pi(J)$. We conclude that $\pi(J)$ is an ideal of R/I.

Let L be an ideal of R/I. Clearly $\pi(\pi^{-1}(L)) \subset L$. Let $u \in L$. Now $u = \pi(x) = I + x$ for some $x \in R$. Moreover $x \in \pi^{-1}(L)$, because $\pi(x) \in L$. It follows that $u \in \pi(\pi^{-1}(L))$. We conclude that $\pi(\pi^{-1}(L) = L$ for all ideals L of R/I.

Let J be an ideal of R. We claim that from this that $\pi^{-1}(\pi(J)) = I + J$, where

$$I + J = \{x + y : x \in I \text{ and } y \in J.\}$$

Now $\pi(x + y) = \pi(y) \in \pi(J)$ for all $x \in I$ and $y \in J$, and therefore $I + J \subset \pi^{-1}(\pi(J))$. Let z be an element of $\pi^{-1}(\pi(J))$. Then $\pi(z) \in \pi(J)$, and therefore $\pi(z) = \pi(y)$ for some $y \in J$. But then $\pi(z - y) = 0$, and therefore $z - y \in I$. Thus $z = x + y$ for some $x \in I$ and $y \in J$. Thus $\pi^{-1}(\pi(J)) \subset I + J$. We conclude that $\pi^{-1}(\pi(J)) = I + J$.

We now show that there is a one-to-one correspondence between the ideals of R/I and the ideals J of R that satisfy $I \subset J$. Let L be an ideal of R/I. Then $\pi^{-1}(L)$ is an ideal of R, $I \subset \pi^{-1}(L)$, and $\pi(\pi^{-1}(L)) = L$. If J is an ideal of R, and if $I \subset J$, then $\pi(J)$ is an ideal of L and $\pi^{-1}(\pi(J)) = I + J = J$. Thus we have a well-defined one-to-one correspondence between ideals of R/I and ideals J of R satisfying $J \subset I$, where $\pi^{-1}(L)$ is the ideal of R corresponding to an ideal L of R/I, and $\pi(J)$ is the ideal of R/I corresponding to an ideal J of R for which $I \subset J$.

B-8 Maximal Ideals

Let R be a unital commutative ring, and let I be a proper ideal of R. (A *proper ideal* of a ring R is an ideal of R that is a proper subset of R. Thus an ideal I of R is a proper ideal of R if and only if $I \neq R$.) We have noted that there is a one-to-one correspondence between the ideals of the quotient ring R/I and the ideals J of R that satisfy $I \subset J$. Now the quotient ring R/I is a unital commutative ring, and we know that a unital commutative ring is a field if and only if the ring has no ideals other than the zero ideal and the whole ring itself (see Lemma 2.4). Putting these facts together, we see that the quotient ring R/I is a field if and only if there are no ideals of R containing the ideal I other than I and R. This motivates the following definition.

Definition Let R be a unital commutative ring. A proper ideal I of R is said to be *maximal* if the only ideals J of R for which $I \subset J$ are the ideals $J = I$ and $J = R$.

Thus a proper ideal I of a unital commutative ring R is a maximal ideal if and only if the quotient ring R/I is a field.

We have made use of Lemma 2.4 in establishing this result. It may aid understanding to prove more directly that if R is a unital commutative ring, and if I is a maximal ideal of R, then the quotient ring R/I is a field.

So let R be a unital commutative ring, and let I be a maximal ideal of R. Then the quotient ring R/I is also a unital commutative ring. In order to show that this ring is a field, it suffices to prove that every non-zero element of the quotient ring R/I is invertible.

Now an element of the quotient ring R/I is a coset of I in R. It is therefore of the form $I + x$ for some $x \in R$. Now the zero element of the quotient ring is represented by the ideal I, where this ideal is regarded as a coset of itself. Also $I + x = I$ if and only if $x \in I$. Thus a non-zero element of R/I can be represented as $I + x$, where $x \in R$ and $x \notin I$. In order to prove that such a coset is an invertible element of R/I, we must prove that, given any element x of R, where $x \neq I$, there exists some element y of R such that $(I + x)(I + y) = I + 1$. Now the definition of multiplication in the quotient ring R/I ensures that $(I + x)(I + y) = I + xy$. Thus an non-zero element $I + x$ of R/I, is invertible if and only if there exists some element y of R such that $xy - 1 \in I$.

So let $I + x$ be a non-zero element of R/I, where $x \in R$ So let R be a unital commutative ring, let I be a maximal ideal of R, and let x be an element of R that does not belong to the ideal I. Then the set $I \cup \{x\}$

generates an ideal J of R. Moreover

$$J = \{z + xr : z \in I \text{ and } r \in R\}.$$

(Indeed one may readily verify that the set on the right hand side of this identity is an ideal of R that contains $I \cup \{x\}$. Moreover the elements of this ideal are contained in every ideal of R that contains $I \cup \{x\}$. These properties characterize the ideal of R generated by the set $I \cup \{x\}$.) But because the ideal I is maximal, either $J = I$ or $J = R$. (This follows directly from the definition of maximal ideals.) But $J \neq I$, because $x \in J$ and $x \notin I$. Therefore $J = R$. It follows that $1 \in J$. Thus there must exist $z \in I$ and $y \in R$ such that $z + xy = 1$. But then $xy - 1 \in I$, and therefore $(I + x)(I + y) = I + 1$. We have proved that if I is a maximal ideal of the unital commutative ring R, then every non-zero element of the quotient field R/I is invertible, and therefore R/I is a field.

B-9 Integer Multiples of Elements of a Ring

Let R be a ring, and let $r \in R$. We define $n.r$ for all positive integers n so that $1.r = r$ and $n.r = (n-1).r + r$ for $n > 1$. We also define $0.r = 0_R$ and $(-n).r = -(n.r)$ for all positive integers n, where 0_R denotes the zero element of the ring R. Then

$$(m + n).r = m.r + n.r, \quad (mn).r = m.(n.r)$$

for all $m, n \in \mathbb{Z}$ and $r \in R$. (This result is merely a special case of Theorem 1.4 expressed in additive notation.)

Let r and s be elements of R. Then $1.(r + s) = r + s = 1.r + 1.s$. Let n be a positive integer. Suppose that $n.(r + s) = n.r + n.s$. Then

$$\begin{aligned}(n+1).(r+s) &= n.(r+s) + (r+s) = (n.r + n.s) + (r+s) \\ &= (n.r + r) + (n.s + s) = (n+1).r + (n+1).s,\end{aligned}$$

because the operation of addition on the ring R is commutative and associative. It follows by induction on n that $n.(r + s) = n.r + n.s$ for all positive integers n. Also $0.(r + s) = 0_R = 0.r + 0.s$, and

$$(-n).(r+s) = -(n.(r+s)) = -(n.r + n.s) = -n.r - n.s = (-n).r + (-n).s.$$

for all positive integers n. It follows that $n.(r+s) = n.r+n.s$ for all integers n.

Now $(1.r)s = rs = 1.(rs)$. Let m be a positive integer. Suppose that $(m.r)s = m.(rs)$. Then

$$((m+1).r)s = (m.r + r)s = (m.r)s + rs = m.(rs) + rs = (m+1).(rs).$$

(Here we are using the requirement that the operations of addition and multiplication in any ring satisfy the Distributive Law.) It follows from the Principle of Mathematical Induction that $(m.r)s = m.(rs)$ for all positive integers m. Also $(0.r)s = 0_R s = 0_R = 0.(rs)$, and $((-m).r)s = (-(m.r))s = -((m.r)s) = -(m.(rs)) = (-m).(rs)$ for all positive integers m. It follows that $(m.r)s = m.(rs)$ for all integers m. A similar proof shows that $r(n.s) = n.(rs)$ for all positive integers n. On replacing r by $m.r$ in this last identity, we find that

$$(m.r)(n.s) = n.((m.r)s) = n.(m.(rs)) = (mn).(rs)$$

for all $m, n \in \mathbb{Z}$ and $r, s \in R$.

B-10 The Characteristic of a Ring

Let R be a unital ring, let 0_R denote the zero element of R, and let 1_R denote the multiplicative identity element of R. Then $1_R 1_R = 1_R$. Let $\rho\colon \mathbb{Z} \to R$ be the function defined such that $\rho(n) = n.1_R$ for each integer n. Then $\rho(m+n) = (m+n).1_R = m.1_R + n.1_R = \rho(m) + \rho(n)$ and $\rho(mn) = (mn).1_R = (m.1_R)(n.1_R) = \rho(m)\rho(n)$ for all integers m and n. It follows that $\rho\colon \mathbb{Z} \to R$ is a ring homomorphism. Therefore its image $\rho(\mathbb{Z})$ is a subring of R, and its kernel $\ker \rho$ is an ideal of $\mathbb{Z}$. Now every ideal of $\mathbb{Z}$ is of the form $p\mathbb{Z}$ for some non-negative integer p. It follows that

$$\{n \in \mathbb{Z} : n.1_R = 0_R\} = \ker \rho = p\mathbb{Z}$$

for some non-negative integer p. This integer p is the *characteristic* $\operatorname{char} R$ of the unital ring R.

Now if the unital ring R is an integral domain, then so is every unital subring of R. In particular $\rho(\mathbb{Z})$ is an integral domain. But $\rho(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, where p is the characteristic of R. Moreover the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is an integral domain if and only if either $p = 0$ or p is a prime number. Thus if R is an integral domain then either $\operatorname{char} R = 0$ or else $\operatorname{char} R$ is a prime number.

In particular, if K is a field, then either $\operatorname{char} K = 0$ or else $\operatorname{char} K$ is a prime number.