

Basic Algebra

Final Version, August, 2006
For Publication by Birkhäuser Boston
Along with a Companion Volume *Advanced Algebra*
In the Series

Cornerstones

Selected Pages from Chapter VIII: pp. 367, 408–413

Anthony W. Knapp

Copyright © 2006 by Anthony W. Knapp
All Rights Reserved

CHAPTER VIII

Commutative Rings and Their Modules

Abstract. This chapter amplifies the theory of commutative rings that was begun in Chapter IV, and it introduces modules for any ring. Emphasis is on the topic of unique factorization.

Section 1 gives many examples of rings, some commutative and some noncommutative, and introduces the notion of a module for a ring.

Sections 2–4 discuss some of the tools related to questions of factorization in integral domains. Section 2 defines the field of fractions for an integral domain and gives its universal mapping property. Section 3 defines prime and maximal ideals and relates quotients of them to integral domains and fields. Section 4 introduces principal ideal domains, which are shown to have unique factorization, and it defines Euclidean domains as a special kind of principal ideal domain for which greatest common divisors can be obtained constructively.

Section 5 proves that if R is an integral domain with unique factorization, then so is the polynomial ring $R[X]$. This result is a consequence of Gauss's Lemma, which addresses what happens to the greatest common divisor of the coefficients when one multiplies two members of $R[X]$. Gauss's Lemma has several other consequences that relate factorization in $R[X]$ to factorization in $F[X]$, where F is the field of fractions of R . Still another consequence is Eisenstein's irreducibility criterion, which gives a sufficient condition for a member of $R[X]$ to be irreducible.

Section 6 contains the theorem that every finitely generated unital module over a principal ideal domain is a direct sum of cyclic modules. The cyclic modules may be assumed to be primary in a suitable sense, and then the isomorphism types of the modules appearing in the direct-sum decomposition, together with their multiplicities, are uniquely determined. The main results transparently generalize the Fundamental Theorem for Finitely Generated Abelian Groups, and less transparently they generalize the existence and uniqueness of Jordan canonical form for square matrices with entries in an algebraically closed field.

Sections 7–11 contain foundational material related to factorization for the two subjects of algebraic number theory and algebraic geometry. Both these subjects rely heavily on the theory of commutative rings. Section 7 is a section of motivation, showing the analogy between a situation in algebraic number theory and a situation in algebraic geometry. Sections 8–10 introduce Noetherian rings, integral closures, and localizations. Section 11 uses this material to establish unique factorization of ideals for Dedekind domains, as well as some other properties.

1. Examples of Rings and Modules

Sections 4–5 of Chapter IV introduced rings and fields, giving a small number of examples of each. In the present section we begin by recalling those examples and giving further ones. Although Chapters VI and VII are not prerequisite for

Pages 368–407 do not appear in this file.

7. Orientation for Algebraic Number Theory and Algebraic Geometry

The remainder of the chapter introduces material on commutative rings with identity that is foundational for both algebraic number theory and algebraic geometry. Historically algebraic number theory grew out of Diophantine equations, particularly from two problems—from Fermat’s Last Theorem and from representation of integers by binary quadratic forms. Algebraic geometry grew out of studying the geometry of solutions of equations and out of studying Riemann surfaces.

These two subjects can be studied on their own, but they also have a great deal in common. The discovery that the plane could be coordinatized and that geometry could be approached through algebra was one of the great advances of all time for mathematics. Since then, fundamental connections between algebraic number theory and algebraic geometry have been discovered at a deeper level, and the distinction between the two subjects is more and more just a question of one’s point of view. The emphasis in the remainder of this chapter will be on one aspect of this relationship, the theory that emerged from trying to salvage something in the way of unique factorization.

By way of illustration, let us examine an analogy between what happens with a certain ring of “algebraic integers” and what happens with a certain “algebraic curve.” The ring of algebraic integers in question was introduced already in Section 4. It is $R = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. The units are ± 1 . Our investigation of unique factorization was aided by the function

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2,$$

which has the property that

$$N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5}).$$

With this function we could determine candidates for factors of particular elements. In connection with the equality $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, we saw that the two factors on the left side and the two factors on the right side are all irreducible. Moreover, neither factor on the left is the product of a unit and a factor on the right. Therefore R is not a unique factorization domain. As a consequence it cannot be a principal ideal domain. In fact, $(2, 1 + \sqrt{-5})$ is an example of an ideal that is not principal. We shall return shortly to examine this ring further.

Now we introduce the algebraic curve. Consider $y^2 = (x - 1)x(x + 1)$ as an equation in two variables x and y . To fix the ideas, we think of a solution as a pair (x, y) of complex numbers. Although the variables in this discussion are complex, it is convenient to be able to draw pictures of the solutions, and one does this by showing only the solutions (x, y) with x and y in \mathbb{R} . Figure 8.6 indicates

the set of solutions in \mathbb{R}^2 for this particular curve. We can study these solutions for a while, looking for those pairs (x, y) with x and y rationals or integers, but a different level of understanding comes from studying functions on the locus of complex solutions. The functions of interest are polynomial functions in the pair (x, y) , and we identify two of them if they agree on the locus. Thus we introduce the ring

$$R' = \mathbb{C}[x, y]/(y^2 - (x - 1)x(x + 1)).$$

There is a bit of a question whether this is indeed the space of restrictions, but that can be settled affirmatively by the “Nullstellensatz” in *Advanced Algebra* and a verification that the principal ideal $(y^2 - (x - 1)x(x + 1))$ is prime.⁸ The ring R' is called the “affine coordinate ring” of the curve, and the curve itself is an example of an “affine algebraic curve.”

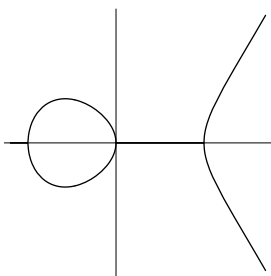


FIGURE 8.6. Real points of the curve $y^2 = (x - 1)x(x + 1)$.

We can recover the locus of the curve from the ring R' as follows. If (x_0, y_0) is a point of the curve, then it is meaningful to evaluate members of R' at (x_0, y_0) , and we let $I_{(x_0, y_0)}$ be the ideal of all members of R' vanishing at (x_0, y_0) . Evaluation at (x_0, y_0) exhibits the ring $R'/I_{(x_0, y_0)}$ as isomorphic to \mathbb{C} , which is a field. Thus $I_{(x_0, y_0)}$ is a maximal ideal and is in particular prime. It turns out for this example that all nonzero prime ideals are of this form.⁹ We return to make use of this geometric interpretation of prime ideals in a moment.

Now let us consider factorization in R' . Every element of R' can be written uniquely as $A(x) + B(x)y$, where $A(x)$ and $B(x)$ are polynomials. The analog

⁸The polynomial $y^2 - (x - 1)x(x + 1)$ is prime since $(x - 1)x(x + 1)$ is not a square, or since Eisenstein’s criterion applies. The principal ideal $(y^2 - (x - 1)x(x + 1))$ is therefore prime by Proposition 8.14. What the Nullstellensatz says when the underlying field is algebraically closed is that the only polynomials vanishing on the zero locus of a prime ideal are the members of the ideal.

⁹In Section 9, Example 3 of integral closures in combination with Proposition 8.45 shows that every nonzero prime ideal of R' is maximal. (In algebraic geometry one finds that this property of prime ideals is a reflection of the 1-dimensional nature of the curve.) The Nullstellensatz says that the maximal ideals are all of the form $I_{(x_0, y_0)}$.

in R' of the quantity $N(a + b\sqrt{-5})$ in the ring R is the quantity

$$\begin{aligned} N(A(x) + B(x)y) &= (A(x) + B(x)y)(A(x) - B(x)y) \\ &= A(x)^2 - B(x)^2y^2 \\ &= A(x)^2 - B(x)^2(x^3 - x). \end{aligned}$$

Easy computation shows that

$$N((A(x) + B(x)y)(C(x) + D(x)y)) = N(A(x) + B(x)y)N(C(x) + D(x)y),$$

and hence $N(\cdot)$ gives us a device to use to check whether elements of R' are irreducible. We find in the equation

$$(x + y)(x - y) = x^2 - (x^3 - x) = -x(x - \frac{1}{2}(1 + \sqrt{5}))(x - \frac{1}{2}(1 - \sqrt{5}))$$

that the two elements on the left side and the three elements on the right side are irreducible. Therefore unique factorization fails in R' .

Although unique factorization fails for the elements of R' , there is a notion of factorization for ideals in R' that behaves well algebraically and has a nice geometric interpretation. Recall that the nonzero prime ideals correspond to the points of the locus $y^2 = (x - 1)x(x + 1)$ via passage to the zero locus, the ideal corresponding to (x_0, y_0) being called $I_{(x_0, y_0)}$. For any two ideals I and J , we can form the product ideal IJ whose elements are the sums of products of a member of I and a member of J . Then $I_{(x_0, y_0)}^k$ may be interpreted as the ideal of all members of R' vanishing at (x_0, y_0) to order k or higher, and $I_{(x_1, y_1)}^{k_1} \cdots I_{(x_n, y_n)}^{k_n}$ becomes the ideal of all members of R' vanishing at each (x_j, y_j) to order at least k_j . We shall see in Section 11 that every nonzero proper ideal I in R' factors in this way. The points (x_j, y_j) and the integers k_j have a geometric interpretation in terms of I and are therefore uniquely determined: the (x_j, y_j) 's form the locus of common zeros of the members of I , and the integer k_j is the greatest integer such that the vanishing at (x_j, y_j) is always at least to order k_j . In a sense, factorization of elements was the wrong thing to consider; the right thing to consider is factorization of ideals, which is unique because of the associated geometric interpretation.

Returning to the ring $R = \mathbb{Z}[\sqrt{-5}]$, we can ask whether factorization of ideals is a useful notion in R . Again IJ is to be the set of all sums of products of an element in I and an element in J . For $I = (2, 1 + \sqrt{-5})$ and $J = (2, 1 - \sqrt{-5})$, we get all sums of expressions $(2a + b(1 + \sqrt{-5}))(2c + d(1 - \sqrt{-5}))$ in which a, b, c, d are in \mathbb{Z} , hence all sums of expressions

$$2(2ac + 3bd) + 2(bc + ad) + 2\sqrt{-5}(bc - ad).$$

All such elements are divisible by 2. Two examples come by taking $a = c = 1$ and $b = d = 0$ and by taking $a = c = 0$ and $b = d = 1$; these give 4 and 6. Subtracting, we see that 2 is a sum of products. Thus $IJ = (2)$. The element 2 is irreducible and not prime, and we know from Proposition 8.14 that the ideal (2) therefore cannot be prime. What we find is that the ideal (2) factors even though the element 2 does not factor. It turns out that R has unique factorization of ideals, just the way R' does.

The prime ideals of the ring R have a certain amount of structure in terms of the primes or prime ideals of \mathbb{Z} . To understand what to expect, let us digress for a moment to discuss what happens with the ring $R'' = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$ of Gaussian integers. This too was introduced in Section 4, and it is a Euclidean domain, hence a principal ideal domain. It has unique factorization. Its appropriate $N(\cdot)$ function is $N(a + ib) = a^2 + b^2$. Problems 27–31 at the end of the chapter ask one to verify that the primes of R'' , up to multiplication by one of the units ± 1 and $\pm i$, are members of R'' of any of the three kinds

$$\begin{aligned} p &= 4n + 3 \text{ that is prime in } \mathbb{Z} \text{ and has } n \geq 0, \\ p &= a \pm ib \text{ with } a^2 + b^2 \text{ prime in } \mathbb{Z} \text{ of the form } 4n + 1 \text{ with } n \geq 0, \\ p &= 1 \pm i \text{ (these are associates).} \end{aligned}$$

These three kinds may be distinguished by what happens to the function $N(\cdot)$. In the first case $N(p) = p^2$ is the square of a prime of \mathbb{Z} and is the square of a prime of R'' , in the second case $N(p)$ is a prime of \mathbb{Z} that is the product of two distinct primes of R'' , and in the third case $N(p)$ is a prime of \mathbb{Z} that is the square of a prime of R'' , apart from a unit factor. The nonzero prime ideals of R'' are the principal ideals generated by the prime elements of R'' , and they fall into three types as well. Each nonzero prime ideal P has a prime p of \mathbb{Z} attached to it, namely the one with $(p) = \mathbb{Z} \cap P$, and the type of the ideal corresponds to the nature of the factorization of the ideal pR'' of R'' . Specifically in the first case pR'' is a prime ideal in R'' , in the second case pR'' is the product of two distinct prime ideals in R'' , and in the third case pR'' is the square of a prime ideal in R'' .

The structure of the prime ideals in R is of the same nature as with R'' . Each nonzero prime ideal P has a prime p of \mathbb{Z} attached to it, again given by $(p) = \mathbb{Z} \cap P$, and the three kinds correspond to the factorization of the ideal pR of R . Let us be content to give examples of the three possible behaviors:

$$\begin{aligned} 11R &\text{ is prime in } R, \\ 2R &\text{ is the product of two distinct prime ideals in } R, \\ 5R &\text{ is the square of the prime ideal } (\sqrt{-5}) \text{ in } R. \end{aligned}$$

We have already seen the decomposition of $2R$, and the decomposition of $5R$ is easy to check. With $11R$, the idea is to show that 11 is a prime element in R . Thus let 11 divide a product in R . Then $N(11) = 11^2$ divides the product of

the $N(\cdot)$'s, 11 divides the product of the $N(\cdot)$'s, and 11 must divide one of the $N(\cdot)$'s. Say that 11 divides $N(a + b\sqrt{-5})$, i.e., that $a^2 + 5b^2 \equiv 0 \pmod{11}$. If 11 divides one of a or b , then this congruence shows that 11 divides the other of them; then 11 divides $a + b\sqrt{-5}$, as we wanted to show. The other possibility is that 11 divides neither a nor b . Then $(ab^{-1})^2 \equiv -5 \pmod{11}$ says that -5 is a square modulo 11, and we readily check that it is not. The conclusion is that 11 is indeed prime in R .

This structure for the prime ideals of R has an analog with the curve and its ring R' . The analogs for the curve case of \mathbb{Z} and $\sqrt{-5}$ for the number-theoretic case are $\mathbb{C}[x]$ and y . The primes of $\mathbb{C}[x]$ are nonzero scalars times polynomials $x - c$ with c complex, and the relevant question for R' is how the ideal $(x - c)R'$ decomposes into prime ideals. We can think about this problem algebraically or geometrically. Algebraically, the ideal of all polynomials vanishing at (x_0, y_0) is $I_{(x_0, y_0)} = (x - x_0, y - y_0)$, the set of all $(x - x_0)A(x) - y_0B(x) + yB(x)$ with $A(x)$ and $B(x)$ in $\mathbb{C}[x]$. The intersection with $\mathbb{C}[x]$ consists of all $(x - x_0)A(x)$ and is therefore the principal ideal $(x - x_0)$. We want to factor the ideal $(x - x_0)R'$.

If we pause for a moment and think about the problem geometrically, the answer is fairly clear. Ideals correspond to zero loci with multiplicities. The question is the factorization of the ideal of all polynomials vanishing when $x = x_0$. For most values of the complex number x_0 , there are two choices of the complex y such that (x_0, y) is on the locus since y is given by a quadratic equation, namely $y^2 = (x_0 - 1)x_0(x_0 + 1)$. Thus for most values of x_0 , $(x - x_0)R'$ is the product of two distinct prime ideals. The geometry thus suggests that

$$(x - x_0)R' = (x - x_0, y - y_0)(x - x_0, y + y_0),$$

where $y_0^2 = (x_0 - 1)x_0(x_0 + 1)$ and it is assumed that $y_0 \neq 0$. We can verify this algebraically: The members of the product ideal are the polynomials

$$\begin{aligned} & ((x - x_0)A(x) + (y - y_0)B(x))((x - x_0)C(x) + (y + y_0)D(x)) \\ &= (x - x_0)^2 A(x)C(x) + (x - x_0)(A(x)(y + y_0)D(x) + C(x)(y - y_0)B(x)) \\ & \quad + (y^2 - y_0^2)B(x)D(x). \end{aligned}$$

The last term on the right side is $((x^3 - x) - (x_0^3 - x_0))B(x)D(x)$ and is divisible by $x - x_0$. Therefore every member of the product ideal lies in the principal ideal $(x - x_0)$. On the other hand, the product ideal contains $(x - x_0)(x - x_0)$ and also $(y^2 - y_0^2) = (x^3 - x_0^3) - (x - x_0) = (x - x_0)(x^2 + x x_0 + x_0^2)$. Since $\text{GCD}((x - x_0), (x^2 + x x_0 + x_0^2)) = 1$, the product ideal contains $x - x_0$. Therefore the product ideal equals $(x - x_0)$.

The exceptional values of x_0 are $-1, 0, +1$, where the locus has $y_0 = 0$. The geometry of the factorization is not so clear in this case, but the algebraic

computation remains valid. Thus we have $(x - x_0)R' = (x - x_0, y)^2$ if x_0 equals $-1, 0,$ or $+1$. The conclusion is that the nonzero prime ideals of R' are of two types, with $(x - x_0)R'$ equal to

- the product of two distinct prime ideals in R' if x_0 is not in $\{-1, 0, +1\}$,
- the square of a prime ideal in R' if x_0 is in $\{-1, 0, +1\}$.

The third type, with $(x - x_0)R'$ prime in R' , does not arise. Toward the end of Chapter IX we shall see how we could have anticipated the absence of the third type.

That is enough of a comparison for now. Certain structural results useful in both algebraic number theory and algebraic geometry are needed even before we get started at factoring ideals, and those are some of the topics for the remainder of this chapter. In Section 11 we conclude by establishing unique factorization of ideals for a class of examples that includes the examples above. In the examples above, the rings we considered were $\mathbb{Z}[X]/(X^2 + 5) = \mathbb{Z}[\sqrt{-5}]$ and $\mathbb{C}[x, y]/(y^2 - (x - 1)x(x + 1)) \cong \mathbb{C}[x][\sqrt{(x - 1)x(x + 1)}]$. In each case the notation $[\cdot]$ refers to forming the ring generated by the coefficients and the expression or expressions in brackets.

First we establish a result saying that ideals in the rings of interest are not too wild. For example, in algebraic geometry, one wants to consider the set of restrictions of the members of $\mathbb{K}[X_1, \dots, X_n]$, \mathbb{K} being a field, to the locus of common zeros of a set of polynomials. The general tool will tell us that any ideal in $\mathbb{K}[X_1, \dots, X_n]$ is finitely generated; thus a description of what polynomials vanish on the locus under study is not completely out of the question. The tool is the Hilbert Basis Theorem and is the main result of Section 8.

Second we need a way of understanding, in a more general setting, the relationship that we used in the above examples between \mathbb{Z} and $\mathbb{Z}[\sqrt{-5}]$, and between $\mathbb{C}[x]$ and $\mathbb{C}[x][\sqrt{(x - 1)x(x + 1)}]$. The tool is the notion of integral closure and is the subject of Section 9.

Third we need a way of isolating the behavior of prime ideals, of eliminating the influence of algebraic or geometric factors that have nothing to do with the prime ideal under study. The tool is the notion of localization and is the subject of Section 10.

In Section 11 we make use of these three tools to establish unique factorization of ideals for a class of integral domains known as “Dedekind domains.” It is easy to see that principal ideal domains are Dedekind domains, and we shall show that many other integral domains, including the examples above, are Dedekind domains. A refined theorem producing Dedekind domains will be obtained toward the end of Chapter IX once we have introduced the notion of a “separable” extension of fields.